Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses

Band: 81 (1990)

Heft: 5

Artikel: Die Chipkarte als kryptographisches Werkzeug

Autor: Forré, Réjane

DOI: https://doi.org/10.5169/seals-903091

Die Chipkarte als kryptographisches Werkzeug

Réjane Forré

Plastikkarten mit eingebetteter integrierter Schaltung (Chipkarten) werden in der Zukunft immer mehr an Bedeutung gewinnen. Ihre verschiedenen Einsatzmöglichkeiten werden beschrieben, wobei der Schwerpunkt auf Sicherheitsaspekte gesetzt wird. Anschliessend wird die Problematik bei der Implementierung von kryptographischen Algorithmen in Chipkarten betrachtet.

Les cartes en plastique munies de circuits intégrés (cartes à puces) sont appelées à prendre de plus en plus d'importance dans l'avenir. Les différentes applications possibles de ces cartes à puces sont décrites en mettant l'accent sur l'aspect sécurité des systèmes. Ensuite, les problèmes liés à l'implémentation d'algorithmes cryptographiqués dans des cartes à puces sont considérés.

Adresse der Autorin

Réjane Forré, Dipl. El.-Ing. ETH, Inst. für Kommunikationstechnik, ETH-Zentrum, 8092 Zürich

Die Idee, in eine Plastikkarte eine integrierte Schaltung einzubauen, wurde im Jahre 1974 vom französischen Journalisten Roland Moreno patentiert. Verschiedene französische Unternehmen und Banken sowie die PTT haben Kommerzialisierungsanstrengungen und Pilottests intensiv unterstützt, einerseits um eine weltweit führende Position auf diesem Gebiet zu erreichen, anderseits weil die Chipkarte als eine potentielle Lösung für die Probleme des explodierenden Checkverkehrs und der zahlreichen Vandalenakte in öffentlichen Telefonkabinen angesehen wurde.

Verschiedene Arten von integrierten Schaltungen (Chips) können in Chipkarten eingebaut werden: es kann sowohl ein kompletter Mikroprozessor, wie auch ein hochspezialisierter Chip, ein Speicherbaustein oder ein einfaches kombinatorisches Netzwerk sein. Manchmal wird der Name *Chipkarte* auch nicht kartenförmigen (aber leicht tragbaren) Gegenständen gegeben, doch ist das Kreditkartenformat am meisten verbreitet.

Die Ähnlichkeit zwischen der traditionnellen Magnetstreifenkarte und der Chipkarte soll nicht überschätzt werden. Von aussen sehen sie praktisch gleich aus, mit Ausnahme der elektrischen Kontakte der Chipkarte. Zwar kann eine Chipkarte in allen Anwendungsbereichen eingesetzt werden, in denen die Magnetstreifenkarte bis jetzt gebraucht wurde, aber die Fähigkeiten der Chipkarte gehen weit darüber hinaus; ihre integrierte Rechenleistung macht sie zu einem aktiven Element. Die Hauptschwächen der Magnetstreifenkarte sind:

- Ihr Speicherplatz ist begrenzt.
- Sie ist rein passiv und ihr Inhalt kann mit verhältnismässig kleinem Aufwand gelesen oder überschrieben werden.
- Die Magnetstreifenlesegeräte benötigen mechanisch aufwendige Vorrichtungen und dürften deshalb in den nächsten Jahren keinen massiven Preissturz erfahren.

Im Vergleich dazu schneidet die Chipkarte gut ab:

- Sie verfügt über 10 bis 100mal mehr Speicherkapazität.
- Sie kann mit festverdrahteter Logik oder mit einem Mikroprozessor ausgerüstet sein. In beiden Fällen kann der Zugang zu gewissen Speicherbereichen gesperrt oder nur nach Eingabe einer korrekten PIN (persönliche Identifikationsnummer) geöffnet werden. Die Information wird als Ladung gespeichert, was eine lichtoptische oder chemische Erkennung verhindert. In den meisten Fachkreisen ist man davon überzeugt, dass auch die aufwendigsten Analyseverfahren der Halbleitertechnik versagen, wenn der Chiphersteller absichtlich Hindernisse vorsieht. Andere Fachkreise schliessen die Möglichkeit einer Analyse mit Elektronenmikroskop nicht aus, aber der Aufwand und die Kosten einer solchen Analyse (wenn sie überhaupt machbar ist) sind mit denjenigen einer Magnetstreifenanalyse nicht zu vergleichen. Prozessorkarten sind ausserdem in der Lage, Sicherheitskontrollen und Ver- und Entschlüsselung selber vorzunehmen.
- Die Chipkarte hat einen einfachen, rein elektrischen Anschluss und kann von einfachen und billigen Endgeräten betrieben werden.

Nun ist es jedoch eine Tatsache, dass die Magnetstreifenkarte schon sehr verbreitet ist, und dass viel Geld in die zugehörige Infrastruktur investiert wurde (Banknotenautomaten, Lesegeräte usw.). Die Chipkarte hat viel bessere Chancen, akzeptiert zu werden, wenn sie in einer ersten Phase mit dieser bestehenden Infrastruktur kompatibel ist. Hybridkarten mit

einem Magnetstreifen auf der Rückseite und Chipkontakten auf der Vorderseite werden bereits hergestellt.

Es ist noch zu erwähnen, dass der Einbau einer integrierten Schaltung in eine Plastikkarte eine echte technische Herausforderung darstellt, vor allem wenn die Karte eine gewisse Strapazierfähigkeit besitzen muss. Um brauchbar zu sein, müssen Chipkarten genügend flexibel sein (Biegungs- und Torsionsbeanspruchungen), Temperaturunterschiede tolerieren und gegenüber elektrostatischen Ladungen und UV-Licht stabil bleiben. Die elektrischen Kontakte müssen funktionsfähig bleiben, auch wenn sie nicht mehr restlos sauber sind. Wegen der Flexibilitätsanforderung dürfen die Chips eine maximale Fläche von etwa 25 mm^2 nicht übersteigen, was eine obere Schranke für die Rechenleistung (C8-Bit-Mikroprozessor) und die Speicherkapazität ergibt. Diese Schranke ist allerdings von der Technologie abhängig und dürfte in Zukunft heraufgesetzt werden.

Im vorliegenden Bericht wird der Akzent auf Sicherheitsaspekte gesetzt, insbesondere auf den Einfluss der Chipkartengrenzen (bezüglich Rechen- und Speicherkapazität) auf die Auswahl, den Entwurf und die Implementierung von kryptographischen Algorithmen.

Grundlagen über Chipkarten und deren Anwendungen

Klassifizierung von Chipkarten

Unter dem Sammelbegriff Chipkarten werden alle Plastikkarten (oder tragbare Gegenstände) eingeordnet, die eine integrierte Schaltung beinhalten. Je nach dem Aufbau dieser Schaltung und den Merkmalen der Karte unterscheidet man verschiedene Kartentypen.

1. Speicherkarten: Sie enthalten ausschliesslich Speicherchips, sind daher einfach, billig und passend für Massenapplikationen, in denen nur eine kleinere Menge Information benötigt wird und keine hohen Sicherheitsanforderungen gestellt werden (vorbezahlte Telefonkarten, öffentliche Verkehrsmittel).

2. Karten mit festverdrahteter Logik: Bei diesem Typ von Karten besteht die Möglichkeit, verschiedene Speicherbereiche mit unterschiedlichen Schutzniveaus zu versehen (Schutz vor Lesen, vor Schreiben oder beides). Solche Karten können personalisiert werden, indem der Zutritt zu gewissen gespeicherten Daten erst nach der Eingabe einer korrekten PIN möglich ist.

3. Prozessorkarten: Diese Karten erfüllen die meisten Anforderungen, die bei Hochsicherheitsanwendungen üblich sind. Sie bestehen aus einem 8-Bit-Mikroprozessor und aus einer - den Bedürfnissen entsprechenden - Auswahl von verschiedenartigen flüchtigen (RAM) und nichtflüchtigen Speicherbereichen (ROM, PROM, EPROM, EEPROM, weiter unten kurz beschrieben). Solche Karten sind in der Lage, gewisse Berechnungen und Kontrollen durchzuführen. Sie können beispielsweise Daten chiffrieren und dechiffrieren. Ein von Bull patentiertes Verfahren erlaubt solchen Karten, sich selbst zu programmieren: die Daten und Programme im EPROM-Speicher können von der Karte verändert werden, gemäss Vorschriften, die durch die ROM-Programme gegeben sind.

4. Prozessorkarten mit Tastatur und Anzeige: Nebst den oben erwähnten Merkmalen sind die sogenannten *Super Smart Cards* mit einer eingebauten elektrischen Speisung (z.B. 3-V-Lithium-Batterie), einer Tastatur und einer Anzeige versehen. Der entscheidende Vorteil dieses Kartentyps betrifft die Sicherheit. Er wird weiter hinten näher erläutert. Dank der internen Batterie sind für solche Karten flüchtige Speichertypen einsetzbar.

Die beiden letzten Kartentypen werden manchmal als *intelligente Karten* bezeichnet.

