Anwendungspotenziale der Nanotechnologie im Bereich der Informations- und Kommunikationstechnik

Gutachten

im Auftrag des Deutschen Bundestags

vorgelegt dem Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag

Michael Friedewald

Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI)
Breslauer Straße 48
76139 Karlsruhe

März 2003

Projektteam:

Dr.-Ing., Dipl.-Wirt.Ing. Michael Friedewald (Projektleitung)
Dipl.-Ing. (FH) Alexander Rothhaas
Peter Zoche M.A.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Ausgangslage

Auf Grund der vielfältigen Anwendungsbereiche wird der Nanotechnologie ein erhebliches Problemlösungspotenzial in Hinblick auf ein besseres Verständnis der Natur, auf Fortschritte in der Grundlagenforschung, auf neuartige Produktionstechniken, auf die ökonomische Leistungs- und Wettbewerbsfähigkeit, auf Herausforderungen im Gesundheitswesen und im Umweltschutz sowie Beiträgen zur Nachhaltigkeit zugemessen.

Als besonders wichtige Einsatzbereiche der Nanotechnologie werden die Mikroelektronik sowie die darauf aufbauende Informations- und Kommunikationstechnik eingestuft. Anwendungspotenziale werden hier vor allem im Bereich der Miniaturisierung und der Entwicklung neuer Bauelemente sowie in der Möglichkeit zur Realisierung neuer Computerkonzepte gesehen. Dies war Gegenstand des im Juni 2002 dem TAB vorgelegten Gutachtens über „Nanotechnologie im Bereich der Informations- und Kommunikationstechnik" (Friedewald et al. 2002). Darüber hinaus wird erwartet, dass sich darauf aufbauend auch neue Anwendungspotenziale ergeben.

Umso wichtiger ist es, die Möglichkeiten und Potenziale der Nanotechnologie in der Informations- und Kommunikationstechnik auszuloten. Dabei besteht noch erheblicher Gestaltungsbedarf in Hinblick auf Entwicklungsrichtungen, Rahmenbedingungen und Voraussetzungen, unter denen sich diese Entwicklung vollziehen soll. Wenn auch das Wissen in der Nanotechnologie international generiert wird, so ist doch die Umsetzung dieses Wissens in die industrielle Praxis und die Festlegung von Rahmenbedingungen, unter denen dies geschieht, weitgehend national geprägt. Hierfür ist fundiertes Orientierungswissen über kurz-, mittel- und langfristig realisierbare sowie visionäre Optionen der Nanotechnologie und ihrer möglichen Folgen erforderlich.

1.2 Ziel dieser Studie

Ziel dieser Studie ist es, die im Rahmen des Gutachtens „Nanotechnologie im Bereich der Informations- und Kommunikationstechnik" gewonnenen Ergebnisse, die sich vor allem auf den Bereich der nanoelektronischen Bauelemente und auf Nano-

technologie basierender Systemarchitektren konzentrierten, um entscheidende Anwendungsaspekte zu erweitern.

Dazu wurden exemplarisch drei Bereiche untersucht, in denen nach möglichen Anwendungspotenzialen gefragt wurde:

- Welche neuen Anwendungen ergeben sich aus den Eigenschaften *neuer nanotechnologischer Werkstoffe* im Bereich der IuK-Technik? Dabei stehen die lichtemittierenden bzw. (halb)leitenden Polymere sowie deren Anwendung für Polytronics und innovative Displays im Vordergrund.
- Welche Anwendungspotenziale ergeben sich durch die *Allgegenwart informationstechnischer Systeme*, wie sie unter den Schlagworten „Ubiquitous Computing" und „Ambient Intelligence" diskutiert werden und die erst durch die extreme Verkleinerung nanoelektronischer Bauelemente und Systeme realisierbar werden?
- Wie ist das Anwendungspotenzial der *Quanteninformationsverarbeitung* einzuschätzen? Dabei soll ein besonderer Fokus auf die krypografischen Verfahren gelegt werden, denen bereits mittelfristig ein Anwendungspotenzial für die sichere Telekommunikation prophezeit wird.

Diese drei Anwendungsbereiche der Nanotechnologie werden im Folgenden charakterisiert, ihre voraussichtliche künftige Entwicklung abgeschätzt und ihre Wechselwirkung mit dem Stand der aktuellen Forschungen hinsichtlich einer fördernden oder hemmenden Wirkung bewertet.

2 Nanotechnologische Displaytechnologien

IuK-Technologien und insbesondere audiovisuelle Medien brauchen vor allem eines: Bildschirme. Neueste Untersuchungen haben ergeben, dass allein in Deutschland momentan fast 55 Mio. Fernseher und über 20 Mio. Computer installiert sind, die mit einem Display ausgestattet sind (Cremer et al. 2003). Dies deutet an, dass es sich bei Markt für neue Displaytechnologien um einen Markt mit riesigem Potenzial handelt. Luther et al. (2002) schätzen allein das Marktvolumen für Flachdisplays bereits für das Jahr 2002 auf 31 Mrd. US$. Für 2005 erwartet das Marktforschungsinstitut DisplaySearch (2002) bereits ein Marktvolumen von 3,3 Mrd. US$.

Eine der wichtigsten zukünftigen Displaytechnologien basieren auf organischen Leuchtdioden (Organic Light Emitting Diodes, OLEDs). 1979 entdeckte der Kodak-Wissenschaftler Chin Tang während seiner Arbeiten mit Solarzellen ein blaues Abstrahlen des verwendeten organischen Materials. Acht Jahre später konnte er mit seinem Kollegen van Slyke erstmals Elektrolumineszenz an sehr dünnen organischen Multischichten bei niedrigen Einsatzspannungen von unter 10 Volt aufzeigen. Dies forcierte eine weltweite intensive Forschung, die 1990 zur Entdeckung der Elektrolumineszenz in Polymeren und innerhalb von zehn Jahren zu ersten Anwendungen führte. Heute arbeiten Entwickler aller wichtigen Elektronikunternehmen sowie eine ganze Reihe von jungen Technologieunternehmen an der Entwicklung von OLED-Displays (vgl. Tabelle 1), deren Anwendungsspektrum vom Fernseher bis neuartigen mobilen IuK-Endgeräten reichen wird. Aus Deutschland sind insbesondere Siemens bzw. Infineon, Schott und Osram Semiconductors sowie das Startup-Unternehmen Covion Organic Semiconductors die wichtigsten Akteure in diesem Technologiefeld.

2.1 Funktionsprinzip von organischen LEDs

Eine prototypische OLED besteht aus wenigen Schichten, die in aufwendigen Verfahren übereinander aufgebracht werden können. Zwei verschiedene Strategien werden hier verfolgt. Pionier Kodak setzt bei der Herstellung ihrer so genannten „Small Molecule OLEDs“ auf eine Technik, bei der die organischen Schichten in Vakuumatmosphäre auf das Trägermaterial aufgedampft werden. Ein von der Cambridge Display Technology entwickeltes Verfahren (PolymerLED) verfolgt einen etwas anderen Ansatz, bei dem das in Flüssigkeit gelöste organische Material durch Spin-Coating oder eine Art Tintenstrahldruck aufgebracht werden. Beide Verfahren sind noch relativ teuer, und etwa 95 % der organischen Substanz geht während des Prozesses verloren. Displays aus PolymerLEDs sind hinsichtlich der Bildqualität

heute noch etwas schlechter als solche aus „Small Molecule OLEDs", versprechen aber deutlich geringere Fertigungskosten in der Massenproduktion (Niesing 2002).

Tabelle 1: Ausgewählte industrielle Akteure bei Organischen Displays und Herstellungsverfahren

Land	Unternehmen	Small Molecules LEDs	Polymer LED
Großbritannien	Cambridge Display Technology		xx
Deutschland	Covion	x	xx
	Siemens	x	xx
Niederlande	Philips		xx
USA	Uniax		x
	Eastman-Kodak	xx	
	Universal Display Technologies	xx	x
	Lucent Technologies		xx
	Fed Corp.	xx	
Japan	Pioneer	xx	
	NEC	xx	
	TDK	xx	
	Mitsubishi	xx	x
	Stanley	xx	x
	Sanyo	xx	
	Idemitsu	xx	
Korea	Lucky Goldstar	xx	

Quelle: Le Barny et al. 2000

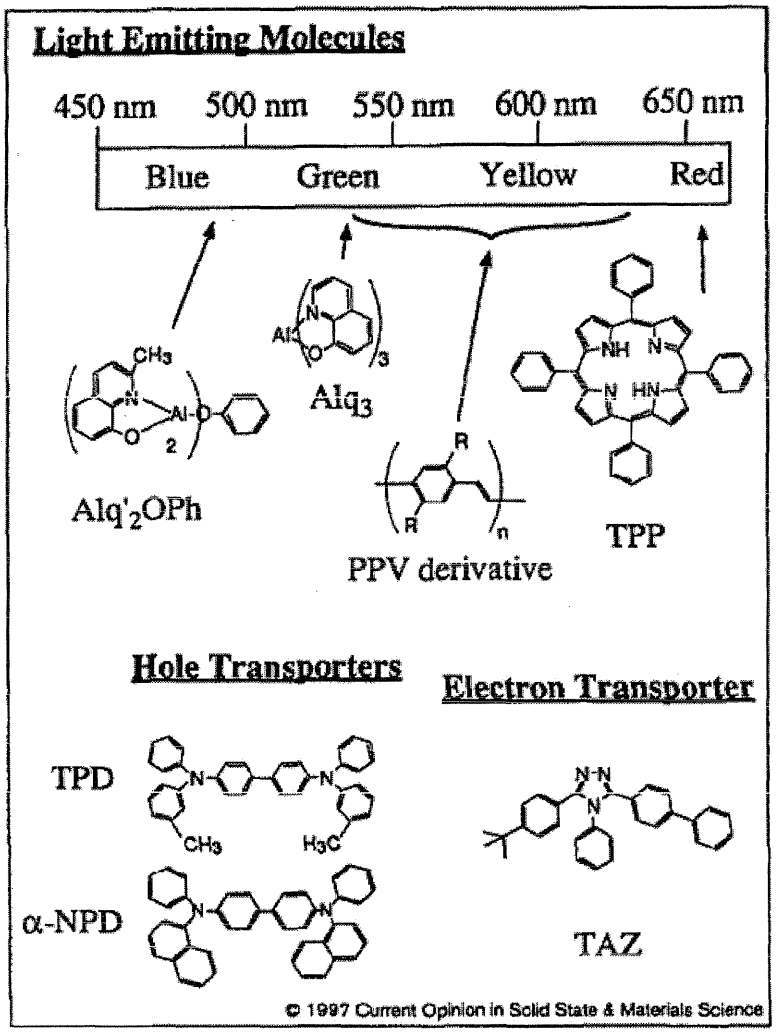
Die Auswahl des Substrats ist vielfältig und bestimmt den späteren Einsatzzweck des Displays maßgeblich. So kann neben einem starren Trägersubstanz wie Glas auch flexible und durchsichtige Materialien aus Polyethylen verwendet werden. Sie beeinflussen die Wirkungsweise nicht.

Auf das Substrat wird zunächst die Anode gesputtert (vgl. Abbildung 1 und 2).[1] Hierfür kann optisch transparentes Indium-Zinn Oxid verwendet werden. Darüber wird eine dünne Schicht aus Kupferphthalocyanin aufgebracht, die als Elektronenbarriere dient. Das folgende Hole Transport Layer (HTL) besteht aus Naphtaphenylbenzid (NPB). Die eigentlich Licht emittierende Schicht aus dotiertem Alq3 (Aluminiumoxinat) hat eine Dicke von nur 35 nm. Darauf wird eine weitere Schicht

[1] Der Begriff *Sputtern* ist an den englischen Begriff *sputtering* angelehnt und bezeichnet das Kathodenzerstäuben bzw. im weiteren Sinne auch die Sputterdeposition des zerstäubten Materials auf ein Substrat. Sputtern ist ein weit verbreitetes und sicheres Verfahren zur Herstellung hochwertiger Schichtsysteme mit hoher Packungsdichte, niedrigsten spezifischen Widerständen und ggf. geringsten optischen Verlusten.

