Beitrag zum Tutorium „Vernetzte Systeme und Sicherheit der Informationsverarbeitung“ der GI-Jahrestagung 1992

Datenschutz garantierende offene Kommunikationsnetze*

Andreas Pfitzmann, Birgit Pfitzmann
Institut für Informatik
Universität Hildesheim
Samelsonplatz 1, W-3200 Hildesheim, FRG
Tel.: 05121 / 883-735, -739
Fax: 05121 / 860475
e-mail: pfitza@informatik.uni-hildesheim.de

Michael Waidner
Institut für Rechnerentwurf und Fehlertoleranz
Universität Karlsruhe
Postfach 6980, W-7500 Karlsruhe 1, FRG
Tel.: 0721 / 608-4024
Fax: 0721 / 370455
e-mail: waidner@ira.uka.de

Zusammenfassung. Immer mehr kommunizieren Menschen und Maschinen über öffentliche Vermittlungsnetze. Sensitive Daten (z.B. personenbezogene Daten, Geschäftsgeheimnisse) können dabei sowohl aus den eigentlichen **Nutzdaten** als auch aus den **Vermittlungsdaten**, z.B. Ziel- und Herkunftsadresse, Datenumfang und Zeit, gewonnen werden.

Wir untersuchen, wie sie vor illegalen und legalen Netzbenutzern, dem Betreiber des Netzes und seinen Angestellten sowie den Herstellern der Vermittlungszentralen geschützt werden können. Manche Vermittlungsdaten, z.B. die genauen Netzadressen der Teilnehmer, müssen auch vor Kommunikationspartnern, etwa Datenbanken, geschützt werden, damit sie nicht als Personenkennzeichen verwendbar werden.

Bei der heute üblichen und von der Deutschen Bundespost auch für die Zukunft geplanten Struktur öffentlicher Netze, insbesondere des diensteintegrierenden ISDN, erlauben auch juristische Datenschutzvorschriften und Verschlüsselung keinen ausreichenden und mit vernünftigem Aufwand **überprüfbaren** Datenschutz. Dies dürfte das im Volkszählungsurteil des Bundesverfassungsgerichts formulierte „Recht auf informationelle Selbstbestimmung” verletzen.

Deshalb werden die zur Abhilfe geeigneten bekannten Grundverfahren zusammen mit einigen Überlegungen zu ihrer Implementierung dargestellt. Danach wird gezeigt, wie diese Grundverfahren zum schrittweisen Ausbau eines Datenschutz garantierenden offenen, zunächst schmalbandigen, später bei Bedarf breitbandigen und diensteintegrierenden Digitalnetzes verwendet werden können.

1 Problemanalyse

1.1 Heutige und geplante Kommunikationsnetze der Deutschen Bundespost

Immer mehr benutzen wir öffentliche Kommunikationsnetze:

- Hörfunk, Fernsehen, Videotext z.B. sind Dienste, die (genauer: deren Informationen) heute vorwiegend über das Rundfunksendernetz der Deutschen Bundespost, mehr und mehr aber über das entstehende Breitbandkabelverteilnetz **verteilt** werden. Zweck des Breitbandkabelverteilnetzes ist die Verbesserung der Dienstqualität durch Erhöhung der verfügbaren Bandbreite: Mehr empfangbare Fernsehprogramme heißt dann Kabelfernsehen, größeres Informationsangebot bei Videotext heißt dann Kabeltext.
- Fernsprechen, Bildschirmtext, elektronisches Postfach (TELEBOX) für elektronische Brief- und Sprachpost, Fernschreiben (TELEX, TELETEX), Fernkopieren (TELEFAX) und Fernwirken

* Dieser Übersichtsartikel deckt den Vortrag *Neue Techniken zur Lösung neuer Probleme* von Andreas Pfitzmann ab. Er basiert auf dem Artikel [PfPW_88], der um die inzwischen erschienene Literatur ergänzt und in den Abschnitten 2.2.1, 2.2.3.1 leicht erweitert wurde.

(TEMEX) sind Dienste, die heute über das analoge Telefonnetz bzw. das digitale Text- und Datennetz der Deutschen Bundespost, beginnend ab 1988 mit höherer Dienstqualität über das dann digitale „Telefonnetz" **vermittelt** werden.

Das heutige analoge Telefonnetz und das dieselben Teilnehmeranschlußleitungen benutzende digitale „Telefonnetz", das ab 1988 in einigen Ortsnetzen und ab etwa 1993 in der ganzen Bundesrepublik entstehen wird, sind schmalbandige Netze, d.h. sie sind im Gegensatz zu breitbandigen Netzen nicht in der Lage, Bewegtbilder guter Qualität (z.B. Fernsehen) zu übertragen.

Zur Zeit benutzen wir also zwei grundsätzlich verschiedene Typen von Netzen:

- **Verteilnetze**, in denen alle Teilnehmerstationen vom Netz dasselbe erhalten und jeder Teilnehmer lokal auswählt, ob und, wenn ja, was er tatsächlich empfangen will, und
- **Vermittlungsnetze**, in denen jede Teilnehmerstation vom Netz individuell nur das erhält, was der Teilnehmer angefordert oder ein anderer Teilnehmer an ihn gesendet hat.

In den realisierten und geplanten öffentlichen Verteilnetzen findet Kommunikation nur in einer Richtung, vom Netz zum Teilnehmer, statt; in Vermittlungsnetzen wird in beiden Richtungen kommuniziert.

Da langfristig ein Netz für alle Dienste, ein sogenanntes **diensteintegrierendes** Netz, zumindest im Teilnehmeranschlußbereich preiswerter als mehrere verschiedene Netze ist und da alle verteilten Dienste auch vermittelt werden können, strebt die Deutsche Bundespost an, ab 1992 alle Dienste in einem Netz zu vermitteln [Rose_85, Schö_84, ScSc_84, ScS1_84, Thom_87].