Es gibt *Single-Chip-* und *Multi-Chip-*Kartenausführungen. Letztere hat den Vorteil einer grösseren Speicherkapazität, aber die Nachteile einer aufwendigen Kartenproduktion und der - mit verhältnismässig kleinem Aufwand - abhörbaren Verbindung zwischen CPU (Central Processing Unit) und Speicherchip. Heutzutage werden für Sicherheitsanwendungen vor allem Single-Chip-Karten eingesetzt.

Im nebenstehenden Rahmen sind kurz die Besonderheiten der verschiedenen Speichertypen erläutert. Je nach geplanter Anwendung kann der eine oder der andere Speichertyp vorteilhaft sein.

Die Normung der Karten wird zum grössten Teil von zwei ISO-Arbeitsgruppen vorgenommen. Bis heute sind aber nur wenige von den notwendigen Chipkarten-Standards definitiv festgelegt.

Applikationen von Chipkarten

Die möglichen Applikationen von Chipkarten können in folgende vier Kategorien eingeteilt werden [25]:

1. Elektronisches Geld: z.B. Bancomat, Zahlungsmittel beim POS (Point Of Sale), Telefonwertkarten (Ersatz von Münzen), Kreditkarten, bargeldloser elektronischer Zahlungsverkehr (EFT, Electronic Funds Transfer und FTC, Financial Transaction Card) usw.

2. Zugriffskontrolle: z.B. Zugriff zu Gebäuden, zu Räumen, zu PCs und Hostrechnern, zu Softwarepaketen, zu Videotex-Diensten, zu gebührenpflichtigen Fernsehketten usw.

3. Persönliche Dateien: z.B. medizinische Daten, Studienbuch, Ausweise und Lizenzen, militärische Personaldaten, Taschenkartei usw.

Speichertypen

ROM (Read Only Memory): kann in grossen Mengen mit einem einheitlichen Informationsinhalt (Programme) hergestellt werden. Diese Information kann nicht mehr verändert werden.

PROM (Programmable Read Only Memory): ist irreversibel programmierbar, mit Hilfe von relativ hohen Strömen, die ausgewählte Verbindugen zum Schmelzen bringen.

EPROM (Erasable Programmable Read Only Memory): kann mit genügend hohen Spannungen (21-25 V) beschrieben werden. Die geschriebene Information kann nicht selektiv gelöscht werden, aber mit UV-Licht kann der ganze Informationsinhalt vernichtet werden. Die heutigen (UV-geschützten) Chipkarten können allerdings nicht mit UV-Licht bestrahlt werden, ohne dass dabei die Karte zerstört wird.

EEPROM (Electrically Erasable Programmable Read Only Memory): ein selektives Löschen und Schreiben von Speicherbereichen ist mit rein elektrischen Mitteln möglich. Von 10 000 bis zu 100 000 Schreibzyklen sind von den Herstellern garantiert. Die Chipfläche ist um den Faktor 3 grösser als diejenige von EPROM-Chips.

RAM (Random Access Memory): flüchtiger Speichertyp, der als Arbeitsspeicher für CPU-Operationen (in Karten ohne interne Speisung) und auch als Datenspeicher in den Super Smart Cards eingesetzt wird.

4. Übernahme von Routinefunktionen: z.B. Inbetriebnahme von Geräten, von Überwachungssystemen usw.

Die Vorteile der Chipkarte als FTC sollen hier anhand des Beispiels des jetzigen Bancomat Systems erläutert werden.

In den letzten zehn Jahren hat die Anzahl Banknotenautomaten dank einer allgemein guten Kundenakzeptanz massiv zugenommen. Die Funktionsweise eines solchen Banknotenautomaten wird anhand des Beispiels in Bild 1 erläutert[1].

Der Benutzer steckt seine Karte in den Automat und gibt seine PIN ein. Das Endgerät liest gewisse Daten von der Karte ab (Bank- und Kundenidentifikation, Kontonummer, Tagesabzüge, Einweg-Abbildung E_Z [PIN] der PIN...). Das Endgerät berechnet selber die - von einem geheimen Schlüssel Z abhängige - Einweg-Abbildung E_Z der vom Benutzer eingegebenen PIN und vergleicht das Resultat mit dem in der Karte gespeicherten Sollwert. Falls die beiden Werte nicht übereinstimmen, wird der Benutzer aufgefordert, nochmals seine PIN einzugeben. Nach dreimaliger falscher PIN-Eingabe wird die Karte gesperrt, und zwar direkt beim Hostrechner, sonst könnte der unberechtigte Kartenbenutzer bei einem anderen Endgerät weitere Versuche machen. Falls die beiden Werte von E_Z (PIN) übereinstimmen, muss das Endgerät noch kontrollieren, ob die Karte in einer Sperrliste aufgeführt ist (gestohlene oder verlorene Karte). Es kann unter Umständen diese Kontrolle vom Hostrechner (z.B. Hostrechner der Bank) durchführen lassen. Dieses System ist durch Offline-PIN-Kontrolle charakterisiert. Bei jedem Wechsel des Schlüssels Z müssen sämtliche Karten und Endgeräte entsprechend modifiziert werden (d.h. mit dem neuen E_Z [PIN] bzw. mit dem neuen Z versehen werden).

Es gibt zahlreiche Varianten zu diesem Schema. Die PIN kann beispielsweise gar nicht in der Magnetkarte gespeichert sein, auch nicht als Einweg-Abbildung, was für die PIN-Kontrolle einen Online-Betrieb (d.h. mit Verbindung zu einem Hostrechner) erfordert. Dabei soll das Endgerät E_Z (PIN) berechnen und zum Hostrechner senden. Der Hostrechner vergleicht den empfangenen Wert mit dem in seinen Dateien vorhandenen Sollwert für den entsprechenden Kunden und sendet dem Endgerät den Entscheid zurück, ob die Transaktion weitergeführt werden darf oder nicht.

Bei jeder Variante von mit Magnetkarten funktionierenden Banknotenautomaten stellen sich folgende grundsätzliche Probleme:

- Die Banknoten müssen vorbereitet werden, sie müssen flach und sauber sein, und der Automat muss regelmässig wieder aufgefüllt werden.
- Der Automat muss mechanisch geschützt sein (robustes Material und meistens fest in einer Mauer eingebaut).
- Der Automat muss über einen Verschlüsselungsalgorithmus verfügen.
- Der Geheimschlüssel Z muss auf sichere Art verteilt und regelmässig geändert werden (beim Hostrechner und beim Endgerät für Online-Systeme, beim Endgerät und auf der Karte für Offline-Systeme).
- Als passives Element kann eine Magnetstreifenkarte die Authentizität eines Endgerätes nicht nachprüfen. Das Vertrauen des Benutzers stützt sich vor allem auf die Tatsache, dass jetzige fest eingebaute Notenautomaten im allgemeinen schwierig zu fälschen sind. Identifiziert wird nur die Karte und der Benutzer.
- Wie schon gesagt, sind die Magnetstreifenkarten kein sicheres Speichermedium; sie können mit kleinem Aufwand gelesen und nachgeahmt werden.

Wenn anstelle von Bancomaten ein auf Chipkarten basierendes POS-Zahlungssystem eingesetzt wird, ergeben sich folgende Vorteile:

- POS-Endgeräte enthalten hauptsächlich elektronische Schaltungen, sind demzufolge billig und können einen grossen Verbreitungsgrad erreichen. Die physikalische Robustheit von Bancomaten wird durch eine mathematische (kryptographische) Robustheit ersetzt.
- Die Benutzeridentität wird von der Karte selbst kontrolliert. Das Endgerät benötigt keinen Verschlüsselungsalgorithmus.
- Ein Chiffrierschlüssel Z kann für jede Session (mittels eines angepassten kryptographischen Schlüsselaustauschprotokolles) von der Chipkarte und vom Hostrechner berechnet werden, in Abhängigkeit von einem geheimen Kartenschlüssel und von frisch generierten Zufallszahlen.
- Die Chipkarte kann ihren Gesprächspartner identifizieren (mittels geeigneter kryptographischer Protokolle). Die Identifikation kann somit gegenseitig sein.
- Die Transaktionsdaten (Betrag, Datum, Uhrzeit, Händler usw.) können direkt auf der Chipkarte gespeichert werden (weniger Papierhandhabung).

Der Vollständigkeit halber müssen noch folgende momentane Mängel der Chipkarte erwähnt werden:

- Die Chipkarte ist im Vergleich zur Magnetstreifenkarte noch teuer, und ihre Dauerhaftigkeit ist zurzeit nicht genügend nachgewiesen.
- Zum Teil fehlen noch die Standards, weshalb viele potentielle Chipkartenanwender mit grossen Investitionen noch zuwarten.
- Die nötige Sicherheitslogik (kryptographische Protokolle und Algorithmen, Erzeugung von Pseudozufallszahlen usw.) ist zum Teil nicht vorhanden oder nicht befriedigend.

Sicherheitsaspekte bei Chipkartensystemen

Zwei Grundkonfigurationen von automatisierten Chipkartensystemen können unterschieden werden: Online- und Offline-Systeme [11].