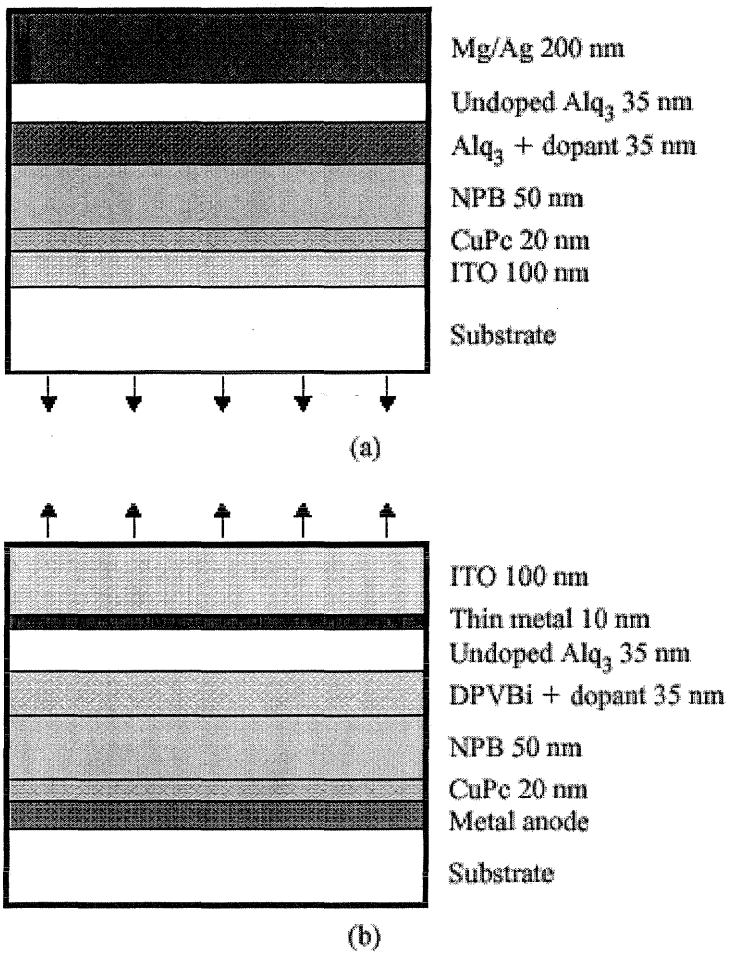
undotiertes Alq3 aufgebracht, die als Electron Transport Layer fungiert. Abschließend wird die Kathode aus Magnesium oder Silber aufgebracht (Howard und Prache 2001).

Abbildung 1: Verschiedene OLED-Basismaterialien und ihre Emissionswellenlänge



Die Dicke der eigentlichen Diode beträgt nur wenige hundert Nanometer. Legt man einen Spannung an, werden positive und negative Ladungsträger, die an den jeweiligen Elektroden injiziert werden, in einer Emissionsschicht zur strahlenden Rekombination gebracht.. Die Ladungsführung durch zusätzliche Schichten in den Transportlagen ermöglicht eine bessere Einstellung des Potenziale und dabei eine größere Präzision bei der Zusammenführung der Ladungsträger.

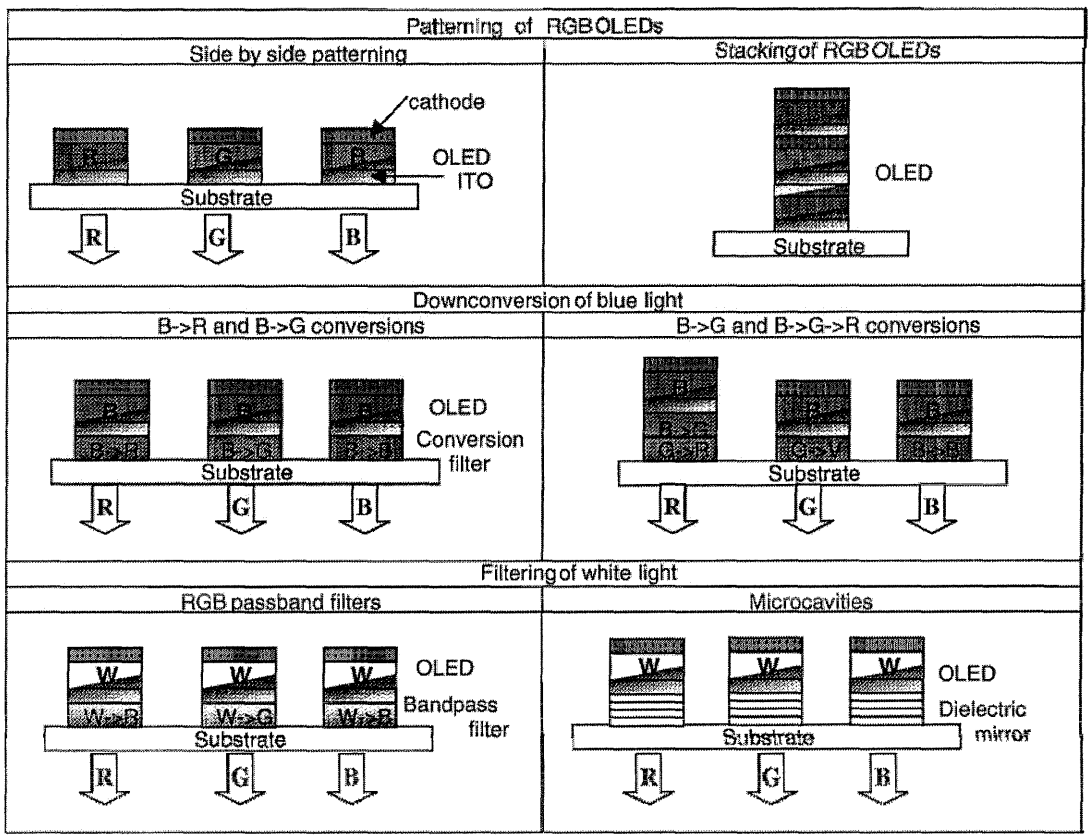
Abbildung 2: Schematischer Aufbau einer einfachen OLED
a) grüne Emission b) weiße Emission



Quelle: Howard und Prache 2001

Zur Herstellung vollfarbiger Displays werden verschieden Ansätze verfolgt (vgl. Abbildung 3) , die auch vom Herstellungsverfahren abhängig sind. In einem Pixel können die OLEDs für die Grundfarben nebeneinander oder gestapelt platziert werden. Dabei kommen Schattenwurfmasken zum Einsatz. Ausgehend von blauen O-LEDs können die RGB-Farben durch Abwärtskonversion erzeugt werden. Umgekehrt ist es möglich, aus dem Licht weißer OLEDS durch Bandpass-Filter oder dielelektrische Spiegel die drei Grundfarben zu erzeugen (Le Barny et al. 2000).

Abbildung 3: Verschiedene Möglichkeiten der Farberzeugung



Quelle: Le Barny et al. 2000

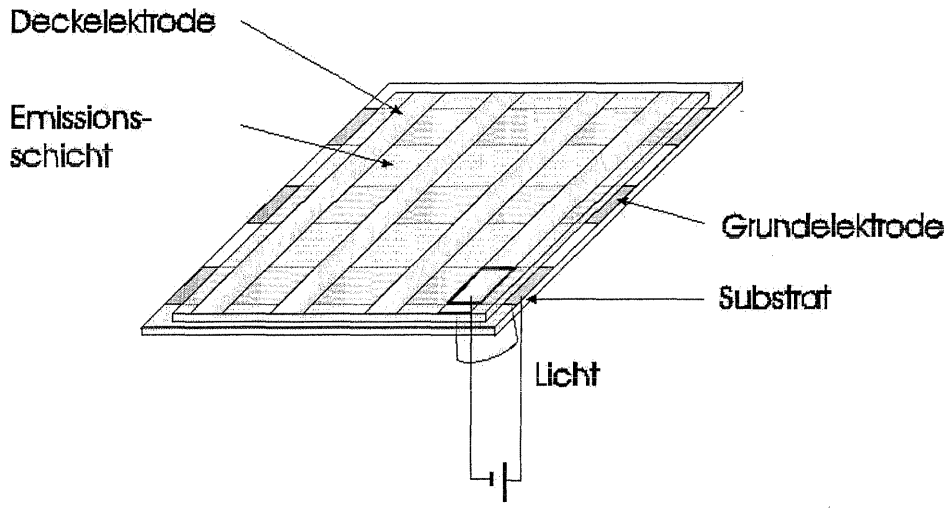
2.2 Vor- und Nachteile von OLED-Displays

Obwohl das prinzipielle Verfahren weit entwickelt ist und bereits erste Produkte: auf dem Markt angeboten werden, hat die OLED-Technologie immer noch mit einigen Kinderkrankheiten zu kämpfen: So verlieren das für die Farbe Blau verwendeten Polymer (Polyfluoren) durch Alterung bereits nach kurzer Zeit seine Leuchtkraft. Sämtliche leuchtenden Polymere dürfen weder mit Wasser noch mit Luftsauerstoff in Berührung kommen, da sich sonst ihre Leuchtkraft verschlechtert. Aus diesem Grunde wurden die OLEDs bisher überwiegend hinter Glas verkapselt. Für flexible Displays wird derzeit an Verfahren zum Aufbau von OLEDs auf PET-Folien gearbeitet. Insgesamt stellen OLEDs sehr hohe Anforderungen an die Synthese der Grundmaterialen, insbesondere an die Strukturreinheit und die Reinheit von Fremdstoffen.

Die Verdrahtung von OLED-Displays erfolgt heute noch auf herkömmliche Weise (Abbildung 4). Dies hat zur Folge, dass neben dem eigentlichen Display eine zusätzliche Platine mit der Ansteuerungselektronik benötigt wird. Es wird aber daran

gearbeitet, auch diese Ansteuerelektronik mit Hilfe polytronischer Bauelemente, d.h. mit Hilfe halbleitender Kunststoffe, zu realisieren. Auf diese Weise sollte es möglich sein, die komplette Steuerelektronik des Displays und langfristig sogar einen ganzen Computer auf der Rückseite der gleichen Folie aufzubringen, auf der auch das OLED-Display aufgebaut ist. So könnten langfristig flexible Computer mit einer Dicke von nur wenigen Millimetern realisierbar werden.

Abbildung 4: Prinzipieller Aufbau eines OLED-Displays



Quelle: http://www.ifw-dresden.de

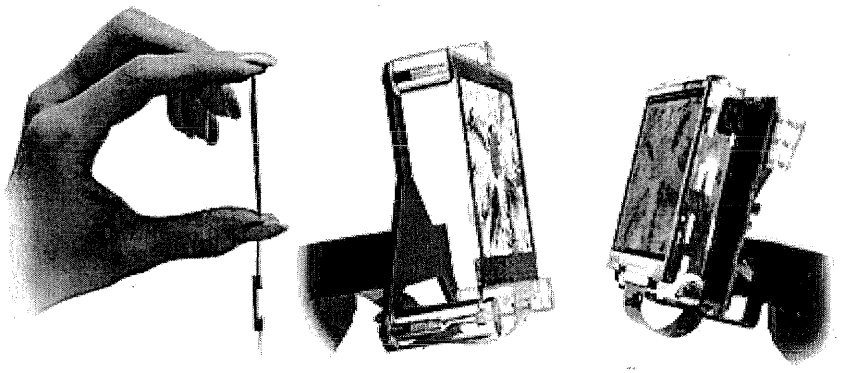
Insgesamt haben OLED-Displays gegenüber herkömmlichen Bildschirmen eine ganze Reihe von Vorteilen:

- OLEDs sind selbst leuchtend, brauchen also keine Hintergrundbeleuchtung. Deswegen haben OLED-Displays schon heute eine deutlich geringere Einbautiefe als herkömmliche Flachbildschirme,
- OLEDs bieten aus einem sehr großen Blickwinkel (bis zu 170 Grad) ein gleichmäßig brillantes Bild,
- wegen der geringe Schaltzeiten eignen sich OLED-Displays auch für die Darstellung von Filmen und anderen Multimedia-Inhalten
- OLED-Displays verbrauchen deutlich weniger Energie und
- lassen sich in hauchdünnen Schichten auf beliebig große Flächen auftragen. Dadurch lassen sich sowohl aufrollbare als auch wandgroße Displays realisieren.

