

JOHANNES VIEHMANN

**ERGÄNZUNGEN ZU „DAS S-NETZWERK UND SEINE
POTENZIELLE WIRTSCHAFTLICHE BEDEUTUNG“**

BERLIN 2018

INHALTSVERZEICHNIS

VORWORT	3
1 ZUSAMMENFASSUNG DER DISSERTATION	4
2 ERGÄNZUNGEN ZUM S-NETZWERK	5
2.1 DAS S-NETZWERK VERTEILUNGSPROBLEM.....	5
2.2 FEINHEITEN DER ROUTENFINDUNG.....	20
2.3 MULTI-PARTITIONS-ROUTING.....	23
2.4 ZUGANGSSICHERHEIT FÜR DIE NUTZER UND SCHUTZ VON GEHEIMNISSEN.....	27
2.5 ERGÄNZUNGEN ZUR ANONYMISIERUNG.....	37
2.5.1 ENTKOPLUNG DER VERSCHIEDENEN AUFGABEN DER ANONYMISIERUNG.....	37
2.5.2 ANONYMES QUANTIFIZIERBARES BEWERTEN UND ABSTIMMEN.....	39
2.6 GESTALTUNG UND ADAPTIERUNG.....	46
2.6.1 AUFBAU, LEGITIMIERUNG UND ORGANISATION.....	46
2.6.2 STANDARDKONFORMITÄT VON IMPLEMENTIERUNGEN.....	53
2.6.3 UMGANG MIT KRITISCHEN EXTERNEN EREIGNISSEN.....	58
2.7 REALISIERUNG IN ÖKOLOGISCHER VERANTWORTUNG.....	63
2.7.1 RESSOURCENVERBRAUCH UND UMWELTBILANZ.....	63
2.7.2 ÖKOLOGISCHE ASPEKTE ZUM BETRIEB DER S-KNOTEN.....	70
2.8 ERGÄNZUNGEN ZUM DEMONSTRATOR.....	75
2.8.1 FORMATE FÜR DEN NACHRICHTENAUSTAUSCH.....	75
2.8.2 MÖGLICHE WEITERE ENTWICKLUNG UND NUTZUNG DES DEMONSTRATORS.....	77
3 ERGÄNZUNGEN ZU DAS S-NETZWERK IN DER WIRTSCHAFT	79
3.1 WIRTSCHAFTLICHE MÖGLICHKEITEN MIT DEM S-NETZWERK.....	79
3.1.1 FAIRE, VERLÄSSLICHE ZUSAMMENARBEIT.....	79
3.1.2 DAS S-NETZWERK ALS PATENTREGISTER.....	82
3.2 PROBLEME IM UMGANG MIT IMMATERIELLEN GÜTERN.....	84
3.3 ENTWICKLUNG VON WIRTSCHAFTSSYSTEMEN.....	88
3.3.1 VOM NATURALGELD BIS ZUM ZEICHENGELD.....	88
3.3.2 RISIKEN VON INFLATION UND DEFLATION	90
3.3.3 UTOPISCHER SOZIALISMUS: FOURIERS PHALANSTÈRE.....	92
3.3.4 STARKE ANONYMITÄT BEI SYSTEMEN OFFENER KONTEN IM S-NETZWERK.....	95
4 VERZEICHNISSE	103
4.1 ABKÜRZUNGEN.....	103
3.1 ABBILDUNGSVERZEICHNIS.....	104
3.2 TABELLENVERZEICHNIS.....	105
3.3 LITERATURVERZEICHNIS.....	106

VORWORT

Die vorliegende Publikation enthält einige Inhalte, die im Zuge meiner Arbeit an meiner Dissertation *Das S-Netzwerk und seine potenzielle wirtschaftliche Bedeutung* an der TU Berlin erschaffen wurden. Diese Inhalte wurden letztlich nicht in die Dissertation selbst aufgenommen, um deren Umfang auf 300 Seiten zu reduzieren.

Der Autor ist jedoch der Meinung, dass diese Inhalte ebenfalls wichtig sind und zu einer umfassenden Darstellung unbedingt dazugehören. Daher wurde hiermit eine externe Publikation geschaffen, auf die aus der Dissertation heraus verwiesen wird.

Für den Leser wurde eine Zusammenfassung der Dissertation in diese Publikation aufgenommen, um das Verständnis zu erleichtern. Dennoch ist diese Ergänzung ohne den Volltext oder andere Publikationen zum Thema S-Netzwerk und Landwirtschaft nur von begrenztem Nutzen. Die Dissertation selbst wird naturgemäß erst nach dieser Publikation veröffentlicht werden, weil aus ihr heraus auf diese Publikation verwiesen wird. Bereits verfügbar sind hingegen z. B. folgende Publikationen:

- Johannes Viehmann: Secure communication with secret sharing in static computer networks with partition in mistrust parties; 2011 Ninth Annual International Conference on Privacy, Security and Trust (PST) Montreal, Quebec, Canada, July 19-21, S.205-212; IEEE 2011
Print-ISBN: 978-1-4577-0582-3; DOI: 10.1109/PST.2011.5971985
http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5971985 (2011-11-14)
- Johannes Viehmann: The Theory of Creating Trust with a Set of Mistrust-Parties and its Exemplary Application for the S-Network; Proceedings of Tenth Annual Conference on Privacy, Security and Trust (PST), Paris (France) 2012, S.185-194; IEEE 2012
Print ISBN: 978-1-4673-2323-9, DOI: 10.1109/PST.2012.6297939
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6297939> (2013-07-22)

Berlin, 4. Dezember 2018

1 ZUSAMMENFASSUNG DER DISSERTATION

Das S-Netzwerk ist konzipiert als eine Plattform, die es ihren Teilnehmern erlaubt, reliable Publikationen und sichere Hinterlegungen zu machen und darauf zuzugreifen. Es kombiniert digitale Langzeitarchivierung in einem Computernetzwerk mit Unleugbarkeit und mit weiteren besonderen Gewährleistungen etwa bezüglich der Zugänglichkeit und der rechtlichen Konsequenzen. Durch das Konzept der Verteilung von Verantwortungen über Misstrauensparteien muss beim S-Netzwerk niemand einzelnen Parteien, Mehrheiten oder anderen Quoren einfach vertrauen. Kooperative Manipulationen werden dabei durch das Misstrauen erschwert, welches durch aktive Tests der Meldepflicht derartiger regelwidriger Kollaborationen geschürt wird. Untragbare, illegale Daten können durch überparteiliche Sperrverfahren in nicht destruktiver Weise auf unleugbar begründeten Zugriff beschränkt werden, ohne dass dies für gemeinschaftliche Manipulationen missbraucht werden kann. Zusammen mit dem Konzept der bidirektionalen verlässlichen Verlinkung im S-Netzwerk, dem S-Web, ergeben sich vielfältige neue Möglichkeiten, auf spezialisierte netzwerkseitige Services zu verzichten und so die operationellen Risiken alleine auf die Korrektheit und Sicherheit des S-Netzwerks zu reduzieren. Zu den aktuellen Entwicklungstrends Cloud und Web of Services bildet das S-Netzwerk gemeinsam mit dem S-Web einen komplementären Gegenentwurf.

Es wird anhand einer Analyse der zu erwartenden Kosten sowie Nutzwerte und Finanzierungsmöglichkeiten gezeigt, dass das S-Netzwerk die für langzeitliche Verfügbarkeit von Daten nötige dauerhafte wirtschaftliche Tragfähigkeit aufweist. Sollte sich das S-Netzwerk etablieren, kann das erhebliche Auswirkungen auf bestehende Geschäftsprozesse, Verwaltungsaufgaben und ganze Industrien haben, insbesondere im Zusammenhang mit beliebig reproduzierbaren immateriellen Gütern. Das S-Netzwerk könnte wegen seiner Verfügbarkeitsgarantien von teuren immaterialgüterrechtlichen Konflikten und Sperrverfahren erdrückt werden. Trotz einiger alternativer Konzepte um mit immateriellen Gütern Geld zu verdienen fehlt noch eine für das S-Netzwerk wünschenswerte Lösung, die restriktive Schutzrechte in der Geldwirtschaft für alle verzichtbar macht.

Mit dem S-Netzwerk als Plattform können auch alternative Wirtschaftsformen wie LETSsysteme und Tauschringe realisiert und eventuell bestehende Skalierungs-, Sicherheits- und Vertrauensprobleme überwunden werden. Die Jadwirtschaft ist als eine neue Alternative zur Geldwirtschaft konzipiert, die mit Jad (Justification, Accounting, Destruction) auf ein Einweg-Bezugsmittel setzt, das nicht frei transferierbar ist. Jad bieten Vorteile insbesondere dort, wo nicht einfach getauscht werden kann, also etwa im Umgang mit beliebig reproduzierbaren Gütern. Die Menge eines nicht frei transferierbaren Bezugsmittels lässt sich leichter steuern. Es reduziert sich die Abhängigkeit von Risikogeschäften wie Krediten und Anleihen, welche im Gegensatz zur Geldwirtschaft in der Jadwirtschaft weder zur Finanzierung der öffentlichen Hand noch zur Steuerung der Menge des Bezugsmittels verwendet werden. Als technische Erfindung kann die Jadwirtschaft parallel zur Geldwirtschaft getestet werden und jeder kann für sich selbst entscheiden, ob er sie nutzen will. Für eine effiziente dezentrale Verwirklichung der Jadwirtschaft wird eine Plattform für reliable Publikationen, sichere Hinterlegungen und verlässliche Verknüpfungen benötigt – eine Plattform wie das S-Netzwerk.

Die interdisziplinäre Dissertation zeigt die technische Machbarkeit von S-Netzwerk, S-Web und Jadwirtschaft anhand eines Demonstrators und sie beleuchtet auch die wirtschaftlichen, rechtlichen, pädagogischen sowie sozialen Aspekte, sodass sie als Ausgangspunkt für weitere Forschungs- und Entwicklungsarbeiten auf dem Weg zur Realisierung der Innovationen dienen kann.

2 ERGÄNZUNGEN ZUM S-NETZWERK

2.1 DAS S-NETZWERK VERTEILUNGSPROBLEM

Die Nutzung von wiederherstellbaren Sicherungskopien zusammen mit Secret Sharing für den Zugriffsschutz bei einer möglichst geringen Zahl an Misstrauensparteien effizient zu gestalten ist ein an sich interessantes kombinatorisches Problem, das *S-Netzwerk Verteilungsproblem*. Dafür werden hier sowohl exakte als auch approximierende Lösungsverfahren vorgestellt.

Die Datenerhaltung beim in der Dissertation gezeigten Ansatz mit Zugriffsschutz durch Secret Sharing mit $N = T = \Psi$ Shares – ohne Verschlüsselungsverfahren mit kurzen Schlüsseln – erfordert pro Share $2 * \Psi - 1$ Sicherungskopien. Zu deren Verteilung werden $\#P = \Psi * (2 * \Psi - 1)$ Misstrauensparteien benötigt. Eine Idee zur Verminderung der notwendigen Anzahl $\#P$ der Misstrauensparteien ist, einen höheren *Threshold* T für das Secret Sharing zu wählen, also $T > \Psi$. Eine größere Zahl von $N = T > \Psi$ Shares braucht zwar noch mehr Speicherplatz. Im Gegenzug wird es jedoch möglich, das für das S-Netzwerk geforderte Schutzniveau mit weniger als $\Psi * (2 * \Psi - 1)$ Misstrauensparteien zu realisieren.

Im Unterschied zum in der Dissertation gezeigten Verfahren mit $T = \Psi$ erhalten bei diesem Ansatz einzelne Misstrauensparteien mehr als einen Share. Die Verteilung der Shares muss dabei so erfolgen, dass jeweils $\Psi - 1$ beliebige P zusammen immer noch mindestens ein Teilstück der Secret Sharing Zerlegung fehlt, um die Daten rekonstruieren zu können. $\Psi - 1$ beliebige P dürfen also zusammen maximal $T - 1$ verschiedene Shares erhalten. Umgekehrt müssen bei Ausfällen oder Fehlern in beliebigen $\Psi - 1$ P die Informationen noch rekonstruierbar und im S-Netzwerk gültig sein, das heißt, es muss auch dann noch jedes der *Threshold* T Shares von mindestens Ψ verschiedenen Misstrauensparteien bestätigt werden.

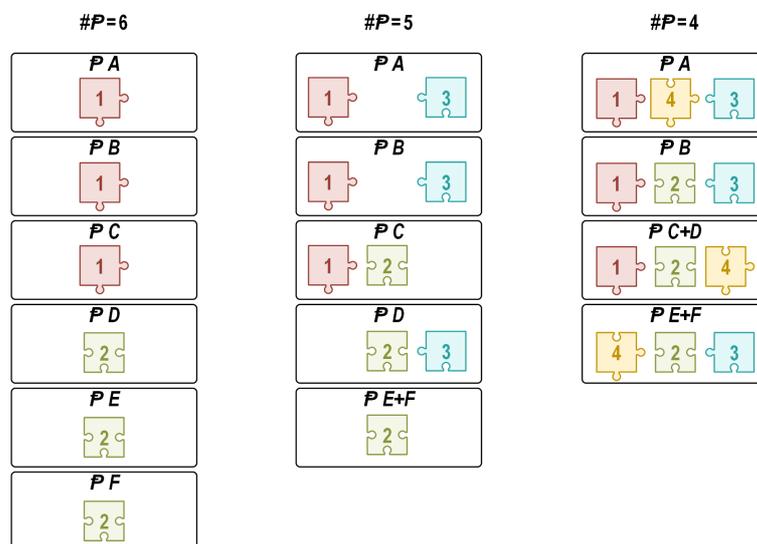


Abbildung 1: Optimale Verteilung der Kopien von Shares mit $\Psi=2$ und verschiedenen Anzahlen $\#P$ von Misstrauensparteien

Abbildung 1 zeigt für $\Psi = 2$, wie auch mit einer reduzierten Anzahl $\#P$ von Misstrauensparteien, die kleiner als $\Psi * (2 * \Psi - 1)$ ist, bei geschickter Verteilung der Kopien von einer erhöhten Zahl von Shares das gleiche Sicherheitsniveau mit dem *Threshold* Ψ erreicht werden kann wie bei $\Psi * (2 * \Psi - 1)$ Misstrauensparteien: Es müssen jeweils mindesten

zwei Misstrauensparteien kooperieren, um das Geheimnis rekonstruieren zu können oder um ein Share manipulieren zu können.

Für $\Psi > 2$ eine optimale Verteilung zu berechnen, sodass mit einer bestimmten Anzahl $\#P$ von Misstrauensparteien und einer möglichst kleinen Secret Sharing Zerlegung das geforderte Sicherheitsniveau erreicht wird, ist eine mathematische Herausforderung. Dieses Problem wird fortan als *S-Netzwerk Verteilungsproblem* bezeichnet.

Darin enthalten ist das bekannte Mengenüberdeckungsproblem (Set Coverage), welches in der Entscheidungsform NP-Vollständig ist [Karp 1972]. Beim Mengenüberdeckungsproblem in der Entscheidungsform geht es darum, für eine Konstante $k \in \mathbb{N}$ zu entscheiden, ob es aus einer Menge S von Teilmengen eines Universums U eine Teilmenge $C \subseteq S$ gibt, sodass die Vereinigung von allen Teilmengen aus C genau U ergibt und C nicht mehr als k Elemente enthält. In der Optimierungsform des Mengenüberdeckungsproblems geht es darum, das kleinste k zu finden, für das eine Überdeckung des ganzen Universums U mit $C \subseteq S$ existiert, bei der C nicht mehr als k Elemente enthält. Die Optimierungsform von Set Coverage ist ebenfalls NP-Hard, liegt aber wahrscheinlich nicht in NP – es ist kein nicht deterministischer Algorithmus polynomialer Laufzeit bekannt, mit dem sich zeigen ließe, dass es keine Lösung mit $k-1$ Elementen geben kann. Gäbe es einen solchen Algorithmus, wäre $NP=co-NP$.

Das *S-Netzwerk Verteilungsproblem* lässt sich mithilfe des Mengenüberdeckungsproblems wie folgt modellieren: Die Menge Z_{N_T} der Shares der Secret Sharing Zerlegung entspricht dem Universum U im Mengenüberdeckungsproblem. Jedes Element der Menge S von Teilmengen eines Universums U beschreibt jeweils für genau eine einzelne Misstrauenspartei, für welche Shares sie zuständig ist.

So betrachtet beinhaltet das *S-Netzwerk Verteilungsproblem* die Bedingung, dass es kein $x \in \mathbb{N} \mid x < \Psi$ geben darf, sodass eine beliebige Vereinigung von x Teilmengen aus S das komplette Universum U ergibt. Anders ausgedrückt: Ψ muss die Lösung k des Mengenüberdeckungsproblems in der Optimierungsform sein.

Im Unterschied zum Mengenüberdeckungsproblem ist jedoch beim *S-Netzwerk Verteilungsproblem* das Universum U nicht vorgegeben. Folglich sind auch die einzelnen Teilmengen in S nicht bekannt. Vorgegeben werden hingegen Ψ und die Anzahl $\#P$ der Teilmengen in S , welche identisch mit der Anzahl der involvierten Misstrauensparteien ist. U muss mindestens Ψ Elemente enthalten und jedes Element aus U muss mindestens in $2*\Psi-1$ verschiedenen Teilmengen aus S vorkommen.

Gesucht sind beim *S-Netzwerk Verteilungsproblem* das minimale Universum U und eine zugehörige Menge S von $\#P$ Teilmengen aus U , für welche Ψ die Lösung des Mengenüberdeckungsproblems in der Optimierungsform ist. Unmittelbar zu dem hier beschriebenen Problem fand sich bei der Recherche zu dieser Arbeit keine Literatur. Im Folgenden wird eine erste Analyse zum *S-Netzwerk Verteilungsproblem* versucht und es werden verschiedene Lösungsverfahren vorgestellt. Dabei werden zunächst exakte Verfahren für kleine Werte entwickelt, welche als Basis für die Entwicklung von weniger Rechenaufwand erfordernden, aber eventuell nicht perfekten Algorithmen dienen sollen.

DIE ANZAHL VON MISSTRAUENS PARTEIEN UND DIE MINIMAL ERFORDERLICHE ANZAHL DER SHARES

Beim *S-Netzwerk Verteilungsproblem* wird die Anzahl $\#P$ der insgesamt zur Verfügung stehenden Misstrauensparteien vorgegeben. Eine Lösung für das *S-Netzwerk Verteilungsproblem* existiert nur genau dann, wenn $\#P$ größer oder gleich $3*\Psi-2$ ist:

Wird bei insgesamt $3*\Psi-3$ oder weniger Misstrauensparteien eine beliebige Teilmenge V der Misstrauensparteien mit $\Psi-1$ Elementen gebildet, gehören maximal $2*\Psi-2$ Misstrauensparteien nicht zu V . Dies sind zu wenige Misstrauensparteien, um einen Share ohne Beteiligung einer Partei aus V zu speichern, denn jedes Element aus U (also jeder Share) muss mindestens in $2*\Psi-1$ verschiedenen Teilmengen (Misstrauensparteien) aus S vorkommen. Die $\Psi-1$ Misstrauensparteien in V erhalten zwangsläufig Kopien aller Shares. Ψ kann folglich nicht die Lösung des Mengenüberdeckungsproblems in der Optimierungsform sein.

Ist die Anzahl $\#P$ der Misstrauensparteien exakt $3*\Psi-2$, gibt es bei jeder beliebigen Teil-

menge V der Misstrauensparteien mit $\Psi-1$ Elementen genau $2*\Psi-1$ andere Misstrauensparteien, die nicht zu V gehören. Die $2*\Psi-1$ Misstrauensparteien, welche nicht zu V gehören, sind hinreichend, um alle notwendigen Kopien eines Shares zu speichern. Wenn alle möglichen Verteilungen der Kopien von Shares über jeweils $2*\Psi-1$ verschiedene Misstrauensparteien genutzt werden, fehlt jeder beliebigen Teilmenge V der Misstrauensparteien mit $\Psi-1$ Elementen genau ein Share. $\Psi-1$ kann also nicht die Lösung des Mengenüberdeckungsproblems in der Optimierungsform sein. Andererseits hat jede beliebige Teilmenge W der Misstrauensparteien mit Ψ Elementen zwingend alle Shares, denn die $2*\Psi-2$ Misstrauensparteien, die nicht zu W gehören, genügen nicht, um die geforderte Verteilung der $2*\Psi-1$ Kopien eines Share zu realisieren. Für $3*\Psi-2$ Misstrauensparteien gibt es daher eine Lösung Ψ des Mengenüberdeckungsproblems in der Optimierungsform. Die optimale Lösung und mithin auch die Lösung des *S-Netzwerk Verteilungsproblems* enthält alle möglichen Verteilungen von Shares mit jeweils $2*\Psi-1$ Kopien, wobei jeder Share genau einer Koalition von $\Psi-1$ Misstrauensparteien fehlt. Die Anzahl $\#U$ der bei $\#P=3*\Psi-2$ minimal erforderlichen Shares lässt sich mit dem Binomialkoeffizienten ausrechnen.

$$\#U = \binom{\#P}{2*\Psi-1} = \binom{\#P}{\Psi-1} \quad |\#P=3*\Psi-2$$

Die gleiche Verteilung von Shares über $3*\Psi-2$ Misstrauensparteien führt auch bei insgesamt mehr als $3*\Psi-2$ Misstrauensparteien dazu, dass Ψ wiederum die Lösung des Mengenüberdeckungsproblems in der Optimierungsform ist. Allerdings gibt es mit zusätzlichen Misstrauensparteien bessere Lösungen, die mit weniger Shares auskommen.

Jeder Share, dessen Kopien über $2*\Psi-1$ Misstrauensparteien verteilt werden, fehlt genau in

$$\binom{\#P-(2*\Psi-1)}{\Psi-1}$$

Koalitionen von $\Psi-1$ Misstrauensparteien. Da jeder möglichen Koalition von $\Psi-1$ Misstrauensparteien wenigstens ein Share fehlen muss, gilt für die Anzahl $\#U$ der mindestens benötigten Shares folgende untere Grenze:

$$\#U \geq \binom{\#P}{\Psi-1} \div \binom{\#P-(2*\Psi-1)}{\Psi-1}$$

Diese untere Grenze wird bei $\#P=3*\Psi-2$ tatsächlich erreicht.

BRUTE-FORCE UND DIE KOMPLEXITÄT DES S-NETZWERK VERTEILUNGSPROBLEMS

Wie bei vielen anderen kombinatorischen und graphentheoretischen Problemen lässt sich für das *S-Netzwerk Verteilungsproblem* relativ einfach ein exakter Algorithmus angeben, mit dem sich alle optimalen Lösungen berechnen ließen, wenn unbegrenzte Rechenleistung und Speicherkapazität zur Verfügung stünden.

Für das S-Netzwerk Verteilungsproblem sieht ein solcher Algorithmus für gegebenes Ψ und $\#P$ wie folgt aus:

- 1 Es sei $\#U = \Psi$;
- 2 Es sei $U = \{ 0, 1, \dots, \#U-1 \}$
- 3 Für jede mögliche Menge S , deren $\#P$ Elemente jeweils Teilmengen von U sind, sodass jedes Element aus U in mindestens $2*\Psi-1$ verschiedenen Teilmengen aus S vorkommt:
 - 3.1 Prüfe für jede mögliche Vereinigung V von $\Psi-1$ Elementen aus S , ob die Vereinigung V das Universum U ergibt.
 - 3.2 Wenn keine Vereinigung V von $\Psi-1$ Elementen aus S das Universum U ergibt und mindestens eine Vereinigung W von Ψ Elementen aus S das Universum U ergibt, sind U und S eine optimale Lösung des *S-Netzwerk Verteilungsproblems* für Ψ und $\#P$.
Ende des Verfahrens.
- 4 Setze $\#U = \#U+1$. Weiter mit Schritt 2.

Praktisch anwendbar ist dieses simple Brute-Force-Verfahren nur für sehr kleine Werte Ψ und $\#P$. Um zu zeigen, wie hoch der Aufwand ist und auch als anschauliche Basis für die weiteren Betrachtungen, bietet es sich an, Schritt 3 mithilfe der Graphentheorie darzustellen.

Die Menge S lässt sich gut als bipartiter Graph modellieren: die $\#U$ Elemente des Universums U sind die Ecken der einen Partitionsklasse, die $\#P$ Elemente der Menge S sind die Ecken der anderen Partitionsklasse. Mithilfe von Kanten lässt sich dann modellieren, welche Elemente aus U zu einer bestimmten Teilmenge aus S gehören.

Eine bekannte kompakte Darstellungsform für Graphen sind die Adjazenzmatrizen, deren Zeilen und Spalten die Ecken repräsentieren und deren Einträge die Werte null oder eins annehmen können. Zwischen einer Ecke, die durch die Zeile Y repräsentiert wird und einer Ecke, welche durch die Spalte X repräsentiert wird, gibt es genau dann eine Kante, wenn der Eintrag an der Stelle Zeile Y , Spalte X in der Adjazenzmatrix den Wert eins hat. Für einen bipartiten Graphen genügt eine Adjazenzmatrix, bei der in den Zeilen nur die Ecken der einen Partitionsklasse und in den Spalten nur die Ecken der anderen Partitionsklasse aufscheinen, da jede Kante eines bipartiten Graphens jeweils eine Ecke aus der einen Partitionsklasse mit einer Ecke aus der anderen Partitionsklasse verbinden muss. Hier ist also eine Darstellung jeder Menge S als $\#U \times \#P$ Adjazenzmatrix möglich. Da jeder Eintrag der Adjazenzmatrix entweder null oder eins sein muss, gibt es insgesamt $2^{\#U \times \#P}$ verschiedene Adjazenzmatrizen. Die Anzahl $\#V$ der für jede einzelne der $2^{\#U \times \#P}$ Mengen S in Schritt 3.1 jeweils zu prüfenden Vereinigungen V entspricht genau der Anzahl der $\Psi-1$ -elementigen Teilmengen aus S und lässt sich folglich mithilfe des Binomialkoeffizienten berechnen:

$$\#V = \binom{\#P}{\Psi-1}$$

Schon bei $\Psi = 3$ und $\#P = 8$ treten für $\#U$ Werte bis 11 auf – bei $\#U = 10$ gibt es keine Lösung und es wäre für $\#U = 3$ bis $\#U = 10$ jeweils ein kompletter Durchlauf durch alle damit möglichen Mengen S erforderlich, zusätzlich für $\#U = 11$ ein Durchlauf bis zum Finden der Lösungen S und U . Alleine schon für die 2^{80} verschiedenen Mengen S bei $\#U = 10$ jeweils zu prüfen, ob jedes Element aus U in mindestens $2*\Psi-1$ verschiedenen Teilmengen aus S vorkommt und wenn ja die $\#V = 28$ Prüfungen von Schritt 3.1 durchzuführen ist nicht praktikabel.

Es ist jedoch möglich, effizientere exakte Algorithmen zu entwickeln, denn viele erzeugbare Mengen S kommen gar nicht als Lösung des S-Netzwerk Verteilungsproblems infrage, etwa weil sie die Bedingung, dass jedes Element aus U mindestens $2*\Psi-1$ – mal in verschiedenen Teilmengen von S vorkommen muss, nicht erfüllen. Es bietet sich an, zu versuchen, sofort nur solche Mengen S zu generieren, welche keine derartigen Bedingungen verletzen.

Außerdem sind nicht alle möglichen Mengen S wirklich verschieden voneinander – viele sind isomorph und unterscheiden sich nur durch die Bezeichnungen der Elemente. Durch passende Umbenennungen – bei der Darstellung als Adjazenzmatrix durch Permutationen von Zeilen und Spalten, gegebenenfalls durch Transposition – lassen sich einige Mengen S ineinander überführen. Anschaulich wird das bei der Betrachtung als gezeichnete Graphen mit Ecken und Kanten: Je nachdem wo die Ecken positioniert werden, können Graphen sehr verschieden aussehen, und trotzdem zueinander isomorph sein, also durch das Verschieben von Ecken unter Beibehaltung der Kanten ineinander überführt werden.

Für die Lösung des *S-Netzwerk Verteilungsproblems* spielen Darstellungsformen und Bezeichnungen keine Rolle – in dem vorgestellten Algorithmus kommen sie nicht vor. Dementsprechend genügt es, für jede Isomorphieklasse, genau einen Repräsentanten zu erzeugen und nur diesen den Prüfungen von Schritt 3 zu unterziehen. Es ist naheliegend, zu versuchen, die Generierung von zueinander isomorphen Mengen S zu vermeiden.

Im Folgenden sollen diese Ansätze kombiniert werden, um einen besseren Algorithmus

zur exakten Lösung des S-Netzwerk Verteilungsproblems zu entwickeln.

EFFIZIENTE EXAKTE LÖSUNGSVERFAHREN FÜR DAS S-NETZWERK VERTEILUNGSPROBLEM

Zur Isomorphie von Graphen besteht eine umfangreiche Literatur. Das Entscheidungsproblem, ob zwei Graphen zueinander isomorph sind, wurde insbesondere im Zusammenhang mit der Komplexitätstheorie intensiv erforscht [Köbler 1993]. Es gibt auch bereits viele Publikationen und Tools zur allgemeinen Generierung von nicht isomorphen Graphen. Einen Überblick liefern [McKay 1998] und [McKay 2014].

DIE SUCHE NACH ANPASSBAREN GENERATOREN FÜR NICHT ISOMORPHE BIPARTITE GRAPHEN

Eigentlich sollte für die Lösung des *S-Netzwerk Verteilungsproblems* zur Generierung von nicht isomorphen bipartiten Graphen ein bestehendes Tool oder zumindest ein etabliertes Verfahren aus der Literatur zur Anwendung kommen. Einige der bekannten Tools zur allgemeinen Generierung nicht isomorpher Graphen ließen sich eventuell auch für die effiziente Erzeugung bipartiter nicht isomorpher Graphen nutzen. Für das *S-Netzwerk Verteilungsproblem* sollen auch weitere Bedingungen zur Einschränkung der zu generierenden Graphen berücksichtigt werden können. Daher sollte der Ausgangspunkt möglichst verständlich und anpassbar sein. Bestehende Tools zur allgemeinen Generierung nicht isomorpher Graphen entsprechend zu modifizieren dürfte schwierig sein, da diese nicht auf Klarheit, sondern auf Geschwindigkeit optimiert werden: *“The emphasis is on the power of the algorithm for solving practical problems, rather than on the theoretical niceties of the algorithm.”*, zitiert aus [McKay 1981].

Eine spezialisierte, dafür möglichst verständliche Lösung für die Generierung nicht isomorpher bipartiter Graphen, wäre ein besserer Ausgangspunkt. Es fand sich jedoch nur sehr wenig Literatur zu diesem Thema. Das ist durchaus überraschend, da bipartite Graphen in der Praxis etwa bei vielen Zuordnungsproblemen eine wichtige Rolle spielen.

Insgesamt wurden nur zwei Publikationen unmittelbar zum Generieren von nicht isomorphen bipartiten Graphen gefunden: [Acketa 1991] und [Ramos 2012]. Das zweite in [Acketa 1991] vorgestellte Verfahren wird hier aufgrund der Klarheit als Ausgangspunkt verwendet. (Hinweis: Bei der Angabe des Algorithmus in [Acketa 1991] fehlt der rekursive Aufruf der Prozedur `Construct_2` innerhalb derselben Prozedur – die gezeigten Ergebnisse sind korrekt, sodass sich der Fehler wohl nur im Pseudocode findet). Dieses Verfahren nutzt eine quasi kanonische Repräsentation (canonical Labeling, zu den verschiedenen Ansätzen wie canonical Labeling und canonical Construction siehe auch [McKay 1998]), nämlich den maximalen Code der Adjazenzmatrix bei fixierten Anzahlen von Einsen in den Zeilen. Dabei darf die Anzahl der Einsen in einer tieferen Zeile der Matrix nicht größer sein als in einer der darüber liegenden Zeilen. Der Code der Matrix ist die Folge aus Nullen und Einsen, die sich ergibt, wenn alle Einträge zeilenweise und von links nach rechts hintereinandergeschrieben werden. Als Ordnung über die Codes dient der Größenvergleich der Binärzahlen, als welche die Codes von Matrizen betrachtet werden können. Der Code ist Maximal, wenn es keine Permutation der Spalten und der Zeilen der Matrix mit einem größeren Code gibt, wobei nur solche Permutationen zu berücksichtigen sind, bei welchen die Anzahlen von Einsen in den Zeilen jeweils erhalten bleiben. Ist die Matrix quadratisch, so muss der Code zusätzlich auch maximal gegenüber der transponierten Matrix sein.

Der Hauptnachteil des Verfahrens ist, dass eine sehr große Anzahl von Matrizen generiert werden muss – die nicht kanonischen Matrizen werden erst anschließend aussortiert. Dadurch, dass nur Matrizen mit monoton absteigender Anzahl von Einsen in den Zeilen generiert werden, werden zwar nicht alle $2^{M \times N}$ Matrizen mit M Zeilen und N Spalten erzeugt, aber immer noch sehr viele isomorphe Matrizen. Die Prüfung, ob eine Matrix kanonisch ist, erzeugt außerdem durch verschachtelte Permutationen von Spalten und Zeilen einen sehr hohen Rechenaufwand. In [Acketa 1991] werden bereits einige Gedanken zur möglichen Beschleunigung skizziert, außerdem ist es möglich, die Permutationen auf bestimmte Bereiche der Adjazenzmatrix zu beschränken.

Konsequent weitergedacht lässt sich aus diesem Verfahren mit quasi kanonischer Repräsentation auch ein Verfahren zur zumindest teilweise direkten kanonischen Konstruktion der nicht isomorphen bipartiten Graphen entwickeln. In [Ramos 2012] wird wohl eine ähnliche Form der kanonischen Konstruktion versucht – der angegebene Algorithmus konnte jedoch weder nach der Beschreibung noch nach dem von der Beschreibung abweichenden Pseudocode so implementiert werden, dass er korrekte Ergebnisse liefert.

Bei dem hier vorgestellten Verfahren zur Generation nicht isomorpher bipartiter Graphen mit kanonischer Konstruktion wird dieselbe quasi kanonische Darstellung wie im zweiten Verfahren aus [Acketa 1991] verwendet, also der maximale Code der Adjazenzmatrix mit absteigend fixierten Anzahlen der Einsen in den Zeilen der Matrix. Allerdings wird zur Lösung des S-Netzwerk-Verteilungsproblems versucht, sofort möglichst nur jene Matrizen zu generieren, die kanonisch anmuten und passen könnten.

Konkret werden Matrizen mit M Zeilen und N Spalten bei diesem Verfahren sofort so konstruiert, dass sich ihr Code alleine durch Spaltenpermutationen nicht mehr vergrößern kann. Dazu wird zeilenweise ermittelt, welche Positionen die Einsen einnehmen können und welche Spaltenpermutationen in einer unterhalb gelegenen Zeile noch möglich sind, sodass der Code in der aktuellen oder einer höheren Zeile nicht kleiner wird.

In der ersten Zeile gibt es bei vorgegebener Anzahl F_0 der Einsen für diese Zeile nur genau eine Anordnung der Einsen, die nicht durch Spaltenpermutationen vergrößert werden könnte: Die ersten F_0 Spalten erhalten den Wert eins. Für die darunterliegenden Zeilen bedeutet das, dass nur Permutationen innerhalb der ersten F_0 Spalten sowie innerhalb der letzten $N - F_0$ Spalten einen größeren Code erzielen könnten, denn jede andere Spaltenpermutation führt zu einer kleineren ersten Zeile und mithin zu einem kleineren Code. F_0 bildet eine Grenze. Für die nächste Zeile mit F_1 der Einsen gibt es daher nicht nur die Möglichkeit, die ersten F_1 Spalten gleich eins zu setzen, sondern es können auch die ersten $F_1 - X$ Spalten und ab dem Index F_0 weitere X Spalten gleich eins gesetzt werden, ohne dass eine beliebige Spaltenpermutation einen größeren Code produzieren könnte. Das X kann ganzzahlige Werte zwischen 0 sowie dem Minimum aus F_1 und $N - F_0$ annehmen. Für die nächste Zeile sind demnach die Grenzen der möglicherweise einen größeren Code produzierenden Spaltenpermutationen jeweils $F_1 - X$, F_0 und $F_0 + X$. Wird die erste Spalte als initiale Grenze betrachtet, so kann sich mit jeder weiteren Zeile die Anzahl der Grenzen maximal verdoppeln.

Für den Fall, dass jede der M Zeilen der Matrix jeweils eine von allen anderen Zeilen verschiedene Anzahl von Einsen hat, gelingt es mit diesem Verfahren sogar, direkt und genau nur alle kanonischen Matrizen zu erzeugen – es ist also im Idealfall keine Prüfung mehr erforderlich, ob Permutationen der M Zeilen oder der N Spalten der Matrix zu einem höheren Code führen könnten.

Wenn mehrere Zeilen dieselbe Anzahl von Einsen aufweisen, genügt dieses Verfahren für sich genommen jedoch nicht, um sicherzustellen, dass die erzeugten Matrizen auch kanonisch sind. Der Grund ist, dass die Reihen mit identischer Anzahl von Einsen permutiert werden können, ohne die Isomorphieklasse zu verlassen. Wenn zwei oder mehr Zeilen übereinander dieselbe Anzahl von Einsen aufweisen, so könnte theoretisch das in [Acketa 1991] präsentierte Verfahren genutzt werden, um zu prüfen, ob mit einer Zeilenpermutation und Spaltenpermutation ein größerer Code produziert werden kann. Dabei werden einfach alle Permutationen generiert und durchprobiert.

Mit der für die quasi kanonische Konstruktion der Zeilen genutzten Idee der Grenzen für die möglichen Spaltenpermutationen lässt sich jedoch ein effizienteres Verfahren entwickeln. Nur die Zeilen mit identischer Anzahl von Einsen werden permutiert. Anstatt für jede Zeilenpermutation alle möglichen Spaltenpermutationen tatsächlich zu generieren und zu durchlaufen, werden nur die Segmente erfasst, in denen Spalten vertauscht werden können. In diesen Segmenten wird dann jeweils in der nächsten Zeile überprüft, ob sich ein größerer Wert als in der unpermutierten Matrix erzeugen ließe. Dazu genügt es, jeweils die Zahl der Einsen in den Segmenten zu zählen, beginnend beim ersten Segment. Hat die permutierte Zeile im zu prüfenden Segment mehr Einsen, ist die unpermutierte Matrix nicht kanonisch und sie kann verworfen werden. Lässt sich in der permutierten Zeile nur ein kleinerer Wert erzeugen, so brauchen nachfolgende Segmente und Zeilen nicht mehr geprüft zu werden, da der Code der Matrix in jedem Fall kleiner wird. Die unpermutierte Matrix könnte also kanonisch sein. Wenn alle Segmente einer permutierten Zeile gleich den Segmenten der entsprechenden Zeile der unpermutierten Matrix sind, so ist mit der

nächsten Zeile und den für diese je nach den Grenzen der Nullen und Einsen verfeinerten Segmenten fortzufahren.

Diese Form der Prüfung, ob die Matrix kanonisch ist, ist zwar immer noch aufwendig, sie erspart aber bereits die Generierung von $N!$ Spaltenpermutationen und Zeilenpermutationen werden nur für Zeilen mit identischen Anzahlen von Einsen durchgeführt. Derartige Zeilen bringen also einen höheren Rechenaufwand mit sich.

Bei jenen Zeilen, welche dieselbe Anzahl von Einsen haben, kann die kanonische Konstruktion folgendermaßen beschleunigt werden: Es bietet sich an, für die tiefer liegenden dieser Zeilen sofort nur jene Folgen von Einsen und Nullen zu erzeugen, die keinen größeren Code haben als die darüber liegenden Zeilen, denn diese Zeilen können untereinander ja beliebig permutiert werden.

Das hier vorgestellte Verfahren zur kanonischen Konstruktion lässt sich leicht an Anforderungen etwa bezüglich der Zeilensummen und Spaltensummen in der Matrix anpassen. Für die nachfolgend präsentierten Messungen wurden ausschließlich Graphen ohne isolierte Ecken erzeugt, also nur solche, bei deren Adjazenzmatrix keine Zeilensumme und keine Spaltensumme gleich null ist. Die Tabelle 1 liefert einen Performance-Vergleich der Generierung nicht isomorpher bipartiter Graphen zwischen dem Verfahren mit quasi kanonischer Repräsentation und dem Verfahren mit quasi kanonischer Konstruktion, wobei jeweils eigene Implementierungen in C#.Net 4.5 getestet wurden und für den Vergleich immer nur ein Prozessorkern auf einem iCore 7 820 Q Prozessor unter Windows 8.1 64 Bit genutzt wurde.

M	N	Anzahl der Isomorphieklassen ohne isolierte Ecken	Dauer kanonische Repräsentation	Dauer kanonische Konstruktion
3	4	42	20 ms	12 ms
4	3	42	20 ms	12 ms
4	4	115	285 ms	36 ms
4	7	5.745	168.333 ms	141 ms
7	4	5.745	75.292 ms	604 ms
5	6	20.755	605.022 ms	650 ms
6	5	20.755	539.190 ms	1.000 ms

Tabelle 1: Nicht isomorphe bipartite Graphen erzeugende Verfahren im Vergleich

Die Implementierungen beider Verfahren zur allgemeinen Generierung nicht isomorpher bipartiter Graphen wurden beide gleichermaßen nicht speziell auf Performance optimiert. Hier soll es darum gehen, nur die möglichen Lösungen des *S-Netzwerk Verteilungsproblems* effizient generieren zu können.

Zur Optimierung des Generators für das *S-Netzwerk Verteilungsproblem* sind folgende Anpassungen möglich: Werden die Shares in den Zeilen der Matrix modelliert, so kann die Anzahl der Einsen für jede Zeile auf den gleichen Wert festgelegt werden, nämlich auf $2*\Psi-1$, also auf die Anzahl der Sicherheitskopien pro Share. Außerdem kann von vorneherein auf die Generierung all jener Graphen verzichtet werden, die identische Zeilen haben. Schließlich darf bei Modellierung der $\#U$ Shares in den Zeilen der Matrix keine Spalte mehr als $\#U-\Psi+1$ Einsen enthalten, denn sonst würden mindestens einer der als Spalte modellierten Misstrauensparteien weniger als $\Psi-1$ Shares fehlen.

Für das *S-Netzwerk Verteilungsproblem* müssen weiters nicht die kompletten Prüfungen aller Zeilenpermutationen durchgeführt werden. Der Exaktheit des Lösungsverfahrens tut es keinen Abbruch, wenn anstelle von genau einem Repräsentanten pro Isomorphieklasse mindestens ein Repräsentant pro Isomorphieklasse geprüft wird. Vom Rechenaufwand her ist es eventuell besser, bei der zeilenweisen Konstruktion nur die ersten Zeilen zu permutieren, denn dabei ist die Zahl der Permutationen relativ gering. Zugleich kann die Konstruktion vieler folgender Zeilen mit relativ wenig Aufwand verhindert werden.

Tabelle 2 zeigt die Auswirkung der Anzahl der Zeilen, welche maximal permutiert und geprüft werden, auf die Laufzeit des Verfahrens zur kanonischen Konstruktion, wobei hier nur Graphen mit Eigenschaften, wie sie für das S-Netzwerk bei einem bestimmten Wert für

Ψ auftreten können, generiert wurden. Die Messwerte stammen von einem iCore 7 820 Q Prozessor unter Windows 8.1 64 Bit. Hier wurde die Implementierung auf Ausführungsgeschwindigkeit optimiert um gerade auch parallele Rechenkapazitäten nutzen zu können und es wurde jeweils gleichzeitig auf allen acht Prozessorkernen gerechnet.

M	N	Ψ	Ohne Permutation		$M-3$ Zeilen mit Permutation		$M-2$ Zeilen mit Permutation		$M-1$ Zeilen mit Permutation		M Zeilen mit Permutation	
			Anzahl	Zeit	Anzahl	Zeit	Anzahl	Zeit	Anzahl	Zeit	Anzahl	Zeit
6	10	3	1.691.082	1,75 s	1.006.575	0,75 s	252.068	0,24 s	66.778	2,21 s	34.433	17,98 s
8	9	3	324.396.816	159,51 s	16.612.478	10,41 s	6.064.250	9,82 s	2.706.888	166,95 s	1.983.800	3.666,29 s
7	13	4	106.637.330	2.781,13 s	10.341.078	137,97 s	2.821.970	48,23 s	1.242.063	548,94 s	614.076	2.259,24 s

Tabelle 2: Unschärfe quasi kanonische Konstruktion für das S -Netzwerk Verteilungsproblem

Selbst mit den genannten Optimierungen ist das gezeigte exakte Verfahren bei $\Psi = 4$ mit 20 oder weniger Misstrauensparteien ($\#P \leq 20$) bereits so aufwendig, dass hierfür bisher noch keine erfolgreichen Brute-Force-Berechnungen durchgeführt wurden. Mit weiteren Verbesserungen der Implementierung und mit dem Einsatz von massiver Rechenleistung mag es beim gegenwärtigen Stand der Technik für $\Psi = 5$ noch für jede relevante Anzahl von Misstrauensparteien möglich sein, das hier vorgestellte exakte Verfahren anzuwenden. Zumindest ab $\Psi = 6$ werden jedoch andere effizientere Lösungsverfahren zwingend erforderlich sein.

NÄHERUNGSVERFAHREN MIT LOKALER OPTIMIERUNG FÜR DAS S -NETZWERK VERTEILUNGSPROBLEM

Eine Möglichkeit, um Berechnungen bei Optimierungsproblemen durchführen zu können, wenn exakte Verfahren zu aufwendig scheinen, besteht darin, sich mit möglichst guten Lösungen zu begnügen, die hoffentlich mit weniger Rechenaufwand zu ermitteln sind und die zweifelsfrei korrekt sind, die aber eventuell nicht ganz optimal sind.

Um solche näherungsweise Optimierungsverfahren finden zu können, bietet es sich allgemein an, auf eine globale Optimierung zu verzichten und stattdessen zu versuchen, lokale, einfacher berechenbare Optimierungskriterien für einzelne Teile der zu generierenden Lösung zu identifizieren und aus den so erzeugten Teillösungen schrittweise eine Komplettlösung zu entwickeln. Für das S -Netzwerk Verteilungsproblem kann ein derartiges Verfahren damit beginnen, $2 \cdot \Psi - 1$ Kopien eines ersten Shares willkürlich an die erforderliche Anzahl von $2 \cdot \Psi - 1$ verschiedenen Misstrauensparteien zu verteilen. Die Verteilungen der weiteren Shares werden in einem iterativen Prozess der Reihe nach berechnet, wobei jeweils nur für den folgenden Share eine Verteilung über die Misstrauensparteien mit bestimmten Eigenschaften gesucht wird – ohne die möglichen Verteilungen etwaig erforderlicher weiterer Shares zu berücksichtigen.

Es stellt sich die Frage, nach welchen Kriterien dabei jeweils die Verteilung des nächsten Shares gewählt werden sollte, also welche Eigenschaften die nächste Verteilung haben sollte. Der Algorithmus, mit welchem in dem exakten Verfahren geprüft wird, ob eine Lösung für das S -Netzwerk Verteilungsproblem gefunden wurde, kann als Ausgangspunkt für die Entwicklung eines Verfahrens zur Verteilung des nächsten Shares bei einem iterativen Konstruktionsverfahren dienen. Die Idee dazu ist, die Menge V aller $\Psi - 1$ elementigen Teilmengen der Misstrauensparteien zu bilden und dann zu versuchen, mit der Verteilung des nächsten Shares dafür zu sorgen, dass möglichst viele der Teilmengen in V den neuen Share nicht erhalten. Die Misstrauensparteien einer jeden Teilmenge aus V , welche den neuen Share nicht erhalten haben, können das Geheimnis nicht ohne die Hilfe weiterer Parteien aufdecken. Für die nächste Runde des Verfahrens können alle Teilmengen aus V entfernt werden, die nicht alle bisher verteilten Shares erhalten haben. Wenn die Menge V leer ist, wurde eine Lösung des S -Netzwerk Verteilungsproblems gefunden.

Selbst dieses Näherungsverfahren ist sehr aufwendig. Die Zahl $\#V$ der $\Psi - 1$ elementigen Teilmengen der $\#P$ Misstrauensparteien lässt sich mit dem Binomialkoeffizienten berechnen:

$$\#V = \binom{\#P}{\Psi-1}$$

DIE SCHWIERIGKEIT DER LOKALEN OPTIMIERUNG

Eine optimale Verteilung des nächsten Shares zu finden, durch welche die maximal mögliche Anzahl an Teilmengen aus V ausgeschlossen wird, ist für sich wiederum ein schwieriges Problem. Jedes Share wird an $2*\Psi-1$ Misstrauensparteien verteilt. Es erhalten also in jeder Runde genau $\#P-(2*\Psi-1)$ Misstrauensparteien den neuen Share nicht. Gesucht ist also die $\#P-(2*\Psi-1)$ elementige Teilmenge aus den Misstrauensparteien, in welcher die meisten Elemente aus V enthalten sind. Anstatt die Komplemente der $\#P$ über $2*\Psi-1$ möglichen Verteilungen zu bilden und für jede einzelne dieser Mengen die darin enthaltenen Elemente aus V zu zählen, bietet es sich an, ein weiteres Näherungsverfahren einzusetzen. Dabei soll die Menge der Misstrauensparteien, welche das nächste Share nicht bekommt, schrittweise gebildet werden. Zunächst wird dazu eine Menge D aus V ausgewählt. Dann wird solange bis D genau $\#P-(2*\Psi-1)$ Elemente enthält das D mit jeweils jener Teilmenge aus V vereint, mit welcher zusammen die meisten weiteren Teilmengen aus V im Verhältnis zur Anzahl der disjunkten Elemente überdeckt werden.

Nachfolgend sind die wichtigsten Schritte des Näherungsverfahrens aufgeführt:

- 1 Wähle und speichere eine beliebige Verteilung der $2*\Psi-1$ Kopien vom ersten Share an $2*\Psi-1$ verschiedene Misstrauensparteien. Es sei D die Menge der Misstrauensparteien, die das erste Share nicht erhalten.
- 2 Erzeuge die Menge V aller $\Psi-1$ elementigen Teilmengen der Misstrauensparteien, welche nicht in D liegen.
- 3 Wenn V leer ist, sind die bisher ermittelten Verteilungen für Kopien von Shares eine Lösung und das Verfahren endet.
- 4 Suche nach der Verteilung des nächsten Shares:
 - 4.1 Das D erhält als neuen Wert eine Teilmenge X aus V .
 - 4.2 Entferne jede Teilmenge aus V , welche in D liegt.
 - 4.3 Es sei $\#D$ die Anzahl der Misstrauensparteien, die D enthält. Wenn $\#D$ kleiner als $\#P-(2*\Psi-1)$ ist, wird D mit jener Teilmenge X aus V vereint, für die $X \cup D$ die maximale Anzahl von Teilmengen aus V im Verhältnis zur Anzahl der Elemente von $X \setminus D$ enthält und für die $X \cup D$ maximal $\#P-(2*\Psi-1)$ Elemente hat. Weiter mit Schritt 4.2.
 - 4.4 Speichere die Misstrauensparteien, welche nicht in D enthalten sind, als Verteilung für die Kopien des nächsten Shares. Weiter mit Schritt 3.

Neben dem Rechenaufwand ist auch die Qualität der globalen Optimierung, welche sich mithilfe einer lokalen Optimierung erzielen lässt, problematisch: Bei der Näherung nach dem angegebenen Verfahren werden die Kopien der ersten Shares flach verteilt werden: Ehr nicht jeder P mindestens eine Kopie eines Shares zugewiesen wurde, bekommt keine P mehr als eine Kopie von nur einem Share zugeteilt. Es findet also anfangs keine Überlappung bei der Verteilung statt. Optimale Lösungen weisen hingegen oft eine weitgehende Überlappung bei der Verteilung der Kopien aller Shares auf. Bessere Ergebnisse lassen sich erzielen, wenn die ersten Shares nicht nach der Näherungsformel verteilt werden, sondern stattdessen verschiedene Überlappungen durchprobiert werden.

Näherungsverfahren mit lokaler Optimierung können im Prinzip jede Lösung liefern, die es überhaupt gibt. In der Praxis erweist es sich jedoch sehr schwierig, ein hinreichend effizientes und qualitativ hochwertiges lokales Optimierungsverfahren für das S-Netzwerk-Verteilungsproblem zu entwickeln. Mit dem hier gezeigten Algorithmus können bis zu $\Psi = 6$ auf den derzeit üblichen Computern Näherungslösungen von mäßiger Qualität für die minimal erforderliche Größe der Secret Sharing Zerlegung und für die optimale Verteilung der Shares berechnet werden. Der Speicherbedarf für die $\#P$ über $\Psi-1=6$ Teilmengen erreicht dabei bereits die Größenordnung von Gigabytes. Um auch für *Thresholds* mit Werten von $\Psi \geq 7$ alle relevanten Lösungen berechnen zu können, müssen effizientere Verfahren gefunden werden.

EFFIZIENTE VERFAHREN FÜR SPEZIALFÄLLE DES S-NETZWERK VERTEILUNGSPROBLEMS

Für Spezialfälle des *S-Netzwerk Verteilungsproblems* lassen sich Lösungsverfahren ent-

wickeln, die ein Laufzeitverhalten aufweisen, welches ihre Anwendung auch für große Ψ erlaubt. Ein Beispiel für einen solchen Sonderfall ist $\#P=3*\Psi-2$, denn dabei werden alle möglichen Verteilungen von $2*\Psi-1$ Kopien eines Shares zwingend benötigt (siehe Kasten „Die Anzahl von Misstrauensparteien und die minimal erforderliche Anzahl der Shares“, Seite 6).

Ein weiterer Sonderfall, bei dem leicht optimale Lösungen berechnet werden können, ist der, dass der zu gewährleistende *Threshold* für den Zugriff nur maximal zwei beträgt. Dies lässt sich nutzen, um nicht nur Lösungen für $\Psi=2$ zu berechnen, sondern auch für beliebige $\Psi > 2$. Die Idee dazu ist, die Menge S der Misstrauensparteien in mehrere disjunkte Teilmengen aufzuteilen, also eine Partition zu erzeugen. Kopien von Shares werden jeweils nur in einer dieser Teilmengen verteilt. Dabei werden die Shares so verteilt, dass aus jeder Teilmenge mindestens eine Partei oder auch mindestens zwei Parteien benötigt werden, um das Geheimnis rekonstruieren zu können – und zwar insgesamt Ψ Parteien. Für einige der Teilmengen wird also eine optimale Verteilung mit dem *Threshold* zwei für den Zugriff berechnet, andere erhalten eventuell nur einen Share.

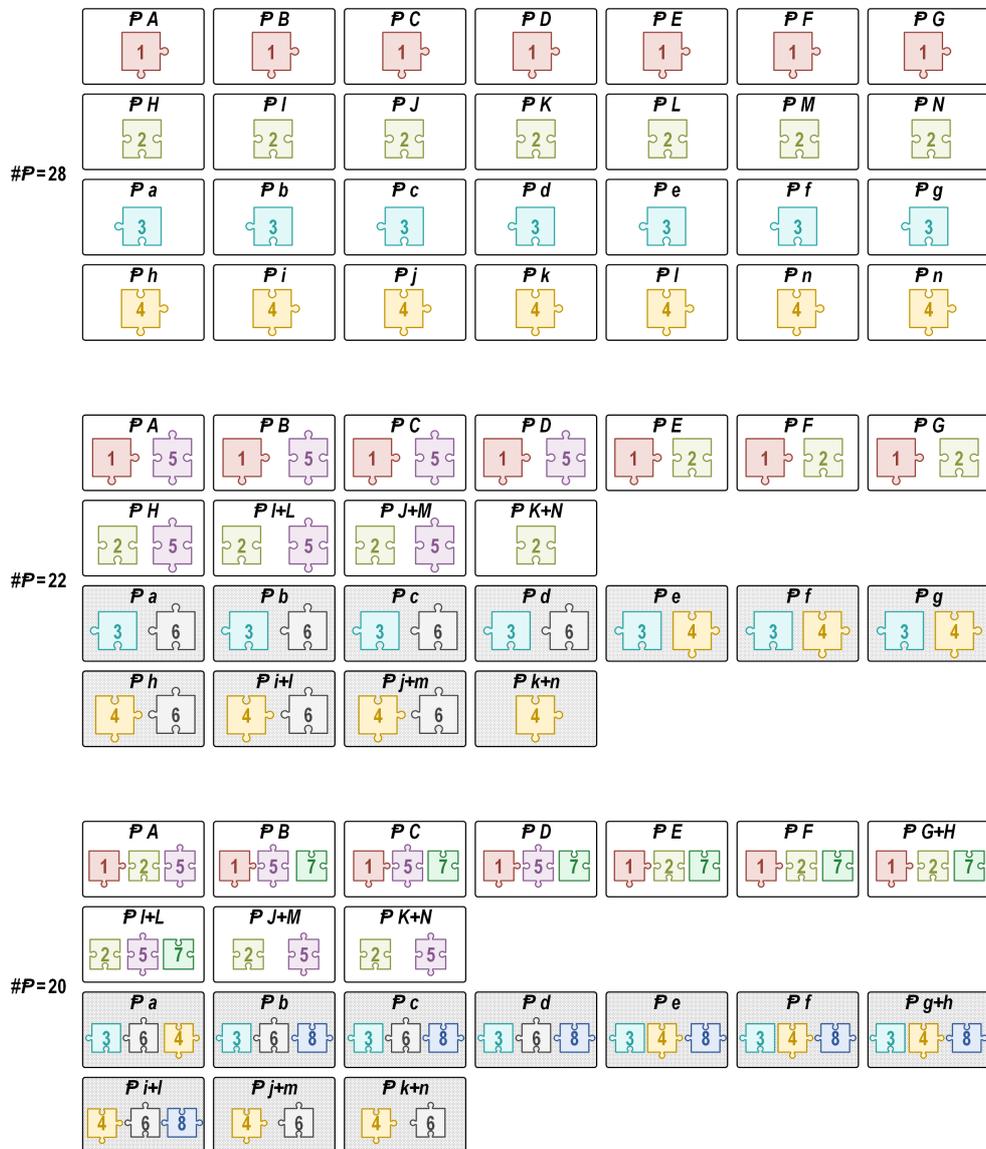


Abbildung 2: Darstellung von Lösungen mit dem Partitionsverfahren bei einem Threshold von $\Psi=4$

Es werden pro Share immer $2*\Psi-1$ Kopien verteilt. Jede Teilmenge der Partition der Misstrauensparteien muss also mindestens $2*\Psi-1$ Parteien enthalten. Wenn der *Threshold* für den Zugriff in einer Teilmenge zwei sein soll, müssen es sogar mindestens $2*\Psi$ Parteien in dieser Teilmenge sein.

Das Berechnen einer Lösung für eine Teilmenge mit *Threshold* zwei für den Zugriff ist vergleichsweise einfach. Erstens ist die Anzahl der Misstrauensparteien in einer Teilmenge viel kleiner als die Gesamtzahl der Misstrauensparteien. Außerdem genügt es, dafür zu sorgen, dass keine Partei in der Teilmenge von allen Shares eine Kopie bekommt. Dies lässt sich auch mit exakten Verfahren für alle relevanten Werte berechnen.