Bei einem Online-System besteht eine (permanente oder momentane) Verbindung zu einer zentralen Über-

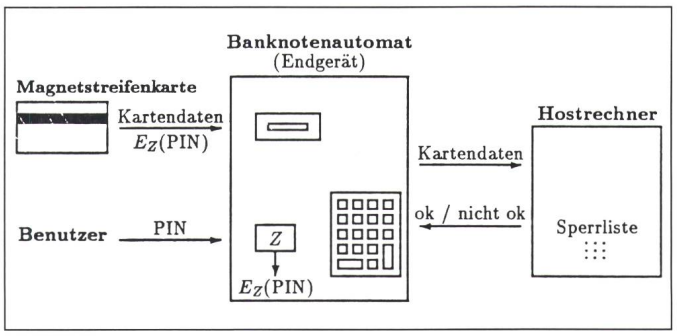


Bild 1
Beispiel für den Ablauf einer Transaktion bei einem konventionellen Banknotenautomaten mit Magnetstreifenleser.

Die PIN wird vom Endgerät selber geprüft. Der Hostrechner sorgt lediglich für die Kontrolle von Sperrlisten (Off-Online-Hybridsystem).

[1] Dieses Beispiel entspricht nicht notwendigerweise dem schweizerischen Bancomat-System, es ist aber bezüglich Schwächen von auf Magnetstreifenkarten basierenden Systemen repräsentativ.

wachungsstelle (Hostrechner), die gewisse Kontrollen (Authentizität der Karte, Restsaldo, Autorisierungslisten, Sperrlisten usw.) durchführt. Da die Identität des Benutzers von seiner eigenen Karte verifiziert wird (PIN oder physiologische Merkmale), spielt das Kartenlesegerät eine reine Vermittlungsrolle und braucht über keine kryptographischen Algorithmen oder Schlüssel zu verfügen. Die Authentizität des Endgerätes wird von der zentralen Überwachungsstelle kontrolliert.

Anders sieht es bei Offline-Konfigurationen aus, wo das Endgerät die Kartenauthentizität prüfen und die Transaktionsdaten auf sichere Art speichern muss. Von Zeit zu Zeit müssen natürlich alle durchgeführten Transaktionen dem Hostrechner mitgeteilt werden. Bei solchen Offline-Konfigurationen besteht die Gefahr eines verfälschten Endgerätes, das zum Beispiel die PIN abspeichert oder vertrauliche Informationen von der Karte abliest. Das Display des Endgerätes könnte auch betrügerisch sein und einen Geldbetrag anzeigen, der mit dem intern verarbeiteten Betrag nicht übereinstimmt. In einer Offline-Konfiguration sollte demzufolge den Super Smart Cards der Vorzug gegeben werden.

- Sie haben eine eigene Tastatur, mit der der Benutzer seine PIN eingeben kann. Die PIN wird dann in der Karte selbst kontrolliert und ist somit nie ausserhalb der Karte verfügbar.
- Sie haben ein eigenes Display und der Benutzer kann sich versichern, dass die angezeigten Beträge auf der Karte und dem Endgerät übereinstimmen.

Der grosse Vorteil der Offline-Konfiguration steckt in den geringeren Kosten. Allerdings muss für gewisse Kontrollen (z.B. Sperrlisten, Restsaldokontrolle) doch eine Verbindung zur zentralen Überwachungsstelle aufgebaut werden. Falls die Sperrlisten nicht zu umfangreich sind, können Kopien davon periodisch den Endgeräten mitgeteilt, bei ihnen gespeichert und nachgeschlagen werden. Es wird die Aufgabe der emittierenden Anstalten sein, die verschiedenen Transaktionstypen in online- und offline-durchführbare Transaktionen zu unterteilen, sowie monatliche oder tägliche Limiten zu setzen usw.

Folgende Sicherheitsfunktionen können je nach Applikation von der Chipkarte erwartet werden:

1. *Speicherung* von geheimzuhaltenden, partiell zugänglichen oder frei zugänglichen Daten.
2. *Identifikation* des rechtmässigen Kartenbenutzers.
3. *Authentifikation* (miteinander kommunizierende Einheiten müssen sich gegenseitig ihre Identitäten nachweisen).
4. *Digitale Unterschriften* (oder Datenauthentifikation, um sicherzustellen, dass eine empfangene Meldung tatsächlich vom angeblichen Sender herkommt, und dass sie auf der Übertragungsstrecke nicht modifiziert wurde).
5. *Daten Ver- und Entschlüsselung* (zu übertragende Daten sollen gegebenenfalls chiffriert werden, zwecks Geheimhaltung und Verhinderung von Einspeisung falscher Daten).
6. *Transaktionszertifikate* (die an einer Transaktion beteiligten Partner sollen nicht behaupten können, dass sie an einer Transaktion nicht teilgenommen hätten, oder dass die Transaktionsdaten nicht stimmen).
7. *Schlüsselverwaltung* (die meisten erwähnten Sicherheitsfunktionen benötigen kryptographische Schlüssel, deren Verteilung, Geheimhaltung und Erneuerung zuverlässig ablaufen müssen).
8. *Schutz gegen Nachahmung* (das Kopieren von echten Karten soll nicht möglich sein).
9. *Schutz gegen Manipulation* (gewisse Daten auf einer Karte sollen nicht veränderbar sein).
10. *Schutz gegen Simulation* (unter Simulation versteht man die Konstruktion eines Gerätes, das eine echte Karte nachahmt, obwohl es intern vielleicht ganz anders gebaut ist).
11. *Sperren* einer missbrauchten Karte (z.B. im Falle von nacheinanderfolgenden falschen PIN-Eingaben).

Diese Funktionen können mit Hilfe von physikalischen oder logischen Massnahmen gewährleistet werden.

Für den Schutz vor Lesen und Verändern der auf der Karte gespeicherten Daten stehen zwei Methoden zur Verfügung (die auch miteinander kombiniert werden können).

1. Unterteilung des Speicherbereiches in Teilbereiche mit unterschiedlichen Schutzniveaus:
   a. *Unzugänglicher Bereich* enthält Daten, die von ausserhalb der Karte nie gelesen werden können und nur für interne Berechnungen verwendet werden (z.B. kryptographische Schlüssel). Zugriff: Read only, nur vom Mikroprozessor.
   b. *Vertraulicher Bereich* für «empfindliche» Daten, z.B. Restsaldo, Beschränkungen des Kartengebrauches, Transaktionsprotokolle usw. Dieser Bereich ist erst dann zugänglich, wenn sich der Kartenbenutzer korrekt identifiziert hat (korrekte PIN-Eingabe). Zugriff: Read/Write nach erfolgter Benutzeridentifikation.
   c. *Allgemein zugänglicher Speicherbereich* enthält z.B. die Identifikation des emittierenden Unternehmens, die Kontonummer des Kartenbesitzers usw. Zugriff: Read only.
   d. *Ungeschützter Speicherbereich* als Notizbuch für den Kartenbenutzer verwendbar. Zugriff: Read/Write.
2. Chiffrierte Speicherung der zu schützenden Daten. Dabei wird der Chiffrierschlüssel mit der PIN und einem geheimen Kartenschlüssel gebildet.

Die Identifikation des rechtmässigen Kartenbenutzers kann auf zwei Weisen erfolgen.

1. *Kontrolle der Benutzerkenntnisse.* Der Benutzer muss eine PIN eingeben, die er aus Sicherheitsgründen nur in seinem Gedächtnis speichern darf (und nicht etwa auf der Karte selbst oder auf einem Begleitzettel).
2. *Erkennung von physiologischen Merkmalen des Benutzers.* Von den bis jetzt vorgeschlagenen Merkmalen (Unterschrift, Handgeometrie, Stimme, Fingerabdrücke usw.) hat sich keines als befriedigend erwiesen, sei es wegen des nötigen Speicherplatzes, wegen zu langen Vergleichszeiten, wegen schlechter Kundenakzeptanz oder wegen ungenügender Zuverlässigkeit. Bei der Verwendung von physiologischen Merkmalen ist es sehr schwierig, sowohl die Wahrscheinlichkeit von Misserfolgen bei rechtmässigen Operationen wie auch die Wahrscheinlichkeit von Erfolgen bei unrechtsmässigen Operationen klein zu halten.