Damit auch breitbandige Dienste vermittelt zum Teilnehmer übertragen werden können, müssen neue Teilnehmeranschlußleitungen (Glasfaser) verlegt werden. Nach und nach wird dadurch ein Breitbandkabelverteilnetz überflüssig. Über ein breitbandiges diensteintegrierendes Vermittlungsnetz können nicht nur alle Dienste angeboten werden, die über ein Breitbandkabelverteilnetz und ein schmalbandiges Vermittlungsnetz zusammen angeboten werden können, sondern auch noch zusätzlich Dienste, die breitbandige Kommunikation zwischen Teilnehmern erfordern, z.B. Bildfernsprechen mit guter Bildqualität.

Da digitale Werte in modernen technischen Systemen nicht nur leichter übertragen, sondern auch leichter verarbeitet, insbesondere vermittelt werden können [Schö_86 Seite 9], wird das diensteintegrierende Netz ein **digitales** Netz sein, abgekürzt ISDN (Integrated Services Digital Network).

Ersetzt das breitbandige ISDN (abgekürzt Breitband-ISDN oder B-ISDN [Steg_85]) das Breitbandkabelverteilnetz, nennt es die Deutsche Bundespost Integriertes Breitbandfernmeldenetz (IBFN) [ScS1_84]. Pilotversuche zur Erprobung des IBFN sind unter der Abkürzung BIGFON (Breitbandiges integriertes Glasfaser-Fernmeldeortsnetz) bekannt [Brau_82, Brau_83, Brau_87].

Die geschilderte Entwicklung ist in Abb. 1 etwas detaillierter dargestellt. Nicht dargestellt und im folgenden auch nicht explizit behandelt sind Funknetze, die als Anschlußnetz für ortsbewegte Teilnehmer, als Ersatznetz in Katastrophenfällen und als Garanten grenzüberschreitender Informationsfreiheit bleibende Bedeutung haben.

Die dieser Planung von der Post zugrundegelegten Leistungsanforderungen der Netzbenutzer sollen im folgenden als gegeben betrachtet werden, und es soll untersucht werden, welche negativen Auswirkungen auf den Datenschutz eine Realisierung nach den Plänen der Post hätte und wie sie sich vermeiden lassen.

Es sei jedoch schon an dieser Stelle bemerkt, daß sowohl die im folgenden geschilderte Datenschutzproblematik wie auch die vorzuschlagenden Gegenmaßnahmen unabhängig von allen Leistungsanforderungen und Diensteintegration auf jedes Kommunikationsnetz zutreffen, das hinreichend offen ist und von einer großen Zahl von Bürgern intensiv genutzt wird, insbesondere also auf das heutige Fernsprechnetz und jedes Netz, das Fernsprechen als einen Dienst integriert [Pfit_86, PPfW_87].

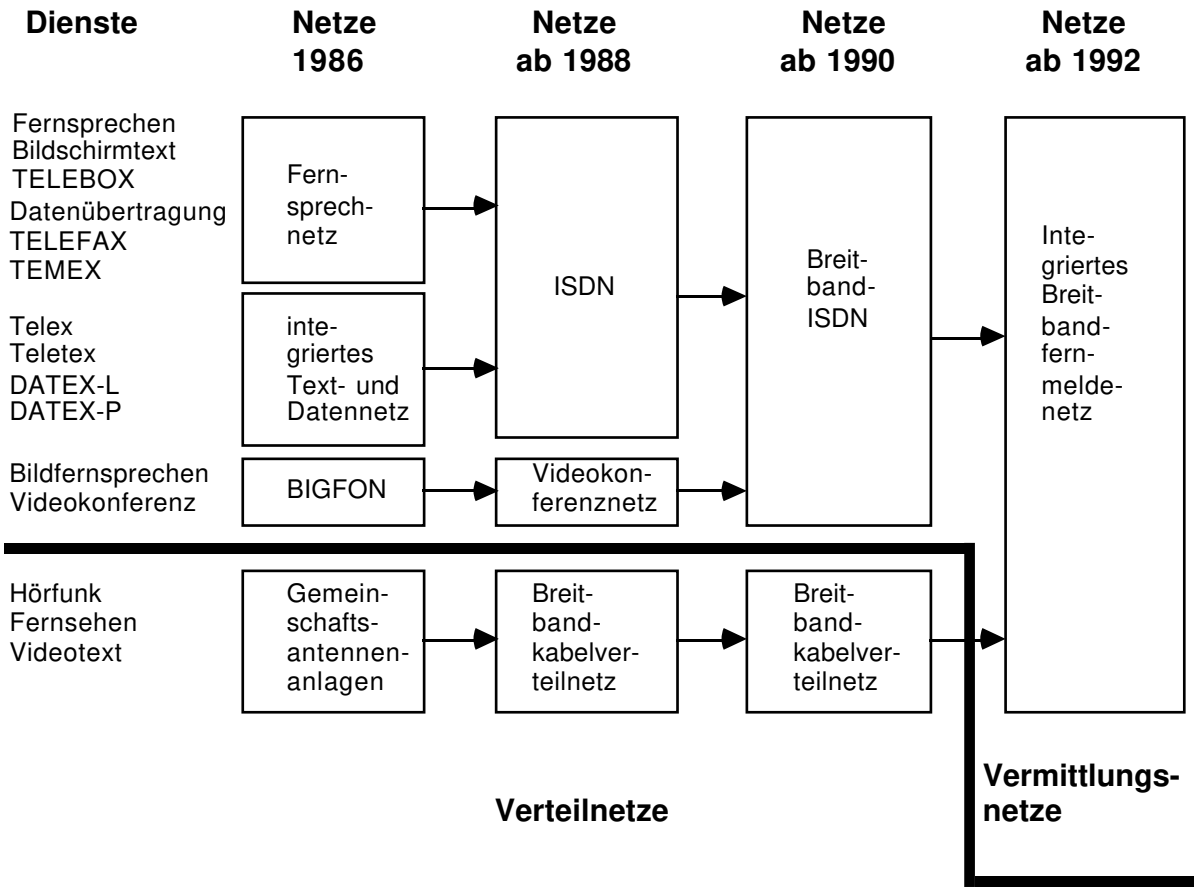


Abb. 1. Geplante Entwicklung der Netze der Deutschen Bundespost

1.2 Welche Beobachtungsmöglichkeiten bieten diese Netze?

Bei den geplanten wie bei allen Kommunikationsnetzen hat man sich zu fragen, wie gut ihre Teilnehmer vor Schaden geschützt sein werden. Die resultierenden Probleme lassen sich grob in zwei Kategorien einteilen:

Das **Sicherheitsproblem**: Ein Teilnehmer kann geschädigt werden, indem eine Diensterbringung für ihn verhindert, verzögert oder verändert wird oder indem eine Kommunikationsbeziehung unter seinem Namen oder auf seine Kosten, jedoch ohne sein Wissen oder seine Billigung aufgebaut wird.