Abbildung 2 veranschaulicht für $\Psi = 4$, wie die Lösungen des *S-Netzwerk-Verteilungsproblems* bei dem Verfahren mit der Partition der Misstrauensparteien gebildet werden: Die Misstrauensparteien werden in dem Beispiel bei $\#P = 22$ sowie bei $\#P = 20$ jeweils in zwei gleichgroße Teilmengen partitioniert. Die eine Teilmenge umfasst jeweils die Misstrauensparteien mit einem Großbuchstaben als Bezeichner, die andere Teilmenge beinhaltet jeweils die Misstrauensparteien mit einem Kleinbuchstaben als Bezeichner. Für beide Teilmengen ist jeweils leicht zu zeigen, dass mindestens Shares von zwei verschiedenen Misstrauensparteien benötigt werden, um alle Shares in der Teilmenge zu erhalten. Da die Teilmengen disjunkt sind, werden insgesamt also mindestens Shares von $\Psi = 4$ verschiedenen Misstrauensparteien benötigt, um das Geheimnis rekonstruieren zu können.

In der bisher präsentierten Form kann das Partitionsverfahren nur angewendet werden, wenn die Anzahl $\#P$ der Misstrauensparteien bei einem geraden Ψ mindestens $\#P = (2*\Psi)*(\Psi \div 2) = \Psi^2$ beträgt beziehungsweise bei einem ungeraden Ψ mindestens $\#P = (2*(\Psi-1))*((\Psi-1) \div 2) + 2*\Psi - 1 = (\Psi-1)^2 + 2*\Psi - 1$ beträgt.

Dieses einfache Partitionsverfahren liefert zwar für bestimmte Anzahlen von Misstrauensparteien schnell optimale oder zumindest sehr gute Lösungen. Es lässt sich aber nicht für alle Anzahlen von Misstrauensparteien nutzen, bei denen es Lösungen für das *S-Netzwerk-Verteilungsproblem* gibt.

Zur Verbesserung des Partitionsverfahrens insbesondere für ungerade Ψ bietet es sich an, für einzelne Teilmengen der Partition der Misstrauensparteien auch einen *Threshold* drei (und eventuell auch noch höher) für den Zugriff auf alle Shares in dieser Teilmenge zu verwenden, sodass drei Parteien aus einer Teilmenge benötigt werden, um das Geheimnis rekonstruieren zu können. Für einen Zugriffs-*Threshold* drei müssen in der Teilmenge mindestens $2*\Psi+1$ Parteien vorhanden sein.

Ist Ψ durch drei teilbar, so reduziert sich die Anzahl $\#P$ der mindestens erforderlichen Misstrauensparteien für das Partitionsverfahren mit *Threshold* drei für den Zugriff in einzelnen Teilmengen auf $\#P = (2*\Psi+1)*(\Psi \div 3)$.

EFFIZIENTE BERECHNUNGEN IN TEILMENGEN BEI THRESHOLD DREI MIT BLÖCKEN

Während bei einem *Threshold* zwei für den Zugriff in Teilmengen ohne Weiteres exakte Berechnungen für alle relevanten Werte von Ψ und alle möglichen Partitionen durchgeführt werden können, scheidet dies bei *Threshold* drei bereits wiederum am zu hohen Aufwand. Das Problem ist, dass die Anzahl der Parteien, an die Kopien von einem jeden Share verteilt werden müssen, linear mit Ψ steigt. Entsprechend groß werden die Teilmengen.

Beim Betrachten der exakten Lösungen, die für kleine Ψ berechnet werden können, offenbart sich jedoch eine Möglichkeit, die Komplexität entscheidend zu reduzieren. Es zeigt sich nämlich, dass bei optimalen Lösungen vielfach ganze Blöcke von Misstrauensparteien jeweils Kopien derselben Shares erhalten. Dies liegt daran, dass die Anzahl der Parteien, welche Kopien von einem Share erhält, groß ist gegenüber dem *Threshold* drei für den Zugriff.

Daraus entstand die Idee, jeweils mehrere Misstrauensparteien in der Teilmenge zusammen als Block wie eine einzige Misstrauenspartei zu behandeln. Zuerst werden die Misstrauensparteien einer Teilmenge in mehrere möglichst gleichgroße Blöcke aufgeteilt. Es wird eine Konstante K bestimmt, die angibt, wie viele Blöcke benötigt werden, um in einer beliebigen Vereinigung dieser K Blöcke

jeweils mindestens $2*\Psi-1$ Parteien zu haben. Mithilfe des exakten Verfahrens wird dann eine optimale Verteilung von Shares mit *Threshold* drei für den Zugriff über diese Blöcke berechnet, wobei von jedem Share Kopien an genau K verschiedene Blöcke verteilt werden müssen. Zuletzst wird eine tatsächliche Verteilung der Shares über die einzelnen Misstrauensparteien in den Blöcken berechnet, wobei sichergestellt werden muss, dass Kopien von jedem Share in genau $2*\Psi-1$ Parteien gespeichert werden.

Durch dieses Verfahren reduziert sich die Komplexität je nach gewählter Anzahl der Blöcke mehr oder weniger stark. Es werden auch unterschiedlich gute Lösungen gefunden, je nachdem, wie viele Blöcke generiert werden. Um möglichst optimale Lösungen zu finden, bietet es sich an, einfach verschiedene Blockgrößen zu probieren und die Ergebnisse zu vergleichen.

Tabelle 3 gibt einen Überblick über die jeweils besten Ergebnisse für ausgewählte Konfigurationen des S-Netzwerk Verteilungsproblems, welche mit den gezeigten Verfahren bisher ermittelt wurden.

Ψ	$\#P$	$\Psi / \#P$	Shares	Shares / Ψ	Berechnung	$\#P / 2*\Psi-1$
2	6	33,33%	2	100,00%	-	2
2	5	40,00%	3	150,00%	Exakt, Lokaloptimierung, Partition	1
2	4	50,00%	4	200,00%	Exakt, Lokaloptimierung, Partition	1
3	15	20,00%	3	100,00%	-	3
3	13	23,08%	4	133,33%	Exakt, Lokaloptimierung, Partition	2
3	12	25,00%	5	166,67%	Exakt, Lokaloptimierung, Partition	2
3	10	30,00%	6	200,00%	Exakt, Lokaloptimierung	2
3	9	33,33%	8	266,67%	Exakt, Lokaloptimierung	1
3	8	37,50%	11	366,67%	Exakt, Lokaloptimierung	1
3	7	42,86%	21	700,00%	Exakt, Lokaloptimierung	1
4	28	14,29%	4	100,00%	-	4
4	25	16,00%	5	125,00%	Exakt, Partition	3
4	22	18,18%	6	150,00%	Exakt, Partition	3
4	21	19,05%	7	175,00%	Exakt, Partition	3
4	20	20,00%	8	200,00%	Lokaloptimierung, Partition	2
4	18	22,22%	10	250,00%	Lokaloptimierung, Partition	2
4	17	23,53%	11	275,00%	Lokaloptimierung	2
4	16	25,00%	13	325,00%	Lokaloptimierung	2
4	15	26,67%	15	375,00%	Lokaloptimierung	2
4	14	28,57%	17	425,00%	Lokaloptimierung	2
5	45	11,11%	5	100,00%	-	5
5	41	12,20%	6	120,00%	Partition	4
5	37	13,51%	7	140,00%	Partition	4
5	36	13,89%	8	160,00%	Partition	4
5	35	14,29%	8	160,00%	Partition	3
5	27	18,52%	14	280,00%	Partition	3
5	18	27,78%	57	1140,00%	Lokaloptimierung	2
6	66	9,09%	6	100,00%	-	6
6	61	9,84%	7	116,67%	Partition	5
6	56	10,71%	8	133,33%	Partition	5
6	55	10,91%	9	150,00%	Partition	5
6	51	11,76%	9	150,00%	Partition	4
6	45	13,33%	12	200,00%	Partition	4
6	44	13,64%	13	216,67%	Partition	4
6	36	16,67%	22	366,67%	Partition	3
6	33	18,18%	40	666,67%	Partition	3
7	91	7,69%	7	100,00%	-	7
7	85	8,24%	8	114,29%	Partition	6

Ψ	$\#P$	$\Psi / \#P$	Shares	Shares / Ψ	Berechnung	$\#P / 2*\Psi-1$
7	79	8,86%	9	128,57%	Partition	6
7	78	8,97%	10	142,86%	Partition	6
7	73	9,59%	10	142,86%	Partition	5
7	65	10,77%	13	185,71%	Partition	5
7	52	13,46%	26	371,43%	Partition	4
8	120	6,67%	8	100,00%	-	8
8	106	7,55%	10	125,00%	Partition	7
8	92	8,70%	12	150,00%	Partition	6
8	90	8,89%	13	162,50%	Partition	6
8	75	10,67%	18	225,00%	Partition	5
8	64	12,50%	30	375,00%	Partition	4
8	58	13,79%	58	725,00%	Partition	3
9	153	5,88%	9	100,00%	-	9
9	137	6,57%	11	122,22%	Partition	8
9	119	7,56%	14	155,56%	Partition	7
9	102	8,82%	19	211,11%	Partition	6
9	85	10,59%	30	333,33%	Partition	5
9	69	13,04%	84	933,33%	Partition	4
10	190	5,26%	10	100,00%	-	10
10	172	5,81%	12	120,00%	Partition	9
10	152	6,58%	15	150,00%	Partition	8
10	133	7,52%	19	190,00%	Partition	7
10	114	8,77%	26	260,00%	Partition	6
10	95	10,53%	73	730,00%	Partition	5

Tabelle 3: Ausgewählte Lösungen für das S-Netzwerk Verteilungsproblem

FAZIT ZU DATENERHALTUNG, ZUGRIFFSSCHUTZ UND ZUM S-NETZWERK VERTEILUNGSPROBLEM

Die Datenerhaltung in Kombination mit dem Schutz vor unberechtigtem Zugriff lässt sich durch Secret Sharing mit einem *Threshold* $\#U$ von mindestens Ψ und eine passende verteilte Sicherung jedes Shares durch $2*\Psi-1$ S-Knoten in verschiedenen Misstrauensparteien realisieren. Existieren $\Psi*(2*\Psi-1)$ oder mehr Misstrauensparteien, so kann $\#U = \Psi$ gewählt werden und dann passt jede Verteilung, bei der keine P mehr als ein Share erhält. Die Anzahl Ψ der Misstrauensparteien, welche übereinstimmen müssen, ist dabei jedoch niedrig im Verhältnis zur Gesamtzahl der Misstrauensparteien $\#P$. Je größer das Quorum Ψ gewählt wird, desto schlechter wird dieses Verhältnis.

Werden bei weniger als $\Psi*(2*\Psi-1)$ Misstrauensparteien die Lösungen des *S-Netzwerk Verteilungsproblems* zur Verteilung der Shares und ihrer Sicherheitskopien genutzt, lässt sich das Verhältnis des Quorums Ψ zur Anzahl der mindestens notwendigen Misstrauensparteien signifikant erhöhen (siehe Tabelle 3, Spalte „ $\Psi / \#P$ “). Der Preis dafür ist die höhere Anzahl $\#U$ benötigter Shares. Dadurch steigt der Speicherplatzbedarf auf den S-Knoten für zugriffsbeschränkte Inhalte um den in Tabelle 3 in der Spalte „Shares / Ψ “ angegebenen Faktor. Außerdem erhöht sich dementsprechend der notwendige Datenverkehr sowohl zum Speichern, zum Prüfen und gegebenenfalls zum Korrigieren als auch für lesende Zugriffe durch Anwender. Schließlich muss eine Zerlegung auch erst zusammengesetzt werden, bevor sie genutzt werden kann, was mit steigender Anzahl der Shares einen größeren Aufwand bedeutet. Auch im Falle der einfachen, an sich wenig rechenintensiven XOR-Verknüpfung der Shares können die notwendigen Speicherzugriffe teuer werden.

Es stellt sich die Frage, welche Konfiguration gewählt werden sollte. In der Realität wird die Anzahl der Misstrauensparteien $\#P$ nicht frei wählbar sein, schließlich müssen die Misstrauensparteien mit bestehenden Rechtsräumen kompatibel sein und die Misstrauensparteien sollten eine gewisse Ausgewogenheit aufweisen. Ψ kann frei festgelegt werden –

und damit ergibt sich die erforderliche Anzahl $\#U$ der Shares. Wie hoch der Speicherbedarf insgesamt ausfallen würde, wenn eine Konfiguration mit einer Mindestanzahl der Shares $\#U$ größer als Ψ gewählt wird, hängt auch davon ab, wie das S-Netzwerk genutzt wird. Schließlich werden nur zugriffsbeschränkte Inhalte um den Faktor $\#U / \Psi$ vergrößert.

REDUZIERTER SECRET SHARING ZUGRIFFSSCHUTZ UND HYBRIDER ZUGRIFFSSCHUTZ

Um den Speicherplatzbedarf gering zu halten, bietet es sich an, einen begrenzten Zugriffsschutz für weniger kritische Inhalte anzubieten. Dabei wird nur ein Secret Sharing mit einem *Threshold* L von $L \leq \#P/2 * \Psi - 1$ verwendet, sodass eine triviale Verteilung der Sicherheitskopien dieser Shares möglich ist, bei der jede Misstrauenspartei höchstens einen der Shares erhält. Da dieses L kleiner als Ψ ist, wird hierbei nicht der volle Zugriffsschutz erreicht. L Misstrauensparteien können das Geheimnis gemeinsam aufdecken. Für manche Anwendungen mag so ein reduzierter Zugriffsschutz völlig hinreichend sein.

Eine weitere Möglichkeit zur Begrenzung des Speicherplatzbedarfs besteht darin, große Dateien mit Schlüsseln zu verschlüsseln, die kleiner als die Dateien selbst sind. Derartige Verschlüsselungsverfahren bieten prinzipiell keine perfekte Sicherheit. Für Anwendungen, für welche die Sicherheit solcher Verschlüsselungsverfahren als hinreichend angesehen wird, bietet es sich jedoch an, nur die kleinen Schlüssel aufwendig und speicherintensiv mit dem Secret Sharing sowie der Verteilung der $2 * \Psi - 1$ Kopien von jedem der $\#U$ Shares auf verschiedene Misstrauensparteien zu schützen. Das S-Netzwerk dient dabei als sichere Austauschplattform relativ kurzer Schlüssel ausschließlich an Berechtigte. Die bereits verschlüsselten und eventuell sehr umfangreichen Daten werden dann ohne weiteren technischen Zugriffsschutz mit insgesamt nur $2 * \Psi - 1$ Kopien im S-Netzwerk gespeichert. Es handelt sich hierbei um ein hybrides Verfahren für den Zugriffsschutz.

Es ist schließlich auch möglich, die beiden genannten Ansätze zur Verringerung des Speicherplatzbedarfs miteinander zu kombinieren, um ein höheres Sicherheitsniveau zu erreichen. Dabei werden die umfangreichen Daten durch Secret Sharing mit einem *Threshold* L von $L \leq \#P/2 * \Psi - 1$ aufgeteilt. Die Shares werden dann mit kurzen Schlüsseln verschlüsselt, bevor sie über die Misstrauensparteien verteilt werden. Die kurzen Schlüssel wiederum werden mit vollem Secret Sharing Schutz publiziert, sodass mindestens Ψ verschiedene Misstrauensparteien kooperieren müssen, um an die Schlüssel zu kommen. Um an die Daten zu kommen, genügt es bei dieser Variante des hybriden Zugriffsschutzes nicht, nur L Shares der Daten zu haben oder die Schlüssel zu kennen – beides wird benötigt.

VERFEINERUNG DER VERTEILUNG VON SHARES MIT BERÜCKSICHTIGUNG DER VERTRAUENS-DISTANZEN

Misstrauensparteien können einander unterschiedlich stark misstrauen. Ein möglicher Indikator dafür ist die *Vertrauensdistanz*. Sollen nicht alle Misstrauensparteien als gleich betrachtet werden, kann versucht werden, unterschiedliche *Vertrauensdistanzen* zu berücksichtigen, um regelwidrigen Koalitionsbildungen besser entgegenwirken zu können. Wenn anzunehmen ist, dass zwischen jenen Misstrauensparteien, die untereinander geringe Vertrauensdistanzen aufweisen, die Wahrscheinlichkeit einer manipulativen Kooperation erhöht ist, könnte versucht werden, die Verteilung der Kopien der Shares so anzupassen, dass Gruppen von sich besonders nahestehenden Misstrauensparteien weder alle Shares erhalten, noch die Mehrheit der Sicherungskopien eines Shares.

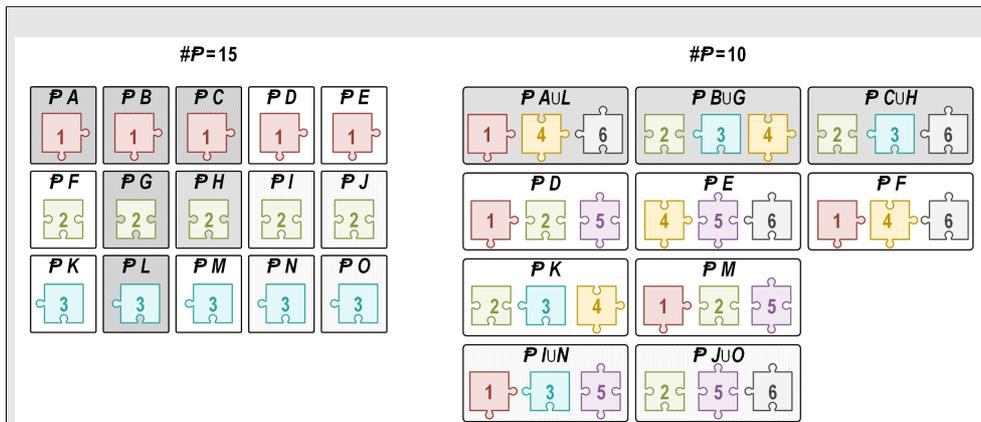


Abbildung 3: Mögliche Verteilungen der Kopien von Shares bei $\Psi = 3$

Abbildung 3 veranschaulicht, wie dies mit einer kleineren Anzahl von Misstrauensparteien funktionieren kann, während es bei einer großen Anzahl von Misstrauensparteien unmöglich ist. In dem Beispiel mit $\#P = 15$ Misstrauensparteien haben die 6 Misstrauensparteien A, B, C, G, H und L untereinander sehr geringe Vertrauensdistanzen. Egal wie die Kopien der drei Shares auf die 15 Misstrauensparteien verteilt werden, sodass keine einzelne P mehr als eine Kopie eines der Shares erhält: A, B, C, G, H und L haben immer entweder alle Shares oder sie können mindestens eines der Shares löschen, weil sie die Mehrheit der Sicherungskopien besitzen. In der Beispielverteilung können sie gemeinsam ohne das Mitwirken einer weiteren P sogar sowohl Share 1 verändern oder löschen als auch das Geheimnis rekonstruieren.

Wenn es bei gleichen staatlichen Grundstrukturen hingegen insgesamt nur 10 Misstrauensparteien geben soll, so können die Staaten der sich besonders nahestehenden Parteien der Partition mit 15 Misstrauensparteien jeweils zu größeren Parteien zusammengefasst werden. In dem Beispiel sind unter anderem A und L, B und G, C und H jeweils so vereint. Bei der gezeigten Verteilung der Kopien von 6 Shares über $\#P = 10$ Misstrauensparteien besitzen AUL, BUG , und CUH zusammen weder alle Shares (ihnen fehlt Share 5) noch mehr als zwei Kopien von einem der Shares. Also benötigen die sich besonders nahestehenden Parteien bei $\#P = 10$ auf jeden Fall mindestens eine weitere P , um Manipulationen durchführen zu können. Beides wäre beispielsweise nicht der Fall, wenn bei ansonsten gleicher Verteilung $P\ CUH$ die Shares $\{4, 5, 6\}$ zugeteilt bekäme und $P\ E$ die Shares $\{2, 3, 6\}$ überantwortet bekäme: Die Misstrauensparteien AUL, BUG , und CUH besäßen zusammen alle Shares und sie würden drei Kopien von Share 4 kontrollieren. Die Lösungen des S-Netzwerk Verteilungsproblems müssen also in einer bestimmten Weise auf die Misstrauensparteien gemappt werden, wenn die Vertrauensdistanzen so berücksichtigt werden sollen.

2.2 FEINHEITEN DER ROUTENFINDUNG

Beim Partitions-Routing kann Wissen über die Vermaschung und die Adressvergabe genutzt werden, um die parteigetreuen Weiterleitungen auch bei Ausfällen und suboptimalen Bekanntschaften kurz zu halten.

ALTERNATIVE ROUTEN BEIM PARTEIINTERNEN ROUTING

Ist von einem Vermittler V aus der Bekannte W , welcher der nächste optimale *Vermittler* in derselben P auf dem Weg zum parteiinternen Zielknoten B wäre, nicht erreichbar, kann innerhalb der P auch auf andere *Vermittler* ausgewichen werden, bis die Erreichbarkeit von W wiederhergestellt ist. Eine optimale Alternative ist schwieriger zu finden, es muss weiter vorausgeschaut werden:

Es sei X ein S-Knoten, der zu P_i gehört. Es sei $M(X)$ die Menge der *Bekanntes* von X , die auch zu P_i gehören. Dann ist für *Vermittler* V der S-Knoten U aus $M(V) \setminus W$ das nächste optimale Weiterleitungsziel auf dem Weg zum Adressaten B , unter dessen *Bekanntes* $M(U)$ ein *Bekannter* die insgesamt kleinste *Adressdistanz* zu der parteiinternen Adresse von B hat. Es wird also nicht geschaut, wie die Nachricht in einem Schritt möglichst nah an das Ziel geführt werden kann, sondern wie die Nachricht in zwei Schritten möglichst nah an das Ziel geleitet werden kann.

Abbildung 4 zeigt den Vorteil des vorausschauenden Berechnens alternativer Routen gegenüber dem einfachen Routing zu dem erreichbaren S-Knoten mit der geringsten Adressdistanz zum Ziel. Beim nur einen Schritt weit schauenden Routing wird von V der S-Knoten L als Alternative ausgewählt. Dies ist gleich in zweierlei Hinsicht ungünstig: Erstens ist B kein *Bekannter* von L . Es wird also mindestens noch ein *Vermittler* benötigt. Zweitens würde der unerreichbare S-Knoten W nach dem einfachen Routing auch von L als nächsten *Vermittler* gewählt werden. Versucht L die Vermittlung an W und ist W auch von L aus nicht erreichbar, entsteht ein zusätzlicher Zeitverlust.

Vorausschauend wird von V hingegen U als nächster *Vermittler* gewählt: Die kleinste Adressdistanz eines *Bekanntes* von U zur parteiinternen Adresse von B ist null, da B ein *Bekannter* von U ist. Mithin kann die alternative Route mit einem einzigen *Vermittler* realisiert werden.

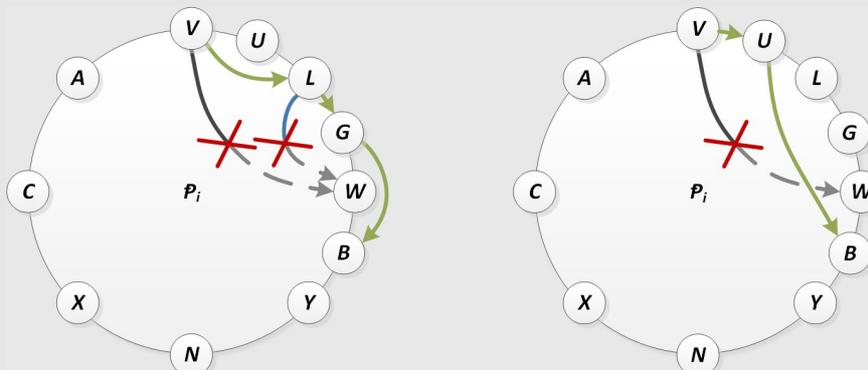


Abbildung 4: Vergleich zwischen einfachem (links) und vorausschauendem (rechts) parteiinternem Routing beim Ausfall von S-Knoten W

Es sei *Vermittler* Y ein *Bekannter* vom parteiinternen Zielknoten B einer *parteiinternen Weiterleitung*. Ist das Ziel B von Y aus temporär nicht erreichbar, so kann eine *parteiinterne Weiterleitung* über die anderen parteiinternen *Bekanntes* von B versucht werden. Jeder S-Knoten der Menge $M(B) \setminus Y$ ist ein möglicher alternativer *Vermittler* und kann als vorläufiges Ziel angesteuert werden.

Die Anzahl an Ausweichmöglichkeiten in P_i steigt logarithmisch mit zunehmender Anzahl $\#K_i$ an S-Knoten in P_i : Jeder S-Knoten in P_i hat zwischen $\lceil \log_8(\#K_i) \rceil - 1$ und $\lceil \log_8(\#K_i) \rceil * 2$ verschiedene parteiinterne *Bekanntes* als Alternativen.

PARTEIÜBERGREIFENDE BEKANNTSCHAFTEN UND PARTEIGETREUES ROUTING

Beim Nachrichtenaustausch zwischen zwei einander nicht bekannten S-Knoten A und B nach dem Partitions-Routing-Protokoll werden für jede Teilnachricht jeweils nur *partei-*

getreue Weiterleitungen verwendet. Für ein effizientes Routing ist es erforderlich, in jeder vermittelnden P einen *Bekannt* von B als finalen *Vermittler* ausfindig zu machen, um diesen als temporäres Ziel einer *parteiiernen Weiterleitung* optimal ansteuern zu können.

Dazu sollen jeweils jene S-Knoten in verschiedenen Misstrauensparteien, welche die gleiche parteiinterne Adresse χ haben, paarweise miteinander bekannt sein. Gibt es in einer Misstrauenspartei P_i noch keinen S-Knoten mit der gleichen parteiinternen Adresse χ , so muss mit dem zu P_i gehörigen S-Knoten eine *suboptimale Bekanntschaft* hergestellt werden, welcher die nächstkleinere bisher vergebene parteiinterne Adresse als χ hat. Wird später ein S-Knoten mit der Adresse χ zu P_i hinzugefügt, wird dieser zum optimalen *Bekannt* und die zuvor erzeugte *suboptimale Bekanntschaft* wird überflüssig.

Prinzipiell ist es möglich, bestehende parteiübergreifende *suboptimale Bekanntschaften* durch neue *suboptimale Bekanntschaften* zu ersetzen, sobald es bezüglich der Adresse besser liegende S-Knoten gibt. Das führt zu optimal kurzen *Weiterleitungen* und ermöglicht ein einfaches Routing. Doch das Schließen von *Bekanntschaften* ist aufwendig. Günstiger dürfte es sein, *suboptimale Bekanntschaften* nur einmalig durch *optimale Bekanntschaften* zu ersetzen.

Folgendes Verfahren für das parteigetreue Routing dient dazu, eine einzelne Nachricht M , die ein Teilstück τ_χ des Partitions-Routing-Protokolls enthält, vom Absender A , der zu P_i gehört, effizient zum Adressaten B zu übermitteln, welcher zu P_j gehört und der die parteiinterne Adresse β hat. Dabei müssen alle Vermittler zu derselben Misstrauenspartei P_v gehören.

Es sei V eine Variable für den aktuell vermittelnden S-Knoten in P_v . Es sei $\Phi(\chi)$ eine Funktion, welche die Runde Z , in der ein S-Knoten X der parteiinternen Adresse χ zu seiner P hinzugefügt wurde: $\Phi(\chi)$ liefert die kleinste natürliche Zahl Z für die gilt:

$$\chi \text{ modulo } \delta^{(G-Z)} = 0 \wedge Z > 0$$

- 1 **Initiale Überstellung:** Zunächst sendet A die Nachricht M an einen *Bekannt* V , der zu P_v gehört.
- 2 **Direkte Vermittlung:** Ist V auch ein *Bekannter* von B , sendet V die Nachricht M direkt an B und das Protokoll endet.
- 3 **Weiterleitung an den optimalen Bekannten von B :** Ziel dieser parteiinternen Weiterleitung in P_v ist ein S-Knoten V_β , der die parteiinterne Adresse β hat.
 - 3.1 Ist V gleich V_β und stellt V fest, dass kein S-Knoten B mit der parteiinternen Adresse β in P_j existiert, endet das Protokoll erfolglos.
 - 3.2 Stellt V fest, dass V_β nicht existiert, geht es mit Schritt 4 weiter.
 - 3.3 Sonst leitet V die Nachricht M an den *Bekannt* weiter, der bei dem Verfahren zum vorausschauenden parteiinternen Routing für das Ziel V_β zu wählen ist. Dieser *Bekannt* wird der neue *Vermittler* V . Weiter mit Schritt 2.
- 4 **Abschlusschritt:** Falls die parteiinterne Adresse von V größer als β ist, wird die Nachricht M an den *Bekannt* von V gesendet, der die nächstkleinere parteiinterne Adresse hat und dieser S-Knoten wird der neue *Vermittler* V .
- 5 **Weiterleitung an einen suboptimalen Bekannten von B :** Ziel dieser parteiinternen Weiterleitung in P_v ist ein S-Knoten, dessen parteiinterne Adresse kleiner als β ist und der ein suboptimaler *Bekannter* von B ist. Die genaue Adresse ist zu suchen. Die suchende Weiterleitung an *suboptimale Bekannte* aus drei Schritten:
 - 5.1 Ist V ein *Bekannter* von B , sendet V die Nachricht M direkt an B in P_j . Das Protokoll endet.
 - 5.2 Wenn die parteiinterne Adresse von V den Wert 0 hat, dann gibt es in P_v keine *Bekannt* von B . Das Protokoll endet.
 - 5.3 Es sei v die parteiinterne Adresse von V . V leitet M an den zu P_v gehörigen *Bekannt* W mit der nächstkleineren parteiinternen Adresse ω weiter, für den gilt: $\Phi(v) \leq \Phi(\omega)$. Dieser *Bekannt* W wird der neue *Vermittler* V .

Weiter mit Schritt 5.1.

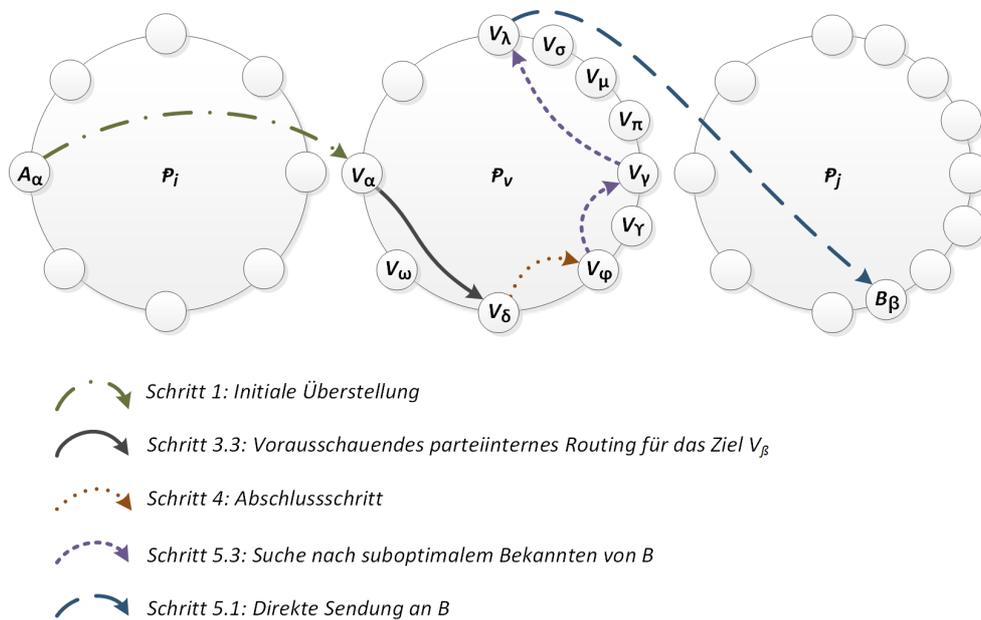


Abbildung 5: Suche nach einem Bekannten von B in P_v beim parteigetreuen Weiterleiten

Abbildung 5 visualisiert exemplarisch das Verfahren für das parteigetreue Routing. In diesem Beispiel wurden alle S-Knoten in P_j hinzugefügt, bevor ein zweiter S-Knoten in P_v hinzugefügt wurde. V_λ ist der erste S-Knoten, der zu P_v hinzugefügt wurde und V_λ ist daher der einzige *Bekante* von B in P_v . Da V_λ ein *suboptimaler Bekannter* von B ist, kommt beim Routing das Suchverfahren zur *Weiterleitung* an einen *suboptimalen Bekannten* (Schritt 5) zur Anwendung. Der S-Knoten V_γ wurden in einer späteren Runde hinzugefügt als V_ϕ – nach der Prüfung von V_ϕ auf eine *suboptimale Bekanntschaft* mit B steht fest, dass V_γ kein *suboptimaler Bekannter* von B sein kann. Daher wird V_γ übersprungen und es erfolgt die Weiterleitung zu V_v als nächstem *Vermittler* (Schritt 5.3). Die S-Knoten V_π , V_μ und V_σ wurden wiederum in einer späteren Runde hinzugefügt als V_v – sie kommen nach der Prüfung von V_v ebenfalls nicht mehr als *Bekante* von B infrage und werden übersprungen.

GRENZEN FÜR DIE SUCHE NACH EINEM SUBOPTIMALEN BEKANNTEN

Um aussichtslose Suchen nach einem suboptimalen Bekannten (Schritt 5) möglichst frühzeitig zu beenden, können S-Knoten für jede fremde Misstrauenspartei P_j eine parteiinterne Adresse als Grenze Ω_j für Weiterleitungen nach P_j speichern, welche den jüngsten S-Knoten identifiziert, für den eine Suche erfolglos war. Dazu muss ein erfolgloses Ende der Suche nach einem suboptimalen Bekannten (Schritt 5.2) an die bisherigen Vermittler kommuniziert werden, damit diese die Grenze Ω_j speichern können. Nur für jene Adressaten mit einer parteiinternen Adresse β für die gilt $(\Phi(\beta) \leq \Phi(\Omega_j)) \vee ((\Phi(\beta) = \Phi(\Omega_j)) \wedge (\beta > \Omega_j))$, die also nach dem S-Knoten geschaffen wurden, der als Grenzmarke dient, ist die Suche nach einem suboptimalen Bekannten in Zukunft noch fortzusetzen. Andernfalls endet das Protokoll.

Außerdem können S-Knoten in einer Misstrauenspartei P_v untereinander kommunizieren, wie groß die Differenz der parteiinternen Adressen von zwei suboptimal Bekannten in P_v und in P_j maximal noch sein kann. Weißt die parteiinterne Adresse v eines *Vermittlers* eine größere Differenz zu β auf, kann die Suche nach einem suboptimalen Bekannten abgebrochen werden und das Protokoll endet.

2.3 MULTI-PARTITIONS-ROUTING

Für das S-Netzwerk wird gefordert, dass Störungen in bis zu $\Psi-1$ Misstrauensparteien kompensiert werden können. Die sichere Kommunikation muss auch beim Ausfall von $\Psi-1$ *parteigetreuen Vermittlungswegen* funktionieren. Bei dem einfachen Partitions-Routing in der bisher gezeigten Form können Ausfälle in $\#P-\Psi$ Parteien kompensiert werden. Wenn die Anzahl der Misstrauensparteien $\#P$ größer als $2*\Psi+1$ ist, ergibt sich eine unnötig hohe Redundanz. Die geforderten Eigenschaften für die Ausfallsicherheit des S-Netzwerks würden auch dann erfüllt werden, wenn es insgesamt nur $2*\Psi-1$ alternative Routen verteilt über eben so viele verschiedene Misstrauensparteien geben würde.

Mit dem im Folgenden präsentierten Multi-Partitions-Routing-Verfahren benötigt jeder S-Knoten unabhängig von $\#P$ nur in $2*\Psi$ fremden Misstrauensparteien *Bekannte*. Dabei wird sichergestellt, dass ein S-Knoten A auch dann sicher mit einem S-Knoten B kommunizieren kann, wenn es weniger als $2*\Psi-1$ Misstrauensparteien gibt, in denen jeweils sowohl A als auch B mindestens einen *Bekannten* haben. Die Idee dazu ist, mehrere Misstrauensparteien bei *Weiterleitungen* so zusammenzufassen, dass sie wie eine einzige Misstrauenspartei agieren und auch so behandelt werden können. Diese zusammengefassten Misstrauensparteien dürfen dabei jeweils nur genau ein Share erhalten.

Es seien die insgesamt $\#P$ Misstrauensparteien durch natürliche Zahlen von 0 bis $\#P-1$ indiziert. Dann muss für das Multi-Partitions-Routing jeder S-Knoten in einer Misstrauenspartei P_K mit dem Index K genau in jenen Misstrauensparteien P_Y *Bekannte* haben, deren Index Y sich schreiben lässt als:

$$Y = (K + H) \text{ modulo } \#P \quad | \quad (H \in \mathbb{Z} \setminus 0) \wedge (|H| \leq \Psi)$$

Mit diesen genau $2*\Psi$ *Bekanntschaften* in $2*\Psi$ fremden Misstrauensparteien lässt sich dann das folgende Multi-Partitions-Routing Verfahren zur sicheren Kommunikation zwischen S-Knoten A in P_a und S-Knoten B in P_b nutzen:

- 1 **Vorbereitung:** Der Absender A erzeugt die Bitfolge X_p bestehend aus X , einem zufälligen Schlüssel K_R sowie Prüfdaten P über K_R und X . Also:

$$X_p = X \circ K_R \circ P(K_R, X)$$

Es sei N eine Konstante für die gilt: $N \in \mathbb{N} \wedge N \geq \Psi$. A bildet eine Secret Sharing Zerlegung $Z_{N\Psi}$ von X_p :

$$Z_{N\Psi}(X_p) = \{S_{N\Psi 0}(X_p), \dots, S_{N\Psi N-1}(X_p)\}$$

Es sei β die Adresse des Adressaten B . Es sei T eine eindeutige Nachrichtenidentifikationsnummer. A generiert N Teilnachrichten τ_* :

$$\tau_* = \beta \circ T \circ S_{N\Psi*}(X_p)$$

- 2 **Aufteilung:** A sendet jedes τ_* über einen sicheren Kanal an einen anderen *Bekannten* in einer fremden Misstrauenspartei, wobei nicht an einen *Bekannten* in P_b gesendet werden darf. A darf dabei keiner P mehr als einen Share von $Z_{N\Psi}(X_p)$ senden.
- 3 **Überprüfung und Weiterleitung:** Jeder S-Knoten V entschlüsselt und prüft auf sicheren Kanälen eingehende Nachrichten M auf Korrektheit.

S-Knoten haben die Aufgabe, jede nicht für sie bestimmte Nachricht M in Richtung des Adressaten B weiterzuleiten. Die S-Knoten werden dadurch zu *Vermittlern* von M .

Es sei v der Index der Misstrauenspartei P_v , zu der *Vermittler* V gehört.

- 3.1 Enthält M keine Identitätsbestätigung I_{A^*} , so ist der *Bekannte*, von dem M stammt, der Absender A . V generiert eine Identitätsbestätigung I_A , welche die S-Adresse α , den Namen und weitere Angaben zur Identität des Absenders A enthält, die manuell ausgetauscht und geprüft wurden, als V und A *Bekanntschaft* geschlossen haben.

Es sei H die kleinste natürliche Zahl, mit der sich der Index b der P des Adressaten B schreiben lässt als $b = (a + H) \text{ modulo } \#P$.

Es sei F die kleinste natürliche Zahl, mit der sich Index v der P des *Vermittlers* V

schreiben lässt als $v = (a + F) \text{ modulo } \#P$.

Variable D habe als *Richtungsangabe* den Wert $D=1$ bei $F < H$, sonst $D=-1$.

Der *Vermittler* V fügt der Nachricht M die Identitätsbestätigung I_A für A als Be glaubigung der Authentizität und die *Richtungsangabe* D hinzu: $M = \tau \circ I_A \circ D$

3.2 Falls der Adressat B dem *Vermittler* V unbekannt ist und V keinen *Bekannt* in P_b hat, erfolgt eine **Weiterleitung in eine andere vermittelnde P** .

3.2.1 **Standard- P -Weiterleitung:** Wenn der Absender A keine *Bekannt* in der Misstrauenspartei P_x mit dem Index $x = (v + D * \Psi) \text{ modulo } \#P$ hat, leitet V M über einen sicheren Kanal an einen *Bekannt* von V in P_x als nächsten *Vermittler* weiter.

Weiter mit Schritt 3.

3.2.2 **Verkürzte P -Weiterleitung:**

Es sei $N(P_x)$ die kleinste natürliche Zahl n , mit der ich der Index x von Misstrauenspartei P_x schreiben lässt als $x = (a + D * n) \text{ modulo } \#P$. $N(P_x)$ ist der Abstand von der Misstrauenspartei P_a , zu der A gehört, in Richtung D zur Misstrauenspartei P_x .

Es sei K die Menge der Misstrauensparteien, in der B *Bekannt* hat und A keine *Bekannt* hat. Jede derartige Misstrauenspartei ist das potenzielle Ziel einer *verkürzten P -Weiterleitung*.

Es sei L die Menge der Misstrauensparteien, in der A *Bekannt* hat und B keine *Bekannt* hat. *Vermittler* in einer solchen Misstrauenspartei sind eventuell erste *Vermittler*, die Schritt 3.2 ausführen müssen.

3.2.2.1 **Belegt durch anderen Share nach Standard- P -Weiterleitung?**

V berechnet für jedes Element P_k aus K , ob es in L ein Element P_l gibt, sodass gilt: $N(P_k) \text{ modulo } \Psi = N(P_l) \text{ modulo } \Psi$. Wenn ja, wird P_k aus K entfernt und P_l aus L entfernt.

3.2.2.2 **Belegt durch anderen Share nach verkürzter P -Weiterleitung?**

Es sei P_k das Element in K , für das $N(P_k)$ minimal ist, und es sei P_l das Element in L , für das $N(P_l)$ minimal ist.

Wenn $N(P_l) \text{ modulo } \Psi \neq N(P_k) \text{ modulo } \Psi$ gilt, wird P_k aus K entfernt und P_l aus L entfernt.

Weiter mit Schritt 3.2.2.2

3.2.2.3 Es sei P_k das Element in K , für das $N(P_k)$ minimal ist. Dann ist P_k die Misstrauenspartei, welche den finalen *Vermittler* stellt. V leitet M über einen sicheren Kanal an einen *Bekannt* von B in P_k als nächsten *Vermittler* weiter.

Weiter mit Schritt 3.

3.3 Der Adressat B ist dem *Vermittler* V unbekannt, V hat aber *Bekannt* in P_b . In diesem Fall erfolgt eine **parteinterne Annäherung an den finalen Vermittler**.

V leitet M über einen sicheren Kanal an einen *Bekannt* von V als nächsten *Vermittler* weiter, der zur gleichen P gehört wie der aktuelle *Vermittler* V , sodass die Nachricht M näher hin zu einem *Bekannt* des Adressaten B gelangt.

Weiter mit Schritt 3.

3.4 Der Adressat B ist ein *Bekannt* des *Vermittlers* V . Dann erfolgt die **finale Vermittlung**. M wird von V über einen sicheren Kanal direkt an den Adressaten B gesendet.

Weiter mit Schritt 4.

4 **Sammlung der Shares:** Der Adressat B entschlüsselt von *Bekannt* auf sicheren Kanälen eingehende Nachrichten M und prüft deren Authentizität und Integrität.

Eintreffende Shares $S_{N_{\Psi^*}(X_P)}$ und die zugehörigen Identitätsbescheinigungen I_{A^*} werden

zusammen mit der Information, aus welcher P sie vermittelt wurden, jeweils unter der Nachrichtenidentifikationsnummer T von M gespeichert.

- 5 **Vereinigung und Überprüfung:** Wenn beim Adressaten B Ψ verschiedene Shares $S_{N\Psi}(X_P)$ aus der Menge $Z_{N\Psi}(X_P)$ mit passender Nachrichtenidentifikationsnummer T und mit übereinstimmenden Identitätsbestätigungen I_{A^*} aus ebenso vielen verschiedenen Misstrauensparteien angekommen sind, rekonstruiert B aus den Shares X_P . Die Integrität wird anhand von X , K_R und den Prüfdaten $P(K_R, X)$ geprüft.

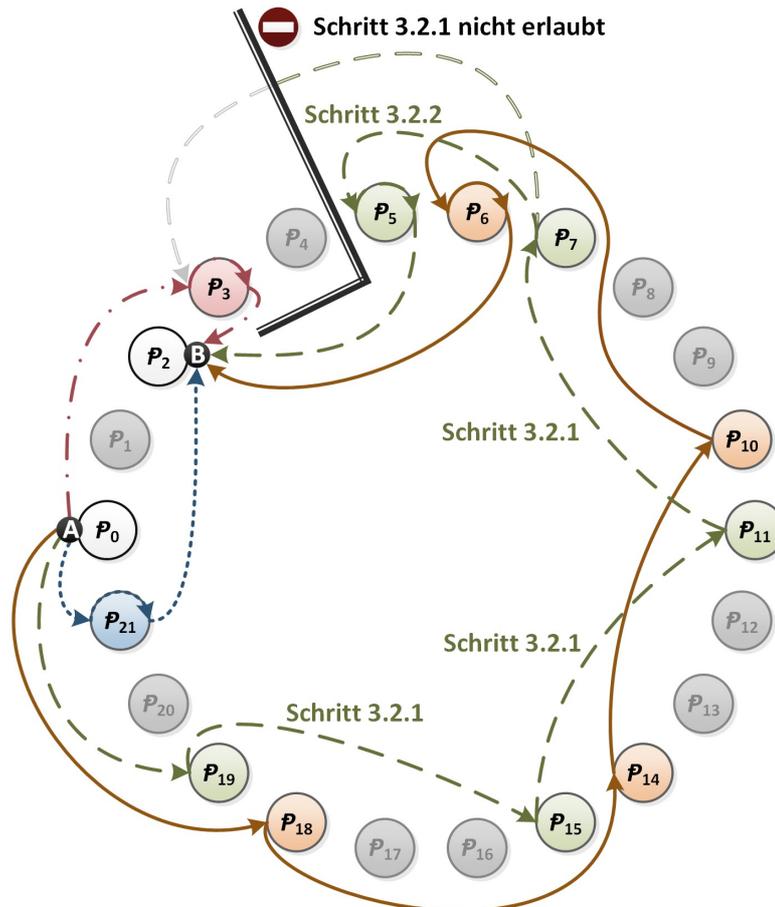


Abbildung 6: Multi-Partitions-Routing von A nach B mit $\Psi = 4$ und $\#P = 22$

Abbildung 6 veranschaulicht den Ablauf des Multi-Partitions-Routings. Die in Schritt 2 erreichten ersten Vermittler in P_3 und P_{21} sind zwar selbst keine *Bekannte* von B, aber in diesen beiden Misstrauensparteien hat B immerhin *Bekannte*. Daher kommt für die beiden in diese Misstrauensparteien gesendeten Shares jeweils ausschließlich das gewöhnliche Partitions-Routing (Schritt 3.3 und 3.4 des Multi-Partitions-Routings) zum Einsatz. Diese Shares werden also von keiner anderen P vermittelt.

Die ersten *Vermittler* in P_{18} und P_{19} stellen hingegen fest, dass es in ihren Misstrauensparteien keine *Bekannte* von B gibt. Also ist Schritt 3.2 auszuführen, wobei jeweils die Bedingung für die *Standard-P-Weiterleitung* (Schritt 3.2.1) erfüllt wird. Gleiches gilt für die nächsten *Vermittler* in P_{15} , P_{14} , P_{11} und P_{10} .

Hingegen wird von der durch einen *Vermittler* in P_7 für die *Standard-P-Weiterleitung* ermittelten nächsten Misstrauenspartei P_3 die Bedingung von Schritt 3.2.1 nicht erfüllt: Absender A hat *Bekannte* in P_3 . Abbildung 6 zeigt, beispielhaft, dass A in Schritt 2 bereits

einen Share an einen S-Knoten in P_3 gesendet hat. Da in keine vermittelnde Misstrauenspartei mehr als ein Share gelangen darf, ist eine *Weiterleitung* an einen *Bekannten* in P_3 keine zulässige Option für einen *Vermittler* in P_7 .

Von dem *Vermittler* in P_7 ist daher die *verkürzte P-Weiterleitung* (Schritt 3.2.2) auszuführen. Zunächst wird die Menge K all der Misstrauensparteien ermittelt, die potenziell letzte Ziele einer *Weiterleitung* nach Schritt 3.2 sein könnten, da in ihnen nur B , nicht aber A *Bekannte* hat. Im Beispiel sind dies P_5 und P_6 .

Dann wird die Menge L jener Misstrauensparteien gebildet, welche die ersten *Vermittler* enthalten, für welche Schritt 3.2 ausgeführt werden könnte, weil in ihnen nur A , nicht aber B *Bekannte* hat. Im Beispiel sind dies P_{18} und P_{19} .

Die beiden Mengen K und L haben immer die gleiche Anzahl an Elementen, da A und B jeweils in gleich vielen Misstrauensparteien *Bekannte* haben. Es stehen also immer genug letzte vermittelnde Misstrauensparteien für alle nach Schritt 3.2 weiterzuleitenden Shares zur Verfügung.

Schritt 3.2.2.1 ergibt hier, dass bereits ein anderer Share per *Standard-P-Weiterleitung* in P_6 gelangen könnte, nämlich der, welcher zuerst in P_{19} weitergeleitet wird, denn es gilt: $N(P_6) \text{ modulo } \Psi = 16 \text{ modulo } \Psi = N(P_{19}) \text{ modulo } \Psi = 4 \text{ modulo } \Psi = 0$.

In Abbildung 6 wird die *Standard-P-Weiterleitung* über P_{19} und P_6 auch visualisiert. Daher darf P_6 kein Ziel einer *verkürzten P-Weiterleitung* sein und folglich ist P_6 aus K zu entfernen und P_{19} ist aus L zu entfernen.

Alle *Misstrauensparteien*, die nach Schritt 3.2.2.1 noch Element von K sind, dürfen mit *verkürzten P-Weiterleitungen* angesteuert werden, allerdings jeweils nur mit maximal einem Share. Dazu werden in Schritt 3.2.2.2, solange das Element P_l in L , für das $N(P_l)$ minimal ist, nicht der erste *Vermittler* des weiterzuleitenden Shares ist, P_l aus L entfernt und das Element P_k in K , für das $N(P_k)$ minimal ist, aus K entfernt.

In Schritt 3.2.2.3 erhält jene Misstrauenspartei P_k in K , für die $N(P_k)$ minimal ist, als final zustellende Vermittlungspartei der *verkürzten P-Weiterleitung* den Share. In dem Beispiel in Abbildung 6 gibt es mit P_5 für den *Vermittler* in P_7 bereits vor Schritt 3.2.2.2 nur noch ein Element in K und somit wird P_5 als final zustellende Vermittlungspartei ausgewählt.

In dem Beispiel der Kommunikation zwischen A in P_0 und B in P_2 ergibt sich folgende Partition der anderen Misstrauensparteien:

$\{P_3\}$, $\{P_{21}\}$, $\{P_6, P_{10}, P_{14}, P_{18}\}$, $\{P_5, P_7, P_{11}, P_{15}, P_{19}\}$, $\{P_1, P_4, P_8, P_9, P_{12}, P_{13}, P_{16}, P_{17}, P_{20}\}$

Jede Teilmenge der Partition wird wie eine einzige Misstrauenspartei behandelt. Die letzte Teilmenge erhält in dem Beispiel keinen Share.

Je nachdem in welchen Parteien *Absender* und *Adressat* liegen und in welche Parteien der *Absender* in Schritt 2 (Aufteilung) Shares übermittelt, ergeben sich unterschiedliche Partitionen der Misstrauensparteien. Daher die Bezeichnung Multi-Partitions-Routing.

Die Anzahl der notwendigen *optimalen Bekannten* pro S-Knoten X reduziert sich mit dem Multi-Partitions-Routing auf:

$$\#B(X) \leq 2 * \lceil \log_{\delta}(\#K_i) \rceil + \Psi * 2$$

Die Obergrenze $\#V$ der Anzahl der benötigten *Vermittler* erhöht sich auf:

$$\#V \leq \sum_{i=0}^{\Psi-1} (2 * (\delta - 1) * \lceil \log_{\delta}(\#K_i) \rceil + 2 + \frac{\#P}{\Psi})$$

2.4 ZUGANGSSICHERHEIT FÜR DIE NUTZER UND SCHUTZ VON GEHEIMNISSEN

Neben der sicheren Kommunikation der S-Knoten untereinander werden auch sichere Verbindungen der Teilnehmer zum Computernetzwerk der S-Knoten benötigt. Teilnehmer müssen insbesondere das Publizieren oder Hinterlegen von Informationen im S-Netzwerk in ihrem Namen autorisieren und willentlich kontrollieren können.

Um ein hohes Maß an Sicherheit zu ermöglichen, werden spezielle Zugangssysteme benötigt. Für die Verbindung von den Zugangssystemen zu den S-Knoten werden zwei verschiedene Konzepte präsentiert: Der Einsatz des eigenen S-Knotens als Proxyserver und der Parallelbetrieb des Zugangssystems zum eigenen S-Knoten.

Damit ein Zugangssystem nur von seinem Besitzer benutzt werden kann, ist eine gegenseitige Authentifikation notwendig, wozu hier eine mögliche Lösung mit zweigeteilter Passwordeingabe skizziert wird.

Sowohl auf S-Knoten als auch auf Zugangssystemen des S-Netzwerks sind geheime Daten zu speichern. Angreifer sollen diese auch bei vollständigem direktem physischem Zugriff auf die Geräte sowie mit großem technischem Aufwand nicht auslesen und irregulär nutzen können. Als ultimative Schutzinstanz gegen Missbrauch sind die geheimen Daten mittels Selbsterstörung vor unbefugtem Zugriff zu sichern.

Als Informationssystem soll das S-Netzwerk im Fernzugriff sicher und verlässlich benutzbar sein. Der Austausch von Nachrichten zwischen einem beliebigen Teilnehmer und einem beliebigen S-Knoten soll wiederum über bestehende Computernetzwerke oder beliebige andere potenziell unsichere und unzuverlässige Verbindungswege erfolgen können.

Diese Kommunikation muss ebenso wie die Kommunikation zwischen den S-Knoten dauerhaft sicher und verlässlich sein. Allerdings handelt es sich hierbei um eine Kommunikation zwischen Personen und Maschinen – nicht um eine Kommunikation von Maschinen untereinander. Es ist eine geeignete Zugangsschnittstelle zwischen Mensch und Maschine zu erschaffen, sodass tatsächlich nur die Person, welcher der Zugang gehört, diesen nutzen kann, um auf die S-Knoten des S-Netzwerks und deren Daten sowie Dienste zuzugreifen.

Diese Zugriffsschnittstelle soll für das S-Netzwerk in Form von persönlichen Zugangssystemen für die einzelnen Teilnehmer gestaltet werden. Ein sicheres Zugangssystem soll selbst ein hochgradig spezialisiertes Computersystem sein, welches auf der einen Seite mit dem Besitzer sowie dessen sonstigen IKT Systemen und auf der anderen Seite mit den S-Knoten interagieren kann.

Zugangssysteme sollen mobil einsetzbar sein und sie müssen aus Sicherheitsgründen minimal gehalten werden, sie dürfen also ausschließlich genau die für den Zugriff auf das S-Netzwerk unmittelbar erforderliche Funktionalität bereitstellen.

KOMMUNIKATION ZWISCHEN DEM ZUGANGSSYSTEM UND DEN S-KNOTEN

Typischerweise werden Zugangssysteme lokal von ihren Besitzern betrieben. Sie werden anders als die S-Knoten realistischweise nicht ständig in Betrieb und online sein, sondern dynamisch bei Bedarf und Gelegenheit gestartet, um mit ihrer Hilfe sichere Verbindungen zum S-Netzwerk aufzubauen. Zugangssysteme sind keine Bestandteile des Peer-to-Peer Netzwerks der S-Knoten und sie erhalten keine eigene S-Adresse.

Die nicht ständig verfügbar zu haltenden Zugangssysteme sind in dem gezeigten Ver-

fahren zur sicheren Kommunikation mit Secret Sharing und (Multi-)Partitions-Routing nicht als *Vermittler* geeignet. Sie sind in diesem Verfahren mangels S-Adresse auch nicht direkt adressierbar. Es gibt jedoch verschiedene Möglichkeiten, wie ein dynamisches Zugangssystem dieses Verfahren ausschließlich als spezieller Sender und Adressat nutzen kann, um mit beliebigen S-Knoten sicher und verlässlich zu kommunizieren, ohne je selbst *Vermittler* zu sein.

Eine Möglichkeit ist die Nutzung des eigenen S-Knotens als **Proxyserver** für den sicheren Zugriff auf die anderen S-Knoten.

In diesem Fall muss das Zugangssystem Z_A einer Teilnehmerin *Alice* am S-Netzwerk nur zu deren eigenem S-Knoten A einen sicheren Kanal aufbauen können. Eine Nachricht M , die von Z_A zu einem beliebigen S-Knoten B gesendet werden soll, wird zunächst über einen sicheren Kanal an A gesendet und dort entschlüsselt. Wenn B ungleich A ist und wenn B kein *Bekannter* von A ist, wendet A das (Multi-)Partitions-Routing Verfahren an, um M zerlegt in mehrere Shares so an B weiterzuleiten, dass keine vermittelnde P mehr als einen Share erhält.

Umgekehrt rekonstruiert A eine nach dem (Multi-)Partitions-Routing Verfahren eintreffende auf mehrere Shares aufgeteilte Nachricht R , die von B an den Teilnehmer *Alice* gesendet werden soll, und übermittelt R bei einer bestehenden Verbindung über einen sicheren Kanal an Z_A . Wenn nicht sofort eine Übermittlung an Z_A möglich ist, speichert A die Nachricht R , um sie beim nächsten Verbindungsaufbau zuzustellen.

Der große Vorteil dieser Lösung ist, dass das Zugangssystem nur zum eigenen S-Knoten seines Besitzers einen direkten sicheren Kanal aufbauen können muss. Das Zugangssystem muss das (Multi-)Partitions-Routing Protokoll gar nicht beherrschen. Ein Schlüsseltausch mit weiteren S-Knoten in fremden Misstrauensparteien, wie er für die S-Knoten beim Schließen von *Bekanntschaften* in fremden Misstrauensparteien erforderlich ist, entfällt folglich für die Zugangssysteme die den eigenen S-Knoten als Proxyserver nutzen komplett.

Nachteil dieser Lösung ist die vollständige Abhängigkeit von der Sicherheit, Korrektheit und Verfügbarkeit des eigenen S-Knotens. Auf dem als Proxy verwendeten eigenen S-Knoten werden alle Nachrichten vom und zum Besitzer entschlüsselt. Anders als für das persönliche Zugangssystem ist für den S-Knoten nicht vorgesehen, dass er im Betrieb jederzeit unter der unmittelbaren Kontrolle des Besitzers steht. Ein als Proxy zu nutzender S-Knoten muss daher besonders sorgfältig gegen mögliche Angriffe abgeschirmt werden. Wird der S-Knoten von einem Dienstleister betrieben, muss der Kunde seinem S-Betreiber vertrauen.

Eine zweite Möglichkeit zur Anbindung des Zugangssystems besteht darin, das Zugangssystem gewissermaßen im **Parallelbetrieb** zum eigenen S-Knoten zu nutzen.

In diesem Fall muss das Zugangssystem das (Multi-)Partitions-Routing Verfahren sowohl als Absender als auch als Adressat beherrschen – nicht aber als *Vermittler*. Um das Verfahren zur sicheren Kommunikation mit Secret Sharing direkt nutzen zu können, muss das Zugangssystem Z_A außerdem direkt zu jenen *Bekannt* des eigenen S-Knotens A , die in fremden Misstrauensparteien liegen, einen sicheren Kanal aufbauen können.

