in: Günter Müller, Andreas Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longman 1997, 83-104

Bausteine zur Realisierung mehrseitiger Sicherheit

Hannes Federrath, Andreas Pfitzmann

TU Dresden, Institut für Theoretische Informatik, 01062 Dresden,
Telefon (0351) 463-8470, -8277, Fax -8255, Email {federrath, pfitza}@inf.tu-dresden.de

Zusammenfassung

Das Papier stellt die wesentlichen Bausteine zur Realisierung von Sicherheitsmerkmalen in IT-Systemen vor. Deren geeigneter Einsatz ermöglicht die Wahrung der Schutzinteressen mehrerer, im Grenzfall aller Beteiligter. Es wird beschrieben, für welche Anforderungen welche Bausteine eingesetzt werden sollten.

1 Einführung

Künftige Datennetze werden offene, heterogene und komplexe Gebilde sein. Interessenkonflikte zwischen Akteuren (Dienstnutzer, Netzbetreiber, Dienstebereitsteller, Abrechnungseinheiten, regulierende Einrichtungen) sind vorprogrammiert. Im engeren Sinne sind hier Schutzinteressen von Bedeutung.

Mehrseitige Sicherheit umfaßt die Einbeziehung der Schutzinteressen *aller* Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Die zunehmende Abwicklung geschäftlicher und privater Kommunikation stellt hierbei eine breite Palette von Anforderungen an die Realisierung von Sicherheit. Beispiele hierfür sind:

- Urheberrecht (geistig-kulturelles Gut soll auch im Zeitalter der Digitalisierung angerechnet werden können),
- Zurechenbarkeit (Menschen treffen verbindliche Absprachen),

- Persönlicher informationeller Schutzraum (Privatheit, Vertraulichkeit).

Eine daraus ableitbare Handlungsstruktur, die mehrseitige Sicherheit einbezieht, muß deshalb auch unterschiedlich starken Partnern die Ausübung ihrer Rechte (Schutzrechte) ermöglichen. Deshalb sind künftige Datennetze entsprechend mehrseitig sicher zu gestalten, da sonst gesellschaftliche Werte in Frage gestellt sind.

Bei der Sicherheit informationstechnischer Systeme unterscheidet man nach der Art der Ereignisse, gegen die die Sicherungsmechanismen wirken sollen, *beabsichtigte Angriffe* (z.B. Abhören, Manipulation und Zerstören von Informationen, aber auch Software und Hardware) und *unbeabsichtigte Ereignisse* (höhere Gewalt, technische Fehler, Fahrlässigkeit). Im Englischen werden die Begriffe *security* für beabsichtigte und *reliability* für unbeabsichtigte Ereignisse verwendet.

Schutz gegen beabsichtigte Angriffe	**... gegen unbeabsichtigte Ereignisse**
Vertraulichkeit • Schutz der Kommunikationsinhalte • Anonymität • Unbeobachtbarkeit • Unverkettbarkeit • Pseudonymität • Sicherheit gegen unbefugten Gerätezugriff	
Integrität und Zurechenbarkeit • Unabstreitbarkeit • Übertragungsintegrität • Abrechnungssicherheit	
Verfügbarkeit • Ermöglichen von Kommunikation	**Verfügbarkeit** • Funktionssicherheit • Technische Sicherheit **Sonstige Schutzziele** • Maßnahmen gegen hohe Gesundheitsbelastung

Tabelle 1: Abgrenzung von Schutz gegen beabsichtigte und unbeabsichtigte Ereignisse

Dieses Papier diskutiert die Schutzmechanismen mehrseitiger Sicherheit. Sie können den Schutzinteressen der Akteure angepaßt und miteinander kombiniert werden.

Ein Schwerpunkt der Betrachtungen liegt auf kryptographischen Schutzmechanismen. Mit ihrer Hilfe ist die Sicherstellung von Vertraulichkeits- und Integritätseigenschaften mög-

lich. Die Sicherstellung von Verfügbarkeitseigenschaften kann durch die kryptographischen Mechanismen zwar unterstützt, aber nicht erreicht werden.

2 Realisierung mehrseitiger Sicherheit

Die Vertrauensverhältnisse zwischen den verschiedenen beteiligten Instanzen innerhalb eines IT-Systems entscheiden stark darüber, welches Schutzniveau erreicht werden kann. Wir unterscheiden dabei

- persönlich erreichbaren Schutz (unilateral erreichbarer Schutz),
- zwischen zwei Parteien erreichbarer Schutz, ohne daß weiteren Instanzen bei der Erbringung der Sicherheit getraut werden muß (bilateral erreichbarer Schutz),
- durch die Kooperation mehrerer Parteien erreichbarer Schutz (multilateral erreichbarer Schutz).

Bevor in den nächsten Kapiteln auf Schutzmechanismen zur Ralisierung von Sicherheit eingegangen wird, sollen die o.g. Beziehungen etwas näher erläutert werden. Dabei werden einige der später erläuterten Schutzmechanismen bereits als Beispiele herangezogen.

2.1 Unilateral erreichbarer Schutz

Die maximal erreichbare persönliche Sicherheit eines Benutzers eines IT-Systems kann nie größer werden als die Sicherheit des Gerätes, mit dem er physisch direkt interagiert. Dieses Gerät wird normalerweise durch ein dem Teilnehmer vertrauenswürdiges Benutzerendgerät realisiert (vgl. [PPSW_95]). Gleichzeitig bildet dieses Gerät den Vertrauensbereich dieses Teilnehmers. Das bedeutet, Angriffe innerhalb dieses Bereichs finden nicht statt. In diesem Vertrauensbereich kann der Nutzer geheime Berechungen durchführen. Darüber hinaus muß das Gerät auch über ein vertrauenswürdiges Benutzerinterface verfügen. Ist ein Benutzerendgerät für den Teilnehmer nicht (mehr) vertrauenswürdig, so können noch so gute kryptographische Systeme ihm keinerlei Sicherheit bieten.

Die **Existenz eines Vertrauensbereichs** ist die Voraussetzung für die persönliche Sicherheit eines Nutzers. Niemand sonst innerhalb des IT-Systems, dem der Nutzer *nicht* vertraut, kann ihm ein solches Gerät bereitstellen, ohne daß die Sicherheitsinteressen dieses Nutzers gefährdet wären. Deshalb bezeichnen wir die persönliche Sicherheit eines Nutzerbereiches primär als unilaterales Problem.

2.2 Bilateral erreichbarer Schutz

2.2.1 Teilnehmer und Endgerät

Leider ist in der Praxis die unilaterale (allein durch den Nutzer) Realisierung eines vertrauenswürdigen Endgerätes schwer bzw. nicht möglich, da ihm meist die technischen Voraussetzungen fehlen werden. Er muß also zumindest noch dem Produzenten des Gerätes vertrauen können. Da nun zumindest zwei Parteien (Teilnehmer, Produzent) an der Erbringung der Sicherheit beteiligt sind, ist der Schutz nur durch bilaterales Vertrauen erreichbar.