Das **Datenschutzproblem**: Ein Teilnehmer kann auch dadurch, daß seine Kommunikation beobachtbar ist, Schaden erleiden.

Die zur Lösung des Sicherheitsproblems notwendigen Maßnahmen sind ausführlich in [VoKe_83] beschrieben und von denjenigen zur Lösung des Datenschutzproblems größtenteils unabhängig. Daher sollen sie im folgenden nicht weiter diskutiert werden. Es sei jedoch erwähnt, daß sie alle von einer digitalen Datenübermittlung ausgehen und damit z.B. auf dem heutigen analogen Telefonnetz nicht oder nur unter erheblichen Leistungseinbußen anwendbar sind.

Somit bleibt zunächst die Frage zu beantworten, welche Auswirkung die oben geschilderte Entwicklung der Netze der Deutschen Bundespost auf den Datenschutz haben wird.

In Abb. 2 ist die Endsituation dieser Entwicklung dargestellt: Alle Dienste, z.B. Fernsehen, Radio, Telefon, Bildschirmtext, werden über eine Glasfaser von der Vermittlungszentrale der Deutschen Bundespost zum Netzabschluß eines Teilnehmers vermittelt.

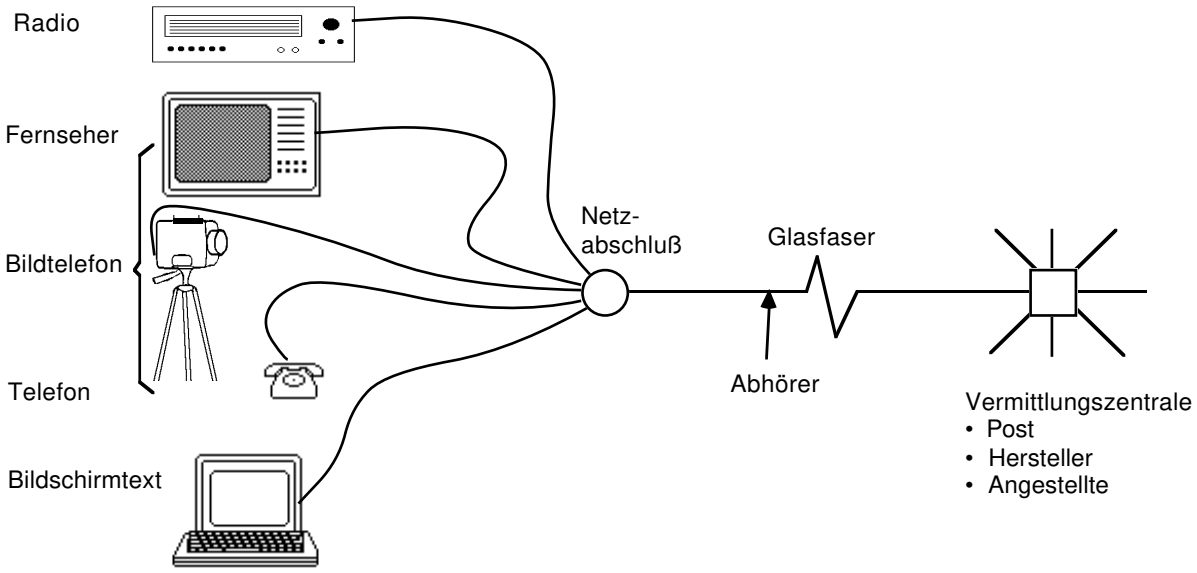


Abb. 2. Beobachtbarkeit des Benutzers im sternförmigen ISDN

Die Glasfaser ist diesem Teilnehmer (bzw. seiner Familie, seiner Firma o.ä.) eindeutig zugeordnet, und über sie wird, da es sich um ein Vermittlungsnetz handelt, nur übertragen, was von ihm oder speziell für ihn bestimmt ist. Folglich stellt die physikalische Netzadresse eine Art **Personenkennzeichen** (Kennzeichen für natürliche oder juristische Personen) dar, unter dem Daten über diesen Teilnehmer gesammelt werden können.

Die dafür auf der Glasfaser und in den Vermittlungszentralen anfallenden Informationen bestehen technisch gesehen aus

- den transportierten **Nutzdaten** (Bild, Ton, Text) und
- den **Vermittlungsdaten** (Adressen der Kommunikationspartner, Datenumfang, Dienstart, Zeit).

Die daraus zu gewinnenden personenbezogenen Daten des Teilnehmers kann man inhaltlich einteilen in:

- **Inhaltsdaten**, d.h. Inhalte vertraulicher (persönlicher oder geschäftlicher) Nachrichten, z.B. von Telefongesprächen oder elektronischer Post.
- **Interessensdaten**, d.h. Informationen über das Interesse des Teilnehmers an Nachrichten, deren Inhalt nicht vertraulich ist. Hierzu zählen die Beobachtungen, welche Zeitungsartikel sich der Teilnehmer schicken läßt, welche Auskünfte er aus Datenbanken, z.B. Bildschirmtext, einholt und was genau er im Fernsehen sieht bzw. im Radio hört:

  Will der Teilnehmer z.B. das Fernsehprogramm wechseln, teilt er dies über seinen Fernseher und seinen Netzabschluß der Vermittlungszentrale mit. Diese überträgt dann statt des bisher gesehenen das angeforderte Fernsehprogramm über die Glasfaser.