Ein Vorteil dieser Lösung liegt darin, dass der Klartext einer Nachricht M zu oder von einem Empfänger B auf keinem einzigen S-Knoten außer auf B vollständig rekonstruiert werden kann. Außerdem kann der Ausfall von bis zu $\Psi-1$ beliebigen S-Knoten den sicheren Zugang zu allen anderen S-Knoten nicht verhindern. Der Parallelbetrieb reduziert allgemein die Abhängigkeit des Besitzers vom eigenen S-Knoten und mithin eventuell auch vom eigenen S-Betreiber.

Andererseits muss das Zugangssystem im Parallelbetrieb ein komplexeres Kommunikationsprotokoll beherrschen und es muss für mindestens $2*\Psi-1$ *Bekannt* von A in fremden Misstrauensparteien aktuelle Verbindungsdaten speichern. Dazu müssen etwaig anfallende Aktualisierungen, etwa Änderungen der möglichen Verbindungswege zu einem bestehenden *Bekannt* oder Erneuerungen von Schlüsseln, auch auf dem Zugangs-

system Z_A nachvollzogen werden.

Zwar fallen solche manuell aufwendigen sicherheitskritischen Aktualisierungen ohnehin für die S-Knoten an, doch bei den S-Knoten können die S-Betreiber Aktualisierungen ohne jede Beteiligung der Besitzer durchführen, da sie ohnehin für die Wartung dieser Systeme verantwortlich sind und weil sie direkten Zugriff auf die S-Knoten haben.

Für ihre Zugangssysteme im Parallelbetrieb sind hingegen die einfachen Teilnehmer selbst verantwortlich. So entsteht durch den Parallelbetrieb von Zugangssystem und eigenem S-Knoten eventuell ein erhöhter Administrationsaufwand für die einfachen Teilnehmer des S-Netzwerks.

Die Frage, welche dieser Lösung zur Anbindung des Zugangssystems die bessere ist, kann jeder Teilnehmer für sich selbst beantworten, denn das S-Netzwerk kann sowohl die Anbindung über den eigenen S-Knoten als Proxyserver als auch den Parallelbetrieb ermöglichen. Wenn ein Teilnehmer Zweifel an der Verfügbarkeit, Sicherheit und Korrektheit des eigenen S-Knotens hat oder wenn er keinem potenziellen S-Betreiber so weitgehend vertrauen möchte, kann er auf den Parallelbetrieb ausweichen. Für viele Teilnehmer mag jedoch die Nutzung des eigenen S-Knotens als Proxyserver aufgrund des geringeren Aufwands und des potenziell einfacheren sowie billigeren Zugangssystems die attraktivere Lösung sein.

Abbildung 7 visualisiert beide Varianten zur Anbindung des Zugangssystems.

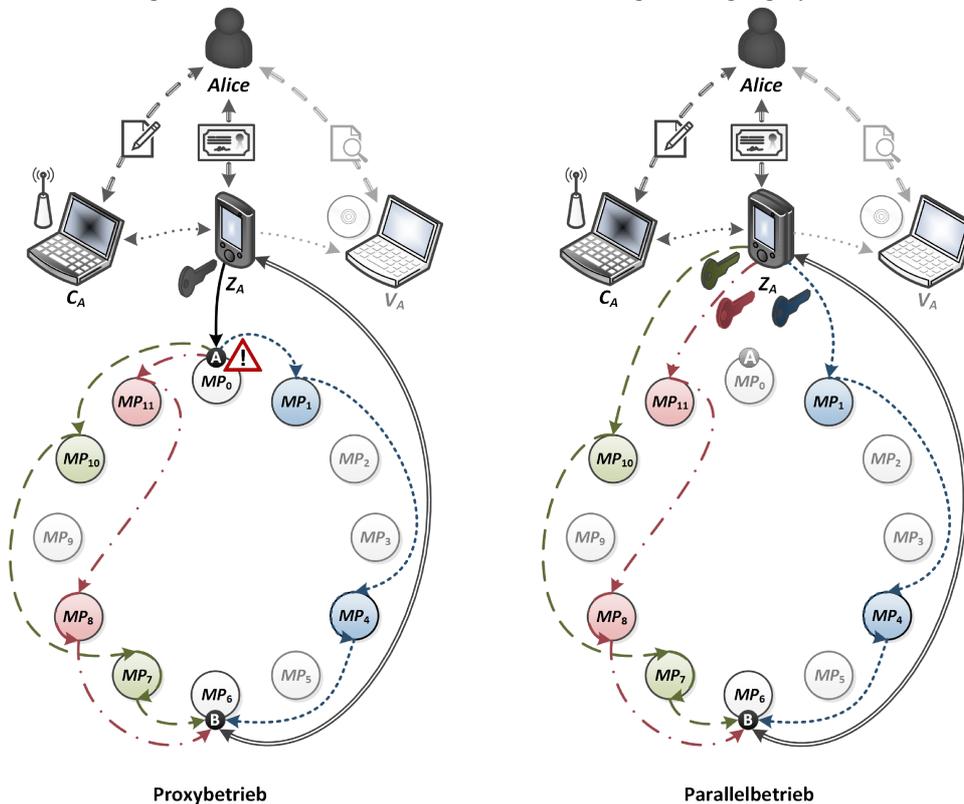


Abbildung 7: Validierung der Daten und Kommunikation von Alice mit S-Knoten B indirekt mithilfe des eigenen S-Knotens A als Proxy sowie direkt mit dem Zugangsgert Z_A im Parallelmodus

BESTANDTEILE UND FUNKTIONSWEISE VON ZUGANGSSYSTEMEN

Zugangssysteme müssen geschützten Speicherplatz bereitstellen. Dort sind die notwendigen Verbindungsdaten und geheimen Schlüssel zu speichern. Wie auch immer die Anbindung von Zugangssystemen an das Computernetzwerk der S-Knoten erfolgt, die

geheimen Schlüsseldaten für den Aufbau von sicheren Kanälen zu bestimmten S-Knoten dürfen die Zugangssysteme unter keinen Umständen verlassen.

Zur Kontrolle und zur Bedienung müssen Zugangssysteme für das S-Netzwerk über geeignete Benutzerschnittstellen verfügen. Darüber hinaus müssen Zugangssysteme über lokale Schnittstellen verfügen, welche einen Datenaustausch mit anderen allgemeinen und potenziell unsicheren Computersystemen des Nutzers ermöglichen. Zugangssysteme sollen über ihre lokalen Schnittstellen Daten zum Senden entgegen nehmen können und sie sollen es ausschließlich ihrem Besitzer erlauben, daraus Nachrichten zu generieren, die dann nach einem der vorgestellten Verfahren so an beliebige S-Knoten gesendet werden können, dass die Eigenschaften eines sicheren Kanals gewährt werden.

Umgekehrt sollen Zugangssysteme ausschließlich ihrem Besitzer über die lokalen Schnittstellen den Inhalt von jenen Nachrichten bereitstellen, welche die Zugangssysteme nach einem der beschriebenen Verfahren geschützt aus dem S-Netzwerk erhalten.

Angesichts der Unleugbarkeit im S-Netzwerk ist besondere Vorsicht bei der Entgegennahme eines Nachrichtenkörpers M von einem nicht vertrauenswürdigen Computersystem C_A zur Sendung an einen beliebigen S-Knoten B geboten: Hat ein Angreifer Eve die vollständige Kontrolle über C_A , so kann er M durch eine beliebige Bitfolge W ersetzen und W über eine lokale Schnittstelle an das Zugangssystem Z_A senden. Der Besitzer $Alice$ vom Zugangssystem Z_A muss die Möglichkeit haben, zu überprüfen, ob der von ihm gewollte Nachrichtenkörper M auch tatsächlich unverändert beim Zugangssystem Z_A ankommt. Diese Überprüfung kann nicht auf C_A geleistet werden – und sie kann auch nicht in Kooperation mit C_A erfolgen, da alle Ausgaben von C_A durch Eve manipuliert werden können. Der Vergleich von einer auf Z_A berechneten Prüfsumme über die zu übermittelnde Nachricht mit einer auf C_A berechneten Prüfsumme bietet keinen zuverlässigen Schutz, da auf C_A durch Manipulation von E eventuell schon $P(W)$ statt $P(M)$ angezeigt wird und weil Z_A dann einen identischen Wert $P(W)$ für die von $Alice$ nicht beabsichtigte Nachricht W liefern würde.

Für einfache und kurze Nachrichten sowie übliche Inhalte kann es sinnvoll sein, das Zugriffssystem Z_A mit Programmen zur Betrachtung auszustatten, sodass Anwender selbst direkt auf Z_A manuell überprüfen können, ob der Nachrichtenkörper M tatsächlich die beabsichtigten Informationen enthält. Für umfangreiche Nachrichten, und spezielle für solche, die Dateien mit ausführbarem Code enthalten, ist das jedoch keine praktikable Lösung – schließlich soll das Zugriffssystem möglichst minimal, sicher und mobil gehalten werden.

Eine Möglichkeit zur Absicherung besteht in der Nutzung eines zweiten allgemeinen Computersystems V_A , welches selbst keine Netzanbindung hat. Zunächst wird der zu übermittelnde Nachrichtenkörper M von C_A auf Z_A übertragen. Dann wird Z_A von C_A getrennt und mit V_A verbunden, auf welchem die tatsächlich auf Z_A kopierten Daten umfangreich geprüft und validiert werden können. Idealerweise sollte die Software auf V_A vor jeder Prüfung neu aufgesetzt werden, sodass immer ein sauberes System zur Verfügung steht. Um unbemerkt einen falschen Nachrichtenkörper W einzuschleusen, genügt es Eve dann nicht, nur C_A manipulieren zu können. Die Kontrolle über eines der sehr begrenzten beziehungsweise abgeschotteten Systeme Z_A oder V_A zu erlangen ist eine erheblich höhere Hürde, als nur C_A angreifen zu müssen. Abbildung 7 veranschaulicht die Idee.

WILLENTLICHE AUTORISATION SICHERSTELLEN

Beim Betrieb eines Zugangssystems Z_A muss gewährleistet werden, dass nur der Besitzer $Alice$ selbst zur Nutzung der Funktionen zum Senden und Empfangen von Daten in der Lage ist. Für Z_A genügt es nicht, nur eine Authentifikation von $Alice$ durchzuführen. Die Anwesenheit von $Alice$ ist lediglich eine notwendige Bedingung. Hinreichend ist es für das S-Netzwerk erst, wenn Funktionsaufrufe auf Z_A willentlich von $Alice$ autorisiert werden.

Solange keine zuverlässigen Technologien bekannt sind, mit denen ausschließlich ein bestimmter Mensch ein Computersystem direkt willentlich steuern kann, soll die

Autorisation für das S-Netzwerk durch die Eingabe eines geheimen Passwortes geschützt werden, das der rechtmäßige Besitzer in seinem Gedächtnis aufbewahren kann. Ein solches Geheimnis physisch direkt aus dem Gehirn auszulesen übersteigt das derzeit für Menschen technisch mögliche.

Dennoch genügt ein Passwort nicht, um auch ausschließlich einen willentlichen Gebrauch sicherzustellen. Damit es genutzt werden kann, muss das Passwort auch an eine Maschine übertragen werden, wobei es eventuell an der Schnittstelle zwischen Mensch und Maschine abgegriffen werden könnte. Um dies zu erschweren, sind für sichere Zugangssysteme zum S-Netzwerk eine Reihe von Maßnahmen angedacht:

Erstens soll die Eingabe des Passwortes über eine Tastatur erfolgen, bei der die Tasten nach jedem Knopfdruck zufällig neu angeordnet werden. Dies lässt sich mit einer Bildschirmtastatur realisieren. Die Bedienung einer Bildschirmtastatur kann jedoch irreführend sein, da etwa leicht ungewollt andere Tasten gedrückt werden können. Besser ist eine Tastatur mit mechanischen Tasten, bei der jede einzelne Taste ein eigenes Display darstellt. Durch die zufällige Anordnung der Tasten verrät die Position des Fingers nichts über das eingegebene Passwort.

Zweitens sollen die wechselnden Beschriftungen der Tasten nur aus sehr zentraler Position vor dem Gerät lesbar sein. Dazu sind sehr blickwinkelabhängige Displays zu verwenden. Ein Mitlesen von der Seite wird dadurch wesentlich schwieriger.

Drittens soll ein sicheres Zugangssystem nur dann zu bedienen sein, wenn sich der Nutzer auch nah vor dem Gerät befindet, sodass der Körper des Nutzers das Zugangsgesamt möglichst gut abschirmt. Wer dem Nutzer über die Schulter schaut, der hat bereits einen ganz anderen Blickwinkel, wenn der Abstand zum sicheren Zugangssystem gering ist. Je weiter weg der Nutzer von seinem sicheren Zugangssystem ist, desto eher wird es möglich sein, aus einem ähnlichen Blickwinkel mitzulesen. Also sollen sichere Zugangssysteme auch Sensoren zur Messung des Abstands des Nutzers enthalten.

Selbst wenn das Mitlesen ausgeschlossen werden kann, ist der freie willentliche Einsatz des Passwortes durch gewisse Bedrohungsszenarien gefährdet. Menschen können erpresst, bedroht und gefoltert werden. Es ist auch möglich, zu versuchen die Widerstandskraft gegen den unwillentlichen Einsatz des Passwortes durch Drogen zu reduzieren.

Auch gegen solche grundlegenden Gefahren können und müssen Maßnahmen ergriffen werden. Beispielsweise können sichere Zugangssysteme mit einem verdeckten Notruf ausgestattet werden, der es selbst in einer unmittelbaren Zwangslage, etwa mit vorgehaltener Waffe, erlaubt, Alarm zu schlagen, ohne dass die Erpresser dies feststellen können. Die Idee dazu ist, dass jeder Teilnehmer auch ein Alarmpasswort festlegen kann. Wenn dieses Alarmpasswort eingegeben wird, so verhält sich das Zugangssystem scheinbar genau wie immer, beispielsweise werden die initiierten reliablen Publikationen oder sicheren Hinterlegungen durchgeführt. Insgeheim wird allerdings automatisch ein zunächst uneinsehbarer Vorbehalt gespeichert. Zugleich wird über die kontaktierten S-Knoten ein stiller Alarm in mehreren Misstrauensparteien ausgelöst, sodass Maßnahmen zur Beendigung der Zwangslage und zur weiteren Untersuchung sowie zur Anklage der mutmaßlichen Erpresser ergriffen werden können.

GEGENSEITIGE AUTHENTIFIKATION ZWISCHEN TEILNEHMER UND ZUGANGSSYSTEM

Das Passwort dient zugleich auch als ein Authentifizierungsmerkmal, mit dem das sichere Zugangssystem feststellen kann, ob es von seinem Besitzer Alice benutzt wird. Neben einem Passwort können weitere Merkmale wie Hardware-Token oder biometrische Merkmale zur Authentifikation verlangt werden.

Die Eingabe von geheimen Codes und anderen Authentifizierungsdaten ist ein hochgradig sicherheitskritischer Vorgang. Das Abgreifen von Passwörtern oder biometrischen Merkmalen gehört zu den einfachsten und effektivsten Angriffen überhaupt. Im simpelsten Fall genügt eine Beobachtung der Eingabe. Bei kombinierten Multi-Faktor Mechanismen

etwa aus Passwort und Karten können manipulierte Lesegeräte verwendet werden, um sich trotzdem Zugriff zu verschaffen. Da solche Angriffe relativ leicht durchzuführen sind, verwundert es nicht, dass beispielsweise Skimming-Angriffe auf Geldautomaten mithilfe von manipulierten Lesegeräten verbreitet vorkommen [MELANI 2011].

Zur Minimierung von potenziellen Angriffspunkten soll für das S-Netzwerk verlangt werden, dass alle sicherheitskritischen Funktionen ausschließlich direkt auf ein und demselben Zugangssystem kontrolliert und ausgeführt werden müssen. Eine Aufteilung zwischen verschiedenen Komponenten, beispielsweise zwischen Chipkarte und Lesegerät, ist für das S-Netzwerk zu riskant. Zugangssysteme für das S-Netzwerk müssen demnach Eingabe- und Ausgabeeinheiten zur Interaktion mit dem Benutzer enthalten, welche eine sichere Authentifikation und Autorisation ermöglichen.

Im Folgenden wird zunächst einmal einfach vorausgesetzt, dass es gelingt, ein Zugangssystem Z_A so zu konstruieren, dass Manipulationen am Gehäuse von Z_A etwa zum Abgreifen der eingegebenen Passwort-Zeichen oder andere Angriffe etwa zum Auslesen von geheimen Daten (z. B. Schlüssel) entweder keinen Erfolg haben können oder dass sie das Zugangssystem Z_A vollständig unbrauchbar machen.

Auch unter dieser starken Voraussetzung genügt es nicht, dass sich nur der Nutzer *Alice* gegenüber dem Zugangssystem authentifizieren muss: Es wäre möglich, dass das komplette Zugangssystem Z_A von einem Angreifer *Eve* gegen ein ähnlich aussehendes Gerät G_E ausgetauscht wird und dass G_E nun etwas völlig anderes tut als das, was der Nutzer *Alice* möchte. Beispielsweise könnte G_E den von *Alice* eingegebenen Code an *Eve* senden. *Eve* könnte den Code in das von *Alice* gestohlene Zugriffsgerät Z_A eingeben und diesen für eigene Zwecke nutzen – ein klassischer Man-in-the-middle-Angriff.

Es ist folglich zwingend erforderlich, dass Nutzer zunächst ihr Zugangssystem sicher authentifizieren, bevor sie ein kritisches Geheimnis (ihr Passwort) vollständig an ihr vermeintliches Zugangssystem preisgeben, welches sie in Wirklichkeit ausspioniert.

Einen sehr rudimentären Schutz bietet eine aufwendige äußere Gestaltung des Zugangssystems Z_A , sodass es schwierig wird, ein für das bloße Auge und für den Tastsinn nicht zu unterscheidendes Austauschgerät G_E herzustellen. Allerdings kann jedes auch nur zu einigermaßen wirtschaftlichen Konditionen herstellbare Gehäuse mit mäßigem Aufwand so reproduziert werden, dass es zumindest von einem durchschnittlichen Beobachter nicht vom Original zu unterscheiden ist. Außerdem haben manche Personen keine oder nur sehr beschränkte optische bzw. haptische Wahrnehmungen zur Verfügung. Nur die wenigsten Personen verfügen über ein fotografisches Gedächtnis. Und wer würde schon tatsächlich bei jeder Benutzung mit der gleichen Sorgfalt prüfen?

Authentifikationsmerkmale des Zugangssystems, die nur mit Messgeräten überprüfbar sind, sind keine sinnvolle Option. Dass zur Prüfung der Echtheit des Zugangssystems bei jedem Einsatz ein Messgerät erforderlich wäre, würde einen erheblichen zusätzlichen Aufwand für die Nutzer bedeuten. Außerdem ließen sich solche Maßnahmen prinzipiell durch Manipulationen an den Messgeräten überwinden. Das Problem würde also nur verlagert.

Ein möglicher Lösungsansatz für Zugangssysteme zum S-Netzwerk ist, dass die Zugangssysteme eine zweigeteilte Passwordeingabe erfordern. Nach den ersten J korrekt eingegebenen Zeichen des Passworts erwartet die Nutzerin *Alice*, dass ihr von ihrem Zugangssystem Z_A ein geheimer Code C_{Z_A} angezeigt wird. Nur wenn das Zugangssystem sofort den korrekten Code C_{Z_A} ausgibt, fährt *Alice* mit der Eingabe der verbleibenden K Zeichen des Passwortes fort und sie erhält daraufhin Zugriff auf die weiteren Funktionen des Zugangssystems.

Damit dieses Verfahren einen Sicherheitsgewinn bringen kann, darf natürlich kein Dritter die eingegebenen Zeichen des Passwortes oder den geheimen Code C_{Z_A} einsehen oder sonst wie mitverfolgen können.

Die zweigeteilte Passwordeingabe mit der zwischenzeitlichen Anforderung des geheimen Codes C_{Z_A} kann außerdem nur dann tatsächlich einen wirksamen Schutz gegen

einen Angriff mit dem kompletten Austausch des Zugangssystems Z_A gegen ein täuschend ähnlich aussehendes Gerät G_E bieten, wenn noch eine weitere Bedingung erfüllt wird, nämlich die beschränkte Reproduzierbarkeit von C_{Z_A} :

Wenn ein Angreifer Eve das Gerät G_E so konstruiert hat, dass die Eingaben des Opfers $Alice$ auf G_E sofort an Eve weitergeleitet werden, dann kann Eve die Eingaben von $Alice$ auf dem gestohlenen Zugangssystem Z_A ausführen beziehungsweise voll automatisiert ausführen lassen. Nach den ersten J Zeichen des Passworts erhält Eve von Z_A den Code C_{Z_A} und sendet diesen an G_E . Gelingt es dem Angreifer Eve , auf G_E den Code C_{Z_A} ohne deutlich erkennbare Verzögerung genau so wie auf Z_A ausgeben zu lassen, so hat $Alice$ keine Möglichkeit, die Manipulation zu erkennen. Für $Alice$ sieht es so aus, als hätte sie ihr korrekt funktionierendes Zugangssystem vor sich. Warum sollte $Alice$ zögern, die verbleibenden K Zeichen des Passwortes einzugeben, welche G_E wiederum an Eve übermittelt? Der Angreifer Eve hat in diesem Fall ein in keiner Weise beeinträchtigtes Zugangssystem Z_A und beide Teile des geheimen Passwortes von $Alice$ in seinen Besitz gebracht.

Damit der Code C_{Z_A} also tatsächlich einen Sicherheitsgewinn bringen kann, muss zusätzlich sichergestellt werden, dass ein Angreifer Eve C_{Z_A} auf keinen Fall ohne deutlich sichtbare Verzögerung auf einem Gerät G_E täuschend ähnlich zur Ausgabe auf Z_A reproduzieren kann. Die elektronisch angesteuerte Anzeige von C_{Z_A} auf einem Display ist dazu ungeeignet, da hier sehr geringe Latenzzeiten erzielt werden können, die für einen Menschen kaum wahrnehmbar wären.

Deutlich schwieriger ist es schon, einen Code C_{Z_A} ohne Verzögerung in einen gegenständlichen Ausdruck zu bringen, der sich noch dazu bereits in einem kompakten Gehäuse befinden muss. Nach Eingabe von den ersten J Zeichen könnte sich ein kleiner „Tresor“ öffnen, sodass der Zugriff auf C_{Z_A} für $Alice$ möglich wird. Die Prüfung von C_{Z_A} durch $Alice$ muss außerdem so erfolgen, dass C_{Z_A} dabei für Dritte nicht zu beobachten ist – also in jedem Fall unter einem Sichtschutz, eventuell nur haptisch.

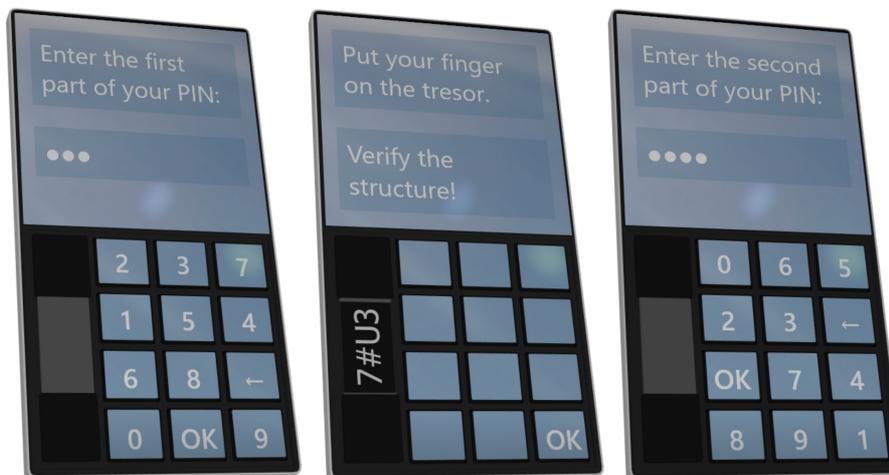


Abbildung 8: Gegenseitige Authentifikation mit einem sicheren Zugangssystem und $C_{Z_A} = 7\#U3$

Eine mögliche Lösung besteht darin, dass $Alice$ ihren Daumen auf die Schiebetür des „Tresors“ legt, bevor sich dieser öffnet. $Alice$ verdeckt so mit ihrem Finger den Code C_{Z_A} , während sie ihn ertasten kann. Der Daumen bleibt in jedem Fall auf der Schiebetür, bis der „Tresor“ wieder geschlossen ist. Abbildung 8 veranschaulicht das Prinzip der gegenseitigen Authentifikation.

Der Daumen und das Gehäuse des Code C_{Z_A} müssen C_{Z_A} nicht nur gegen das sichtbare Spektrum des Lichts abschirmen. Es darf für Angreifer nicht möglich sein, Informationen über die Beschaffenheit von Code C_{Z_A} zu gewinnen, während die Haut von $Alice$ den Code C_{Z_A} gut ertasten können muss. Entsprechend sorgfältig müssen die Materialien und

Strukturen ausgewählt werden.

Die gegenseitige Authentifikation muss nur durchgeführt werden, wenn das sichere Zugangssystem zwischenzeitlich aus der Hand gegeben wurde oder wenn es aus den Augen gelassen wurde. Ansonsten kann der Nutzer angemeldet bleiben, beliebige Lesezugriffe durchführen und das Publizieren oder Hinterlegen neuer Daten mit einem einzigen Knopfdruck auf dem Zugangssystem autorisieren (Single-Sign-On). Um zu verhindern, dass ein Anwender das angemeldete Zugangssystem versehentlich dritten überlässt, ist neben einem Timeout bei Nichtbenutzung auch der Einsatz von Sensoren denkbar, die eine Abmeldung durchführen, sobald sich die Person, welche die gegenseitige Authentifikation durchgeführt hat, vom Zugriffssystem entfernt.

SCHUTZ DER GEHEIMNISSE – NÖTIGENFALLS DURCH ZERSTÖRUNG

Vorausgesetzt wurde für die Überlegungen zum zuvor skizzierten Verfahren zur gegenseitigen Authentifikation mit zweigeteilter Passwordeingabe und mit dem Code C_{Z_A} , dass jeder Versuch eines Angreifers zum Auslesen von geheimen Daten aus Z_A ohne Kenntnis des Passwortes zum Scheitern verurteilt sein muss. Diese Voraussetzung muss durch geeignete technische Maßnahmen geschaffen werden.

Im Folgenden geht es um potenzielle Angriffe auf Zugangssysteme sowie auch auf andere Computersysteme des S-Netzwerks wie die S-Knoten, welche nicht ausschließlich über die intentionalen Schnittstellen dieser Systeme erfolgen (*Side Channel Attacks*). Ein Angreifer könnte beispielsweise versuchen, direkt durch Messungen die Zustände von einzelnen Bauelementen eines Speichers auszulesen, anstatt den Inhalt über den regulären Speichercontroller abzufragen.

Side Channels eignen sich insbesondere, um kryptografische Maßnahmen zum Schutz von geheimen Informationen zu umgehen. Selbst wenn vertrauliche Daten etwa immer nur verschlüsselt gespeichert werden, und sie nur bei Bedarf im Prozessor entschlüsselt werden, können durch physische Messungen über *Side Channels* eventuell bereits Rückschlüsse auf den Klartext gezogen werden.

Für derartige Attacken muss ein Angreifer so weit physischen Zugriff zu seinem Zielsystem erlangen, dass er Messungen durchführen kann. Einen einfachen und effektiven Schutz bietet daher die Verhinderung eben dieses Zugriffs durch Wachsamkeit und eine sichere, abgeschirmte Aufbewahrung.

Ein gegenständlicher Tresorraum mit etablierter Sicherheitstechnik etwa in Form einer hochgradig stabilen Außenwand mag zwar keinen perfekten Schutz gegen Eindringlinge bieten, er kann aber eine zusätzliche hohe Hürde bedeuten. Die S-Knoten können ohne Weiteres in einem Tresorraum betrieben und während des gesamten Betriebes in diesem verbleiben. Im Zusammenspiel mit weiteren Maßnahmen wie Videoüberwachung, Alarmanlagen und abgeschirmten Stromquellen lässt sich so für S-Knoten ein wirksamer Schutz gegen physische Angriffe realisieren.

Für Zugangssysteme des S-Netzwerks eignet sich ein derartiges Sicherungskonzept des Wegsperrens jedoch kaum: Nicht jeder Teilnehmer hat einen eigenen hochgradig sicheren gegenständlichen Tresor im Haus. Außerdem sollen die Zugangssysteme auch mobil nutzbar sein. Es ist davon auszugehen, dass Zugangssysteme mit relativ geringem Einsatz gestohlen oder geraubt werden können. Sie können sogar einfach verloren gehen und von Fremden gefunden werden.

Kann für ein Gerät nicht ausgeschlossen, dass es in die physische Kontrolle von Angreifern fällt, muss die Sicherheit vor den dadurch möglichen Angriffen in dem Gerät selbst gewährleistet werden.

Das direkte messtechnische Auslesen etwa von heute üblichen gewöhnlichen SRAM oder EEPROM Speicherzellen unter Umgehung der regulären Schnittstellen ist eine ernst zu nehmende Bedrohung. Ein Überblick für physische Attacken gegen konfigurierbare Hardware (FPGA) für kryptografische Anwendungen findet sich in [Wollinger 2003].

Viele physische Attacken zum Extrahieren von geheimen Informationen aus Mikro-Strukturen erfordern einen erheblichen technischen Aufwand und sehr präzise Messungen, was schon einen gewissen Schutz zumindest gegen Angreifer mit beschränkten Mitteln bieten kann.

Doch im Fall eines Zugangssystems Z_A mit zweigeteiltem Passwortschutz für das S-Netzwerk muss eben auch ein geheimer Code C_{Z_A} geschützt werden, der für den Besitzer manuell ohne weitere technische Hilfsmittel erkennbar oder ertastbar und validierbar sein muss. Dieser Code ist bei geöffnetem „Tresor“ mit einfachsten Mitteln auslesbar.

Es lässt sich nach derzeitigem technischem Kenntnisstand kein handliches und bezahlbares Gehäuse herstellen, das nicht aufgebrochen werden könnte. Jeder „Tresor“, der klein genug ist, um in ein mobiles Zugangssystem zu passen, kann mit Gewalt geöffnet werden. Was jedoch möglich erscheint, ist die Konstruktion eines Gehäuses, bei dem die geheimen Informationen im Fall eines gewaltsamen Eindringens zuverlässig unbrauchbar gemacht werden können.

Die Idee der Selbstzerstörung von Daten als letzte Schutzmaßnahme ist nicht neu. Entsprechende Erfindungen wurde etwa für SmartCards im Patent DE4018688C2 „*Verfahren zum Schutz einer integrierten Schaltung gegen das Auslesen sensibler Daten*“ (Hans-Detlef Brust 1998) und für Festplatten im Patent US 7099110 B2 „*Dead on demand disk technology*“ (Roger Detzler 2006) veröffentlicht. Auch einige kommerziell erhältliche Produkte setzen auf Zerstörung als Schutzmaßnahme, etwa der DataLocker Enterprise von eSecurityToGo, eine verschlüsselten Festplatte mit eigenem Keypad zur Passworteingabe, bei der im Fall von Brute Force Angriffen eine Selbstzerstörung ausgelöst werden kann (<http://www.esecuritytogo.com/ProductInfo.aspx?productid=DL1000E>, 2015-01-07).

Für die Selbstzerstörung physischer Systeme bei gewaltsamem Eindringen sind sowohl chemische als auch elektrische Mechanismen denkbar. Zur Zerstörung von digitalen Daten auf Speichermedien genügt eventuell bereits ein überschreiben. Das physische System muss dabei nicht dauerhaft unbrauchbar gemacht werden. Bei sicheren Zugangssystemen genügt es, wenn beim gewaltsamen Aufbrechen die geheimen Schlüssel für den Verbindungsaufbau zu S-Knoten zerstört werden. Der physisch ausgeprägte Code C_{Z_A} wird dadurch bereits unbrauchbar und wertlos. Eine Zerstörung des Codes C_{Z_A} muss nicht gewährleistet werden.

Angreifer können versuchen, Selbstzerstörungsmechanismen wirkungslos zu machen, etwa indem sie die Temperatur extrem ändern. Um dem entgegen zu wirken, kann es sinnvoll sein, verschiedene Mechanismen zu kombinieren.

Das S-Netzwerk bietet grundsätzlich gute Voraussetzungen für die Selbstzerstörung als letzte Schutzmaßnahme für die Wahrung von Geheimnissen: Sowohl Zugangssystem als auch einzelne S-Knoten können im Notfall zerstört werden, ohne dass dies irreversible Verluste zur Folge hätte und ohne dass dies die Garantien des S-Netzwerks bezüglich der Verfügbarkeit der darin publizierten oder hinterlegten Informationen verletzt würde. Die auf diesen Systemen gespeicherten geheimen Schlüssel dienen nur dem Schutz der Kommunikation – sie können durch neue manuell auszutauschende Schlüssel ersetzt werden. Die zu bewahrenden Inhalte von bis zu $\Psi-1$ beliebigen komplett zerstörten S-Knoten können jederzeit wiederhergestellt werden.

Bei anderen die Vertraulichkeit währenden Speicherdiensten wie etwa dem in [Klieme 2011] vorgeschlagenen elektronischen Safe ist die Selbstzerstörung hingegen keine zulässige Option – hier sind private Schlüssel unbedingt geheim zu halten und zugleich zu bewahren, andernfalls sind die Daten verloren. Client und / oder Safe Anbieter sind hier ein Single Point of Failure ([Klieme 2011], S. 58).

Für sichere Zugangssysteme zum S-Netzwerk erscheint es in jedem Fall sinnvoll und angemessen, den Einbau von wirksamen Selbstzerstörungsmechanismen zu verlangen. Hochgradig mobile Zugangssysteme fallen einfach zu leicht in die Hände potenzieller Angreifer. Die Zerstörung eines sicheren Zugangsgärts verhindert nur temporär den Zugang eines einzigen Teilnehmers am S-Netzwerk.

Zweifelhafter ist der Nutzen von Selbstzerstörung bei S-Knoten. S-Knoten können physisch geschützt und abgeschirmt werden. Sie können tatsächlich in bewachten Tresorräumen betrieben werden. Außerdem könnten Angreifer versuchen, Selbstzerstörungsmechanismen auf S-Knoten dazu zu missbrauchen, unliebsame Inhalte zu beseitigen. Angreifern würde es genügen, die Selbstzerstörung auf Ψ S-Knoten zu aktivieren. Bei S-Knoten muss der potenzielle Nutzen sorgfältig gegen die Gefahren abgewogen werden, welche durch Selbstzerstörungsmechanismen erst entstehen. Es braucht also ein Risikomanagement.

2.5 ERGÄNZUNGEN ZUR ANONYMISIERUNG

2.5.1 ENTKOPPLUNG DER VERSCHIEDENEN AUFGABEN DER ANONYMISIERUNG

Dazu kann die Kommunikation von jenen Diensten, welche die Prüfung der Identität bewältigen sollen, hin zu jenen Diensten, welche die Prüfung des Inhalts bewältigen sollen, indirekt über zusätzliche Weiterleitungsdienste abgewickelt werden. Die Idee dabei ist, dass ein Dienst, der die Identität des Kommentators prüfen soll, mindestens Informationen von $T-2$ verschiedenen Diensten zur Weiterleitung benötigt, um einen Dienst zu identifizieren, der die Prüfung des Inhalts durchführen soll und umgekehrt.

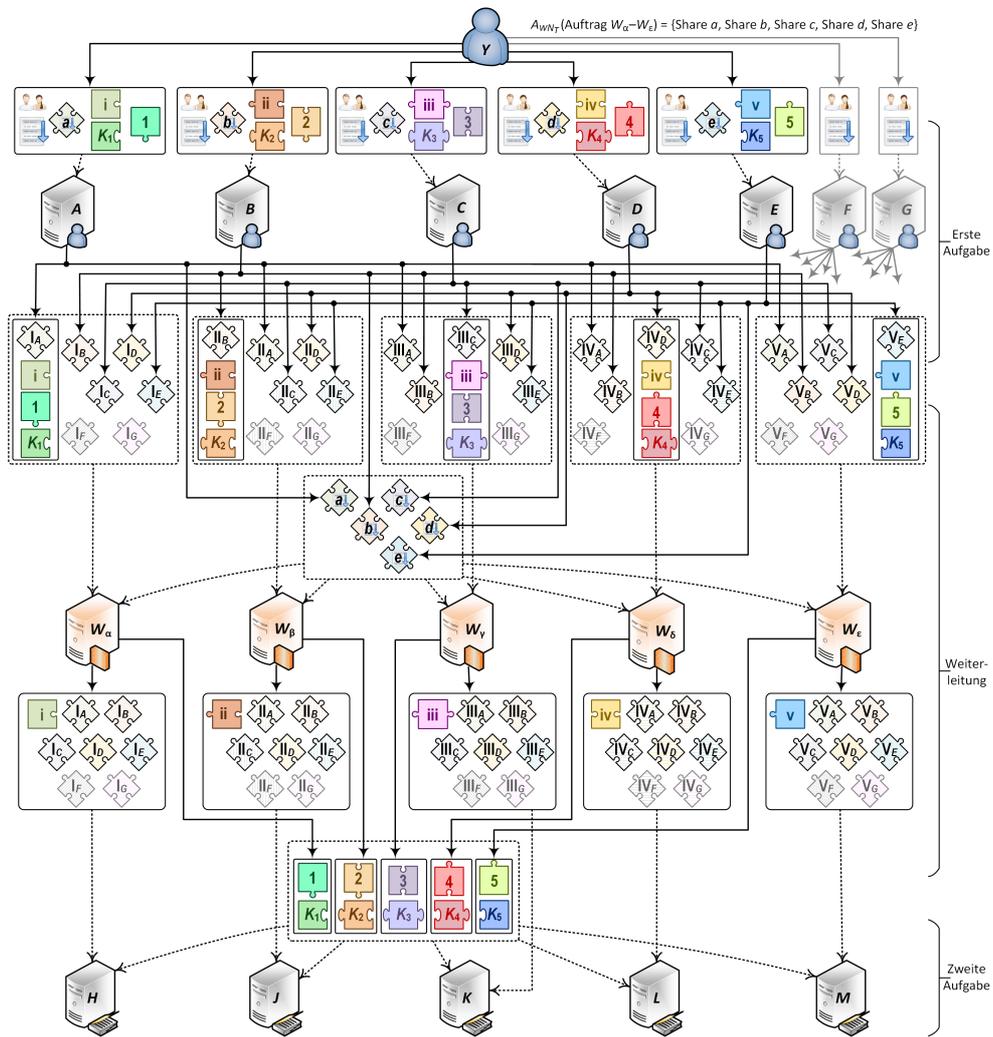
Jeder Auftrag zu einer Weiterleitung muss dabei von mindestens T verschiedenen Diensten bestätigt werden. Die kritischen Informationen, welche nur Dienste zur Bewältigung der ersten Aufgabe und Dienste zur Bewältigung der dritten Aufgabe benötigen – also die Zugehörigkeitsbescheinigungen – müssen vor der Sendung zum ersten weiterleitenden Dienst so zerlegt werden, dass daraus kein weiterleitender Dienst Informationen über die Identität des Kommentators gewinnen kann. Ebenso dürfen jene kritischen Informationen, die nur zur Bewältigung der zweiten Aufgabe benötigt werden – also der Inhalt κ – keinem weiterleitenden Dienst zugänglich gemacht werden. Ihre Zerlegung darf also erst im letzten Weiterleitungsschritt aufgehoben werden.

Jedem Dienst dürfen nur jene Dienste genannt werden, an welche unmittelbar Nachrichten zu senden sind. Informationen darüber, wo ein Auftrag herkommt, dürfen nicht weitergegeben werden. Jeder Auftrag zur Weiterleitung muss bereits vom Kommentator per Secret Sharing geschützt werden und die Shares dürfen erst bei genau den Weiterleitungsdiensten zusammenkommen, für welche der Auftrag jeweils bestimmt ist.

Abbildung 9 visualisiert das Prinzip der Weiterleitung für einen *Threshold* $T=3$ und $N=5$, also mit Redundanz. Die Dienste F und G dienen ausschließlich zur Zugehörigkeitsbestätigung und sie werden nur benötigt, damit Ausfallsicherheit geboten werden kann, wenn das offene Secret Sharing von Mengen zum Einsatz kommt, um die genaue Zusammensetzung der Gruppe G geheim zu halten.

Wenn der *Threshold* größer als zwei ist, sollte zwischen Diensten zur Prüfung der Zulässigkeit des Inhalts (zweite Aufgabe) und Diensten zur Veröffentlichung des Kommentars (dritte Aufgabe) ebenfalls nur indirekt über $T-2$ Weiterleitungsdienste kommuniziert werden, damit weniger als T Dienste keinen Zusammenhang zwischen Inhalt und Ziel des Kommentars herstellen können.

Insgesamt wird somit zur Anonymisierung von Kommentaren ein regelrechtes Geflecht mit mindestens $(3+2*(T-2))*T$ verschiedenen Diensten benötigt – wobei mit dieser Anzahl noch keine Redundanz besteht. Anstatt einfach auf einen hohen *Threshold* T zu setzen, bietet es sich an, wiederum auf die Verteilung der Verantwortung über verschiedenen Misstrauensparteien zu setzen, sodass die Bildung von manipulativen Kollaborationen zwischen verschiedenen Betreibern von Diensten zur Anonymisierung riskant wird. Es kann dabei eventuell an die für das S-Netzwerk ohnehin vorgesehene Schaffung von Misstrauensparteien angeknüpft werden. In jedem Fall können S-Netzwerk sowie S-Web genutzt werden, um eine zuverlässige Kommunikation in dem Anonymisierungsverfahren abzusichern und um insbesondere unleugbare Bestätigungen weitergeben zu können.



Legende zur Bedeutung der Pfeile:

Wer publiziert / hinterlegt was Auf was besteht Leseszugriff durch wen

Abbildung 9: Teil des Verfahrens für anonyme Kommentare mit Weiterleitung bei $T=3$

2.5.2 ANONYMES QUANTIFIZIERBARES BEWERTEN UND ABSTIMMEN

Um unabhängige Werturteile oder Wahlergebnisse zu erhalten, ist Anonymität wichtig. Zugleich dürfen nicht beliebig viele Stimmen derselben Person in das Ergebnis einfließen. Mit dem S-Web, spezialisierten externen Anonymisierungsdiensten und *sperrenden Bestätigungen* lassen sich beide Anforderungen erfüllen. Zusätzlich kann auch die Möglichkeit geschaffen werden, die eigene anonymisierte Stimme nachträglich zu ändern. Bei vollständiger Überprüfbarkeit auf Korrektheit lässt sich mithilfe von *Meilensteinen* eine konstante Auswertungszeit für die Ergebnisse unabhängig von der Anzahl der abgegebenen Stimmen erzielen.

Das in der Dissertation erörterte Problem, anonyme Kommentare zu ermöglichen, für die zugleich die Zugehörigkeit des Kommentators zu einer gewissen Gruppe von Personen bescheinigt wird, ist nah verwandt mit den Herausforderungen der anonymen Bewertungen und anonymen Abstimmungen. Auch bei Bewertungen sowie Abstimmungen muss es in der Regel trotz Anonymität nachweisbar sein, dass die Wertung oder Stimme von einer Person aus einer Gruppe von Stimmberechtigten stammt. Dennoch gibt es einige Unterschiede:

Anders als bei Kommentaren ist die inhaltliche Zulässigkeit nach der S-Verfassung bei typischen Bewertungen etwa mit Schulnoten oder mit null bis fünf Sternen kein Thema: Der Inhalt der Bewertung ist nicht mehr als eine Zahl und als Werturteil fällt die Bewertung eines beliebigen Ziels gemäß der S-Verfassung immer unter den Schutz der Meinungsfreiheit. Bei Abstimmungen sind lediglich die beschränkten Wahlmöglichkeiten, welche vorab und ohne Anonymisierung publiziert werden, auf inhaltliche Zulässigkeit zu prüfen – die einzelnen Stimmen enthalten wiederum nur Zahlen.

SICHERSTELLEN, DASS JEDER STIMMBERECHTIGTE HÖCHSTENS EINE STIMME PRO ZIEL HAT

Bei Bewertungen und Abstimmungen wird verlangt, dass jede Person aus einer Gruppe G der Stimmberechtigten für ein Ziel X höchstens eine Bewertung bzw. Stimme abgeben darf. Im Vergleich zu Kommentaren ist also eine zusätzliche Art von identitätsbezogener Zulässigkeitsprüfung erforderlich. Über die Bescheinigung der Zugehörigkeit zu G hinaus ist für anonyme Bewertungen und Abstimmungen unbedingt zu gewährleisten, dass jede beliebige Person Y aus G zu dem Ziel X höchstens eine Stimme abgeben kann, ohne dass feststellbar ist, ob und wie Y über das Ziel X wirklich abgestimmt hat.

Zur Durchführung der anonymen Stimmabgabe kann wiederum ein Geflecht von verschiedenen Anonymisierungsdiensten eingesetzt werden, ähnlich wie zur anonymen Kommentierung. Allerdings müssen die Dienste, welche die Identität von Auftraggeber Y erfahren und welche die Zugehörigkeit von Y zur Gruppe G prüfen sollen, zusätzlich auch sicherstellen, dass Y für Ziel X nur maximal eine anonyme Stimme abgibt. Als Ergebnis der Prüfungen soll im Erfolgsfall letztlich von mindestens *Threshold* T Diensten bestätigt werden, dass der Auftrag von einer Person aus G stammt und dass die Person zum ersten und einzigen Mal für X eine Stimme abgibt, ohne die Identität des Auftraggebers Y zu verraten. So wie vor diesen Diensten etwa mithilfe des offenen Secret Sharings für Mengen die genaue Zusammensetzung der Gruppe G geheim gehalten werden kann, soll vor ihnen auch das genaue Ziel X der Abstimmung oder Bewertung verborgen bleiben können.

Die Idee um das zu erreichen ist, dass Y zunächst eine Menge P von mehreren potenziellen Zielen generiert, welche Ziel X enthält. Für jedes Ziel in der Menge P veröffentlicht Y eine leere persönliche Stimme, die fortan als *sperrende Bestätigung* dafür gilt, dass für dieses Ziel nur eine anonyme (eventuell wiederum leere) Stimme abgegeben wird. Für sämtliche Ziele in P kann von Y in einem gemeinsamen Auftrag anonym abgestimmt werden, wobei auch eine leere anonyme Stimme zulässig ist. Alle *sperrenden Bestätigungen* werden dazu von Y mit einem *öffentlichen Auftrag* an die ersten

Anonymisierungsdienste verlässlich verlinkt. Dadurch, dass sowohl die *sperrenden Bestätigungen* als auch der Auftrag öffentlich sind, können die ersten Anonymisierungsdienste prüfen, dass Y tatsächlich zuvor noch für kein Ziel in P eine Stimme abgegeben hat und dass Y noch keine andere Anonymisierung in Auftrag gegeben hat.

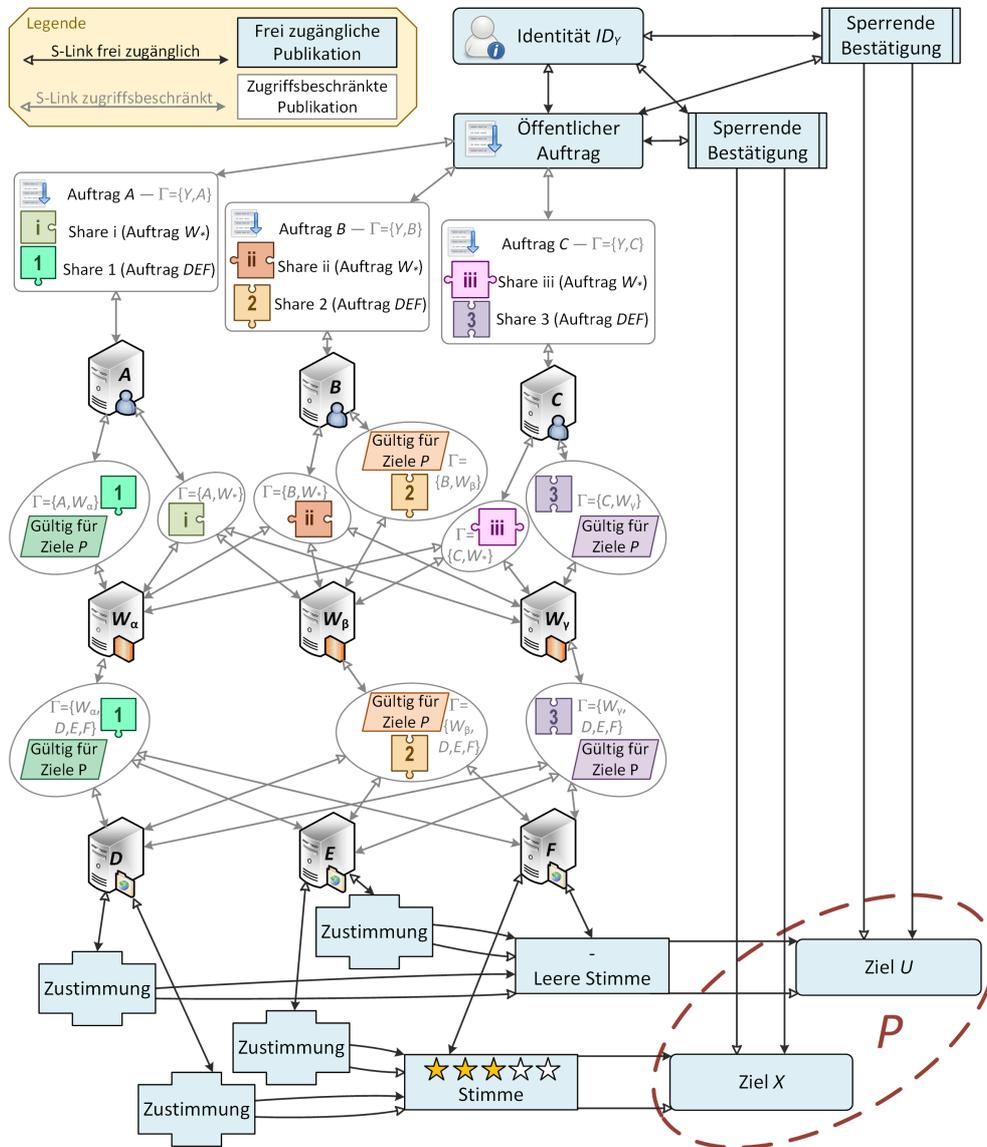


Abbildung 10: Verfahren zur Anonymisierten Abstimmung mit Threshold 3

Jeder erste Anonymisierungsdienst erhält zusätzlich noch individuelle geheime Informationen, und zwar jeweils genau einen Share von jeder Secret Sharing Zerlegungen der Aufträge für die in dem Verfahren nachfolgenden Anonymisierungsdienste. Die tatsächlichen Stimmen werden durch das Secret Sharing vor den ersten Anonymisierungsdiensten geheim gehalten. Nach erfolgreicher Prüfung, dass Y jedes Ziel in P maximal einmal bewertet, bestätigt jeder erste Anonymisierungsdienst den nachfolgenden Anonymisierungsdiensten lediglich, dass für diesen Anonymisierungsauftrag für alle Ziele in P eine korrekte *sperrende Bestätigung* vom Auftraggeber durchgeführt wurde. Dabei bleibt die Identität von Auftraggeber Y geheim.

Abbildung 10 zeigt beispielhaft die im Zuge der Anonymisierung der Stimmen von Auftraggeber Y für die Ziele in P (U und X) entstehenden Datenstrukturen. Jeder der ersten Anonymisierungsdienste A , B und C bescheinigt die Gültigkeit der zu anonymisierenden Stimmabgaben für alle Ziele in P . Die in dem Verfahren nachfolgenden Anonymisierungsdienste W_α , W_β und W_γ erfahren weder die Identität von Y noch die Stimmwerte für die Ziele in P . Der finale Anonymisierungsdienst F veröffentlicht die anonymen Stimmen. Die anderen beiden finalen Anonymisierungsdienste D und E beglaubigen die anonyme Stimme lediglich, sodass jeweils nur eine anonyme Stimme pro Ziel publiziert wird.

DIE MÖGLICHKEITEN UND GRENZEN DER ANONYMISIERUNG MIT SPERRENDEN BESTÄTIGUNGEN

Mit den *sperrenden Bestätigungen* von potenziellen Zielen P wird nicht verraten, welche der Ziele in P tatsächlich eine gültige anonyme Stimme erhalten und welche dieser Ziele nur eine leere Stimme erhalten. Eventuell lassen sich jedoch aus der Kombination der öffentlich zugänglichen Informationen der *sperrenden Bestätigungen* und der finalen anonymen Stimmen trotzdem Rückschlüsse ziehen.

Damit eine anonyme Stimme nicht eindeutig mit der *sperrenden Bestätigung* in Verbindung gebracht werden kann, muss zunächst einmal eine gewisse zeitliche Trennung zwischen der Sperrung und der Publikation der Stimme durch finale Anonymisierungsdienste sichergestellt werden. Ansonsten wäre die Wahrscheinlichkeit hoch, dass unmittelbar nach *sperrenden Bestätigungen* von Zielen in P anonym publizierte Stimmen zu Zielen in P eben mit der Sperrung zusammenhängen. Es bietet sich an, Sperrungen und anonyme Stimmen mit großer zeitlicher Unschärfe zu versehen, also ein großes Publikationszeitintervall anzugeben und den Gültigkeitszeitraum nur zu bestimmten regelmäßigen Terminen beginnen zu lassen, beispielsweise jeweils zum Ersten des Monats.

Um sich selbst zu schützen, sollte Y die Menge P außerdem so bilden, dass jedes einzelne Ziel in P jeweils von anderen Personen als potenzielles Ziel gesperrt wird – und zwar zeitnah, in demselben Publikationsintervall. Dazu ist es zweckdienlich, zu bewertende Ziele vorab anonym an Sammelstellen zu registrieren. Wer eine Bewertung durchführen möchte, der fügt seiner Menge P an potenziellen Zielen einige zuvor bei der Sammelstelle gemeldete Ziele hinzu; möglichst solche, für die erst wenige *sperrende Bestätigungen* als potenzielles Bewertungsziel abgegeben werden. Selbst für Ziele, die tatsächlich im Publikationsintervall nur eine einzige anonyme Bewertung erhalten würden, können so diverse sperrende Bestätigungen der potenziellen Bewertung durch verschiedene Personen erschaffen werden. Damit steigt die Wahrscheinlichkeit, dass zu Beginn des Gültigkeitszeitraums der anonymen Stimmen für jedes Ziel jeweils eine ganze Reihe von *sperrenden Bestätigungen* existieren, welche im gleichen Publikationszeitraum erschaffen wurden.

Es ist jedoch, selbst wenn für ein Ziel X zeitnah viele *sperrenden Bestätigungen* erfolgen und entsprechend viele anonyme Stimmabgaben in Auftrag gegeben werden, nicht sicher, dass damit auch das gewünschte Maß an Anonymität erzeugt werden kann. Wenn alle Sperrungen für das potenzielle Ziel X auch zu einer gültigen, nicht leeren Stimme führen würden, wäre für alle ersichtlich, dass jede Person, die eine Sperrung für X publiziert, auch wirklich über Ziel X abgestimmt hat. Hätten gar alle Stimmen zufällig den gleichen Wert, wäre die Anonymität komplett aufgehoben.

Wenn für ein Ziel im Publikationszeitintervall keine *sperrenden Bestätigungen* und Aufträge vorliegen, für die leeren Stimmen publiziert werden sollen, so könnten die Auftraggeber von den Anonymisierungsdiensten zumindest gefragt werden, ob sie entweder auf die Anonymität oder auf die Bewertung verzichten möchten.

NACHTRÄGLICHE ÄNDERUNGEN DER EIGENEN STIMME

Mit *sperrenden Bestätigungen* für anonyme Stimmen lässt sich verhindern, dass versehentlich mehrere Stimmen einer Person für dasselbe Ziel in die Auswertung aufgenommen werden. Nach dem bisher vorgestellten Verfahren bleibt jedes Ziel in der Menge P fortan für den Auftraggeber Y gesperrt – unabhängig davon, ob im Zuge des Anonymisierungsauftrags eine gültige Stimme oder eine leere Stimme publiziert wird.

Es kann jedoch je nach Anwendungsfall auch wünschenswert sein, dass Nutzer ihre eigene Stimme nachträglich noch ändern können. Gerade um die Bereitschaft zu stärken, Ziele alleine zur Unterstützung der Anonymisierung mit einer *sperrenden Bestätigung* zu blockieren und eine leere Stimme abzugeben, dürfte es sehr förderlich sein, wenn diese

Stimme nachträglich noch geändert werden könnte.

Aufsetzend auf dem bisher gezeigten Verfahren für anonyme Abstimmungen kann erlaubt werden, dass Auftraggeber Y nachträglich für einzelne Ziele in P Änderungen an den jeweiligen Stimmwerten in Auftrag geben darf. Dazu erteilt Y genau den ersten Anonymisierungsdiensten, welche Y schon mit der ursprünglichen anonymen Abstimmung für alle Ziele in P betraut hat, einen geheimen Zusatzauftrag, wobei die Stimmänderung durch Secret Sharing geschützt vor den ersten Anonymisierungsdiensten geheim bleibt. Der Zusatzauftrag für die Änderung wird dann von den ersten Anonymisierungsdiensten über die gleichen nachfolgenden Anonymisierungsdienste weitergeleitet wie bei der ursprünglichen Stimmabgabe. Die Änderung der Stimme wird schließlich von einem finalen Anonymisierungsdienst als S-Link mit der ursprünglichen Stimme verlässlich verknüpft und von *Threshold* T minus eins weiteren finalen Anonymisierungsdiensten bestätigt.

Bei der Auswertung zählt immer nur die letzte Änderung im Auswertungszeitraum. Es bleibt weiterhin möglich, das Ergebnis zu einem früheren Zeitpunkt zu berechnen und die Änderungen nachzuvollziehen.

IMPLEMENTIERUNG VON ANONYMEN ABSTIMMUNGEN UND TEST DER AUSWERTUNGSPERFORMANCE

Eine Auswertung von den persönlich sowie anonym abgegebenen Stimmen kann vollständig auf den S-Knoten durchgeführt werden, ohne dass diese Systeme dafür spezielle Funktionalität bereitstellen müssten. Die notwendigen Abfragen über die S-Links sind durchaus komplex, gerade wenn Änderungen der Stimmen erlaubt sein sollen. Abbildung 11 zeigt die durchzuführenden Schritte.