Für die PIN-Überprüfung ist die Chipkarte selbst verantwortlich (und nicht das Endgerät oder der Hostrechner, wie bei konventionellen Magnetkartensystemen). Es ist möglich, den Speicher einer Chipkarte in mehrere Teilbereiche zu unterteilen und jedem Teilbereich eine eigene PIN und eine eigene Anwendung zuzuordnen (multifunktionale Karte). Allerdings dürfte die PIN-basierte Benutzeridentifikation in Zukunft ein beträchtliches Problem werden: jeder Benutzer wird vielleicht eine oder mehrere uni- oder multifunktionale Chipkarten besitzen, und für jede Anwendung wird er eine

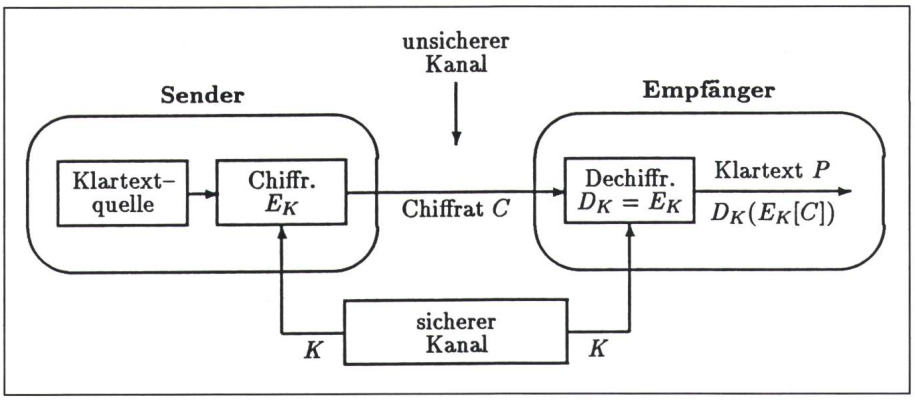


Bild 2 Symmetrisches Verschlüsselungssystem.
Der geheime Schlüssel K muss vor der Kommunikation durch einen sicheren Kanal dem Sender und dem Empfänger mitgeteilt werden.

PIN auswendig lernen müssen. Die Versuchung, die gleiche PIN für alle Anwendungen zu wählen, wird gross sein, was selbstverständlich auf Kosten der Sicherheit geht.

Jede Authentizitätsprüfung (von miteinander kommunizierenden Partnern oder von empfangenen Daten) erfolgt auf der Basis von einer im voraus vereinbarten Information (z.B. geheime oder öffentliche Schlüssel), und dynamischen (d.h. von Fall zu Fall variierenden) Daten:

- *Datum und Uhrzeit* können verwendet werden, aber die meisten Chipkarten besitzen keine Speisung und folglich keine interne Uhr.
- Sogenannte *Message Authentification Codes (MAC)* können in Abhängigkeit von der übertragenen Information gebildet werden, aber alleine verhindern sie ein Wiederspielen (Replay) nicht. Wenn der MAC nur von der gesendeten Meldung abhängt, können die Meldung und der zugehörige MAC aufgenommen werden und später wieder eingespielt werden (nicht akzeptabel, wenn es sich z.B. um einen Zahlungsauftrag handelt . . .).
- *Challenge/Reply-Protokolle* werden meistens bevorzugt. Der Prüfer stellt eine unvorhersagbare Frage (meistens in Form einer Zufalls- oder Pseudozufallszahl), und um diese Frage richtig beantworten zu können, muss der geprüfte Partner ein geheimes Stück Information besitzen. Die Public-Key-Verfahren sind für solche Protokolle besonders gut geeignet.

Um die Authentizität ihres Gesprächspartners nachprüfen zu können, muss eine Chipkarte über einen kryptographischen Algorithmus und eine unvorhersagbare, von aussen nicht beeinflussbare Pseudozufallszahlenquelle verfügen. Im nächsten Kapital werden die verschiedenen kryptographischen Werkzeuge näher betrachtet.

Probleme bei der Implementierung von kryptographischen Algorithmen in Chipkarten

Grundlagen der Kryptographie

In [16] ist folgende Definition angegeben:

«Die Wissenschaft oder auch Kunst der Kryptographie hat zum Hauptziel, die Geheimhaltung, Authentizität und Integrität von Nachrichten sicherzustellen.»

Zur Geheimhaltung von Daten, die durch unsichere Kanäle übertragen werden sollen, gibt es verschiedene Chiffrierverfahren. Der Chiffriervorgang entspricht einer schlüsselabhängigen invertierbaren Abbildung E vom Klartext P auf den Chiffrattext $C = E(P)$. Zur Dechiffrierung wird die inverse, ebenfalls schlüsselabhängige Transformation $D(C) = E^{-1}(C) = E^{-1}[E(P)] = P$ vom rechtmässigen Empfänger durchgeführt.

Ein Kryptosystem hat dann eine optimale Sicherheit, wenn keine krypto analytische Attacke effizienter ist als ein systematisches Ausprobieren aller möglichen Schlüssel (Exhaustive search). Diese optimale Sicherheit ist leider praktisch nie nachweisbar für konkrete, brauchbare Kryptosysteme. Es ist nämlich meistens sehr schwierig, eine untere Schranke für die Lösung eines gegebenen Problems anzugeben. Der Entwurf von Kryptosystemen verläuft daher oft mit «Feedback»: jede neue Attacke gegen ein Chiffrierverfahren deutet auf dessen Schwächen hin und liefert gegebenenfalls neue Entwurfskriterien.

Die heute gebräuchlichen digitalen Chiffrierverfahren können in zwei Kategorien unterteilt werden: symmetrische und asymmetrische Verfahren.

Bei *symmetrischen Verfahren* (auch klassische oder One-Key-Verfahren genannt) müssen der Sender und der Empfänger vor der chiffrierten Kommunikation über einen gemeinsamen, geheimen Schlüssel K einig werden (Bild 2). Dieser Schlüssel dient sowohl zur Chiffrierung wie auch zur Dechiffrierung.

Bei *asymmetrischen Verfahren* (Bild 3) wird die Chiffrierung mit einem *öffentlichen Schlüssel* e_i, die Dechiffrierung mit einem geheimen Schlüssel d_i ausgeführt. Asymmetrische Verfahren beruhen auf sogenannten *Falltür-Einwegfunktionen* (trapdoor one-way functions). Solche Funktionen können einfach berechnet werden, aber ihre Inversen sind ohne Kenntnis der Falltüre extrem schwierig und in vernünftiger Zeit nicht zu bewältigen. In einem asymmetrischen Kryptosystem ist einerseits das Chiffrat eine Falltür-Einwegfunktion des Klartextes (der

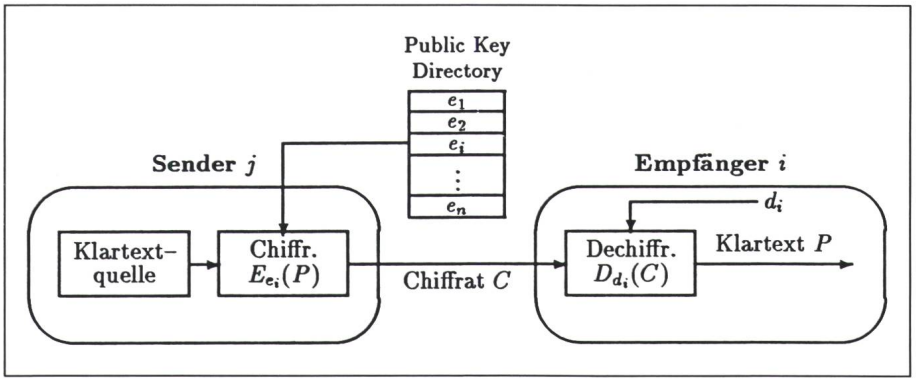


Bild 3 Asymmetrisches (Public-Key) Verschlüsselungssystem.
Der Sender j findet den öffentlichen Schlüssel e_i des i-ten Teilnehmers in einem beglaubigten Public-Key-Directory und chiffriert den Klartext P mit e_i. Nur der beabsichtigte Empfänger kennt den entsprechenden Dechiffrierschlüssel d_i und ist somit in der Lage, aus dem Chiffrattext C den Klartext P rückzugewinnen.

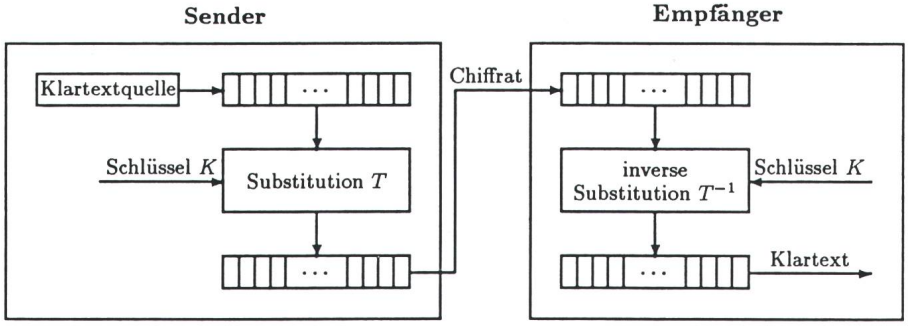


Bild 4 Funktionsweise eines Block Cipher-Systems
(Blockchiffrierung).

geheime Schlüssel d_i stellt die Falltüre dar), und andererseits muss der geheime Schlüssel d_i auch eine Einwegfunktion des öffentlichen Schlüssels l_i sein (mit oder ohne Falltüre).
Die heute verwendeten symmetrischen Chiffrierverfahren gehören zu einer von zwei Familien: die *Block-Chiffrierverfahren* und die *Bitstromchiffrierverfahren* (Block- und Stream-Ciphers).

In einem Block Cipher-System (Bild 4) wird der Klartext in Blöcke von fester Länge unterteilt. Jeder Block wird durch eine schlüsselabhängige Substitution T auf einem Chiffratblock abgebildet. Dabei muss die Blocklänge genügend gross sein, sonst könnte die Substitution T von einem Kryptoanalytiker tabelliert werden. Sehr oft werden Block Cipher-Systeme in einem Modus betrieben, wo das vorherige Chiffrat auf die Chiffrierung des nächsten Klartextblocks miteinwirkt (CFB, cipher feedback mode). Weitere Betriebsmodi wurden in [6] vorgeschlagen.