  Interessensdaten charakterisieren nicht nur natürliche Personen, sondern auch Firmen: Welche Fachaufsätze und Patente eine Firma anfordert, gibt z.B. ziemlich genaue Hinweise auf die von ihr gerade durchgeführten Forschungs- und Entwicklungsarbeiten.
  Interessensdaten waren bisher in Netzen überhaupt nicht zu gewinnen.
- **Verkehrsdaten**, also z.B. wann der Teilnehmer wie lange mit wem kommuniziert. Diese können aus den Vermittlungsdaten gewonnen werden. Daß auch sie sensitiv sein können, zeigt ein Beispiel: Fast täglich kommuniziert Teilnehmer A mit einem kommunistischen oder (der politischen Ausgewogenheit des Beispiels wegen) rechtsradikalen Zeitungsverlag ...

  Aber auch für einen Teilnehmer, der in dieser Hinsicht „nichts zu verbergen hat", ergeben die Verkehrsdaten bereits interessante Bausteine für ein Persönlichkeitsbild, z.B. Konsumgewohnheiten, Freundeskreis, Tagesablauf, Kontakte mit Polizei und Ärzten.

Verkehrsdaten können nicht nur Persönlichkeitsrechte natürlicher Personen, sondern auch Geschäftsinteressen juristischer Personen verletzen. Steigt z.B. das Verkehrsaufkommen zwischen zwei konkurrierenden Firmen sprungartig an, so legt dies Vermutungen über eine gemeinsame Produktentwicklung nahe.

Eine Möglichkeit, an diese Daten zu gelangen, ist das Abhören der Glasfaser. Glasfasern sind zwar etwas abhörsicherer als elektrische Leitungen, aber auch ihr Abhören stellt kein prinzipielles technisches Problem dar [Horg_85 Seite 36].

Noch einfacher und zudem für viele Teilnehmer auf einmal erhalten diejenigen die Daten, die sie sich direkt aus der Vermittlungszentrale beschaffen können.

Zunächst einmal kann die Post (und damit der Staat, genauer seine Geheimdienste) als Betreiber der Vermittlungsanlagen beliebig Daten speichern und auswerten lassen. Innerhalb weiter Grenzen darf sie dies auch, wie dem Bericht der Landesbeauftragten für den Datenschutz in Baden-Württemberg, Dr. Ruth Leuze, zu entnehmen ist [Leuz_83 Seite 114, vgl. auch Leuz_84 Seite 24, 25]:

„... der Betreiber von Bildschirmtext darf über jeden Teilnehmer speichern, wann, wie lange und wie oft er auf welche Weise den Bildschirmtext in Anspruch nahm."

Weiter können Personen (z.B. Postangestellte, Wartungstechniker) oder Organisationen (z.B. Hersteller), die Zugang zur Vermittlungszentrale haben oder hatten, alle dort erfaßbaren Informationen erhalten: Vermittlungszentralen sind heute komplexe Rechensysteme mit vielfältigen Möglichkeiten zum Installieren **„Trojanischer Pferde"** [Home_??], d.h. von Systemteilen, die Information auf verborgenen Kanälen einem nicht empfangsberechtigten Empfänger zukommen lassen [PoKl_78, Loep_85].

Ein solches „Trojanisches Pferd" kann dabei direkt installiert werden, z.B. während einer Wartungsmaßnahme, oder aber indirekt durch ein zur Entwicklung der Vermittlungszentrale verwendetes Werkzeug, das in jedes mit ihm entworfene Produkt ein „Trojanisches Pferd" einbaut [Thom_84, Pfit1_90].

Das Finden „Trojanischer Pferde" ist äußerst schwierig und, da eine diesbezügliche Systemüberprüfung auch nach jeder Wartungsmaßnahme nötig ist, sehr aufwendig. (Es sei angemerkt, daß bei Fernwartung der Betreiber der Anlage möglicherweise gar nicht erfährt, daß eine Wartungsmaßnahme stattfindet.)

Das Erschreckende ist, daß die Deutsche Bundespost anscheinend nicht einmal den Versuch unternehmen will, nach „Trojanischen Pferden" zu suchen, wie das folgende Beispiel der Bildschirmtextzentrale in Ulm zeigt:

Der Hersteller der Bildschirmtextzentrale muß den Systemaufbau der Deutschen Bundespost nicht offenlegen, was das Aufspüren „Trojanischer Pferde" vollends unmöglich macht. Der Bundesbeauftragte für den Datenschutz, Dr. Reinhold Baumann, schreibt darüber [BfD_85 Seite 25]:

„Wer Daten verarbeitet, muß die Wirkung der dafür eingesetzten Programme genau kennen. Deshalb hat es überrascht, daß der Deutschen Bundespost als Betreiber des Bildschirmtext-Systems keine umfassende Dokumentation aller eingesetzten Programme vorliegt. Zur Begründung dafür hat sie auf ihre vertraglichen Regelungen mit der Lieferfirma IBM hingewiesen. Dadurch ist es der Deutschen Bundespost verwehrt, sich genaue Kenntnis der Programme in allen Details ohne Hilfe Dritter zu verschaffen. Vor diesem Hintergrund erscheint schwer vorstellbar, wie die Deutsche Bundespost ihrer Verantwortung für die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme (§ 15 Nr. 2 BDSG) gerecht werden kann."

Da der Personenkreis, der an die im Netz, insbesondere in den Vermittlungszentralen, anfallenden Daten gelangen kann, so groß ist, wird es auch ausländischen Geheimdiensten möglich sein, die Daten zu erhalten.

Interessensdaten können außer durch Abhören der Glasfaser oder über die Vermittlungszentralen auch noch von großen Kommunikationspartnern, etwa Datenbanken oder Zeitungsverlagen, gesammelt werden, sofern diese die Identitäten der Dienstnutzer erfahren.