Fall1: In vielen Anwendungen gehen Benutzerendgeräte dauerhaft in den Verfügungsbereich anderer Instanzen über, die damit auch die physische Kontrolle über das Gerät erlangen. Ein Beispiel hierfür sind Telefonkarten, die ein Telekommunikationsunternehmen ausgibt. Mit dem Kauf einer solchen Karte besitzt ein potentieller Angreifer ein „Gerät" des Telekommunikationsunternehmens. Ohne physische Schutzmaßnahmen könnte er es beliebig ausforschen und manipulieren, um unberechtigt (unbezahlt) Dienste zu nutzen. Das bedeutet, das Gerät muß ausforschungssicher (oder engl. **tamper resistant**) sein. Da dem Angreifer u.U. viel Zeit (im Bereich von Monaten oder gar Jahren) zum Angriff zur Verfügung steht und er außerdem in vielen Fällen beim Angriff die Zerstörung des Gerätes riskieren kann, ohne entdeckt zu werden, ist die Abwehr solcher Angriffe mit sehr hohem Aufwand verbunden und dauerhaft praktisch nicht möglich, da jederzeit neuartige Angriffsmöglichkeiten entdeckt werden können.

Fall 2: Die Ausforschungssicherheit von Geräten ist jedoch nicht erst nötig, wenn eine Instanz ein Gerät an eine andere Instanz zum dauerhaften Verbleib weitergibt. Ebenso müssen die geheimen Daten (z.B. Schlüssel) in einem persönlichen Gerät eines Nutzers bei Verlust des Gerätes gegen Ausforschung durch den Finder bzw. Dieb geschützt werden.

Fall 3: In der Praxis sind auch solche Benutzerendgeräte problematisch, die beim regulären Betrieb für gewisse Zeit in den physischen Verfügungsbereich anderer Instanzen übergehen, beispielsweise Chipkarten, die in fremde Geräte gesteckt werden (vgl. [CZ_96]). So genügt in machen Fällen die Auswertung der elektromagnetischen Strahlung des Gerätes während der Ausführung einer kryptographischen Operation, um auf geheime Daten zu schließen. In diesem Fall sind allerdings nur physisch unentdeckbare (nicht zerstörende) Angriffe möglich und die zur Verfügung stehende Zeit des Angreifers ist stärker beschränkt als im Fall 1.

2.2.2 Schutz zwischen zwei Kommunikationspartnern

Vertraulichkeit des Nachrichtenaustauschs und **Integritätssicherung** von Nachrichten sind typische bilaterale Schutzziele zwischen zwei Kommunikationspartnern. So bleibt z.B. eine Nachricht nur dann vertraulich gegenüber Dritten, wenn *beide* Teilnehmer einer

Kommunikationsverbindung die Nachricht vertraulich behandeln. Jeder Teilnehmer muß dem anderen jeweils vertrauen; die Sicherheit ist nur bilateral erreichbar. Für die Überprüfung der Nachrichtenintegrität gilt dies ebenfalls.

Authentikationsverfahren mit symmetrischen Schlüsseln, aber auch Verschlüsselungssysteme mit öffentlichen Schlüsseln sind typische Schutzmechanismen, um bilaterale Schutzziele zu erreichen.

2.3 Multilateral erreichbarer Schutz

Die **digitale Signatur** ist ein Verfahren, mit dem multilateraler Schutz erreicht werden kann. Zunächst gewährleistet auch sie bilaterale Sicherheit, solange Sender und Empfänger sich einig sind über die Korrektheit der Signatur. Im Streitfall können jedoch Empfänger und Sender eine Dritte Instanz einschalten, welche die Signatur nach objektiven Gesichtspunkten als korrekt anerkennt oder ablehnt, ohne daß die Schutzinteressen einer Partei (Sender, Empfänger, Dritter) verletzt werden (multilateraler Schutz). Bei der digitalen Signatur heißt dies konkret, daß der Signierer seinen geheimen Schlüssel im Streitfall nicht offenlegen muß. Allgemeiner formuliert bedeutet dies, daß nur der Signierer Signaturen leisten kann, während jeder andere die Korrektheit der Signatur überprüfen kann.

Es gibt auch Schutzziele, die ausschließlich multilateral erreichbar sind. Hierzu gehören Anonymität und Unbeobachtbarkeit, aber auch die Verfügbarkeit. **Verfügbarkeit** der Kommunikation ist beispielsweise minimal 3-lateral: Die beteiligten Parteien sind die beiden Kommunikationspartner sowie mindestens ein Kommunikationsdiensterbringer. Jede der drei Parteien muß willens und fähig sein zu kommunizieren bzw. die Kommunikationsverbindung herzustellen.

Bei **Anonymität** ist geschützt, wessen Handlungen innerhalb einer sog. Anonymitätsgruppe nicht mit seiner Identität verkettbar sind. Genaue Definitionen findet man in [Pfit_90, S.15]. Da typischerweise eine Handlung nur dann anonym ist, wenn sie nicht durch einen Angreifer nicht zu ihrem Urheber zugeordnet werden kann, müssen mehrere unterschiedliche und nicht angreifende Parteien innerhalb einer Anonymitätsgruppe agieren. Deshalb ist Anonymität nur multilateral erreichbar.

Nachdem ein allgemeiner Überblick über notwendige Beziehungen zwischen verschiedenen Instanzen gegeben wurde, sollen nun verschiedene Schutzmechanismen zur Realisierung von Vertraulichkeit, Integrität und Verfügbarkeit beschrieben werden.

3 Vertraulichkeit

In den folgenden Abbildungen befindet sich links und rechts je ein Vertrauensbereich der jeweiligen Teilnehmer. In der Mitte unten befindet sich der Angriffsbereich, d.h. der Bereich, wo Angriffe berücksichtigt sind.

3.1 Konzelationssysteme

3.1.1 Symmetrisches kryptographisches Konzelationssystem

Die bekanntesten und ältesten kryptographischen Systeme sind symmetrische Konzelationssysteme. Ihre bekanntesten modernen Vertreter sind DES und IDEA (siehe z.B. [Schn_96]).

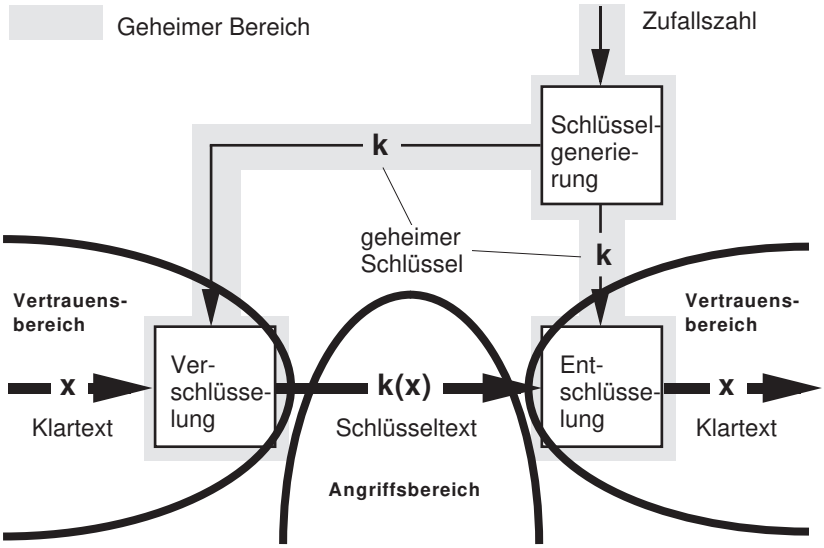

Abbildung 1: Symmetrisches kryptographisches Konzelationssystem

Wenn eine Nachricht *x* verschlüsselt über ein unsicheres Netz gesendet werden soll, muß zuvor der Schlüssel *k* bei Sender und Empfänger vorliegen. Wenn sich Sender und Empfänger vorher getroffen haben, können sie *k* bei der Gelegenheit austauschen. Wenn aber einer die Netzadresse des anderen (z.B. eines Dienstanbieters in einem offenen System) aus einem Verzeichnis (z.B. einer Art Telefonbuch) entnimmt und beide nun vertraulich kommunizieren wollen, wird es schwierig. In der Praxis geht man daher meist von der Existenz einer vertrauenswürdigen „Schlüsselverteilzentrale“ *Z* aus.