2.2 Anwendungen

OLED-Kleindisplays haben schon vor einiger Zeit Serienreife erlangt. So hat Pioneer bereits 1999 ein monochromes OLED-Display für Autoradios vorgestellt, und Motorola bracht im Jahr 2000 ein erstes Mobiltelefon mit einem farbigen OLED-Display auf den Markt. Die in Abschnitt XX.2 aufgeführten Eigenschaften lassen eine Vielzahl von verschiedenen Anwendungen im Displaybereich möglich erscheinen. Die geringe Leistungsaufnahme und geringe Einbautiefe prädestinieren sie für einen Einsatz in allen mobilen Kommunikationsgeräten wie Handy oder PDA (Abbildung 5). Die meisten Hersteller von Mobiltelefonen bzw. deren Zulieferer sind deshalb bei der Entwicklung und Nutzung von OLED-Kleindisplays aktiv (neben Motorola, insbesondere Kodak und Sanyo).

Abbildung 5: Links und Mitte: OLED-Display. Rechts im Vergleich ein LCD-Modul



Quelle: http://www.c2s.de/funklehrgang/fernsehen/neuetechnologien.htm

Flexible Displays aus mikrometerdünner Folie könnten im Kugelschreiber oder im Laptopscharnier aufgewickelt liegen und bei Bedarf ausgerollt werden (Abbildung 6). Auf diese Weise ließe sich beispielsweise eine drahtlos übermittelte, federleichte und hochaktuelle elektronische Zeitung realisieren, die heutigen Verfahren des elektronischen Papiers Konkurrenz machen. Außerdem sind solche Displays ein Kernelemente von allgegenwärtigen informationstechnischen Systemen (vgl. Kapitel 3).

Auch bei Projektoren sind Geräte mit OLED-Technologie in der Entwicklung. So hat Siemens den Prototypen eines streichholzschachtelgroßen Tageslichtprojektor entwickelt, der auf ein Mobiltelefon aufgesteckt und zur Präsentation in Besprechungen oder zum Internet-Surfen mit dem Handy genutzt werden kann. Im Aufsteckmodul beleuchtet ein LED-Array über einen Strahlteiler ein Mikrodisplay, das dem Licht die Bildinformation aufmoduliert. Ein solcher „Mini-Beamer" kann nach Angaben des Herstellers auf jede Fläche projizieren und erreicht heute einen Lichtstrom, der dazu ausreicht, eine postkartengroße Fläche auszuleuchten. Nach Ein-

schätzung der Industrie ist mit optimiertem Design und lichtstärkeren Leuchtdioden innerhalb von zwei Jahren allerdings eine zehnmal größere Leistung erreichbar (Otten 2002)

Abbildung 6: Designmuster eines flexiblen, aufrollbaren Displays der Zukunft

Quelle: Siemens

Geringes Nachleuchten und schnelle Schaltzeiten ermöglichen Multimediaanwendungen, insbesondere großformatige Flachfernseher, die wie Bilder an der Wand hängen. Es ist allerdings zu erwarten, dass sich solche Geräte erst sehr langsam – vermutlich erst deutlich nach 2010 – in der Breite durchsetzen werden. Grund hierfür ist die große installierte Basis an herkömmlichen Fernsehern und die anfangs sehr hohen Preise für Großbildfernseher mit Flachdisplays, die erst allmählich auf das für die Konsumenten akzeptable Niveau sinken werden (vgl. Cremer et al. 2003).

Auch die Entwicklung neuer und leichterer Head-Mounted-Displays ist mit Hilfe der OLEDs möglich. So bietet die amerikanische Firma eMagin erste Mikrodisplays für Videobrillen her. Solche Displays haben eine Vielzahl von Anwendungen im kommerziellen und militärischen Bereich. Dazu gehören Visualisierungen in der Architektur und Medizin, Fernwartung und Prozesskontrolle, Navigations- und Flugleitsysteme, aber auch das „Digital Battlefield". Zunehmend werden 3D-Technologien auch für Heimanwendungen genutzt. Dazu zählen vor allem Spiele mit dreidimensionaler Grafik, u. a. auch für mobile Endgeräte wie PDAs und Mobiltelefone.

Wie auch andere Technologien im Monitorbereich müssen sich OLED-Displays mit den Referenzeigenschaften der Kathodenstrahlröhre messen. Wird ein durchsichti-

ges oder flexibles Substrat verwendet, besitzt die OLED-Technologie aber deutlich über die Eigenschaften der konventionellen Technologie hinaus und erschließt neue Anwendungsfelder, von der intelligenten Fensterscheibe bis zum aufrollbaren Bildschirm.

2.4 Weitere nanotechnologische Displaytechnologien

Die Herstellung flacher und Energie sparender Displays erscheint auch auf der Basis von Kohlenstoff-Nanoröhren möglich. Im Gegensatz zu den OLED-Displays handelt es sich dabei allerdings um „Feldemissions-Displays" (FED), die in ihrer Funktionsweise herkömmlichen Kathodenstrahlröhren ähneln. Unter Feldemission versteht man den Austritt von Elektronen aus einem elektrischen Leiter ins Vakuum in Gegenwart einer geeignet hohen Feldstärke. Solche Feldemissionen können u. a. durch Kohlenstoff-Nanoröhren realisiert werden.

Da Kohlenstoff-Nanoröhren bei Raumtemperatur eine mit Metallen vergleichbare Leitfähigkeit haben, können sie als Feldemitter genutzt werden. Wird eine Spannung an sie angelegt, emittieren sie aufgrund ihres geringen Durchmessers sehr effektiv Elektronen. Choi et. al. (1999) ist es kürzlich am Samsung Advanced Institute of Technology in Korea gelungen ein solches flaches, lichtstarkes Display zu bauen.

Nach Einschätzung von Fachleuten ist die Entwicklung von Feldemissions-Displays angesichts der Fortschritte bei den OLEDs etwas in den Hintergrund getreten, wichtige Pioniere in diesem Feld (z. B. Motorola) haben ihre Aktivitäten sogar ganz eingestellt. Diese Entwicklung ist auch vor dem Hintergrund zu sehen, dass FEDs ursprünglich die Lücke zwischen den relativ kleinen LCD-Displays und den sehr großen Plasmadisplays schließen sollten. Insbesondere durch die Fortschritte bei den LCD-Displays ist diese Lücke mittlerweile deutlich kleiner geworden (Pribat 2002).

Darüber hinaus sind FEDs auf der Basis von Kohlenstoff-Nanoröhren noch nicht über den Status der Grundlagenforschung hinaus. Eine Marktreife ist innerhalb der nächsten 5 Jahre kaum zu erwarten. Inwieweit sich FEDs dann gegen alternative, heute bereits sehr viel weiter entwickelte Technologien wie OLED-Displays werden durchsetzen können, bleibt unsicher.

3 Allgegenwärtige informationstechnische Systeme und Nanotechnologie

Der Topos der allgegenwärtigen Informationsverarbeitung (Ambient Intelligence, Ubiquitous Computing) beschreibt die Allgegenwärtigkeit von kleinsten, miteinander drahtlos vernetzten Computern. Entscheidend ist dabei, dass sie unsichtbar in beliebige Alltagsgegenstände eingebaut oder an diese angeheftet werden können. Damit wird die Möglichkeit geschaffen, mit Hilfe von Sensoren die Umwelt eines Gegenstandes zu erfassen. Diese mit Informationsverarbeitungs- und Kommunikationsfähigkeiten ausgestatteten Gegenstände werden in die Lage versetzt zu „wissen", wo sie sich befinden, welche anderen Gegenstände in der Nähe sind und was in der Vergangenheit mit ihnen geschah.

„Smart devices" und die umfassende Informatisierung und Vernetzung fast beliebiger Dinge des Alltages werden in den kommenden Jahren aus technischer Sicht tatsächlich realisierbar. Die Tendenz geht weg vom PC und dem Computer als Werkzeug, hin zum „computing without computers". Dabei soll der Mensch in unaufdringlicher Art bei seinen Arbeiten und Tätigkeiten unterstützt und von lästigen Routinearbeiten weitgehend befreit werden (Gershenfeld 1999, Weiser 1991).

Wir befinden uns bereits mitten in diesem Trend „alles, immer, überall": Das Internet wird mobil zugreifbar, und auf dem Markt tauchen immer mehr persönliche „information appliances" wie drahtlos vernetzte PDAs, Internetfähige Handys oder elektronische Bücher und Reiseführer auf. Während es sich bei diesen Geräten im allgemeinen um Computer handelt, die überall mit hingenommen werden können, meint der Begriff des Ubiquitous Computing genauer, die Einbettung informationstechnologischer Anwendungen in Umgebungen und Abläufe, mit dem Ziel, dass Informationstechnologie überall vorhanden ist. Dieser Definition entsprechen bereits heute Informationstechnologien, die in Haushaltsgeräten, Steuerungen und Leitsystemen Verwendung finden. Sie sind dort für den Anwender weitgehend unsichtbar eingebettet.

Neue Entwicklungen in der Mikroelektronik und den Materialwissenschaften (z.B. Miniatursensoren, „leuchtendes Plastik", „elektronische Tinte") und Fortschritte der Kommunikationstechnik (insbesondere im drahtlosen Bereich) tragen dazu bei, dass es bald kleinste und spontan miteinander kommunizierende Rechner im Überfluss geben kann. In Form von nanoskaligen Bauelementen, neuartigen Werkstoffen (z. B. für Displays) oder bislang nicht realisierbaren Bio-Sensoren ist die Nanotechnologie eine der entscheidenden Faktoren in dieser Entwicklung.

Die futuristisch-idealistisch erscheinende Vision des Ubiquitous Computing, bei der zur „Verbesserung der Welt" Alltagsdinge mit Kommunikations- und Informations-

verarbeitungsfähigkeit angereichert und mit neuen Nutzungsschnittstellen ausgestattet werden, ist längst nicht so fern, wie es scheinen mag. Zukunftsstudien gehen von einer Realisierbarkeit wichtiger Aspekte bis zum Jahr 2010 aus (Ducatel et al. 2001; IST Advisory Group 2002).

3.1 Beiträge der Nanotechnologie zur technischen Basis allgegenwärtiger informationstechnischer Systeme

Die wichtigste technologische Basis für die Entwicklung allgegenwärtiger informationstechnischer Systeme ist „Moores Gesetz", jene Mitte der Sechzigerjahre vom Intel-Gründer Gordon Moore aufgestellte und immer noch gültige Regel, nach der sich die Integrationsdichte und Leistungsfähigkeit von integrierten Schaltkreisen alle 18 Monate verdoppelt. Dadurch wurden Mikroprozessoren schließlich so billig und massenhaft herstellbar, dass sie heute nicht nur in Computern, sondern praktisch in allen Geräten des täglichen Lebens eingesetzt werden, vom Staubsauger über die Mikrowelle bis zum PKW. Hier verschwindet die Computertechnik hinter der Fassade bekannter Funktionalitäten. Ubiquitous Computing ist die Extrapolation dieses Trends in die Zukunft.