Zum Schluß kann man sich nun natürlich fragen, welche Beobachtungsmöglichkeiten ein **nicht diensteintegrierendes**, im Teilnehmeranschlußbereich **analoges rechnergesteuertes Vermittlungsnetz** bzw. das **heutige Telefonnetz** bietet:

- Auch bei Verzicht auf Diensteintegration kann bereits die Rechnersteuerung der Vermittlung allein zur effizienten Auswertung der Verkehrsdaten mißbraucht werden.
- Daher bietet ein analoger Anschluß an ein rechnergesteuert vermittelndes Fernsprechnetz sogar weniger Datenschutz als ein nur zum Fernsprechen genutzter digitaler ISDN-Anschluß, denn beider Verkehrsdaten sind gleichermaßen beobachtbar, der Besitzer eines analogen Anschlusses kann sich aber nur schwer gegen Abhören schützen, da die üblichen Maßnahmen zum Schutz der Inhaltsdaten (vgl. ausführlicher 1.4) eine digitale Übertragung voraussetzen.
- Letzteres gilt natürlich auch für das heutige Telefonnetz. Durch Weiterentwicklung der Sprecher- [DaPr_89 Seite 192f, 203f] und später auch der Spracherkennung [Wall_87] könnte dies selbst bei unveränderter Beibehaltung des heutigen Telefonnetzes innerhalb weniger Jahre zu einer automatisierten Überwachung der Inhaltsdaten vieler Teilnehmer (in der Art einer „Rasterabhörfahndung") mißbraucht werden.

1.3 Notwendigkeit vorbeugenden Datenschutzes als Gegenmaßnahme

Die von der Deutschen Bundespost geplante Struktur des ISDN und seiner breitbandigen Erweiterungen gestattet also eine effiziente Überwachung der Benutzer. Dies birgt einerseits die Gefahr der Massenüberwachung, bietet andererseits aber auch zusätzliche Möglichkeiten, einzelne verdächtige Teilnehmer abzuhören.

Daher sind die teilweise unterschiedlichen Interessen von Individuum und Staat gegeneinander abzuwägen.

1.3.1 Das Recht auf informationelle Selbstbestimmung

In der Begründung des Volkszählungsurteils vom Dezember 1983 leitete das Bundesverfassungsgericht aus den im Grundgesetz verankerten Grundrechten ein Recht auf informationelle Selbstbestimmung ab. Wörtlich heißt es dort [Bund_83 Seite 272]:

> *„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."*

Der im Urteil beschriebene Zustand, in dem sich die Bürger nicht sicher sind, ja nicht sicher sein können, ob sie überwacht werden oder nicht, ist nun aber genau der, der durch die Realisierung der Postpläne herbeigeführt wird, denn ein Bürger wird die Benutzung des ISDN und damit das Eingehen der Gefahr der Überwachung nur unter großen Nachteilen vermeiden können:

Da das ISDN z.B. das heutige Fernsprechen enthalten wird und seine rechnergesteuerten Vermittlungszentralen die bisher ausschließlich eingesetzten elektromechanischen Ortsvermittlungszentralen vollständig ersetzen sollen, wird jeder heutige Fernsprechteilnehmer, also fast jeder Haushalt, zwangsläufig zum Benutzer des ISDNs oder zumindest seiner rechnergesteuerten Vermittlungszentralen. Nehmen z.B. die Banken ihre Chance wahr und statten zahlreiche Läden mit POS-Terminals aus, so dürfte auch hier jeder Kaufwillige faktisch zur Benutzung neuer Bankdienste gezwungen werden (ähnlich wie heute der Besitz eines Giro-Kontos für Gehaltsempfänger fast zwingend ist oder wie in den USA teilweise nur noch mit Kreditkarten statt Bargeld bezahlt werden kann).

Damit ist die Planung der Deutschen Bundespost **verfassungsrechtlich** sehr bedenklich. Auf diese Situation kann man nun auf verschiedene Art reagieren:

Man könnte versuchen, das Datenschutzproblem zu umgehen, indem die Weiterentwicklung der Kommunikationsnetze, insbesondere die Errichtung diensteintegrierender Digitalnetze mit ihren gegen Angriffe anfälligen komplizierten Vermittlungszentralen, verhindert wird [Kubi_87, KuRo_86].

Sofern aber an den durch solche Netze ermöglichten neuen Diensten oder Qualitätsverbesserungen für schon existierende Dienste Interesse besteht, wird man ihre Einführung nicht verhindern können und wollen, zumal ein Beibehalten des im Teilnehmeranschlußbereich analogen Telefonnetzes innerhalb weniger Jahre ebenfalls zu unlösbaren Datenschutzproblemen führen kann (vgl. Schluß von 1.2).

Geht man also von der Existenz eines leistungsfähigen flächendeckenden offenen Digitalnetzes für die Zukunft aus, wie wir es im folgenden tun werden, so ist zumindest zu fordern, die für eine Überwachung notwendigen Handlungen gesetzlich zu verbieten (was zum Teil durch das Fernmeldegeheimnis bereits der Fall ist).

Aber ein Verbot ist nur dann wirkungsvoll, wenn seine Einhaltung mit angemessenem Aufwand **überprüft** und durch Strafverfolgung gesichert und der ursprüngliche Zustand durch Schadensersatz **wiederhergestellt** werden kann. Beides ist in der geschilderten Situation leider nicht gegeben:

„Datendiebstahl" allgemein, speziell das direkte Abhören von Leitungen oder Kopieren von Daten aus Vermittlungsrechnern, ist kaum feststellbar, da sich an den Originaldaten nichts ändert. Ebenso ist, wie oben erwähnt, das Installieren „Trojanischer Pferde" kaum festzustellen und erst recht nicht die unerlaubte Weiterverarbeitung von Daten, die man legal (oder auch illegal) erhalten hat. Dies bedeutet, daß auch dann, wenn die Post sich an der Durchsetzung des Gesetzes zu beteiligen versucht, nicht einmal entdeckt werden kann, wenn Angestellte, Hersteller von Vermittlungszentralen oder Datenbanken, die die Identitäten der Dienstnutzer erfahren, es übertreten.

