

Photoadressierbare Polymere – eine Lösung für die Speicherung großer, sensibler Datenmengen auf Plastikkarten

H. Jüngermann, S. Völkening, T. Hupe ¹

Kurzfassung

Plastikkarten zur Authentisierung sind heute allgegenwärtig. Im Portemonnaie der meisten Bürger befinden sich eine Vielzahl davon, z.B. Kreditkarte, Bankkarte, Mitarbeiter- und Krankenkassenausweis. An eine Multifunktionskarte, die einen Großteil der Karten durch eine einzige ersetzen soll, werden folgende Anforderungen gestellt: Kontrollmöglichkeit der Zugriffsrechte, Sicherstellung der Privatsphäre, hohe Speicherkapazität, Fälschungssicherheit und akzeptable Kosten auch für die Schreib-/Lesegeräte.

Diese Anforderungen werden von einem Kartensystem auf Basis photoadressierbarer Polymer als Speichermedium und einer speziellen holographischen Speichertechnik erfüllt.

Auf einer Karte lassen sich mehrere Hundert MByte an Daten unterbringen. Die Daten werden in Form von unsichtbaren Polarisationshologrammen abgelegt. Sie werden optisch mit einem Laserstrahl ausgelesen. Durch eine Hardware-Kodierung, d.h. eine Modulation des Laserstrahls, können Zugriffsrechte geregelt werden: nur wenn die richtige Modulation bekannt ist, kann auf die Daten zugegriffen werden; für jede Anwendung lässt sich ein anderer Modulationsschlüssel verwenden. Die Ver- und Entschlüsselung erfolgen analog, d.h. es lassen sich sehr hohe Schlüssellängen realisieren, ohne dass die Zeit zur Ver- oder Entschlüsselung ansteigt.

Die Fälschungssicherheit ist dadurch gegeben, dass die Hologramme nicht kopiert und ohne Wissen des Schlüssels nicht ausgelesen werden können.

Die Manipulation der Daten ist ausgeschlossen, da in einem Hologramm keine einzelnen Informationseinheiten erkennbar sind, sondern die Information stets nur als Ganzes auslesbar ist.

Die Kombination der photoadressierbaren Speicherpolymere mit der speziellen holographischen Speichertechnik erlaubt die Ablage großer Mengen sensibler Daten auf preisgünstigen Plastikkarten und ist daher auch für die Realisierung einer Multifunktionskarte geeignet.

Stichworte: Holographische Datenspeicherung, Hardware-Verschlüsselung, Multifunktionskarte, photoadressierbare Polymere

¹ Bayer Innovation GmbH, Düsseldorf

1. Einleitung

Durch die wachsende Vernetzung und die zunehmende Globalisierung der Gesellschaft wird es immer wichtiger, dass jede einzelne Person in die Lage versetzt wird, sich eindeutig zu authentifizieren.

Früher reichte im Allgemeinen ein Personalausweis, um eine Identität nachweisen zu können. In Folge der zunehmenden maschinellen Datenverarbeitung verfügt ein Mensch heute zusätzlich über einen Firmenausweis, einen Krankenkassenausweis, eine Kredit- oder EC-Karte – alles Instrumente, mit denen er nachweisen kann, dass er derjenige ist, den er vorgibt zu sein. Diese Grundlage verschafft ihm Zugang zu seinem Arbeitsplatz, zu Krankenkassenleistungen, zu seinem Konto usw.

Und ein Ende der Einsatzmöglichkeiten ist noch nicht abzusehen. Bereits intensiv diskutiert wird die Einführung der Gesundheitskarte, daneben gibt es Überlegungen zu einer Jobkarte und anderen Ausweissystemen.

Aufgrund der Vielfältigkeit der Anwendungen ist davon auszugehen, dass die Zahl der Ausweiskarten zukünftig noch steigen wird – es sei denn, eine Multifunktionskarte ließe sich umfassend realisieren.