Die durch das Moore'sche Gesetz induzierte „schleichende Revolution" hinsichtlich der Leistungsfähigkeit elektronischer Komponenten führt dazu, dass kleinste spontan und drahtlos miteinander kommunizierende Prozessoren bald quasi im Überfluss vorhanden sein werden. Mit dieser absehbaren „Überschwemmung" der Welt durch Rechenleistung wird ein Paradigmenwechsel in der Computeranwendung eingeläutet: Kleinste und billige Prozessoren, Speicherbausteine und Sensoren können zu diversen preiswerten „information appliances" zusammengebaut werden, die drahtlos mit dem Internet verbunden und für spezielle Aufgaben maßgeschneidert sind (Norman 1998; Want und Borriello 2000), sie können darüber hinaus aber auch aufgrund ihrer geringen Größe und ihres vernachlässigbaren Preises in viele Alltagsgeräte eingebaut werden. Dies gilt insbesondere für nach dem Verfahren der Weich-Lithografie hergestellte (polytronische) Bauelemente, die preiswert und massenhaft auf dünne Folien aufgedruckt werden können (vgl. Friedewald et al. 2002, S. 46ff.)

Immer wichtiger werden die Ergebnisse der Mikrosystemtechnik und auch der Nanoelektronik, welche beispielsweise zu kleinsten integrationsfähigen Sensoren führen, die unterschiedlichste Parameter der Umwelt aufnehmen können. Neuere Sensoren reagieren nicht nur auf die klassischen Größen Licht, Beschleunigung, Temperatur etc., sondern können auch Gase und Flüssigkeiten analysieren oder generell den sensorischen Input vorverarbeiten und so gewisse Muster (z.B. Fingerabdruck oder Gesichtsformen) erkennen.

Aus dem Bereich der Materialwissenschaft kommen Entwicklungen, die den Computern der Zukunft eine gänzlich andere äußere Form geben können oder sogar dafür sorgen, dass Computer auch äußerlich nicht mehr als solche wahrgenommen werden, weil sie vollständig mit der Umgebung verschmelzen.

Hier sind unter anderem Licht emittierende Polymere zu nennen, die Displays aus hochflexiblen, dünnen und biegsamen Plastikfolien ermöglichen (vgl. Kapitel 2). Außerdem wird auch an „elektronischer Tinte" und „smart paper" gearbeitet, welche Papier und Stift zum vollwertigen, interaktiven und hoch mobilen Ein- und Ausgabemedium mit einer uns wohl vertrauten Nutzungsschnittstelle erheben. Zwar ist hier noch einiges an technischer Entwicklungsarbeit zu leisten und man dürfte von einem breiteren kommerziellen Einsatz noch einige Jahre entfernt sein, jedoch existieren bereits Prototypen von elektronischem Papier und elektronischer Tinte, und die Bedeutung für die Praxis, wenn Papier quasi zum Computer wird oder umgekehrt der Computer sich als Papier materialisiert, kann kaum hoch genug eingeschätzt werden.

Zukunftsweisend sind auch Entwicklungen im Bereich von „Body Area Networks" – hier kann der menschliche Körper selbst als Medium zur Übertragung von Signalen sehr geringer Stromstärken genutzt werden. Allein durch Anfassen eines Gerätes oder Gegenstandes kann diesem dann eine eindeutige Identifikation (die beispielsweise von der Armbanduhr in den Körper eingespeist wird) übermittelt werden; auf diese Weise könnten Zugangsberechtigungen, personalisierte Konfigurierungen von Geräten oder die Abrechnung von Dienstleistungen erfolgen. Auch mit Kleidern aus Stoffen, die leitfähige Fasern enthalten, wird im Bereich des „wearable computing" experimentiert. Fasern, die beim Dehnen ihren elektrischen Widerstand ändern, ermöglichen jedenfalls interessante Mensch-Maschine-Schnittstellen, da so Körperbewegungen erfasst werden können oder Funktionen beispielsweise durch leichtes Ziehen an einem Stück der Kleidung ausgelöst werden können (vgl. Newman 2003).

Neben nanoelektronischen Bauelementen und Displays sind nanotechnologische Energiequellen für die allgegenwärtige Informationstechnik von besonderer Bedeutung. Die Batterietechnik macht im Vergleich zur sonstigen Effizienzsteigerung in der Informations- und Kommunikationstechnik eher langsame Fortschritte. Immerhin konnte die Kapazität typischer Batterien auf Ni-Cd- und Ni-MH-Basis in den letzten 20 Jahren um durchschnittlich 5 % pro Jahr vergrößert werden (Estrin et al. 2002). Die Energiedichte hat dabei mittlerweile einen Wert von 1 Joule pro mg erreicht. Für mobile Anwendungen ist auch das Maß „Energie pro Gewicht" relevant. Man hat die Hoffnung, mit neuen nanotechnologischen Materialien, z.B. auf Lithium-Polymerbasis, im Jahr 2010 Werte von 2 Joule pro mg zu erreichen. Mit einer Energie von 1 Joule können bei gegenwärtiger Technik ca. 10 Millionen Bits an Daten über drahtlos übertragen werden, wobei dieser Wert in den nächsten Jahren mindestens um den Faktor 10 gesteigert werden kann (vgl. Doherty et al. 2001),

da der Energiebedarf typischer Hardwareelemente mit der (sinkenden) mikroelektronischen Strukturbreite korreliert.

Batterien lassen sich mittlerweile in dünner (0,5 mm) und biegsamer Bauform herstellen. Neben der Entwicklung bei Batterien gibt es eine intensive Suche nach alternativen Energiequellen. Brennstoffzellen mit nanotechnologischen Katalysatoren und Membranen erreichen eine 10- bis 40-fach höhere Energiedichte als Batterien, allerdings lassen sie sich derzeit nicht beliebig klein verwirklichen. Für den Betrieb von Laptops und ähnlichen Geräten sollten solche Brennstoffzellen jedoch bald auf den Markt kommen (vgl. Luther et al. 2002). Weitere Möglichkeiten, Energie in geringem Umfang aus der Umwelt abzuschöpfen, besteht z.B. bei mechanischer Energie aus vibrierenden Fensterscheiben, Körperbewegungen etc. (Paradiso 2000).

Schließlich bietet die Bottom-Up-Nanotechnologie die Möglichkeit zur Energieerzeugung durch molekulare Linear- oder Rotationsmotoren. Solche Nanomotoren könnten etwa aus ringförmigen Enzym-Molekülen aus der Gruppe der Adenosithriphosphat-Synthase bestehen. Solche Generatoren könnten mit einer geeigneten Lithografietechnik dem Halbleitersubstrat positioniert werden und gezielt an solchen Stellen Energie produzieren, wo sie auch benötigt wird (Soong et al. 2000). Die Nutzung solch rein nanotechnologischen Energiequellen in der Praxis der Informations- und Kommunikationstechnik liegt allerdings in unbestimmter Zukunft.

Immer stärker miniaturisierte Hardwareelemente zu sinkenden Preisen sind allerdings nicht die einzige Voraussetzung für die Realisierung von allgegenwärtigen informationsverarbeitenden Systemen. Ebenso wichtig sind Fortschritte im Bereich der ubiquitären Kommunikation, der Softwaretechnik, des Knowledge Managements sowie insbesondere bei der Entwicklung von benutzerfreundlichen, adaptiven und kontextsensitiven Formen der Mensch-Computer-Interaktion (vgl. hierzu Mattern 2003).

3.2 Anwendungsbereiche allgegenwärtiger informationstechnischer Systeme

So breit wie die technische Basis allgegenwärtiger informationstechnischer Systeme ist auch deren Anwendungsspektrum. Mit dem Anspruch einer unsichtbaren Unterstützung des Menschen bei jeder Form von Tätigkeit ist fast in allen Bereichen des privaten und geschäftlichen Lebens ein Einsatz dieser Technologie möglich. Im folgenden wird ein Überblick über solche Anwendungen gegeben, die in besonders auf den Fortschritten der Nanotechnologie basieren. Diese finden sich vor allem im Bereich der Gesundheit und Sicherheit sowie des Handels bzw. Einkaufens.

3.2.1 Gesundheit und Sicherheit

Die fortschreitende Miniaturisierung elektronischer Bauelemente sowie eine Vielzahl kleiner und leistungsfähiger Sensoren, hat den Gesundheitsbereich zum besonders lohnenden Anwendungsgebiet der allgegenwärtigen Informationsverarbeitung werden lassen.

Durch die geringe Größe wird es heute möglich, leistungsfähige Computer ohne große Umstände dauerhaft mit sich zu führen oder diese in die Kleidung zu integrieren (wearable computer). Dies bietet die Möglichkeit, den Gesundheitszustand älterer, chronisch kranker oder mit bestimmten Risiken belasteten Personen sowie von Patienten nach bestimmten medizinischen Eingriffen kontinuierlich, auch außerhalb von Kliniken zu überwachen. Bei einem solchen System[2] (Abbildung 7) werden neuartige, häufig nanotechnologische Sensoren unmittelbar am Körper getragen und ermöglichen die kontinuierliche, belastungsfreie Erfassung medizinisch relevanter Vitalparameter (Puls, Blutdruck, Glukosepegel, etc.). Bei Parametern, die nicht unmittelbar durch Sensoren registriert werden, können nanotechnologische „Labs-on-a-Chip" die notwendigen Analysen durchführen. Die aufgezeichneten Daten werden drahtlos an eine mobile Basisstation und von dort an eine zentrale Datenbank (z. B. Patientenakte) oder Überwachungszentrale weitergeleitet.

Auf Basis eines solchen Monitorings sind eine ganze Reihe von gesundheitsrelevanten Leistungen möglich. Die stets aktuellen Daten stehen etwa dem Arzt für eine verbesserte Diagnose und Therapieplanung bzw. –überwachung zur Verfügung. In Kombination mit einem Expertensystem oder eines anderen wissensbasierten Verfahrens ist auch eine Unterstützung des Mediziners bei der Diagnose möglich.

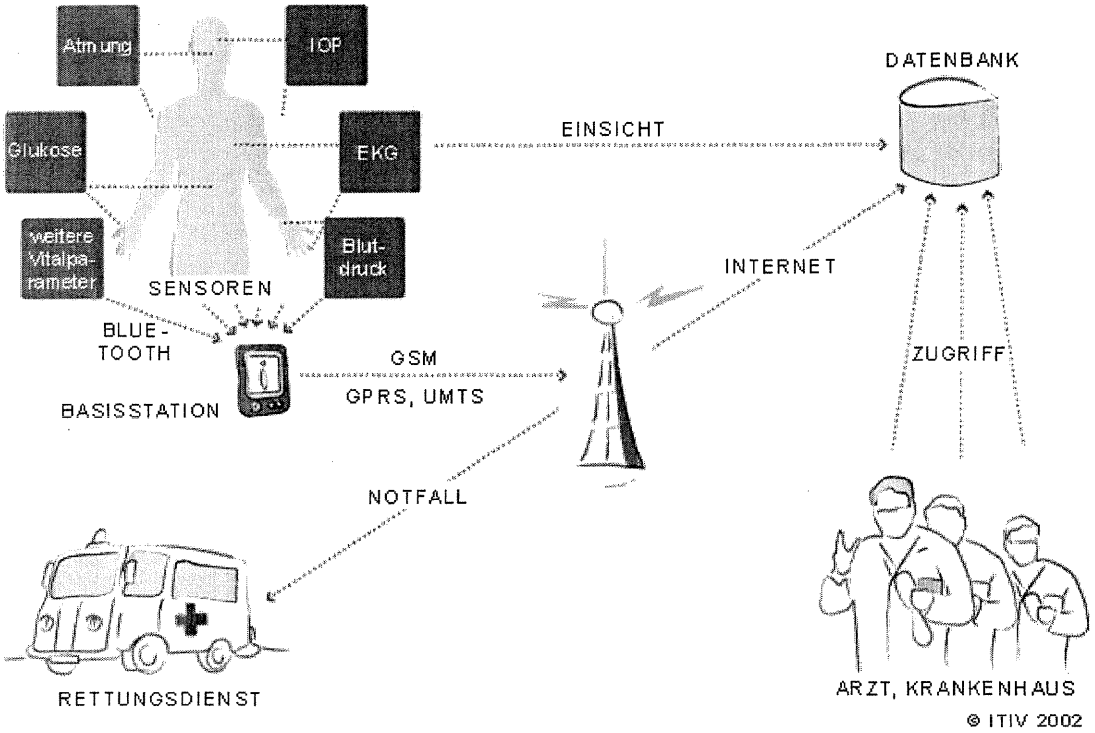
Darüber hinaus können im Falle einer Notfallsituation der Patient noch frühzeitig gewarnt und ein Rettungsdienst alarmiert werden, wobei dem Arzt bereits Informationen zur Art des Notfalls geliefert werden können (Kunze et al. 2002).