Jeder Teilnehmer A tauscht bei der Anmeldung zum offenen System einen Schlüssel mit Z aus, etwa k_{AZ}. Wenn nun A mit B kommunizieren will und noch keinen Schlüssel mit B gemeinsam hat, so fragt er bei Z an. Z generiert einen Schlüssel k und schickt ihn sowohl an A als auch an B, und zwar mit k_{AZ} bzw. k_{BZ} verschlüsselt. Von da an können A und B den Schlüssel k benutzen, um in beide Richtungen verschlüsselte Nachrichten zu schicken. Die Vertraulichkeit ist natürlich nicht sehr groß: Außer A und B kann auch Z alle Nachrichten entschlüsseln.

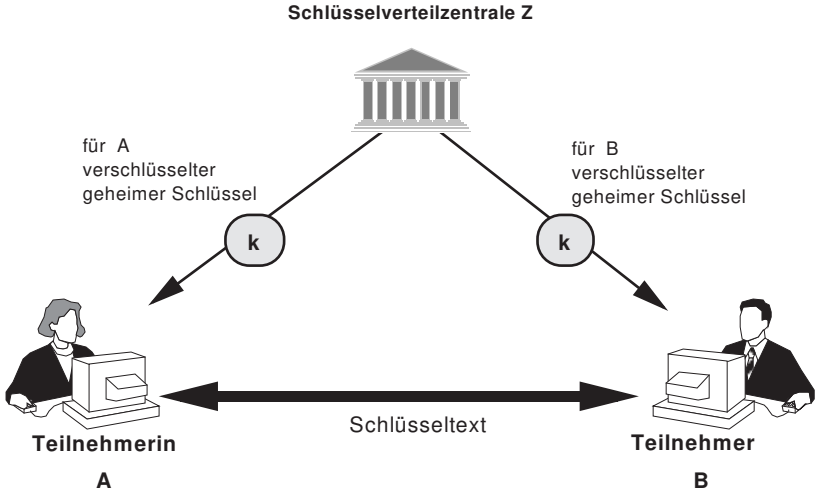

Abbildung 2: Schlüsselverteilung bei symmetrischen Konzelationssystemen

3.1.2 Asymmetrisches kryptographisches Konzelationssystem

Die bekanntesten Vertreter asymmetrischer kryptographisches Konzelationssysteme sind RSA und ElGamal (siehe [Schn_96]). Im Vergleich zu symmetrischen Konzelationssystemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 1000).

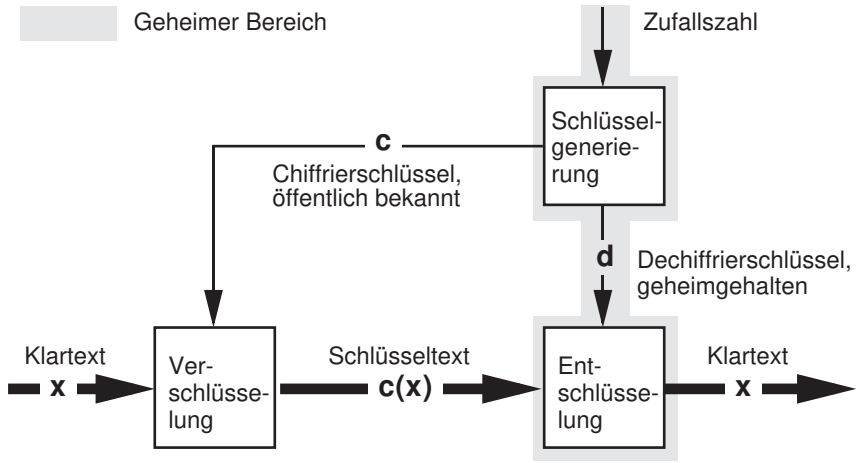

Abbildung 3: Asymmetrisches kryptographisches Konzelationssystem

Asymmetrische Konzelationssysteme wurden erfunden, um die Schlüsselverteilung zu vereinfachen. Hier sind zum Ver- und Entschlüsseln verschiedene Schlüssel c und d erforderlich, und nur d muß geheimgehalten werden. Damit man c tatsächlich nicht geheimhalten muß, darf natürlich d nicht mit vernünftigem Aufwand aus c zu bestimmen sein.

Nun kann jeder Benutzer A sich selbst ein Schlüsselpaar (c_A, d_A) generieren und muß d_A nie jemand anderem mitteilen. Der öffentliche Schlüssel c_A muß so verteilt werden, daß jeder andere Teilnehmer B, der A eine vertrauliche Mitteilung schicken will, an c_A gelangt. B kann c_A offen in sein Adreßbuch schreiben. Auch können Bekannte sich c_A weitererzählen. Für Kontakte mit Unbekannten könnte c_A gleich mit in dem Verzeichnis stehen, wo B die Netzadresse von A nachschaut. Gibt es kein solches Verzeichnis außerhalb des Netzes, so kann ein im Netz agierendes Schlüsselregister R an seine Stelle treten. Man beachte, daß R die Nachrichten nicht entschlüsseln kann.

3.1.3 Symmetrisches steganographisches Konzelationssystem

Bei der Verwendung von Kryptographie ist im Kommunikationsnetz erkennbar, ob gerade vertraulich oder authentisiert kommuniziert wird, sofern keine weiteren Schutzmaßnahmen ergriffen werden. Bei Steganographie ist das nicht der Fall. Steganographische Konzelationssysteme betten geheimzuhaltende Nachrichten in harmlos wirkende Hüllnachrichten (z.B. digitalisierte Fotos oder Sound-Dateien) ein, so daß für Außenstehende, die nur den Stegotext beobachten, nicht einmal die Existenz der geheimen Nachricht erkennbar ist und damit auch nicht ihr Inhalt. Insbesondere Multimedia-Kommunikation, aber auch bereits das normale ISDN-Telefon bieten geeignete Hüllnachrichten in Hülle und Fülle.

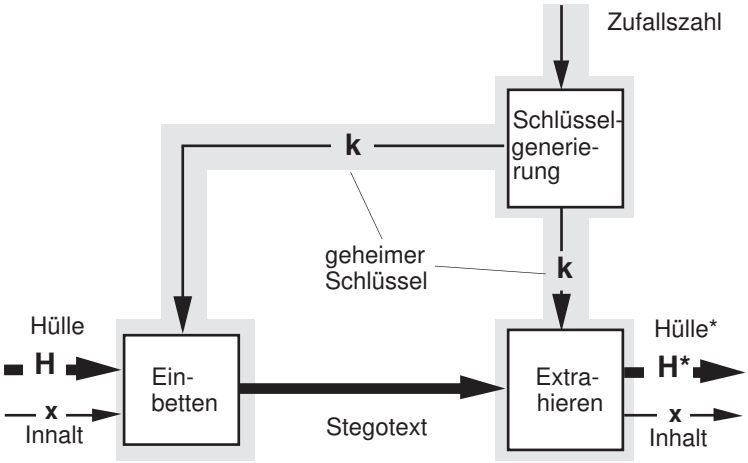

Abbildung 4: Symmetrisches steganographisches Konzelationssystem

Ein Nachteil der steganographischen Konzelation ist, daß zum Übertragen einer bestimmten Informationsmenge ein Vielfaches an Hüllinformation benötigt wird. Der Grund liegt darin, daß *x* meist nur in den niederwertigsten Bits der Hüllinformation untergebracht werden kann, da nur diese Bits je nach Hüllinformation derart indeterministisch sind, daß ihre Veränderung für den Außenstehenden zu keiner beobachtbaren Beeinträchtigung der Hüllinformation führt.