In einem (additiven) Stream-Cipher-System wird ein in binärer Darstellung vorliegender Klartext mit einer (ebenfalls binären) Schlüsselfolge $\tilde{Z}$ bitweise Exklusiv-Oder (EXOR)-addiert (Bild 5). Ein solches System ist nur dann sicher, wenn die Schlüsselfolge $\tilde{Z}$ unvorhersehbar ist, wenn sie also von einer echt zufälligen Bitfolge nicht unterschieden werden kann. Die deterministische Gesetzmässigkeit, die diese Schlüsselstromfolge bestimmt, muss auch nach Beobachtung eines sehr langen Abschnittes von $\tilde{Z}$ nicht entdeckt werden können. Nebst den statistischen Eigenschaften der Pseudozufallssequenz $\tilde{Z}$, die denjenigen echter Zufallssequenzen möglichst ähnlich sein sollten, ist ihre *lineare Komplexität* ebenfalls von zentraler Bedeutung für die Sicherheit des Stream Ciphers. Jede periodische Sequenz (Periode p) kann bekanntlich von einem linear rückgekoppelten Schieberegister (Linear Feddback Shift-Register, LFSR) der Länge $L \leq p$ erzeugt werden. Die Länge des kürzesten LFSR, das eine gegebene Sequenz $\tilde{Z}$ erzeugen kann, nennt man ihre lineare Komplexität. Falls die Schlüsselfolge $\tilde{Z}$ eine lineare Komplexität L aufweist, genügt die Beobachtung von $2L$ Bit von $\tilde{Z}$, um das *lineare Aequivalent d.h. das kürzeste LFSR, das die betrachtete Schlüsselstromsequenz geniessen kann)* des entsprechenden Schlüsselstromgenerators zu bestimmen [17]. Deshalb muss die Schlüsselstromsequenz $\tilde{Z}$ durch eine sehr hohe lineare Komplexität charakterisiert sein. Diese Eigenschaft ist notwendig, aber nicht hinreichend, für die Sicherheit des Stream Cipher-Systems.

Viele in der Praxis auftretenden Schlüsselstromgeneratoren beinhalten einen oder mehrere LFSR, je nach dem ob sie gemäss Bild 6 oder gemäss Bild 7 aufgebaut sind. Die Struktur nach Bild 6 verlangt, dass ein Zugriff zu den einzelnen Zellen des LFSR möglich sein muss. Hingegen werden in Bild 7 nur die jeweiligen Ausgänge der LFSR benötigt. Linear rückgekoppelte Schieberegister haben den Vorteil, dass sie - unabhängig vom Anfangszustand, sofern er verschieden von Null ist - Sequenzen mit guten statistischen Eigenschaften erzeugen können, falls sie ein primitives Rückkopplungspolynom besitzen.

Verfahrenspezifische Implementierungsprobleme

Bei der Realisierung eines kryptographischen Algorithmus in einer Chipkarte stellen sich je nach Typ (Stream-, Block- oder Public-Key-Ciphers) spezifische Probleme, die in diesem Abschnitt betrachtet werden sollen. Die folgende Bemerkung gilt aber für *alle* Arten von Verschlüsselungsalgorithmen: Die Chipkarten sind mit einem einzigen Mikroprozessor ausgerüstet, der sowohl für die Dateneinen- und -ausgabe wie für die Verschlüsselung selber verantwortlich ist. Wenn die Chipkarte als Chiffriergerät gebraucht werden soll, müssen bei der Berechnung der Verschlüsselungsrate die Verzögerungen bei der Ein- und Ausgabe berücksichtigt werden.

Probleme bei der Realisierung von Stream Cipher-Systemen

Bei Stream Cipher-Systemen ist das grösste Problem die Realisierung des Schlüsselstromgenerators. Um Generatoren gemäss Bild 6 oder 7 effizient zu realisieren, sei es in Soft- oder Hardware, müssen der oder die LFSR und die Funktion f effizient realisiert werden.

Linear rückgekoppelte Schieberegister sind für gewisse Längen als käufliche Bausteine erhältlich, aber der Zugriff zu einzelnen Zellen ist nur bei kleinen Längen möglich. Für die softwaremässige Implementierung von LFSR wurden verschiedene Speicherorganisierungsmethoden vorgeschlagen [26]. Die einfachste Anordnung (lineare Anordnung), wo die Registerinhalte in aufeinanderfolgenden Speicherworten abgelegt werden, ist leider für grössere Schieberegisterlängen sehr ineffizient, da bei jedem Takt die Gesamtheit der Worte um eine Stelle zyklisch geschoben werden muss. Eine elegante Lösung für die Erzeugung von maximal langen Sequenzen bietet die Parallelstruktur an [14; 26]: geeignete Phasen werden parallel erzeugt und eine Parallel-Serie-Wandlung liefert die gewünschte Sequenz. Diese Methode wurde ursprünglich für Hardware-Realisierungen von LFSR entwickelt und später für Software-Realisierungen angepasst.

Bezüglich der Realisierung der Funktion f können hier keine allgemeinen Regeln angegeben werden.

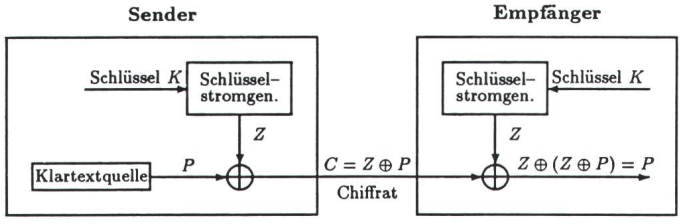


Bild 5
Funktionsweise eines Stream Cipher-Systems
(Bitstromchiffrierung)

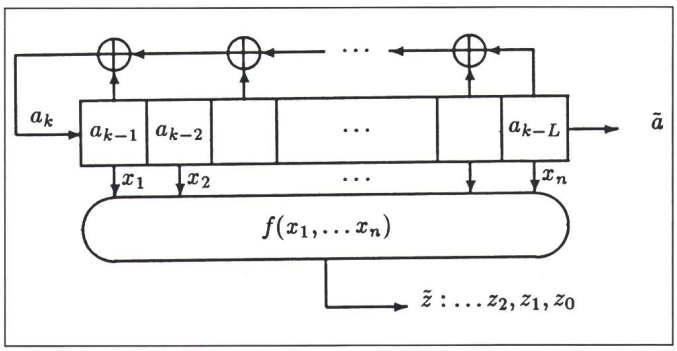


Bild 6
Schlüsselstromgenerator mit einem einzigen LFSR, dessen Zellen durch die nichtlineare Funktion f verknüpft werden, um die Schlüsselstrom sequenz $\tilde{Z}$ zu erzeugen.

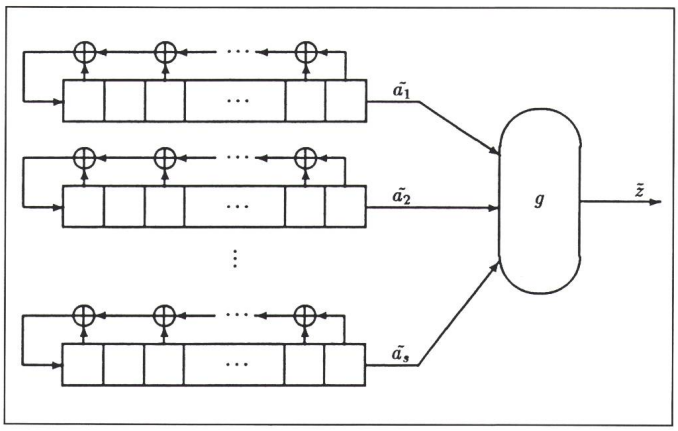


Bild 7
Schlüsselstromgenerator mit mehreren LFSR, deren Ausgangssequenzen durch die Funktion g verknüpft werden, um die Schlüsselstromsequenz $\tilde{Z}$ zu erzeugen.

Für jede konkrete Funktion f muss die Implementierung untersucht und optimiert werden.

Der Vollständigkeit halber soll noch erwähnt werden, dass die zwei Generatortypen aus Bild 6 und 7 keineswegs die einzigen verwendeten Typen sind. Sie sind aber ziemlich ausführlich untersucht worden. Es werden z.B. auch Schlüsselstromgeneratoren mit nichtlinear rückgekoppelten Schieberegistern eingesetzt (vgl. Sicrypt-Stream Cipher, der von Siemens verwendet wird). Eine spezielle Gruppe von Stream Cipher-Systemen wird manchmal als *selbstsynchrone* Stream Ciphers [4] bezeichnet: der Schlüsselstrom wird in Abhängigkeit vom vorherigen Chiffrattext erzeugt (analog zum Cipher Feedback Mode von Block Cipher-Systemen). Jeder Bitübertragungsfehler kann leider die korrekte Dechiffrierung beim Empfänger verhindern, was bei der einfachen Struktur von Bild 5 nicht der Fall ist, da ein falsch detektiertes Chiffratbit nur einen 1-Bit-Fehler im dechiffrierten Klartext verursacht. Vor- und Nachteile der beiden Modi werden in [20] unter die Lupe genommen.