Neben Vorsorge und Diagnose liegt ein wesentliches Anwendungspotenzial der Nanotechnologie im kontrollierten und zielorientierten Transport („Drug Delivery") von medizinisch wirksamen Stoffen, der auf Basis der gemessenen Vitalparameter gesteuert wird, z.B. bei Diabetespatienten (vgl. Luther et al. 2002, S. 74ff.).

---

2 Ein solches System zur Überwachung des Gesundheitszustandes von Personen wird besipielsweise in dem vom BMBF geförderten Projekt „Personal Health Monitoring System mit innovativer mikrosystemtechnischer Sensorik" entworfen (http://www.phmon.de).

Abbildung 7: Entwurf eines Personal Health Monitoring Systems mit mikrosystemtechnischer und nanotechnologischer Sensorik



Quelle: http://www.phmon.de/images/system.gif

Ein ähnlicher Ansatz wird für die Erhöhung der Sicherheit im Straßenverkehr verfolgt. Auch soll der Fahrer durch eine Vielzahl von kleinen, möglichst wenig störenden Sensoren während der Fahrt überwacht werden. Da es bei dieser Anwendung vor allem um die Erkennung von Symptomen einer eingeschränkten Fahrtüchtigkeit geht, kommen Sensoren zum Einsatz, mit denen Müdigkeit oder ein erhöhter Alkohol- bzw. Drogenkonsum erkannt werden kann (Healey et al. 1999; DaimlerChrysler 2002).

Eine besondere Form der sicherheitsrelevanten Fahrerüberwachung ist das so genannte „affective computing", bei dem man Emotionen, Gefühle und Empfindungen des Menschen registriert. Zu diesem Zweck werden Daten über Blutdruck, Muskelaktivität oder Leitfähigkeit der Haut dazu genutzt, um festzustellen, ob sich ein Autofahrer in einer Stresssituation befindet (Pompei et al. 2002).

In allen diesen Fällen wird die Information dazu genutzt, die Verkehrssicherheit zu erhöhen. Die dabei denkbaren Maßnahmen reichen von der automatischen Verhinderung, ein Fahrzeug starten zu können über automatische Geschwindigkeits- und Bremssysteme bis hin zur Unterdrückung ablenkender Reize in Stresssituationen.

3.2.2 Handel und Einkauf

Das Anwendungspotenzial der allgegenwärtigen Informationsverarbeitung in Handel und Einkauf basiert auf der Möglichkeit zur „intelligenten" Kennzeichnung von Waren. Dabei werden bereits in naher Zukunft die heutigen Barcodes durch Etiketten ersetzt, auf denen weitergehende Informationen über die gekennzeichnete Ware gespeichert sind und drahtlos abgefragt werden können. Die drahtlose Abfrage wird bereits seit Jahren bei Diebstahlsicherungen angewendet, künftige Etiketten können aber sehr viel mehr Daten speichern als die heutige Information „bezahlt" oder „nicht bezahlt".

Voraussetzung für den massenhaften Einsatz solch intelligenter Etiketten ist, dass sie massenhaft und zu geringen Kosten hergestellt werden können. Passive Etiketten, sogenannte RFIDs (Radio Frequency Identifiers) kosten heute zwischen 0,10 und 1 EURO, mit fallender Tendenz.

Durch Verfahren der Nano-Weich-Lithografie (vgl. Friedewald et al. 2002, S. 46ff.) können Stempel, auch aus gekrümmten Materialien, hergestellt werden, die eine kontinuierliche Herstellung preiswerter und genügend leistungsfähiger Folienchips erlauben.

Im Einzelhandel können mit Hilfe dieser Etiketten eine Vielzahl neuer Dienste angeboten werden (Nicklous und Welsch 2003, Friedewald et al. 2003):

- Kunden können mit einem passenden Endgerät die auf dem Etikett gespeicherte Information (Preis, Inhaltsstoffe, Verfallsdatum, etc.) abfragen.
- Eine in diesem Gerät gespeicherte elektronische Einkaufsliste kann dazu genutzt werden, einen Kunden im Laden zu den benötigten Waren zu dirigieren und dabei beispielsweise auf Sonderangebote hinzuweisen.
- Zum Bezahlen können die Preisinformationen drahtlos von der Kasse ausgelesen werden.

Als weitere Möglichkeiten im Umfeld des Handels werden diskutiert:

- Die drahtlose Überwachung von Lagerbeständen und Logistikströmen mit Hilfe von drahtlos abfragbaren Etiketten.
- Die selbstständige Überwachung von technischen Einrichtungen (Autos, Maschinen) und die frühzeitige Erkennung von Schäden und Wartungsintervallen. Ein Beispiel hierfür ist der „intelligente Reifen", an dem u.a. die Fa. Continental arbeitet.

Da einfache elektronische Etiketten bereits heute im breiten Einsatz sind, ist damit zu rechnen, dass intelligente Etiketten auf Basis nanotechnologischer Herstellverfahren bereits in wenigen Jahren im praktischen Einsatz sein werden. Dabei wird es

zunächst zu einem „unsichtbaren" Ersatz älterer Etikettierungstechniken kommen. Die Durchsetzung der skizzierten neuen Dienstleistungen wird erheblich davon abhängen, inwieweit diese von den Kunden akzeptiert werden, da auf Seiten der Anbieter nicht unerhebliche Investitionen für den Aufbau einer passenden Kommunikationsinfrastruktur getätigt werden müssen. Darüber hinaus ist der Nutzwert davon abhängig, ob sich ein einheitlicher Standard etabliert, oder ob Kunden je nach Anbieter mit Insellösungen konfrontiert werden.

3.3 Bewertung

So sehr der angesprochene und auf vielen Gebieten erkennbare technische Fortschritt auch faszinieren mag: Klar ist, dass sich längst nicht jede erwünschte Verbesserung über die inkrementelle Optimierung technologischer Parameter erreichen lässt, die Realisierung der Vision des Ubiquitous Computing ist alles andere als trivial. Gut ein Jahrzehnt nach Veröffentlichung des grundlegenden Artikels von Mark Weiser (1991) erscheinen nach Expertenmeinung „many aspects of Mark Weiser's vision of ubiquitous computing ... as futuristic as they did in 1991" (Davies und Gellersen 2002).

Die oben kurz beschriebenen Beispiele und die Vorstellung von allgegenwärtigen Informationstechnologien veranlassen Optimisten zu euphorischen Reaktionen, da die Technologie ein erhebliches Potenzial besitzt, das Leben der Menschen erleichtern. Auf der anderen Seite werden vor allem Befürchtungen geweckt, durch allgegenwärtige Informationssysteme werde die Grundlage für einen totalen Überwachungsstaat gelegt.

Angesichts der zu erwartenden Allgegenwärtigkeit des Computers und den daraus resultierenden möglichen wirtschaftlichen, sozialen und gesellschaftlichen Auswirkungen stellt sich die Frage nach den vorhandenen Gestaltungsspielräumen. Die im folgenden angerissenen Fragen bzw. Probleme sind gleichermaßen eine technische und ökonomische wie auch eine politisch-juristische Herausforderung (vgl. Bohn et al. 2003).

Insbesondere stellt sich angesichts der Erfassung und drahtlosen Übertragung einer Vielzahl von teilweise hochsensiblen personenbezogenen Daten (z.B. Gesundheitsdaten) die Frage nach der *Datensicherheit* und dem *Schutz der Privatspäre* in bislang nicht gekannter Größenordnung. Dabei kann – je nach Sichtweise – das Ubiquitous Computing die Reichweite und Auswirkungen heutiger Datenschutzmechanismen grundlegend verändern und dadurch in Zukunft substanziell andere „soziale Landschaften" hervorbringen. Insbesondere ist eine weitere Verschiebung sozialer, räumlicher und zeitlicher Grenzen zu erwarten wie dies bereits bei der Einführung anderer Medientechnologien (z.B. Email) zu beobachten war.

Im Bereich der gesellschaftlichen Probleme ist vor allem daran zu denken, dass allgegenwärtige informationstechnische Systeme den Grad der *Abhängigkeit* von der korrekten und zuverlässigen Funktionsweise der Technik erheblich erhöht. Dies ist gerade in solchen Anwendungsbereichen besonders kritisch, in denen auch der größte Nutzen erwartet wird, wie etwa im Gesundheitsbereich.

In diesem Zusammenhang stellt sich die Frage nach der *Beherrschbarkeit* eines Systems, das aus Myriaden von „intelligenten" und damit wenigstens teilweise autonom agierenden Dingen sichergestellt werden kann. Dies betrifft nicht nur das technische System selbst, sondern auch die darauf aufbauenden Anwendungen. So verspricht zwar die durch ubiquitäre Informationstechnik unterstützte Wirtschaft ein besonders hohes Maß an Flexibilität, in der Realität kann sich das entstehende System aber als so unüberschaubar und dynamisch herausstellen, dass es von keinem Anbieter und Nachfrager mehr überschaut werden kann.

Ferner stellt sich die Frage nach der *Zurechenbarkeit von Handlungen*, bei denen der Mensch in erheblichem Maße durch ein technisches System unterstützt wird. Kann einem menschlichen Nutzer noch die Verantwortung zugeschrieben werden, wenn beispielsweise bei einem Ticket-System eines Verkehrsbetriebs zwei technische Systeme einen Beförderungsvertrag aushandeln? Und wie kann man in einer solchen Welt einen Überblick über die Vielzahl der mehr oder weniger automatisch abgeschlossenen Verträge behalten, oder gar die Transaktionen auf ihre Rechtmäßigkeit im einzelnen überprüfen.

Schließlich bleibt die Frage, wie angesichts der gut gemeinten „Unterstützung" des Menschen dessen *Entscheidungsautonomie* sichergestellt werden kann. So wird niemand bezweifeln, dass das „intelligente Auto" mit Fahrer- und Fahrzeugüberwachung einen gewichtigen Beitrag zur Verkehrssicherheit leisten kann. Die Grenze zwischen einem notwendigen und vom Fahrer akzeptierten Eingriff (z. B. automatisches Bremsen vor einem Hindernis) und einer als unakzeptabel betrachteten Intervention, zu der schon eine automatisch Geschwindigkeitskontrolle zählen kann, ist allerdings sehr schmal.

4 Quanteninformationsverarbeitung und -kryptografie

Insbesondere für die Kryptografie erweisen sich Quanteninformationstechniken als besonders interessant. Dabei kann man die Verwendung von Quantencomputern und Quantenalgorithmen für die Kryptoanalyse und den Quantenschlüsselaustausch für sichere, verschlüsselte Information unterscheiden.

Die Sicherheit heutiger Kryptografieverfahren basiert darauf, dass sich bestimmte mathematische Funktionen deutlich weniger effizient berechnen lassen als deren Umkehrfunktion. Mit dem Aufkommen des Quantum Computing ist diese Voraussetzung in Frage gestellt. Quantencomputer machen sich Effekte der Quantentheorie zugute, so dass sie bestimmte Probleme erheblich schneller lösen können als klassische Computer. Obwohl es bislang noch keine funktionsfähigen Quantencomputer gibt, sind sich Fachleute darüber einig, dass einige der wichtigsten Kryptografieverfahren ihren praktischen Wert verlieren könnten.