Bisher sind nur *symmetrische* steganographische Konzelationssysteme bekannt. Die selbstverständlich mögliche Hintereinanderschaltung eines asymmetrischen Konzelationssystems und symmetrischen Stegosystems führt nicht zu einem asymmetrischen Stegosystem!

3.2 Anonymität und Unbeobachtbarkeit

Bereits steganographische Konzelationssysteme erlauben in gewissen Grenzen den unbeobachtbaren Austausch von Nachrichteninhalten, indem in einer unauffälligen Hüllnachricht verborgene Informationen ausgetauscht werden können. Trotzdem bleibt der Zugriff auf die Hüllinformationen beobachtbar. Mittels spezieller Schutzmechanismen kann die Unbeobachtbarkeit des Nachrichtenaustauschs allgemein und des Sendens und Empfangens von Nachrichten jedoch erreicht werden.

Die hierzu verwendeten Mechanismen nutzen meist die oben beschriebenen kryptographischen Basismechanismen in speziellen Kommunikationsprotokollen und/oder speziellen Nachrichtenformaten aus.

Bekannte Schutzmechanismen für Anonymität und Unbeobachtbarkeit sind

- Schutz des Empfängers durch Verteilung (Broadcast) und implizite Adressierung,
- Schutz des Senders durch Dummy Traffic, DC-Netze (überlagerndes Senden, [Chau_88]) und Ring-Netze [Pfit_90],
- Schutz der Kommunikationsbeziehung zwischen Sender und Empfänger durch Mixe [Chau_81, Pfit_90],
- Schutz von Datenbankzugriffen durch „Blindes Lesen“ (Blinded Message Service, [CoBi_95]),
- Schutz des Senders gegen Peilbarkeit (in Funknetzen) durch Bandspreiztechniken (Spread Spectrum Systems, [Torr_92, PiSM_82])
- Schutz von Aufenthaltsorten (in Funknetzen und mobilen Festnetzen) durch spezielle Pseudonyme sowie anonyme und unbeobachtbare Verfahren zum Location Management (siehe z.B. [Pfit_93, KFJP_96, FeJP_96] sowie weitere Artikel in diesem Buch).

Aus Platzgründen ist es leider nicht möglich, auf alle oben erwähnten Mechanismen einzugehen. Deshalb sollen nur Broadcast, das Mix-Konzept, das DC-Netz und Bandspreiztechniken kurz erläutert werden.

3.2.1 Schutz des Empfängers durch Verteilung (Broadcast)

Einer der einfachsten und wirkungsvollsten Schutzmechanismen ist Verteilung. Jeder Nutzer eines Komunikationsnetzes erhält alle Nachrichten aller anderen Teilnehmer. Handelt es sich um vertrauliche Daten, können sie mit den o.a. Basismechanismen problemlos verschlüsselt werden. Ebenso ist eine Integritätssicherung mit Authentikationssystemen möglich.

Die Adressierung eines Nutzers kann in Broadcast-Systemen sowohl explizit als auch implizit erfolgen. Bei expliziten Adressen kann jeder den Empfänger einer Nachricht erkennen. Damit die Nachrichten nur vom intendierten Adressaten erkannt werden können, werden sie mit impliziten Adressen versehen. *Implizite* Adressen kennzeichnen im Gegensatz zu *expliziten* weder einen Ort im Netz noch eine Station, sondern sie sind nur ein ansonsten bedeutungsloses und mit nichts anderem in Beziehung zu setzendes Merkmal für den Empfänger. Er kann daran erkennen, ob eine Nachricht für ihn bestimmt ist. *Offene* implizite Adressen können von Unbeteiligten auf Gleichheit getestet werden. Eine geeignete Realisierung sind Zufallszahlen, die vom Empfänger mittels eines Assoziativspeichers, in den alle für die Station gerade gültigen impliziten Adressen geschrieben werden, sehr effizient erkannt werden können. *Verdeckte* implizite Adressen können außer vom Adressaten von niemand auf Gleichheit getestet werden. Der Test auf Gleichheit durch den Adressaten stellt eine kryptographische Operation dar und ist deshalb auch für den Adressaten deutlich aufwendiger als bei offenen impliziten Adressen.

3.2.2 Das Mix-Konzept

Die folgende Darstellung soll einen Eindruck vermitteln, wie durch das Mix-Netz unbeobachtbare Kommunikation ermöglicht wird. Die Idee wurde in [Chau_81] vorgestellt. Für eine ausführliche Diskussion des Mix-Netzes seien [PfWa_87, PfPW_88, Pfit_90, PfPf_90, PfPW_91, Pfit_93, Cott_95] empfohlen.

Das Mix-Konzept kommt in Vermittlungsnetzen zum Einsatz. Ein Mix-Netz verbirgt die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht. Hierzu wird die Nachricht über sog. Mixe geschickt. Ein Mix verbirgt dabei die Verketttung zwischen eingehenden und ausgehenden Nachrichten. Hierzu muß ein Mix

- eingehende Nachrichten speichern (Pool), bis genügend viele Nachrichten von genügend vielen Absendern vorhanden sind,
- ihr Aussehen verändern, d.h. sie umkodieren,
- die Reihenfolge der ausgehenden Nachrichten verändern, d.h. sie umsortieren und evtl. in einem Schub (Batch) ausgeben.

Um Angriffe durch Nachrichtenwiederholung zu verhindern, muß zu Beginn noch geprüft werden, ob eine eingehende Nachricht bereits gemixt wurde. Damit keine Verkettung zwischen eingehenden und ausgehenden Nachrichten über deren Länge möglich ist, sollten alle (eingehenden) Nachrichten die gleiche Länge haben, ebenso die ausgehenden.

Die technische Einrichtung, die dies leistet, wird Mix genannt. Um unbeobachtbare Kommunikation zu erreichen, wird die Nachricht entsprechend vorbereitet und über mehrere Mixe zum Empfänger transportiert. Die durchlaufenen Mixe sollten bzgl. ihres Entwurfs, ihrer Herstellung und ihres Betreibers möglichst unabhängig sein. Andernfalls könnten Mixe (oder gar ganze Mix-Ketten) überbrückt und so die Kommunikationsbeziehung aufgedeckt werden.

Das Ziel des Mix-Netzes ist, daß alle Mixe, die von einer Nachricht durchlaufen wurden, zusammenarbeiten müssen, um die Kommunikationsbeziehung zwischen Sender und Empfänger aufzudecken.