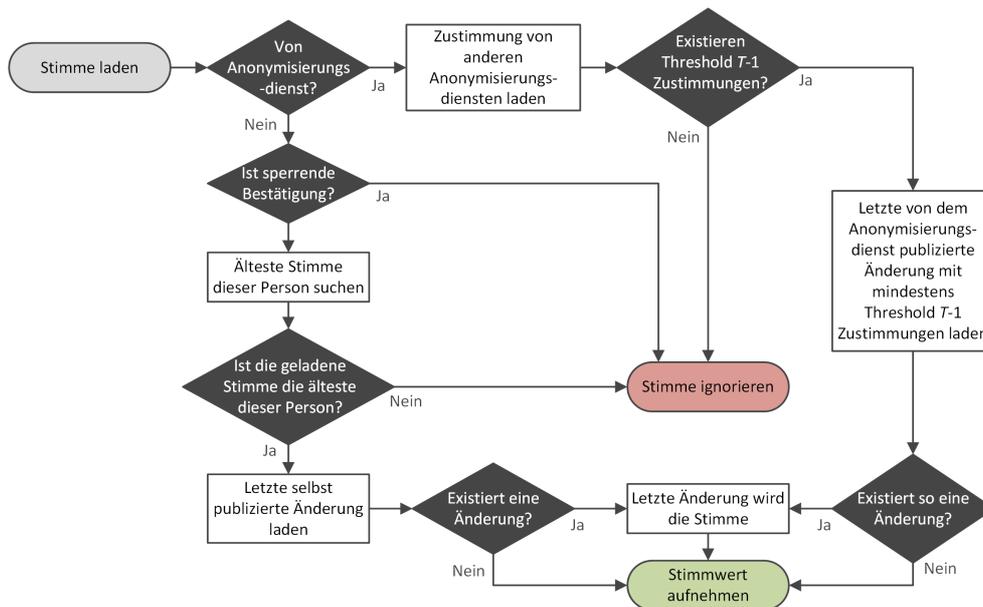


Abbildung 11: Entscheidungsdiagramm für die Auswertung von Abstimmungen

Die Ausführung solcher Anfragen kann signifikant Rechenzeit und Speicher benötigen. Es ist zwar nur eine zur Anzahl der Stimmen lineare Zunahme zu erwarten, aber dennoch könnte sich daraus eine erhebliche Last für die S-Knoten ergeben. Außerdem sollen Abstimmungsergebnisse schnell verfügbar sein und es liefert keinen Mehrwert, immer wieder die gleiche Abzählung durchführen zu lassen.

Stattdessen bietet es sich an, regelmäßig die Ergebnisse bis zu einem gewissen Zeitpunkt als *Meilenstein* abzuspeichern. Bei neuen Abfragen über das Ergebnis werden dann nur die Stimmen seit dem letzten *Meilenstein* analysiert. Nichtsdestotrotz kann im S-Web

jederzeit die Auszählung zwischen zwei beliebigen *Meilensteinen* überprüft werden. Werden regelmäßig *Meilensteine* publiziert und werden vorangehende Meilensteine nicht oder nur stichprobenartig geprüft, ist für die Auswertung eine nahezu konstante Performance unabhängig von der Anzahl der insgesamt abgegebenen Stimmen zu erwarten.

Zur Überprüfung dieser Erwartungen und zur Veranschaulichung des Potenzials wurde eine Implementierung von Anonymisierungsdiensten für Abstimmungen geschaffen, welche zusammen mit dem S-Netzwerk-Demonstrator betrieben werden kann. Die im Folgenden dargestellten Messwerte wurden auf einem Dell Precision 7510 Notebook mit Intel i7-6820HQ Quadcore (2.7Ghz), 16 GByte RAM und 256 GByte Solid State Disc ermittelt. Jeder hier angegeben Wert ist der arithmetische Mittelwert aus drei einzelnen Messergebnissen, welche wiederum die mittleren Ergebnisse aus fünf Einzelmessungen sind.

Tabelle 4 und Abbildung 12 zeigen den quasi linearen Anstieg der benötigten Rechenzeit mit der Anzahl der Stimmen. Schwankungen ergeben sich gerade bei vielen Stimmen insbesondere durch das Caching der großen Datenmengen – die absolut erzielbare Performance ist hochgradig implementierungsabhängig. Mit Meilensteinen zeigt sich ab 100 Stimmen im Rahmen der Messgenauigkeit wie zu erwarten eine konstante Performance.

Anzahl der Stimmen	Dauer in Sekunden ohne Meilensteine	Dauer in Sekunden mit Meilensteinen alle 100 Stimmen
10	0,03 s	0,03 s
100	0,09 s	0,08 s
1.000	0,90 s	0,08 s
10.000	4,70 s	0,09 s
100.000	39,00 s	0,09 s
1.000.000	568,19 s	0,08 s

Tabelle 4: Performance der Evaluation einer anonymen Abstimmung mit Threshold 3

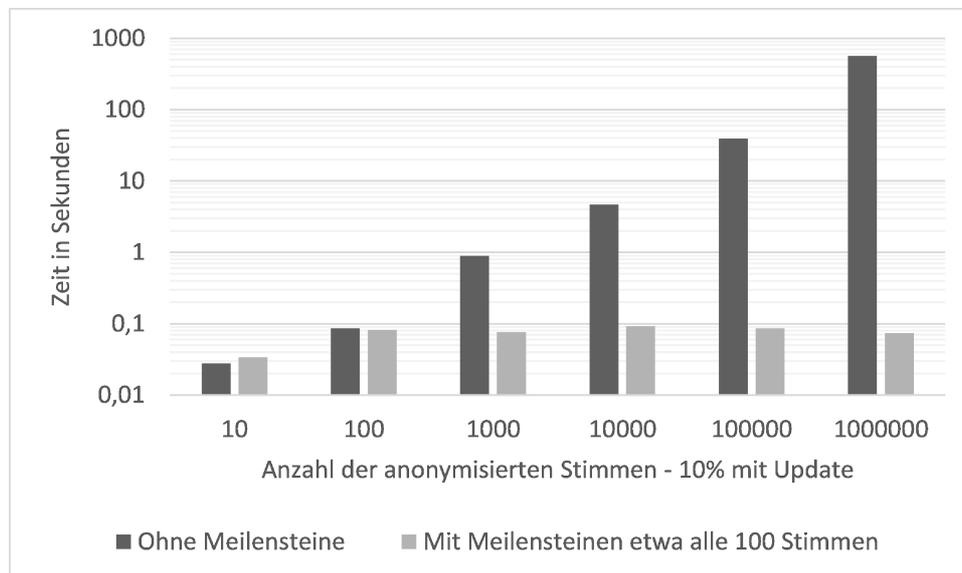


Abbildung 12: Performance der Evaluation einer anonymen Abstimmung mit Threshold 3

Ein höherer *Threshold T* bietet zwar einen besseren Schutz, führt aber auch zu einer geringfügig höheren Rechenlast. Tabelle 5 und Abbildung 13 zeigen die Messergebnisse für die Auswertung von 10.000 Stimmen, von denen 1000 nachträglich geändert wurden mit verschiedenen *Thresholds*.

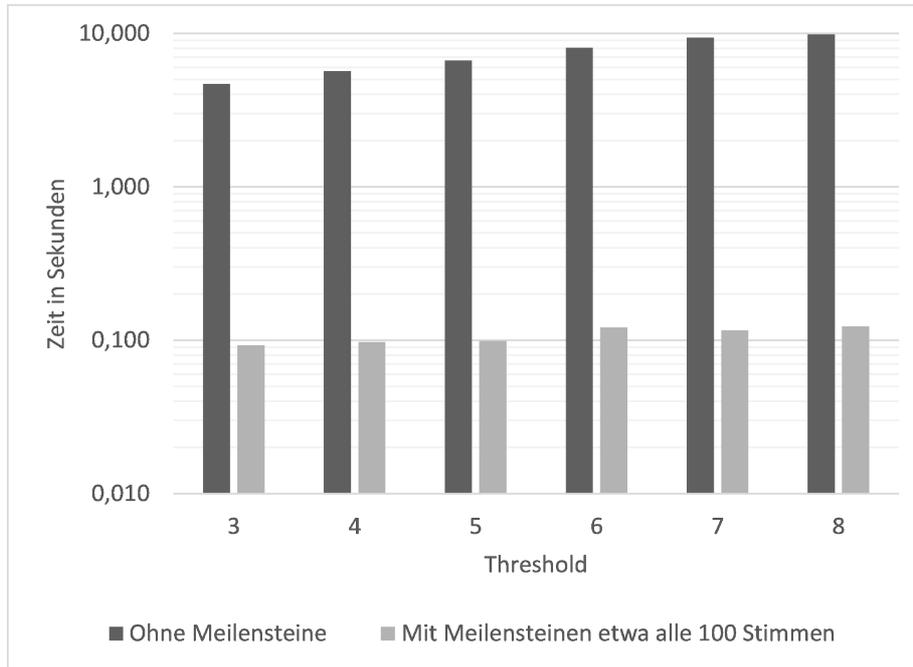


Abbildung 13: Abhängigkeit der Dauer der Analyse anonymer Abstimmungen vom Threshold

Threshold	Dauer in Sekunden ohne Meilensteine	Dauer in Sekunden mit Meilensteinen alle 100 Stimmen
3	4,70 s	0,09 s
4	5,67 s	0,10 s
5	6,66 s	0,10 s
6	8,05 s	0,12 s
7	9,37 s	0,12 s
8	9,88 s	0,12 s

Tabelle 5: Abhängigkeit der Performance der Analyse anonymer Abstimmungen vom Threshold

ÜBERPRÜFBARKEIT DER KORREKTHEIT

Neben der Erhöhung des *Thresholds* T für die Anzahl der Anonymisierungsdienste, von denen Übereinstimmung gefordert wird, gibt es weitere Möglichkeiten, um die Korrektheit der anonymisierten Stimmen zu forcieren. Zum einen muss die Anzahl der anonymen Stimmen für jedes Ziel immer kleiner gleich der Anzahl der *sperrenden Bestätigungen* verschiedener Herausgeber für das Ziel sein. Anonymisierungsdienste können nur so viele anonyme Stimmen publizieren, wie sie Aufträge von verschiedenen Auftraggebern erhalten.

Ist die Anonymität nur optional, kann weiters erlaubt werden, dass Auftraggeber ihre Stimme mit einem zufälligen Identifikationsmerkmal ausstatten, welches zusammen mit der anonymisierten Stimme publiziert werden muss. Sind die Zufallsdaten hinreichend groß, kann der Auftraggeber dann seine eigene anonymisierte Stimme mit hoher Sicherheit identifizieren. Wenn die eigene Stimme nicht korrekt anonym publiziert wurde, kann der Auftraggeber jeden einzelnen am Verfahren beteiligten Anonymisierungsdienst separat überprüfen lassen. Jegliche Kommunikation in dem Verfahren ist unleugbar im S-Netzwerk hinterlegt. Eine Untersuchungskommission kann für einen von ihr zu analysierenden Schritt

kontrollieren, ob der involvierte Anonymisierungsdienst korrekt gearbeitet hat. Dazu muss der Untersuchungskommission nur die Kommunikation mit dem zu untersuchenden Dienst offenbart werden. Keine einzelne Untersuchungskommission muss sowohl die Identität des Auftraggebers als auch das Ziel und den Stimmwert erfahren. Für unterlassene oder falsch ausgeführte Schritte kann rechtlich eine Nachbesserung durchgesetzt werden.

VERTRAULICHE ABSTIMMUNGEN MIT GEHEIMEN ERGEBNISSEN

Im vorgestellten Verfahren für anonyme Kommentare ist vorgesehen, dass von den finalen Anonymisierungsdiensten lediglich vom Kommentator erzeugte Shares des Kommentars im S-Netzwerk publiziert werden. Dadurch bleibt der Inhalt κ des Kommentars vor diesen Diensten geheim. Wird dieser Ansatz auf ein Verfahren für anonyme Bewertungen oder Abstimmungen übertragen, hat das Konsequenzen:

Per Secret Sharing zerlegte und geschützte Stimmen können nicht lokal auf S-Knoten ausgewertet werden, da die Stimmwerte nicht im Klartext vorliegen. Um etwa den Durchschnitt über alle Bewertungsergebnisse zu berechnen, müssen für jede einzelne Bewertung mindestens *Threshold T* Shares von verschiedenen S-Knoten geladen und vereint werden.

Außerdem kann jede vom Auftraggeber selbst per Secret Sharing geschützte Stimme auch vom Auftraggeber identifiziert werden. Der Auftraggeber hat die zufälligen Shares mit Prüfdaten selbst erzeugt und er kann sie wiederfinden. Er kann obendrein beweisen, dass die von ihm beauftragte anonymisierte Stimme von ihm stammen muss: Dazu genügt es, die Shares sicher im S-Netzwerk zu hinterlegen, bevor der Auftrag zur anonymen Abstimmung erteilt wird. Nur der Auftraggeber kennt schon vorab die Shares seiner Stimme und die Zeitangabe der sicheren Hinterlegung kann dieses frühzeitige Wissen beweisen. Die Selbstoffenbarung der eigenen Stimme ist so möglich – die Anonymität ist nur optional.

GEHEIME WAHLEN MIT DEM S-NETZWERK

Bei vielen Abstimmungen und Wahlen sollen während des Abstimmungsvorgangs noch keine Teilergebnisse veröffentlicht werden, damit andere Wähler nicht von Zwischenresultaten in ihren Entscheidungen beeinflusst werden. Wenn die Stimmen für eine schnelle Auswertung auf den S-Knoten von den finalen Anonymisierungsdiensten im Klartext veröffentlicht werden sollen, könnten die finalen Anonymisierungsdienste vorab auch Zwischenergebnisse verraten. Um das zu verhindern, sollten die finalen Anonymisierungsdienste erst zum Ende des Abstimmungszeitfensters Shares von den zu veröffentlichenden Stimmen erhalten.

Bei streng geheimen und freien Wahlen ist die Geheimhaltung der eigenen Stimme nicht optional, sondern verpflichtend. Für eine streng geheime Wahl muss deshalb zusätzlich sichergestellt werden, dass bei der Stimmabgabe kein Zeuge zugegen ist und dass keine Aufzeichnungen davon angefertigt werden. Eine streng geheime und freie Wahl kann folglich kaum aus der Ferne von einem unkontrollierten Ort aus durchgeführt werden. Die in Deutschland mögliche Briefwahl ist keine geheime Wahl in diesem strengen Sinne: Die Wahlzettel könnten in der Gegenwart von Zeugen ausgefüllt und als Briefe aufgegeben werden, sodass die Geheimhaltung der Stimme nicht gewährt wäre. Oder die Wahlzettel könnten unter dem Druck von Erpressern ausgefüllt sowie von diesen kontrolliert aufgegeben werden. Wenigstens gegen letztere Bedrohung sind beim S-Netzwerk mit dem Alarmcode bei sicheren Zugangsgeräten Maßnahmen vorgesehen (siehe Anhang 2.4). Gegen Bezeugungen von Wahlentscheidungen gibt es hingegen bei der Stimmabgabe an unkontrollierten Orten auch mit dem S-Netzwerk keinen Schutz.

An dem Einsatz von speziellen Wahlkabinen führt bei einer streng geheimen und freien Wahl beim gegenwärtigen Stand der Forschung und der Technik kein Weg vorbei. Das S-Netzwerk könnte lediglich im Zusammenspiel mit Wahlkabinen für die Stimmabgabe sowie für die papierlose Sammlung, Aufbewahrung und Auswertung der Stimmen streng geheimer Wahlen genutzt werden.

2.6 GESTALTUNG UND ADAPTIERUNG

Jeder Interessent soll sich aktiv daran beteiligen können, das S-Netzwerk zu erschaffen, es an neue Gegebenheiten anzupassen und es zu evaluieren sowie zu verbessern. Für die initiale Gestaltung und für die im laufenden Betrieb erforderlichen organisatorischen Abläufe müssen Konzepte entwickelt werden, welche es ermöglichen, sich mit dem S-Netzwerk in seiner fortschreitenden Entwicklung zu identifizieren.

2.6.1 AUFBAU, LEGITIMIERUNG UND ORGANISATION

Damit das S-Netzwerk realisiert werden kann, müssen die Standards und Regeln der S-Verfassung in offener Diskussion gefunden, ausgestaltet und durch eine Abstimmung ausgewählt werden. Auch wenn das S-Netzwerk bereits besteht, muss es möglich sein, Änderungen an der S-Verfassung vorzunehmen, damit etwa neue technische oder politische Entwicklungen berücksichtigt werden können.

Trotz des Minimalitätsprinzips ist die Umsetzung des S-Netzwerks eine intradisziplinäre Herausforderung, bei der größte Sorgfalt geboten ist, um nicht leichtfertig das Vertrauen in das S-Netzwerk unwiederbringlich zu beschädigen oder zu zerstören.

Schon bei der Ausgestaltung des innersten Kerns des S-Netzwerks gibt es erheblichen Spielraum: Je nachdem, wie die Standards der S-Verfassung formuliert und ausgerichtet werden, kann der Charakter des Gesamtsystems höchst unterschiedlich angelegt werden.

Es muss beispielsweise festgelegt werden, wie weit die Freiheitsrechte gehen sollen. Für das Konzept zur Vertrauensbildung durch Misstrauensparteien müssen etwa deren Anzahl und die Grenzen der einzelnen Misstrauensparteien bestimmt werden.

Wer trifft letztlich die Entscheidungen: Was soll die S-Verfassung regeln, erlauben, vorschreiben oder verbieten? Wie konkret sollen die Vorgaben zur Implementierung sein und wie sollen sie ggf. an neue Anforderungen angepasst werden? Wie wird sichergestellt, dass die Standards der S-Verfassung auch eingehalten werden und dass sich die Teilnehmer möglichst mit den dahinter steckenden Ideen identifizieren können?

Die genaue Festlegung der S-Verfassung ist eine umfangreiche und verantwortungsvolle Aufgabe. Das nachstehende Konzept soll eine transparente, faire und zielgerichtete Organisation des S-Netzwerks garantieren. Wie Abbildung 14 zeigt, ist es unterteilt in vier reguläre zeitlich aufeinanderfolgende Phasen: die formlose Phase, die formgebende Phase, die aufbauende Phase und die fortlaufende Phase. Zusätzlich ist als fünfte Phase auch eine geordnete Auflösung des S-Netzwerks mit Migration auf eine andere Plattform vorgesehen.

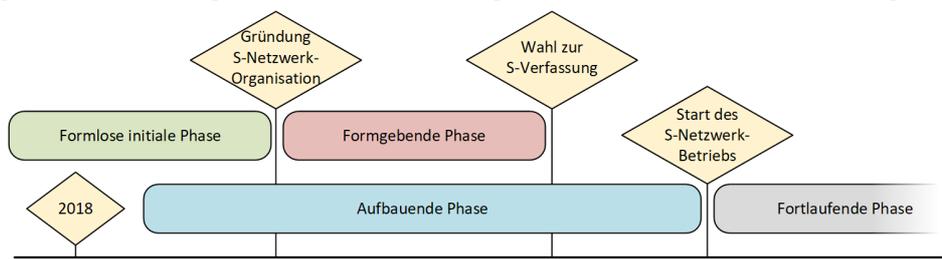


Abbildung 14: Phasen der Entwicklung des S-Netzwerks

1. FORMLOSE INITIALE PHASE: ENTWICKLUNG DER IDEEN

Die erste Phase dient zur Vorbereitung des Aufbaus des S-Netzwerkes und sie hat bereits begonnen: Beispielsweise wird in dieser Publikation die Grundidee zum S-Netzwerk vorgestellt und es werden mögliche Konzepte zur Verwirklichung sowie ein voll funktionsfähiger technischer Prototyp präsentiert. Es sind jedoch auch andere Ansätze denkbar, um

eine Plattform für reliable Publikationen und sichere Hinterlegungen zu erschaffen (etwa mit PKI oder *Blockchain*). Alle Möglichkeiten sollten durchdacht und unvoreingenommen als Alternativen mit ihren Stärken und Schwächen in Betracht gezogen werden.

Damit das S-Netzwerk sein volles Potenzial in positivem Sinne entfalten kann, sind alle Interessierten aufgerufen, sich an der Findung sowie Weiterentwicklung der Ideen für das S-Netzwerk bis zur fertigen Umsetzung und darüber hinaus zu beteiligen: Grundsätzlich soll jeder einen Beitrag leisten können, der dazu ernstlich gewillt ist. Auf wissenschaftlichen Konferenzen sollen die Möglichkeiten vorgetragen und diskutiert werden. Eventuell kann es auch schon in der ersten Phase spezielle Konferenzen für das S-Netzwerk geben.

In dieser initialen Phase soll in die Breite entwickelt werden: Die Ideen sollen auf den Tisch kommen. Verschiedene Konzepte und Prototypen können in Konkurrenz zueinander entwickelt werden. Es können schon mehrere alternative Entwürfe zum potenziellen Inhalt der S-Verfassung angefertigt und sogar bis zur Vollständigkeit ausgearbeitet werden.

In der ersten Phase werden noch keine Entscheidungen getroffen. Es kann auf feste Regeln, formale Anforderungen und auf koordinative organisatorische Maßnahmen weitgehend verzichtet werden. In der ersten Phase werden von Interessenten verschiedene Ideen und Ansätze frei entwickelt – in loser Kooperation oder in Konkurrenz zueinander.

2. FORMGEBENDE PHASE: DIREKTE BASISDEMOKRATIE UND S-NETZWERK-ORGANISATION

Erst mit der zweiten Phase beginnt der formal organisierte Aufbau des S-Netzwerks. Aus den verschiedenen Entwürfen, Möglichkeiten und Ideen muss eine S-Verfassung entwickelt werden, die möglichst vielen Interessenten auch akzeptabel und nützlich erscheint.

Dort, wo sich nicht objektiv eindeutig die besten Lösungen aus mehreren alternativen Möglichkeiten herauskristallisieren, wo keine Kompromisse gefunden werden können, müssen irgendwann Entscheidungen gefällt werden. Für das S-Netzwerk ist nicht zu erwarten, dass es immer einen eindeutig besten Weg, ein klares „nur so“ oder „so auf keinen Fall“ geben wird. Entsprechend streitbar können einzelne Punkte der S-Verfassung sein.

Um so wichtiger ist es, dass die Interessenten am S-Netzwerk in die Entscheidungsprozesse eingebunden werden. Also sollen alle Entscheidungen bezüglich des Inhalts der S-Verfassung direkt durch basisdemokratische Wahlen getroffen werden.

DIREKTE DEMOKRATIE

Das S-Netzwerk soll eine Plattform zum aktiven Mitmachen für seine Teilnehmer werden. Alle Interessenten am S-Netzwerk sind potenzielle künftige Teilnehmer desselben und sie sollen an der Gestaltung der S-Verfassung mitwirken können. Wo sich kein Konsens erzielen lässt, wo eine Entscheidung gefällt werden muss, verspricht eine direkt demokratische Abstimmung mit Mehrheitsprinzip als Verfahren zur Entscheidungsfindung den Vorteil der gleichberechtigten Partizipation.

In einer repräsentativen Demokratie hingegen werden nur Repräsentanten gleichberechtigt gewählt. Diese Repräsentanten sind dann in einem gewissen Rahmen dazu privilegiert, konkrete Entscheidungen alleine zu fällen, was Raum für Willkür, Wahlbetrug durch das Brechen von Wahlversprechen und Korruption öffnet. Gewählte Repräsentanten sind wie „Vertrauensparteien“ – ihr korrektes Verhalten lässt sich nicht sicherstellen. Beim S-Netzwerk sollen jegliche Abhängigkeiten von „Vertrauensparteien“ vermieden werden: Es wäre also inkonsequent, ausgerechnet bei der Gestaltung der S-Verfassung auf Repräsentanten zu vertrauen. Direkte Demokratie kommt bei wichtigen Entscheidungen ohne privilegierte Repräsentanten aus.

Vorbehalte gegen die direkte Demokratie gibt es neben dem Abstimmungsaufwand an sich eine ganze Reihe – und ebenso viele Gegenargumente ([Verhulst 2007], S. 75ff). Von Kritikern wird etwa das Engagement sowie die Kompetenz der potenziellen Wähler als zu niedrig eingeschätzt. Dagegen lässt sich einwenden, dass alleine schon die Möglichkeit zur direkten Abstimmung auch zu mehr Interesse führen und einen Lernprozess in Gang setzen kann:

“Political incompetence is not a cause, but an effect, of the fact that in purely representative democracies citizens are not allowed to participate directly in political decision-making on substantive issues.”, zitiert aus [Kaufmann 2010], S. 63.

Mit dieser Festlegung der zukünftigen Entscheidungsfindungsmethode ist bereits eine erste wichtige Entscheidung getroffen – bevor direkte basisdemokratische Wahlen überhaupt durchgeführt werden können. Darüber hinaus muss auch vorab bereits bestimmt werden, wer wählen darf, wie gewählt wird, und was zur Abstimmung kommt.

Schon die Frage, wer wahlberechtigt sein soll, hat es in sich. In vielen demokratischen Ländern wird auf die Staatsbürgerschaft und auf das Alter Wert gelegt. So gilt aktuell etwa in Deutschland bei der Bundestagswahl ein Mindestalter von 18 Jahren („*Wahlberechtigt ist, wer das achtzehnte Lebensjahr vollendet hat*“, Artikel 38 Absatz 2 [GG 1949/2010]). Bei Landtagswahlen in Deutschland gibt es unterschiedliche Altersregelungen. So liegt das Mindestalter in Brandenburg bei 16 Jahren ([BbgLWahlG 2004/2014] Abschnitt 2 § 5), unter anderem in Bayern hingegen bei 18 Jahren ([LWG 2002/2011] Artikel 1 (1) 1.).

Derartige aus der Luft gegriffene Altersregelungen verstoßen gegen das Grundgesetz („*Alle Menschen sind vor dem Gesetz gleich*“, Artikel 3 Absatz 1 [GG 1949/2010]) sowie gegen das explizite Diskriminierungsverbot der Charta der Grundrechte der Europäischen Union („*Diskriminierungen insbesondere wegen des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, der politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung sind verboten.*“, Artikel 21 (1) [EU 2012]). Eine Abhängigkeit des Wahlrechts vom Lebensalter ergibt auch einfach keinen Sinn – warum sollte eine einen Tag früher geborene Person weniger qualifiziert sein, abzustimmen?

Wenn es eine Beschränkung des Wahlrechts geben soll, so darf die Beschränkung nicht altersabhängig sein. Der Erwerb und Nachweis notwendiger Kompetenzen kann eine rechtlich zulässige Voraussetzung für die Wahlberechtigung sein, wenn diese Bedingung für alle gleichermaßen gilt. Für die Bundestagswahl könnte beispielsweise der erfolgreiche Abschluss der Pflichtschule als Voraussetzung bestimmt werden.

Für die Abstimmungen bezüglich des S-Netzwerks wäre es wünschenswert, das Wahlrecht an den Erwerb und Nachweis der Kompetenzen zu knüpfen, welche auch die Voraussetzung für die Teilnahme am S-Netzwerk sein sollen. Was genau diese Kompetenzen sind und wie sie nachzuweisen sind, wird jedoch erst in der S-Verfassung festgelegt werden. Solange es noch keine S-Verfassung gibt, steht dieses Kriterium nicht zur Verfügung. Die Anforderungen sind in der formgebenden Phase eventuell ohnehin anders: Um die politischen, rechtlichen, technischen und sozialen Fragen, die bei Abstimmungen über die initiale Gestaltung der S-Verfassung anstehen, erfassen zu können und um darüber im eigenen Interesse abstimmen zu können, wird ein hohes Maß an Bildung benötigt. Daher ist es vielleicht sinnvoll, die Hochschulreife als Voraussetzung zur Wahlberechtigung bei Abstimmungen über die S-Verfassung in der formgebenden Phase zu wählen.

Die Fragen, über die abgestimmt werden soll, müssen ebenso wie die Antwortmöglichkeiten ausformuliert werden. Schließlich müssen auch die Abstimmungen selbst durchgeführt und ausgewertet werden. Es soll dazu eine offene Organisation geschaffen werden: die **S-Netzwerk-Organisation**. Gedacht ist die S-Netzwerk-Organisation als ein Arbeitsbündnis, welches zunächst zur Bewältigung der formgebenden Phase auf einer offenen Konferenz definiert und gegründet werden soll. In der S-Verfassung soll die S-Netzwerk-Organisation zur Unterstützung der fortlaufenden Phase offiziell verankert werden.

Alles, was die S-Netzwerk-Organisation tut, muss öffentlich gemacht werden. Die S-Netzwerk-Organisation dient in erster Linie der Koordination und Verwaltung. Sie soll alle eingehenden Vorschläge, Ideen und Entwürfe zur Spezifikation der Standards und Regeln des S-Netzwerks sammeln und dazu beitragen, sie zusammen mit Externen in eine geeignete Form zu bringen. Die S-Netzwerk-Organisation soll dazu alle an sie herangetragenen Vorschläge publizieren. In einem offenen Prozess sollen die Ideen und Konzepte zusammengeführt, weiterentwickelt und ausgefeilt werden. Die S-Netzwerk-Organisation soll dabei für Transparenz sorgen, beraten und vermitteln. Sie soll Qualitätsanforderungen formulieren und sicherstellen, dass alle Interessenten ihre Kommentare abgeben können.

Freie und unabhängige Entwickler, Wissenschaftler, Juristen sowie Interessenten auf der ganzen Welt sollen sich mithilfe der S-Netzwerk-Organisation an der Ausformulierung des Entwurfs der S-Verfassung beteiligen können. Gemeinsam gilt es, den Entwurf bis zur Abstimmungsreife zu bringen. Wo es keinen Konsens gibt, müssen sämtliche den Qualitätsanforderungen genügende alternative Vorschläge als Antwortmöglichkeiten auf eine Abstimmungsfrage ausformuliert werden. Dem dabei vorhandenen gestalterischen Freiraum muss bei der basisdemokratischen Abstimmung darüber, welche Alternativen des Entwurfs letztlich in die S-Verfassung einfließen sollen, durch einen geeigneten Abstimmungsmodus Rechnung getragen werden, um Manipulationen der Wahl möglichst zu vermeiden.

DER ABSTIMMUNGSMODUS UND SEIN EINFLUSS AUF DAS ERGEBNIS

Ziel der demokratischen Abstimmungen zum S-Netzwerk ist es, eine für möglichst viele tragbare S-Verfassung zu generieren. Zur Wahl gestellt werden sollen in der formgebenden Phase konkret jeweils mehrere verschiedene alternative Versionen für jeden Punkt der S-Verfassung, für den es mehrere Gestaltungsoptionen gibt. Die wesentlichen Unterschiede zwischen den verschiedenen Versionen sollen unmittelbar neben den Wahlmöglichkeiten erklärt werden, um die Wahl zu erleichtern. Die Aufbereitung für jede einzelne alternative Möglichkeit muss so gut sein, dass die potenziellen Wähler die entscheidenden Unterschiede verstehen können. Doch wie soll der Wahlberechtigte seine Präferenzen kenntlich machen können?

Ein naiver Ansatz wäre, dass der Wahlberechtigte jeweils nur genau die eine Version kennzeichnet (etwa mit einem Kreuz), welche er favorisiert. Gewählt wäre dann jeweils die Version, welche relativ zu den Alternativen am häufigsten gekennzeichnet wurde. Dieser Modus ist jedoch für Wahlen zur S-Verfassung untauglich, da die Abstimmung manipuliert werden könnte: Es seien *A* und *B* zwei mögliche Versionen für einen Artikel in der S-Verfassung. Die Befürworter von *A* könnten die Wahrscheinlichkeit, dass Version *A* die Wahl gewinnt, selbst wenn die Mehrheit gegen *A* ist, einfach erhöhen, indem sie die Aufnahme mehrerer zu Version *B* ähnlicher alternativer Versionen B_1 bis B_N als Wahlmöglichkeiten anstelle von nur einer Version *B* beantragen. Personen, die nicht für *A* stimmen wollen, müssten sich dann entscheiden, welcher Version von B_1 bis B_N sie ihre einzige Stimme geben wollen. Version *A* könnte die meisten Stimmen bekommen, obwohl deutlich mehr Wähler *A* auf keinen Fall wollen und für eine der Versionen von B_1 bis B_N stimmen.

Für die Wahlen zur S-Verfassung soll stattdessen bei der Abstimmung jede alternative Version für sich bewertet werden. Es bietet sich an, zur Bewertung auf eine fünfstufige ganzzahlige Skala mit Werten zwischen minus zwei für völlig unakzeptabel und plus zwei für perfekt zu setzen. Es gewinnt dann unter den Alternativen die Version, für welche die Summe über alle gültigen Bewertungen maximal ist. In dem Beispiel würden Sympathisanten von den Versionen B_1 bis B_N die Version *A* mit minus zwei bewerten, während sie alle Versionen von B_1 bis B_N je nach Gefallen mit plus eins oder mit plus zwei positiv bewerten könnten. Selbst wenn keine einzelne Version von B_1 bis B_N für sich mehr Höchstwertungen erhalte wie Version *A*, würde in dem Beispiel doch der Wille der Mehrheit gewahrt bleiben, dass sich auf keinen Fall Version *A* durchsetzen darf.

Eine Hauptaufgabe der S-Netzwerk-Organisation liegt darin, die notwendigen direkten demokratischen Abstimmungen anzukündigen und zu unterstützen. Derzeit gibt es keine Infrastruktur, die eine weltweite elektronische Abstimmung über Computernetzwerke erlauben würde. Für eine streng geheime Wahl kann auf spezielle Wahlkabinen ohnehin nicht verzichtet werden. Ob für die Abstimmungen zur Schaffung der S-Verfassung der erhöhte Aufwand einer streng geheimen Wahl gerechtfertigt ist, sei dahin gestellt.

In jedem Fall bringen demokratische Abstimmungen Aufwand mit sich. Die S-Netzwerk-Organisation muss entsprechende Mittel etwa durch Spenden sammeln. Sie muss Helfer sowie möglichst unabhängige Beobachter zur Durchführung und zur Auswertung gewinnen. Die zweite formgebende Phase endet mit der Fertigstellung der S-Verfassung.

ANERKENNUNG DER S-VERFASSUNG DURCH INDIVIDUELLEN VERTRAGSABSCHLUSS

Für das S-Netzwerk müssen Regeln geschaffen und zur Anwendung gebracht werden, es benötigt ein solides rechtliches Fundament. Regeln durchsetzen, besonders, wenn andere Personen davon betroffen sind, ist schwierig. Strafandrohungen und weitere Zwangsmaßnahmen können Regeln gewaltsam zur Geltung verhelfen. Zielführender wäre es jedoch, wenn die Regeln akzeptiert oder besser gewollt würden – wenn sie als hilfreich oder als notwendig anerkannt würden.

Akzeptanz für eine Verfassung zu schaffen – egal ob es sich um eine Konstitution für einen Staat oder für eine Informationsplattform handelt – ist eine ähnliche Herausforderung wie die Schaffung von Vertrauen, dass die in der Verfassung festgeschriebenen Regeln auch angewendet werden. Demokratie, der Wille einer Mehrheit, wird vielfach als Rechtfertigung für das Fundament genutzt:

„Im 20. Jahrhundert wurde die Demokratie – zum ersten Mal in der Menschheitsgeschichte – als weltweite Norm anerkannt. Dieser Standard wird zwar fast nirgendwo erreicht und die Demokratie wird in vielen Teilen der Welt beständig mit Füßen getreten. Aber bis auf einige Ausnahmen (zum Beispiel Saudi-Arabien, Bhutan) berufen sich alle nur erdenklichen Regime auf demokratische Legitimation.“, zitiert aus [Verhulst 2007], S. 7.

Damit eine Mehrheit ein Fundament wie eine Verfassung erschaffen kann, bedarf es bereits umfangreicher Regeln und Strukturen. Es muss in einer Demokratie festgelegt werden, wer denn zum „herrschenden Volk“ gehören soll und wie dieses Volk Macht ausüben soll. Für eben diese Voraussetzungen besteht wiederum das Akzeptanzproblem. Eine befriedigende Selbstrechtfertigung kann so nie gelingen. Demokratische Legitimation von Grund auf ist unmöglich.

Die S-Verfassung wird nicht anerkennungswürdig, wenn sie von einer Mehrheit beschlossen wurde. Anerkennung ist eine individuelle Entscheidung, jeder kann sie nur für sich treffen. Die Bestimmungen der S-Verfassung beziehen sich nur auf das S-Netzwerk. Es genügt, wenn sie von den betroffenen freiwilligen Teilnehmern selbst akzeptiert werden.

Für aktive Teilnehmer am S-Netzwerk lässt sich die persönliche Anerkennung der S-Verfassung sicherstellen: Die Kenntnisnahme und das Verstehen der S-Verfassung sind Voraussetzungen für die Teilnahme am S-Netzwerk. Die Akzeptanz der S-Verfassung wird durch den individuellen Abschluss eines S-Vertrags von jedem angehenden Teilnehmer besiegelt. Mit dem persönlichen S-Vertrag verkündet ein Teilnehmer die S-Verfassung als Ausdruck seines freien Willens und er verpflichtet sich selbst, die darin enthaltenen Regeln zu achten. Es besteht kein Zwang, keine unbedingte Notwendigkeit zum Abschluss eines S-Vertrags und zur Teilnahme am S-Netzwerk.

Die S-Verfassung kann im Laufe der Zeit geändert werden – und zwar nur nach den Vorgaben der S-Verfassung durch direkte Abstimmungen mit einer qualifizierten Mehrheit der Teilnehmer am S-Netzwerk. Sind derart basisdemokratisch beschlossene Änderungen der S-Verfassung für einen Teilnehmer inakzeptabel, hat er jederzeit die Option, den S-Vertrag zu kündigen.

Neben Bestimmungen für die Teilnehmer am S-Netzwerk wird die S-Verfassung auch Regeln für das Außenverhältnis zu Externen enthalten müssen. Dazu gehören Festlegungen, wie externe Personen Rechtsmittel als Reaktion auf Publikationen oder Hinterlegungen im S-Netzwerk geltend machen können, etwa um sich selbst zu schützen. Diese Regeln können auch unmittelbar Personen betreffen, welche die S-Verfassung nicht kennen oder welche sie bewusst ablehnen. Um Anfeindungen zu vermeiden, sollte die S-Verfassung Externen einfache Wege bieten, sie betreffende Fälle klären zu lassen – möglichst ohne Nachteile gegenüber aktiven Teilnehmern am S-Netzwerk.

Schließlich muss die S-Verfassung auch Regeln dafür enthalten, was genau geschehen soll, wenn das S-Netzwerk von außen angegriffen wird. Wiederum sind möglicherweise externe Personen betroffen, welche die S-Verfassung in keiner Weise anerkennen – allerdings nur, wenn sie aktiv gegen das S-Netzwerk vorgehen. Diese Regeln dienen der Selbstverteidigung.

Damit die abstrakten rechtlichen Regeln der S-Verfassung überhaupt anwendbar sind, benötigt das S-Netzwerk konkrete Implementierungen der S-Verfassung in gültige Rechtsrahmen. Und diese Rechtsrahmen beinhalten bestehende Gesetze, Staaten und Institutionen zur Durchsetzung der Regeln der S-Verfassung. Die Anerkennung des S-Netzwerks hängt letztlich auch davon ab, wie fundiert, wie akzeptiert die einzelnen Bestandteile der Rechtsrahmen sind.

RECHT, DAS NICHT VOM HIMMEL FÄLLT

Moderne Rechtsstaaten beanspruchen die Rechtshoheit und ein umfassendes Gewaltmonopol auf jenem Territorium, welches sie mit all seinen Ressourcen als ihr souveränes Gebiet betrachten.

Um Staaten zu legitimieren und um ihre Ansprüche zu begründen sowie zu rechtfertigen gibt es neben den erwähnten demokratischen Legitimationsversuchen verschiedene weitere Ansätze, beispielsweise Völkische (z. B. sich auf eine gemeinsame Kultur berufende), Historische (durch besondere Ereignisse wie eine Revolution), Religiöse (etwa das Gottesgnadentum) oder Philosophische (etwa das Recht des Stärkeren). Jeder dieser Ansätze ist problematisch. De facto werden Staaten und ihre Grenzen vielfach nicht anerkannt, woraus Konflikte sowie Kriege entstehen. Auch in Deutschland treten Akzeptanzprobleme auf. Gegenwärtig etwa mit den sogenannten *Reichsbürgern*, welche sich weigern, die Bundesrepublik Deutschland anzuerkennen [Schumacher 2016].

Ausgehend von den Überlegungen zur S-Verfassung lässt sich auch ein ganz anderer Ansatz denken, um eine Staatsverfassung zu fundieren und dabei eine neue Art von Staat zu erschaffen: Nämlich den freien individuellen Vertragsabschluss zur Anerkennung der Verfassung als Voraussetzung für die Staatsbürgerschaft. Dieser Ansatz soll hier zumindest grob skizziert werden. Die Staatsbürgerschaft würde nicht als ein Geburtsrecht verschenkt und die Mündigkeit müsste nicht in unhaltbar diskriminierender, grotesker Weise an das Lebensalter geknüpft werden. Voraussetzung für die Staatsbürgerschaft wäre, sich zuerst mit der Verfassung vertraut zu machen. Es müsste ein Nachweis geliefert werden, dass die Verfassung verstanden wird und dass die notwendigen Fähigkeiten zur Ausübung der Bürgerrechte sowie Bürgerpflichten vorhanden sind. Außerdem müsste die Verfassung als Ausdruck des eigenen freien Willens durch den Abschluss eines Vertrags anerkannt werden, in dem sich der Bürger verpflichtet, die Regeln der Verfassung zu achten. Eine freie Entscheidung zum Vertragsabschluss ist nur dann gewährleistet, wenn es realistische Alternativen gibt. Es müsste also möglich sein, einen anderen Staat mit einer anderen Verfassung zu wählen.

Dieser Ansatz könnte zu einer besseren Identifikation mit der Verfassung und dem Staat führen. Er bietet einen starken Anreiz zum Erwerben von politischen sowie rechtlichen Kompetenzen und er kommt ohne jeden moralischen philosophischen, religiösen oder ideologischen Überbau aus: Die Verfassung ist nichts als eine vertragliche Übereinkunft der Staatsbürger über gemeinsame Regeln.

3. AUFBAUENDE PHASE: ERSTE IMPLEMENTIERUNG DER S-VERFASSUNG

Sobald die S-Verfassung steht, können in den einzelnen lokalen Rechtsräumen S-Rechtsrahmen erschaffen werden. Erst an dieser Stelle kommt bestehenden Staaten oder Staatenbunden eine Rolle in der Erschaffung des S-Netzwerkes zu. Zugleich können fortan auf privatwirtschaftlicher Seite gezielt den Anforderungen der S-Verfassung genügende *sichere Zugangssysteme* sowie S-Knoten entwickelt und gefertigt werden. Unternehmen können sich für die Tätigkeit als S-Betreiber aufstellen und entsprechende Leistungen anbieten.

Bevor die S-Rechtsrahmen und die anderen notwendigen Entwicklungen im S-Netzwerk genutzt werden können, muss sichergestellt werden, dass diese Implementierungen den Maßgaben der S-Verfassung auch genügen. Wer dies wie kontrolliert, wird in der S-Verfassung selbst genau festgelegt. Es ist naheliegend, für die Kontrollen und Prüfungen auf das gleiche Konzept zu setzen, welches das S-Netzwerk auch sonst vertrauenswürdig und manipulationssicher machen soll: Auf die Aufteilung der Verantwortlichkeiten über verschiedene Misstrauensparteien.

Voraussetzung für den Betrieb des S-Netzwerkes ist, dass es in jeder Misstrauenspartei mindestens einen S-Rechtsrahmen gibt und dass jeweils mindestens ein S-Knoten in Betrieb gehen kann. Mit der Eröffnung des S-Netzwerkes endet die dritte aufbauende Phase.

4. FORTLAUFENDE PHASE: KONTROLLE, KOORDINATION UND WEITERENTWICKLUNG

Das S-Netzwerk und insbesondere die S-Verfassung sollen langfristig ausgerichtet sein. Dennoch kann es wünschenswert oder notwendig werden, Optimierungen und ggf. auch grundlegende Änderungen durchzuführen, schließlich steht die Welt nicht still.

Das Sammeln von Ideen, Vorschlägen und Entwürfen zur Anpassung und Verbesserung der S-Verfassung und des S-Netzwerkes kann über das S-Web vorgenommen werden. Die S-Netzwerk-Organisation soll weiter ihre unterstützende Rolle bei der Ausarbeitung behalten, wie schon bei der Erschaffung der S-Verfassung in der formgebenden Phase.

Ob Änderungen an der S-Verfassung durchgeführt werden, soll direkt basisdemokratisch entschieden werden, wobei die S-Netzwerk-Organisation wiederum für die Betreuung der Abstimmungen zuständig sein soll. Wahlberechtigt sollen ab Beginn der fortlaufenden Phase in der Regel nur die aktiven Teilnehmer des S-Netzwerkes als direkt Betroffene sein. Folglich kann und soll das S-Netzwerk selbst bei der Durchführung der Abstimmungen genutzt werden, was die Arbeit der S-Netzwerk-Organisation erleichtern kann.

Wichtig ist im laufenden Betrieb neben der Möglichkeit zur Anpassung der S-Verfassung auch die Sicherstellung der Einhaltung der Maßgaben der S-Verfassung. Beim Prüfen und Kontrollieren auf Konformität zur S-Verfassung handelt es sich um Tätigkeiten,

die immer wieder anfallen, auch wenn das S-Netzwerk schon läuft. Die Umsetzung etwaiger Änderungen der S-Verfassung muss auch in den konkreten Implementierungen erfolgen, damit sie Wirkung entfalten können. Denn egal wie ausgefeilt und aktuell die Normen, Spezifikationen und Standards in der S-Verfassung auch gelingen mögen, entscheidend ist letztlich, was davon in der Realität auch Wirkung zeigt.

5. AUFLÖSUNGSPHASE: MIGRATION AUF EINE NACHFOLGEPLATTFORM

Das S-Netzwerk als technisches System kann im Laufe der Zeit veralten. Eventuell wird es irgendwann eine Plattform geben, die all das kann, was das S-Netzwerk bietet und noch mehr. Oder es entsteht eine Plattform, die vertrauenswürdiger, sicherer, effizienter ist, als das S-Netzwerk. Eine Plattform, die wirtschaftlich attraktiver ist und die mehr Nutzer anzuziehen vermag.

Wenn das S-Netzwerk durch den Fortschritt überwunden wird, so ist dies eine erfreuliche Entwicklung. Es wäre absurd, das S-Netzwerk trotz überlegener Alternativen weiterhin als eigenständige Plattform unverändert erhalten zu wollen. Mit Weiterentwicklungen zu reagieren, welche nur darauf abzielen, ein anderswo bereits realisiertes Level zu erreichen, ist unter Umständen auch keine gute Idee. Dann ist es vielleicht besser, die Inhalte, welche gemäß der Regeln der S-Verfassung verfügbar bleiben müssen, auf die neue Plattform zu migrieren und den bisherigen Teilnehmern am S-Netzwerk zukünftig den Zugriff über die neue Plattform zu ermöglichen.

Für eine mögliche Auflösung müssen in der S-Verfassung Regeln festgelegt werden – und zwar erstens, unter welchen Umständen und wie genau eine Auflösung zugunsten einer alternativen Plattform eingeleitet werden kann sowie zweitens, wie die Migration auf die neue Plattform organisiert und durchgeführt werden soll. Das könnte sinngemäß etwa so gestaltet werden:

§X – Auflösung und Übersiedlung

§X.1 – Das S-Netzwerk kann nur aufgelöst werden, wenn die verfügbar zu haltenden Inhalte auf eine neue Plattform migriert werden, welche die Eigenschaften von den reliablen Publikationen und sicheren Hinterlegungen wahrt und welche überall dort nutzbar ist, wo das S-Netzwerk nutzbar ist. Die neue Plattform muss außerdem Abfragen über S-Links so unterstützen, wie es auf den S-Knoten gemäß der S-Verfassung möglich ist.

§X.2 – Eine Abstimmung über die Auflösung des S-Netzwerks zugunsten einer neuen Plattform, auf die gültige Inhalte zu übersiedeln sind, kann jeder Teilnehmer am S-Netzwerk verlangen, wenn die neue Plattform mehr aktive Nutzer aufweist als das S-Netzwerk oder wenn mindestens 10% der aktiven Teilnehmer am S-Netzwerk diesen Antrag unterstützen. Ist für eine potenzielle neue Plattform die Abstimmung verlangt, kann für diese Plattform zwei Jahre lang keine neue Abstimmung eingefordert werden.

§X.3 – Wird eine Abstimmung nach §X.2 verlangt, lässt die S-Netzwerk-Organisation in allen Misstrauensparteien gerichtlich prüfen, ob die neue Plattform §X.1 erfüllt.

§X.4 – Ist die neue Plattform gemäß §X.3 zulässig, muss die Abstimmung im S-Netzwerk durchgeführt werden. Die Wahl muss mindestens zwei Monate vor Ende des Abstimmungszeitraums von der S-Netzwerk-Organisation ausgeschrieben werden, wobei alle aktiven Teilnehmer am S-Netzwerk direkt per S-Mail einzuladen sind. Für die Auflösung ist eine Zustimmung der absoluten Mehrheit der aktiven Teilnehmer am S-Netzwerk erforderlich. Schrumpft die Anzahl der aktiven Teilnehmer am S-Netzwerk während der letzten zwei Monate vor Ende des Abstimmungszeitraums um mehr als 10 % oder um mehr als 30 % im letzten Jahr vor dem Ende des Abstimmungszeitraums, genügt eine einfache Mehrheit.

§X.5 – Ist die Auflösung zugunsten einer anderen Plattform wie in §X.4 reglementiert beschlossen, führt die S-Netzwerk-Organisation zusammen mit den S-Betreibern die Migration auf die neue Plattform durch. Das S-Netzwerk ist dazu noch mindestens ein Jahr weiter zu betreiben, um einen nahtlosen Übergang für alle zu ermöglichen. Die letzten zwei Monate sind nur noch lesende Zugriffe zu gestatten. Bestehende Teilnahmen am S-Netzwerk enden automatisch nach einem Jahr, ohne dass es einer Kündigung bedarf.

§X.6 – Nach der Abschaltung des S-Netzwerks dokumentiert die S-Netzwerk-Organisation auf der neuen Plattform den vollständigen Migrationsprozess, bevor sie sich selbst auflöst.

§X.7 – Die Kosten für die Maßnahmen in §X.3 bis §X.6 sind aus den Rücklagen für den Umgang mit kritischen Ereignissen sowie aus den regulären Beiträgen der noch aktiven Teilnehmer zu begleichen. Nicht benötigte Rücklagen für den Umgang mit kritischen Ereignissen sind nach erfolgreicher Migration durch die S-Netzwerk-Organisation zugunsten der neuen Plattform zu reinvestieren, bevor sich die S-Netzwerk-Organisation selbst auflöst.

2.6.2 STANDARDKONFORMITÄT VON IMPLEMENTIERUNGEN

Die Implementierungen von abstrakten technischen Standards können objektiv überprüft werden, sodass ein einheitliches Qualitätsniveau garantiert werden kann. Bei den lokalen Implementierungen abstrakter rechtlicher Standards können konkret anwendbare Gesetze sowie Verträge zumindest ihrem Wortlaut nach ebenfalls objektiv auf Konformität untersucht werden. Zu prüfen, ob in der Praxis der Rechtsprechung und in den Rechtsfolgen die angestrebte Äquivalenz auch erreicht wird, ist hingegen schwierig. Außerdem können sich rechtliche Rahmen, die praktische Rechtsprechung und deren reale Auswirkungen immer wieder ändern. Mit Abweichungen in einzelnen souveränen Rechtsräumen muss jederzeit gerechnet werden und es müssen angemessene Reaktionen darauf festgeschrieben werden.

Die in der S-Verfassung verankerten technischen Standards sollen dazu beitragen, ein einheitliches Qualitätsniveau für alle Beteiligten im ganzen S-Netzwerk zu garantieren. Diese abstrakten Standards enthalten sowohl funktionale als auch sicherheitstechnische Anforderungen an die Implementierungen der S-Knoten sowie der *sicheren Zugangssysteme*. Die Erfüllung der Anforderungen und das Bestehen von in der S-Verfassung vorgeschriebenen Prüfungen ist Zulassungsvoraussetzung für den Einsatz im S-Netzwerk.

Die technischen Standards beschreiben dazu nicht nur genau, was ein System zu leisten hat, sondern sie sollen auch Kriterien und Prüfungsvorlagen enthalten, anhand derer idealerweise objektiv eindeutig festgestellt werden kann, ob eine potenzielle Implementierung tatsächlich eine korrekte Umsetzung der Spezifikation ist oder nicht. Für die Durchführung der Qualitätsprüfungen können etablierte Techniken wie formale Methoden mit theoretischen Korrektheitsbeweisen, Codeanalysen, Messungen, Tests sowie Simulationen und Experimente genutzt werden.

Im besten Fall führt der Einsatz dieser Techniken zu unbestreitbaren, scharfen Ergebnissen: Eine Maschine funktioniert entweder genau so, wie sie soll, oder eben nicht. Bei komplexen Systemen wie den S-Knoten oder den sicheren Zugangssystemen und erst recht, wenn der komplette informationstechnische Teil des S-Netzwerks als Gesamtsystem betrachtet werden soll, wird nach derzeitigem Stand keine perfekte Qualitätsprüfung durchführbar sein. Beispielsweise wäre ein vollständiges Testen aller möglichen Eingaben viel zu aufwendig. Um dennoch ein gutes technisches Qualitätsniveau sicherstellen zu können, ist es wichtig, die verschiedenen analytischen Methoden in Kombination so einzusetzen, dass erstens die jeweiligen Stärken der einzelnen analytischen Methoden ausgenutzt werden und dass zweitens gerade die kritischen Aspekte besonders genau analysiert werden. Dazu ist ein gezieltes risikobasiertes Management der analytischen Techniken erforderlich.

An der Entwicklung von Werkzeugen und Prüfungsvorlagen zur Qualitätssicherung bei den Implementierungen der in der S-Verfassung verankerten technischen Standards sollen sich alle Interessenten beteiligen können. Diese Entwicklungen dürfen über die Grenzen von Misstrauensparteien hinaus kooperativ vorangetrieben werden und die fertigen Hilfsmittel dürfen in allen Misstrauensparteien eingesetzt werden. Im Gegensatz zu den Implementierungen von S-Knoten und von *sicheren Zugangssystemen* wird bei den Werkzeugen und Prüfungsvorlagen zur Qualitätssicherung also keine streng getrennte Heterogenität zwischen den Misstrauensparteien gefordert. Dies hilft den Aufwand gering zu halten und es ist sinnvoll, denn es soll jede einzelne misstrauensparteispezifische Implementierung eines S-Knotens oder eines *sicheren Zugangssystems* alle anwendbaren Prüfungen auf die Konformität zu den Standards der S-Verfassung bestehen, egal woher die bei der Prüfung benötigten Werkzeuge und Prüfungsvorlagen stammen.

Um zur offiziellen Zulassungsvoraussetzung werden zu können, müssen Entwicklungen von Werkzeugen und Prüfungsvorlagen zur Qualitätssicherung bei der S-Netzwerk-Organisation eingereicht und vollständig offengelegt werden. Anschließend wird für

eine gewisse Zeit auf Feedback zu den Entwicklungen gewartet. Wenn es keinen begründeten Widerspruch gibt, erfolgt schließlich die Aufnahme in die Liste der Zulassungsvoraussetzungen. Auch gegen bereits zulassungsrelevante Werkzeuge und Prüfungsvorlagen zur Qualitätssicherung kann jederzeit Widerspruch erhoben werden. Ist der Widerspruch objektiv verifizierbar, kann eine Streichung aus der Liste der Zulassungsvoraussetzungen erfolgen. Sollte sich ein Widerspruch nicht objektiv eindeutig verifizieren oder falsifizieren lässt, kann die S-Netzwerk-Organisation eine Abstimmung durchführen.

Zulassungsprüfungen etwa für Implementierungen von S-Knoten oder von *sicheren Zugangssystemen* müssen stets von einem Quorum von Experten (etwa S-Betreibern) aus mindestens Ψ verschiedenen Misstrauensparteien durchgeführt und bestätigt werden. Prüfungsergebnisse von Zulassungsprüfungen müssen im S-Netzwerk publiziert werden.

Zusätzlich zu den obligatorischen Zulassungsprüfungen sollen alle Teilnehmer am S-Netzwerk die Möglichkeiten haben, Prüfungen der technischen Korrektheit ihrer eigenen Systeme im laufenden Betrieb des S-Netzwerks durchzuführen. Auffällige Ergebnisse können im S-Netzwerk publiziert und der S-Netzwerk-Organisation gemeldet werden.

GLEICHES RECHT?

In jedem lokalen Rechtsraum, in dem das S-Netzwerk verfügbar sein soll, müssen die rechtlichen Voraussetzungen dafür geschaffen werden. Die rechtlichen Anforderungen der S-Verfassung müssen in S-Rechtsrahmen mit Gesetzen, Institutionen und S-Verträgen implementiert werden. Auch hierfür ist eine Qualitätssicherung erforderlich.

Es ist eine große Herausforderung, die rechtlichen Standards möglichst minimal zu halten, aber dennoch so flexibel, dass ihre Umsetzung für souveräne Rechtsstaaten zumutbar ist. Bei dieser Implementierung sollen die Souveränen eines jeden bestehenden Rechtsraums jeweils die Möglichkeit haben, eigene Lösungen zu finden, die den lokalen Besonderheiten des Rechtsraums gerecht werden können.

Da dennoch eine rechtliche Äquivalenz für alle Teilnehmer garantiert werden soll, muss die Freiheit der Gestaltung von S-Rechtsrahmen und S-Verträgen begrenzt sein. Dazu müssen die Standards der S-Verfassung so umfangreich und genau gestaltet werden, dass ihre Implementierungen auch wirklich näherungsweise gleichwertige Bestimmungen in den unterschiedlichen Rechtsräumen erschaffen. Um entscheiden zu können, ob in einem Rechtsraum eine zulässige Implementierung der rechtlichen Verankerung des S-Netzwerks vorliegt oder nicht, müssen klare Kriterien festgelegt werden.

Die rechtlichen Vorgaben in der S-Verfassung beinhalten Forderungen, welche rechtlichen Voraussetzungen etwa in Form von Gesetzen für die S-Rechtsrahmen des S-Netzwerks geschaffen werden müssen und was in den S-Verträgen zu stehen hat. Die Standardkonformität der Gesetzestexte und der Vertragstexte kann objektiv überprüft werden.

Dem Wortlaut nach äquivalente Bestimmungen sind jedoch nicht hinreichend, um rechtliche Gleichheit sicherzustellen – sie müssen in der Praxis auch überall gleichermaßen angewandt und durchgesetzt werden. Ermessensspielräume für die Rechtsprechung, die sich aus der Notwendigkeit zur Abwägung zwischen verschiedenen kollidierenden Rechten ergeben, lassen sich bestenfalls minimieren, nicht aber komplett vermeiden.

Die Implementierung von rechtlichen Standards führt nicht zu einer deterministischen Maschine, die entweder standardkonform funktioniert oder eben nicht. Es genügt nicht, ein Zulassungsverfahren zu entwickeln und einmalig anzuwenden. Es muss vielmehr im laufenden Betrieb fortwährend sichergestellt werden, dass in der Realität eine rechtliche Gleichheit im Sinne der Standards der S-Verfassung gewährleistet wird. Dazu müssen Rechtssprechung und Rechtsfolgen in der Praxis observiert werden. Die das S-Netzwerk betreffende lokale Rechtssprechung soll im S-Netzwerk einheitlich dokumentiert werden und im S-Web mit den betroffenen abstrakten Vorgaben der S-Verfassung verlässlich verknüpft werden, sodass die Entscheidungen und ihre Grundlagen in verschiedenen Rechtsräumen zu einer bestimmten Angelegenheit leicht zu finden und zu vergleichen sind.

UNTERSCHIEDE BEI GLEICHLAUTENDEN RECHTSFOLGEN

Sogar dann, wenn in verschiedenen Rechtsräumen für gleichrangige Fälle tatsächlich äquivalent lautende Urteile gefällt werden und selbst wenn die Urteile gesetzeskonform vollstreckt werden, kann die Vollstreckung noch hochgradig unterschiedlich ausfallen.