Die Wiederherstellung des ursprünglichen Zustands müßte vor allem darin bestehen, alle entstandenen Daten zu löschen. Man ist aber nie sicher, ob nicht noch weitere Kopien existieren, da Datenträger großer Kapazität physisch sehr klein und spottbillig sind [Pfit1_90]. Außerdem können sich Daten im Gedächtnis von Menschen festsetzen, wo das Löschen besser nicht angestrebt werden sollte.

Da also **juristischer** Datenschutz alleine nicht genügt, bleibt nur die Möglichkeit zu untersuchen, ob durch **vorbeugende** (größtenteils **technische**) **Datenschutzmaßnahmen** das Erstellen von Persönlichkeitsprofilen verhindert werden kann. Dies bedeutet, daß man die Benutzung der Netze, die auf den Netzen angebotenen Dienste oder gar die Netze selbst soweit anders gestaltet, daß von vornherein im Netz keine Möglichkeit besteht, ohne explizite Einwilligung des Teilnehmers über ihn Daten zu erfassen.

1.3.2 Individualüberwachung im staatlichen Interesse

Ein oft gehörter Einwand gegen vorbeugende (und deshalb nicht unterlaufbare) technische Datenschutzmaßnahmen ist, daß sie gesellschaftlich nicht wünschenswert seien, da ein Interesse bestehe, bei begründetem Verdacht das Verhalten Einzelner beobachten zu können (G 10-Gesetz, § 100 StPO).

Hier kann man entgegnen, daß der technische Fortschritt auch auf anderen Gebieten als Kommunikationsnetzen eine Fülle neuer Überwachungstechniken hervorbringt:

- Immer kleinere und perfektere Abhörmikrofone [Horg_85 Seite 31] oder die Abtastung von Fensterscheiben mittels Laserstrahl durch mehrere hundert Meter entfernte Geräte [Hor2_85] erlauben die Wiedergabe aller Geräusche, z.B. aller Gespräche im Zimmer und am Telefon sowie des gewählten Fernseh- oder Radioprogramms.
- Alles auf Bildschirmen Angezeigte kann mit einem handelsüblichen Gerät im Wert von rund fünfzig US-Dollar über Entfernungen von 1000 m aufgefangen und auf einem Fernsehgerät dargestellt werden [Eck_85].
- Optische Überwachung ist durch immer bessere und billigere Kameras möglich (neben der klassischen Methode der persönlichen Verfolgung). In Zukunft erlauben vielleicht auch Aufklärungssatelliten nicht nur die Beobachtung militärischer Operationen, sondern auch die Erstellung von Bewegungsprofilen privater Bürger.

Dadurch ist eine umfassendere Überwachung weniger Einzelner möglich als durch die bisherige Telefonüberwachung. Gegen manche dieser Techniken gibt es Gegenmaßnahmen, z.B. sehr schmutzige Fensterscheiben gegen die Laserüberwachung oder Abschirmung von Terminals (Verfahren und Normen für letzteres sind unter den Kürzeln COMSEC und TEMPEST bekannt [Horg_85]). Da aber auch bisher niemand gezwungen war, am Telefon Belastendes von sich zu geben, ergibt sich nur dasselbe Problem wie mit der bisherigen Telefonüberwachung: Gerade diejenigen, die wirklich Gesetze übertreten, greifen vermutlich zu Schutzmaßnahmen (z.B. Steganographie, Kuriere, Funk), während jemand, der sich keines Unrechts bewußt ist, beobachtbar ist.

Die geplanten Kommunikationsnetze hingegen würden nicht nur eine viel umfassendere Beobachtung Einzelner, sondern auch ohne großen Aufwand das Beobachten der gesamten Bevölkerung ermöglichen, und zwar nicht nur durch den eigenen Staat (Geheimdienst), sondern auch durch Fernmeldefirmen, Systemprogrammierer, fremde Staaten (Geheimdienste) usw.

Dieser Aufwandsunterschied zwischen Beobachtung über diensteintegrierende Digitalnetze und anderen Überwachungstechniken beantwortet auch den umgekehrten Einwand, ob es sich überhaupt lohne, Daten in Netzen zu schützen, ohne gleichzeitig Gegenmaßnahmen gegen alle anderen Überwachungsmöglichkeiten anzugeben und zu ergreifen.

In entfernterer Zukunft könnten aber einige der anderen Überwachungsmöglichkeiten zu ebenso großen Datenschutzproblemen führen. Außerdem werden einige der Daten, die in Kommunikationsnetzen geschützt werden sollen, über Personalinformationssysteme, maschinenlesbare Personalausweise u.ä. ebenfalls in Rechenanlagen gelangen. Hier ergibt sich (wie bei den Vermittlungszentralen) das Problem, daß die Einhaltung von Datenschutzgesetzen und -vereinbarungen nicht mit vernünftigem Aufwand überprüfbar ist.

1.4 Was kann man durch Verschlüsselung erreichen?

Kommunikation wird technisch üblicherweise durch Verschlüsselung der Daten mittels eines Konzelationssystems gegen unbefugte Kenntnisnahme geschützt. Dieses soll garantieren, daß der Inhalt einer gesendeten Nachricht nur den Besitzern eines bestimmten Schlüssels zugänglich ist.

1.4.1 Konzelationssysteme und ihre Schlüsselverteilung

Hinsichtlich der erlaubten und möglichen Verteilungen dieser Schlüssel unterscheidet man zwischen **symmetrischen** und **asymmetrischen Konzelationssystemen**. Erstere werden oftmals auch konventionelle Kryptosysteme, letztere Kryptosysteme mit öffentlichen Schlüsseln genannt.

In einem symmetrischen Konzelationssystem (Abb. 3), wozu alle klassischen Konzelationssysteme gehören [Denn_82, DaPr_89, Hors_85], wird die Kommunikation zwischen zwei Partnern dadurch gesichert, daß beide einen gemeinsamen geheimen Schlüssel *k* (key) kennen, der sowohl zur Ver- als auch zur Entschlüsselung dient.