Hierbei steht im Zentrum der Überlegungen weniger der Abgleich und die Harmonisierung bestehender Authentifizierungsverfahren, als vielmehr die Eignung des Ausweissystems, mehr als nur die spezifische Ausweisfunktion zu erfüllen. Hierbei spielen drei Aspekte eine maßgebliche Rolle:

- Die Privatsphäre einer Person muss gewahrt sein, d.h. beim Auslesen der Karte dürfen Personen nur auf die für sie bestimmten Informationen Zugriff haben.
- Ein kombiniertes System stellt höhere Anforderungen an den Speicherplatz. Auf den heute gebräuchlichen Karten befindet sich ein Magnetstreifen oder ein Chip; die Speicherkapazität beschränkt sich bei den heute zu akzeptablen Preisen verfügbaren Speicherkarten auf etwa 100 KB.
- Schließlich entscheiden auch die Kosten von Multifunktionskarten und der dazugehörigen Schreib- und Lesegeräte über deren breite Einführung.

Im Folgenden soll eine neue Speichertechnologie vorgestellt und diskutiert werden, welche die genannten Vorgaben berücksichtigt.

Die Frage, die geklärt werden soll, lautet: Wie kann man eine große Menge an Daten so auf einer Karte abspeichern, dass Personen nur die Daten auslesen können, die für sie bestimmt sind? Dabei soll die Karte sicher gegenüber Fälschung und Manipulation und darüber hinaus auch noch preiswert sein.

Die Antwort liegt in der Kombination eines optischen Speichermaterials mit einer besonderen Speichertechnik, der Polarisationsholographie, und einer Hardware-Verschlüsselung. Die genannten Komponenten werden im Folgenden näher vorgestellt.

2. Das Speichermaterial

Das Speichermaterial muss preiswert sein, eine hohe Speicherdichte garantieren und über Möglichkeiten der sicheren Datenablage verfügen. Diese Punkte werden durch so genannte photoadressierbare Polymere erfüllt. Dieses Material ist licht-aktiv, genauer gesagt sind es bestimmte Molekülgruppen im Polymer, die auf Lichteinstrahlung reagieren. Diese Molekülgruppen richten sich aus, wenn polarisiertes Licht einer bestimmten Wellenlänge auf sie trifft. Dies ist in Abb. 1 illustriert.

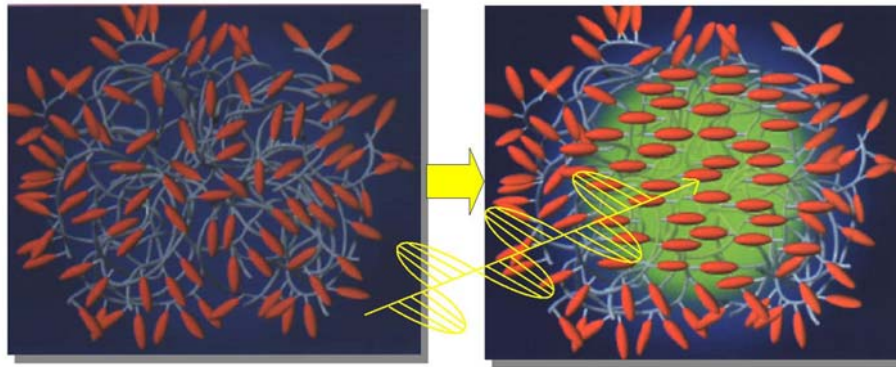


Abb. 1: Durch Bestrahlen mit polarisiertem Laserlicht richten sich die Polymere im Speichermaterial aus. Die Ausrichtung bleibt auch bei Abschalten des Lichts erhalten, so dass sich auf diese Weise Informationen einschreiben lassen.

Dabei bestimmt die Polarisationsrichtung des Lichts die Orientierung der Molekülgruppen im Polymer. Wird das Licht fokussiert, d.h. örtlich begrenzt, so werden nur diejenigen Bereiche im Polymer ausgerichtet, die vom Licht erfasst werden. Auf diese Weise lassen sich Informationen in das Polymer einschreiben. Dabei liegt die Information in Form von Bereichen lokaler Ordnung auf molekularer Ebene in einem ansonsten ungeordneten Polymer vor.