So kann eine Verurteilung zu Freiheitsentzug vieles bedeuten, je nachdem wo und wie diese Strafe vollzogen wird. Es gibt eine Reihe von internationalen Abkommen, welche dazu dienen, rechtliche Mindeststandards für den Freiheitsentzug und andere Zwangs- sowie Strafmaßnahmen zu etablieren ([UN 1984]). Auch die Überwachung der Einhaltung von rechtlichen Mindeststandards – etwa durch regelmäßige internationale Kontrollen – lässt sich in Abkommen festschreiben ([Europarat 1987], [UN 2002]) und mithin fördern. Solche Mindeststandards sollen auch in die S-Verfassung aufgenommen werden.

Auch wenn die rechtlichen Rahmenbedingungen beispielsweise für den Freiheitsentzug so auf gemeinsame Standards gesetzt werden, kann es in der Praxis bei der Umsetzung doch zu deutlichen Abweichungen kommen. So zeigt etwa die Studie [Coyle 2004], dass es auch innerhalb der Europäischen Union große Abweichungen zwischen den offiziellen Bestimmungen für die Haft und den realen Haftbedingungen gibt.

“the major areas of concern about prison conditions in the countries reviewed relate not to the law but to basic defects in prison conditions and treatment. These sometimes amount to inhuman and degrading treatment, largely due to overcrowding, health problems and a failure in some countries to acknowledge the basic humanity of those deprived of their liberty, often expressed in institutional racism and xenophobia.”, zitiert aus [Coyle 2004], S. 20.

Für die Unterschiede sind nicht immer nur unterschiedliche gesetzliche Regelungen und die Gefängniswärter verantwortlich. Differenzen zeigen sich etwa auch im Bereich der persönlichen Sicherheit der Gefangenen, wobei Gewalt von Mitgefangenen eine erhebliche Rolle spielen kann. Aus ([Dünkel 2009], Abbildung 8) lässt sich bezüglich der Viktimisierungserfahrungen entnehmen, dass etwa in Finnland nur 3,9 % der befragten Gefangenen angegeben haben, in der Haft von Mitgefangenen erpresst oder körperlich verletzt worden zu sein, während sich im deutschen Bundesland Schleswig-Holstein bis zu 11,3% der Befragten als Opfer von Körperverletzung sahen und 9,3 % als Opfer von Erpressungen). In Lettland gaben sogar 28,1 % an, in der Haft Opfer von Körperverletzungen geworden zu sein. Entsprechend fühlen sich in lettischen Gefängnissen 47,4 % der Befragten bedroht, während es in Finnland mit 15,6 % erheblich weniger sind.

Vielleicht ist es unrealistisch, zu hoffen, dass in allen Staaten vergleichbare Rechtsfolgen geschaffen werden können. Was hingegen sicher möglich wäre, ist die Abbildung und Berücksichtigung der bestehenden Unterschiede etwa in den Haftbedingungen in der Schnittstelle der S-Verfassung. Je nachdem, wie hart die Haftbedingungen sind, könnte dann zum Ausgleich etwa die in der S-Verfassung für ein Vergehen vorgesehene Dauer der Freiheitsstrafe angepasst werden. Wie diese Aufrechnung zu geschehen hat, und wie die lokalen Bedingungen zu bemessen sind, müsste in der S-Verfassung festgelegt werden.

SCHWIERIGKEITEN BEI DER PRÜFUNG DER EINHALTUNG RECHTLICHER STANDARDS

In Europa sorgt gemäß [Europarat 1987] Artikel 1 das European Committee for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment (CPT) für internationale Inspektionen aller Haftorte. Für Personen, die aufgrund von Bestimmungen in der S-Verfassung verurteilt werden, könnten vergleichbare Inspektionsteams mit Vertretern aus verschiedenen Misstrauensparteien vorgeschrieben werden. Inspektionen können neben der Überwachung von Haftorten und anderen Einrichtungen bzw. Verfahren zur Vollstreckung von Urteilen auch dazu eingesetzt werden, um bereits die mit dem S-Netzwerk in Zusammenhang stehenden rechtlichen Prozesse zu überwachen.

Eine dauerhafte und lückenlos flächendeckende Kontrolle wird jedoch aufgrund des zu erwartenden Aufwands nicht praktikabel sein. Ob die rechtlichen Bestimmungen eingehalten werden, kann durch sporadisch einsetzbare externe Beobachter nur mit bedingter Zuverlässigkeit erfasst werden. Auch unangekündigte Inspektoren werden alleine durch die Präsenz von als solchen erkennbaren Kontrolleuren nur ein (eventuell geschöntes oder beschränktes) Zerrbild der „normalen“ Wirklichkeit ohne Inspektoren zu Gesicht bekommen.

OBSERVATION UND TÄUSCHUNG

Der Einsatz von Beobachtern kann schon durch deren Anwesenheit zu Verfälschungen führen. Eventuell wird gezielt etwas inszeniert, um einen falschen Eindruck zu erzeugen. Solchenizyn hat in seinem teils autobiografischen Roman *Der erste Kreis der Hölle* den Beobachtungen einer ausländischen Dame beim Besuch im Butyrka Gefängnis und der Inszenierung dessen, was sie beobachten sollte, ein literarisches Denkmal gesetzt. Sogar das Sonnenlicht wird dabei vorgetäuscht.

„Dafür hatte man auf dem Turm der Butyrka-Kirche einen Mann postiert, der mit Hilfe eines Drehspiegels allen Sonnenschein einfiel und in die Fenster der Zelle 72 lenkte.“, zitiert aus [Solchenizyn 1968/1973], S. 440.

Die Grenzen der Inszenierbarkeit werden in dem Moment, wo Essen gereicht wird, eigentlich auch überschritten, das Verhalten der Häftlinge lässt sich nicht mehr steuern – die „*Urinstinke*“ der sonst immerzu Hungernden treten hervor. Doch durch die kulturelle Distanz lässt sich die Beobachtung erklären: „*der Dolmetscher erklärte ihnen, daß es sich um eine russische Volkssitte handle.*“ So kommt die Dame trotz des beobachteten befremdlichen, hundeartigen Verhaltens der Gefangenen am Ende zu dem absurden Schluss, dass es sich um ein „*großartiges Gefängnis*“ handle. (Zitate aus [Solchenizyn 1968/1973], S. 444f)

Werden Beobachter derart erfolgreich getäuscht, so sind sie nicht einfach wirkungslos, sondern sie stützen das Regime, welches das Recht mit Füßen tritt, mit ihren Berichten auch noch und sie verhöhnern damit die Opfer, belasten die Glaubwürdigkeit etwaig überlebender Zeugen.

Neben dem Beobachten ist auch ein Testen der Handhabung der rechtlichen Maßgaben von innen heraus denkbar. Dazu kann sich z. B. unter speziell abgesicherten Bedingungen eine Testperson scheinbar einer Verletzung der S-Verfassung schuldig machen, um zu prüfen, ob die rechtlichen Maßnahmen korrekt angewandt werden. Dies kann sogar bis zum Antritt einer Strafe gehen, um einen authentischen Eindruck von innen heraus zu gewinnen.

Das Testen der rechtlichen Standardkonformität kann etwa aus Tests des korrekten Meldeverhaltens für die Unterbreitung eines Scheinangebotes zur Kooperation über mehrere Misstrauensparteien hinweg entwickelt werden. Wichtig ist, dass keinen dauerhaften Schäden entstehen können und dass die Testpersonen immer rehabilitiert werden.

TEST UNTER EXTREMEN BEDINGUNGEN: FREIWILLIGE INHAFTIERUNG ZUR INFORMATIONSGEWINNUNG

Ein Beispiel für eine Person, die sich freiwillig in eine extrem gefährliche Haft begeben hat, um von innen heraus als Betroffener beobachten zu können, ist der Pole Witold Pilecki, der sich 1940 von Deutschen verhaften ließ und so in das Konzentrationslager in Auschwitz gelangte.

“Thus, I am expected to describe bare facts only, as my colleagues want it. It was said: 'The more strictly you will adhere to nothing but facts, relating them without comments, the more valuable it will be'. So, I will try... but we were not made of wood... not to say of stone (but it seemed to me that also stone had sometimes to perspire). Sometimes, among facts being related, I will insert my thought, to express what was felt then. I do not think if it must needs decrease the value of what is to be written. We were not made of stone - I was often jealous of it - our hearts were beating - often in our throats, with some thought rattling somewhere, probably in our heads, which thought I sometimes caught with difficulty... About them - adding some feelings from time to time - I think that it is only now when the right picture can be rendered.”, zitiert aus [Pilecki 1943].

Pilecki ist 1943 aus dem Lager geflohen und er hat einen Bericht [Pilecki 1943] über seine Erlebnisse verfasst, welcher unter anderem der britischen Regierung zugestellt wurde. Pilecki überlebte nach dem KZ noch den Aufstand von Warschau, an dem er beteiligt war, und den 2. Weltkrieg.

1948 wurde er von den Kommunisten hingerichtet und erst 1990 rehabilitiert [Świerczek 2008].

Das freiwillige sich in Haft Begeben von Pilecki war eine unvergleichliche Heldentat. Er musste mit Folter und dem Tod rechnen, für ihn es gab keinen verlässlichen Weg zurück in die Freiheit.

Tests und Kontrollen durch Beobachter aus verschiedenen Misstrauensparteien können zwar helfen, Missstände aufzudecken und das S-Netzwerk eignet sich auch als Medium, um diese zu kommunizieren. Mit der Entdeckung und der Publizierung von Missständen sind dieselben jedoch noch nicht aus der Welt geschafft. Das Bekanntwerden erzeugt vielleicht einen gewissen Druck zur Korrektur, aber das wird vielleicht nicht immer genügen.

WAS PASSIERT BEI BEHARRLICHER ABWEICHUNG?

Für das S-Netzwerk sollen keine übergeordneten globalen rechtlichen Institutionen erschaffen werden – die einzelnen Rechtsräume bleiben vollständig souverän. Es gibt keine globale Macht, die im Fall von lokalen Verstößen gegen die Grundbestimmungen der S-Verfassung des S-Netzwerks die Einhaltung der Ordnung erzwingen könnte.

Weigert sich also etwa ein mächtiger Staat plötzlich, den gemeinsamen Bestimmungen und Regeln der S-Verfassung weiterhin Geltung zu verschaffen, sind die Möglichkeiten zur Einflussnahme auf diesen Staat naturgemäß beschränkt.

Gewiss kann durch das Zusammenstehen der übrigen Staaten oder Staatenbunde, welche am S-Netzwerk teilnehmen, ein gewisser Druck aufgebaut werden. Es könnten beispielsweise wirtschaftliche Sanktionen gegen den seine vertraglichen Verpflichtungen verletzenden Staat verhängt werden. Die Wirksamkeit und Durchsetzbarkeit solcher Schritte muss gerade gegenüber großen, weitgehend autarken Staaten bezweifelt werden. Außerdem würden damit auch Personen getroffen, die nicht am S-Netzwerk teilnehmen. Derartige wirtschaftliche Sanktionen oder gar militärische Druckmittel verstoßen gegen die Grundwerte und Prinzipien eines freiheitlichen, freiwilligen S-Netzwerks. In den Bestimmungen der S-Verfassung dürfen solche Maßnahmen nicht verankert werden.

Das S-Netzwerk soll auch gar nicht auf internationale, etwa „völkerrechtlich verbindliche“ Abkommen gestützt sein. Das S-Netzwerk soll nicht aufgrund von staatlichen und zwischenstaatlichen Beschlüssen bestehen. Das Bereitstellen eines gültigen S-Rechtsrahmens ist eine freiwillige Leistung eines souveränen Rechtsraums und dessen Souveränität muss durch das S-Netzwerk vollumfänglich geachtet werden.

Konkrete Maßnahmen, die zur Verfügung stehen, wenn sich in einem Rechtsraum keine rechtliche Standardkonformität im Sinne der S-Verfassung mehr herstellen lässt, sind die Androhung einer temporären Aussperrung und eines kompletten Ausschlusses aus dem S-Netzwerk. Damit diese Ansagen auch Wirkung zeigen können, muss auch eine realistische Umsetzbarkeit der angedrohten Maßnahmen gewährt sein, ohne dass dadurch gleich das gesamte S-Netzwerk unbrauchbar wird oder extreme Kosten entstehen. Auch muss verhindert werden, dass diese Maßnahmen missbraucht werden können. Sie sollten daher unter eine direkte basisdemokratische Kontrolle gestellt werden.

Die unmittelbaren Folgen des (temporären) Ausschlusses eines Rechtsraums sind im Wesentlichen darauf beschränkt, dass die Personen dieses Rechtsraumes nicht mehr aktiv an der Gemeinschaft des S-Netzwerks teilnehmen können. Der verlässliche Zugriff auf Inhalte im S-Netzwerk ist ihnen dann nicht mehr möglich.

Wenn die Mitgliedschaft im S-Netzwerk wertvoll genug ist, wenn die Teilnehmer nicht bereit sind, auf das S-Netzwerk zu verzichten, ist der mögliche (zeitweilige) Ausschluss eines Rechtsraums ein angemessen zielgenaues Druckmittel, um lokale Verstöße gegen die gemeinsamen Regeln und Bestimmungen der S-Verfassung zu bekämpfen.

Ein Staat, dessen Bürger unbedingt am S-Netzwerk teilhaben wollen, wird dann nicht ohne Weiteres den Ausschluss riskieren wollen. Zum einen muss also das S-Netzwerk attraktiv sein, zum anderen muss natürlich auch die Möglichkeit des Ausschlusses eines Rechtsraums realistisch und ohne übermäßige Nachteile für das S-Netzwerk gegeben sein.

2.6.3 UMGANG MIT KRITISCHEN EXTERNEN EREIGNISSEN

Es muss damit gerechnet werden, dass plötzlich große Teile des S-Netzwerks wegfallen können – eventuell kann dies auch dauerhaft geschehen. Der korrekte Betrieb des verbleibenden S-Netzwerkes muss trotzdem weiterhin gewährt werden können. Dazu sind in der S-Verfassung Maßnahmen wie die Datenmigration innerhalb einer Misstrauenspartei von einem Rechtsraum zu einem anderen, eventuell eigens dafür zu schaffenden Rechtsraum festzulegen.

Die Auseinandersetzung mit den bedrohlichen Szenarien im Zuge eines Risikomanagements soll helfen, das S-Netzwerk gezielt auf denkbare Vorkommnisse mit potenziell unerwünschten Folgen vorzubereiten. Schäden und Katastrophen können durch Schwachstellen in den technischen Systemen des S-Netzwerks oder durch beteiligte Personen ausgelöst werden. Zusätzlich können auch externe Einflüsse wie Naturgewalten zu einer Bedrohung für das S-Netzwerk werden. Gerade externe Bedrohungen lassen sich kaum kontrollieren. Entfesselte Gewalten am Ausbruch zu hindern kann unmöglich sein.

GAU UND SUPER-GAU

“Anything that can go wrong will go wrong!”, – diese aus der Erfahrung geborene pessimistische Weisheit ist weithin als *“Murphy's law”* bekannt. Zur Entstehung und zum historischen Hintergrund von *“Murphy's law”* sei hier auf [Spark 2003] verwiesen.

Soll das S-Netzwerk höchsten Sicherheitsanforderungen genügen und soll es so vertrauenswürdig wie möglich werden, muss ein defensives, alle denkbaren Risiken ernst nehmendes Design gewählt werden. Mit dem zeitnahen Eintreten von mehreren kritischen Ereignissen sowie von Ketten von kritischen Ereignissen („Klumpenrisiken“) ist zu rechnen. Nicht zuletzt aufgrund von der langzeitlichen Ausrichtung des S-Netzwerkes ist davon auszugehen, dass irgendwann auch vermeintlich sehr unwahrscheinliche kritische Ereignisse in ungünstigen Konstellationen eintreten werden. Das schließt insbesondere auch die Berücksichtigung der schlimmsten Katastrophenszenarien ein, die überhaupt vorstellbar sind (GAU, größter anzunehmender Unfall).

Es können natürlich zusätzlich noch Dinge passieren, die jenseits der Vorstellungskraft liegen, bevor sie erstmalig real eintreten. Katastrophen, welche die Grenzen des a priori Antizipierbaren überschreiten, werden als Super-GAU bezeichnet. Selbst mit einem sehr sorgfältigen und vorsichtigen Risikomanagement ist eine gezielte Vorbereitung auf das Udenkbare nicht zu bewerkstelligen. Umso wichtiger ist es, unspezifische Sicherheitsreserven anzulegen.

Wenn für das S-Netzwerk kritische Entwicklungen nicht unterbunden werden können, etwa weil sie durch unkontrollierbare externe Ereignisse ausgelöst werden könnten, müssen zumindest schadensbegrenzende Maßnahmen ergriffen werden. Die Konsequenzen des Unvermeidlichen dürfen keine Katastrophe für das S-Netzwerk und seine Teilnehmer werden. Also müssen die Folgen eingedämmt werden, soweit dies mit im Verhältnis zum potenziellen Schaden vertretbarem Aufwand zu bewerkstelligen ist.

Im Folgenden sollen für einige besonders kritische vorstellbare Katastrophenszenarien, die außerhalb des S-Netzwerks und unabhängig von seinen Teilnehmern ausgelöst werden können, mögliche Maßnahmen zur Schadensbegrenzung betrachtet werden.

AUSSCHEIDEN VON GANZEN RECHTSRÄUMEN

Das S-Netzwerk kann nur in Rechtsräumen existieren, in denen die rechtlichen Standards der S-Verfassung in S-Rechtsrahmen verankert sind und auch angewendet werden. Staaten oder Staatenbunde mit bisher intakter rechtlicher Basis für das S-Netzwerk können jederzeit die rechtlichen Rahmenbedingungen so verändern, dass davon auch die dortige rechtliche Verankerung der S-Verfassung ausgehebelt wird. Dies kann einerseits durch neue Gesetze oder durch einen Wandel des Staates bzw. Staatenbundes an sich (Zerfall, Vereinigung mit anderem Staat) herbeigeführt werden. Andererseits kann es indirekt ausgelöst

werden, wenn ein Staat oder Staatenbund nicht mehr die korrekte Anwendung seiner Implementierungen der S-Verfassung gewährleisten will oder kann.

Darüber, ob eine rechtliche Basis gültig ist, entscheiden in der S-Verfassung zu spezifizierende parteiübergreifende Prüfverfahren, welche eventuell basisdemokratische Abstimmungen zur letztinstanzlichen Entscheidungsfindung vorsehen. Wird im Zuge einer Überprüfung festgestellt, dass für einen Rechtsraum keine zur S-Verfassung konforme rechtliche Basis mehr existiert, wird in diesem Rechtsraum der Fortbestand des S-Netzwerks gefährdet. Erfolgt keine Korrektur, um wieder Konformität herzustellen, muss der Staat oder Staatenbund schlimmsten Falls aus dem S-Netzwerk ausgeschlossen werden.

Für das Ausscheiden von einem Staat oder von einem Staatenbund aus der Gemeinschaft jener Rechtsräume, in denen eine gültige Basis für das S-Netzwerk besteht, muss – unabhängig davon, wodurch diese Veränderung ausgelöst wird – ein geregeltes Prozedere festgelegt sein, damit das S-Netzwerk in anderen Rechtsräumen weiterhin bestehen und bestimmungsgemäß funktionieren kann.

Wie weitreichend die Folgen des Ausschlusses eines Rechtsraums R_A sind, hängt zunächst einmal davon ab, ob nach dem Ausscheiden von R_A in jener Misstrauenspartei P_i , zu der R_A bisher gehörte, noch mindestens eine gültige rechtliche Basis für das S-Netzwerk in einem anderen real existierenden Rechtsraum R_B besteht.

Gibt es nach wie vor einen solchen Rechtsraum R_B , der zu P_i gehört und in welchem die rechtlichen Voraussetzungen für den Betrieb des S-Netzwerks weiterhin gegeben sind, so können die S-Knoten, welche zuvor in dem nun ausscheidenden Rechtsraum R_A verankert waren, in den Rechtsraum R_B migriert werden. Fortan werden die migrierten S-Knoten in R_B betrieben, sodass sie nach wie vor in der gleichen Misstrauenspartei P_i verankert sind. Dazu ist eine Kooperation vonseiten des ausscheidenden Rechtsraumes R_A nicht erforderlich, notfalls können die auf den betroffenen S-Knoten gespeicherten Daten aus den Sicherungskopien im restlichen S-Netzwerk rekonstruiert werden. Lediglich die Verbindungsdaten für alle nach R_B migrierten S-Knoten zu jenen S-Knoten, die ihre Bekannten sind, müssen neu manuell ausgetauscht werden.

Die Zugänge aller Teilnehmer, die im ausscheidenden Rechtsraum R_A vertraglich verankert waren, werden geschlossen. Die S-Verträge dieser Teilnehmer werden durch den Ausschluss von R_A automatisch aufgekündigt, da es in R_A keinen gültigen S-Rechtsrahmen mehr gibt. Um wieder aktiv am S-Netzwerk teilnehmen zu können, bleibt den betroffenen Personen nur die Option, sich in einem Rechtsraum R_B , in dem weiterhin eine gültige rechtliche Basis für das S-Netzwerk besteht und der möglichst zur gleichen Misstrauenspartei P_i gehört, um den Abschluss eines neuen S-Vertrags zu bemühen. Eventuell wird dies nur möglich sein, wenn ein Wohnsitz in R_B gesucht wird – die weitere Teilnahme am S-Netzwerk erfordert dann also unter Umständen auch eine Migration der Person.

Weitreichender sind die Konsequenzen, wenn nach dem Ausscheiden eines Rechtsraums R_A in der Misstrauenspartei P_i keine gültige rechtliche Basis für das S-Netzwerk mehr besteht. In diesem Fall können die bisher in R_A verankerten und betriebenen S-Knoten nicht in einen anderen bestehenden Rechtsraum R_B in P_i migriert werden.

Es könnte versucht werden, fortan auf die Misstrauenspartei P_i zu verzichten und die zuvor in P_i zu speichernden und dort verfügbar zu haltenden Daten auf S-Knoten in anderen noch verfügbaren Misstrauensparteien mit intakten Rechtsrahmen zu verteilen. Es müsste dabei sichergestellt werden, dass etwaig bestehender Zugriffsschutz bestehen bleibt und dass die derart umverteilten Daten nach wie vor gefunden werden könnten.

Möglicherweise könnte auch ganz ohne die Misstrauenspartei P_i das gleiche Sicherheitsniveau des S-Netzwerks mit identischem Threshold Ψ aufrechterhalten werden. Rein technisch gesehen kann das bei jeder Anzahl der noch verfügbaren Misstrauensparteien größer gleich $3*\Psi - 2$ erreicht werden. Kommt für den Zugriffsschutz ohnehin ein Verfahren mit kurzen Schlüsseln ohne perfekte Sicherheit zum Einsatz, genügen $2*\Psi - 1$ andere Misstrauensparteien.

Die Migration aller Daten aus einer ganz ausscheidenden Misstrauenspartei ist mit be-

trächtlichem Aufwand verbunden. Je nach Konfiguration und eingesetzter Sicherheitstechnik werden fortan unter Umständen mehr Shares und mithin mehr Speicherplatz benötigt, um das gleiche Niveau beim Zugriffsschutz erreichen zu können.

Die Qualität des S-Netzwerks würde durch den Wegfall einer Misstrauenspartei wohlmöglich dauerhaft verschlechtert.

Außerdem könnte der Ausfall einer Misstrauenspartei sicherheitstechnisch nicht mehr kompensiert werden, sobald die Mindestzahl der Misstrauensparteien unterschritten würde. Also wird ohnehin auch ein weiteres Konzept benötigt, um den Fortbestand des S-Netzwerks in jedem Fall sichern zu können, wenn einer Misstrauenspartei die letzte gültige rechtliche Basis abhandenkommt.

Eine mögliche Alternative besteht in der radikalen Lösung, einen neuen souveränen Rechtsraum R_N für die Existenzsicherung von P_i zu erschaffen. Ein eigenständiges kleines Hoheitsgebiet muss nicht notwendigerweise von einem bestehenden Staat durch Verzicht auf ein Stück von dessen Staatsgebiet bereitgestellt werden. Es ist beispielsweise auch denkbar, eine schwimmende Station auf internationalen Gewässern als Hoheitsgebiet für den Rechtsraum R_N zu erschaffen. Die S-Verfassung muss in R_N implementiert werden, also muss in R_N ein vollständiger S-Rechtsrahmen erschaffen werden. In dem Rechtsraum R_N muss mindestens ein S-Betreiber rechtlich verankert sein, welcher die S-Knoten aus P_i auf dem Hoheitsgebiet von R_N verwaltet. Außerdem wird eine eigenständige Judikative und eventuell auch eine eigene Exekutive benötigt. Personen, die zu P_i gehören und die weiter am S-Netzwerk teilnehmen möchten, könnten dann unter Umständen in den Rechtsraum R_N migrieren. Sie müssten dazu nicht zwingend auf dem Hoheitsgebiet von R_N leben, es könnte eine Personenfreizügigkeit mit anderen Staaten geschaffen werden, die eine gültige Basis für das S-Netzwerk bieten.

Das Ausscheiden des letzten Rechtsraums aus einer Misstrauenspartei ist für das S-Netzwerk immer ein besonders schwerer Verlust und mit manuellem Aufwand verbunden. Um die Wahrscheinlichkeit dafür zu senken, dass eine Misstrauenspartei irgendwann ohne intakte rechtliche Basis dasteht, sollten zu jeder Misstrauenspartei mindestens zwei, idealerweise Threshold Ψ oder mehr verschiedene unabhängige Rechtsräume zugeordnet werden.

SCHWERWIEGENDE PHYSISCHE ZERSTÖRUNGEN

Die physische Vernichtung und Ausschaltung von Teilen der Infrastruktur des S-Netzwerks kann nach derzeitigem Stand der Forschung und der Technik nicht mit hundertprozentiger Sicherheit verhindert werden.

Gelegentliche durch die Beschädigung von Hardware bedingte Ausfälle von einzelnen technischen Komponenten, etwa von S-Knoten, werden im laufenden Betrieb des S-Netzwerks erwartet. Sie können, solange gleichzeitig nur Komponenten in weniger als Ψ Misstrauensparteien betroffen sind, im laufenden Betrieb kompensiert werden, ohne dass es zu Datenverlusten, zu Integritätsverlusten, zu größeren Ausfällen oder auch nur zu Verzögerungen kommt. Das restliche S-Netzwerk funktioniert dank des dezentralen Designs praktisch unbeeinträchtigt weiter.

Obwohl bei Ausfällen durch physische Zerstörung in insgesamt weniger als Ψ Misstrauensparteien keine irreparablen Schäden an den Informationen im S-Netzwerk entstehen, erhöht sich doch temporär das Risiko dafür, dass Manipulationen durchgeführt werden können. Schließlich dauert es eine gewisse Zeit, bis Schäden an Hardware behoben werden können. In diesem Zeitfenster ist es leichter, gezielt Verluste am Datenbestand des S-Netzwerks herbeizuführen. Wenn beispielsweise schon $\Psi - N \mid N \in \mathbb{N}$ Sicherungskopien in eben so vielen verschiedenen Misstrauensparteien durch physische Zerstörung vernichtet wurden und vorerst auch nicht repariert werden können, weil die physischen Systeme, auf denen dies geschehen sollte, noch nicht wieder einsatzfähig sind bzw. weil noch kein Ersatz bereitgestellt werden konnte, genügt es einem Angreifer bereits, nur noch N weitere

Sicherungskopien zu vernichten, um etwa einen irreparablen Datenverlust herbeizuführen.

Mögliche Ursachen für schwere physische Zerstörungen, die auch Systeme in mehreren Misstrauensparteien gleichzeitig schädigen können, sind beispielsweise:

- Naturkatastrophen mit potenziell großflächigen Zerstörungen
 - Erdbeben und Vulkanausbrüche, Tsunami
 - Extreme Wetterphänomene
 - Meteoriteneinschläge
- Menschlich verursachte Katastrophen mit potenziell großflächigen Zerstörungen
 - Aggressionen
 - Kriege
 - Terrorakte
 - Unfälle
 - Nuklearer Vorfall
 - Stromausfall (Blackout)

Gerade bei schwerwiegenden Zerstörungen etwa durch Naturkatastrophen ist davon auszugehen, dass die entstandenen Schäden an den technischen Systemen des S-Netzwerks nicht umgehend repariert werden können. In einem Krisengebiet müssen wahrscheinlich zunächst andere Prioritäten gesetzt werden, etwa zur Behebung von Zerstörungen an vitaleren Infrastrukturen oder unmittelbar zur Rettung von Leben. Bevor beispielsweise S-Knoten wieder ihre Aufgaben übernehmen können, muss ohnehin eine Versorgung mit Strom gesichert werden und es müssen funktionsfähige Kommunikationskanäle bereitgestellt werden.

Das Zeitfenster von der Zerstörung von technischer Infrastruktur für das S-Netzwerk bis zu ihrer voll funktionalen Wiederherstellung kann leicht mehrere Tage oder auch Wochen betragen, gerade wenn lokal im Krisengebiet dringendere Probleme bestehen, als etwa die Wiederherstellung von S-Knoten.

Also müssen geeignete Verfahrensweisen entwickelt werden, damit das Sicherheitsniveau des S-Netzwerks möglichst wenig beeinträchtigt wird. Mittelfristige Ausfälle von durch Katastrophen und Krisen direkt betroffenen logischen S-Knoten können nur dann vermieden werden, wenn die S-Knoten provisorisch außerhalb von Krisenregionen betrieben werden können, bis die akute Notlage überwunden ist. Idealerweise sollte der provisorische Betrieb eines S-Knotens S außerhalb des Katastrophengebietes in einem Rechtsraum stattfinden, der zur gleichen Misstrauenspartei P_i gehört wie der S-Knoten S .

Wenn sämtliche einer Misstrauenspartei P_i zugeordneten Rechtsräume von einer Krise betroffen sind, müssen die zu P_i gehörenden S-Knoten eventuell temporär außerhalb von P_i betrieben werden. Dies muss in einem von jeweils mindestens Threshold Ψ Misstrauensparteien kontrollierten, in der S-Verfassung vorgegebenen Rahmen geschehen, sodass Manipulationen mit weniger als Ψ beteiligten Misstrauensparteien durch das Provisorium nicht begünstigt werden. Da es sich nur um zeitlich begrenzte Maßnahmen für Notstandssituationen handeln soll, ist ein erhöhter Aufwand durch massive Kontrollen mit Kontrolleuren aus mindestens Ψ Misstrauensparteien vertretbar.

In der S-Verfassung können für katastrophal schwere physische Zerstörungen Beistandspflichten zwischen den Misstrauensparteien und Hilfeleistungen zum Überwinden von massiven Beschädigungen der technischen Infrastruktur des S-Netzwerks verbindlich vereinbart werden.

FATALE GROSSRÄUMIGE ZERSTÖRUNGEN

Die bisher gezeigten Sicherungskonzepte für die Inhalte des S-Netzwerks sind bei Ereignissen mit flächenmäßig sehr weit ausgedehnter destruktiver Wirkung eventuell nicht hinreichend: Wenn gleichzeitig mehr als Ψ S-Knoten in mehr als Ψ verschiedene

Misstrauensparteien zerstört werden, können auch im S-Netzwerk irreparable Schäden in Form von Datenverlusten entstehen. Speziell beim Zusammentreffen von mehreren katastrophalen Ereignissen oder in Kriegen kann eine entsprechend großräumige Zerstörung durchaus auftreten.

Um beispielsweise auch im Fall eines Weltkrieges und insbesondere auch dann, wenn dabei Atomwaffen eingesetzt werden, Daten bewahren und die Funktionalität aufrechterhalten zu können, sind weitergehende Schutzmaßnahmen erforderlich. Es ist sicher fraglich, wie wichtig das S-Netzwerk mit seinen Inhalten in einem solchen Szenario überhaupt noch sein kann.

Für die Langzeitarchivierung wird jedoch auch gerade der Anspruch erhoben, bedeutende Informationen und mithin das kulturelle Erbe sowie das Wissen der Menschheit auch über die Untergangsszenarien hinaus zu bewahren. Und es gibt Projekte, welche genau auf eine Bewahrung etwa auch in schlimmsten Kriegen abzielen. In Deutschland werden zu diesem Zweck am „zentralen Bergungsort“, im *Barbarastollen* bei Oberried in Baden-Württemberg, Mikrofilmrollen in Stahlfässern unter dem Schutz von 200 Metern stabilem Gneis gelagert [Fuchs 2011].

Das Haager Abkommen vom 14. Mai 1954 für den Schutz von Kulturgut bei bewaffneten Konflikten [UNESCO 1954] stellt eine wichtige völkerrechtliche Grundlage für Kriegsfälle dar. Der *Barbarastollen* ist derzeit der einzige Ort in Deutschland, der den höchsten Sonderschutz nach diesem Abkommen genießt ([Fuchs 2011], S. 17).

Man könnte versuchen, die Infrastruktur für das S-Netzwerk und insbesondere die S-Knoten, auf welchen die Sicherungskopien gespeichert werden, ebenfalls an geschützten Bergungsorten unterzubringen, an denen sie sogar oberirdische Explosionen von Atombomben und andere verheerende Ereignisse unbeschadet überstehen könnten.

Mit der Kombination von der dezentralen Verteilung von Sicherungskopien und dem starken Schutz der einzelnen Kopien könnte die Datenbewahrung im S-Netzwerk auch bestimmte fatale Katastrophen unbeschadet überstehen, die massive Zerstörungen in Ψ oder mehr verschiedenen Misstrauensparteien verursachen und die bei ungeschützten S-Knoten zwangsläufig zu Datenverlusten führen würden.

Allerdings kostet die Erschließung von hochgradig sicheren Bergungsräumen auch erhebliche Aufwendungen. Für den Betrieb von S-Knoten ist eine zuverlässige Stromversorgung, Datenverbindung und Kühlung notwendig. Ferner ist eine fortlaufende starke Bewachung der Eingänge notwendig, denn von innen heraus ist eine Zerstörung der Inhalte eines Bergungsraums wiederum leicht möglich.

Neben dem Krieg gibt es eine zweite Art von Katastrophen, die mit einem Schlag zumindest auf dem halben Globus schwerste Zerstörungen verursachen können: Tsunamis können alle Küsten eines Ozeans überfluten. Durch einen einzigen Tsunami kann es also leicht zu massiven Zerstörungen in Ψ oder mehr verschiedenen, geografisch sehr distanzierten Misstrauensparteien kommen. Ein Beispiel dafür, wie real diese Bedrohung ist, ist der Tsunami vom 26.12.2004 im Indischen Ozean [Iwan 2006], wobei die Flutwelle nicht nur auf Sumatra, Sri Lanka, in Indien und in Thailand große Zerstörungen verursachte und viele Todesopfer forderte, sondern auch in großer räumlicher Entfernung zum Epizentrum des auslösenden Erdbebens, etwa auf den Malediven (Distanz etwa 2500 km) und in Somalia (Distanz über 5000 km) [Fritz 2005].

Zum Schutz vor Tsunamis und Überflutungen kann die bedachte Wahl des Standortes von Rechenzentren für das S-Netzwerk bereits hinreichend sein. Allerdings gibt es nicht in jedem Rechtsraum einen passenden Standort. Das gilt beispielsweise für viele Inselstaaten, deren größte Erhebung sich unter der Höhe von Flutwellen befindet, wie sie von Tsunamis ausgelöst werden können. In einem solchen Rechtsraum wäre zum effektiven Schutz vor Tsunamis und Überflutungen im Allgemeinen ein künstlicher Bergungsraum erforderlich.

Welches Sicherheitsniveau für das S-Netzwerk und seine Inhalte angestrebt werden soll und welches Maß an Katastrophenschutz erreicht werden soll, ist eine politische Entscheidung, über die in der formgebenden Phase abzustimmen ist.

2.7 REALISIERUNG IN ÖKOLOGISCHER VERANTWORTUNG

Das S-Netzwerk soll sich dauerhaft entwickeln können – es ist ganz auf die langfristige Zukunft ausgerichtet. Konsequenterweise soll die Verwirklichung des S-Netzwerks auch nachhaltig betrieben werden.

2.7.1 RESSOURCENVERBRAUCH UND UMWELTBILANZ

Durch die Sicherheitskonzepte und durch die garantierte dauerhafte Verfügbarkeit des S-Netzwerks entsteht im Falle einer Realisierung absehbar ein signifikanter und fortwährender Ressourcenbedarf sowie Energiehunger. Es obliegt der gemeinsamen Verantwortung der Entwickler, Betreiber und der Teilnehmer, eine sinnlose Verschwendung zulasten der Natur und auf Kosten künftiger Generationen zu vermeiden. Dem soll konzeptionell vom Beginn der Entwicklung an Rechnung getragen werden mit ökologischem Design und mit in der S-Verfassung festgeschriebenen Standards.

Kommunikations- und Informationstechnik haben alleine schon durch die verbreitete Nutzung und den damit verbundenen Energiebedarf Auswirkungen auf die Umwelt. Der Anteil der Kommunikations- und Informationstechnik am Gesamtstromverbrauch in Deutschland liegt laut [Cremer 2003] immerhin bei 8%, Tendenz steigend.

Die Erfassung des Energieverbrauchs eines sich bereits in der Praxis im Betrieb befindlichen Systems, etwa eines physischen Servers, ist mit Messgeräten präzise möglich. Auch Leistungsdaten sind mit Benchmark-Programmen messbar, sodass sich die Energieeffizienz leicht bestimmen lässt.

BENCHMARKS FÜR DIE ENERGIEEFFIZIENZ IN DER IT

Die Energieeffizienz wird in der Informationstechnik oft als Rechenleistung pro Watt angegeben. Gemessen wird die Rechenleistung mit Hilfe von Programmen wie LINPACK [Dongarra 2011] und als Einheit dienen typischerweise Operationen pro Zeiteinheit, etwa floating point operations per second (FLOPS). Für Supercomputer, die z. B. für komplexe wissenschaftliche Berechnungen genutzt werden, ist diese einfache Bestimmung der Energieeffizienz durchaus realistisch, da hier oftmals die volle Rechenleistung über lange Kalkulationen und Simulationen hinweg benötigt wird. Ein Ranking der energieeffizientesten Großrechner findet sich in der Green500 Liste (<http://www.green500.org> – abgerufen am 23. Juli 2018).

Die Rechenleistung pro Watt unter Volllast ist jedoch für Systeme wie S-Knoten, bei denen je nach Aufkommen von Benutzeranfragen sehr unterschiedliche Belastungen und sogar längere Phasen des Leerlaufs zu erwarten sind, kaum aussagekräftig:

“IT computing environments are almost exclusively NOT steady state and are almost exclusively NOT run at 100% of the available compute potential of the system. There can be significant differences between power characteristics for a computer system at high utilization compared to one operating at low utilization. There can also be significant differences in the way a power management feature manages power at a low, but steady utilization point, compared to the way it manages power in an environment where the workload fluctuates rapidly between high and low volumes.”, zitiert aus [SPEC Power Committee 2010], S. 5.

Um realistische, reproduzierbare und vor allem mit Werten für andere Systeme vergleichbare Ergebnisse zur Energieeffizienz im laufenden Betrieb zu ermitteln, muss es möglich sein, verschiedene Auslastungen zu simulieren und zu berücksichtigen. Für die Messung der Energieeffizienz speziell von Servern gibt es dazu z. B. den standardisierten SPECpower_ssj2008 Benchmark (<http://www.spec.org/power> – abgerufen am 23. Juli 2018), der differenzierte Werte für unterschiedliche Nutzungsgrade liefert. Eine Analyse der Ergebnisse dieses Benchmarks für verschiedene Systeme findet sich in [Hsu 2011]. Ein Vergleich zwischen SPEC Power und anderen Energie-Benchmark-Programmen findet sich in [Poess 2010].

Energieverbrauch sowie Energieeffizienz nur im laufenden Betrieb zu betrachten liefert jedoch ein unvollständiges Bild und erlaubt noch keine ökologische Gesamtbeurteilung. Energie- und Ressourcenbedarf sowie Umweltverträglichkeit von einzelnen informationstechnischen Hardware-Komponenten müssen grundsätzlich jeweils über die beabsichtigte Nutzung hinausgehend betrachtet werden – über den ganzen Lebenszyklus hinweg.

Das umfasst zunächst die Erschaffung des Gerätes, welche in der Regel Energie, Rohstoffe sowie eine Transportinfrastruktur und Transportleistungen beansprucht, wodurch umweltschädliche Emissionen freigesetzt werden können und eventuell nur begrenzt verfügbare Ressourcen aufgebraucht werden. Die in [Angerer 2009] vorgestellte Studie gibt Auskunft über die Rohstoffe, welche für die Produktion von diversen hochtechnologischen Produkten jeweils benötigt werden.

Der bestimmungsgemäße Einsatz oder Betrieb kann natürlich ebenfalls einen signifikanten Verbrauch verursachen und eine fortlaufende Belastung für die Natur bedeuten. Schließlich muss auch die Entsorgbarkeit und insbesondere die nützliche Wiederverwendbarkeit von Geräten bzw. von den eingesetzten Materialien am Ende des Lebenszyklus Beachtung finden.

ELEKTROSCHROTT

Durch Informationstechnik entstehen derzeit erhebliche Abfallmengen. Alleine für die USA fielen laut [USEPA 2011] im Jahr 2009 2,37 Millionen amerikanische Tonnen Elektroschrott an, wovon nur 25% zum Recycling gebracht wurden.

Die Initiative *Solving the E-waste Problem (StEP)* ist eine Organisation, welche sich wissenschaftlich mit den Möglichkeiten der Entsorgung und Wiederverwendung von ausrangierten elektronischen Geräten bzw. der darin eingesetzten Materialien beschäftigt.

Um die schädlichen Auswirkungen von elektronischem „Schrott“ auf die Natur einzudämmen, gibt es verschiedene Ansatzpunkte, für die jeweils eigene Task-Forces in der StEP Initiative existieren [Adrian 2011]:

- Sinnvolle Weiternutzung von veralteten Geräten (ReUse)
- Verzicht auf Giftstoffe, Verwendung von wiederverwendbaren Materialien und Kennzeichnung derselben (ReDesign)
- Recycling der Materialien (ReCycle)
- Verbindliche Regeln etwa zur Rücknahme von bestimmten Gerätetypen durch die Hersteller (Policy)

Ein Beispiel für solche Regulierungen ist die Waste Electrical and Electronic Equipment (WEEE) Directive der Europäischen Union, welche in [Huisman 2007] analysiert wird.

Ein Indikator für die Umweltverträglichkeit eines Produktes ist der CO₂ Ausstoß, der durch dieses Produkt über dessen ganzen Lebenszyklus hinweg verursacht wird. Dieser Wert wird auch als CO₂ Fußabdruck bezeichnet.

Angaben für den CO₂ Fußabdruck von einzelnen IT Systemen finden sich etwa in [Böttner 2011], wobei hier eine effektive Nutzungsdauer von fünf Jahren zugrunde gelegt wird und auch die verschiedenen Standards zur Berechnung des CO₂ Fußabdrucks vorgestellt werden. Die Nutzungsdauer ist entscheidend für eine ökologische Gesamtbeurteilung: Je geringer die Einsatzdauer ausfällt, desto stärker fallen die Erschaffung und die Entsorgung im Verhältnis zum laufenden Betrieb ins Gewicht.

Für neuartige Systeme lässt sich eventuell nicht prognostizieren, wie lange sie durchschnittlich halten werden und wie groß die Streuung sein wird, da Erfahrungswerte naturgemäß noch nicht vorhanden sind. Technische Weiterentwicklungen oder Änderungen im Bedarf können auch eine vorzeitige Ablösung von noch fehlerfrei arbeitenden Systemen sinnvoll oder notwendig machen. In Bereichen mit einer hohen Innovationsrate und geringen Erfahrungswerten, speziell in der Informationstechnik, lässt sich die effektive Nutzung nur mit einer gewissen Unsicherheit abschätzen.

Weitere Schwierigkeiten ergeben sich aus der Veränderbarkeit von Systemen, die sich aus einer Vielzahl von verschiedenen dynamisch verbundenen Geräten zusammensetzen: In einem offenen informationstechnischen Netzwerk wie dem Internet variieren die

Konstellationen und Quantitäten der beteiligten Einzelsysteme ständig. Eine exakte Erfassung des Energieverbrauchs des Internets etwa wäre nur zu bestimmten Zeitpunkten möglich, da sich das zu untersuchende Gesamtsystem über die Zeit laufend verändert.

Auch lassen sich solche Systeme nicht immer ohne Weiteres isoliert betrachten: Große Teile der Infrastruktur, welche für das Internet genutzt wird, dienen nicht ausschließlich für das Internet, sondern auch für Telefonie oder für das Kabelfernsehen.

GREEN IT

Da die Informations- und Kommunikationstechnik in erheblichem Maß Ressourcen verbraucht und Umweltprobleme verursacht, hat sich ein eigenes Forschungsfeld eröffnet, das darauf abzielt, die ökologische Verträglichkeit dieser Techniken zu verbessern. Beispielsweise wird in [Gupta 2003] der Energiebedarf für das Internet analysiert und es werden Sparpotenziale aufgezeigt.

Für die umfangreichen Bestrebungen, möglichst umweltverträgliche Informations- und Kommunikationstechnik zu entwickeln und zu produzieren, haben sich die Bezeichnung Green IT und Green Computing etabliert [Murugesan 2008].

Firmen aus der IT-Branche legen inzwischen großen Wert auf die Umweltverträglichkeit ihrer Produkte. Als Beispiele für die Bestrebungen seien hier Apple [Jobs 2007 a] oder Microsoft [Fontana 2008] genannt. In [Kounatze 2009] findet sich eine Studie über 92 verschiedene Initiativen zum Thema Green IT, die über den Rahmen eines einzelnen Unternehmens hinausgehen.

Schon bei der Erforschung von neuen Möglichkeiten und bei der frühen Planung von Produkten sowie Systemen sollten die Folgen für die Umwelt berücksichtigt werden. Forscher und Designer haben eine besondere ökologische Verantwortung, da sie frühzeitig die möglichen ökologischen Auswirkungen ihrer Erkenntnisse sowie Ideen abschätzen können und die weitere davon ausgehende Entwicklung entscheidend beeinflussen können. In Anbetracht der drängenden Umweltprobleme wie dem Klimawandel sollte es für alle Forscher und Erfinder eine Selbstverständlichkeit sein, die Auswirkungen ihrer Innovationen auf die Umwelt zu hinterfragen und zu beleuchten.

In einer ökologischen Bilanzierung müssen natürlich auch mögliche positive Effekte berücksichtigt werden. Kommunikations- und Informationstechnik verursacht nicht nur Belastungen, sondern sie ermöglicht vielleicht auch Einsparungen und Verbesserungen für die Umwelt an anderen Stellen: Im Fall des Internets ist beispielsweise zu beachten, dass etwa durch die Ersetzung von papiergebundenen durch elektronische Briefe oder durch den Einsatz von Audio- oder Videokonferenzen anstelle von persönlichen Treffen mit unter Umständen langen Anreisewegen auch wieder Energie und Rohstoffe gespart werden können. Eine Reihe von Fallstudien für die positiven ökologischen Effekte von Informationstechnologie findet sich in [Neves 2010].

ÖKOLOGISCHE BETRACHTUNG DES S-NETZWERKS: IM SPANNUNGSFELD DER INTERESSENKONFLIKTE

Aufgrund der potenziell erheblichen ökologischen Auswirkungen eines großen vernetzten Computersystems erscheint eine umfassende Analyse der Umweltverträglichkeit im Fall des S-Netzwerkes geradezu obligatorisch. Wenn das S-Netzwerk verwirklicht wird, entsteht durch die Erschaffung und den Betrieb der informationstechnischen Infrastruktur sowie durch weitere Erfordernisse zur Erfüllung der hohen Ansprüche in Sachen Sicherheit, Verfügbarkeit und Vertrauenswürdigkeit ein erheblicher Ressourcen- und Energiebedarf. Werden von Anfang an ökologische Aspekte in der Konzipierung, Planung und Umsetzung des S-Netzwerkes berücksichtigt, so kann dies einen signifikanten Unterschied machen. Bis zum Ende der formgebenden Phase zur Schaffung des S-Netzwerkes, spätestens bis zur Abstimmung über die S-Verfassung, sollte eine vollständige Analyse der ökologischen Aspekte erfolgen, damit die Erkenntnisse daraus in die weitere Entwicklung einfließen können. Hier sollen im Folgenden bereits einige Gedanken zur Umweltverträglichkeit des S-Netzwerkes vorgestellt werden.

Wie hoch der Bedarf an Ressourcen und Energie für das S-Netzwerk konkret sein wird, das wird bereits wesentlich von den genauen Spezifikationen der S-Verfassung abhängen. So bestimmt etwa die Festlegung des Thresholds Ψ und der Anzahl $\#P$ der Misstrauensparteien nicht nur das Maß der Redundanz im S-Netzwerk und mithin das erzielbare

Sicherheits- sowie Zuverlässigkeitsniveau, sondern auch die Größenordnung der zu speichernden, zu verschlüsselnden und zu übertragenden Datenmengen im S-Netzwerk. Ein höherer Threshold Ψ bringt zwar mehr Sicherheit, führt aber auch zu mehr Datenaufkommen und einem entsprechend höheren Ressourcenverbrauch etwa zur Bereitstellung der nötigen Speicherkapazitäten und Rechenkapazitäten. Ebenso führt eine geringere Anzahl $\#P$ der Misstrauensparteien als $\Psi \cdot (2 \cdot \Psi - 1)$ zu erhöhtem Speicherplatzbedarf und Datenaufkommen, wenn der Zugriffsschutz mit perfekt sicherem Secret Sharing erfolgt. Sicherheitstechnisch ist hingegen ein großes Verhältnis von Ψ zu $\#P$ erstrebenswert.

ABSCHÄTZUNG DES SPEICHERPLATZBEDARFS

Neben den Vorgaben aus der S-Verfassung und der Datenmenge, welche die Teilnehmer im S-Netzwerk speichern, wird der Ressourcenverbrauch auch von der qualitativen Art der Nutzung des S-Netzwerks abhängen. Entscheidend ist, welcher Zugriffsschutz für welche Datenmengen gewählt wird. Nicht alle Inhalte werden zugriffsbeschränkt sein und für manche Inhalte genügt eventuell ein Zugriffsschutz mit reduziertem Secret Sharing oder mit einem der vorgestellten Verfahren mit kurzen Schlüsseln.

Tabelle 6 zeigt für verschiedene Konfigurationen des S-Netzwerks, wie sich exemplarische Verteilungen des Schutzbedürfnisses von Daten auf die im S-Netzwerk entstehende Datenmenge auswirken. Dabei ist N die Anzahl an Shares, die für vollen Secret Sharing Zugriffsschutz benötigt werden. Es sei R die maximale Anzahl an Shares, für den gilt: $R \cdot (2 \cdot \Psi - 1) \leq \#P$. Mit auf R Shares reduziertem Secret Sharing lässt sich ein effizienterer Zugriffsschutz für Inhalte mit geringerem Schutzbedürfnis realisieren, bei dem jede Misstrauenspartei nur eine Kopie genau eines Shares verfügbar halten muss.

Ψ	$\#P$	N	R	0 Shares: 80 %	0 Shares: 20 %	0 Shares: 80 %	Kein Schutz: 20 %
				R Shares: 0 %	R Shares: 0 %	R Shares: 15 %	R Shares: 60 %
				N Shares: 20 %	N Shares: 80 %	N Shares: 5 %	N Shares: 20 %
5	45	5	5	1620,00%	3780,00%	1620,00%	3780,00%
5	36	8	4	2160,00%	5940,00%	1620,00%	3780,00%
5	27	14	3	3240,00%	10260,00%	1755,00%	4320,00%

Tabelle 6: Speicherplatzbedarf auf den S-Knoten im Verhältnis zur effektiven Datenmenge

Je mehr das S-Netzwerk als Plattform für offene Daten sowie für Daten benutzt wird, die nur einen geringen Zugriffsschutz benötigen, desto weniger negativ wirkt sich ein großes Verhältnis vom Threshold Ψ zur Anzahl $\#P$ der Misstrauensparteien auf den Speicherplatzbedarf aus. Zur Beurteilung der ökologischen Eigenschaften einer möglichen Konfiguration für das S-Netzwerk muss daher auch abgeschätzt werden, wie intensiv von dem Zugriffsschutz per Secret Sharing Gebrauch gemacht wird.

Das Konzept zur Datensicherung im S-Netzwerk beruht auf Redundanz. Es kann nur dann dauerhaft funktionieren, wenn immer wieder die Korrektheit der Sicherungskopien überprüft wird und wenn etwaige Fehler korrigiert werden. Je häufiger die Korrektheit der Sicherungskopien geprüft wird, desto geringer ist die Wahrscheinlichkeit, dass es zu Datenverlusten kommt. Andererseits verursacht das Überprüfen der Kopien Datenverkehr und Rechenlast auf den S-Knoten. Eine allzu hohe Frequenz der Prüfungen wird durch den daraus entstehenden Aufwand die Umwelt stark belasten.

Es ergeben sich offenbar Interessenkonflikte zwischen den Sicherheitsbedürfnissen auf der einen Seite und den Anliegen des Umweltschutzes sowie der ökologischen Verträglichkeit durch Ressourcenschonung auf der anderen Seite.

DAS S-NETZWERK – EIN BALANCEAKT

Das S-Netzwerk soll nicht nur sicher, zuverlässig und dabei möglichst ökologisch werden, es soll auch leistungsstark sein und eine gute Performance bieten. Das S-Netzwerk muss

mit seiner aufwendigen Sicherheitstechnik kein Hochleistungsmedium für Echtzeitanwendungen wie etwa Videokonferenzen in 3D-QHD werden – dazu ist es nicht gedacht. Aber eine zu niedrige Performance im Vergleich zu anderen Computernetzwerken könnte dazu führen, dass das S-Netzwerk als Speicherplattform gar nicht akzeptiert wird. Kurze Zugriffszeiten (Latenzzeiten) und hohe effektive Datenübertragungsraten sind erstrebenswert, damit die Nutzer nur geringe Wartezeiten hinnehmen müssen und damit eine hohe Präzision etwa bezüglich der rechtsgültigen Feststellbarkeit des Publikationszeitpunktes erzielt werden kann. Für die zu erreichende Performance werden in der S-Verfassung mit der garantierten Durchführungszeit ζ_X und der garantierten Zugriffszeit ϵ_X gewisse Mindeststandards festgelegt.

Es müssen Leistungsreserven geschaffen werden, damit diese Vorgaben auch unter ungünstigen Umständen eingehalten werden können. Der Einsatz von möglichst leistungsstarker informationstechnischer Infrastruktur steht wiederum im Konflikt mit Umweltschutz und Ressourcenschonung. Wird nur die Performance betrachtet, so müssten immer die schnellsten verfügbaren Geräte eingesetzt werden. Ökologisch verträglicher ist hingegen oftmals eine längerfristige Nutzung der bestehenden Systeme. Auf Energiesparmaßnahmen, welche etwa Taktraten bei geringer Last senken oder Teile der Hardware zwischenzeitlich abschalten, müsste zur Maximierung der Performance ebenfalls verzichtet werden, denn das Reaktivieren und Beschleunigen bei stärkerer Belastung kostet Zeit.

BEISPIEL FÜR ENERGIESPARRMASSNAHMEN MIT VERTRETBARER LEISTUNGSEINBUSSE

Durch ein effizientes Anpassen von Rechenleistung bzw. Übertragungsraten an den aktuellen Bedarf und durch die Nutzung von Ruhezuständen in Netzwerkgeräten wie Routern sind beispielsweise signifikante Energieersparungen möglich, sofern leichte Performanceeinbußen, speziell Anstiege der Latenzzeiten, als vertretbar anzusehen sind:

“For instance, our practical algorithms stand to halve energy consumption for lightly utilized networks (10-20%).” ... “Moreover this energy can be saved without noticeably increasing loss and with a small and controlled increase in latency (<10ms).”, zitiert aus [Nedevschi 2008].

Für das S-Netzwerk sind solche geringfügigen Verzögerungen vielleicht nicht kritisch. Daher können für das S-Netzwerk wohlmöglich alle Netzwerkgeräte mit entsprechenden Maßnahmen zum Energiesparen betrieben werden.

Sicherheitsinteressen stehen auch mit der Leistungsmaximierung im Konflikt: Das Erhöhen von Ψ verbessert die Sicherheit und Zuverlässigkeit des S-Netzwerks, es kostet aber auch Performance, da mehr Shares und Sicherungskopien erzeugt beziehungsweise verarbeitet werden müssen. Je höher Ψ gewählt wird, desto mehr Rechenleistung und Datendurchsatz muss etwa bei den einzelnen S-Knoten bereitgestellt werden, damit ein bestimmtes Level an Performance etwa bei der Durchführung einer reliablen Publikation gehalten werden kann.

Es ergibt sich ein komplexes Spannungsfeld von miteinander im Konflikt stehenden Interessen, die alle ihre Berechtigung haben und zu denen auch noch die Wirtschaftlichkeit hinzukommt.

Für das S-Netzwerk können dabei gewisse Prioritäten gesetzt werden: An oberster Stelle stehen die Sicherheitsbedürfnisse – Sicherheit und Zuverlässigkeit sind schließlich die Hauptanliegen bei der Erschaffung des S-Netzwerks. Wenn das S-Netzwerk inkorrekt funktioniert und keines Vertrauens würdig ist, verliert es seine Daseinsberechtigung.

Langlebigkeit ist ebenfalls ein erklärtes Ziel für die Erschaffung des S-Netzwerks, und da ökologische Auswirkungen langfristig spürbar sind, sollte Umweltschutz sowie Ressourcenschonung auch hohe Priorität eingeräumt werden. Es lohnt sich nicht, ein technisch hochgradig zukunftstaugliches System zu erschaffen und dafür die Zukunft von künftigen Generationen schwer zu belasten oder gar zu zerstören.

Eine gute Performance ist zwar auch wünschenswert und in einem gewissen Maße notwendig. Die Folgen von Leistungsschwankungen und anderen Performanceproblemen

wirken sich jedoch eher kurzfristig aus. Das Design des S-Netzwerks soll langfristig ausgerichtet sein, entsprechend sollen die Prioritäten gesetzt werden.

RECHTLICHE MÖGLICHKEITEN, EINE UMWELTGERECHTE IT-INFRASTRUKTUR ZU FÖRDERN

Mit sorgfältig durchgeführten Analysen und Prognosen bietet sich beim S-Netzwerk die Chance, Umweltschutzfragen vom Beginn der Planung an zu berücksichtigen und mit geeigneten Maßnahmen sowie Konzepten die Voraussetzungen für ein ökologisch möglichst verträgliches S-Netzwerk zu schaffen.

Eine einheitliche Linie mit verbindlichen Vorgaben für den Naturschutz kann im ganzen S-Netzwerk über Landesgrenzen hinweg vereinbart und durchgesetzt werden: In die S-Verfassung können global strenge Standards für einen umweltfreundlichen Betrieb des S-Netzwerks festgeschrieben werden. Durch die notwendige rechtliche Verankerung wird daraus wo immer den Einwohnern die Teilnahme am S-Netzwerk ermöglicht werden soll durch gesetzliche Implementierungen anwendbares und verbindlich gültiges Recht.

Das einheitliche rechtliche Grundgerüst der S-Verfassung, welches initiativ von den Entwicklern des S-Netzwerks zu gestalten ist, unterscheidet das S-Netzwerk von anderen rein technischen Entwicklungen. Dieses Potenzial muss auch zum Wohle der Umwelt ausgeschöpft werden.

JENSEITS DER INFORMATIONSTECHNIK

Das S-Netzwerk besteht nicht nur aus Computer- und Kommunikationstechnik. Verwaltungstechnische Notwendigkeiten wie die manuellen Identitätsprüfungen und der manuelle Schlüsselaustausch müssen auch als ein ökologischer Faktor berücksichtigt werden.