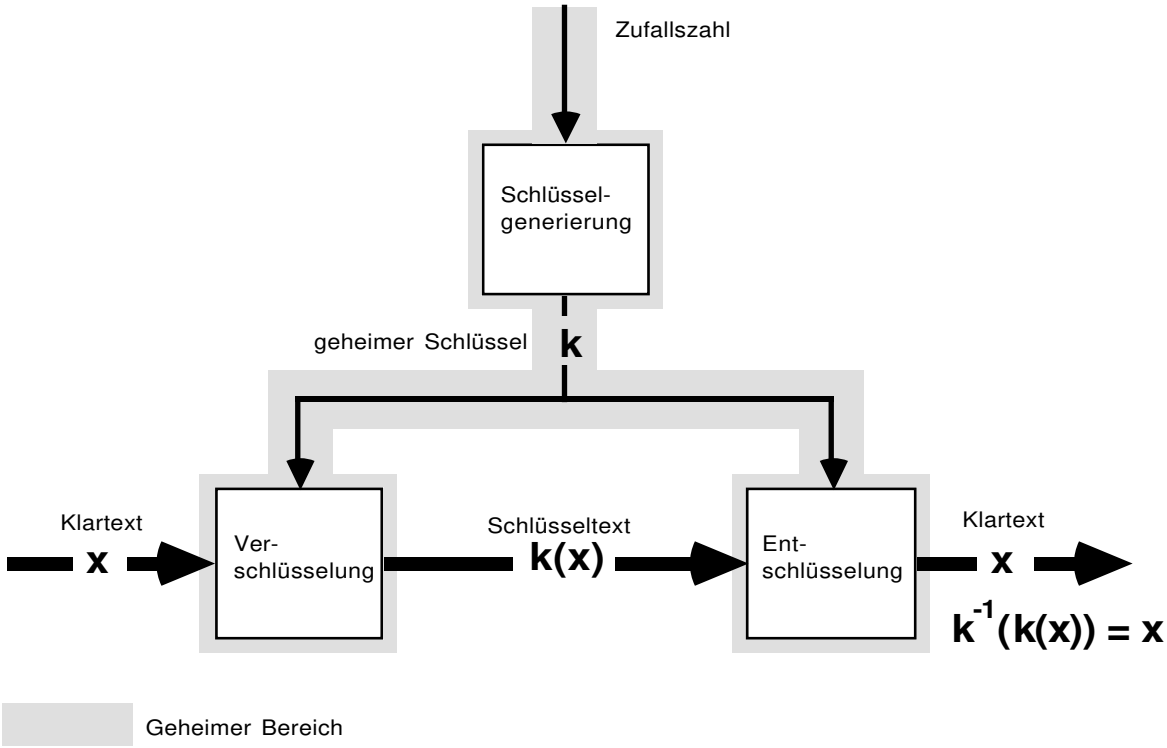


Abb. 3. Symmetrisches Konzelationssystem

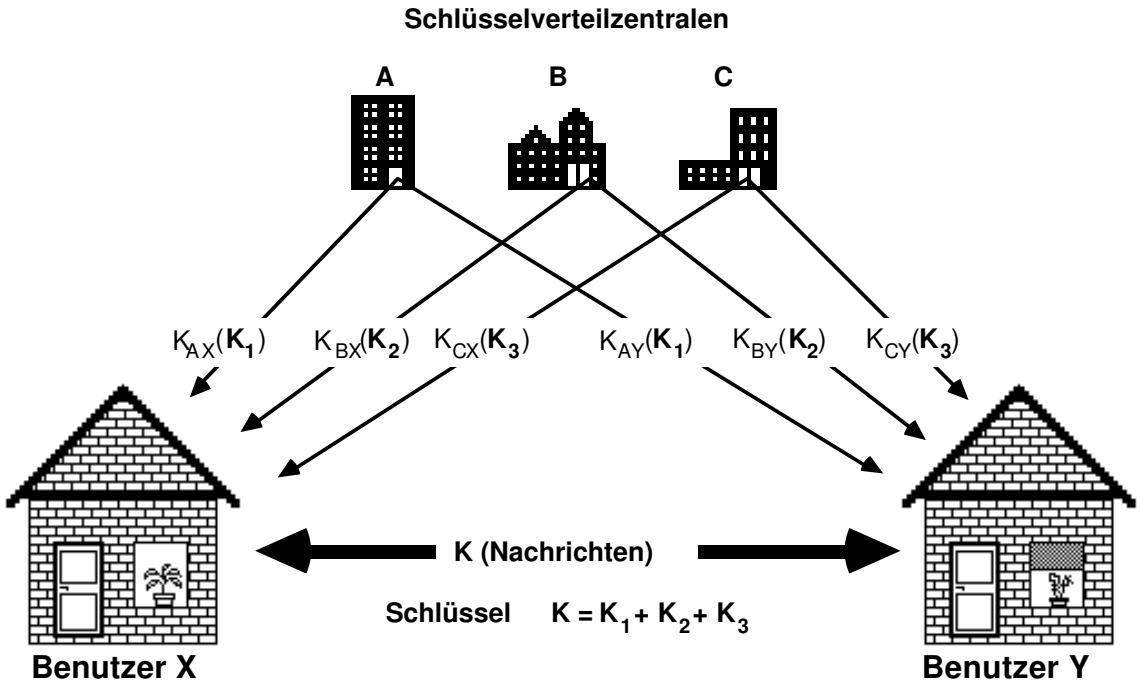


Abb. 4. Schlüsselverteilung mit mehreren Zentralen bei symmetrischem Konzelationssystem

Damit wird ein Schlüssel nicht einem bestimmten Teilnehmer, sondern einer bestimmten Kommunikationsbeziehung zugeordnet. Um eine Kommunikationsbeziehung gesichert beginnen zu können, müssen sich beide Partner zuvor auf einen gemeinsamen Schlüssel einigen. Bei offenen Netzen muß dies über das Netz selbst erfolgen können, da man nicht davon ausgehen kann, daß die Partner vorher schon in direktem Kontakt miteinander standen. Für dieses Schlüsselverteilproblem existieren im wesentlichen zwei Lösungsansätze.