Um die Information auslesen zu können, bestrahlt man das Polymer wieder mit polarisiertem Licht. Strahlt man mit dem polarisierten Licht durch das Polymermaterial, so wirkt das Polymer vereinfachend ausgedrückt wie ein Filter. Eine Lichtwelle mit der Polarisationsrichtung parallel zu den ausgerichteten Molekülen wird ungehindert durchgelassen. Eine Lichtwelle mit der Polarisationsrichtung senkrecht zu den

ausgerichteten Molekülen wird nicht durchgelassen. Auf diese Weise lassen sich ungeordnete und geordnete Bereiche im Polymer unterscheiden und die eingeschriebene Information lässt sich auslesen.

Die theoretische Speicherdichte des Materials wird durch die Wellenlänge λ des verwendeten Schreib- und Leselichts beschränkt; sie beträgt $1 / \lambda^2$. Bei Verwendung eines Lasers mit einer Wellenlänge von $\lambda = 532 \text{ nm}$ ergibt sich eine Speicherdichte von $3,5 \text{ Mbit} / \text{mm}^2$. Dies reicht für eine Vielzahl von Anwendungen aus.

Es liegt also ein Speichermaterial vor, das sich mit polarisiertem Licht beschreiben und auslesen lässt. Informationen ließen sich darin wie auf einer CD oder DVD abspeichern, d.h. digital in Form von Nullen und Einsen, wobei die Einsen z.B. die geordneten Bereiche im Polymer darstellen, die Nullen die ungeordneten. Eine solche Speicherung hat jedoch den Nachteil, dass sie leicht ausgelesen werden kann; es bedarf lediglich eines polarisierten Lichtstrahls. Die Daten müssten auf digitaler Ebene verschlüsselt werden und man müsste Informationen, die für unterschiedliche Personen bestimmt sind, digital mit unterschiedlichen Schlüsseln verschlüsseln.

Neben einer komplexen Schlüsselverwaltung hätte dies den Nachteil, dass Brute-Force-Methoden mit einem Computer angewandt werden könnten, um die Informationen zu entschlüsseln, sobald jemand die Nullen und Einsen ausgelesen hat.

Daher soll an dieser Stelle ein anderer Weg gewählt werden: Informationen werden holographisch gespeichert.

3. Holographische Datenspeicherung

Ein Hologramm stellt ein Interferenzmuster dar, das durch Überlagerung von zwei Lichtstrahlen entsteht. Dies ist in Abb. 2 illustriert.

Ein Laserstrahl wird zunächst in zwei Teilstrahlen aufgeteilt. Der eine Teilstrahl wird durch eine Maske geleitet. Auf diese Weise werden dem Strahl die zu speichernden Informationen aufgeprägt. Der zweite Teilstrahl ist der so genannte Referenzstrahl. Dieser wird so umgeleitet, dass er mit dem Informationsstrahl im photoadressierbaren Polymer überlagert wird. Dadurch entsteht in dem Material ein spezielles Muster (Interferenzmuster), das Hologramm.

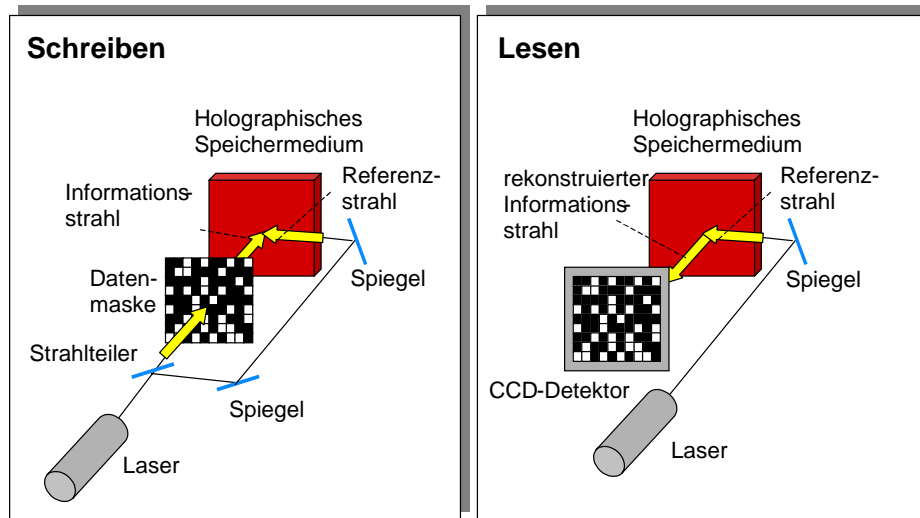


Abb. 2: Schematische Darstellung eines holographischen Speicherverfahrens. Die Informationen werden in Form von Datenmasken eingeschrieben. Dabei wird nicht die Datenseite selbst gespeichert, sondern die holographisch verschlüsselte Datenseite. Details siehe Text.