Eine Nachricht, die einen Mix durchläuft, ist nur innerhalb eines Schubes bzw. des Nachrichtenpools anonym. Deshalb muß sichergestellt sein, daß es nie vorkommt, daß ein Angreifer alle Nachrichten außer einer kennt, denn das käme der Deanonymisierung dieser Nachricht gleich. Arbeiten alle anderen Sender und Empfänger der zusammen in einem Schub gemixten Nachrichten zusammen, ist die Kommunikationsbeziehung ebenfalls aufgedeckt.

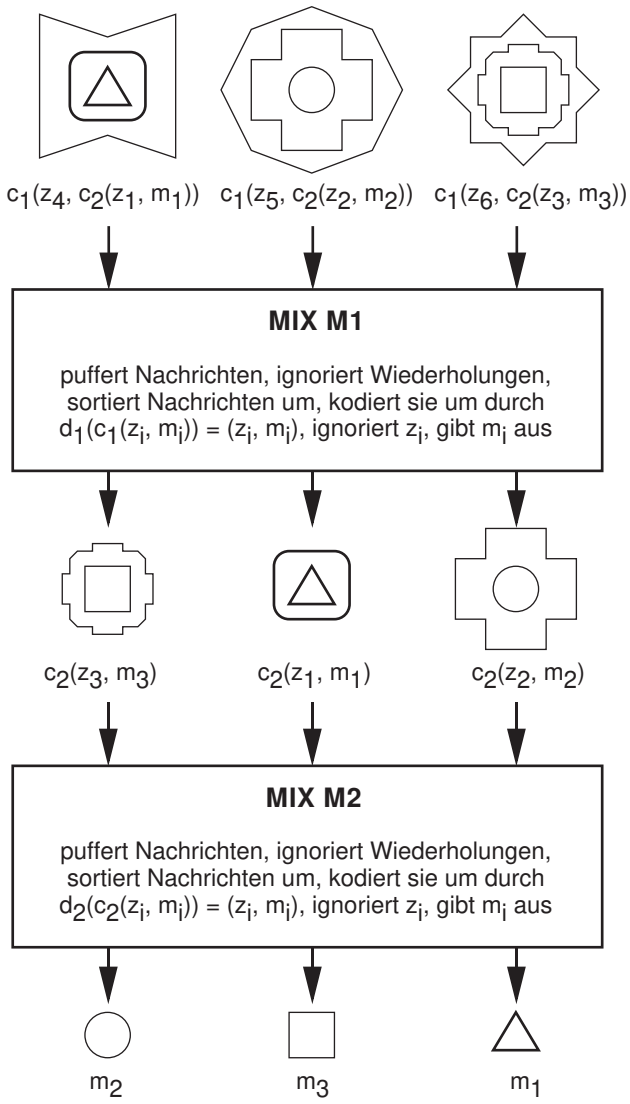

Abbildung 5: Umkodieren gemixter Nachrichten

Falls nicht genügend eingehende Nachrichten vorhanden sind, müssen künstliche erzeugt werden, damit die Verzögerungszeit einer Nachricht minimiert wird (Dummy Traffic). Hierzu sollte jeder Sender, der einen Mix benutzt, zwischen seinen sinnvollen Nachrichten sog. Leernachrichten senden, die (außer für den empfangenden Mix) nicht von sinnvollen

Nachrichten zu unterscheiden sind. Ebenso könnte der Mix eine stets konstante Anzahl von Ausgabenachrichten produzieren, die der Empfänger bzw. ein folgender Mix wieder als Leernachricht erkennt. Durch Dummy Traffic kann ein Angreifer außerdem nicht mehr feststellen, wann ein Sender wirklich senden will und wann nicht.

Die Kernfunktion eines Mixes ist das Umkodieren der Nachrichten. Hierzu wird mit Hilfe eines asymmetrischen Kryptosystems jede zu mixende Nachricht mit dem geheimen Schlüssel des Mixes entschlüsselt (umkodiert) und an den nächsten Mix weitergeschickt. Das Mix-Netz erreicht wegen der Verwendung asymmetrischer Verschlüsselung nur komplexitätstheoretische Sicherheit.

Damit in den Mixen die Umkodierung ablaufen kann, muß der Sender die zu mixende Nachricht entsprechend vorbereiten, d.h. mit den öffentlichen Schlüsseln c_i der Mixe Mi (i=1…n) nach folgender Vorschrift rekursiv verschlüsseln:

$$m_i = c_i(z_i, A_{Mi+1}, m_{i+1}) \quad \text{mit } i=n\ldots1$$

Es sei m_{n+1} die Nachricht, die der Empfänger erhalten soll. Die Emfängeradresse sei entsprechend A_{Mn+1}. Der Sender sendet m_1 mit A_{M1} adressiert in das Mix-Netz. Die Zufallszahlen z_i müssen bei Verwendung eines deterministischen Kryptosystems mitverschlüsselt werden, da sonst ein Angreifer die ausgehenden Nachrichten eines Mixes erneut verschlüsseln und so die passende eingehende Nachricht ermitteln könnte. Beim Umkodieren wirft der Mix die z_i einfach weg.

Das beschriebene Schema ist in der Lage, den Sender einer Nachricht zu schützen. Möchte dieser auch Nachrichten unbeobachtbar empfangen, kommen sog. anonyme Rückadressen zum Einsatz.

Hierzu bildet der spätere Empfänger seine anonyme Rückadresse nach folgende Vorschrift:

$$r_i = c_i(k_i, A_{Mi+1}, r_{i+1}) \quad \text{mit } i=n\ldots1$$

A_{Mn+1} ist die eigene Empfängeradresse und r_{n+1} ein sog. Adreßkennzeichen, an dem der Empfänger erkennt, welche Rückadresse vom Sender benutzt wurde. Dies ist nötig, um die k_i zu rekonstruieren, die in die Rückadresse hineinkodiert wurden. Der Empfänger veröffentlicht seine anonyme Rückadresse z.B. in einem öffentlichen Verzeichnis.

Der Sender einer Nachricht sendet die Rückadresse zusammen mit der zu übermittelnden Nachricht m an das Mix-Netz. Die Mixe Mi entschlüsseln die anonyme Rückadresse, verschlüsseln die mitgeschickte Nachricht unter dem gefundenen Schlüssel k_i mit einem symmetrischen Kryptosystem und schicken die Nachricht zusammen mit dem restlichen Teil der anonymen Rückadresse an den nächsten Mix bzw. den Empfänger. Im Verlauf dieses Prozesses entsteht so die Nachricht

$$m_i = k_{i-1}(m_{i-1}) \quad \text{mit } i=2\ldots(n+1) \text{ und } m_1 := m.$$

Beim Empfänger muß nun aus dem Adreßkennzeichen r_{n+1} hervorgehen, welche k_i verwendet wurden, damit die Nachricht m_{n+1} wieder entschlüsselt werden kann. Damit die Unbeobachtbarkeit des Empfängers nicht aufgehoben wird, darf jede anonyme Rückadresse nur einmal verwendet werden bzw. wird bei wiederholter Verwendung vom Mix ignoriert (Nachrichtenwiederholung).

3.2.3 Das DC-Netz: Schutz des Senders

Beim DC-Netz [Chau_88] wird durch sog. überlagerndes Senden aller Teilnehmer des Netzes der Schutz des Senders erreicht. Vertiefende Betrachtungen finden sich z.B. in [Pfit_90, LuPW_91, PfWa1_91].