Durch die vorgesehene Aufteilung vieler Verantwortlichkeiten auf verschiedene Misstrauensparteien sind solche Schritte zwangsläufig internationale, weltumspannende Aktionen. Der logistische und manuelle Aufwand zur Identitätsprüfung steigt mit der Anzahl der Misstrauensparteien, in denen eine *Bekanntschaft* hergestellt werden muss.

Es müssen eventuell reale Personen, physische Dokumente oder gegenständliche Schlüsseldatenträger rund um den Globus bewegt werden – und zwar mit hohen Sicherheitsvorkehrungen. Je nach eingesetzter Technik, etwa mit Einwegschlüsseln, muss der Schlüsseltausch für jede *Bekanntschaft* wiederholt werden, sobald Schlüssel verbraucht oder nicht mehr sicher sind.

Ökologisch potenziell belastende Faktoren sind neben den dabei durchzuführenden (Flug-) Reisen und Transporten auch die benötigten Datenträgermedien.

Die interne Organisation des S-Netzwerks an sich kann auch einen gewissen Energie- und Ressourcenbedarf verursachen, etwa bei der Durchführung von Konferenzen oder von geheimen Abstimmungen.

Im laufenden Betrieb beeinflussen die aktiven Teilnehmer des S-Netzwerkes über ihr Nutzungsverhalten maßgeblich den Energie- und Ressourcenverbrauch, welcher durch die informationstechnische Infrastruktur des S-Netzwerks verursacht wird.

Das S-Netzwerk sollte nur dann zum Speichern von Daten genutzt werden, wenn auch wirklich die erzielbare unleugbare Verlässlichkeit von reliablen Publikationen oder sicheren Hinterlegungen benötigt wird. Der Einsatz von Secret Sharing für den Zugriffsschutz sollte auf das unbedingt notwendige Maß reduziert werden.

Im Rahmen des Erlernens und des obligatorischen Nachweisens der Medienkompetenz für das S-Netzwerk sollen die potenziellen Teilnehmer für die mit dem Beitritt verbundene ökologische Verantwortung sensibilisiert werden. Dabei kann es nicht nur darum gehen, auf die Folgen des Ressourcenbedarfs der IT-Infrastruktur des S-Netzwerkes hinzuweisen. Vielmehr muss auch und gerade auf das erhebliche Potenzial zur Schonung der Umwelt durch den klugen Einsatz des S-Netzwerks Wert gelegt werden.

S-Netzwerk und S-Web bieten die Voraussetzungen, viele Arten von Geschäften ganz

ohne Papier abzuwickeln, und das auch aus großer räumlicher Distanz. Möglichkeiten wie Fair-Non-Repudiation Kommunikation und Fair-Contract-Signing mit allen Teilnehmern können anstelle von gegenständlicher Post und von Geschäftsreisen unmittelbar dazu beitragen, Ressourcen zu sparen und die Umwelt zu schonen.

Dadurch, dass die Verfügbarkeit der Inhalte dauerhaft garantiert wird, entfällt die Notwendigkeit, unverzichtbar erscheinende Daten zu kopieren und sie extra lokal auf Systemen unter eigener Kontrolle zu speichern sowie zu pflegen. Neue Werke, welche im S-Netzwerk publizierte Inhalte als Bestandteile verwenden, brauchen die Quellen nicht zu duplizieren und zu integrieren, um sicherzustellen, dass sie unverändert verfügbar bleiben (nicht-lineares Schreiben mithilfe von S-Links). Die intelligente Nutzung des S-Netzwerks und des S-Webs kann dazu führen, dass letztlich trotz der über S-Knoten verteilten Sicherungskopien sogar weniger Speicherplatz benötigt wird, als wenn die Daten mehrfach, aber eben jeweils sehr unzuverlässig im Internet und auf Client-Systemen gespeichert würden.

Der Einsatz des S-Netzwerks in der Wirtschaft hat das Potenzial, neben einzelnen Geschäftsprozessen sogar das Wirtschaftssystem selbst grundlegend zu verändern, sodass auch weitere, erheblich stärkere positive ökologische Folgen denkbar sind.

Engagierte Teilnehmer mit hoher Kompetenz in der Mediennutzung und in der Mediengestaltung können dazu führen, dass das S-Netzwerk keine Belastung für die Umwelt wird, sondern letztlich einen wertvollen Beitrag zu ihrem Schutz leistet.

2.7.2 ÖKOLOGISCHE ASPEKTE ZUM BETRIEB DER S-KNOTEN

Die Entwicklung und der permanente Betrieb jener Computersysteme, auf denen die logischen S-Knoten laufen sollen, führt zu einem beträchtlichen Ressourcen- und Energiebedarf.

Es soll möglich sein, S-Knoten als eigenständige physische Systeme oder auch als virtuelle Server zu betreiben, wobei jeweils unterschiedliche ökologische Maßgaben entsprechend der technischen Möglichkeiten gelten sollen.

Die physischen Umsetzungen der logischen S-Knoten bilden den informationstechnischen Kern des S-Netzwerks. Die zu einem Peer-Netzwerk verbundenen S-Knoten stellen die Funktionalität zum reliablen Publizieren, zum sicheren Hinterlegen sowie zum verlässlichen Verlinken von Informationen bereit und gewähren nach den Regeln der S-Verfassung Zugriff auf die Daten.

Die Redundanz der Verteilung von Sicherungskopien auf S-Knoten in verschiedenen Misstrauensparteien sorgt dafür, dass ein Ausfall von weniger als Ψ beliebigen S-Knoten zur selben Zeit zu keinen Beeinträchtigungen der Korrektheit oder der garantierten Verfügbarkeit der Inhalte des S-Netzwerkes führen kann.

Trotzdem soll jeder einzelne S-Knoten auch möglichst jederzeit erreichbar sein, um die Wahrscheinlichkeit, dass jemals Ψ S-Knoten gleichzeitig nicht erreichbar sind, so gering wie möglich zu halten. Außerdem können dadurch Nachrichten effizient weitergeleitet werden, ohne dass es zu unnötigen Verzögerungen kommt, weil einzelne S-Knoten zeitweilig nicht korrekt reagieren. Es gilt, für logische S-Knoten die richtige Balance zwischen hochgradiger Verfügbarkeit und umweltschonender Ressourcenschonung zu finden.

Es gibt im Wesentlichen zwei verschiedene Ansätze zur Realisierung von unabhängigen logischen S-Knoten auf physischen Computersystemen:

Zum einen ist die Umsetzung von je einem logischen S-Knoten auf jeweils einem eigenständigen physischen Rechner machbar.

Zum anderen können mit Virtualisierungslösungen [Goldberg 1974] mehrere zur selben Misstrauenspartei gehörende logische S-Knoten auf einem gemeinsamen Computersystem betrieben werden. Dabei wird mithilfe eines als *Virtual Machine Monitor* bezeichneten Programms für jeden S-Knoten eine eigene komplette Rechnerumgebung simuliert, die sogenannte *Virtual Machine*. In einer *Virtual Machine* können Betriebssysteme und Anwendungsprogramme installiert, gestartet und genutzt werden, ohne dass sie extra angepasst werden müssen. Die *Virtual Machine* präsentiert sich darin laufender Software wie ein eigenständiges physisches Computersystem, das exklusiv zur Verfügung steht. Die Verantwortung dafür, dass sich mehrere gleichzeitig laufende *Virtual Machines* nicht in die Quere kommen und dass ihnen die notwendigen physischen Ressourcen zur Verfügung gestellt werden, liegt beim *Virtual Machine Monitor*. Auch private Cloud-Systeme könnten für den Betrieb virtueller S-Knoten genutzt werden, bei denen die Virtualisierungslösung verteilt über mehrere physische Computersysteme betrieben wird.

Für das S-Netzwerk sollen die S-Betreiber die freie Wahl zwischen eigenständigen physischen Umsetzungen und Virtualisierungslösungen für ihre S-Knoten haben. Beide Lösungsansätze werden im Folgenden speziell aus ökologischer Perspektive miteinander verglichen und es werden pragmatische Maßgaben für die S-Verfassung vorgeschlagen.

MÖGLICHE VORTEILE DER EIGENSTÄNDIGKEIT

Wenn jeder logische S-Knoten auf einem eigenen physischen Computer betrieben wird, so hat dies neben der einfacheren Software-Architektur und der stringenter Struktur der eins zu eins Entsprechung auch eine ganze Reihe von praktischen Vorteilen, die teilweise auch sicherheitsrelevant sein können:

Der Entwicklungsaufwand wird gegenüber Virtualisierungslösungen reduziert, es wird keine Virtualisierungsumgebung mit *Virtual Machine Monitor* und *Virtual Machine* benötigt. Es kann im Vergleich zur Architektur der Virtualisierungslösung auf zwei komplette Schichten verzichtet werden. Dadurch werden potenzielle Fehlerquellen ausgeschlossen.

In der Praxis sind *Virtual Machines* nicht vollkommen in sich geschlossen und sauber voneinander sowie vom *Virtual Machine Monitor* getrennt [Ferrie 2007]. Gelingt ein „Ausbruch“ aus einer *Virtual Machine*, so kann sich die Kompromittierung eines einzelnen darin laufenden S-Knotens auf sämtliche S-Knoten, die in anderen *Virtual Machines* desselben *Virtual Machine Monitors* laufen, ausbreiten. Ein Beispiel für eine derartige Attacke, welche eine Schwachstelle in VMWare nutzte, findet sich in [Shelton 2005]. Eigenständige physische Realisierungen der logischen S-Knoten haben dieses Risiko nicht, was als ein klarer konzeptioneller Sicherheitsvorteil zu werten ist.

Je nachdem, wie die einzelnen gegenständlichen Rechner räumlich verteilt sind, kann die eigenständige physische Umsetzung der logischen S-Knoten auch eine gegenüber Virtualisierungslösungen bessere Ausfallsicherheit bei lokal begrenzten physischen Ereignissen wie Naturkatastrophen bieten: Wird beispielsweise ein Serverraum zerstört, in dem nur ein einziger physischer Server mit genau einem logischen S-Knoten betrieben wird, so fällt auch nur dieses eine logische System vorübergehend aus, bis es repariert oder ersetzt werden kann, während alle anderen logischen S-Knoten weiterhin verfügbar sein können.

Virtualisierungslösungen, bei denen mehrere logische S-Knoten auf nur einem einzigen physischen Computersystem betrieben werden, bieten eine solche Stabilität nicht: Der Ausfall des einzigen physischen Rechners wird dann auch sämtliche darauf laufenden logischen S-Knoten gleichzeitig betreffen. Verteilt betrieben Virtualisierungslösungen (private Cloud) können hingegen sogar eine erhöhte Ausfallsicherheit bieten. Andererseits vergrößert sich dadurch die Komplexität und somit die potenzielle Angriffsfläche.

Beim S-Netzwerk soll jeder Teilnehmer die Möglichkeit erhalten, selbst S-Betreiber zu werden. Für jene, welche den damit verbundenen Aufwand und die erhöhte Verantwortung auf sich nehmen, weil sie keinem anderen S-Betreiber vertrauen wollen oder können, soll es auf jeden Fall möglich sein, nur einen, nämlich genau den eigenen logischen S-Knoten selbst zu betreiben. Wenn ein S-Betreiber nur für einen einzigen S-Knoten zuständig ist und dafür einen eigenständigen physischen Computer bereitstellt, bringt es nichts, darauf eine Virtualisierungsumgebung einzusetzen. Virtualisierungslösungen sind überhaupt nur für jene S-Betreiber interessant, welche mehrere S-Knoten zu betreuen haben.

Bei dem Ansatz der Umsetzung von logischen S-Knoten auf eigenständigen physischen Computern steht jeweils die gesamte Rechenleistung und Speicherkapazität des physischen Systems garantiert und jederzeit exklusiv dem einen darauf laufenden logischen S-Knoten zur Verfügung. Insbesondere bei einer gleichmäßig über alle S-Knoten verteilten intensiven Nutzung des S-Netzwerks verspricht dieser Ansatz eine gute Performance.

Bei der Virtualisierung müssen sich hingegen nicht nur mehrere logische S-Knoten einen gemeinsamen physischen Server teilen, sondern auch die Virtualisierungsumgebung selbst benötigt bereits Ressourcen.

Anders als in der Software-Emulation werden zwar bei der vollen Virtualisierung viele Operationen und Anweisungen tatsächlich native auf der realen Hardware ausgeführt [Goldberg 1974] und nicht in Software nachgebildet, was erhebliche Performancevorteile gegenüber der Software-Emulation bringen kann. Außerdem unterstützen aktuelle Prozessoren die Virtualisierung mit speziellen Erweiterungen [Fisher-Ogden 2006], um die Performanceverluste durch die Virtualisierung gering zu halten. Dies zeigt jedoch nicht immer den gewünschten Effekt und je nach Anwendung ist ein System in einer *Virtual Machine* Umgebung selbst mit spezieller Hardware-Beschleunigung nach wie vor langsamer als ein direkt auf der physischen Hardware laufendes System [Adams 2006]. Eine Lösung mit Virtualisierung muss bei gleichmäßig verteilter, konstant hoher Auslastung der logischen S-Knoten entsprechend mehr Rechenleistung aufbieten, um den Performanceverlust durch die Virtualisierung zu kompensieren, was Ressourcen und Energie kostet.

MÖGLICHE VORTEILE DER VIRTUALISIERUNG

Bei einer nicht gleichmäßig hohen Verteilung der Lasten ergibt sich bezüglich Performance und Effizienz ein anderes Bild, eventuell mit erheblichen Vorteilen für Virtualisierungslösungen:

Wenn die Lasten auf den einzelnen logischen S-Knoten starken Schwankungen unterliegen und wenn sie die überwiegende Zeit deutlich unter den zu erwartenden Maximalwerten bleiben, so muss ein eigenständiges physisches Computersystem, auf dem nur ein einziger logischer S-Knoten betrieben wird, genügend Rechenleistung, Speicher und Bandbreite für die eher seltenen Lastspitzen bereithalten, während die meiste Zeit nur ein kleiner Bruchteil der bereitgestellten Kapazitäten benötigt und genutzt wird. Aufgrund des Herstellungsaufwands für die meist ungenutzten Leistungsreserven ist dies ökologisch unvorteilhaft. Außerdem ist auch die Energieeffizienz des Betriebs bei überwiegend niedriger Auslastung je nach Hardware trotz eventuell vorhandener Energiesparfunktionen deutlich geringer als bei voller Auslastung, wie etwa die in [Hsu 2011] veröffentlichte Studie zeigt.

Laufen hingegen mehrere logische S-Knoten mittels Virtualisierung auf einem einzigen physischen Computersystem, so können sich die Schwankungen der Lasten an den einzelnen S-Knoten ausgleichen, sodass eine sehr viel weniger stark schwankende Gesamtlast über alle S-Knoten in der Virtualisierungsumgebung zu verzeichnen ist. Insbesondere kann es sehr unwahrscheinlich werden, dass jemals alle im selben *Virtual Machine Monitor* laufenden logischen S-Knoten gleichzeitig die höchste Leistung erbringen müssen.

Das physische System, auf dem die Virtualisierung läuft, muss dann nicht notwendigerweise Kapazitäten bereithalten, um die theoretische Maximallast, die sich aus der Summe der zu erwartenden Maximallasten an allen darauf laufenden S-Knoten ergibt, bewältigen können. Es wird folglich absolut betrachtet für die gleiche Anzahl von logischen S-Knoten bei Virtualisierungslösungen weniger Rechenleistung, Speicherplatz und Transferleistung benötigt als bei Lösungen mit physisch eigenständigen eins zu eins Umsetzungen der S-Knoten. Gleichzeitig wird eine homogene und relativ hohe Auslastung der Hardwarekapazitäten begünstigt. Die Virtualisierung von mehreren S-Knoten in einem *Virtual Machine Monitor* kann daher bei entsprechend schwankender Lastverteilung auf einzelnen S-Knoten deutlich bessere ökologische Eigenschaften erzielen als die physische Eigenständigkeit von S-Knoten.

Virtuelle Server bieten gegenüber physisch eigenständigen Servern bei einer für Letztere typischen Auslastung von durchschnittlich unter 10% ihrer Kapazität ein erhebliches direktes Energiesparpotenzial in der Größenordnung von gegenwärtig 89% [Talaber 2009]. Da einzelne S-Knoten ähnliche Aufgaben auszuführen haben wie typische Server mit Datenbankdiensten, sind derartige Lasten auch für S-Knoten zu erwarten. Die Umsetzung von S-Knoten in Virtualisierungsumgebungen bietet demnach ein vergleichbares Energiesparpotenzial. Aus ökologischer Sicht dürften Virtualisierungslösungen also erhebliche Vorteile bringen.

Ein Computersystem, auf dem eine Virtualisierungsumgebung mit Dutzenden logischen S-Knoten laufen soll, wird sinnvollerweise erheblich leistungsstärker dimensioniert werden als ein System, auf dem nur ein einzelner logischer S-Knoten betrieben werden muss. Dies kann dazu führen, dass einzelnen logischen S-Knoten in der Virtualisierungslösung bei besonderem Bedarf – je nach zeitgleicher Auslastung der anderen S-Knoten in derselben Virtualisierungsumgebung – deutlich mehr Kapazitäten zur Verfügung gestellt werden können. Durch die flexible Zuteilung der gemeinsamen Ressourcen mehrerer S-Knoten in der gleichen Virtualisierungsumgebung kann die Performance einer Virtualisierungslösung besser sein als bei Lösungen mit einer physisch eigenständigen eins zu eins Umsetzung der logischen S-Knoten, obwohl die Virtualisierungslösung insgesamt weniger Rechenleistung, Speicherplatz und Transferleistung bereitstellt und obwohl die Virtualisierungstechnik an sich Leistung kostet.

VERTEILUNG ZWISCHEN S-KNOTEN IN EINER MISSTRAUENSAPARTEI

Zur sicheren Aufbewahrung der im S-Netzwerk gespeicherten Daten müssen Sicherungskopien nach den Regeln der S-Verfassung auf S-Knoten in verschiedenen Misstrauensparteien aufgeteilt werden.

Aus dem sicherheitskritischen Regelwerk ergibt sich jedoch nur, in welche Misstrauensparteien eine Kopie zu gelangen hat oder von welchen Misstrauensparteien Bestätigungen für die Korrektheit von Daten einzufordern sind. Es wird aber nicht festgelegt, welcher S-Knoten innerhalb von einer ausgewählten Misstrauenspartei die Sicherungskopie erhalten, pflegen und verfügbar halten soll.

Für die Datensicherheit und für den Zugriffsschutz spielt es im Konzept des S-Netzwerks keine Rolle, welcher S-Knoten in ein und derselben Misstrauenspartei eine Kopie speichert. Die S-Knoten in einer Misstrauenspartei sind gleichberechtigt.

Wenn jede Sicherungskopie in einer bestimmten Misstrauenspartei einfach auf einem beliebigen S-Knoten gespeichert würde, könnte dies eine sehr inhomogene Verteilung zur Folge haben. Einige S-Knoten müssten eventuell sehr viele Sicherungskopien und große Datenmengen speichern, auf die vielleicht auch noch besonders häufig zugegriffen wird. Andere S-Knoten würden hingegen nur geringe Datenmengen zu speichern haben und kaum genutzt werden. Gerade wenn S-Knoten alleine auf eigenen physischen Systemen betrieben werden, müssten Systeme für stark genutzte S-Knoten mit großem Datenbestand, entsprechend leistungsstark dimensioniert werden. Auf Systemen, auf welchen nur wenig genutzte S-Knoten betrieben werden, würden zugleich eventuell bestehende Speicherkapazitäten und vorhandene Rechenleistung nicht ausgereizt.

Durch die unausgeglichene Verteilung von Sicherungskopien innerhalb von Misstrauensparteien könnte es vorkommen, dass die Speicherkapazität einzelner Systeme bereits voll ausgeschöpft wird und durch die Bereitstellung zusätzlicher physischer Speicher erweitert werden müsste, während andere Systeme in derselben Misstrauenspartei noch über große freie Kapazitäten verfügen. Wenn das S-Netzwerk über riesige Mengen ungenutzten Speicherplatz verfügen würde und dennoch einzelne Systeme erweitert werden müssten, so wäre das verschwenderisch und ökologisch gesehen unverantwortlich.

Diese Problematik betrifft besonders physische Systeme, auf welchen exklusiv nur ein einziger logischer S-Knoten läuft. Ob die logischen S-Knoten in ein und derselben Virtualisierungsumgebung hingegen untereinander bezüglich ihrer Nutzung ausbalanciert sind, macht keinen Unterschied, schließlich werden der vorhandene Speicherplatz und die bestehende Rechenkapazität ohnehin untereinander geteilt. Aber es könnte auch zu unausgeprägten Lastverteilungen zwischen verschiedenen Großrechnern mit Virtualisierungsumgebungen kommen.

Um inhomogene Verteilungen zu vermeiden, könnte die Auswahl eines S-Knotens zum Speichern einer Sicherungskopie anhand von bestehenden Auslastungen und von freien physischen Kapazitäten durchgeführt werden. Dazu müssten die S-Knoten einer Misstrauenspartei untereinander beziehungsweise an sichere Zugangssysteme ihre Speicherbelegungen kommunizieren können. Derartige zusätzliche Funktionalität ist sicherheitstechnisch nicht optimal. Die ökologischen und auch ökonomischen Vorteile rechtfertigen jedoch vermutlich ein solches Feature.

Die Zentralität eines Großrechners, auf dem viele virtuellen S-Knoten betrieben werden, kann auch so genutzt werden, dass sich daraus ein ökologischer Vorteil ergibt. Ein Rechenzentrum kann direkt zusammen mit einem effizienten Kraftwerk gebaut werden, sodass keine langen verlustbehafteten Stromleitungen zur Energieversorgung notwendig sind. Außerdem können die notwendigen Spannungen durch einen einzigen, effizienten Wandler für das gesamte System bereitgestellt werden.

Computersysteme produzieren mit ihrem Stromverbrauch in erheblichem Ausmaß Wärmeenergie, was oftmals eine aufwendige Kühlung erforderlich macht. Um die Energie abzuführen und eine Überhitzung zu vermeiden wird die Wärme etwa mittels eines durch Ventilatoren erzeugten Luftzugs in die umgebende Atmosphäre abgeführt, wofür wiederum zusätzliche Energie verbraucht wird.

Bei großen Rechenzentren lohnt es sich eventuell, diese Wärmeenergie wieder intelligent zu nutzen und sie nicht einfach sinnlos an die Atmosphäre blasen. Eine Möglichkeit besteht in der Verwendung von Flüssigkeiten als Kühlmittel. Wasser beispielsweise nimmt die Wärmeenergie effizient auf und ist ein guter Energieträger. Nutzen

lässt sich so erwärmtes Wasser etwa als Fernwärme zur Versorgung von Haushalten im Umkreis.

Für ein physisches Computersystem, das so dimensioniert ist, dass es nur einen einzigen S-Knoten trägt, lohnt sich weder ein eigenes Kraftwerk noch eine gezielte Weiternutzung der Abwärme.

ÖKOLOGISCHE STANDARDS FÜR S-KNOTEN

Die S-Verfassung kann für S-Betreiber verbindliche Vorgaben machen, auf welchen Systemen sie ihre S-Knoten wie zu betreiben haben. Ökologisch betrachtet ist bei der für das S-Netzwerk anzunehmenden ungleichmäßigen Belastung der einzelnen S-Knoten die Virtualisierung vieler S-Knoten auf Großrechnern zu favorisieren. Betreiber von mehr als einer bestimmten Anzahl von S-Knoten können durch die S-Verfassung dazu verpflichtet werden, eine umweltschonende Virtualisierungslösung einzusetzen.

Auf diese Weise bleibt es einzelnen Personen, die niemandem vertrauen wollen und welche sich als S-Betreiber qualifizieren, trotzdem möglich, ihren eigenen S-Knoten auf einem eigenständigen physischen System ohne Virtualisierung zu betreiben.

Die S-Verfassung kann noch weiter gehen und für beide Ansätze jeweils verbindliche Vorgaben etwa zum Stromverbrauch im Verhältnis zur bereitgestellten Leistung machen. Auch zu der Art und Weise, wie der genutzte Strom erzeugt wird, können Regeln festgelegt werden.

Ökologische Standards müssen die sich mit der Zeit ändernden technischen Möglichkeiten berücksichtigen, damit sie tatsächlich wirkungsvoll zu Umweltschutz und Ressourcenschonung beitragen können. Manche Vorgaben können vielleicht im Verhältnis zum aktuellen Stand der Technik gemacht werden, sodass sie automatisch mit dem Fortschritt skalieren. Beispielsweise könnte die minimale Rechenleistung pro Kilowattstunde auf einen gewissen Prozentsatz der effizientesten gegenwärtig verfügbaren Computersysteme festgelegt werden. Die Maßgaben sollten trotzdem regelmäßig überprüft und gegebenenfalls manuell angepasst werden.

2.8 ERGÄNZUNGEN ZUM DEMONSTRATOR

2.8.1 FORMATE FÜR DEN NACHRICHTENAUSTAUSCH

Für den Demonstrator mussten Protokolle für den Datenaustausch mit S-Knoten voll spezifiziert und implementiert werden. Die Protokolle für ein reales S-Netzwerk werden vielleicht anders aussehen, aber die vorläufigen Versionen vermitteln bereits eine Idee vom zu erwartenden Overhead pro Nachricht.

Fehler: Referenz nicht gefunden zeigt die Datenstruktur von Nachrichten im UBF-Format, welche in dem S-Netzwerk-Demonstrator der Einfachheit halber für alle Protokolle verwendet wird:

Länge in Bytes	Anzahl	Datentyp (little-endian)	Bedeutung	Benötigt in den Protokollen:
1	1	Byte	Start Tag	SNA, SNPM, SNPB, SNS
9	1	Byte, Long	S-Adresse Absender	SNA, SNPM, SNPB, SNS
1	1	Byte	Absender Information (sicheres Zugangsgerät / S-Knoten)	SNA, SNPM, SNPB, SNS
9	1	Byte, Long	S-Adresse Adressat	SNA, SNPM, SNPB, SNS
1	1	Byte	Adressat Information (sicheres Zugangsgerät / S-Knoten)	SNA, SNPM, SNPB, SNS
8	1	Long	Zeitangabe	SNA
2	1	Enum (Short)	Aktion	SNA
1	0-1	Byte	Start Vermittler-Liste Tag	SNPM
10	0-2 ³¹	Byte, Byte, Long	Tag + S-Adresse Vermittler	SNPM
1	0-1	Byte	End Vermittler-Liste Tag	SNPM
21	0-1	Byte, Byte-Array, Integer	Tag, IP-Adresse und Portnummer nächstes Ziel	SNPM
1	1	Byte	Cypher Typ	SNPB
1	1	Byte	MAC Typ	SNPB
8	1	Long	Nachricht ID	SNPB
9	0-1	Tag, Long	Tag + Cypher-Key ID / Position	SNPB
9	0-1	Tag, Long	Tag + MAC-Key ID / Position	SNPB
21	0-1	Byte, Byte-Array, Integer	Tag, IP-Adresse und Port-Nummer für Rückmeldung	SNS
1	0-1	Byte	Cypher Typ für direkte Antwort	SNS
1	0-1	Byte	MAC Typ für direkte Antwort	SNS
17-65	0-1	Byte-Array	Tag + Cypher-Key für direkte Antwort	SNS
17-65	0-1	Byte-Array	Tag + MAC-Key für direkte Antwort	SNS
2	1	Enum (Short)	Bedeutung der Nachricht (des Nachrichtenkörpers)	SNA, SNPM, SNPB, SNS
1	0-1	Byte	Tag für den Nachrichtenkörper	SNA, SNPM, SNPB, SNS
8	0-1	Long	Länge Nachrichtenkörper	SNA, SNPM, SNPB, SNS
0-2 ⁶³	0-1	Byte-Array	Nachrichtenkörper	SNA, SNPM, SNPB, SNS
1	1	Byte	End Tag	SNA, SNPM, SNPB, SNS

Tabelle 7: S-Netzwerk-Demonstrator Nachricht in UBF-Codierung

IMPLEMENTIERUNGSDetails zum UBF-Format für den Nachrichtenaustausch

Auch die SNS-Nachrichten des Demonstrators enthalten keine explizite Angabe der Gesamtlänge. Im UBF-Format beginnt jedes Feld variabler Länge bereits mit der Längeninformation für das jeweilige Feld und so ist ein effizientes Auslesen der kompletten Nachricht ohnehin möglich. Dadurch entfällt die Notwendigkeit, zuerst die Länge der gesamten SNS-Nachricht in UBF-Codierung zu bestimmen. Die SNS-Nachricht kann direkt beim Schreiben in das UBF-Format auch über eine TCP/IP-Verbindung gesendet werden, unabhängig davon, wie lang sie ist.

Für ein effizientes direktes Lesen und Schreiben von Daten im UBF-Format bei Netzwerkverbindungen wurde für den S-Netzwerk-Demonstrator extra eine optimierte Netzwerkstrom Klasse implementiert, die im Gegensatz zu der .Net eigenen Netzwerkstrom Klasse ein Caching verwendet und auch ein begrenztes Zurücksetzen der Lese-Position erlaubt.

Alle Nachrichten im Demonstrator verfügen zusätzlich über einige in Fehler: Referenz nicht gefunden nicht aufgeführte Felder, welche nur für die Protokollierung, die grafische Darstellung und die Animation des Nachrichtenflusses verwendet werden.

2.8.2 MÖGLICHE WEITERE ENTWICKLUNG UND NUTZUNG DES DEMONSTRATORS

Der S-Netzwerk-Demonstrator soll weiterentwickelt und am Ende der formgebenden Phase an die Spezifikationen der S-Verfassung angepasst werden, sodass der Demonstrator als Testumgebung für die Entwicklung realistischer Implementierungen von S-Knoten und sicheren Zugangssystemen sowohl in der aufbauenden Phase als auch in der fortlaufenden Phase genutzt werden kann.

Der S-Netzwerk-Demonstrator zeigt, was technisch mit begrenztem Aufwand bereits machbar ist, und er kann auch einen Eindruck davon vermitteln, wie es sein könnte, das S-Netzwerk und das S-Web zu nutzen. Darüber hinaus sind weitere Möglichkeiten zur Nutzung des S-Netzwerk-Demonstrators denkbar. Allerdings ist nicht all das, was vorstellbar erscheint, auch automatisch förderlich für die weitere Entwicklung des S-Netzwerks.

Auf den ersten Blick erscheint etwa die Idee verlockend, die für den S-Netzwerk-Demonstrator geschaffenen Implementierungen von S-Knoten als Code-Basis für die Entwicklung von S-Knoten für ein reales S-Netzwerk zu nutzen. Das ist jedoch aus mehreren Gründen keine gute Idee. Beim Demonstrator ging es darum, mit beschränkten Mitteln Systeme zu erschaffen, die zeigen, wie das S-Netzwerk prinzipiell funktionieren kann. Komfortable, schnelle Entwicklung und experimentelle Flexibilität hatten daher hohe Priorität. Eine Anpassung an das, was für das S-Netzwerk wirklich wichtig ist – Implementierungssicherheit, Robustheit, Minimalität, Performance – wäre mit einem hohen Aufwand verbunden. Ein sauberer Neustart dürfte die bessere Lösung sein. Komponenten für das reale S-Netzwerk müssen eben von Beginn an mit ganz anderen Prioritäten gestaltet und entwickelt werden als der experimentelle Demonstrator.

Außerdem soll es ohnehin viele von Grund auf verschiedene Implementierungen geben, denn heterogene Redundanz bietet immerhin die Chance, dass etwaige Schwachstellen nicht in allen Systemen gleichermaßen vorkommen. Idealerweise sollte jede Misstrauenspartei ihre eigenen Systeme entwickeln. Eine gemeinsame Code-Basis als Ausgangspunkt wäre da kontraproduktiv.

Aus dem S-Netzwerk-Demonstrator kann und soll trotzdem mehr werden als nur eine frühe Studie und Vorführung der Möglichkeiten des S-Netzwerks. Der Demonstrator eignet sich bereits ohne Weiteres als Lern- und Experimentierumgebung. Er kann in dieser Funktion insbesondere in der formlosen initialen Phase und in der formgebenden Phase zur Unterstützung der Entwicklung von den technischen Spezifikationen der S-Verfassung genutzt werden. Neue Ideen können im Demonstrator implementiert und ohne hohen Aufwand erprobt werden. Der S-Netzwerk-Demonstrator ermöglicht es, verschiedene virtuelle S-Netzwerke mit abweichenden Konfigurationen zu testen und die Messergebnisse zu vergleichen.

Für die aufbauende Phase bietet es sich an, den Demonstrator an die dann bereits beschlossenen Standards der S-Verfassung anzupassen, sodass technisch jederzeit komplette virtuelle S-Netzwerke mit genau den Protokollen und sonstigen Vorgaben der S-Verfassung simuliert werden können.

Der Demonstrator soll zu einer Testplattform ausgebaut werden, die es ermöglicht, in virtuellen S-Netzwerken auch Implementierungen von einzelnen Komponenten wie S-Knoten zu testen, welche für den realen Einsatz gedacht sind. Die Verwaltungsprogramme des Demonstrators müssen dazu angepasst werden, damit beispielsweise Bekanntschaften zwischen virtuellen S-Knoten und S-Knoten für den realen Einsatz geschlossen werden können. Der Demonstrator mit seinen virtuellen S-Netzwerken soll durch den Ausbau zur Testplattform und Testumgebung die Möglichkeit bieten, frühzeitig eine Qualitätssicherung zu beginnen (Test-Driven Development), sogar noch bevor für den Praxiseinsatz vorgesehene Implementierungen für Kompatibilitäts- und Integrationstests überhaupt zur Verfügung stehen.

Auch in der fortlaufenden Phase, wenn das S-Netzwerk schon realisiert worden ist, kann es überaus nützlich sein, Neuentwicklungen und Weiterentwicklungen, etwa von Implementierungen von S-Knoten, ohne großen Aufwand in dem kontrollierten Rahmen eines virtuellen S-Netzwerks zu testen. Mit einem virtuellen S-Netzwerk als Testumgebung lassen sich Dinge Testen, welche sich im Zusammenspiel ausschließlich mit anderen für den Praxiseinsatz zulassungsfähigen Komponenten nicht testen ließen. Beispielsweise dürfen real zulassungsfähige S-Knoten keine Funktionalität zur Manipulation oder Beschädigung einer Sicherungskopie bieten. Folglich ließen sich Reaktionen auf Manipulationen oder Fehler gar nicht testen.

Im Zusammenspiel mit nicht zulassungsfähigen virtuellen S-Knoten in einem virtuellen S-Netzwerk bieten sich hingegen Möglichkeiten, unerwünschte Ereignisse zu simulieren. Damit lässt sich z. B. systematisch testen, wie die für eine Zulassung vorgesehenen S-Knoten auf eine Anfrage zur Überprüfung und zur Reparatur reagieren, wenn das Quorum im S-Netzwerk andere Daten für korrekt befindet, ohne dass die Daten auf dem zur Zulassung gedachten S-Knoten manipuliert werden müssen. Die Manipulationen erfolgen ausschließlich auf den virtuellen S-Knoten im Demonstrator. Es braucht zum umfassenden Testen in jedem Fall auch virtuelle S-Netzwerke mit nicht zulassungsfähigen, Manipulationen ermöglichenden Komponenten.

Auch Entwickler von Anwendungsprogrammen und automatisierten Diensten etwa zur Anonymisierung können davon profitieren, ihre Produkte zunächst mit virtuellen S-Netzwerken zu erproben, anstatt das reale S-Netzwerk mit aufwendigen Publikationen und Hinterlegungen ausschließlich zu Testzwecken im Zuge der Entwicklungsarbeit zu überfluten. Tests können dadurch auch immer wieder von genau dem gleichen Datenbestand ausgehend wiederholt werden – in virtuellen S-Netzwerken gibt es keine unleugbare Datenerhaltung.

Es ist naheliegend, den Demonstrator in der fortlaufenden Phase weiterhin als Testplattform zu nutzen. Anders als bei den Implementierungen von S-Knoten oder sicheren Zugangssystemen kann ein und dieselbe Testplattform in allen Misstrauensparteien eingesetzt werden – schließlich müssen alle Systeme den gleichen in der S-Verfassung festgeschriebenen Spezifikationen genügen. Heterogenität der Werkzeuge zur Qualitätssicherung zwischen verschiedenen Misstrauensparteien ist nicht erforderlich. Zusätzlich zum S-Netzwerk-Demonstrator können in beliebiger parteiübergreifender Zusammenarbeit weitere Simulations- und Testumgebungen geschaffen werden und jede dieser Plattformen zur Qualitätssicherung kann in allen Misstrauensparteien gleichermaßen eingesetzt werden. Jede Implementierung von Spezifikationen der S-Verfassung sollte Prüfungen mit allen parteiübergreifend verfügbaren Werkzeugen zur Qualitätssicherung standhalten.

3 ERGÄNZUNGEN ZU DAS S-NETZWERK IN DER WIRTSCHAFT

3.1 WIRTSCHAFTLICHE MÖGLICHKEITEN MIT DEM S-NETZWERK

Mit dem S-Netzwerk und mit der verlässlichen Verlinkung des S-Webs lassen sich einige kritische Geschäftsabläufe neu gestalten, sodass Kosten sowie Zeit gespart werden können und rechtliche Unsicherheiten beseitigt werden können.

3.1.1 FAIRE, VERLÄSSLICHE ZUSAMMENARBEIT

Eine neue Form der verlässlichen Zusammenarbeit wird mit dem S-Netzwerk und dem S-Web ermöglicht. Dadurch können innovative schöpferische Prozesse in losen Gemeinschaften entstehen, bei denen sich trotzdem jederzeit rechtsgültig feststellen lässt, wer welchen Beitrag zu welchem Zeitpunkt geleistet hat und welche rechtlichen Ansprüche sich daraus eventuell ergeben.

Der Einsatz des S-Netzwerks bietet sich über Verwaltungsaufgaben, Kommunikationsaufgaben und Vertragsangelegenheiten hinaus auch im kreativen Bereich an. Für die Zusammenarbeit von beliebigen Teilnehmern kann das S-Netzwerk als geschützter und hoch verfügbarer gemeinsamer Speicherplatz dienen, wobei ganz genau und rechtsverbindlich protokolliert wird, was wann passiert. Damit lässt sich wirksam verhindern, dass andere Personen die eigenen Inhalte als ihr Werk ausgeben: Wird ein Zugriffsschutz mit Secret Sharing verwendet und beginnt der Gültigkeitszeitraum erst kurz nach dem Publikationszeitpunkt, müssen jene, die Ideen und Beiträge anderer fälschlicherweise als ihre eigenen ausgeben wollen, die aufwendigen Sicherheitsmaßnahmen des S-Netzwerks überwinden, um dieselben Informationen mit einem früheren Zeitstempel versehen zu können.

Werden alle Arbeitsschritte einer Kooperation jeweils direkt im S-Netzwerk gespeichert, so gelten für jeden einzelnen Schritt automatisch die Eigenschaften einer reliablen Publikation oder einer sicheren Hinterlegung. Eine derartige Kooperation wird hier fortan als *verlässliche Zusammenarbeit* bezeichnet. Für den S-Netzwerk-Prototyp wurde mit dem *NonNon-Editor* eine Beispiel-Anwendung entwickelt, welche die Möglichkeiten der *verlässlichen Zusammenarbeit* mithilfe des S-Netzwerks demonstrieren soll.

NONNON-EDITOR

Der *NonNon-Editor* (Non-repudiation, Non-destructive Editor) ist ein dynamischer Text-Editor, mit dem mehrere Personen gemeinsam gleichzeitig an ein und demselben Dokument arbeiten können, ähnlich wie dies etwa bei Etherpad [Vollmer 2012] funktioniert. Allerdings benötigt der *NonNon-Editor* keinen speziellen Server. Zunächst wird mit dem *NonNon-Editor* ein (eventuell leeres) Text-Dokument als Wurzel in das S-Netzwerk gestellt, welches dann kollaborativ bearbeitet werden kann. Jede Änderung wird als eigene reliable Publikation oder sichere Hinterlegung ausgeführt und per S-Link mit der unveränderlichen Wurzel verlinkt. Wenn sich eine Änderung nicht direkt auf das Wurzel-Dokument bezieht, sondern auf eine bereits weiter editierte Fassung, so wird ebenfalls per S-Link auf die Letzte der Änderungen verwiesen, welche zuvor durchgeführt werden müssen. Alle Daten werden garantiert unverändert bis zum Ende der Gültigkeitsdauer im S-Netzwerk verfügbar gehalten, sodass immer nachvollziehbar bleibt, wer was zu welchem Zeitpunkt beigesteuert hat und auf welche Fassung sich eine Editierung jeweils bezieht.

Die im S-Netzwerk publizierten oder hinterlegten sowie verlinkten Änderungen werden clientseitig abgerufen und vom *NonNon-Editor* dynamisch in das Wurzel-Dokument

integriert, um die gewünschte Fassung des Dokuments zu generieren. Von der Idee her entspricht dies dem “pounce” des in [Nelson 1980/1990] (Seite 2/16) vorgestellten *nicht sequenziellen Schreibens*. Beim *nicht sequenziellen Schreiben* können verschiedene Bearbeitungsäste entstehen, da sich von jeder beliebigen Fassung ausgehend immer wieder neue alternative Änderungen publizieren lassen.

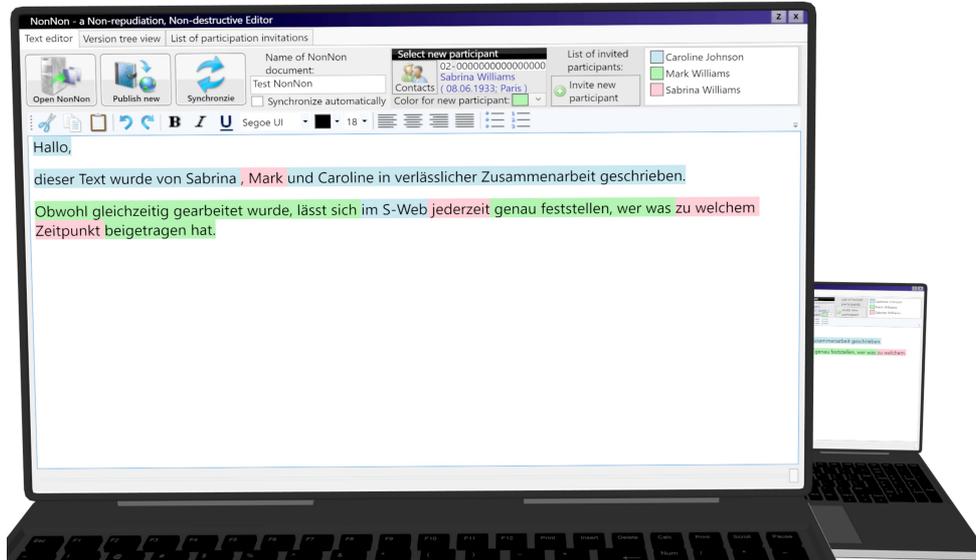


Abbildung 15: Screenshot von mehreren Instanzen des NonNon-Editors im Demonstrator

Im *NonNon-Editor* wird in der Regel mit der jeweils aktuellsten Fassung gearbeitet, und zwar von mehreren Personen gleichzeitig – ohne, dass eine Verästelung in verschiedene alternative Versionen gewünscht wird. Dabei kann es passieren, dass mehrere Personen quasi gleichzeitig Änderungen publizieren, welche sich auf dieselbe Fassung des Dokuments beziehen. In einem solchen Fall stellt der *NonNon-Editor* zunächst fest, ob die Änderungen sich gegenseitig ausschließen, ob also dieselben Elemente im Dokument auf verschiedene Weisen abweichend editiert werden sollen. Im Zweifelsfall werden dazu alle publizierten Änderungen innerhalb eines Toleranzzeitfensters, die sich auf dieselbe Fassung des Dokuments beziehen, in jeder möglichen Reihenfolge ausgeführt. Wenn das Ergebnis unabhängig von der Reihenfolge identisch ist, können alle Änderungen in ein und demselben Dokument durchgeführt werden. Andernfalls liegt eine Kollision vor.

Falls es keine Kollision gibt, so gelten die Änderungen als gleichzeitig ausgeführt. Die neue aktuelle Fassung ergibt sich somit aus der vorherigen Fassung und all diesen gleichzeitig ausgeführten Änderungen gemeinsam. Eine folgende Editierung wird mit allen zuletzt gleichzeitig getätigten Änderungen verlinkt.

Liegt hingegen eine Kollision zwischen verschiedenen Editierungen von ein und derselben Fassung des Dokuments vor, so entsteht zunächst einmal eine Astgabelung: Es gibt fortan mindestens zwei verschiedene alternative Versionen des Dokuments. In diesem Fall werden die Beteiligten gefragt, mit welcher Fassung sie weiterarbeiten möchten. Sie können dies in einem Chat innerhalb des *NonNon-Editors* diskutieren, wobei diese Kommunikation wiederum verlässlich über das S-Web realisiert wird. Einigen sie sich auf eine bestimmte Version, können sie gemeinsam auf dieser aufbauend weiterarbeiten. Wenn hingegen keine Einigung auf eine bestimmte Version zustande kommt, können die Beteiligten jeweils an Versionen ihrer Wahl weiterarbeiten. Die verschiedenen Versionen bleiben dabei über eine Baumansicht des *NonNon-Editors* erreichbar.

Abbildung 16 veranschaulicht die Funktionsweise der Hauptschleife des *NonNon-Editors* mit der Kollisionshandhabung in einem Flussdiagramm.

Ein umfangreiches Dokument mit sehr vielen Änderungen in den *NonNon-Editor* zu laden und die aktuellste Fassung aufzubauen kann lange dauern, schließlich muss jede Änderung einzeln ausgewertet werden. Um dieses Problem zu reduzieren, bietet es sich an, von Zeit zu Zeit eine vollständige aktuelle Fassung des Dokuments als Meilenstein mit allen eingepflegten Änderungen zu publizieren und diese als neue gemeinsame Basis für die weitere Zusammenarbeit zu nutzen. Der korrekte Aufbau des Meilensteins bleibt jederzeit für alle Beteiligten überprüfbar. Es genügt, dies einmal zu überprüfen und fortan nur noch vom letzten Meilenstein auszugehen. Der *NonNon-Editor* unterstützt das automatisierte Anlegen und Nutzen solcher Meilensteine.

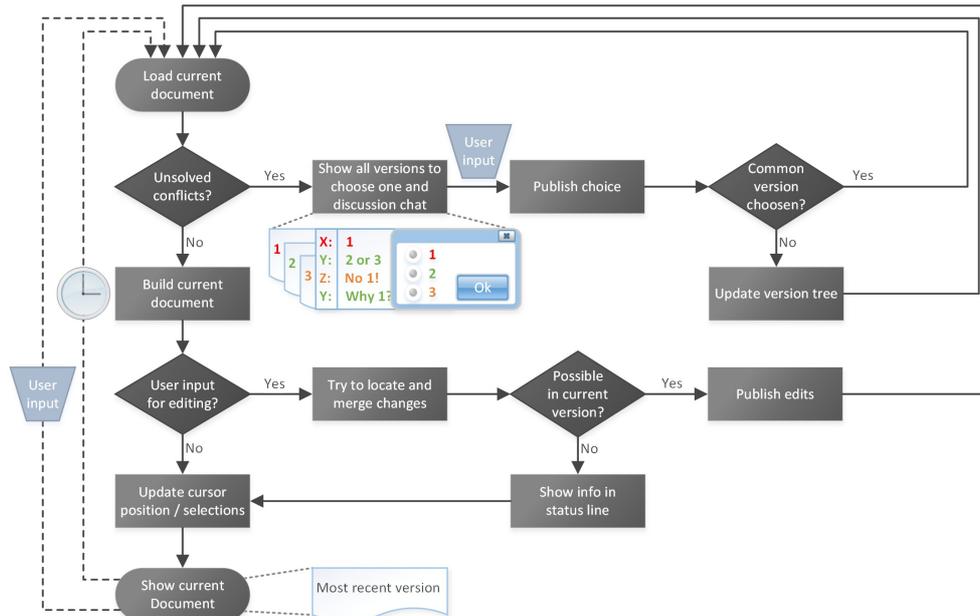


Abbildung 16: Schema der Aktualisierung des *NonNon-Editors* mit Konfliktmanagement

Der *NonNon-Editor* ist insbesondere gedacht, um Brainstormings durchzuführen oder um gemeinsam neue Ideen zu entwickeln. Kein Beteiligter soll sich dabei sorgen müssen, dass jemand anders die eigenen Ideen stehlen könnte, um sie als seine eigenen Ideen auszugeben. Dadurch soll eine neue, offenere Kommunikationskultur ermöglicht werden, in der die heute oft nötige strategische Zurückhaltung der eigenen Einfälle weitgehend überwunden wird. Das S-Netzwerk verhindert jedes Vordatieren des Publikationszeitpunkts. Ohne die diesbezüglichen starken Schutzmaßnahmen des S-Netzwerks technisch zu überwinden, können andere höchstens versuchen, zeitnah quasi den gleichen Gedanken zu publizieren. Wenn die Änderungen am gemeinsamen Dokument sehr hochfrequent publiziert werden, könnte es durchaus passieren, dass andere schon nach wenigen gelesenen Zeichen auf dieselbe Idee kommen und diese eventuell sogar schneller verschriftlichen, ehr auf den Punkt bringen. Um das zu verhindern, kann im *NonNon-Editor* zusätzlich ein Hochsicherheitsmodus aktiviert werden, in dem Änderungen am Dokument zunächst nur für den Herausgeber sichtbar mit hoher Frequenz sicher hinterlegt werden, bis dieser einen Gedanken abgeschlossen hat. Damit wird frühestmöglich belegbar, wann die Idee kam. Erst auf Anweisung des Herausgebers erfolgt jeweils die für andere sichtbare Publikation der ganzen Änderung auf einen Schlag.

3.1.2 DAS S-NETZWERK ALS PATENTREGISTER

Mit dem S-Netzwerk lässt sich sicher dokumentieren, wer zu welchem Zeitpunkt welche Idee hatte. Das Patentrecht könnte für die heikle Feststellung der Neuheit auf die Zeitangaben in reliablen Publikationen oder sicheren Hinterlegungen zurückgreifen und im S-Web könnte ein damit verknüpftes globales Patentregister geschaffen werden.

Ein Patent garantiert zeitlich befristete Schutzrechte zur exklusiven gewerblichen Nutzung von technischen Erzeugnissen, Herstellungs- oder Arbeitsverfahren in seinem Gültigkeitsbereich. Patente werden in Deutschland erteilt, wenn die Erzeugnisse oder Verfahren neu sind, auf einer erfinderischen Tätigkeit beruhen und wenn sie gewerblich nutzbar sind. Neuheit plus erfinderische Tätigkeit bedeutet hier, für einen „durchschnittlichen Fachmann“ in nicht naheliegender Weise über den Stand der Technik hinausgehend ([PatG 1936/2011] §1, §3, §4). Der Zeitpunkt (Priorität), zu dem auf Neuheit zu prüfen ist, wird je nach Patentsystem auf verschiedene Weisen bestimmt:

Das *Erstanmelderprinzip* wird derzeit fast überall in der Welt verwendet, etwa in Deutschland ([PatG 1936/2011] §3, §35). Die Innovation zum Stand der Technik wird dabei zum Anmeldezeitpunkt beim Patentamt geprüft. Der Vorteil ist, dass sich leicht feststellen lässt, wann genau dieser kritische Zeitpunkt ist. Ein Nachteil ist, dass jede Veröffentlichung vor der Anmeldung die Neuheit zerstört. Das gilt auch für den Erfinder selbst: Eigene Publikationen verunmöglichen eine spätere Patentanmeldung [Bagley 2008]. Außerdem ist eine Patentanmeldung mit Kosten verbunden, was für Privatpersonen und kleine Unternehmen eine zu hohe Hürde sein kann [McFadyen 2007].

In den USA wurde bis 2013 das *Ersterfindungsprinzip* genutzt. Ausschlaggebend für die Feststellung der Neuheit war der Zeitpunkt der Erfindung, nicht der Patentanmeldung ([USPA 2007], 35 U.S.C. 102). Der genaue Zeitpunkt der Erfindung ist jedoch schwierig festzustellen. Wurde dieselbe Erfindung zugleich von verschiedenen Parteien beansprucht, so führte dies zu komplizierten rechtlichen Verfahren [Carnathan 1998].

Es gibt gute Gründe für eine globale Vereinheitlichung der Patentsysteme [Willis 2009]. Die USA nutzen daher seit 2013 eine Annäherung an das *Erstanmelderprinzip*, die auch Merkmale des *Ersterfindungsprinzips* enthält. Dazu zählt die *grace period*: So sind in den USA weiterhin eigene Publikationen bis zu einem Jahr vor der Patentanmeldung nicht neuheitsschädigend. Das gilt auch für Publikationen Dritter, welche nach einer eigenen Publikation erfolgen [USCongress 2012]. Da sich nicht immer genau feststellen lässt, wer was wann veröffentlicht hat, sind über die Abfolge wieder rechtliche Auseinandersetzungen zu erwarten. Wie beim *Ersterfindungsprinzip* besteht ferner Rechtsunsicherheit für die Nutzung einer bereits publizierten, noch nicht zum Patent angemeldeten Erfindung, da sie per nachträglicher Patentanmeldung der Allgemeinheit entzogen werden kann.

Mithilfe des S-Netzwerks bietet sich ein neues Prinzip an: Für die Prüfung auf Neuheit könnte auf den Zeitpunkt abgestellt werden, zu dem Erfindungen zuerst im S-Netzwerk reliabel publiziert oder sicher hinterlegt werden. Ideen könnten etwa durch kooperatives Schreiben mit dem *NonNon-Editor* in verlässlicher Zusammenarbeit entwickelt werden, dann wären sie automatisch sofort im S-Netzwerk gesichert. Wissenschaftler könnten so einfach frühstmöglich publizieren – noch während offen an der Erfindung gearbeitet wird – ohne Verluste befürchten zu müssen und ohne sich schon mit den formalen Anforderungen für Patentanmeldungen auseinandersetzen zu müssen. Es würden noch keine Kosten zur Patentanmeldung anfallen. Der Herausgeber Π und der genaue Publikationszeitpunkt T eines jeden Beitrags zur Erfindung könnten rechtsgültig festgestellt werden. Patentanmeldungen könnten bis zu einem Jahr später erfolgen. Um Rechtsunsicherheiten durch spätere Patentanmeldungen zu vermeiden, könnte ferner gefordert werden, dass unmittelbar ein Vorbehalt für eine eventuelle spätere Patentanmeldung publiziert werden muss. Nichts, was ohne entsprechenden Vorbehalt der Allgemeinheit zugänglich gemacht wurde, könnte

im Nachhinein durch ein Patent blockiert werden.

Weiters bietet es sich an, das S-Netzwerk auch als globale Plattform für die Patentanmeldung am Patentamt und für das Patentregister ([PatG 1936/2011] §30) zu verwenden, um diese effizient und verlässlich zu realisieren. Dabei könnte gleich per S-Link auf die *Erstveröffentlichung* verwiesen werden, aus deren Publikationszeitpunkt T sich unmittelbar der Prioritätszeitpunkt ergeben würde.

3.2 PROBLEME IM UMGANG MIT IMMATERIELLEN GÜTERN

Immaterielle Güter sind wirtschaftlich und rechtlich hart umkämpft und dabei gibt es in der Praxis oft nur Verlierer.

ZWEIFELHAFTE EINNAHMEN FÜR DEUTSCHE VERWERTUNGSGESELLSCHAFTEN

Das deutsche Urheberrecht erlaubt gemäß §53 [UrhG 1965/2011] in gewissen Grenzen das Anfertigen von Kopien zum privaten Gebrauch. Als Ausgleich wird in §54 ein Anspruch der Rechteinhaber gegenüber den Herstellern von allen Geräten und Datenträgern konstruiert, mit deren Hilfe eine Vervielfältigung möglich ist. Ein Problem ist dabei, dass es solche Gebühren in vielen Ländern nicht gibt, wodurch der Wettbewerb verzerrt wird [Wilkens 2005]. Die Formulierungen im UrhG sind sehr weitgehend interpretierbar. Es klingt zwar gut, dass „Maßgebend für die Vergütungshöhe ist, in welchem Maß die Geräte und Speichermedien als Typen tatsächlich für Vervielfältigungen nach § 53 Abs. 1 bis 3 genutzt werden“ (zitiert aus §54a [UrhG 1965/2011]). Aber wie sich das Ausmaß der Nutzung für Privatkopien erfassen lassen soll, das steht nicht im Gesetz.

Erhoben werden die Gebühren auf zum Kopieren nutzbare Geräte und Datenträger in Deutschland durch die *Verwertungsgesellschaften*, welche dazu in der *Zentralstelle für private Überspielungsrechte* (ZPÜ) kooperieren. Dadurch, dass die Höhe der Abgaben im UrhG nur durch unzureichend festgelegt ist, kommt es zu Konflikten zwischen der ZPÜ und den Herstellern von betroffenen Geräten und Datenträgern. Ein Streitfall resultierte etwa aus der Erhöhung der Gebühr für Speicherkarten über 4GB zum 1.7.2012 um 1850% durch die ZPÜ [Schnurer 2012]. Begründet wurde die erhöhte Forderung skandalöserweise damit, dass dadurch der Ausfall von zuvor unrechtmäßig kassierten Gebühren kompensieren werden soll:

„Die gesamtvertraglich vereinbarte Vergütung betrug für sämtliche in Deutschland in den Verkehr gebrachten USB-Sticks und Speicherkarten 0,10 EUR pro Stück und galt“ ... „unabhängig vom konkreten Einsatzzweck. Beispielsweise waren von der vertraglichen Vereinbarung auch Speicherkarten erfasst, die in Fotokameras eingesetzt wurden.“ ... „Diese pauschalierende Vorgehensweise konnte nach den in den Jahren 2010 und 2011 ergangenen Entscheidungen des Europäischen Gerichtshofs nicht mehr beibehalten werden.“ ...

„Die Verwertungsgesellschaften und die Verbände haben noch in 2011 Verhandlungen über den Abschluss eines neuen Gesamtvertrages für USB-Sticks und Speicherkarten aufgenommen. Diese Verhandlungen wurden im Februar 2012 für gescheitert erklärt, da die Verbände nicht bereit waren, den geänderten rechtlichen Rahmenbedingungen Rechnung zu tragen und bei einer etwa verkleinerten Bemessungsgrundlage eine höhere Vergütung pro Stück zu akzeptieren.“, zitiert aus [GEMA 2012].

Obwohl für Kopiergeräte bereits eine pauschale Abgabe kassiert wird, werden für Kopien zusätzliche Zahlungen verlangt, so z. B. VG Musikedition durch die GEMA für die Vervielfältigung von Noten in Kindergärten [Jessen 2010] [Mühlbauer 2010]. Kitas müssen demnach nicht nur Gebühren zahlen, sondern auch den Verwaltungsaufwand stemmen, welcher durch die Pflicht zur Dokumentation der Kopien entsteht. Da Kindergartenkinder in der Regel weder Noten noch Texte selbstständig lesen können und die Kopien nur dem Singen zusammen mit den Eltern dienen, verzichten manche Kindergärten in Konsequenz auf die Verteilung von Kopien [Daller 2010], oder sie weichen auf alte, inzwischen gemeinfreie Noten und Texte aus [Ernst 2011] – was nicht im Sinne der lebenden Künstler sein kann, deren Interessen die *Verwertungsgesellschaften* vertreten sollten.