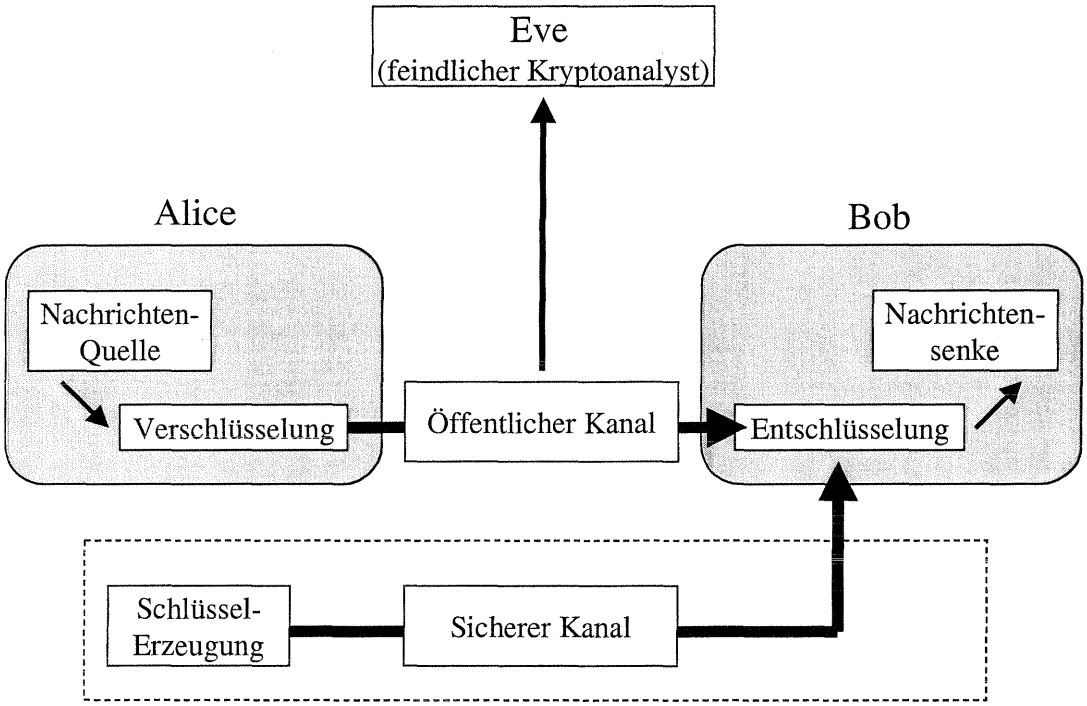
Im Gegenzug macht die Quantentheorie auch neue Kryptografieverfahren möglich, die (zumindest theoretisch) absolute Sicherheit selbst vor Quantencomputern bieten können. Anders als die bisherigen Kryptografieverfahren, deren Sicherheit auch vor klassischen Computern nur auf Vermutungen basiert, sind die Quantenkryptografieverfahren beweisbar sicher.

4.1 Quantenkryptoanalyse

Bis in die 1970er Jahre war die Schlüsselverteilung das größte Problem der Kryptografie. Um Nachrichten sicher austauschen zu können, mussten zwei Parteien im Besitz des gleichen Schlüssels sein, den niemand anders kennen durfte. Bevor man also Nachrichten austauschen konnte, musste man zuerst den Schlüssel austauschen – im Prinzip das gleiche Problem.

Gelöst wurde dieses Problem durch *asymmetrische Verschlüsselungsverfahren* wie *RSA* Mitte der 1970er Jahre. Dabei werden zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet: Jede Person generiert sich ein Schlüsselpaar, das aus einem *öffentlichen* und einem *privaten Schlüssel* besteht. Sie behält den privaten Schlüssel für sich und gibt den öffentlichen Schlüssel möglichst weit bekannt. Wenn eine Person (traditionell Alice genannt) einer anderen (Bob genannt) eine Botschaft zukommen lassen will, verwendet sie Bobs öffentlichen Schlüssel zum Verschlüsseln der Nachricht (vgl. Abbildung 8). Diese Botschaft kann nur Bob mit seinem privaten Schlüssel decodieren (vgl. Singh 2000, 327).

Abbildung 8: Schema der Quantenkryptografie



Quelle: Brooks 1999

Damit dies funktioniert, müssen privater und öffentlicher Schlüssel in einer ganz bestimmten Weise zusammenhängen. Zugleich muss es unmöglich sein, aus dem öffentlichen Schlüssel den privaten zu gewinnen, da sonst die Sicherheit des Verfahrens dahin wäre. Dafür werden mathematische Ein-Weg-Funktionen verwendet, die sich nur in eine Richtung effizient durchführen lassen, während die Gegenrichtung nicht in annehmbarer Zeit gelöst werden kann. Die *Primfaktorzerlegung* stellt eine solche Funktion dar: zwei Primzahlen lassen sich ganz einfach miteinander multiplizieren; der Aufwand ist quadratisch, steigt also auch für große Zahlen nur gering an. Das Ergebnis dieser Multiplikation wieder in die beiden Faktoren zu zerlegen, wird dagegen bei großen Zahlen sehr schnell schwieriger, da sämtliche Möglichkeiten durchprobiert werden müssen: der Aufwand steigt exponentiell.

Die asymmetrischen Kryptografieverfahren machen sich dies zugute: Alice wählt zwei Primzahlen p und q als ihren privaten Schlüssel und gibt N = p x q als ihren öffentlichen Schlüssel bekannt. Zum Verschlüsseln wird eine andere Ein-Weg-Funktion verwendet, die unter Verwendung von N nur in einer Richtung effizient durchgeführt werden kann. Zum Entschlüsseln wird die Gegenrichtung benötigt, diese kann aber mit realistischem Aufwand nicht durchgeführt werden, solange nur N bekannt ist (heutige Computer würden bei den üblichen Schlüssellängen Millionen von Jahren dafür brauchen).

Die zum Verschlüsseln gewählten Funktionen sind aber von so spezieller Art, dass sie ihren Ein-Weg-Charakter verlieren, sobald p und q bekannt sind: dann kann auch die Gegenrichtung effizient berechnet werden. Daher kann eine mit dem öffentlichen Schlüssel codierte Nachricht nur mit dem dazu gehörigen privaten Schlüssel entschlüsselt werden. Somit ist sichergestellt, dass nur Alice selbst die für sie bestimmten Nachrichten lesen kann (vgl. Singh 2000, 333 f).

Die Sicherheit der asymmetrischen Kryptografieverfahren basiert somit auf der Tatsache, dass sich große Zahlen nicht effizient faktorisieren lassen. Der Aufwand wächst bei allen bekannten klassischen Algorithmen exponentiell. Damit lassen sich diese Verfahren vor *Brute-Force*-Angriffen schützen, indem man die verwendeten Schlüssel groß genug wählt. Kann man dagegen Quantenalgorithmen benutzen, gelten diese Effizienzgrenzen nicht mehr, da Quantenalgorithmen sich bestimmter Eigenschaften der Quantenwelt, etwa der Superposition von Quantenzuständen, bedienen, um in deutlich effizienterer Weise zu einem Resultat zu kommen, als dies mit klassischen Algorithmen möglich ist (Gruska 1999, 101).

Quantenalgorithmen profitieren davon, dass Superpositionen auch beim Transformieren eines Quantenzustands erhalten bleiben. So werden bei einem einfachen Rechenschritt auf einem Quantenregister aus n Qubits 2^n Operationen auf je einem Basiszustand gleichzeitig ausgeführt. Anstelle der exponentiellen Rechenzeit, die klassische Algorithmen benötigen, können sie also mit exponentieller Quanteninterferenz arbeiten und so die Rechenzeit polynomiell halten (vgl. Gruska 1999, 103).

Ein Quantenalgorithmus zur Faktorisierung wurde von Peter Shor (1994) entwickelt. *Shors Algorithmus* nützt Quanteneffekte, um Zahlen in polynomieller Zeit zu faktorisieren. Sobald also Quantenrechner mit einer ausreichenden Zahl von Quantenbits gebaut werden können, wären die wichtigsten momentan verwendeten Kryptografieverfahren (auch solche die auf diskreten Logarithmen und elliptischen Kurven basieren) auf einen Schlag unsicher (vgl. Gruska 1999, 111 f).

Demnach würde „die Entwicklung eines voll funktionsfähigen Quantencomputers unsere Privatsphäre gefährden, den elektronischen Handel untergraben und sämtliche Vorstellungen von nationaler Sicherheit zunichte machen. (...) Welches Land auch immer ihn als erstes einsetzt, es wird in der Lage sein, die Post seiner Bürger zu überwachen, die Gedanken der wirtschaftlichen Konkurrenz zu lesen und die Planungen seiner Gegner zu belauschen. Der Quantencomputer steckt zwar noch in den Kinderschuhen, doch ist er als potenzielle Gefahr für das Individuum, für den internationalen Handel und für die globale Sicherheit“ (Singh 2000, S. 400).

4.2 Quantenkryptografische Verfahren zur Schlüsselerzeugung

Ein Ausweg aus diesem sich (langfristig) stellenden Problem ist der Einsatz von quantenkryptografischen Verfahren zur Schlüsselerzeugung. Dabei wird der fundamentale Unterschied zwischen klassischen und Quantenbits in Bezug auf ihre Kopierbarkeit genutzt. Während klassische Bits sehr einfach und ohne Informationsverlust kopiert („geklont") werden können, ist dies bei Quantenbits – und generell bei beliebigen Quantenzuständen – nicht möglich. Ein Versuch, eine Kopie zu machen, führt wie jede Messung zu Informationsverlust. Entweder die Kopie ist nicht perfekt, erhält also nur einen Teil der im Original enthaltenen Informationen, oder der Zustand des Originals wird unwiderruflich zerstört (Gruska 1999, 68 f.). Diese kann man für die Entwicklung von abhörsicheren Kryptografieverfahren nutzen. Denn anders als bei klassischen Verfahren, deren Sicherheit zwar sehr wahrscheinlich ist, aber nicht bewiesen werden kann, sind die Quantenkryptografieverfahren beweisbar sicher (Gruska 1999, 217 f.).

Im Gegensatz zu Shors Algorithmus werden für solche Verfahren keine Quantencomputer benötigt, sondern lediglich Transmitter und Detektoren, um Quantenzustände zu erzeugen und zu messen. Das erste und bekannteste Verfahren zur Quantenschlüsselerzeugung (QKG, engl. *quantum key generation*) wurde 1984 von Bennett und Brassard vorgestellt (siehe Kasten). Seit den frühen 1990er Jahren wurden eine Vielzahl von alternativen quanenkypoafischen Pookollen entwickelt, die dieses Grundverfahren modifiziert und erweitert haben. Dabei wurden vor allem die Effizienz der Übertragung (Bandbreite bzw. Datenrate) und die Fehlererkennung verbessert.[3]

Verfahren zum Quantenschlüsselaustausch nach Bennett und Brassard (1984)

Alice und Bob können bei diesem Verfahren auf folgende Weise gemeinsam einen geheimen Schlüssel generieren, um anschließend eine mit diesem Schlüssel kodierte Nachricht auszutauschen: Alice hat die Möglichkeit, Photonen mit vier unterschiedlichen Polarisationsrichtungen (0, 45, 90 und 135 Grad) zu senden. Diese Richtungen entsprechen den Quantenzuständen $|1\rangle$, $|0'\rangle$, $|0\rangle$ und $|1'\rangle$. Bobs Detektor kann so eingestellt werden, dass er entweder zwischen $|0\rangle$ und $|1\rangle$ unterscheiden kann oder zwischen $|0'\rangle$ und $|1'\rangle$. Die Standardbasis ($|0\rangle$ und $|1\rangle$) und die Dualbasis ($|0'\rangle$ und $|1'\rangle$) sind nach der Heisenberg'schen Unschärferelation miteinander unvereinbar, so dass es nicht möglich ist, mit einer Messung zwischen allen vier Möglichkeiten zu unterscheiden.

---

3 Beispielhaft seien genannt: (1) das Verfahren von Bennett (1992), das mit zwei statt vier nichtorthogonalen Basen auskommt sowie (2) das Verfahren von Lo und Chau (1999), das auf verschränkten Quantenzuständen basiert, deshalb aber den Einsatz eines Quantencomputers auf beiden Seiten der Kommunikation voraussetzt.