Die Teilnehmer haben paarweise miteinander Schlüssel ausgetauscht, die sie vor den anderen Teilnehmern geheim halten. Das Netz ist getaktet und das Funktionsprinzip jedes Taktes (auch Runde genannt) ist einfach: Alle Teilnehmer, die nichts zu senden haben, senden eine kodierte Leerbotschaft (Null-Bits). Derjenige, der etwas zu senden hat, sendet seine Botschaft kodiert. Leernachrichten bzw. echte Botschaften werden dabei mit allen symmetrischen Schlüsseln, die ein Teilnehmer mit anderen Teilnehmern paarweise ausgetauscht hat, lokal bitweise XOR verknüpft und als sog. lokale Summe auf das Netz gegeben. Durch die lokale XOR-Verknüpfung der (Leer)-Botschaft mit den Schlüsseln sieht eine lokale Summe für denjenigen, der nicht alle lokalen Schlüssel kennt, wie Zufallszahlen aus. Durch die globale Überlagerung (Summierung) aller lokalen Summen heben sich die paarweisen Schlüssel weg, die Leerbotschaften liefern keinen Beitrag und es entsteht so die Botschaft, die ihrerseits alle Teilnehmer erhalten.

Beispiel (siehe Abb. 6): Es kooperieren drei Teilnehmer in einem DC-Netz. Sie haben vorher paarweise miteinander Schlüssel ausgetauscht. Teilnehmer A will eine Botschaft senden. B und C senden Leernachrichten.

Mit diesem Verfahren wird der Schutz des Senders erreicht. Unabhängig davon kann durch implizite Adressierung der Schutz des Empfängers erreicht werden und zusätzlich durch Konzelations- und Authentikationsverfahren die Vertraulichkeit und Integrität der Botschaft.

Ein dem überlagernden Senden sehr ähnliches Verfahren zur unbeobachtbaren Abfrage von Datenbanken wurde in [CoBi_95] vorgestellt. Durch paralleles Senden eines Anfragevektors an mehrere unabhängige Datenbanken mit gleichem Informationsbestand bildet jede Datenbank eine lokale XOR-Verknüpfung mehrerer Datenbankeinträge und sendet diese als Antwortvektor an den Teilnehmer zurück. Der Teilnehmer hat seine Anfragevektoren vorher so gebildet, daß die globale XOR-Verknüpfung der erhaltenen Antwortvektoren genau den gewünschten Datenbankeintrag ergibt.

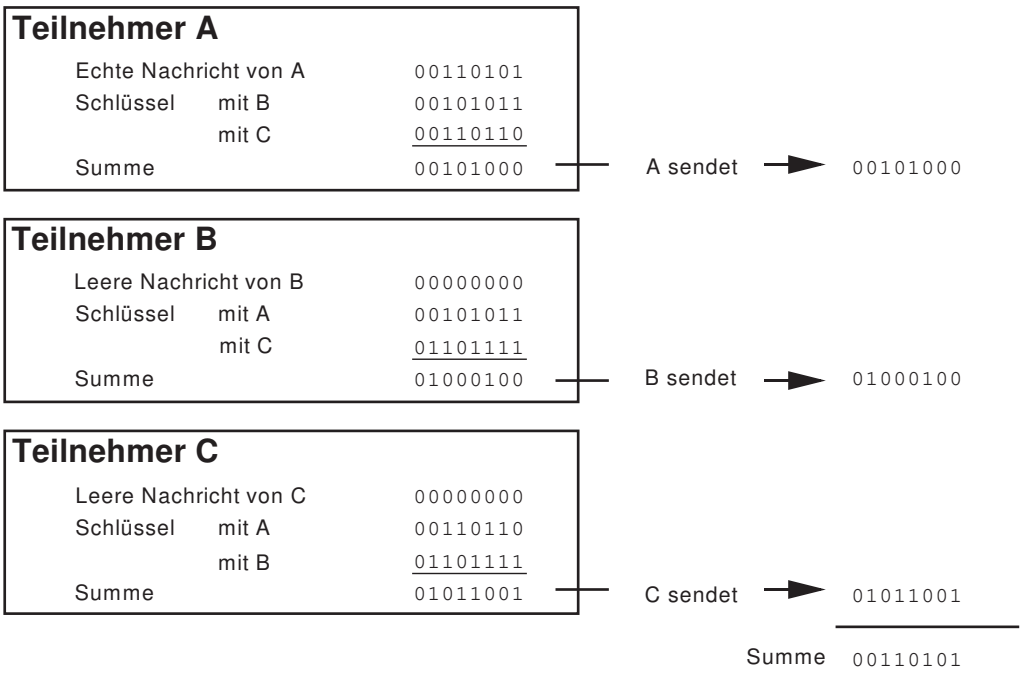

Abbildung 6: Bitweises Überlagerndes Senden im DC-Netz

3.2.4 Spread Spectrum Systems

Um beim DC-Netz die Unbeobachtbarkeit des Sendens zu erreichen, mußten alle Teilnehmer gleichzeitig senden. In mobilen Netzen, bei denen die Endgeräte über eine Funkschnittstelle mit dem Kommunikationsnetz verbunden sind, kommt noch hinzu, daß ein sendender Teilnehmer aufgrund der Wellenausbreitungseigenschaften peil- und damit ortbar ist. Will sich ein Teilnehmer gegen diese funktechnische Lokalisierung schützen, muß er spezielle Sendeverfahren einsetzen, die eine Peilung zumindest für Außenstehende verhindern. Der angewendete Mechanismus arbeitet ähnlich dem eines symmetrischen Konzelationssystems und wird Direct Sequence Spread Spectrum genannt. Die über die Funkschnittstelle zu übertragende Information wird mittels eines breitbandigen Spreizcodes, der geheimzuhalten ist, spektral gespreizt. Dadurch wird jedes zu übertragende Informationsbit auf das gesamte zur Verfügung stehende Frequenzband verteilt und verschwindet so im Rauschen. Kennt man den verwendeten Spreizcode, kann man mittels einer Korrelationsfunktion das Informationsbit wiedergewinnen.

Für weiterführende Informationen zu den Grundlagen der Bandspreiztechniken seien [Torr_92, PiSM_82] empfohlen. In [ThFe_95, FeTh_95] finden sich Überlegungen zur Anwendung von Direct Sequence Spread Spectrum im Mobilfunk.

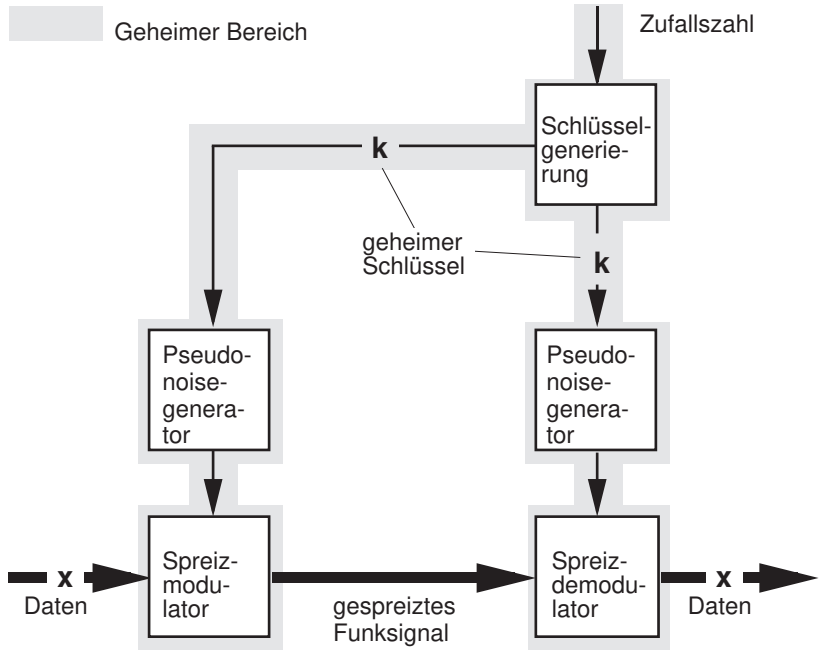

Abbildung 7: Direct Sequence Spread Spectrum

Mittels Spread Spectrum Systems kann auch Steganographie betrieben werden. Da gespreizte Signale wenig störanfällig sind, eignen sie sich z.B. als robust eingebettete Urheberinformationen eines steganographischen Authentikationssystems.