Dieses Hologramm hat folgende Eigenschaften:

- Bestrahlt man das Hologramm nur mit dem Referenzstrahl, so wird der Informationsstrahl reproduziert (Abb. 2 rechts), das heißt, die Information kann wieder sichtbar gemacht werden.
- In einem Hologramm sind die gespeicherten Daten auch auf mikroskopischer Ebene nicht mehr zu erkennen. Während bei optisch digital gespeicherten Informationen eine Reihe von Nullen und Einsen direkt einer Informationseinheit zugeordnet werden kann, ist eine Informationseinheit im Hologramm über die gesamte Fläche „verschmiert“. Dies lässt sich wie folgt zeigen: Zerbricht man das Hologramm in zwei Teile, so erhält man bei Bestrahlung der einzelnen Teile jeweils ein komplettes Bild, das jedoch etwas kontrastärmer ist. Damit wird deutlich, dass jede Informationseinheit in allen Teilen des Hologramms gespeichert und nicht lokalisierbar ist. Daraus folgt, dass eine Manipulation der Daten ausgeschlossen ist. Man kann nicht einfach einzelne Bits verändern. Wenn man Bereiche im Hologramm vernichtet (z.B. durch Kratzer), wird die Information zunehmend kontrastärmer, verschwindet jedoch nicht und wird auch nicht inhaltlich verändert.
- Sollte man das Hologramm auf mikroskopischer Ebene sichtbar machen können, so ist es nicht möglich, aus dem Muster die Daten zu extrahieren.

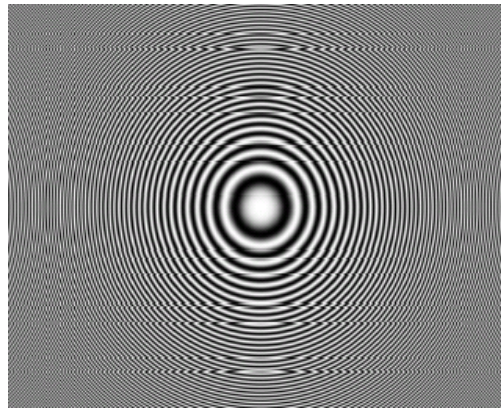


Abb. 3: Schematische Darstellung eines Hologramms. Die Information ist nicht lokalisierbar, sondern als Interferenzmuster über das gesamte Hologramm, „verschmiert“.

4. Hardware-Verschlüsselung

Die Holographie bietet die Möglichkeit einer analogen Hardware-Verschlüsselung. Die Information kann aus dem Hologramm durch Bestrahlen mit dem Referenzstrahl ausgelesen werden. Wurde der Referenzstrahl beim Einschreiben der Information moduliert, so muss auch beim Auslesen diese Modulation verwendet werden. Ansonsten erhält man nur Rauschen. D.h., nur wer die Modulation kennt, kann die Daten lesen.

Die Kodierung des Referenzstrahls erfolgt ebenfalls mit einer Maske (siehe Abb. 4).