Probleme bei der Realisierung von Block Cipher-Systemen

Der am weitesten verbreitete Chiffrieralgorithmus ist sicher der im Jahre 1977 entstandene *Data Encryption Standard* (DES [5]). Es handelt sich um ein Blockchiffrierverfahren mit einer Klartext- und Chiffratblocklänge von 64 Bit und einem Schlüssel von 56 Bit. Trotz vieler Bemühungen wurde bis jetzt keine wesentliche strukturelle Schwäche an diesem Algorithmus entdeckt, ausser seine oft als zu kurz betrachtete Schlüssellänge.

Der DES ist ein *Produkt Cipher:* er besteht aus einem in sich einfachen Grundbaustein, der vom Klartext mehrmals (16mal) durchlaufen wird.

Bei einer Hardware-Realisierung stellt sich zunächst die Frage nach der Anzahl Grundbausteinrealisierungen. Falls man diesen Baustein nur einmal realisiert, wird das System alle 16 Rechenzyklen einem Chiffratblock abliefern[2]. Hingegen ist bei einer 16maligen Implementierung des Grundbausteins ein Pipeline-Betrieb möglich, und die Verschlüsselungsrate beträgt nach Auffüllung der Pipeline 1 Chiffratblock pro Rechenzyklus. Im DES besteht der Grundbaustein unter anderem aus 8 Substitutionsboxen (S-Boxen), die tabellarisch angegeben sind und sechs Bit auf vier abbilden. Eine 16fache Realisierung ist daher zu umständlich und die Chip-Designer erklären sich mit Verschlüsselungsraten von etwa 32 MBit/s zufrieden [30]. Der DES eignet sich wegen seiner tabellarisch angegebenen S-Boxen besonders gut für Hardware-Realisierungen, in denen die S-Boxen in einem ROM fest programmiert werden.

Bei Software-Realisierungen des DES auf Chipkarten sind viel bescheidenere Verschlüsselungsraten erreichbar, in der Grössenordnung[3] von 160 bit/s. Der DES wurde übrigens hauptsächlich für Hardware-Realisierungen entworfen, zu Zeiten, als die Chipkarten noch nicht aktuell waren. Im Hinblick auf den neuen Bedarf an softwaremässig effizient implementierbaren kryptographischen Algorithmen, wurde der japanische FEAL (Fast Data Encipherment Algorithm [19; 29] entwickelt. Seine S-Boxen sind durch einen sehr einfachen arithmetischen Ausdruck gegeben, nämlich eine Addition modulo 256 und ein zyklisches Rotieren um zwei Bit ($\mathrm{Rot}_2[(X + Y + \delta) \bmod 256]$). Das führt dazu, dass der FEAL ebenso in Hardware wie auch in Software sehr effizient realisierbar ist. Auf dem Markt ist ein FEAL-Chip erhältlich[4], der durch eine Verschlüsselungsrate von 96 MBit/s charakterisiert ist. Auf Chipkarten erreichen Assembler-FEAL-Programme Verschlüsselungsraten zwischen 16 und 173 kbit/s (je nach verwendetem Mikroprozessor [18]) bei einem bescheidenen Speicherplatzbedarf von etwa 450 Byte. In seiner ersten 6-Runden-Version wurde der FEAL-Algorithmus gebrochen [2], und die Frage, ob der um zwei Runden erweiterte FEAL-8 sicher ist, kann noch nicht beantwortet werden. Der DES ist zwar seit 1977 ein bewährter Algorithmus, leider wurden aber die bei seiner Entwicklung massgebenden Designkriterien nie öffentlich bekanntgemacht (mit Ausnahme von gewissen Eigenschaften der S-Boxen, die in [3] formuliert sind). Deshalb ist es unmöglich, den FEAL (oder einen anderen Block Cipher) im Hinblick auf diese Kriterien zu testen. Um sich von der Sicherheit eines neuen Block Ciphers zu überzeugen, stehen vor allem die von *Shannon* [28] empfohlenen Eigenschaften von *Diffusion* und *Confusion* zur Verfügung:

Diffusion: jeder Klartextbit soll viele Chiffratbits beeinflussen, damit die Statistik des Klartextes im Chiffrattext nicht mehr erkennbar ist.

[2] 1 Rechenzyklus = 1 Durchlauf des Grundbausteins

[3] Zahl für eine Chipkarte von GEC Card Technology, England

[4] Referenz NLC5001F

Confusion: es muss möglichst kompliziert und aufwendig sein, die Abhängigkeit zwischen Statistik des Klartextes und Statistik des Chiffrattextes zu analysieren und zu beschreiben.

Es ist auch bekannt, dass ein guter Block Cipher keine linearen Strukturen besitzen sollte [21; 9]. Aber wie man sich vor unbekannten, neuartigen kryptoanalytischen Attacken schützen soll, bleibt eine offene Frage. Der einzige Verschlüsselungsalgorithmus, dessen Sicherheit als absolut bezeichnet werden kann, ist der sogenannte one-time pad [15], der eine echt zufällige binäre Sequenz zum Klartext EXOR-addiert. Leider ist dieses Verfahren für die meisten Anwendungen nicht brauchbar, da vor der chiffrierten Kommunikation ein zu langer Schlüssel auf sichere Art und Weise übertragen werden müsste. Um 1 Bit Klartext zu chiffrieren, braucht man nämlich 1 Bit Schlüssel*. Der Aufwand zur sicheren Übertragung von solchen Mengen Schlüsselbit ist nur in seltenen, hochsicheren Anwendungen gerechtfertigt. Dann können z.B. grosse Mengen von Schlüsselbit auf Magnetbändern gespeichert werden, die zum beabsichtigten kommunizierenden Partner persönlich abgegeben werden müssen. Im Gegensatz zu diesem absolut sicheren Chiffrierverfahren bestehen bei allen gebräuchlichen Algorithmen statistische Abhängigkeiten zwischen dem Klartext und dem Chiffrat, die eventuell in einer kryptoanalytischen Attacke zum Ertrag gebracht werden können.

Probleme bei der Realisierung von Public-Key-Systemen

Eigentlich könnten die Public-Key-Systeme auch als Blockverfahren bezeichnet werden, da sie den Klartext blockweise verarbeiten. Ihr grundsätzlicher Unterschied zu den im letzten Abschnitt besprochenen Block Ciphers besteht in ihrem asymmetrischen Charakter: die Verschlüsselungsoperation $E(\cdot)$ ist öffentlich, kann von jedem Teilnehmer durchgeführt werden, aber der resultierende Chiffrattext kann ausschliesslich mit einer geheimen, nur vom berechtigten Empfänger bekannten Entschlüsselungsoperation $D(\cdot)$ dechiffriert werden. Selbstverständlich weisen alle Public-Key-Verfahren folgende Eigenschaft auf:

$$D[E(x)] = x. \qquad (1)$$

Viele Public-Key-Verfahren sind *kommutativ*, d.h. sie weisen zusätzlich die Eigenschaft

$$E[D(y)] = y \qquad (2)$$

auf, was sehr nützlich ist für Authentifikationsprotokolle [4]. Ein solches Protokoll sei hier anhand von Bild 8 kurz erläutert. Der Teilnehmer B will seinen Kommunikationspartner authentifizieren. Er sendet ihm eine Zufallszahl M. Der Teilnehmer A «dechiffriert» sie mit seiner geheimen Entschlüsselungsoperation D_A, und sendet $D_A(M)$ dem Teilnehmer B. Mit Hilfe der öffentlichen Verschlüsselungsoperation E_A «verschlüsselt» der Teilnehmer B die empfangene Meldung und vergleicht das Resultat mit dem Sollwert M. Falls die beiden Werte übereinstimmen, gilt der Teilnehmer A als authentifiziert, da niemand ausser ihm $D_A(M)$ berechnen konnte, und die gleiche Prozedur wird in entgegengesetzter Richtung zur Authentifikation von B ausgeführt.

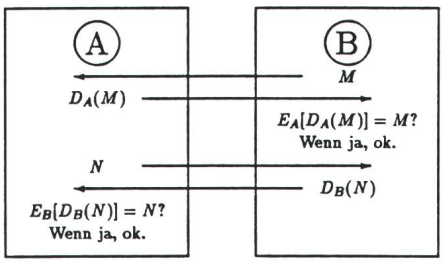


Bild 8 Ein auf Public-Key-Verfahren beruhendes Challenge/Reply-Authentifikationsprotokoll.

Das bekannteste Public-Key-Verfahren, das sowohl für Ver- und Entschlüsselung wie auch für Authentifikation verwendbar ist, ist das nach den Namen seiner Erfinder (Rivest, Shamir and Adleman [23]) genannte RSA. Wir wollen hier die Einzelheiten dieses Verfahrens nicht anschauen, sondern nur die Aspekte betrachten, die für die Realisierung problematisch sein können. Die Chiffrierung und die Dechiffrierung bestehen beim RSA-Verfahren in einer Exponentiation modulo einer sehr grossen Zahl (gross heisst hier 100–200 Dezimalstellen). Die Exponentiation von grossen Zahlen zu grossen Exponenten modulo grosser Zahlen ist sowohl software- wie auch hardwaremässig nicht einfach zu realisieren.