Damit Alice und Bob einen Schlüssel der Länge n austauschen können, erzeugt Alice zwei Reihen von Zufallsbits der Länge m, wobei m deutlich größer als n ist. Bob erzeugt eine weitere solche Reihe. Alice sendet Bob die erste Reihe von Zufallsbits über einen Quantenkanal; dabei sendet sie Nullen zufällig (gemäß der zweiten Zufallsreihe) als |0> oder |0'>; bei den Einsen wird analog vorgegangen. Bob entscheidet gemäß seiner eigenen Zufallsreihe vor jeder Messung, ob er den Detektor orthogonal oder diagonal einstellt, d. h. ob er bei der Messung die Standard- oder die Dualbasis verwendet. Nur wenn Bob die gleiche Polarisierungsrichtung wie Alice wählt, erhält er ein eindeutiges Ergebnis. Sind die Polarisierungsrichtungen unterschiedlich, ist das Ergebnis von Bobs Messung zufällig, wobei die Information über die ursprünglichen Polarisation verloren geht.

Anschließend vergleichen Alice und Bob für jedes übertragene Bit die von ihnen verwendeten Polarisationsrichtungen. Für den gemeinsamen Schlüssel werden nur die Bits verwendet, bei denen Bob die richtige Polarisationsrichtung gewählt hat. Dieser Informationsaustausch kann öffentlich stattfinden, da eventuelle Lauscher damit nichts anfangen können, ohne die Bits selbst gemessen zu haben – was sie nicht tun können, ohne den Schlüssel zu zerstören und somit entdeckt zu werden (Gruska 1999, 224–227).

Die Rohschlüssel von Alice und Bob werden normalerweise nicht völlig übereinstimmen, da Übertragungsfehler (z.B. durch Abhörversuche) auftreten können. Um zu überprüfen, ob die Übertragung von einem Unbefugten belauscht wird, vergleichen Alice und Bob einen zufällig gewählten Ausschnitt des Rohschlüssels über den öffentlichen Kanal. Überschreitet die bei diesem Vergleich ermittelte Fehlerrate einen bestimmten Grenzwert wird der komplette Schlüssel verworfen. Ansonsten wird zur Extraktion des endgültigen Schlüssels eine Fehlerkorrektur und eine Kompression des Rohschlüssels („privacy amplification")[4] durchgeführt. Diese Vorgehensweise stellt sicher, dass die zur Ver- und Entschlüsselung verwendete Bitfolge übereinstimmt, Zufallscharakter besitzt und nur Alice und Bob bekannt ist.

4 Mit diesem Schritt soll die Wahrscheinlichkeit verringert werden, dass ein Lauscher aus den wenigen ihm möglicherweise bekannten Bits weiteren Nutzen ziehen kann. Dafür werden aus dem korrigierten Rohschlüssel zufällige Untermengen ausgewählt und so ein kürzerer und „geheimerer" Schlüssel gewonnen (Gruska 1999, S. 224).

Tabelle 2: Übertragungsbeispiel für das Protokoll

Alice' Zufallsreihe	1	0	0	1	0	0	0	1	1
Position von Alice Polarisationsfilter	+	×	+	×	+	+	×	+	+
Polarisation der gesendeten Photonen	|	/	—	\	—	—	/	|	|
Position von Bobs Polarisationsfilter	+	+	×	×	+	×	×	×	+
Bobs Messergebnis	|	—	/	\	—	/	/	/	|
Übereinstimmung der Polarisationsrichtung	✓			✓	✓		✓		✓
Schlüssel	1			1	0		0		1

Quelle: Bennett und Brassard (1984)

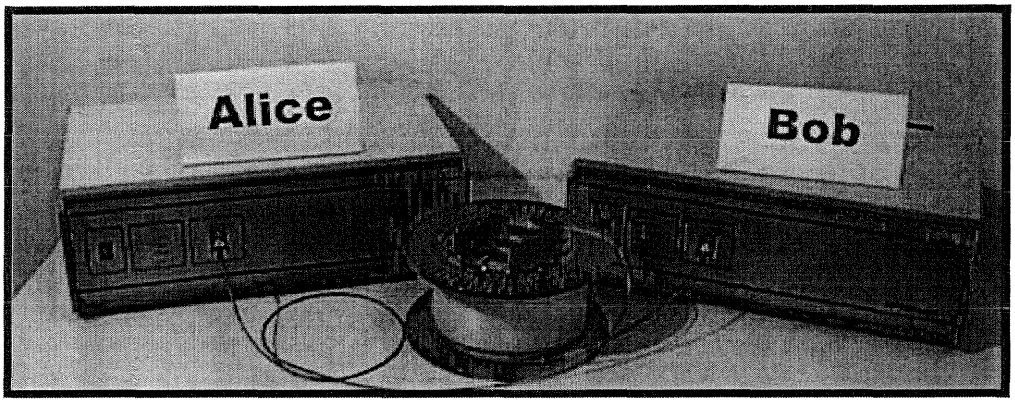
Die theoretische wie auch die experimentelle Seite der Quantenkryptografie sind heute bereits weit fortgeschritten, es bestehen aber immer noch Defizite bei der technologischen Umsetzung.

Für die zuverlässige Realisierung eines quantenkryptografisch gesicherten Kommunikationssystems wird vor allem ein Transmitter zur Erzeugung einzelner Photonen benötigt. Solche so genannten Photonengewehre basieren häufig auf Nanotechnologie, z. B. Quantenpunkten. Auch die Detektion einzelner Photonen ist bislang noch nicht in jeder Hinsicht befriedigend gelöst. Insbesondere funktionieren die derzeit fortschrittlichsten Detektoren weit unterhalb der für die Telekommunikation verwendeten Wellenlängen. Es kommen zwar langsam auch Ein-Photon-Detektoren auf den Markt, die für die kommerziell bedeutsamen Wellenlängen geeignet sind, ihre Empfindlichkeit reicht aber noch nicht für einen quantenkryptografischen Schlüsselaustausch aus (Mullins 2002). Da für die Realisierung solcher Detektoren keine grundlegenden wissenschaftliche Probleme zu lösen sind, gehen Experten davon aus, dass Ein-Photon-Detektoren für die kommerziell bedeutsamen Wellenlängenbereiche mittelbar verfügbar sein werden.

Neben den geeigneten Transmittern und Detektoren stellt die Überbrückung großer Entfernungen das größte Problem der Quantenkryptografie dar. Beim Transport von Photonen durch ein Trägermedium (normalerweise Luft oder ein Glasfaserkabel) nimmt nämlich mit der Entfernung auch das Risiko zu, dass das Photon mit seiner Umwelt interagiert und dabei den Quantenzustand verliert. Bislang ist es gelungen, Photonen mit einer geringen Fehlerrate in Glasfaserkabeln 67 km und im Freien 23,4 km weit zu transportieren (Stucki et al. 2002; Kurtsiefer et al. 2002). Für den praktischen Einsatz bedarf neben der weiteren Erhöhung der Reichweite und der Übertragungsrate vor allem der Entwicklung eines Quantenrepeaters, mit dem aus den bisherigen Punkt-zu-Punkt-Verbindungen ein Netz aufgebaut werden könnte. Obwohl es theoretische Konzepze für einen Quantenrepeater gibt (Tittel et al. 1999), ist eine Realisierung nach Experteneinschätzung bislang nicht absehbar (Gottesmann und Lo 2000; Lo 2000).

Dennoch sind heute bereits erste kommerzielle Quantenkryptografiesysteme auf dem Markt. So bietet die schweizer Firma ID Quantique mittlerweile ein kommerzielles System für etwa 100.000 Euro azuverlässigen, einen Schlüsselaustausch über maximal 60 km erlaubt. Es handelt sich dabei um die kommerzielle Variante des experimentellen Systems der Genfer Forschungsgruppe von Nicolas Gisin, das zwar zuverlässig, aber nur bei relativ geringen Datenraten arbeitet.[5]

Abbildung 9: Quantenkryptografisches System der Fa. ID Quantique aus Genf



Quelle: http://www.idquantique.com

Vor kurzem wurde berichtet, es sei gelungen, die bei der Quantenkryptografie verwendeten polarisierten Photonen zu „klonen" (Lamas-Linares 2002). Bislang sind sich die Experten nicht einig, inwieweit das Experiment die Quantenkryptografie unsicher macht. Es mahnt zumindest zur Vorsicht, sich all zu sehr auf die angeblich absolute Sicherheit der Quantenkryptografie zu verlassen; dafür gebe es zu viele potenzielle Angriffsflächen, von denen nicht alle offensichtlich seien – selbst für Experten (New Scientist News vom 29.3.2002).

Es gibt noch weitere Gründe, die eine (rasche) Ausbreitung der Quantenkryptografie wenig realistisch erscheinen lassen. Da ist zunächst der enorme apparative Aufwand, der erheblich verringert werden müsste – etwa auf die Größe einer Smartcard –, um für alltägliche Anwendungen akzeptabel zu sein. Auch die Kosten quantenkryptografischer Lösungen sind prohibitiv. So hat die Erfahrung gezeigt, dass der überwiegende Teil der Kunden kaum bereits ist, für einen deutlich besseren Schutz auch deutlich mehr Geld zu bezahlen. Schließlich ist auch nicht sicher, wie sich die nationalen Regierungen gegenüber einer Technologie verhalten werden, die nicht nur für sich selbst, sondern auch ihren Gegner absolute Sicherheit bietet (Lo 1999).

---

5 Bei einer Überragungsstrecke von 10 km wird eine Datenrate von 4000 bit pro Sekunde erreicht, bei 20 km sind es noch 1500 bit pro Sekunden und bei 60 km nur noch 100 bit pro Sekunde.

Wegen dieser Einschränkungen wird sich die Quantenkryptografie nach Experteneinschätzung nicht zu einem Verfahren für alltägliche Anwendungen entwickeln; für höchste Sicherheitsansprüche im militärischen oder nachrichtendienstlichen Umfeld wird ihre Nutzung bereits ernsthaft diskutiert. In diesem Zusammenhang ist zu erwarten, dass erneut Debatten aufflammen, wie sie im Zusammenhang mit der konventionellen Kryptografie in den 1990er Jahren geführt wurden, als die US-Regierung genau darüber wachte, dass fortschrittliche Verschlüsselungstechniken nicht exportiert wurden – nicht einmal in Staaten der westlichen Welt (Weisman 1991).

Insbesondere warnen Experten vor euphorischen Reaktionen, angesichts der theoretisch beweisbaren „absoluten" Sicherheit der Quantenkryptografie. Gute Kryptografie allein ist für die Sicherheit in der Information und Kommunikation nicht ausreichend, viel entscheidender ist vielfach das Umfeld. So schreibt der Sicherheitsexperte Bruce Schneier „I found that the weak points had nothing to do with the mathematics. They were in the hardware, the software, the networks, and the people. Beautiful pieces of mathematics were made irrelevant through bad programming, a lousy operating system, or someone's bad password choice. I learned to look beyond the cryptography, at the entire system, to find weaknesses. (...) Security is a chain; it's only as secure as the weakest link" (Schneier 2000, xii).

Deshalb muss eindringlich darauf hingewiesen werden, dass man sich nie leichtfertig der Illusion von Sicherheit aus einer einzigen Sichtweise hinzugeben, sondern die Sicherheit eines Systems immer wieder aus verschiedenen Perspektiven in Frage stellen sollte (mehrseitige Sicherheit) (vgl. Rannenberg et al. 1996). In dieser Hinsicht erscheinen die großartigen Versprechen von absolut beweisbarer Sicherheit, mit denen die Quantenkryptografie antritt, eher als Gefahr. Die Quantentechnologie bietet enorme Vorteile; ein auch in der Praxis absolut abhörsicheres Kommunikationssystem wird aber in der Praxis nicht daraus hervorgehen.

5 Fazit

Die Nanotechnologie hat ihr direktes Hauptanwendungsfeld zwar in erster Linie in der Vorstufe zu den Chips (Prozessoren und Speicherchips) als Bauelementen der Elektronik (vgl. Friedewald et al. 2002), sie ermöglicht auf Basis neuer nanotechnologischer Bauelemente auch neue Anwendungen.