Abhilfe sollen nach dem Willen der *Verwertungsgesellschaften* und einiger Politiker Pauschalverträge schaffen [Mühlbauer 2011]. Für die Kindergärten in Bayern wurde bereits ein pauschaler Preis von 290.000 € pro Jahr vereinbart, wofür die Steuerzahler aufkommen müssen [Drescher 2011]. Auch wenn die *Verwertungsgesellschaften* mit solchen Maß-

nahmen kurzfristig mehr Einnahmen erzielen können: Die verbreitete Empörung [Görlach 2010] über die Forderungen an Kindergärten könnte die Bereitschaft zur korrekten Meldung und Zahlung an die *Verwertungsgesellschaften* nachhaltig beeinträchtigen. Es handelt sich also wohlmöglich um einen Pyrrhussieg.

DIE VIELEN KÄMPFE DER GEMA

Die GEMA erfährt Widerstand nicht nur in Form von massiver Kritik, Kampagnen und in diversen juristischen Auseinandersetzungen, sondern auch durch Angriffe von Hackern, denen sie regelmäßig ausgesetzt ist. Im Juni 2011 wurde beispielsweise die GEMA-Homepage durch eine Distributed Denial of Service (DDoS) Attacke lahmgelegt [Reißmann 2011 2]. Ein aufsehenerregender Angriff erfolgte im August 2011. Dabei wurde ein schwaches Passwort genutzt, um Kontrolle über Server der GEMA zu gelangen. Es wurden sensible Daten heruntergeladen und es

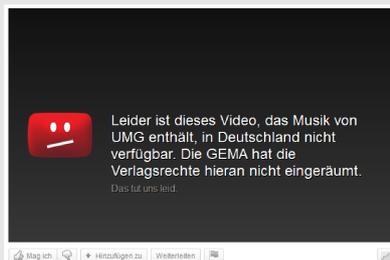


Abbildung 17: Youtube Sperre (Screenshot von Johannes Viehmann)

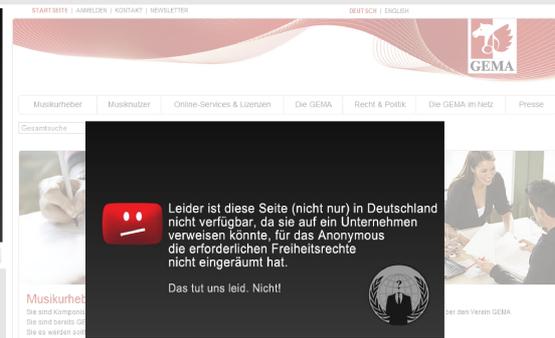


Abbildung 18: Umleitungsziel der GEMA-Seite nach dem Angriff (Screenshot von Johannes Viehmann)

wurde eine Umleitung auf eine Seite eingerichtet, welche die GEMA verspottet [Sobiraj 2011].

Im Dezember 2011 gab es eine DDoS Attacke auf die GEMA-Server, wobei Internetnutzer zum Besuch einer Seite aufgefordert wurden, von welcher Scripte für den Angriff abgerufen und ohne Zutun auf dem Rechner der Nutzer ausgeführt wurden. Obwohl diese sehr einfach gemachte Attacke nur geringe Auswirkungen hatte, folgte Monate später eine groß angelegte Polizeiaktion gegen die am Angriff beteiligten Personen mit über hundert Hausdurchsuchungen und Beschlagnahmungen von Computern [Hochert 2012]. Zwar besteht rechtlich mit §303b [StGB 1871/2012] durchaus eine Norm, mit der nach Auffassung der Literatur [Ferner 2010] und nach der praktischen Rechtsprechung DDoS Attacken verfolgt werden können. Allerdings scheint in diesem Fall weder die Verhältnismäßigkeit gewahrt zu sein, noch werden die Drahtzieher damit getroffen. Für das Image und die Akzeptanz der GEMA war die Aktion wohl wiederum kein Gewinn.

DIE FILTER FALLE

Rechteinhaber an immateriellen Gütern und deren Vertreter wie *Verwertungsgesellschaften* fordern von Plattformen wie Youtube, dass die Betreiber die von Anwendern widerrechtlich dort platzierte urheberrechtlich geschützte Inhalte aufspüren und unzugänglich machen. Bei großen Portalen ist dies nur mit dem Einsatz von automatischen Filtern praktikabel. Solche Filter können sowohl über den Inhalt der Videos als auch über beschreibende Wörter arbeiten.

In Deutschland wird bisweilen beides verlangt [LG Hamburg 2012] – obwohl dies umstritten ist [Briegleb 2012]. Speziell bei Filtern über beschreibende Wörter besteht die Schwierigkeit, unterscheiden zu müssen, ob nun tatsächlich auch das geschützte Werk im Video in unzulässiger Weise vorkommt. Eventuelle handelt es sich beispielsweise nur um eine zulässige Rezension zu dem Werk [Kuhn 2012].

Welche Inhalte tatsächlich gegen das Urheberrecht verstoßen, das lässt sich oftmals nicht leicht feststellen. Dies gilt speziell für Werke, in die mehrere urheberrechtlich geschützte Inhalte von verschiedenen Rechteinhabern einfließen. Wenn ein komplett mit *Crowdfunding* zu finanzierendes Werk zur freien Verfügung gestellt werden soll, so können

etwaig darin enthaltene urheberrechtlich geschützte Inhalte von Dritten entsprechend lizenziert werden. Gemeint sind Lizenzen, die den Rechteinhabern (einmalig) Vergütungen in für diese angemessener Höhe gewähren, wofür die Rechteinhaber auf weitere Ansprüche für die freie Weitergabe des neuen Werkes verzichten. Die Vergütung wird mit den *Crowdfunding* Einnahmen finanziert. Dies wurde beispielsweise bei dem Film *Sita Sings the Blues* für die Musik gemacht. Die darin enthaltenen Musikstücke sind dann nur für ihre Verwendung in dem gratis verfügbaren Film ohne weitere Kosten lizenziert.

Auf Plattformen wie YouTube spüren Filter für urheberrechtlich geschützte Inhalte eventuell auch solche Werke auf, für die bereits eine angemessene Vergütung an die Rechteinhaber gezahlt wurde. Im Fall von *Sita Sings the Blues* ist genau das passiert: Google hat das YouTube-Video für Deutschland sperren lassen, da hier keine Vereinbarung mit der für die Musikrechte zuständigen *Verwertungsgesellschaft* GEMA bestand. Wie sollte Google feststellen können, dass die Verwendung der Musik in diesem Film durch einen speziellen Lizenzvertrag freigestellt wurde?



Abbildung 19: Protestvideo von Nina Paley gegen die Sperrung ihres Films auf Youtube in Deutschland, Screenshots von <http://www.youtube.com/watch?v=LpTPTQ3e0Jg> (2012-06-26)

Als die Urheberin Nina Paley bei einem Besuch in Deutschland die Sperrung entdeckte, reagierte sie mit einem Protestvideo. Auf ihre Beschwerde hin wurde der Film wieder freigeschaltet. Nichtsdestotrotz hat die zeitweilige Sperrung die Verbreitung des Films behindert und es war Zufall, dass sie überhaupt entdeckt wurde und in Folge behoben werden konnte.

Mit dem S-Netzwerk wäre es immerhin möglich, erworbene Lizenzen von den Rechteinhabern als reliable Publikationen im S-Netzwerk im S-Netzwerk publizieren zu lassen. Bei geeigneter verlässlicher Verlinkung könnten automatische Filter überprüfen, ob für urheberrechtlich geschützte Werke die erforderlichen Rechte eingeholt wurden. Für wortbasierte Filter und die Problematik etwa mit Rezensionen böte aber auch das S-Netzwerk keine vernünftige Lösungsmöglichkeit.

Filter, die vorab prüfen, ob Inhalte zulässig sind, sind beim S-Netzwerk nicht vorgesehen, denn sie würden eine unkontrollierbare Vorzensur ermöglichen.

EINE ZUKUNFT OHNE PROFESSIONELLE SCHÖPFER IMMATERIELLER GÜTER

Wenn mit einer Plattform wie dem S-Netzwerk jeder seine eigenen Ideen und Werke erschaffen und publizieren kann, stellt sich auch die Frage, ob es professionelle Vollzeit-Schöpfer *immaterieller Güter* überhaupt braucht. Durch die Möglichkeiten des Internets erhalten Profis bereits zunehmend Konkurrenz von Amateuren [Bernard 2012].

Dass Urheber und Erfinder von ihren Werken leben können müssen, um kreative Höchstleistungen vollbringen zu können, wird vielfach propagiert [Fritzsche 2012] [Meißner 2012]. Allerdings war etwa William Shakespeare kein professioneller Vollzeit-Autor, sondern er war zugleich auch Theaterunternehmer und Schauspieler ([Schabert 1972], S. 153-156), was zu seinen Lebzeiten einträglicher war (vgl. [Schabert 1972], S. 150). Noch bis ins frühe 18. Jahrhundert hinein gab es den Beruf eines freien Schriftstellers nicht, denn ein Autor konnte „noch nicht auf eine angemessene Honorierung durch den Buchhandel hoffen. Er benötigte deshalb einen einträglichen Hauptberuf“ (zitiert aus [Wittmann 1991], S. 143). Entstehen konnte der Beruf des Autors, der für die Massen schreibt, erst mit dem Buchdruck und der Verbreitung der Fähigkeit zu lesen.

“Scribal culture could have neither authors nor publics such as were created by typography”, zitiert aus [McLuhan 1962/1967], S. 130.

Die Schriftsteller des Sturm und Drang und der Weimarer Klassik verdienten bereits an ihrem Schaffen [Engelsing 1976], aber ein Johann Wolfgang von Goethe war z. B. trotzdem ab 1776 auch Berufspolitiker [Rothe 1998] und ab 1791 bis 1817 Leiter des Hoftheaters Weimar [Lederer 1936]. Obwohl sie nicht nur von dem lebten, was sie für ihre Werke von ihren Gönnern und Verlegern bekamen, sondern zusätzlich als Solisten sowie Kapellmeister aktiv waren sowie SchülerInnen bzw. StudentInnen unterrichteten, um Geld zu verdienen, konnten Komponisten wie Johann Sebastian Bach [Gimpel 2009], Ludwig van Beethoven [Skowroneck 2010] [Thayer 1866-1917], Franz Liszt [Hilmes 2011] [Keiler 1986] oder Gustav Mahler [Schaberth 1969] ihre großen Werke erschaffen.

Die These, dass Schöpfer immaterieller Güter von dieser Tätigkeit ihren Lebensunterhalt bestreiten können müssen, ist damit kaum haltbar. Streitbar scheint nicht erst die Höhe einer *angemessenen Vergütung*. Eventuell braucht es gar keinen materiellen Anreiz, weil die schöpferische Tätigkeit zusätzlich zum anderweitig zu bestreitenden Broterwerb an sich attraktiv genug ist. Vielleicht geht das wirklich Geniale aus einem nicht kontrollierbaren inneren Antrieb hervor:

„Der Kunsthandwerker kann.“ ... „Aber der Künstler muß. Er hat keinen Einfluß darauf, von seinem Willen hängt es nicht ab.“, zitiert aus [Schönberg 1910].

Selbst falls dem so sein sollte, falls das Immaterialgüterrecht abgeschafft würde und künftig nur Amateure immaterielle Güter schaffen sollten, würde das nicht bedeuten, dass die Erzeugung dieser Güter nicht finanziert werden müsste. Denn die Erschaffung von *immateriellen Gütern* kann sogar ohne jede Vergütung für die Arbeitsleistung der Schöpfer mit erheblichen Kosten (z. B. für Energie, gegenständliche Ressourcen) verbunden sein. Bezahlte Profis könnten wohlmöglich durch ehrenamtlichen Einsatz verzichtbar sein. Geeignete Finanzierungskonzepte werden hingegen für gewisse Projekte aufgrund der Sachkosten zweifelsfrei weiterhin benötigt, auch wenn sie von Amateuren unentgeltlich umgesetzt werden.

3.3 ENTWICKLUNG VON WIRTSCHAFTSSYSTEMEN

Bezugsmittel, Transaktionssysteme sowie darauf aufbauende Wirtschaftsformen wurden und werden durch mehr oder weniger technische Innovationen in Kombination mit bisweilen schmerzhaften Lernprozessen anhand praktischer Erfahrungen geprägt.

3.3.1 VOM NATURALGELD BIS ZUM ZEICHENGELD

Ein Blick in die Vergangenheit zeigt, dass sich verschiedenste Güter als geldartiges allgemeines Bezugsmittel nutzen lassen, ohne dass es einer Finanzhoheit mit Monopol auf die Geldschöpfung bedarf, wobei mit dem Zeichengeld sogar der Abstraktionsschritt zu einem außerhalb der Geldfunktion quasi nutzlosen Bezugsmittel gelang.

Sich auf ein *allgemeines Bezugsmittel* zu einigen, erleichtert den Handel ungemein. Die schwierige Entscheidung, was genau dieses *allgemeine Bezugsmittel* sein soll, hat weitreichende Konsequenzen. Im Laufe der Geschichte wurden zum Beispiel Getreide [Preisigke 1910/1971] oder Salz ([Schleiden 1875/2012] S. 68ff) als *allgemeines Bezugsmaß* und als *Tauschmittel* verwendet. Diese Güter bieten sich dazu an, weil sie feinkörnig vorliegen und entsprechend klein unterteilte Wertverhältnisse verkörpern können. Schlechter eignet sich beispielsweise lebendes Vieh, mit dem sich nur gröber, ungenauer handeln lässt und dessen Haltung sowie Tausch mit hohem Aufwand verbunden sind. Bei *Naturalgeld* handelt es sich generell um in der Natur vorkommende, nicht wesentlich weiterbearbeitete Nutzgüter oder auch um Lebewesen, die in der Regel allgemein begehrt werden und die zwar selten, aber für den Handel in ausreichenden Mengen verfügbar sind.

Das *Naturalgeld* hat auch unabhängig von der Geldfunktion einen konkreten Nutzen: Die beispielhaft erwähnten Güter dienen Menschen unter anderem auch als Nahrung. Durch die Verwendung als *Naturalgeld* erhöht sich der Wert des Gutes, weil es zusätzlich auch als *allgemeines Bezugsmittel* begehrt wird und mithin eine erhöhte Nachfrage zu erwarten ist.

Idealerweise sollte das *Naturalgeld* leicht zu transportieren und vor allem problemlos zu lagern (bzw. zu halten) sein, damit es auch gespart werden kann. Letzteres ist Voraussetzung, um auch große Investitionen auf einmal tätigen zu können.

SCHNECKENWÄHRUNG

Ein in Südostasien, Ozeanien und Afrika weitverbreitetes Naturalgeld war die Schale der Kaurischnecke [Schilder 1952/2008]. Diese Schalen lassen sich beispielsweise zu Schmuck verarbeiten. Sie sind relativ leicht, haltbar und sie lassen sich damit auch gut horten.

Schneckengeld war nicht auf die Vor- und Frühgeschichte beschränkt, in Teilen Neuguineas hat diese Währung sich beispielsweise bis in die 1960er Jahre erhalten.

„In Tahiti begann ich meine unmittelbaren Vorbereitungen für die Expedition ins Innere Neuguineas. Ich sammelte Kauri-Schnecken.“ ... „normalerweise geht man“ ... „zu einer Bank, um Geld zu tauschen. Aber die Währung der Dani wird an keiner Bank der Erde notiert – man muß sie sammeln“, zitiert aus [Harrer 1965].

Erst in den letzten 50 Jahren wurde die Kaurimuschel weitgehend aus der Geldfunktion verdrängt ([Voirol 2011], S. 84).

Vom heute üblichen Zahlungsmittel unterscheidet sich *Naturalgeld* insbesondere dadurch, dass es einfach in der Natur gefunden werden kann.

Anders ist das bei *Gerätegeld* oder *Warengeld*, das zunächst hergestellt werden muss. Im Laufe der Zeit wurden beispielsweise Schmuck oder Werkzeuge (etwa Sichel, siehe [Sommerfeld 1994]) als *Gerätegeld* verwendet. In Deutschland wurde unmittelbar nach dem verlorenen Zweiten Weltkrieg neben direktem Tausch bekanntermaßen auch auf

Zigaretten als Notgeld zurückgegriffen ([Oppermann 2010], S. 35).

Die als *Warengeld* oder *Gerätegeld* verwendeten Objekte haben wiederum unabhängig von ihrer Verwendung und Akzeptanz als *allgemeines Bezugsmittel* einen konkreten Nutzen, durch den sich ein Wert jenseits der Geldfunktion ergibt. Dieser Wert wird, wie auch beim *Naturalgeld*, nicht mit dem Tauschwert übereinstimmen, denn durch die zusätzliche Nutzung in der Geldfunktion erhöht sich die Nachfrage. Aber selbst wenn die Objekte aus welchen Gründen auch immer ihre Geldfunktion verlieren sollten, so bleiben den Besitzern zumindest anderweitig brauchbare Güter von beachtlichem Wert.

Im Unterschied zum *Naturalgeld* können *Waren-* und *Gerätegeld* nicht einfach in der Natur gewonnen werden – es ist stets ein erheblicher Arbeitsaufwand zur Erzeugung neuen Geldes erforderlich. Als Lohn einer arbeitsteiligen Wirtschaft erscheint eine Geldform, in der Arbeit steckt, eventuell gerechter zu sein. Andererseits haben die Produzenten der Waren oder Geräte, welche die Geldfunktion haben, den Vorteil der erhöhten Nachfrage nach ihren Erzeugnissen, weil diese eben zusätzlich auch als *Bezugsmittel* gebraucht werden. Hersteller von anderen Waren und Gütern, die keine Geldfunktion haben, werden dadurch unter Umständen benachteiligt. Es besteht die Gefahr, dass zu viel *Waren-* und *Gerätegeld* im Vergleich zu anderen Gütern produziert wird, was zu Inflation und Ressourcenverschwendung bei gleichzeitiger Unterversorgung mit anderen Gütern führen kann.

Ob nun *Geräte-*, *Waren-* und *Naturalgeld* nur als Vorformen des eigentlichen Geldes anzusehen sind, da die zugrunde liegenden Gegenstände auch ganz andere Verwendungen haben als nur hortbares Bezugsmittel zu sein, ist eine Definitionssache des Geldbegriffes.

Es gibt allerdings auch Beispiele dafür, dass Geräte wie Messer nur als Geldmittel und nicht mehr zum Schneiden geschaffen wurden: Durch die Art ihrer Fertigung waren sie rein technisch nie in der Funktion etwa eines Messers verwendbar – sie dienten offenbar nur noch als Symbole [Gruen 2004/2005]. Diese Geldform wird *Zeichengeld* genannt ([Sommerfeld 1994], S. 11f). Die als Zeichen benutzten Gegenstände sind funktional unzweifelhaft und ausschließlich *allgemeines Bezugsmaß* und *Tauschmittel*. Sie weisen damit den Weg zu den Geldformen, die heute verbreitet Verwendung finden.

3.3.2 RISIKEN VON INFLATION UND DEFLATION

Absichtlich oder versehentlich verfehlte Geldpolitik hatte wiederholt katastrophale, über das rein Wirtschaftliche weit hinausgehende Konsequenzen.

Die Geldwirtschaft funktioniert nur, wenn die Kaufkraft des Geldes eine gewisse Stabilität hat. Die Kaufkraft von *Fiatgeld* oder von *immateriellem* Geld ergibt sich in der freien Wirtschaft alleine durch das Angebot von Geld und die Nachfrage nach dem Geld. Bei *Kurantmünzen* bzw. *Kreditgeld* können auch Angebot und Nachfrage nach den Substanzen respektive Deckungsgütern eine Rolle spielen.

HYPERINFLATION IN DER WEIMARER REPUBLIK

Verringert sich der Wert einer Geldeinheit im Zahlungsverkehr (*Inflation*), wird die Geldfunktion des Sparens beeinträchtigt. Wenn die Kaufkraft zu schnell schwindet, wird niemand das Geld akzeptieren. *Inflation* können Zentralbanken eindämmen, indem sie die Geldmenge reduzieren – vorausgesetzt, das Problem wird erkannt und der Wille zum Gegensteuern ist vorhanden.

Welche Folgen die zu lockere Geldpolitik einer Zentralbank haben kann, hat sich eindrücklich in der Weimarer Republik gezeigt. Bis 1923 entwickelte sich durch die maßlose Ausdehnung der Geldmenge eine *Hyperinflation* aus der schon im Kaiserreich seit Beginn des Ersten Weltkriegs hohen *Inflation*. Damit wurden nicht nur gesparte Vermögen und bestehende Schulden vernichtet. Die Kaufkraft des Geldes schwand so schnell, dass selbst ein täglich bezahlter Lohn schon deutlich abgewertet war, bevor er investiert werden konnte. Der Geldbedarf wuchs ab einem gewissen Punkt so schnell, dass die Druckereien trotz privatwirtschaftlicher Unterstützung nicht nachkamen und auch die Verteilung nicht mehr zu bewältigen war ([Blaich 1985], S. 10-11). Dies führte zur Schaffung von lokalem Notgeld wie dem Anilin-Dollar [Freitag 2012]. Die *Zentralbank* hatte mit ihrem Geld-Monopol auch jede Handlungsinitiative zur Bewältigung der Krise verloren. Letztlich war der Untergang der Reichsmark [Fergusson 1975/2010] nicht mehr abzuwenden.

Die unmittelbaren materiellen Folgen der Hyperinflation trafen viele Deutsche hart – eine neue existenzielle Bedrohung kurz nach dem verlorenen Krieg. Es kam zu einer fatalen Erosion auch der ideellen Werte, welche den Nährboden für künftige Verbrechen bereitete:

“only the most powerful, the most resourceful and unscrupulous, the hyenas of economic life, can come through unscathed. The great mass of those who put their trust in the traditional order, the innocent and unworldly, all those who do productive and useful work, but don't know how to manipulate money, the elderly who hoped to live on what they earned in the past – all these are doomed to suffer. An experience of this kind poisons the morale of a nation. A straight line runs from the madness of the German Inflation to the madness of the Third Reich.”, zitiert aus [Mann 1942/1975], S. 63.

DEFLATION UND DIE GROSSE DEPRESSION: DIE WELTWIRTSCHAFTSKRISE

Vergrößert sich die Kaufkraft einer Geldeinheit hingegen (*Deflation*), so wird es unattraktiv, das Geld auszugeben. Die Hortung verspricht mehr Gegenwert: Wer noch wartet, kann sich später für die gleiche Geldsumme mehr leisten. Zurückhaltung wird zur dominanten Strategie. Durch das Sparen wird die umlaufende Geldmenge weiter begrenzt. Werden die Preise zur Kompensation des verminderten Konsums weiter reduziert, so verstärkt sich die *Deflation*: Schließlich steigt die Kaufkraft des Geldes durch den Preisverfall weiter. Das Sparen wird damit noch profitabler. Bei *Kreditgeld* oder *Kurantmünzen* ist die Geldmenge durch Fördermengen und Produktionsaufwand des Geldes bzw. des *Deckungsgutes* nach

oben begrenzt. Deswegen kann einer *Deflation* eventuell nicht durch eine Ausdehnung der Geldmenge begegnet werden, ohne mit bisherigen Garantien brechen zu müssen.

In der Weltwirtschaftskrise ab 1929 kam es in der Weimarer Republik zu einer *Deflation*. Die *Deflation* zeigte erhebliche Auswirkungen auf die zusammenbrechende Wirtschaft, die Zahl der Arbeitslosen stieg zeitweise auf über sechs Millionen.

Seit 1924 war die *goldgedeckte* Reichsmark die offizielle Währung der Weimarer Republik mit fixem Wechselkurs zum US-Dollar. Die Politik der *Zentralbank* zielte in der Weltwirtschaftskrise darauf ab, die *Golddeckung* trotz des Abflusses von Gold und Golddevisen aufrechtzuerhalten. Dazu musste sie die Geldmenge reduzieren. Diese Entscheidung war weder frei noch an den wirtschaftlichen Erfordernissen orientiert: Durch den *Young-Plan* war die *Zentralbank* in Deutschland nicht bemächtigt, die Deckung der Reichsmark zu mindestens 40% mit Gold und den fixen Wechselkurs der Mark zum US-Dollar zu lösen ([Blaich 1985], S. 96). Auf deutscher Seite wurde die Strategie gewählt, durch den wirtschaftlichen Zusammenbruch infolge der – vereinbarungsgerechten – *deflationären* Politik mit dem eisernen Festhalten am *Goldstandard* den Alliierten vor Augen zu führen, dass die Reparationsforderungen nicht leistbar sind ([Blaich 1985], S. 99). Diese Strategie ging auf: Mit dem *Hoover-Moratorium* und mit der Konferenz von Lausanne 1932 wurden die Reparationsforderungen Englands und Frankreichs aufgeschoben und größtenteils aufgegeben ([Hardach 1976], S. 130f, [Blaich 1985] S. 106).

Die Ablehnung einer Ausdehnung der Geldmenge zugunsten der Belebung des Arbeitsmarktes und der Konjunktur ließ sich auch deshalb durchsetzen, weil die Befürchtung verbreitet war, dass es nach der Erfahrung der *Hyperinflation* 1923 bei einer Lockerung der Geldpolitik sofort zu Panikreaktionen und mithin zu einer neuerlichen unkontrollierbaren Inflation kommen würde (Inflationsangst), welche irrtümlich für das größere Übel gehalten wurde [Borchardt 1985].

Letztlich hatte die *Deflation* nicht nur unmittelbare wirtschaftliche Not und Massenarbeitslosigkeit zur Folge, sondern sie ermöglichte den extremistischen Parteien den Aufstieg und schließlich den Nationalsozialisten die Machtergreifung. Damit wurde der nächste Weltkrieg eingeleitet.

Wird *Fiatgeld* eingesetzt, kann die *Zentralbank* durch beliebige Ausdehnung der Geldmenge gegen eine *Deflation* vorgehen. Die Menge von *ungedektem* Geld kann mit jeglichen wirtschaftlichen Erfordernissen skalieren. Unter Umständen ist es vielleicht eine Herausforderung, dafür zu sorgen, dass neues Geld die Kaufkraft mindernd eingesetzt wird und dass es nicht zu Fehlallokationen kommt, aber prinzipiell gibt es mit *Fiatgeld* für eine *Zentralbank* genügend Handlungsspielraum, um ihre Aufgabe zu erfüllen und eine *Deflation* wirkungsvoll zu bekämpfen.

Natürlich könnte es bei *ungedektem* Geld zur *Hyperinflation* kommen, da die Geldmenge bei *Fiatgeld* nicht nach oben begrenzt ist – aber eben nur, wenn die *Zentralbank* diese willentlich herbeiführt. *Ungedecktes* Geld hat sich folgerichtig gegenüber *gedeckten* Währungen und *Kurantmünzen* durchgesetzt und ist heute das übliche Zahlungsmittel.

3.3.3 UTOPISCHER SOZIALISMUS: FOURIERS PHALANSTÈRE

Große Kommunen in *Phalanstères* genannten speziellen Siedlungen sind ein Beispiel für Innovationen, die zwar durchaus technische Aspekte haben, die aber eben auch der überzeugten Mitwirkung aller Mitglieder bedürfen. Einige der sozialen, gesellschaftlichen, ökonomischen und umweltpolitischen Ideen Fouriers wurden inzwischen auf andere Weise verwirklicht – mithilfe technischer Erfindungen anderer.

Der Marxismus, der dem Anspruch nach wissenschaftlich und realistisch sein soll, ist als *Ideologie* auf massenhafte Überzeugung angewiesen. Utopischer Sozialismus klingt noch mehr nach – realitätsferner – *Ideologie*. Nach Träumerei statt *technischer Innovation*.

Die Lehre des Sozialisten Charles Fourier befürwortet anders als der Kommunismus keine Gleichmacherei, will Gegensätze nicht nivellieren. Fourier tritt gegen jede Form von Zurückhaltung und Unterdrückung der natürlichen Neigungen und Triebe ein, alles soll sich frei entfalten können. Die Vielfalt der Verschiedenheiten soll noch verfeinert werden.

„In der Harmonie muß es Geschmacksrichtungen aller Art geben, weil die Mittel vorhanden sind, alle zu befriedigen.“ ... „Kultur durch Anziehung kann nur entstehen, wenn es Leidenschaften jeder Schattierung gibt.“, zitiert aus [Fourier 1820/1978], S. 130.

Harmonie nennt Fourier seine neue Ordnung: Zentrales Element seiner Idee sind die *Phalanstères*. *Phalanstères* sind kleine Retortensiedlungen, in denen als *Phalange* bezeichnete soziale und wirtschaftliche Gemeinschaften von etwa 1800 Personen leben und arbeiten ([Fourier 1829], S. 118ff). Innerhalb einer *Phalange* bilden sich nach den verschiedenen Interessen *Serien* genannte Untergruppen (*Serien* der Arbeit, der Liebe ...), in denen diese Interessen dann befriedigt werden können ([Fourier 1829], S. 62ff). Fourier fordert, dass in der *Phalange* jeder arbeiten soll. Bemerkenswert für die Zeit sind Fouriers Forderungen zur vollständigen Emanzipation der Frau und seine Überzeugung, dass die Frauen in vielen vermeintlichen Männerdomänen besser sein würden, wenn man sie nur lassen würde. Gearbeitet werden soll in alle 1-2 Stunden wechselnden Berufen nach eigener Wahl, um Abstumpfung und Langeweile vorzubeugen. Die Arbeitsplätze sollen luxuriös sein, es soll viele Pausen geben – die Tätigkeit werde dann aus Freude erfolgen, anstatt aus Not. Da alle in bis zu 40 verschiedenen Tätigkeiten aktiv werden sollen, wären möglichst ausgeglichene gerechte Löhne laut Fourier für jeden Einzelnen erstrebenswert. Egoismus und Habgier kämen demnach in der *Harmonie* auch der Gemeinschaft zugute.

Einkünfte ergeben sich in der *Harmonie* aus Kapital, Arbeit und Talent. Es gibt keine Lohngleichheit. Außergewöhnliche Leistungen sollen entsprechend gewürdigt werden, zum Beispiel in der Forschung. Auch künstlerische Schöpfungen sollen mit viel Geld gewürdigt werden. Weder die freie Geldwirtschaft (inklusive Einkünften aus Kapital) noch Unterschiede zwischen Arm und Reich würden durch die *Phalanstères* beseitigt, die Folgen würden aber laut Fourier abgemildert, weil zusätzlich eine Grundsicherung vorgesehen ist: Nahrung, Kleidung, sogar Wein und ein allgemeiner Überfluss an Vergnügen sollen innerhalb der *Phalange* gratis sein. Daher könnten alle ihren Lohn sparen. Jeder soll ein kleiner Eigentümer werden (« *le pauvre, en harmonie, a de nombreuses chances de fortune:* » ... « *il est petit propriétaire, il a l'esprit de propriété* », zitiert aus [Fourier 1829], S. 366f).

UMWELTSCHUTZ BEI FOURIER

Nicht nur für die Arbeiter, auch für die Umwelt soll durch die Phalanges gesorgt werden. Fourier weist bereits zu Beginn der Industrialisierung auf die Schäden hin, welche diese verursacht. Damit ist Fourier seiner Zeit weit voraus. Erfindungen, die helfen könnten, etwa den Rauch einzudämmen, sollen seiner Ansicht nach besonders reich belohnt werden ([Fourier 1829], S. 111f). Fourier weiß nicht nur darauf hin, dass etwas gegen die Umweltverschmutzung getan werden muss, sondern er beschreibt auch die Idee zu einer geeigneten *technischen Erfindung*, bleibt dabei aber abstrakt und

vage. Eine *konkrete technische Erfindung*, z. B. die des Katalysators, liefert er nicht. Fourier bereitet also gedanklich den Boden für Entwicklungen und er versucht diese zu motivieren. Tatsächlich wurden entsprechende Erfindungen von anderen auch erbracht - allerdings erst sehr viel später.

Sind die *Phalanstères*, für die Fourier beispielsweise architektonische Pläne mit Grundrissen und wirtschaftliche Berechnungen anstellt, nun als konkrete *technische Erfindung* anzusehen, deren *gestalterische Wirkung* Fouriers Visionen indirekt Wirklichkeit werden lassen könnte? Oder ist eine *ideologische* Überzeugungsarbeit im Sinne von Fouriers Lehre die Voraussetzung, um Veränderungen in seinem Sinne herbeiführen zu können?

Bei Fourier gibt es im Gegensatz zu Marx keinen Aufruf zur Revolution, zum gewaltsamen Umsturz. Es sollen vielmehr die freiwilligen ersten *Phalanstères* durch ihr Beispiel überzeugen und andere anstecken. Die Möglichkeit, derartige Prototypen zu erschaffen und diese quasi als Experiment zu nutzen, deutet auf eine konkrete *technische Erfindung* hin.

Allerdings: Innerhalb eines *Phalanstères* spielt die Überzeugung eine entscheidende, treibende Rolle. Die *Ideologie* Fouriers, so freiheitlich sie erscheint, verträgt sich z. B. mit keiner beschränkenden Moral. Fourier bedient sich einer verführerischen Sprache, um etwas zu bewegen, um die Harmonie verlockend erscheinen zu lassen – um zu überzeugen.

FREIE LIEBE? INTERAKTION VON ÜBERZEUGUNGEN, ERFINDUNGEN UND ANDEREN ENTWICKLUNGEN

„Häßlichkeiten an Körper und Seele, Mißtrauen, Krankheiten, allgemeiner Betrug legen dem Aufkeimen der verschiedenen Arten der Liebe, die wir geschildert haben, unüberwindliche Hindernisse in den Weg. Doch wir gründen unsere Berechnungen nicht auf die Zivilisation, sondern auf eine Ordnung, in der auch die geringsten Menschen reich, höflich, aufrichtig, liebenswert, tugendhaft und - außer im sehr hohen Alter - schön sein werden.“

...
„Mit gutem Grund darf ich verheißen, daß die Harmonie Keime der freihellichen Liebe hervorbringen wird, die in der entgegengesetzten Richtung wirken wie unsere Bräuche und“ ... „eine hochherzige und heilige Trunkenheit, eine erhabene Wollust bescheren wird, die unserem heutigen Egoismus weit überlegen ist“, zitiert aus [Fourier 1820/1978], S. 146f.

Fourier stellt die für seine Zeit skandalöse Forderung nach *freier Liebe* auf. Mit der blumig beschriebenen Vision versucht er, zu begeistern, zu überzeugen. Fourier präsentiert keine *technische Erfindung*, deren *gestalterische Wirkung* zu *freier Liebe* führen würde. Die Idee der *freien Liebe* im Sinne Fouriers wurde etwa im Zuge der *Sexuellen Revolution* aufgegriffen und hat durchaus Wirkung in der Realität gezeigt, auch wenn es bei wenigen experimentellen Kommunen blieb.

Eine konkrete *technische Erfindung* auf diesem Gebiet ist hingegen etwa die Antibabypille, welche unbestreitbar gesellschaftliche Veränderung herbeigeführt hat [Becke 2010]. „Kein Medikament zog solch große gesellschaftliche Veränderungen nach sich wie die oralen Verhütungsmittel.“, zitiert aus [Streller 2011], S. 270. Die Antibabypille transportiert keine *Ideologie*, keine *Glaubenslehre* oder Einstellung, sondern sie verhindert primär ungewollte Schwangerschaften. Sie erlaubt zwar Frauen auch das Ausleben einer promiskuen Sexualität ohne Gefahr zu laufen, unbeabsichtigt ein Baby von einem der vielen Partner zu bekommen. Aber die Pille kann genauso gut in einer streng monogamen Beziehung zur Familienplanung eingesetzt werden. Die Antibabypille wird außer zur Empfängnisverhütung auch therapeutisch eingesetzt, etwa gegen Akne [Pricop 2007]. Einige Frauen nehmen die Pille nur, weil die darin enthaltenen Hormone sich etwa positiv auf das Hautbild auswirken können und Menstruationsbeschwerden damit vermindert werden können, obwohl sie in völliger Enthaltensamkeit leben. Wie das Sexleben einer Konsumentin aussieht, das ist nicht Sache der Pille. Die Pille leistet sicher keine Propagierung von *freier Liebe* oder von Sexualität ohne Fortpflanzungsfunktion – sie eröffnet nur neue Potenziale.

Trotz ihrer Neutralität können *technische Erfindungen* Gegenstand *ideologischer* Auseinandersetzungen werden. Wie andere Verhütungsmittel wird die Antibabypille von manchen *Glaubenslehren* und *Ideologien* abgelehnt und bekämpft. Mit der Enzyklika *Humanae Vitae* erlaubt der Papst Paul der VI. Katholiken etwa nur eine therapeutische Nutzung [Paul VI. 1968]. Dass *technische Erfindungen* nicht nur jene betreffen, welche sie nutzen wollen, zeigt sich auch bei der Pille: Die Hormone gelangen in die Gewässer und sie können andere Lebewesen schädigen [Löttscher 2008].

Gab es zunächst begünstigt durch die Markteinführung der Pille sowie auch schon wegen der Zurückdrängung von Syphilis in den 1950er Jahren durch das Medikament Penicillin (eine weitere konkrete *technische Innovation*) Tendenzen zu einer sexuellen Befreiung [Francis 2013], zur Liebe mit immer neuen Partnern, so hat sich dies durch HIV und Aids in den 1980er Jahren wieder gewandelt. Das Auftreten dieser Krankheit hatte eine erhebliche *gestalterische Wirkung*: Weil die Immunschwäche bis heute gefährlich ist und weil auch Kondome keinen hundertprozentigen Schutz bieten, sind Enthaltsamkeit und Monogamie plötzlich zu einer rationalen Strategie zur Verhinderung von Neuinfektionen geworden. Dies wurde und wird *ideologisch* verwendet um konservative Moralvorstellungen („Treue“) zu propagieren [Santelli 2006]. Mit der Entwicklung und Verfügbarkeit von schnellen HIV-Tests sowie Erfolgen bei (auch prophylaktischen) Therapien zeichnet sich allerdings eine neuerliche Trendwende ab: Mit der schwindenden Todesangst wird auch die Vorsicht eventuell wieder abnehmen [Dannecker 2006]. Die *technische Entwicklung* eines Impfstoffes oder Heilmittels für HIV könnte die Bedingungen für *freie Liebe* weiter verbessern.

Der technische Fortschritt hat manches von Fouriers Träumen inzwischen wahr werden lassen – und zwar ohne Überzeugung der breiten Masse von Fouriers Idealen. Die konkreten *technischen Erfindungen*, denen eine verändernde *gestalterische Wirkung* in Fouriers Sinne zugesprochen werden kann, haben letztlich andere geliefert.

3.3.4 STARKE ANONYMITÄT BEI SYSTEMEN OFFENER KONTEN IM S-NETZWERK

Mit mehreren Verteilern können regelkonforme Transaktionen zwischen Konten und Zahlvorgänge im S-Web anonymisiert werden, ohne einzelnen Parteien vertrauen zu müssen. Auch erweiterte Kaufgeschäfte mit Auslieferung eines Guts und mit verlässlichem Feedback lassen sich mithilfe des S-Netzwerks anonymisieren.

Mit einer einzelnen Partei als *Verteiler* und einer Vereinbarung zwischen der zahlenden *Alice* und dem empfangenden *Bob* wird nur eine schwache Form der Anonymisierung erreicht. Insbesondere ist *Alice* bei dem in der Dissertation in Kapitel 2.3.4 gezeigten Verfahren gegenüber *Bob* nicht anonym. Außerdem lässt sich für Dritte eventuell ein Zusammenhang zwischen der Überweisung von *Alice* an den *Verteiler* und der Überweisung vom *Verteiler* an *Bob* herstellen, wenn beide denselben Betrag χ aufweisen.

Zur Verbesserung bietet es sich an, statt zweier Überweisungen mit dem Betrag χ jeweils mehrere Überweisungen mit zufälligen Beträgen, welche in Summe χ ergeben, zu tätigen. Damit *A* und *B* anonym voreinander bleiben, sollten ferner Verträge nur mit dem *Verteiler* *V* geschlossen werden. Ein entsprechendes Protokoll könnte wie folgt aussehen.

1 *A* legt Beträge χ_{V_1} bis χ_{V_N} fest, welche in Summe χ ergeben, wobei *N* eine zufällig gewählte natürliche Zahl ist. *A* erzeugt für jeden der Beträge χ_{V_1} bis χ_{V_N} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck θ_{V_1} bis Zweck θ_{V_N} entstehen.

A legt Beträge χ_{B_1} bis χ_{B_M} fest, welche in Summe χ ergeben, wobei *M* eine zufällig gewählte natürliche Zahl ist. *A* erzeugt für jeden der Beträge χ_{B_1} bis χ_{B_M} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck θ_{B_1} bis Zweck θ_{B_M} entstehen.

A offeriert *V* einen geheimen Vertrag ε_{AV} darüber, dass *A* über *V* den Betrag χ mit dem Betreff θ_B an *B* überweist. Dieser beinhaltet für *V* die Verpflichtung, die Beträge χ_{B_1} bis χ_{B_M} separat mit dem jeweilig vom Index entsprechenden Zweck θ_{B_1} bis θ_{B_M} über einen langen Zeitraum δ_B verteilt an *B* zu überweisen, wenn *A* die Beträge χ_{V_1} bis χ_{V_N} separat mit dem jeweilig vom Index entsprechenden Zweck θ_{V_1} bis θ_{V_N} über einen langen Zeitraum δ_V verteilt an *V* überweist.

Außerdem legt der Vertrag ε_{AV} fest, dass *V* mit *B* einen geheimen rechtsgültigen Vertrag ε_{VB} darüber abschließen muss, dass *B* die Zahlung mit dem Betreff θ_B und dem Betrag χ durch *M* separate über einen langen Zeitraum δ_B verteilte Überweisungen mit den Beträgen χ_{B_1} bis χ_{B_M} sowie dem jeweilig vom Index entsprechenden Zweck θ_{B_1} bis θ_{B_M} durch den *Verteiler* *V* akzeptieren wird.

2 *V* und *B* schließen den geheimen rechtsgültigen Vertrag ε_{VB} ab.

3 *V* schließt mit *A* den geheimen rechtsgültigen Vertrag ε_{AV} ab.

4 *A* überweist für alle einsehbar von seinem Konto K_A separat jeden einzelnen Betrag aus χ_{V_1} bis χ_{V_N} mit dem jeweils vom Index entsprechenden Zweck aus θ_{V_1} bis θ_{V_N} auf das Konto K_V von *Verteiler* *V*, wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_V verteilt verbucht werden.

5 *V* überweist für alle einsehbar von seinem Konto K_V separat jeden einzelnen Betrag aus χ_{B_1} bis χ_{B_M} mit dem jeweils vom Index entsprechenden Zweck aus θ_{B_1} bis θ_{B_M} auf das Konto K_B von Empfänger *B*, wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_B verteilt verbucht werden.

In diesem in Abbildung 20 dargestellten Verfahren kennen nur *A*, *B* und *V* den Betrag χ . Zwar überweist *A* in Summe den Betrag χ an *V*. Für alle außer für *A* und *V* ergibt sich daraus jedoch kein Hinweis, ob die *N* einzelnen Transaktionen einem gemeinsamen Zweck dienen und an einen gemeinsamen Empfänger überwiesen werden sollen, oder ob es sich um bis zu *N* völlig unabhängige zu anonymisierende Zahlungsvorgänge handelt. Die einzelnen Überweisungen in Schritt 3 werden über einen langen Zeitraum δ_V hinweg verteilt getätigt. Aus der zeitlichen Abfolge der einzelnen Buchungen ergeben sich keine Erkenntnisse über

einen möglichen Zusammenhang, denn eventuell nutzt A den *Verteiler* V in der Zeit δ_V auch noch für Teilbuchungen zu anderen zu anonymisierenden Überweisungen.

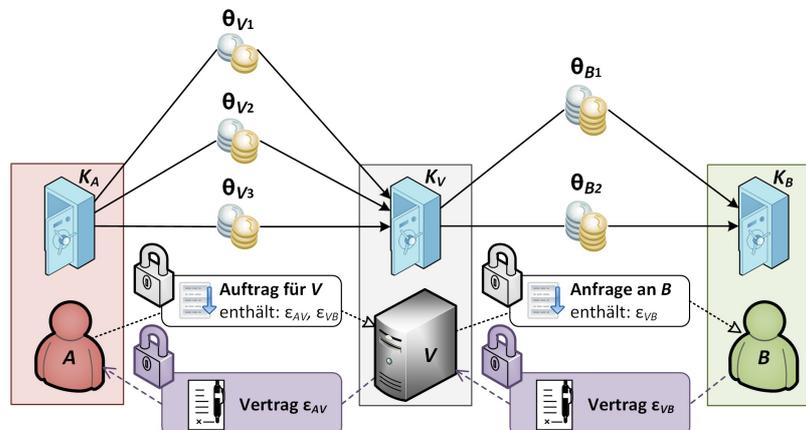


Abbildung 20: Auch gegenüber dem Empfänger anonyme Überweisung

V überweist zwar ebenfalls in Summe den Betrag χ an B , aber bei den M einzelnen Transaktionen könnte es sich nicht bloß um eine, sondern um bis zu M verschiedene unabhängige zu anonymisierende Zahlungsvorgänge für verschiedene Kunden handeln. Die einzelnen Teilüberweisungen in Schritt 4 werden über einen langen Zeitraum δ_B hinweg verteilt getätigt. Aus der zeitlichen Abfolge der einzelnen Buchungen ergeben sich wiederum keine Erkenntnisse über einen möglichen Zusammenhang, denn eventuell tätigt der *Verteiler* V in der Zeit δ_B auch noch Teilbuchungen für andere zu anonymisierende Überweisungen an B . Je intensiver das Konto K_V des *Verteilers* V für anonyme Transaktionen genutzt wird und je länger die Zeiträume δ_V und δ_B gewählt werden, desto besser ist die erzielbare Anonymisierung.

ZEITNAH GARANTIERTE ANONYME ZAHLUNG UND PRÜFUNGEN DURCH VERTEILER

Bei dem hier gezeigten Verfahren ergibt sich durch die langen Zeiträume δ_V und δ_B eine große zeitliche Verzögerung, bis die Überweisung komplett bei B ankommt. Wenn eine sofortige rechtsverbindliche Zahlungsbestätigung für B gewünscht wird, kann A nach Schritt 3 V die Zahlung von χ_{V1} bis χ_{VN} in einem geheimen Vertrag garantieren. Eventuell analysiert V zuerst anhand des offenen Kontos von A , wie wahrscheinlich die Begleichung der Schuld ist. Gegen Ausfallrisiken kann V eine Kautions $> \chi$ einfordern, die nach der Zahlung von χ_{V1} bis χ_{VN} erstattet wird. V kann anschließend B die Zahlung von χ_{B1} bis χ_{BM} in einem geheimen Vertrag sofort garantieren.

Banken müssen die rechtliche Zulässigkeit einer Überweisung etwa anhand von Sperr- und Embargolisten prüfen. Ein *Verteiler* V kann in den gezeigten Verfahren derartige Prüfungen übernehmen, sodass sich anonyme Überweisungen nicht für illegale Zwecke nutzen lassen. Auch bei Zahlvorgängen, wenn B ein Produkt nur an Personen einer bestimmten Gruppen G verkaufen darf, kann V prüfen und bezeugen, ob A zu G gehört, ohne B Genaueres zur Identität von A zu verraten.

Der *Verteiler* V kann bei dem bisher gezeigten Verfahren jedem Interessenten mitteilen, welche Transaktionen er durchführt, denn V kennt jeweils den Sender A , den Empfänger B und den Betrag χ . Bezüglich der Wahrung ihrer Anonymität müssen also sowohl A als auch B dem *Verteiler* V und mithin einer einzelnen Partei vollkommen vertrauen.

ANONYME ÜBERWEISUNGEN IM S-NETZWERK MIT MEHREREN VERTEILERN

Wird ein höheres Sicherheitsniveau angestrebt, bei dem keiner einzelnen dritten Partei vertraut werden muss, wie es für das S-Netzwerk selbst grundsätzlich angestrebt wird, sind zusätzliche *Verteiler* erforderlich. Das folgende in Abbildung 21 und in Fehler: Referenz nicht gefunden visualisierte Protokoll nutzt dazu Secret Sharing Verfahren und es benötigt

vier Verteiler U , V sowie C und D um eine anonyme Überweisung mit dem Betreff θ_B und mit dem Betrag χ eines Senders A an einen Empfänger B zu ermöglichen, die nur aufgedeckt werden kann, wenn mindestens zwei der Verteiler sich inkorrekt verhalten.

1 A legt Beträge χ_{C_1} bis χ_{C_N} und χ_{D_1} bis χ_{D_M} fest, welche alle zusammen in Summe χ ergeben, wobei N und M zufällig gewählte natürliche Zahlen sind. A erzeugt für jeden der Beträge χ_{C_1} bis χ_{C_N} und χ_{D_1} bis χ_{D_M} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck θ_{C_1} bis Zweck θ_{C_N} und Zweck θ_{D_1} bis Zweck θ_{D_M} entstehen.

A legt Beträge χ_{U_1} bis χ_{U_K} und χ_{V_1} bis χ_{V_L} fest, welche alle zusammen in Summe genau die Summe über χ_{C_1} bis χ_{C_N} ergeben, wobei K und L zufällig gewählte natürliche Zahlen sind. A erzeugt für jeden der Beträge χ_{U_1} bis χ_{U_K} und χ_{V_1} bis χ_{V_L} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck θ_{U_1} bis Zweck θ_{U_K} und Zweck θ_{V_1} bis Zweck θ_{V_L} entstehen.

A legt Beträge $\chi_{U_{K+1}}$ bis χ_{U_H} und $\chi_{V_{L+1}}$ bis χ_{V_J} fest, welche alle zusammen in Summe genau die Summe über χ_{D_1} bis χ_{D_M} ergeben, wobei H und J zufällig gewählte natürliche Zahlen sind für die gilt $H > K + 1$ und $J > L + 1$. A erzeugt für jeden der Beträge $\chi_{U_{K+1}}$ bis χ_{U_H} und $\chi_{V_{L+1}}$ bis χ_{V_J} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck $\theta_{U_{K+1}}$ bis Zweck θ_{U_H} und Zweck $\theta_{V_{L+1}}$ bis Zweck θ_{V_J} entstehen.

A legt Beträge χ_{B_1} bis χ_{B_Q} fest, welche in Summe genau die Summe über χ_{U_1} bis χ_{U_H} ergeben, wobei Q eine zufällig gewählte natürliche Zahl > 1 ist. A legt Beträge $\chi_{B_{Q+1}}$ bis χ_{B_R} fest, welche in Summe genau die Summe über χ_{V_1} bis χ_{V_J} ergeben, wobei R eine zufällig gewählte natürliche Zahl ist, für die $R > Q + 1$ gilt. A erzeugt für jeden der Beträge χ_{B_1} bis χ_{B_R} jeweils eine zufällige Zeichenfolge als Zweck, sodass Zweck θ_{B_1} bis Zweck θ_{B_R} entstehen.

A bereitet einen geheimen Vertrag ε_{UB} zwischen U und B vor, in dem sich B verpflichtet, einen Teil der Zahlung mit dem Betreff θ_B durch Q separate Überweisungen von dem Verteiler U mit den Beträgen χ_{B_1} bis χ_{B_Q} und mit dem jeweilig vom Index entsprechenden Zweck θ_{B_1} bis θ_{B_Q} über einen langen Zeitraum δ_B verteilt zu akzeptieren.

A bereitet einen geheimen Vertrag ε_{VB} zwischen V und B vor, in dem sich B verpflichtet, einen Teil der Zahlung mit dem Betreff θ_B durch $R - Q$ separate Überweisungen von dem Verteiler V mit den Beträgen $\chi_{B_{Q+1}}$ bis χ_{B_R} und mit dem jeweilig vom Index entsprechenden Zweck $\theta_{B_{Q+1}}$ bis θ_{B_R} über einen langen Zeitraum δ_B verteilt zu akzeptieren.

Ferner bereitet A einen geheimen Vertrag ε_{CU} vor, mit dem Verteiler U dem Verteiler C zusichert, den Vertrag ε_{UB} mit B abgeschlossen zu haben. Mit ε_{CU} bestätigt U außerdem, Überweisungen von C an U mit den Beträgen χ_{U_1} bis χ_{U_K} und mit dem jeweilig vom Index entsprechenden Zweck θ_{U_1} bis θ_{U_K} über einen langen Zeitraum δ_U für die Leistung der im Vertrag ε_{UB} erwähnten Zahlungen an B zu verwenden.

Ferner bereitet A einen geheimen Vertrag ε_{DU} vor, mit dem Verteiler U dem Verteiler D zusichert, den Vertrag ε_{UB} mit B abgeschlossen zu haben. Mit ε_{DU} bestätigt U außerdem, Überweisungen von D an U mit den Beträgen $\chi_{U_{K+1}}$ bis χ_{U_H} und mit dem jeweilig vom Index entsprechenden Zweck $\theta_{U_{K+1}}$ bis θ_{U_H} über einen langen Zeitraum δ_U für die Leistung der im Vertrag ε_{UB} erwähnten Zahlungen an B zu verwenden.

Ferner bereitet A einen geheimen Vertrag ε_{CV} vor, mit dem Verteiler V dem Verteiler C zusichert, den Vertrag ε_{VB} mit B abgeschlossen zu haben. Mit ε_{CV} bestätigt V außerdem, Überweisungen von C an V mit den Beträgen χ_{V_1} bis χ_{V_L} und mit dem jeweilig vom Index entsprechenden Zweck θ_{V_1} bis θ_{V_L} über einen langen Zeitraum δ_V für die Leistung der im Vertrag ε_{VB} erwähnten Zahlungen an B zu verwenden.

Ferner bereitet A einen geheimen Vertrag ε_{DV} vor, mit dem Verteiler V dem Verteiler D zusichert, den Vertrag ε_{VB} mit B abgeschlossen zu haben. Mit ε_{DV} bestätigt V außerdem, Überweisungen von D an V mit den Beträgen $\chi_{V_{L+1}}$ bis χ_{V_J} und mit dem jeweilig vom Index entsprechenden Zweck $\theta_{V_{L+1}}$ bis θ_{V_J} über einen langen Zeitraum δ_V für die Leistung der im Vertrag ε_{VB} erwähnten Zahlungen an B zu verwenden.

Weiters bereitet A einen geheimen Vertrag ε_{AC} vor, mit dem *Verteiler C* dem Auftraggeber A zusichert, den Vertrag ε_{CU} mit dem *Verteiler U* abgeschlossen zu haben und den Vertrag ε_{CV} mit dem *Verteiler V* abgeschlossen zu haben. Mit ε_{AC} bestätigt C außerdem, Überweisungen von A an C mit den Beträgen χ_{C1} bis χ_{CN} und mit dem jeweilig vom Index entsprechenden Zweck θ_{C1} bis θ_{CN} über einen langen Zeitraum δ_C für die Leistung der in den Verträgen ε_{CU} und ε_{CV} erwähnten Zahlungen zu verwenden.

Schließlich bereitet A einen geheimen Vertrag ε_{AD} vor, mit dem *Verteiler D* dem Auftraggeber A zusichert, den Vertrag ε_{DU} mit dem *Verteiler U* abgeschlossen zu haben und den Vertrag ε_{DV} mit dem *Verteiler V* abgeschlossen zu haben. Mit ε_{AD} bestätigt D außerdem, Überweisungen von A an D mit den Beträgen χ_{D1} bis χ_{DM} und mit dem jeweilig vom Index entsprechenden Zweck θ_{D1} bis θ_{DM} über einen langen Zeitraum δ_D für die Leistung der in den Verträgen ε_{DU} und ε_{DV} erwähnten Zahlungen zu verwenden.

Jeder der Verträge enthält zusätzlich Anweisungen zum Senden der Nachrichten und zum Abschließen der Verträge im Sinne dieses Protokolls.

A erzeugt eine Secret Sharing Zerlegung

$$Z_{22}(\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB}) = \{ T_{220}(\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB}), T_{221}(\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB}) \}$$

Es sei $T_{U1} = T_{220}(\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB})$ und $T_{U2} = T_{221}(\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB})$.

A erzeugt eine Secret Sharing Zerlegung

$$Z_{22}(\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB}) = \{ T_{220}(\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB}), T_{221}(\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB}) \}$$

Es sei $T_{V1} = T_{220}(\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB})$ und $T_{V2} = T_{221}(\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB})$.

A sendet $\varepsilon_{AC} \circ T_{U1} \circ T_{V1}$ so an C , dass nur A und C auf die Nachricht zugreifen können.

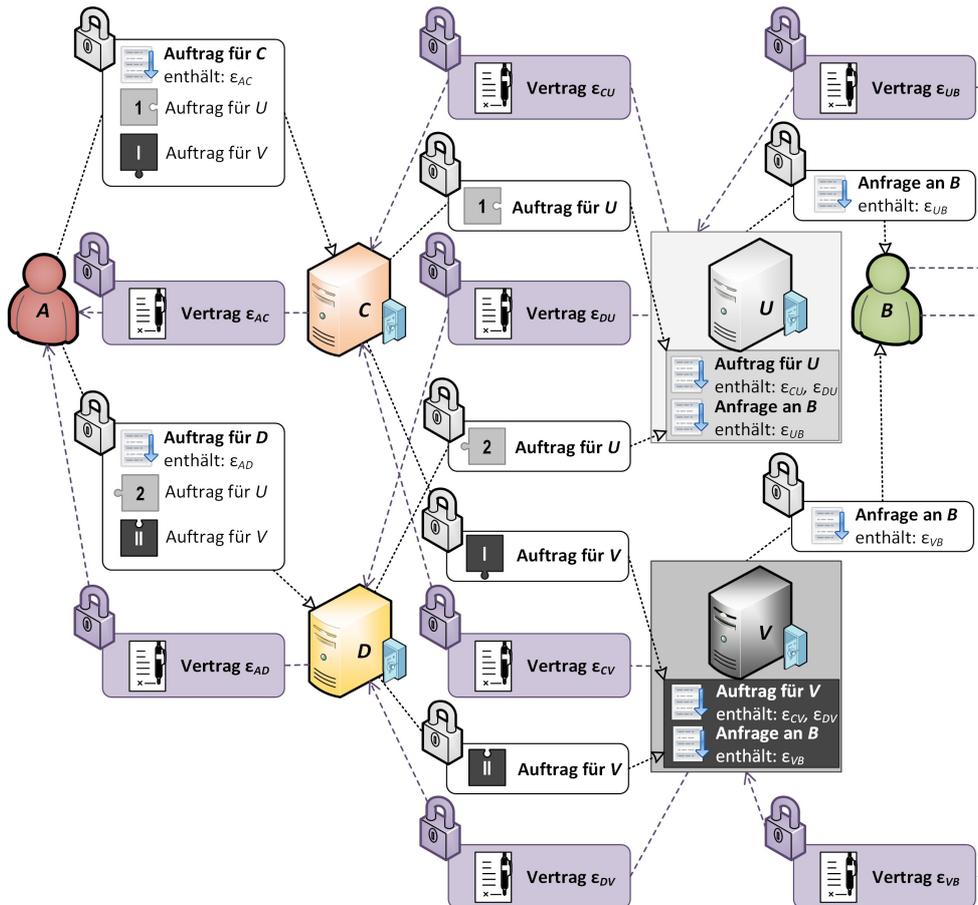


Abbildung 21: Anonyme Transaktion mit Secret Sharing – Verträge

- 2 A sendet $\varepsilon_{AD} \circ TU_2 \circ TV_{ii}$ so an D , dass nur A und D auf die Nachricht zugreifen können.
- 3 C sendet TU_1 so an U , dass nur A und U auf die Nachricht zugreifen können.
- 4 C sendet TV_1 so an V , dass nur A und V auf die Nachricht zugreifen können.
- 5 D sendet TU_2 so an U , dass nur A und U auf die Nachricht zugreifen können.
- 6 D sendet TV_{ii} so an V , dass nur A und V auf die Nachricht zugreifen können.
- 7 U fügt TU_1 und TU_2 zu $\varepsilon_{CU} \circ \varepsilon_{DU} \circ \varepsilon_{UB}$ zusammen. U sendet ε_{UB} so an B , dass nur U und B auf die Nachricht zugreifen können.
- 8 V fügt TV_1 und TV_{ii} zu $\varepsilon_{CV} \circ \varepsilon_{DV} \circ \varepsilon_{VB}$ zusammen. V sendet ε_{VB} so an B , dass nur V und B auf die Nachricht zugreifen können.
- 9 B schließt den Vertrag ε_{UB} mit U .
- 10 B schließt den Vertrag ε_{VB} mit V .
- 11 U schließt den Vertrag ε_{CU} mit C .
- 12 U schließt den Vertrag ε_{DU} mit D .
- 13 V schließt den Vertrag ε_{CV} mit C .
- 14 V schließt den Vertrag ε_{DV} mit D .
- 15 C schließt den Vertrag ε_{AC} mit A .
- 16 D schließt den Vertrag ε_{AD} mit A .