Ein Multichip RSA-Modul (mit 6 Chips) wurde realisiert, das bei einer Exponent- und Moduluslänge von 512 Bit eine Verschlüsselungsrate von 17 kBit/s erreicht [12]. Eine andere Multichip-Realisierung [22] mit 333 Chips brachte die Verschlüsselungsrate zu 29 kBit/s. Für Chipkarten kommen jedoch nur Ein-Chip-Realisierungen in Betracht. In [27] wird eine Ein-Chip-Realisierung beschrieben, die mit 3 MBit/s ver- und mit 0,2 MBit/s entschlüsseln kann. Die Verschlüsselungsrate eines RSA-Hardware-Modules hängt wie gesagt von der Implementierung der Exponentiation ab, deren Leistungsfähigkeit vom Aufwand für eine Addition, eine Multiplikation und eine Modulo-Operation abhängt. Zwecks Effizienz muss der Aufwand für diese Operationen sowie die Anzahl nötiger modularer Multiplikationen für eine Exponentiation, minimal gehalten werden.

Hardware-RSA-Realisierungen sind also im Vergleich zu Stream- und Block Ciphers sehr langsam. Wie erwartet, schneiden Software-Lösungen gar nicht besser ab: die Exponentiation zu einem 500-Bit-Exponenten modulo einer 500-Bit-Zahl kann in einem 8-Bit-Mikroprozessor kaum effizient realisiert werden. Sie erfordert einerseits einen ziemlich grossen Programmierungsaufwand und liefert anderseits sehr kleine Verschlüsselungsraten. Softwaremässige RSA-Implementierungen werden deshalb praktisch nur für Authentifizierungsprotokolle und digitale Unterschriften verwendet. Bei einer direkten Programmierung in einem Chipkarten-Mikroprozessor (Typ HD65901) wurde eine Rechenzeit von 1380 s für die Exponentiation einer 512-Bit-Zahl erreicht [13]. Da diese Zahl für die meisten Applikationen zu gross ist, wurde die Möglichkeit untersucht, Teilberechnungen vom Hostrechner durchführen zu lassen. Das in [13] beschriebene Verfahren SETPUR (Sichere Exponentiation trotz potentiell unsicherer Rechenhilfe) lieferte eine Exponentiation in etwa 50 s.

Es gibt weitere Public-Key-Verfahren, z.B. das Schlüsselaustauschverfahren von Diffie und Hellman [7] und das Verfahren von ElGamal [8], die beide auf der Exponentiation in einem endlichen Körper $GF(q)$ beruhen. Aus praktischen Gründen wählt man meistens $q = 2^n$, mit einem Exponenten n, der mit Rücksicht auf Sicherheitsanforderungen deutlich grösser als 1000 gewählt werden muss [1]. Für die Realisierung dieser Exponentiation wurden vor allem kombinatorische Netzwerke untersucht [31; 24].

Zur interaktiven Identifikation und zur Erzeugung von digitalen Unterschriften haben Fiat und Shamir [10] einen vielversprechenden Algorithmus vorgeschlagen. Er basiert auf der

Schwierigkeit des Ziehens der Quadratwurzel einer Zahl modulo einer grossen Zahl *n*, deren Faktorisierung unbekannt ist. Das Sicherheitsniveau dieses Schemas ist durch die Grösse gewisser Parameter steuerbar. Für ein Sicherheitsniveau von 2^{-20} müssen z.B. die kommunizierenden Partner während der Beweisführung 323 Byte austauschen, und jede Chipkarte muss 320 Byte ROM für die Speicherung von geheimen Werten reservieren. Die durchzuführenden Berechnungen beschränken sich auf modulare Multiplikationen (keine Exponentiation, im Gegensatz zu den meisten anderen Public-Key-Verfahren). Zur Chiffrierung kann dieser Algorithmus aber nicht verwendet werden.

Zusammenfassung und Schlussfolgerungen

Die wesentlichen Vorteile der Chipkarte gegenüber der Magnetstreifenkarte sind

- Ihre eingebaute *Rechenkapazität*, die es möglich macht, die Karte als *aktives* kryptographisches Werkzeug in Identifikations-, Authentifikations- und Verschlüsselungsaufgaben einzusetzen.
- Ihre grössere Speicherkapazität und die Möglichkeit, verschiedene Speicherbereiche mit unterschiedlichen Sicherheitsniveaus zu versehen. Geheime Schlüssel können zum Beispiel auf sichere Weise in der Karte gespeichert werden, nämlich so, dass sie nur in vorgegebenen Situationen vom Mikroprozessor benutzt werden, aber niemals überschrieben oder von aussen gelesen werden können. Transaktionsdaten können ebenfalls gespeichert und unter gewissen Bedingungen reaktualisiert werden.
- Ihre einfache, rein elektrische Anschlussweise: Chipkarten können von einfachen, billigen Endgeräten betrieben werden, was ihre höheren Herstellungskosten kompensiert und einen grossen Verbreitungsgrad gestattet.

Bei der softwaremässigen Implementierung von Chiffrieralgorithmen in Chipkarten stellen sich aber Speicherplatz- und Rechenleistungsprobleme. Aus Kosten- und Strapazierfähigkeitsgründen können nämlich (zurzeit) nur 8-Bit-Mikroprozessoren zusammen mit (z.B.) 6 kByte ROM, 128 kByte RAM und 8 kByte EPROM[5] in einer Kreditkartenformat-Plastikkarte eingebaut werden.

Bei der Realisierung von Block-Cipher-Systemen sind die Struktur der S-Boxen (in Tabellenform oder analytisch vorgegeben) sowie die Anzahl Runden für die Implementierbarkeit und die erzielbaren Leistungen entscheidend. In einem einfachen Mikroprozessor ist nämlich kein Pipelining vorhanden und jede Runde muss sequentiell abgearbeitet werden.

Die aktuellen Public-Key-Verfahren basieren auf aufwendigen arithmetischen Operationen mit sehr grossen Zahlen und können in Chipkarten höchstens für Authentifikationszwekke oder digitale Signaturen verwendet werden. Für Verschlüsselung leisten sie zu niedrige Raten. Es gibt aber spezielle Methoden, die Teilberechnungen von einem angeschlossenen Hostrechner durchführen lassen, ohne dabei brauchbare Information über geheime Parameter freizusetzen. Die damit erreichten Chiffrierraten sind erheblich grösser.

[5] Daten der Bull CP8 SPOM 11 Chipkarte

Literatur

[1] *T. Beth* und *D. Gollmann:* Kryptologie und Datensicherheit. Teil II: Aspekte der technischen Realisierung von Public-Key-Verfahren. E und I 105(1988)1, S. 12...18.

[2] *B. den Boer:* Cryptanalysis of F.E.A.L. In: Advances in Cryptology: Eurocrypt '88. – Lecture notes in computer science, vol. 330 – Berlin a.o., Springer-Verlag, 1988, p. 293...299.

[3] *E. F. Brickell, J. H. Moore* and *M. R. Purtill:* Structure in the S-boxes of the DES. In: Advances in Cryptology: Crypto '86. – Lecture notes in computer science, vol. 263 – Berlin a.o., Springer-Verlag, 1987; p. 3...8.

[4] *D. E. Denning:* Cryptography and data security. Reading/Massachusetts, Addison-Wesley, 1982.

[5] Data encryption standard. Federal Information Processing Standards Publication 46. Washington D. C., National Bureau of Standards, January 1977.

[6] Des modes of operation. Federal Information Processing Standards Publication 81. Washington D. C., National Bureau of Standards, December 1980.

[7] *W. Diffie* and *M. E. Hellman:* New directions in cryptography. IEEE Trans. on Information Theory IT-22(1976)6, p. 644...654.

[8] *T. Elgamal:* A puplic key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory IT-31(1985)4, p. 469...472.

[9] *J.-H. Evertse:* Linear structures in blockciphers. In: Advances in Cryptology: Eurocrypt '87. – Lecture notes in computer science, vol. 304 – Berlin a.o., Springer-Verlag, 1988, p. 249...266.

[10] *A. Fiat* and *A. Shamir:* How to prove yourself: practical solutions to identification and signature problems. In: Advances in Cryptology: Crypto '86. – Lecture notes in computer science, vol. 263 – Berlin a.o., Springer-Verlag, 1987; p. 186...194.

[11] *A. S. Glass* und *J. L. Massey:* Plastikkarten – wie intelligent ist sicher? Landis & Gyr Mitteilungen 32(1985)2, S. 22...39.

[12] *F. Hoornaert* a.o.: Fast RSA-hardware: dream or reality? In: Advances in Cryptology: Eurocrypt '88. – Lecture notes in computer science, vol. 330 – Berlin a.o., Springer-Verlag, 1988, p. 257...264.