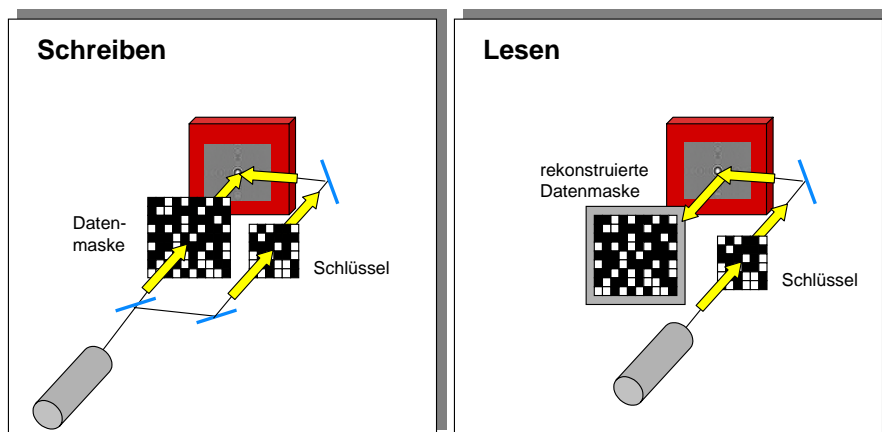


Abb. 4: Schematische Darstellung der Hardware-Verschlüsselung bei der holographischen Datenspeicherung. Nur wenn der Referenzstrahl mit der richtigen

Schlüsselmaske moduliert wird, kann die vorher eingeschriebene Datenmaske rekonstruiert werden.

Sollen Daten für verschiedene Anwendungen auf der Karte gespeichert werden, werden einfach verschiedene Masken verwendet. Die Bank erhält Lesegeräte mit der Maske, mit der die Bankdaten auf der Karte verschlüsselt sind, der Arzt Lesegeräte mit der Maske, mit der die medizinischen Informationen verschlüsselt sind. Dabei müssen die Masken nicht statisch sein. Es lassen sich programmierbare Masken, so genannte *Spatial Light Modulator* verwenden, die für den Kunden entsprechend programmiert werden.

5. Sicherheitstechnische Bewertung

Durch die analoge Verschlüsselung lassen sich sehr hohe Schlüssellängen realisieren, ohne dass ein höherer „Rechenaufwand“ zur Entschlüsselung erforderlich wäre, wie dies bei digitalen Verfahren der Fall ist.

Der erforderliche Aufwand zum „Knacken“ des Codes mittels Brute-Force-Methoden kann damit fast beliebig hoch getrieben werden.

Durch die Verschlüsselung wird auch die Privatsphäre des Kartenbesitzers gewährleistet. Daneben lässt sich der Schlüssel zum Auslesen der Daten aufteilen: einen Teil des Schlüssels erhält der Kartenbesitzer, den anderen Teil der Betreiber. Das Auslesen der Karte erfolgt nur, nachdem der Kartenbesitzer seinen Teil in Form einer PIN oder eines biometrischen Merkmals in das Lesegerät eingegeben hat. Ein Auslesen ohne Autorisierung durch den Kartenbesitzer wird verhindert.

Für die Fälschungssicherheit ist erforderlich, dass die holographisch kodierten Informationen nicht kopiert werden können. Die kleinsten Strukturen in dem Hologramm sind in der Größenordnung der Wellenlänge des Lichts, das zum Einschreiben der Daten verwendet wurde. Sie können mit einem Polarisationsmikroskop nicht sichtbar gemacht und kopiert werden. Eine analoge Kopie durch ein holographisches Verfahren, wie es beim so genannten *Contact Printing* erfolgt, ist hier ebenfalls ausgeschlossen. Durch die spezielle Verwendung der Polarisationsholographie können analoge Kopien einfach erkannt werden.

Schließlich verhindert die holographische Speicherung eine Manipulation der Daten, wie in Abschnitt 3 beschrieben wurde.

6. Zusammenfassung

Ausgangspunkt dieser Abhandlung war die Suche nach einer Möglichkeit, eine große Menge an Daten sicher auf einer preiswerten Karte so abzulegen, dass nur autorisierte Personen Zugriff auf die für sie bestimmten Informationen haben.

Das in den vergangenen Abschnitten im Detail vorgestellte holographische Speicherverfahren in einem Speichermedium aus einem photoadressierbaren Polymer ist nach Ansicht der Autoren in der Lage, diese Anforderungen zu erfüllen. Die Elemente, die eine hohe Sicherheit gegenüber Fälschung, Manipulation, ungewolltem Auslesen und Kopie gewährleisten, wurden angesprochen.

In dem Vortrag sollen verschiedene Angriffsszenarien durchgespielt und gezeigt werden, wie hoch der Aufwand zur Überwindung der Technologie ist.

Vor diesem Hintergrund werden mögliche konkrete Anwendungen der Technologie aufgezeigt.