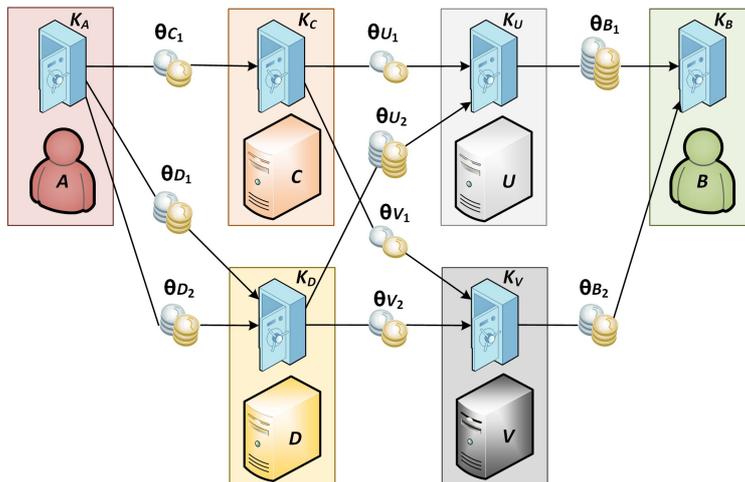


Abbildung 22: Anonyme Transaktion mit Secret Sharing – Geldtransfers

- 17 A überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_A separat jeden einzelnen Betrag aus χ_{C1} bis χ_{CN} mit dem jeweils vom Index entsprechenden Zweck aus θ_{C1} bis θ_{CN} auf das Konto K_C von Verteiler C , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_C verteilt verbucht werden.
- 18 A überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_A separat jeden einzelnen Betrag aus χ_{D1} bis χ_{DM} mit dem jeweils vom Index entsprechenden Zweck aus θ_{D1} bis θ_{DM} auf das Konto K_D von Verteiler D , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_D verteilt verbucht werden.
- 19 C überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_C separat jeden einzelnen Betrag aus χ_{U1} bis χ_{UK} mit dem jeweils vom Index entsprechenden Zweck aus θ_{U1} bis θ_{UK} auf das Konto K_U von Verteiler U , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_U verteilt verbucht werden.
- 20 C überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_C separat jeden einzelnen Betrag aus χ_{V1} bis χ_{VL} mit dem jeweils vom Index entsprechenden Zweck aus θ_{V1} bis θ_{VL} auf das Konto K_V von Verteiler V , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_V verteilt verbucht werden.

- 21 D überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_D separat jeden einzelnen Betrag aus $\chi_{U_{K+1}}$ bis χ_{U_H} mit dem jeweils vom Index entsprechenden Zweck aus $\theta_{U_{K+1}}$ bis θ_{U_H} auf das Konto K_U von *Verteiler* U , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_U verteilt verbucht werden.
- 22 D überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_D separat jeden einzelnen Betrag aus $\chi_{V_{L+1}}$ bis χ_{V_J} mit dem jeweils vom Index entsprechenden Zweck aus $\theta_{V_{L+1}}$ bis θ_{V_J} auf das Konto K_V von *Verteiler* V , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_V verteilt verbucht werden.
- 23 U überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_U separat jeden einzelnen Betrag aus χ_{B_I} bis χ_{B_Q} mit dem jeweils vom Index entsprechenden Zweck aus θ_{B_I} bis θ_{B_Q} auf das Konto K_B von Empfänger B , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_B verteilt verbucht werden.
- 24 V überweist für alle Teilnehmer am Tauschring einsehbar von seinem Konto K_V separat jeden einzelnen Betrag aus $\chi_{B_{Q+1}}$ bis χ_{B_R} mit dem jeweils vom Index entsprechenden Zweck aus $\theta_{B_{Q+1}}$ bis θ_{B_R} auf das Konto K_B von Empfänger B , wobei die einzelnen Überweisungen zufällig über den Zeitraum δ_B verteilt verbucht werden.

Die *Verteiler* C und D haben in diesem Protokoll nur Kontakt zu A , zu U sowie zu V und sie kennen nur diese. Die Identität des Empfängers wird durch das Secret Sharing vor ihnen verborgen – sie erhalten von beiden Zerlegungen jeweils nur einen Share. Die *Verteiler* U und V haben nur Kontakt zu C , zu D sowie zu B und kennen nur diese. Erst wenn mindestens zwei der *Verteiler* ihre geheim zu haltenden Informationen kombinieren, können sie zur anonymisierten Transaktion sowohl den Sender A als auch den Empfänger B benennen. Kein *Verteiler* kann alleine die Höhe des insgesamt zu überweisenden Betrags χ ermitteln – jeder erhält nur einen zufälligen Teil des Betrags.

Empfänger B kennt in diesem Protokoll nur die *Verteiler* V und U . Um an die Identität von Sender A zu kommen, benötigt B zumindest von zwei der vermittelnden Parteien geheime Informationen.

Die Geheimhaltung kann auch aufrechterhalten werden, wenn einer der *Verteiler* die eingehenden Überweisungen nicht vertragskonform weiterleitet. In einem fälligen Rechtsstreit kann für jeden *Verteiler* eine eigene Kommission gebildet werden, die untersucht, ob sich der jeweilige *Verteiler* korrekt verhalten hat. Auf diese Weise erfährt jede Untersuchungskommission nicht mehr, als ein einzelner *Verteiler* wissen darf. Mithin können Kommissionen keine Verbindung zwischen Sender A und Empfänger B der Transaktion herstellen.

ZEITNAH GARANTIERTE ANONYME ZAHLUNGEN UND PRÜFUNGEN BEI MEHREREN VERTEILERN

Durch die langen Zeiträume δ_C , δ_D , δ_U , δ_V , δ_B entstehen besonders ausgedehnte zeitliche Verzögerungen, bis die Transaktion vollständig abgeschlossen ist. Wird eine sofortige Bestätigung der Transaktion benötigt, muss die Zahlung von A ausgehend nach Abschluss der Verträge ε_{AC} und ε_{AD} durch zusätzliche Garantien zunächst gegenüber den *Verteilern* C und D besiegelt werden. Anders als bei Verfahren mit nur einem *Verteiler* können C und D in dem Verfahren mit vier *Verteilern* auf dem offenen Konto K_A von A anhand des Kontostands nur eingeschränkt prüfen, ob A die nötigen Mittel für die Durchführung der Überweisung wahrscheinlich haben wird, denn sie haben keine Informationen über die Gesamthöhe χ der Überweisung, sondern nur jeweils über die Teilbeträge, welche sie jeweils weiterüberweisen sollen.

Genügt C und D eine rechtsverbindliche Selbstverpflichtung von A , die Zahlung tatsächlich durchzuführen, nicht, können sie von A eine Kautions einfordern, die jeweils größer als die von ihnen zu verteilende Beträge ist und die sie zurückerstatten, wenn A seiner Verpflichtung nachkommt. C und D garantieren dann jeweils gegenüber U und V , dass die Durchführung der Transaktion erfolgen wird. U und V geben schließlich ihrerseits eine Garantie gegenüber B ab.

Etwaige Prüfungen auf die rechtliche Zulässigkeit von Transaktionen bei gleichzeitiger Wahrung der Anonymität erfordern eventuell ein Zusammenwirken aller *Verteiler*. Beispielsweise können C und D unabhängig voneinander für U und V bescheinigen, dass A zu einer bestimmten Gruppe G von Personen gehört, ohne dabei U und V weitere Informationen über die Identität von A zu ver-

raten. U und V können dann jeweils für sich prüfen, ob eine Person aus G eine Überweisung an B tätigen darf. Wenn A dies vertraglich gestattet, können U und V die Zugehörigkeit von A zu G auch an B kommunizieren. Dies kann genutzt werden, um beispielsweise Produkte zu erstellen, die nicht an alle Personen verkauft werden dürfen, ohne die eigene Identität vollständig preisgeben zu müssen.

Durch den Einsatz von weiteren Parteien als zusätzliche *Verteiler* lässt sich die Anzahl der *Verteiler*, deren Informationen benötigt werden, um einzelne Zahlungsvorgänge aufdecken zu können, weiter steigern. Damit die geheimen Informationen von mindestens drei vermittelnden Parteien benötigt werden, um die Überweisung aufdecken zu können, werden bereits insgesamt neun *Verteiler* benötigt. Weil mit der Anzahl der *Verteiler* auch der Aufwand pro Zahlvorgang signifikant steigt, macht es eventuell Sinn, den Nutzern verschiedene Grade der Anonymisierung anzubieten – je nachdem, wie sensibel ihnen eine Transaktion erscheint, können sie dann jeweils ein bestimmtes Sicherheits-Level auswählen.

ANONYMES EINKAUFEN UND VERLÄSSLICHES FEEDBACK FÜR ANONYM ERSTANDENE PRODUKTE

Beim anonymen Einkaufen geht es nicht nur darum, einen Betrag von einem Konto auf ein anderes zu überweisen, sondern es soll im Gegenzug auch ein Produkt erstanden werden – und zwar möglichst ohne die Anonymität und Sicherheit, welche bei der Transaktion erreicht wird, gleich wieder zu verspielen.

Wird in einem Geschäft vor Ort ein Produkt persönlich erworben und gleich mitgenommen, so könnte die Identität des Käufers eventuell über eine Gesichtserkennung aufgedeckt werden, selbst wenn der Bezahlvorgang selbst keinerlei Informationen über die Identität des Käufers verrät. Als mögliche Gegenmaßnahme kann versucht werden, das Gesicht so zu maskieren, dass keine Erkennung gelingen wird, allerdings sind dabei eventuell gesetzliche Vorgaben wie Verhüllungsverbote zu beachten.

Beim Einkaufen aus der Ferne mithilfe von Kommunikationsmedien wird die direkte physische Exposition des Käufers gegenüber dem Verkäufer vermieden. Um Anonymität bei Kaufgeschäften im Fernabsatz wahren zu können, genügt es nicht, nur anonyme Zahlungen in Form des *allgemeinen Bezugsmittels* durchführen zu können. Für das anonyme Einkaufen müssen auch der Bestellvorgang und der Auslieferungsvorgang des Produkts irgendwie anonym organisiert werden. Eine Übermittlung des Produkts von Anbieter B an Kunde A etwa mit einem gewöhnlichen Paketdienst würde voraussetzen, dass B im Zuge der Bestellung genaue Informationen über die Identität von A verraten werden – mindestens eine Lieferadresse, über die A erreichbar ist.

Stattdessen bietet es sich an, die Bestellung, Bezahlung und Auslieferung des Produktes über das Netz der *Verteiler* abzuwickeln. Die Bestellung wird im Zuge der Vertragsabschlüsse für die anonyme Transaktion zur Bezahlung mitverhandelt, wobei zugleich auch geeignete Lieferbedingungen festgelegt werden. In dem Verfahren mit vier *Verteilern* würde B das Produkt nach dem Abschluss der Verträge zunächst mit einem gewöhnlichen Paketdienst (bei einem physischen Produkt) bzw. per S-Mail (bei immateriellen Gütern) an *Verteiler U* oder *Verteiler V* senden, welche es dann an *Verteiler C* oder *Verteiler D* weiterreichen würden, denen schließlich die Zustellung an A obläge. Der mehrfache Versand führt bei gegenständlichen Produkten naturgemäß zu einem bedeutenden Mehraufwand und dauert auch entsprechend länger.

Bei Kaufgeschäften ist Anonymität typischerweise besonders für Kunden interessant – niemand soll wissen, was gekauft wird. Was hingegen ein kommerzieller Anbieter offeriert und zu welchen Konditionen er verkauft, das wird im Kontrast dazu häufig mit Absicht publik gemacht und beworben. Angesichts dessen kann für anonyme Zahlvorgänge auch bei Anonymisierungsverfahren mit mehreren *Verteilern* eventuell darauf verzichtet werden, die letzte Transaktion an den Empfänger B versplittet von verschiedenen *Verteilern* durchführen zu lassen. In dem Verfahren mit vier *Verteilern* würden die Verteiler U und V durch

einen einzigen *Verteiler W* ersetzt. Gibt es nur einen letzten *Verteiler W*, erfährt *W* die Gesamthöhe der Zahlung. Dieser Betrag ist jedoch der Preis eines Produkts des Anbieters *B* oder einer Summe über die Preise mehrerer Produkte von *B* und mithin aufseiten des Kontos des Anbieters *B* keine Überraschung – erst recht kein großes Geheimnis.

Trotzdem gibt es auch für anonyme Bestellungen aus der Ferne Szenarien, in denen mehrere letzte Verteiler wünschenswert oder erforderlich sind, sofern keine einzelne Partei Möglichkeiten zur unentdeckten Manipulation haben soll. Das gilt etwa dann, wenn *B* ein Produkt nur an Personen einer bestimmten Gruppen *G* verkaufen darf. Gäbe es nur einen letzten *Verteiler*, könnte dieser einfach behaupten, für eine Person aus *G* zu bestellen. Deshalb sollte eine notwendige Bezeugung, ob *A* zu *G* gehört, unabhängig von mehreren letzten *Verteilern* in verschiedenen Misstrauensparteien eingefordert werden.

Eine weitere Anforderung, welche das anonyme Einkaufen erfüllen sollte und bei deren Umsetzung mehrere letzte *Verteiler* einen Mehrwert bieten können, ist die Möglichkeit, Rückmeldungen zu dem erstandenen Produkt geben zu können. Die Rückmeldung sollte anonym sein können, zugleich sollte sich aber belegen lassen, dass das beurteilte Produkt tatsächlich von der urteilenden Person käuflich erworben wurde. Die Meinung verifizierter Käufer hat eben eine andere Qualität, sie stammt zumindest nicht von Personen, welche das Produkt nicht selbst kennen, oder gar von Maschinen. Für die Übermittlung des Feedbacks kann wiederum das Netz der *Verteiler* verwendet werden, welche für die Anonymisierung der Transaktion verwendet werden. Die reliable Publikation der Rückmeldung folgt dabei genau der Kette der Verträge des Überweisungsvorgangs. Die Rückmeldung wird nur genau so weitergeleitet, wie die Transaktionen tatsächlich gelaufen sind. Kommen mehrere *Verteiler* zum Einsatz, so erhalten alle *Verteiler*, die nicht direkt an *B* überwiesen haben, nur einzelne Shares der Rückmeldung. Erst die letzten *Verteiler* setzen das Feedback zusammen. Durch die letzten *Verteiler* kann dann eine inhaltliche Prüfung der Rückmeldung auf Vereinbarkeit mit den Regeln des S-Netzwerks erfolgen. Einer der letzten *Verteiler* veröffentlicht das Feedback zu dem Angebot und die anderen bestätigen die Korrektheit oder sie widersprechen und melden dies, sodass nach dem Fehler gesucht werden kann.

EXEMPLARISCHE TRANSAKTIONSANONYMISIERUNGSDIENSTE FÜR DEN S-NETZWERK-DEMONSTRATOR

Um die Technik der anonymen Transaktionen mit dem S-Netzwerk demonstrieren zu können, wurden eigens voll automatisierte Anonymisierungsservices als *Verteiler* entwickelt. Ein solcher *Verteiler* ist ein eigener Server, der ein Client-Programm für den S-Netzwerk-Demonstrator steuert. Dieser Server wartet auf Aufträge zur Anonymisierung und führt diese soweit möglich durch. Die zu Demonstrationszwecken entwickelten Anonymisierungsdienste stellen keine eigene Netzwerkschnittstelle bereit, auf der sie eingehende Nachrichten empfangen. Stattdessen wird ausschließlich das S-Netzwerk zur Kommunikation genutzt, genauer wird einfach regelmäßig nach neuen S-Links auf einen Anker gesucht, mit welchen ein Auftrag initiiert werden kann.

Die S-Links bei den Anonymisierungsverfahren enthalten ausschließlich öffentlich zugängliche Daten – alle geheimen Informationen werden in den Aufträgen gespeichert, welche per Secret Sharing vor unbefugten Zugriffen geschützt werden.

In der Realität müssten Anonymisierungsdienste die gestückelten Weiterüberweisungen über lange Zeiträume verteilt durchführen, damit keine Zusammenhänge zwischen den Teiltransaktionen ersichtlich werden. Diese Zeiträume sollten zumindest in der Größenordnung von Tagen liegen. Beim Demonstrator lassen sich jedoch auch kurze Zeiträume (Minuten) festlegen, damit das Testen und Erproben erleichtert wird.

Die beispielhaften *Verteiler* für den S-Netzwerk-Demonstrator unterstützen bei Systemen mit offenen Konten (Tauschringe, *Jadwirtschaft*) sowohl anonyme Überweisungen als auch anonyme Kaufvorgänge mit Bestellung, Bezahlung und den notwendigen Informationen für eine Auslieferung entlang des Netzes der Anonymisierungsservices. Außerdem bieten sie Unterstützung für verlässliches anonymisiertes Feedback verifizierter Käufer.

4 VERZEICHNISSE

4.1 ABKÜRZUNGEN

ALLGEMEIN ÜBLICHE ABKÜRZUNGEN

bzw.	beziehungsweise
et al.	et alii / aliae / alia (und andere)
f.	folgende (eine)
ff.	folgende (mehrere)
GB	Gigabyte
ggf.	gegebenenfalls
KB	Kilobyte
MB	Megabyte
ms	Millisekunden
Prof.	Professor(in)
s	Sekunden
S.	Seite
u. a.	unter anderem
z. B.	zum Beispiel

SPEZIELLE ABKÜRZUNGEN UND SYMBOLE IN DER PUBLIKATION

A	Autorisierer
Σ	Änderungsliste
Γ	Zielpublikum
Δ	Gültigkeitszeitraum
Ξ	Intentionale Interpretation
Π	Herausgeber
T	Publikationszeitpunkt
Λ	Publikationsort
ε	endliche Zeit
Ψ	Threshold (Quorum)
\mathcal{P}	Misstrauenspartei / Misstrauensparteien

3.1 Abbildungsverzeichnis

Abbildung 1: Optimale Verteilung der Kopien von Shares mit $\Psi=2$ und verschiedenen Anzahlen #P von Misstrauensparteien.....	5
Abbildung 2: Darstellung von Lösungen mit dem Partitionsverfahren bei einem Threshold von $\Psi=4$	14
Abbildung 3: Mögliche Verteilungen der Kopien von Shares bei $\Psi = 3$	19
Abbildung 4: Vergleich zwischen einfachem (links) und vorausschauendem (rechts) partei-internen Routing beim Ausfall von S-Knoten W.....	20
Abbildung 5: Suche nach einem Bekannten von B in Pv beim parteigetreuen Weiterleiten	22
Abbildung 6: Multi-Partitions-Routing von A nach B mit $\Psi = 4$ und #P = 22.....	25
Abbildung 7: Validierung der Daten und Kommunikation von Alice mit S-Knoten B indirekt mithilfe des eigenen S-Knotens A als Proxy sowie direkt mit dem Zugangsgerät ZA im Parallelmodus.....	29
Abbildung 8: Gegenseitige Authentifikation mit einem sicheren Zugangssystem und $CZA = 7\#U3$	33
Abbildung 9: Teil des Verfahrens für anonyme Kommentare mit Weiterleitung bei $T=3$	38
Abbildung 10: Verfahren zur Anonymisierten Abstimmung mit Threshold 3.....	40
Abbildung 11: Entscheidungsdiagramm für die Auswertung von Abstimmungen.....	42
Abbildung 12: Performance der Evaluation einer anonymen Abstimmung mit Threshold 3	43
Abbildung 13: Abhängigkeit der Dauer der Analyse anonymer Abstimmungen vom Threshold.....	44
Abbildung 14: Phasen der Entwicklung des S-Netzwerks.....	46
Abbildung 15: Screenshot von mehreren Instanzen des NonNon-Editors im Demonstrator	80
Abbildung 16: Schema der Aktualisierung des NonNon-Editors mit Konfliktmanagement	81
Abbildung 17: Youtube Sperre (Screenshot von Johannes Viehmann).....	85
Abbildung 18: Umleitungsziel der GEMA-Seite nach dem Angriff (Screenshot von Johannes Viehmann).....	85
Abbildung 19: Protestvideo von Nina Paley gegen die Sperrung ihres Films auf Youtube in Deutschland, Screenshots von http://www.youtube.com/watch?v=LpTPTQ3e0Jg (2012-06-26).....	86
Abbildung 20: Auch gegenüber dem Empfänger anonyme Überweisung.....	96
Abbildung 21: Anonyme Transaktion mit Secret Sharing – Verträge.....	98
Abbildung 22: Anonyme Transaktion mit Secret Sharing – Geldtransfers.....	99

3.2 Tabellenverzeichnis

Tabelle 1: Nicht isomorphe bipartite Graphen erzeugende Verfahren im Vergleich.....	11
Tabelle 2: Unscharfe quasi kanonische Konstruktion für das S-Netzwerk Verteilungsproblem.....	12
Tabelle 3: Ausgewählte Lösungen für das S-Netzwerk Verteilungsproblem.....	17
Tabelle 4: Performance der Evaluation einer anonymen Abstimmung mit Threshold 3.....	43
Tabelle 5: Abhängigkeit der Performance der Analyse anonymer Abstimmungen vom Threshold.....	44
Tabelle 6: Speicherplatzbedarf auf den S-Knoten im Verhältnis zur effektiven Datenmenge.....	66
Tabelle 7: S-Netzwerk-Demonstrator Nachricht in UBF-Codierung.....	76

3.3 LITERATURVERZEICHNIS

- [Acketa 1991] Dragan M. Acketa, Zoran Budimac, Ratko Tomic: A Construction of Non-Isomorphic "Small" Bipartite Graphs; Mathematics Series, Volume 21, Number 2, S. 161-173; Univ. u Novom Sadu 1991; (2014-11-24)
http://www.dmi.pmf.uns.ac.rs/nsjom/Papers/21_2/NSJOM_21_2_161_173.pdf
- [Adams 2006] Keith Adams, Ole Agesen: A comparison of software and hardware techniques for x86 virtualization; Proceedings of the 12th international conference on Architectural support for programming languages and operating systems; ACM New York 2006; ISBN:1-59593-451-0 doi>10.1145/1168857.1168860 (2011-11-02)
<http://dl.acm.org/citation.cfm?doid=1168857.1168860>
- [Adrian 2011] Stephanie Adrian et al.: StEP Annual Report 2010; Solving the E-waste Problem(StEP) Initiative, United Nations University Bonn 2011; (2011-10-25)
http://www.step-initiative.org/pdf/annual-report/Annual_Report_2010.pdf
- [Angerer 2009] Gerhard Angerer et al.: Rohstoffe für Zukunftstechnologien, Fraunhofer IRB Verlag, Stuttgart 2009; ISBN: 978-3-8167-7957-5
- [Bagley 2008] Margo A. Bagley: The Need for Speed (and Grace): Issues in a First-Inventor-to-File World; Berkeley Technology Law Journal, Volume 23, Issue 3, S. 1035-1060; Boalt Hall School of Law, University of California at Berkeley 2008; (2013-05-30)
http://btlj.org/data/articles/23_3/1035-1061.pdf
- [BbgLWahlG 2004/2014] Landtag Brandenburg: Wahlgesetz für den Landtag Brandenburg (Brandenburgisches Landeswahlgesetz - BbgLWahlG) In der Fassung der Bekanntmachung vom 28. Januar 2004 (GVBl.I/04, [Nr. 02], S.30) zuletzt geändert durch Artikel 3 des Gesetzes vom 11. Februar 2014 (GVBl.I/14, [Nr. 07]); Brandenburg 2004/2014; (2016-02-01) <http://bravors.brandenburg.de/de/gesetze-212893>
- [Becke 2010] Anna-Luisa Becke: Der Einfluss der Pille auf den Wandel von Sexualität, GRIN Verlag 2010; ISBN: 978-3-640-73590-7
- [Bernard 2012] Andreas Bernard, Till Krause: Dem Amateur ist nichts zu schwör; Süddeutsche Zeitung Magazin Heft 24/2012, S. ; Süddeutsche Zeitung München 2012; (2012-07-09) <http://sz-magazin.sueddeutsche.de/texte/anzeigen/37685/1/1>
- [Blaich 1985] Fritz Blaich: Der Schwarze Freitag, Inflation und Wirtschaftskrise, Deutscher Taschenbuch Verlag München 1985; ISBN: 3-423-04515-9
- [Borchardt 1985] Knut Borchardt, Gerald D. Feldman (Hrsg.): Das Gewicht der Inflationsangst in den wirtschaftspolitischen Entscheidungsprozessen während der Wirtschaftskrise; Schriften des Historischen Kollegs, Kollequien 6, Die Nachwirkungen der Inflation auf die deutsche Geschichte, S. 233-260; R. Oldenburg Verlag München 1985; ISBN: 3-486-52221-3
- [Böttner 2011] Hellmut Böttner, Karsten Schischke, Nils F. Nissen: Carbon Footprinting of Information Technology Products based on ISO standards; 2011 IEEE International Conference on Consumer Electronics - Berlin (ICCE-Berlin), S. 291-295; IEEE 2011; Print ISBN: 978-1-4577-0233-4, Digital Object Identifier: 10.1109/ICCE-Berlin.2011.6031836 (2011-10-25) <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6031836>
- [Briegleb 2012] Volker Briegleb: GEMA legt im YouTube-Streit Berufung ein; Heise Zeitschriften Verlag Hannover 2012; (2012-06-19)
<http://www.heise.de/newsticker/meldung/GEMA-legt-im-YouTube-Streit-Berufung-ein-1580860.html>
- [Carnathan 1998] Sean T. Carnathan: Patent Priority Disputes – A Proposed Re-Definition of “First-to-Invent”; Alabama law review, Volume 49, Number 3, S. 755-815; University of Alabama 1998; ISSN: 0002-4279 (2013-05-29)

- <http://www.law.ua.edu/pubs/lrarticles/Volume%2049/Number%203/carnathan.pdf>
- [Coyle 2004] Andrew Coyle, Jean-Louis Antoine-Gregoire, The International Centre for Prison Studies, King's College London, University of London: CONDITIONS OF IMPRISONMENT IN EU MEMBER STATES AND THE CANDIDATE COUNTRIES; European Parliament Brussel 2004; PE 358.897 (2011-10-17) <http://www.pedz.uni-mannheim.de/daten/edz-ma/ep/04/iv2003-04-02-en.pdf>
- [Cremer 2003] Clemens Cremer et al.: Der Einfluss moderner Gerätegenerationen der Informations- und Kommunikationstechnik auf den Energieverbrauch in Deutschland bis zum Jahr 2010 – Möglichkeiten zur Erhöhung der Energieeffizienz und zur Energieeinsparung in diesen Bereichen (Kurzfassung); Fraunhofer ISI, Karlsruhe 2003; urn:nbn:de:0011-n-16181-26 (2011-10-26) <http://publica.fraunhofer.de/eprints/urn:nbn:de:0011-n-16181-26.pdf>
- [Daller 2010] Thomas Daller: Gema-Gebühren, Kindergärten klagen über "Geldschneiderei"; Süddeutsche Zeitung München 2010; (2012-06-13) <http://www.sueddeutsche.de/muenchen/erding/gema-gebuehren-kindergaerten-klagen-ueber-geldschneiderei-1.1022670>
- [Dannecker 2006] Martin Dannecker: Abschied von Aids; Zeitschrift für Sexualforschung, Volume 19, Issue 1, S. 63-67; Georg Thieme Verlag Stuttgart, New York 2006; DOI: 10.1055/s-2006-921528 (2013-06-24) <https://www.thieme-connect.com/ejournals/abstract/10.1055/s-2006-921528>
- [Dongarra 2011] Jack J. Dongarra: Performance of Various Computers Using Standard Linear Equations Software, (Linpack Benchmark Report); Netlib Repository at University of Tennessee and Oak Ridge National Laboratory 2011; (2011-10-21) <http://www.netlib.org/benchmark/performance.ps>
- [Drescher 2011] Stefan Drescher: Streit um Gema-Gebühren in Kindergärten beigelegt; Presse-Druck- und Verlags-GmbH Augsburg Allgemeine Online 2011; (2012-06-13) <http://www.augsburger-allgemeine.de/politik/Streit-um-Gema-Gebuehren-in-Kindergaerten-beigelegt-id14702476.html>
- [Dünkel 2009] Frieder Dünkel: International vergleichende Strafvollzugsforschung; Uni Greifswald, Veröffentlicht auch in: H.-J. Schneider (Hrsg.): Internationales Handbuch der Kriminologie. Band 2; de Gruyter Berlin 2009; (2011-10-19) http://www.rsf.uni-greifswald.de/fileadmin/mediapool/lehrstuehle/duenkel/Duenkel_Intern_StVollzForsch_HB_Schneider.pdf
- [Engelsing 1976] Rolf Engelsing: Wie viel verdienten die Klassiker? Zur Entstehung des Schriftstellerberufs in Deutschland; Neue Rundschau, 87. Jahrgang 1976 Erstes heft, S. 124-136; S. Fischer Verlag Berlin 1976;
- [Ernst 2011] Dagobert Ernst: „Musikpiraten“ wollen Kitas aus der Gema-Not befreien; WAZ New Media Essen 2011; (2012-06-12) <http://www.derwesten.de/politik/musikpiraten-wollen-kitas-aus-der-gema-not-befreien-id4659676.html>
- [EU 2012] EU Mitgliedsstaaten durch das Europäische Parlament, den Rat und die Kommission: Charta der Grundrechte der Europäischen Union; Amtsblatt der Europäischen Union, C 326, S. 391-407; EU, Vertragsabschluss in Straßburg 2012; ISSN: 1977-088X, DOI: 10.3000/1977088X.C_2012.326.deu (2016-02-01) <http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ:C:2012:326:TOC>
- [Europarat 1987] Mitgliedstaaten des Europarates: European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment; Council of Europe Strasbourg 1987; ETS No. 126 (2011-10-18) <http://www.cpt.coe.int/en/documents/ecpt.htm>
- [Fergusson 1975/2010] Adam Fergusson: When Money Dies, Original 1975 William

Kimber & Co. Ltd., used edition United States by PublicAffairs, Perseus Books Group 1975/2010; 987-1-58648-994-6

[Ferner 2010] Jens Ferner: Distributed Denial of Service (DDoS) Attacken: Strafbar oder nicht?; Anwaltskanzlei Ferner, Alsdorf 2010; (2012-06-19) <http://www.internetstrafrecht.com/distributed-denial-of-service-ddos-attacken-straftbar-oder-nicht/internet-strafrecht/internetstrafrecht/>

[Ferrie 2007] Peter Ferrie: Attacks on Virtual Machine Emulators; Symantec, Mountain View 2007; (2011-11-03) http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf

[Fisher-Ogden 2006] John Fisher-Ogden: Hardware Support for Efficient Virtualization; University of California, San Diego 2006; (2011-11-02) <http://cseweb.ucsd.edu/~jfisherogden/hardwareVirt.pdf>

[Fontana 2008] John Fontana: How Microsoft is going green; Network World, IDG (International Data Group), Framingham 2008; (2011-10-27) <http://www.networkworld.com/news/2008/010908-microsoft-green.html>

[Fourier 1820/1978] Charles Fourier, Übersetzung aus dem Französischen von Eva Moldenhauer: Aus der neuen Liebeswelt, Verlag Klaus Wagenbach Berlin 1820/1978; ISBN: 3-8031-2032-2

[Fourier 1829] Charles Fourier: Le Nouveau monde industriel et sociétaire, ou Invention du procédé d'industrie attrayante et naturelle distribuée en séries passionnées, Bossange père Paris 1829;

[Francis 2013] Andrew M. Francis: The Wages of Sin: How the Discovery of Penicillin Reshaped Modern Sexuality; Archives of Sexual Behavior, Volume 42, Issue 1, S. 5-13; Springer US 2013; DOI: 10.1007/s10508-012-0018-4 (2013-01-30) <http://link.springer.com/article/10.1007/s10508-012-0018-4>

[Freytag 2012] Bernd Freytag: Dollars aus der Chemiefabrik ; Frankfurter Allgemeine Zeitung 2012; (2012-10-25) <http://www.faz.net/aktuell/wirtschaft/wirtschaftsgeschichte-dollars-aus-der-chemiefabrik-11588671.html>

[Fritz 2005] Hermann Fritz, members of the Tsunami Research Center at the University of Southern California: Tsunami research; Georgia Tech Savannah 2005; (2011-10-21) <http://savannah.gatech.edu/cee/groups/tsunami/index.html>

[Fritsch 2012] Conrad Fritsch: Urheberrecht: Kreativität muss sich für Künstler auszahlen; Zeit Online Hamburg 2012; (2013-06-12) <http://www.zeit.de/kultur/musik/2012-05/musik-angebote-netz-sendelogik>

[Fuchs 2011] Ursula Fuchs (Chefredakteurin), Bernhard Preuss, Lothar Porwich et al.: Bevölkerungsschutz Magazin 3. Quartal 2011; Herausgegeben im Auftrag des Bundesministeriums des Innern vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Bonn 2011; (2011-10-20) http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Publ_magazin/bsmag_3_11.pdf

[GEMA 2012] GEMA Pressemitteilung: Statement zum ZPÜ-Tarif für USB-Sticks und Speicherkarten; GEMA – Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte Berlin, München 2012; (2012-06-18) <https://www.gema.de/presse/pressemitteilungen/presse-details/article/statement-zum-zpue-tarif-fuer-usb-sticks-und-speicherkarten.html>

[GG 1949/2010] Parlamentarische Rat der Bundesrepublik Deutschland : Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2010 (BGBl. I S. 944) geändert worden ist, Bundesgesetzblatt, online Version

- durch: Bundesministeriums der Justiz in Zusammenarbeit mit der juris GmbH 1949 / 2010;
- [Gimpel 2009] Volkmar Gimpel et al.: Johann Sebastian Bach und die Universität, in: 600 Jahre Alma mater Lipsiensis, Zur Geschichte der Universität Leipzig; Universität Leipzig 2009; (2013-06-13) <http://www.uni-leipzig.de/~agintern/uni600/ug151.htm>
- [Goldberg 1974] Robert P. Goldberg: Survey of virtual machine research; IEEE Computer Society 1974
- [Görlach 2010] Alexander Görlach: Netz läuft Sturm gegen Abzocke bei Weihnachtsliedern; Bild Digital Berlin 2010; (2012-06-13) <http://www.bild.de/politik/2010/politik/bei-weihnachtsliedern-14696978.bild.html>
- [Gruen 2004/2005] Sarah Gruen: The Chinese Monetary System: From Ancient Times to the Early Modern Period; Grove City College 2004/2005; (2013-06-18) http://www2.gcc.edu/dept/econ/assc/papers2005/chinamonetary_gruen.pdf
- [Gupta 2003] Maruti Gupta, Suresh Singh: Greening of the internet; SIGCOMM '03 Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications; ACM New York 2003; ISBN:1-58113-735-4 doi>10.1145/863955.863959 (2011-10-27) <http://doi.acm.org/10.1145/863955.863959>
- [Hardach 1976] Gerd Hardach: Weltmarktorientierung und relative Stagnation, Duncker und Humblot Berlin 1976; ISBN: 3-428-03675-1
- [Harrer 1965] Heinrich Harrer: Ich komme aus der Steinzeit, Deutsche Buch-Gemeinschaft Berliner Druck und Buchbinderei GmbH 1965;
- [Hilmes 2011] Oliver Hilmes: Liszt: Biographie eines Superstars, Siedler 2011; Print-ISBN: ISBN: 978-3-570-55170-7, eISBN: 978-3-641-05633-9
- [Hochert 2012] Judith Horchert, Marcel Rosenbach: Nach Gema-Attacke: Razzia trifft Anonymous-Mitläufer, Anonymous-Attacke gegen Gema führt zu Hausdurchsuchungen; SPIEGEL ONLINE GmbH, Hamburg 2012; (2013-06-05) <http://www.spiegel.de/netzwelt/netzpolitik/anonymous-attacke-gegen-gema-fuehrt-zu-hausdurchsuchungen-a-838656.html>
- [Hsu 2011] Chung-Hsing Hsu, Stephen W. Poole: Power Signature Analysis of the SPECpower_ssj2008 Benchmark; 2011 IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), S. 227-236; IEEE 2011; Print ISBN: 978-1-61284-367-4, Digital Object Identifier: 10.1109/ISPASS.2011.5762739 (2011-10-25) <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=05762739>
- [Huisman 2007] Jaco Huisman et al.: "2007 Review of Directive 2002/96 on Waste Electrical and Electronic Equipment (WEEE)", Final Report to European Commission; European Commission 2007; (2011-10-25) http://ec.europa.eu/environment/waste/weee/pdf/final_rep_unu.pdf
- [Iwan 2006] Wilfred D. Iwan and others: Great Sumatra Earthquakes and Indian Ocean Tsunamis of 26 December 2004 and 28 March 2005 ; Earthquake Engineering Research Institute Oakland
- [Jessen 2010] Elisabeth Jessen: Hamburger KITAS sollen fürs Singen teure Gebühren bezahlen, Hamburger Abendblatt Online am 27.12.2010; Axel Springer AG Hamburg 2010; (2012-06-12) <http://www.abendblatt.de/hamburg/article1738926/Hamburger-Kitas-sollen-fuers-Singen-teure-Gebuehren-bezahlen.html>
- [Jobs 2007 a] Steve Jobs: A Greener Apple; Apple, Cupertino 2007; (2011-10-27) <http://www.apple.com/hotnews/agreenerapple/>
- [Karp 1972] Richard M. Karp: Reducibility Among Combinatorial Problems; University of California at Berkeley 1972; (2011-07-07) <http://www.cs.berkeley.edu/~luca/cs172/karp.pdf>
- [Kaufmann 2010] Bruno Kaufmann, Rolf Büchi, Nadja Braun: The IRI Guidebook to

- Direct Democracy in Switzerland and beyond, Initiative & Referendum Institute Europe Marburg 2010; ISBN: 978-3-940716-03-3
- [Keiler 1986] Allan Keiler: Liszt and the Weimar Hoftheater; , S. 431-450; Akadémiai Kiadó 1986; (2013-06-11) <http://www.jstor.org/stable/902434>
- [Klieme 2011] E. Klieme, L. Strick, W. Wunderlich, J. Braun, A. Wiesmaier: Der elektronische Safe als vertrauenswürdiger Cloud Service; ISPART Hamburg 2011; (2015-02-10) http://www.isprat.net/fileadmin/downloads/pdfs/ISPRAT-Studie_Cloud-Safe_V1_20120121.pdf
- [Köbler 1993] Johannes Köbler, Uwe Schöning, Jacobo Torán: The graph isomorphism problem, Birkhäuser Boston 1993; 0-8176-3680-3
- [Kounatze 2009] Christian Reimsbach Kounatze: contributed to the OECD Conference on "ICTs, the environment and climate change", Helsingør, Denmark, 27-28 May 2009; OECD 2009; DOI 10.1787/222431651031 (2011-10-31) <http://www.oecd.org/dataoecd/47/12/42825130.pdf>
- [Kuhn 2012] Johannes Kuhn: Urteil im Gema-Streit, YouTube in der Filter-Falle; Süddeutsche Zeitung München 2012; (2012-06-19) <http://www.sueddeutsche.de/digital/urteil-im-gema-streit-youtube-in-der-filter-falle-1.1338111>
- [Lederer 1936] Max Lederer: Goethe und das Theater; Neophilologus, Volume 21, Issue 1, S. 202-212; Kluwer Academic Publishers 1936; Print ISSN: 0028-2677, DOI: 10.1007/BF01510117 (2013-06-11) <http://link.springer.com/article/10.1007/BF01510117>
- [LG Hamburg 2012] Landgericht Hamburg: Urteil vom 20. April 2012 - Az. 310 O 46110; openJur e.V. Hamburg 2012; (2012-06-26) <http://openjur.de/u/311130.html>
- [Lötscher 2008] Veronika Lötscher, Michael Matthies (Hrsg.): Humanarzneimittel in Gewässern am Beispiel der Steroidhormone; Neue Umweltproblemstoffe Oktober 2008, Beitrag Nr. 49, S. 11-21; Universität Osnabrück 2008; ISSN: 1433-3805 (2012-11-15) <http://www.usf.uos.de/usf/literatur/beitraege/texte/049-hauptseminar08.pdf#page=11>
- [LWG 2002/2011] Landtag Bayern: Gesetz über Landtagswahl, Volksbegehren und Volksentscheid (Landeswahlgesetz - LWG) in der Fassung der Bekanntmachung vom 5. Juli 2002 Zuletzt geändert am 25. Oktober 2011 (GVBl S. 506); 2002/2011; (2016-02-01) http://www.wahlen.bayern.de/lw/erster_teil.htm
- [Mann 1942/1975] Thomas Mann: Inflation: The Witches' Sabbath.; Encounter, Vol. XLIV, No. 2, February 1975, S. 60-63; Encounter Ltd. 1942/1975; (2012-10-23) <http://www.unz.org/Public/Encounter-1975feb-00060>
- [McFadyen 2007] Rebecca C.E. McFadyen: The First-to-File Patent System: Why Adoption Is Not an Option; Rich. J.L. & Tech. Volume XIV, Issue 1 (2007-2008), S. 1-63; HeinOnline 2007; (2013-05-30) <http://heinonline.org/HOL/LandingPage?collection=journals&handle=hein.journals/jolt14&div=17>
- [McKay 1981] Brendan D. McKay: Practical Graph Isomorphism; 10th. Manitoba Conference on Numerical Mathematics and Computing, Congressus Numerantium, 30 (1981), S. 45-87; Winnipeg, 1980 1981; (2015-01-14) <http://cs.anu.edu.au/~bdm/nauty/PGI>
- [McKay 1998] Brendan D. McKay: Isomorph-Free Exhaustive Generation; Journal of Algorithms, Volume 26, Issue 2, S. 306-324; ACM 1998; doi:10.1006/jagm.1997.0898 (2015-08-19) <http://www.sciencedirect.com/science/article/pii/S0196677497908981>
- [McKay 2014] Brendan D. McKay, Adolfo Piperno: Practical graph isomorphism, II; Journal of Symbolic Computation, Volume 60, January 2014, S. 94-112; Elsevier 2014; doi:10.1016/j.jsc.2013.09.003 (2014-11-24) <http://www.sciencedirect.com/science/article/pii/S0747717113001193>
- [McLuhan 1962/1967] Marshall McLuhan: the gutenbergs galaxy, Routledge & Kegan

Paul London 1962/1967;

[Meißner 2012] Malte Meißner, Interview mit Christian Hufgard: Pirat zu Urheberrechtsstreit: Künstler sollen von ihrer Kunst leben können; Verlag Der Tagesspiegel Berlin 2012; (2013-06-12) <http://www.tagesspiegel.de/medien/digitale-welt/pirat-zu-urheberrechtsstreit-kuenstler-sollen-von-ihrer-kunst-leben-koennen/6444028.html>

[MELANI 2011] Melde- und Analysestelle Informationssicherung MELANI: Informationssicherung - Lage in der Schweiz und international - Halbjahresbericht 2011/1; Informatikstrategieorgan Bund ISB, Nachrichtendienst des Bundes NDB, Schweiz 2011; (2015-01-07) <http://www.melani.admin.ch/dokumentation/00123/00124/01128/index.html?lang=de>

[Mühlbauer 2010] Peter Mühlbauer: Gema kassiert jetzt auch bei Kindergärten, Telepolis; Heise Zeitschriften Verlag Hannover 2010; (2012-06-12) <http://www.heise.de/tp/blogs/6/148618>

[Mühlbauer 2011] Peter Mühlbauer: Kindergarten-Gema über Pauschalvertrag?; Heise Zeitschriften Verlag Hannover 2011; (2012-06-13) <http://www.heise.de/tp/artikel/34/34247/1.html>

[Murugesan 2008] San Murugesan: Harnessing Green IT: Principles and Practices; IT Professional Jan.-Feb. 2008 Volume: 10 Issue:1, S. 24-33; IEEE Computer Society 2008; ISSN: 1520-9202, Digital Object Identifier: 10.1109/MITP.2008.10 (2011-10-27) <http://www.sis.pitt.edu/~dtipper/2011/GreenPaper.pdf>

[Nedeveschi 2008] Sergiu Nedeveschi, Lucian Popa, Gianluca Iannaccone, Sylvia Ratnasamy, David Wetherall: Reducing network energy consumption via sleeping and rate-adaptation, published in: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation; USENIX Association San Francisco 2008 2008; (2011-12-21) <http://www.usenix.org/event/nsdi08/tech/nedeveschi.html>

[Nelson 1980/1990] Theodor Holm Nelson: Literary Machines, Mindful Press, Sausalito CA 1980/1990;

[Neves 2010] Luis Neves et al.: Evaluating the carbon-reducing impacts of ICT; Global e-Sustainability Initiative (GeSI), Boston Consulting Group (BCG) 2010; (2011-10-25) <http://www.bcg.com/documents/file59352.pdf>

[Oppermann 2010] Karolin Oppermann, Maren Büttner (Hg.), Sabine Horn (Hg.): „Die Straße des Verderbens“ – Schwarzmarkt und Göttinger Nachkriegskriminalität; Alltagsleben nach 1945 : Die Nachkriegszeit am Beispiel der Stadt Göttingen, S. 31-56; Universitätsverlag Göttingen 2010; ISBN: 978-3940344816 (2013-06-18) <http://www.oapen.org/search?identifizier=400001;keyword=Alltagsleben%20nach%201945%20:%20Die%20Nachkriegszeit%20am%20Beispiel%20der%20Stadt%20G%C3%B6ttingen>

[PatG 1936/2011] Patentgesetz (PatG): Patentgesetz in der Fassung der Bekanntmachung vom 16. Dezember 1980 (BGBl. 1981 I S. 1), das zuletzt durch Artikel 13 des Gesetzes vom 24. November 2011 (BGBl. I S. 2302) geändert worden ist; Bundesministerium der Justiz, Berlin Deutschland 1936/2011; (2012-05-10) <http://www.gesetze-im-internet.de/bundesrecht/patg/gesamt.pdf>

[Paul VI. 1968] Giovanni Battista Enrico Antonio Maria Montini (Papst Paul VI.): Humanae Vitae; Vatikan 1968; (2012-11-16) http://www.vatican.va/holy_father/paul_vi/encyclicals/documents/hf_p-vi_enc_25071968_humanae-vitae_ge.html

[Pilecki 1943] Witold Pilecki, translated by Jacek Kucharski: Witold's Report; PRZYPOMNIJMY O ROTMISTRZU 1943/2008; (2011-10-18) <http://witoldsreport.blogspot.com/2008/05/volunteer-for-auschwitz-report-by.html>

- [Poess 2010] Meikel Poess, Raghunath Othayoth Nambiar, Kushagra Vaid, John M. Stephens Jr., Karl Huppler, Evan Haines: Energy benchmarks: a detailed analysis; Published in Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking; ACM New York 2010; ISBN: 978-1-4503-0042-1 doi>10.1145/1791314.1791336 (2011-10-31) <http://dl.acm.org/citation.cfm?doid=1791314.1791336>
- [Preisigke 1910/1971] Friedrich Preisigke: Girowesen im griechischen Ägypten, Georg Olms Verlag, Hildesheim, New York 1910/1971;
- [Pricop 2007] Florentina Pricop, Andreea Valter, Oana Chelemen: Prescribing oral contraceptives on cosmetic purpose in adolescents; Proceedings of the 18th World Congress on Fertility and Sterility (IFFS 2004), International Congress Series, Volume 1271 , S. 319-322; Elsevier 2007; DOI: 10.1016/j.ics.2004.05.081 (2012-11-16) <http://www.sciencedirect.com/science/article/pii/S053151310401115X>
- [Ramos 2012] Oscar Fernández Ramos: An algorithm for constructing all non-isomorphic bipartite graphs, published in: Graded Betti numbers of edge ideals; Universidad de Valladolid 2012; (2014-11-24) <https://uvadoc.uva.es/handle/10324/1769>
- [Reißmann 2011 2] Ole Reißmann: Internetseite außer Betrieb: Anonymous bestraft Gema für YouTube-Streit; SPIEGEL ONLINE GmbH, Hamburg 2011; (2013-06-05) <http://www.spiegel.de/netzwelt/netzpolitik/internetseite-ausser-betrieb-anonymous-bestraft-gema-fuer-youtube-streit-a-769347.html>
- [Rothe 1998] Wolfgang Rothe: Der politische Goethe: Dichter und Staatsdiener im deutschen Spätabsolutismus, Vandenhoeck und Ruprecht, Göttingen 1998; ISBN: 3-525-01220-9
- [Santelli 2006] John Santelli, Mary A. Ott, Maureen Lyon, Jennifer Rogers, Daniel Summers, Rebecca Schleifer: Abstinence and abstinence-only education: A review of U.S. policies and programs; Journal of Adolescent Health, Volume 38, Issue 1, S. 72-81; Elsevier 2006; DOI: 10.1016/j.jadohealth.2005.10.006 (2013-06-24) <http://www.sciencedirect.com/science/article/pii/S1054139X05004672>
- [Schabert 1972] Ina Schabert: Shakespeare-Handbuch, Alfred Kröner Verlag Stuttgart 1972; ISBN: 3520-38601-1
- [Schaberth 1969] Irmgard Schaberth: Gustav Mahlers Wirken am Hamburger Stadttheater; Die Musikforschung, 22. Jahrg., H. 4 , S. 443-456; Bärenreiter 1969; (2013-06-13) <http://www.jstor.org/stable/41116456>
- [Schilder 1952/2008] Maria Schilder: Die Kaurischnecke, Westarp Wissenschaften Hohenwarsleben 1952/2008; ISBN: 978-3-89432-535-0
- [Schleiden 1875/2012] Matthias Jacob Schleiden: Salz: seine Geschichte, seine Symbolik und seine Bedeutung im Menschenleben. Eine monographische Skizze (Nachdruck), SEVERUS Verlag Hamburg 1875/2012; ISBN: 978-3-86347-284-9
- [Schnurer 2012] Georg Schnurer: ZPÜ erhöht Abgaben auf USB-Sticks und Speicherkarten drastisch; Heise Zeitschriften Verlag Hannover 2012; (2012-06-13) <http://www.heise.de/newsticker/meldung/ZPUe-erhoeht-Abgaben-auf-USB-Sticks-und-Speicherkarten-drastisch-1583790.html>
- [Schönberg 1910] Arnold Schönberg: Probleme des Kunstunterrichts; Ernst Viktor Zenker, Wien; digitalisiert: Bibliothek des Arnold Schönberg Centers 1910
- [Schumacher 2016] Gerhard Schumacher: Vorwärts in die Vergangenheit: Durchblick durch einige "reichsideologische" Nebelwände, JMB Verlag 2016; ISBN: 978-3944342979
- [Shelton 2005] Tim Shelton, Art Manion: VMware NAT Service vulnerable to buffer overflow via FTP PORT/EPRT commands; US-CERT Security Operations Center, Department of Homeland Security, Washington 2005; (2011-11-03)

<http://www.kb.cert.org/vuls/id/856689>

[Skowroneck 2010] Tilman Skowroneck: Beethoven the Pianist (Musical Performance and Reception), Cambridge University Press 2010; ISBN: 978-0521119597

[Sobiraj 2011] Lars Sobiraj: Anonymous nimmt Webseite der GEMA vom Netz (Update); InQnet GmbH 2011; (2013-06-05) <http://www.gulli.com/news/16918-anonymous-nimmt-webseite-der-gema-vom-netz-update-2011-08-23>

[Solchenizyn 1968/1973] Alexander Solschenizyn, Elisabeth Mahler (Übersetzung aus dem Russischen), Nonna Nielsen-Sokkeby (Übersetzung aus dem Russischen): Der erste Kreis der Hölle, Fischer Taschenbuch Verlag Frankfurt am Main 1968/1973; ISBN: 3-436-01799 X

[Sommerfeld 1994] Christoph Sommerfeld: Gerätegeld Sichel: Studien zur monetären Struktur bronzezeitlicher Horte im nördlichen Mitteleuropa, De Gruyter 1994; ISBN-13: 978-3110129281

[Spark 2003] Nick T. Spark: A History of Murphy's Law, Periscope Film Los Angeles 2003/2006; ISBN 978-0978638894

[SPEC Power Committee 2010] SPEC Power Committee: Power and Performance Benchmark Methodology; Standard Performance Evaluation Corporation, Gainesvill 2010; (2011-10-25) http://www.spec.org/power/docs/SPEC-Power_and_Performance_Methodology.pdf

[StGB 1871/2012] Strafgesetzbuch (StGB): Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 5 Absatz 3 des Gesetzes vom 24. Februar 2012 (BGBl. I S. 212) geändert worden ist; Bundesministerium der Justiz, Berlin Deutschland 1871/2012; (2012-05-10) <http://www.gesetze-im-internet.de/bundesrecht/stgb/gesamt.pdf>

[Streller 2011] Sabine Streller, Klaus Roth: 50 Jahre Pille in Deutschland; Chemie in unserer Zeit, Volume 45, Issue 4, S. 270–291; Wiley, Weinheim 2011; ISSN: 0009-2851, DOI: 10.1002/ciuz.201100561 (2012-11-16) <http://onlinelibrary.wiley.com/doi/10.1002/ciuz.201100561/pdf>

[Talaber 2009] Richard Talaber (editor), Tom Brey, Larry Lamers (contributors): Using Virtualization to Improve Data Center Efficiency, WP 19; The Green Grid, Beaverton (Oregon) 2009; (2011-11-25) <http://www.thegreengrid.org/~media/WhitePapers/White%20Paper%2019%20-%20Using%20Virtualization%20to%20Improve%20Data%20Center%20Efficiency.pdf?lang=en>

[Thayer 1866-1917] Alexander Wheelock Thayer: Ludwig van Beethovens Leben, Band 1 bis 5, Breitkopf & Härtel, Leipzig 1866-1917;

[UN 1984] United Nations General Assembly: Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; Adopted and opened for signature, ratification and accession by General Assembly resolution 39/46 of 10 December 1984, New York 1984, entered into force 1987; (2011-10-18) <http://www2.ohchr.org/english/>

[UN 2002] United Nations General Assembly: Optional Protocol to the Convention against Torture and other Cruel, Inhuman or Degrading Treatment or Punishment ; Adopted on 18 December 2002 at the fifty-seventh session of the General Assembly of the United Nations by resolution A/RES/57/199, New York 2002, entered into force 2006; (2011-10-17) <http://www2.ohchr.org/english/>

[UNESCO 1954] Contract prepared with the help of UNESCO, in the name of "The High Contracting Parties": Convention for the Protection of Cultural Property in the Event of Armed Conflict with Regulations for the Execution of the Convention 1954; Deposited at UNESCO 1954; (2011-10-20) <http://unesdoc.unesco.org/images/0008/000824/082464mb.pdf>

- [UrhG 1965/2011] Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz): Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 2 Absatz 53 des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 3044) geändert worden ist; Bundesministerium der Justiz, Berlin Deutschland 1965/2011; (2012-05-10) <http://www.gesetze-im-internet.de/bundesrecht/urhg/gesamt.pdf>
- [USCongress 2012] 112th Congress of the USA: H.R. 1249 (enr) - An Act To amend title 35, United States Code, to provide for patent reform; U.S. Government Printing Office (GPO) 2012; (2013-05-29) <http://www.gpo.gov/fdsys/search/pagedetails.action?packageId=BILLS-112hr1249enr>
- [USEPA 2011] U.S. Environmental Protection Agency, Office of Resource Conservation and Recovery: Electronics Waste Management in the United States Through 2009; Prepared by ICF International for the U.S. Environmental Protection Agency, Washington 2011; (2011-10-25) <http://epa.gov/wastes/conserves/materials/ecycling/docs/fullbaselinereport2011.pdf>
- [USPA 2007] U.S. Patent Act: United States Code Title 35 - Patents; United States Patent and Trademark Office 2007; (2012-08-13) http://www.uspto.gov/web/offices/pac/mpep/consolidated_laws.pdf
- [Verhulst 2007] Jos Verhulst, Arjen Nijeboer, Mit einem Beitrag von Gerald Häfner, Übersetzung von Andreas Linke: Direkte Demokratie; Fakten, Argumente, Erfahrungen, Democracy International Brüssel 2007; ISBN: 9789078820024
- [Voirol 2011] Beatrice Voirol: Sich windende Wege: Ethnografie der Melo-Schnecke in Papua, Indonesien; Göttinger Beiträge zur Ethnologie Vol. 4, Universitätsverlag Göttingen 2011; ISBN: 978-3941875838
- [Vollmer 2012] Andreas Vollmer: Einfach gleichzeitig schreiben – Etherpad; cms-journal 35 / März 2012, S. 52-53; Humboldt-Universität zu Berlin 2012; (2013-05-27) <http://edoc.hu-berlin.de/cmsj/35/vollmer-andreas-52/PDF/vollmer.pdf>
- [Wilkens 2005] Andreas Wilkens: Bitkom warnt vor "deutschem Sonderweg" bei Urheberrechtsabgaben; Heise Zeitschriften Verlag Hannover 2005; (2012-06-13) <http://www.heise.de/newsticker/meldung/Bitkom-warnt-vor-deutschem-Sonderweg-bei-Urheberrechtsabgaben-160572.html>
- [Willis 2009] Robert R. Willis: International Patent Law: Should United States and Foreign Patent Laws be Uniform? An Analysis of the Benefits, Problems, and Barriers; North Carolina Journal of Law and Technology, Volume 10, Issue 2, S. 283-311; University of North Carolina 2009; (2013-05-29) http://www.ncjolt.org/sites/default/files/Willis_Robert_v10i2_283_312_0.pdf
- [Wittmann 1991] Reinhard Wittmann: Geschichte des deutschen Buchhandels, Verlag C. H. Beck München 1991; ISBN: 3-406-35425-4
- [Wollinger 2003] Thomas Wollinger, Christof Paar : How Secure Are FPGAs in Cryptographic Applications; Lecture Notes in Computer Science Volume 2778, S. 91-100; Springer 2003; Print ISBN: 978-3-540-40822-2; DOI 10.1007/978-3-540-45234-8_10 (2015-02-10) http://link.springer.com/chapter/10.1007/978-3-540-45234-8_10
- [Świerczek 2008] Lidia Świerczek: Biography Rotamaster Witold Pilecki; Muzeum of Wola 2008; (2011-10-18) <http://www.pilecki.ipn.gov.pl/portal.php?serwis=rpe&dzial=1025&id=8193&poz=5>