[13] *G. Lassmann:* Zur Realisierung von asymmetrischen kryptographischen Verfahren durch Mikrocomputer-Chipkarten. Bericht N. I 921 536 580/89 der Forschungsgruppe FI 17. Technischer Bericht des Forschungsinstituts des Fernmeldetechnischen Zentralamtes (FTZ), April, 1989.

[14] *A. Lempel* and *W. L. Eastman:* High speed generation of maximal length sequences. IEEE Trans. on Computers C-20(1971)2, p. 227...229.

[15] *J. L. Massey:* An introduction to contemporary cryptology. Proc. IEEE 76(1988)5, p. 533...549.

[16] *J. L. Massey:* Standardisierung kryptographischer Dienste. Bull. SEV/VSE 77 (1986)7, S. 367...371.

[17] *J. L. Massey:* Shift-register synthesis and BCH decoding. IEEE Trans. on Information Theory IT-15(1969)1/I, p. 122...127.

[18] *S. Miyaguchi:* FEAL-8 program for IC cards. Kanagawa-ken/Japan, NTT Communications and Information Processing Laboratories, January 1989.

[19] *S. Miyaguchi, A. Shiraishi* and *A. Shimizu:* Fast data encipherment algorithm FEAL-8. Review of the Electrical Communications Laboratories 36(1988)4, p. 433...437.

[20] *F. Piper:* Stream ciphers. E und M 104(1987)12, p. 564...568.

[21] *J. A. Reeds* and *J. L. Manferdelli:* DES has no per round linear factors. In: Advances in Cryptology: Crypto '84. – Lecture notes in computer science, vol. 196 – Berlin u.a., Springer-Verlag, 1985, p. 377...389.

[22] *R. L.-Rivest:* RSA chips (past/present/future). In: Advances in Cryptology: Eurocrypt '84. – Lecture notes in computer science, vol. 209 – Berlin a.o., Springer-Verlag, 1985, p. 159...165.

[23] *R. L. Rivest, A. Shamir* and *L. Adleman:* A method for obtaining digital signatures and public -key cryptosystems. Communications of the ACM 21 (1978)2, p. 120...126.

[24] *B. A. Saws* and *C. K. Rushforth:* A cellular-array multiplier for GF (2m). IEEE Trans. on Computers C-20(1971)3, p. 1573...1578.

[25] *I. Schaumüller-Bichl:* Chipkarten und ihre Bedeutung in kryptographischen Systemen. E und M 104(1987)12, S. 543...546.

[26] *P. Schoebi:* Untersuchungen zur Sicherheit und Realisierbarkeit von analogen und digitalen kryptologischen Systemen. Dissertation der ETH Zürich, Nr. 7433, 1983.

[27] *H. Sedlak:* The RSA cryptography processor. In: Advances in Cryptology: Eurocrypt '87. – Lecture notes in computer science, vol. 293 – Berlin a.o., Springer-Verlag, 1988, p. 95...105.

[28] *C. E. Shannon:* Communication theory of secrecy systems. Bell. Syst. Techn. J. 28(1949)4, p. 656...715.

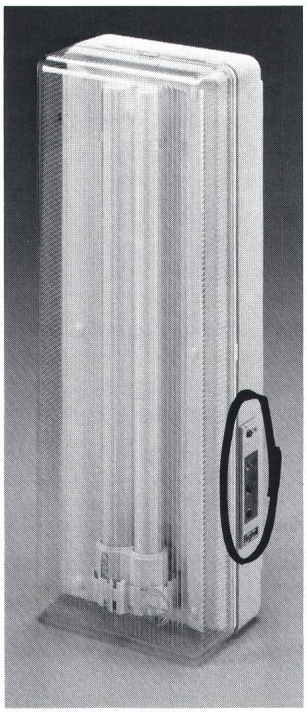
[29] *A. Shimizu* and *S. Miyaguchi:* Fast data encipherment algorithm FEAL. In: Advances in Cryptology: Eurocrypt '87. – Lecture notes in computer science, vol. 293 – Berlin a.o., Springer-Verlag, 1988, p. 267...278.

[30] *I. Verbauwede* a.o.: Security considerations in the design and implementation of a new DES chip. In: Advances in Cryptology: Eurocrypt '87. – Lecture notes in computer science, vol. 293 – Berlin, Springer-Verlag, 1988, p. 287...300.

[31] *C. C. Wang* a.o.: VLSI architectures for computing multiplications and inverses in GF (2m). IEEE, Trans. on Computers C-34(1985)8, p. 709...717.

NEUHEIT !
NOTLEUCHTEN, DIE SICH SELBER TESTEN !

Pratica Autotest



Die neue Generation im Gebiete der Notleuchten!

PRATICA Autotest führt auf selbstständige Weise periodische Tests durch.
Allfällige Störungen werden sofort durch ein LED-Signal angezeigt.

LED Zeichenerklärung:

LED **grün** Spannungsanzeige
muss immer eingeschaltet sein.

LED **gelb** zeigt den Zustand der Fluo-Röhre an.
Leuchtet auf, wenn die Röhre ausgewechselt werden muss.

LED **rot** zeigt den Zustand der Batterie an.
Leuchtet auf wenn die Ladung der Batterie ungenügend ist.

LED **rot** zeigt Störungen der Elektronik an.

Kontrolle des Betriebes:

Jede Woche führt das Gerät während 1 Minute folgende Kontrollen aus:

- Umschaltung auf Notbetrieb
- Korrekter Betrieb der Elektronik (inverter)
- Lichtstärke der Fluo-Röhre.

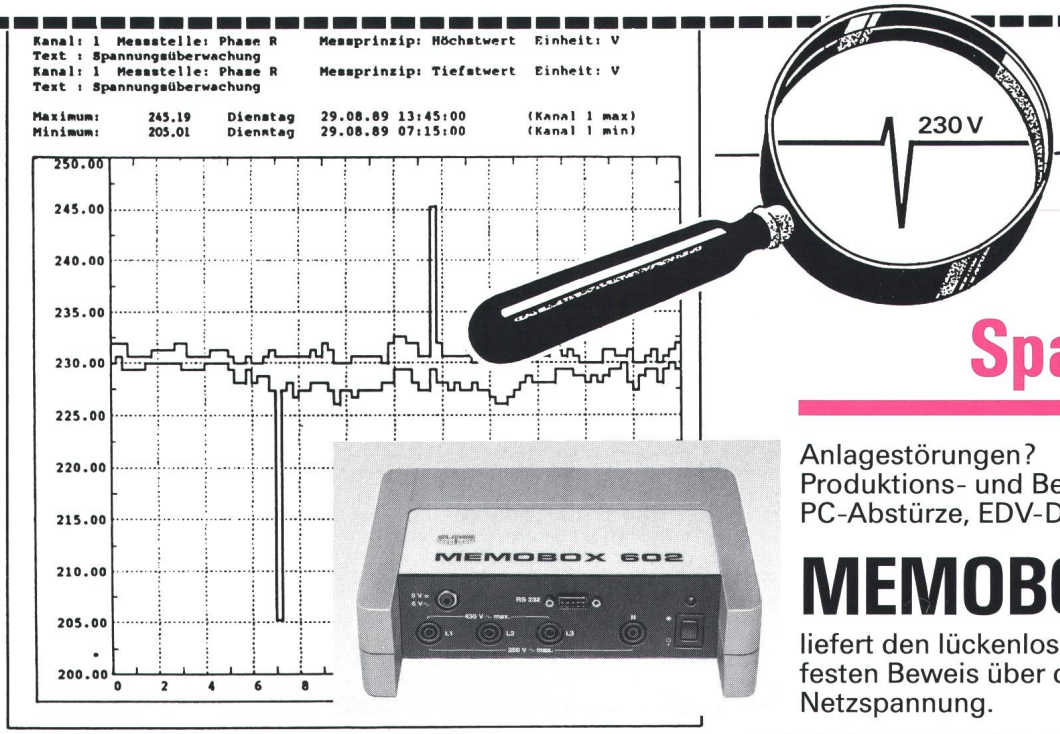
Allfällige Störungen werden sofort durch ein LED-Signal angezeigt.

Autonomie-Kontrolle:

Alle 4 Monate kontrolliert das Gerät die Ladung der Akkus. Allfällige Störungen werden sofort durch ein LED-Signal angezeigt.

Nicola Pagliaccio
Eclairage de secours
Service après vente

Chemin des Croix-Rouges 10, 1007 Lausanne
Tél. (021) 20 22 13/14 Fax (021) 20 96 64



Spannung!

Anlagestörungen?
Produktions- und Betriebsunterbrüche?
PC-Abstürze, EDV-Datenverluste?

MEMOBOX 602

liefert den lückenlosen, hieb- und stichfesten Beweis über die Qualität Ihrer Netzspannung.

ELMES STAUB + CO AG
Systeme für die Messtechnik
Bergstrasse 43
CH-8805 **Richterswil**
Telefon 01-784 22 22
Fax 01-784 64 07

Spannungs-BON für ausführliche Unterlagen.
Die ersten 100 Einsender erhalten zusätzlich ein nützliches Präsent.

Firma _____

Adresse _____

PLZ/Ort _____

zuständig SEV