So der Bereich *nanotechnologische Displaytechnologien* ein besonders prägnantes Beispiel für das enorme Substitutionspotenzial der Nanotechnologie, den reibungslosen Einzug von nanotechnolgischen Lösungen in Produkte und die Kooperation zwischen Grundlagenforschung und industrieller Entwicklung. Hier wird deutlich, dass die Nanotechnologie im Bereich der IuK-Technik vor allem durch ihre indirekten „Hebeleffekte" auf in der Wertschöpfungskette nachgelagerte Marktcluster wirkt.

Im Fall von Systemen der *allgegenwärtigen Informationsverarbeitung* (Ubiquitous Computing) leistet die Nanotechnologie wichtige Beiträge zur technologischen Basis dieses Anwendungsfeldes. Dabei sind die extreme Miniaturisierung, die Konstruktion neuartiger Sensoren und die Möglichkeit zur Produktion billiger und leistungsfähiger polytronischer Schaltungen die wichtigsten Impulse der Nanotechnologie. Neben der technologischen Grundlegung durch die Nanotechnologie zeigt dieses Anwendungsgebiet aber auch die Vielzahl der gesellschaftlichen Problemfelder auf, die durch die Möglichkeiten der Nanotechnologie geschaffen werden.

So stellt die Möglichkeit zur Sammlung, Verbreitung und Verarbeitung einer Vielzahl von teilweise personenbezogenen Daten Technik, Staat und Gesellschaft vor eine Vielzahl von Problemen aus dem Bereich der Persönlichkeitsrechte – insbesondere des Datenschutzes, der informationellen Selbstbestimmung und der wachsenden Abhängigkeit wichtiger gesellschaftlicher Funktionen von technologischen Lösungen.

Werden auf die im Rahmen dieses Gutachten lediglich angerissenen Probleme keine ausreichenden Lösungen gefunden, könnte die breite Akzeptanz für die allgegenwärtige Informationsverarbeitung und die dahinter stehende Nanotechnologie gefährdet sein. In wenig demokratischen Gesellschaftsformen kann das Kontrollpotenzial zur Realisierung von Orwell'schen Überwachungsstrukturen führen. In Gesellschaften mit gesichertem Schutz der Individualsphäre hingegen könnte die allgegenwärtige Informationsverarbeitung als technischer Fortschritt für die Lösung wichtiger Probleme und als Ausweitung individueller Freiheitsräume wahrgenommen und akzeptiert werden. Damit steht und fällt auch das erhebliche wirtschaftlich Potenzial dieser Anwendung

Der Bereich der *Quantenkryptografie* erscheint auf den ersten Blick durch die klar umrissene und eng begrenzte Anwendung wenig Konfliktpotenzial zu bergen. Sichere Kommunikation ist sowohl für staatliche Stellen wie auch für Wirtschaftsunternehmen in Zeiten globaler Unsicherheit bzw. Konkurrenz ein elementares Bedürfnis. Dennoch bergen die scheinbar „absolut" sicheren Verfahren der Quantenkryptografie die Gefahr, dass innerhalb des komplexen Systems der technisch vermittelten Kommunikation nicht-technische Faktoren vernachlässigt werden. Das in Deutschland seit einigen Jahren favorisierte Konzept der mehrseitigen Sicherheit gibt hier Anregungen, welche Maßnahmen neben geeigneten Kryptografieverfahren ergriffen werden müssen, um ein Höchstmaß an Sicherheit für die Kommunikation zu erreichen.

6. Literatur

Bennett, C. H. (1992): Quantum Cryptography Using Any Two Nonorthogonal States. In: Physical Review Letters 68, Nr. 21, S. 3121-3124.

Bennett, C. H.; Brassard, G. (1984): Quantum Cryptography: Public Key Distribution and Coin Tossing. In: Proceedings of the IEEE Conference on Computers, Systems and Signal Processing, Bangalore: IEEE Press, S. 175-179.

Bohn, J.; Coroama, V.; Langheinrich, M. et al. (2003): Allgegenwart und Verschwinden des Computers: Leben in einer Welt smarter Alltagsdinge. In: Grötker, R. (Hrsg.): Privat! Kontrollierte Freiheit in einer vernetzten Welt. Hannover: Heise Verlag.

Brooks, M. (Hrsg.) (1999): Quantum Computing and Communications. London: Springer.

Burrows, P. E.; Forrest, S. R.; Thompson, M. E. (1997): Prospects and applications for organic light-emitting devices. In: Current Opinion in Solid State and Material Sciences 2, Nr. 2, S. 236-143.

Choi, W. B.; Chung, D. S.; Kang, J. H. et al. (1999): Fully sealed, high-brightness carbon-nanotube field-emission display. In: Applied Physical Letters 75, Nr. 20, S. 3129-3131.

Cremer, C.; Eichhammer, W.; Friedewald, M. et al. (2003). 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. Bericht an das Bundesministerium für Wirtschaft und Technologie. Karlsruhe: ISI.

DaimlerChrysler (Hrsg.) (2002): Hallo, wach? Die Ermüdung des Fahrers rechtzeitig und zuverlässig erkennen. In: Hightech Report 2/2002, S. 56-57.

Davies, N.; Gellersen, H.-W. (2002): Beyond Prototypes: Challenges in Deploying Ubiquitous Systems. In: Pervasive Computing 1, Nr. 1, S. 26-35.

DisplaySearch (2002): DisplaySearch Releases Annual Report on Flat Panel Display Electronics: Driver, Transmitter/Receiver and Scaling Engine IC Revenue to Triple from 2000 to 2005 and Reach $9.5 Billion. Presseerklärung vom 6. September 2002 (http://www.displaysearch.com/press/2002/090600.htm).

Doherty, L.; Warneke, B. A.; Boser, B. E.; Pister, K. S. J. (2001): Energy and Performance Considerations for Smart Dust. In: International Journal of Parallel Distributed Systems and Networks 4, Nr. 3, S. 121-133.

Ducatel, K.; Bogdanowicz, M.; Scapolo, F. et al. (2001). Scenarios for Ambient Intelligence in 2010. Sevilla: Institute for Prospective Technological Studies (IPTS).

Friedewald, M.; Da Costa, O.; Punie, Y. et al. (2003): Science and Technology Roadmapping: Ambient Intelligence in Everyday Life (AmI@Life). Sevilla: Institute for Prospective Technology Studies. In Vorbereitung.

Gershenfeld, N. A. (1999): Wenn die Dinge denken lernen. München und Düsseldorf: Econ.

Gruska, J. (1999): Quantum Computing. London: McGraw-Hill.

Healey, J.; Seger, J.; Picard, R. (1999). Quantifying Driver Stress: Developing a System for Collecting and Processing Bio-Metric Signals in Natural Stress. Technical Report. Cambridge, Mass.: M.I.T. Media Laboratory.

Howard, W. E.; Prache, O. F. (2001): Microdisplays based upon organic light-emitting diodes. In: IBM Journal of Research and Development 45, Nr. 1, S. 115-127.

IST Advisory Group. (2002): Strategic Orientations and Priorities for IST in FP6. Luxembourg: Office for Official Publications of the European Communities.

Kunze, C.; Großmann, U.; Stork, W.; Müller-Glaser, K. D. (2002): Application of Ubiquitous Computing in personal health monitoring systems. In: Kongressbericht der 36. Jahrestagung der Deutschen Gesellschaft Für Biomedizinische Technik (DGBMT) im VDE, Karlsruhe, 25.–28. September 2002. Berlin: Schiele & Schön, S. 360–362.

Kurtsiefer, C.; Zarda, P.; Halder, M. et al. (2002): A step towards global key distribution. In: Nature 419, S. 450.

Lamas-Linares, A.; Simon, C.; Howell, J. C.; Bouwmeester, D. (2002): Experimental Quantum Cloning of Single Photons. In: Science 296, S. 712-714.

Le Barny, P.; Dentan, V.; Facoetti, H. et al. (2000): Application of organic electroluminiscent materials in visualisation. In: Comptes Rendus de l'Académie des Sciences, Série IV (Physics) 1, Nr. 4, S. 493-508.

Lo, H.-K. (2000): Will Quantum Cryptography ever Become a Successful Technology in the Marketplace? In: Physics World, June 2000, S. 17. (Ausführliche Fassung unter http://arxiv.org/abs/quant-ph/9912011)

Lo, H.-K.; Chau, H. F. (1999): Unconditional security of quantum key distribution over arbitrarily long distances. In: Science 283, Nr. 5410, S. 2050-2056.

Luther, W.; Malanowski, N.; Wevers, M. et al. (2002). Nanotechnologie - Teilstudie Wissenschaftlich-technische Grundlagen. Gutachten für den Deutschen Bundestag. Düsseldorf: VDI Technologiezentrum, Zukünftige Technologien Consulting.

Mattern, F. (2003): Ubiquitous Computing: Szenarien einer informatisierten Welt. In: Zerdick, A.; Picot, A. et al. (Hrsg.): E-Merging Media - Digitalisierung der Medienwirtschaft. Berlin und Heidelberg: Springer.

Mullins, J. (2002): Making Unbreakable Code. In: IEEE Spectrum 39, Nr. 5, S. 40-45.

Newman, C. (2003): Stoffe, die mitdenken. In: National Geographic Deutschland 1/2003.

Nicklous, M. S.; Welsch, M. (2003): Intelligente Etiketten. In: Sauerburger, H. (Hrsg.): Ubiquitous Computing. Heidelberg: dpunkt (HMD. Theorie und Praxis der Wirtschaftsinformatik, 229), S. 81-89.

Niesing, B. (2002): Leuchtende Kunststoffe. In: Fraunhofer Magazin 3/2002, S. 30-31.

Norman, D. A. (1998): The Invisible Computer. Cambridge, Mass.: MIT Press.

Otten, D. (2002): Maxidisplays und Miniprojektoren. In: Pictures of the Future Frühjahr 2002.

Paradiso, J. (2000): Renewable Energy Sources for the Future of Mobile and Embedded Computing. Invited talk at Computing Continuum Conference, San Francisco, 16 March 2000.

Pompei, F. J.; Sharon, T.; Buckley, S. J.; Kemp, J. (2002): An Automobile-Integrated System for Assessing and Reacting to Driver Cognitive Load. In: Proceedings of Convergence 2002. IEEE SAE, S. 411-416.

Pribat, D. (2002): FEDs in the Landscape of Flat Panel Displays: Strengths and Weaknesses. Paper presented at the 15th International Vacuum Microelectronics Conference and 48th International Field Emission Symposium (IVMC & IFES 2002), Lyon, France, July 7-11, 2002.

Rannenberg, K.; Pfitzmann, A.; Müller, G. (1996): Sicherheit, insbesondere mehrseitige IT-Sicherheit. In: Informationstechnik und Technische Informatik (it+ti) 38, Nr. 4, S. 7-10.

Schneier, B. (2000): Secrets and Lies: Digital Security in a Networked World. New York: Wiley.

Shor, P. W. (1994): Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20–22, 1994: IEEE Computer Society Press, S. 124–134.

Singh, S. (2000): Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. Frankfurt am Main: Büchergilde Gutenberg.

Soong, R. K.; Bachand, G. D.; Neves, H. P. et al. Powering an Inorganic Nanodevice with a Biomolecular Motor. In: Science 290, S. 1555-1558.

Stucki, D.; Gisin, N.; Guinnard, O. et al. (2002): Quantum key distribution over 67 km with a plug & play system. In: New Journal of Physics 4, S. 41.1-41.8.

Tittel, W.; Brendel, J.; Gisin, N. et al. (1999): Quantenkryptografie. In: Physikalische Blätter 55, Nr. 6, S. 25-30.

Want, R.; Borriello, G. (2000): IEEE Computer Graphics and Applications20, Nr. 3 (Special Issue on Information Appliances).

Weiser, M. (1991): The Computer for the 21st Century. In: Scientific American 265, Nr. 3, S. 66-75.

Weissman, C. (1991): A national debate on encryption exportability, in: Communications of the ACM, 34(1991), Nr. 10, S. 162.