4 Integrität und Zurechenbarkeit

4.1 Authentikationssysteme

4.1.1 Symmetrisches kryptographisches Authentikationssystem

Ein symmetrisches kryptographisches Authentikationssystem ist in Abbildung 8 dargestellt. Hier wird die Nachricht durch den kryptographischen Algorithmus links nicht unverständlich gemacht, sondern es wird ein Prüfteil *MAC* (Message Authentication Code) an *x* angehängt. Der Empfänger kann anhand von *x* auch den richtigen MAC bilden und prüfen, ob der mit der Nachricht mitgekommene damit übereinstimmt.

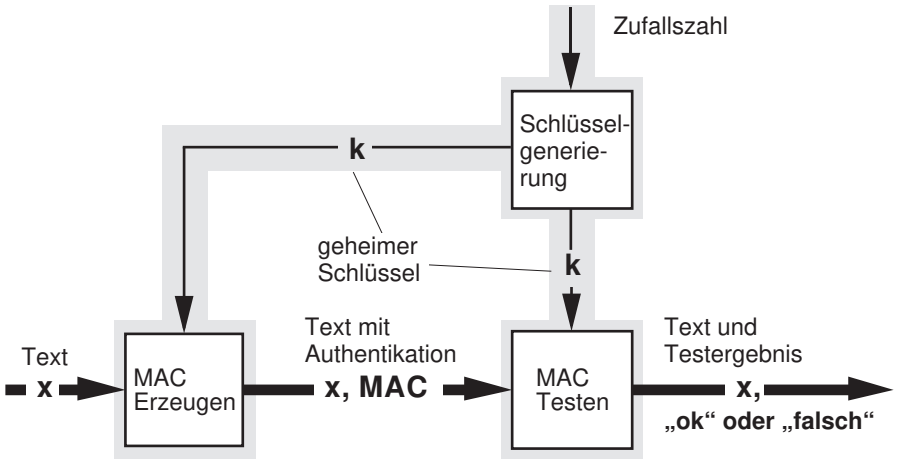

Abbildung 8: Symmetrisches kryptographisches Authentikationssystem

Die Schlüsselverteilung kann wie bei symmetrischen Konzelationssystemen erfolgen. Entsprechend könnte die Schlüsselverteilzentrale auch diesmal gefälschte Nachrichten unterschieben.

4.1.2 Asymmetrisches kryptographisches Authentikationssystem

Asymmetrische kryptographische Authentikationssysteme werden auch **digitale Signatursysteme** genannt und vereinfachen zunächst die Schlüsselverteilung analog zu asymmetrischen Konzelationssystemen. Ihr Hauptvorteil ist aber ein anderer: Der Empfänger *B* einer unterschriebenen Nachricht von *A* kann jedem anderen, der auch *A*s öffentlichen Schlüssel t_A kennt, beweisen, daß diese Nachricht von *A* stammt. Dies geht bei einem symmetrischen Authentikationssystem nicht: Selbst wenn z.B. vor Gericht die Schlüsselverteilzentrale bestätigen würde, welchen Schlüssel *A* und *B* hatten, kann ja *B* den MAC genausogut selbst erzeugt haben. Bei digitalen Signatursystemen ist jedoch *A* der einzige, der die Unterschrift erzeugen kann. Deswegen sind digitale Signatursysteme unumgänglich, wenn man rechtlich relevante Dinge digital in *zurechenbarer* Weise abwickeln will, z.B. bei digitalen Zahlungssystemen. Sie entsprechen dort der Funktion der eigenhändigen Unterschrift in heutigen Rechtsgeschäften.

Im Gegensatz zur symmetrischen Authentikation wird bei der digitalen Signatur ein eigener Testalgorithmus benötigt, der mit dem öffentlichen Schlüssel *t* arbeitet.

Man beachte, daß die Möglichkeit, den Testschlüssel privat mit seinem Kommunikationspartner auszutauschen, nur in dem Fall genügt, daß man diesem Partner vertraut, d.h. das Signatursystem nur als bequeme Form gegenseitiger Authentikation benutzt. Will man

aber sicher sein, daß eine Signatur später ggf. vor Gericht anerkannt wird, muß man sich versichern, daß man den richtigen Testschlüssel hat, d.h. zumindest zur Kontrolle bei einem Schlüsselregister nachfragen.

Die Beglaubigung (auch Zertifizierung genannt) des öffentlichen Testschlüssels bezieht sich – wie bei den öffentlichen Konzelationsschlüsseln – nicht auf den Schlüssel allein, sondern auf den *Zusammenhang* zwischen Schlüssel und Teilnehmer.

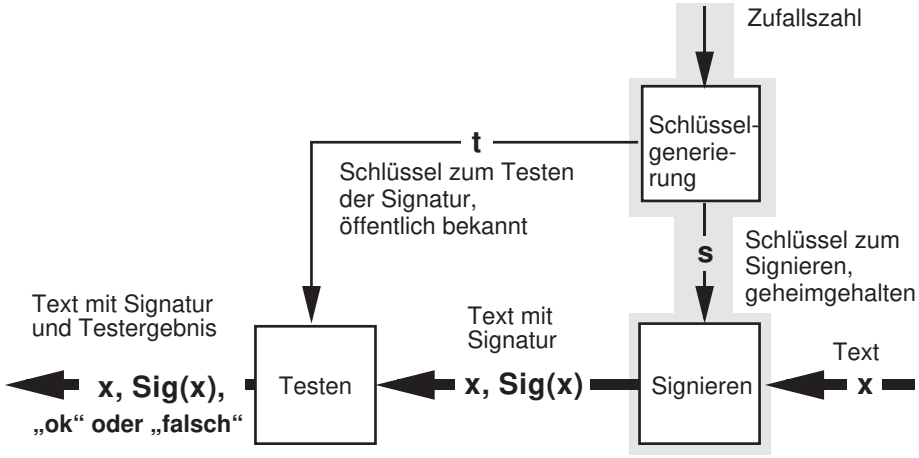

Abbildung 9: Signatursystem

4.1.3 Steganographisches Authentikationssystem

Steganographische Authentikationssysteme sind unter dem Namen **Watermarking** bekannt. Sie spielen für die Wahrnehmung von Urheberrechten an digitaler Information eine wichtige Rolle. Die Hülle (siehe steganographisches Konzelationssystem) stellt dabei die urheberrechtlich zu schützende Information dar. Die Urheberinformation sei x. Nun kommt es *nicht* darauf an, eine möglichst große Menge an Informationen x in die Hülle einzubetten. Vielmehr soll die Urheberinformation möglichst *robust* eingebettet werden. Am Beispiel digitaler Bilder wird dies deutlicher: Trotz einer Veränderung von Bildparametern (Größe, Farbe, Helligkeit etc.) oder Ausschneiden von Bildteilen zum Zwecke der eigenen Nutzung soll die Urheberrechtsinformation erhalten bleiben.

5 Verfügbarkeit

Wie bereits erwähnt, können kryptographische Systeme allein das Schutzziel Verfügbarkeit nicht realisieren. Die Verfügbarkeit von Daten, Programmen und Diensten kann je-

doch durch die adäquate technische Gestaltung der Kommunikationsinfrastruktur sichergestellt werden. Dabei spielen der Grad an **Diversität und Entwurfskomplexität** eine entscheidende Rolle.

So sollte im Interesse der Überschaubarkeit eine Kommunikationsinfrastruktur mit geringstmöglicher Entwurfskomplexität gewählt werden, damit sie keine, zumindest keine schweren, verborgenen Entwurfsfehler enthält. Ebenso sind Diversitätsengpässe zu vermeiden.

Ein diversitäres Kommunikationsnetz mit mehrfach redundanter und unterschiedlicher Leitungsführung kann so z.B. den Totalausfall von Teilen des Netzes vermeiden. Bei Funk könnte auf unterschiedliche Frequenzbänder ausgewichen werden, sobald Störungen auftreten. Besonders problematisch sind evtl. vorhandene Kommunikationsengpässe, z.B. Netzübergänge.

Verfügbarkeit kann nicht isoliert von den Schutzzielen Vertraulichkeit und Integrität betrachtet werden. So könnte z.B. die Störung der Verfügbarkeit für andere Teilnehmer zur Deanonymisierung und damit Beobachtbarkeit eines bestimmten Teilnehmers führen, falls die Teilnehmer zusammen in einer Anonymitätsgruppe hätten handeln sollen. Andererseits können z.B. Authentikationsmaßnahmen den unerkennbaren und unentdeckbaren Betriebsmittelentzug (und damit Verfügbarkeitsverlust) für andere Teilnehmer verhinden, wenn jeder Zugriff auf Betriebsmittel nur authentisiert erfolgen darf.

6 Zusammenfassung: Schutzziele

Die abschließende Übersicht stellt noch einmal alle Schutzziele und deren Schutzmechanismen gegenüber:

Schutzziele	Schutzmechanismen
Vertraulichkeit	
Nachrichteninhalte sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben.	bilateral: symm. Konzelationssysteme multilateral: asymm. Konzelationssysteme
Sender und/oder *Empfänger* von Nachrichten sollen voreinander *anonym* bleiben können, und *Unbeteiligte* (inkl. Netzbetreiber) sollen *nicht in der Lage* sein, sie *zu beobachten*.	nur multilateral erreichbar: Broadcast, Dummy Traffic, Mixe, DC-Netze, Ring-Netze, Blinded Message Service u.a.
Weder potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) sollen ohne Einwilligung den *momentanen Ort* einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers ermitteln können.	nur multilateral erreichbar: Spread Spectrum Systems, spezielle Verfahren zum Location Management

Integrität	
Fälschungen von *Nachrichteninhalten* (inkl. des *Absenders*) sollen erkannt werden.	bilateral: MACs (symm. Auth.) multilateral: Dig. Signaturen (asymm. Auth.)

Zurechenbarkeit	
Gegenüber einem Dritten soll der Empfänger *nachweisen* können, daß Instanz *x* die Nachricht *y gesendet hat*.	multilateral: Digitale Signaturen (von *x* unter *y*)
Der Absender soll das *Absenden* einer Nachricht mit korrektem Inhalt *beweisen* können, möglichst sogar den Empfang der Nachricht.	multilateral: Digitale Signaturen (des Empfängers)
Niemand kann dem Netzbetreiber *Entgelte* für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.	multilateral: Digitale Signaturen, spezielle Signaturverfahren (blinde Signaturen), anonyme und unbeobachtbare Abrechungsverfahren

Verfügbarkeit	
Das Netz ermöglicht Kommunikation zwischen allen Partnern, die dies *wünschen* (und denen es nicht verboten ist).	nur multilateral erreichbar: diversitäre Netze mit geringstmöglicher Entwurfskomplexität, Engpässe vermeiden

Tabelle 2: Zuordnung von Schutzzielen und Schutzmechanismen

7 Literatur

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65-75.

CoBi_95 David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers. 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

Cott_95 Lance Cottrel: Mixmaster & Remailer Attacks. http://www.obscura.com/~loki/remailer-essay.html.

CZ_96 Computer Zeitung: Heiße Chipkarten geben Code Preis, Computer Zeitung 31. Oktober 1996, Seite 1.

FeJP_96 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: Mixes in mobile communication systems: Location management with privacy. Information Hiding, R. Anderson [Hrsg.], LNCS 1174, Springer-Verlag, Berlin 1996, 121-135.

FeTh_95 Hannes Federrath, Jürgen Thees: Schutz der Vertraulichkeit des Aufenthaltsorts von Mobilfunkteilnehmern. Datenschutz und Datensicherung DuD 19/6 (1995) 338-348.

KFJP_96 Dogan Kesdogan, Hannes Federrath, Anja Jericho, Andreas Pfitzmann: Location managment strategies increasing privacy in mobile communication. Sokratis K. Katsikas, Dimitris Gritzalis (ed.), Informations Systems Security, IFIP SEC '96 Conference Committees, Chapman & Hall, London, 1996, 39-48.

LuPW_91 Jörg Lukat, Andreas Pfitzmann, Michael Waidner: Effizientere fail-stop Schlüsselerzeugung für das DC-Netz. Datenschutz und Datensicherung DuD 15/2 (1991) 71-75.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen. Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

PfPf_90 Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 373-381.

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze. Informatik-Spektrum 11/3 (1988) 118-142.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. Proc. Kommunikation in verteilten Systemen, IFB 267, Springer-Verlag, Berlin 1991, 451-463.

PfWa1_91 Birgit Pfitzmann, Michael Waidner: Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit. Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Berlin 1991, 302-320.

PfWa_87 Andreas Pfitzmann, Michael Waidner: Networks without user observability. Computers & Security 6/2 (1987) 158-166.

PiSM_82 R.L. Pickholtz, D.L. Schilling, L.B. Milstein: Theory of Spread-Spectrum-Communications – A Tutorial. IEEE Transactions on Communications 30/5 (1982) 855-878.

PPSW_95 Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Vertrauenswürdiger Entwurf portabler Benutzerendgeräte und Sicherheitsmodule. Hans H. Brüggemann, Waltraud Gerhardt-Häckl (ed.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS '95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 329-350.

Schn_96 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, (2nd ed.) New York 1996.

ThFe_95 Jürgen Thees, Hannes Federrath: Methoden zum Schutz von Verkehrsdaten in Funknetzen. Hans H. Brüggemann, Waltraud Gerhardt-Häckl (ed.): Verläßliche IT-Systeme, Proceedings der GI-Fachtagung VIS '95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 180-192.

Torr_92 Don J. Torrieri: Principles of Secure Communication Systems. 2nd ed., Artech House Books, 1992.