Der klassische sieht die Verwendung einer Schlüsselverteilzentrale vor, mit der jeder Teilnehmer vor Beginn seiner Teilnahme am Netzgeschehen außerhalb des Netzes einen Schlüssel vereinbart hat. Auf Anfrage generiert sie einen Schlüssel für eine Kommunikationsbeziehung und teilt ihn den künftigen Kommunikationspartnern unter Verwendung der mit den jeweiligen Teilnehmern vereinbarten Schlüssel vertraulich und authentiziert mit [DaPr_89, NeSc_87, OtRe_87].

Da eine solche Zentrale durch Kenntnis aller verwendeten Schlüssel potentiell alle gesendeten Nachrichten entschlüsseln kann, ist aus Datenschutzgründen diese einfache Lösung zumindest für dienste-integrierende offene Netze nicht akzeptabel. Ein Ausweg ist die Verwendung vieler unabhängiger Schlüsselverteilzentralen, die je einen Schlüssel generieren und beiden Kommunikationspartnern mitteilen (Abb. 4). Die Kommunikationspartner verwenden als Schlüssel die Summe aller mitgeteilten Schlüssel, so daß alle Schlüsselverteilzentralen zusammenarbeiten müßten, um die Summe zu errechnen und die Kommunikation zu überwachen.

Der zweite Ansatz verwendet zur Schlüsselverteilung ein asymmetrisches Konzelationssystem, wie es unten beschrieben wird.

Das bekannteste moderne symmetrische Konzelationssystem ist DES (data encryption standard, [DaPr_89, DES_77, Hors_85]), das vom NBS (der amerikanischen Normungsbehörde für den öffentlichen Bereich) als Zwischenlösung (bis zur Normung eines besseren) definiert wurde. Seine Sicherheit ist zwar nicht bewiesen, es hat aber bis heute allen (bekanntgegebenen) Versuchen standgehalten, es zu brechen [BiSh_90, BiSh4_91]. Die schnellsten auf DES beruhenden, auf einem Chip implementierten Geräte verschlüsseln derzeit 20 Mbit/s [Abbr_84, AT&T_86, KaRS_85, Bras_88 § 3.4].

Mit dem bei DES verwendeten Prinzip lassen sich durch Änderung von Teilfunktionen und Verwendung längerer Schlüssel viele weitere gut implementierbare und ähnlich schnelle symmetrische Konzelationssysteme konstruieren, deren Sicherheit zwar auch nicht bewiesen, aber wesentlich weniger zweifelhaft ist als die von DES [Pfit_90, Aßma_89, PfAß_90]. Daneben gibt es auch ein symmetrisches System, dessen Sicherheit vollständig bewiesen wurde [Shan_49], das aber leider aufgrund seines hohen Schlüsselverteilaufwandes für die meisten Zwecke unpraktikabel ist, und Systeme, deren Sicherheit wie die der folgenden asymmetrischen Systeme relativ bewiesen wurde, deren Verschlüsselungsgeschwindigkeit aber dafür auch nicht höher ist als bei jenen [LuRa_86].

Die Idee der asymmetrischen Konzelationssysteme (Abb. 5) wurde erst 1976 veröffentlicht [DiHe_76] und löst das Schlüsselverteilungsproblem auf überraschend einfache Weise: Statt einen einzigen Schlüssel zum Ver- und Entschlüsseln zu verwenden, verteilt man diese Funktion auf zwei zusammengehörige Schlüssel c und d. Der Schlüssel d soll nur zum Entschlüsseln (dechiffrieren) dienen und muß natürlich geheimgehalten werden, weshalb er auch privater Schlüssel genannt wird. Der Schlüssel c hingegen soll nur das Verschlüsseln (chiffrieren), nicht jedoch das Entschlüsseln ermöglichen, weshalb er veröffentlicht werden kann und daher auch öffentlicher Schlüssel genannt wird. Insbesondere darf man also keine realistische Möglichkeit haben, ein unbekanntes d aus dem zugehörigen c herzuleiten.

Rein theoretisch könnte man d aus c natürlich immer durch Durchprobieren aller möglichen Schlüssel bestimmen, denn nur das richtige d entschlüsselt alle mit c verschlüsselten Nachrichten richtig. Es muß daher so viele Möglichkeiten geben, daß dies praktisch keinerlei Erfolg verspricht.

Außerdem müssen, damit niemand kurze Standardnachrichten erraten und mit dem öffentlichen Schlüssel testen kann, Klartexte jeweils sehr viele verschiedene mögliche Verschlüsselungen besitzen. Dies kann man erreichen, indem man die Nachrichten vor der Verschlüsselung mit zufällig gewählten Zeichenketten verlängert oder indem man ein bereits **indeterministisch** verschlüsselndes Konzelationssystem (probabilistic encryption, [GoMi_82, BlGo_85]) verwendet.

Einfacher als das Herleiten von d aus c muß hingegen das Generieren eines beliebigen Paares von zueinander passenden c und d sein, da dies der Schlüsselbesitzer am Anfang selbst durchführen muß.

Durch ein asymmetrisches Konzelationssystem entsteht die Möglichkeit, einen Schlüssel oder genauer ein Schlüsselpaar (c,d) statt einer Kommunikationsbeziehung einem einzelnen Benutzer zuzuordnen, der sich

zudem diesen Schlüssel selbst generieren kann. Möchte jemand mit diesem Benutzer gesichert kommunizieren, so muß er sich lediglich dessen öffentlichen Chiffrierschlüssel *c* besorgen. Dies kann entweder durch eine offene Anfrage an den gewünschten Benutzer geschehen, wodurch allerdings Authentikationsprobleme entstehen [Inge_84, RiSh_84], oder unter Verwendung zentraler, gegen Manipulation gesicherter Register (Abb. 6), deren Verwalter jetzt durch die Kenntnis der öffentlichen Schlüssel keine Möglichkeit zum Mithören verschlüsselter Nachrichten mehr erhalten.

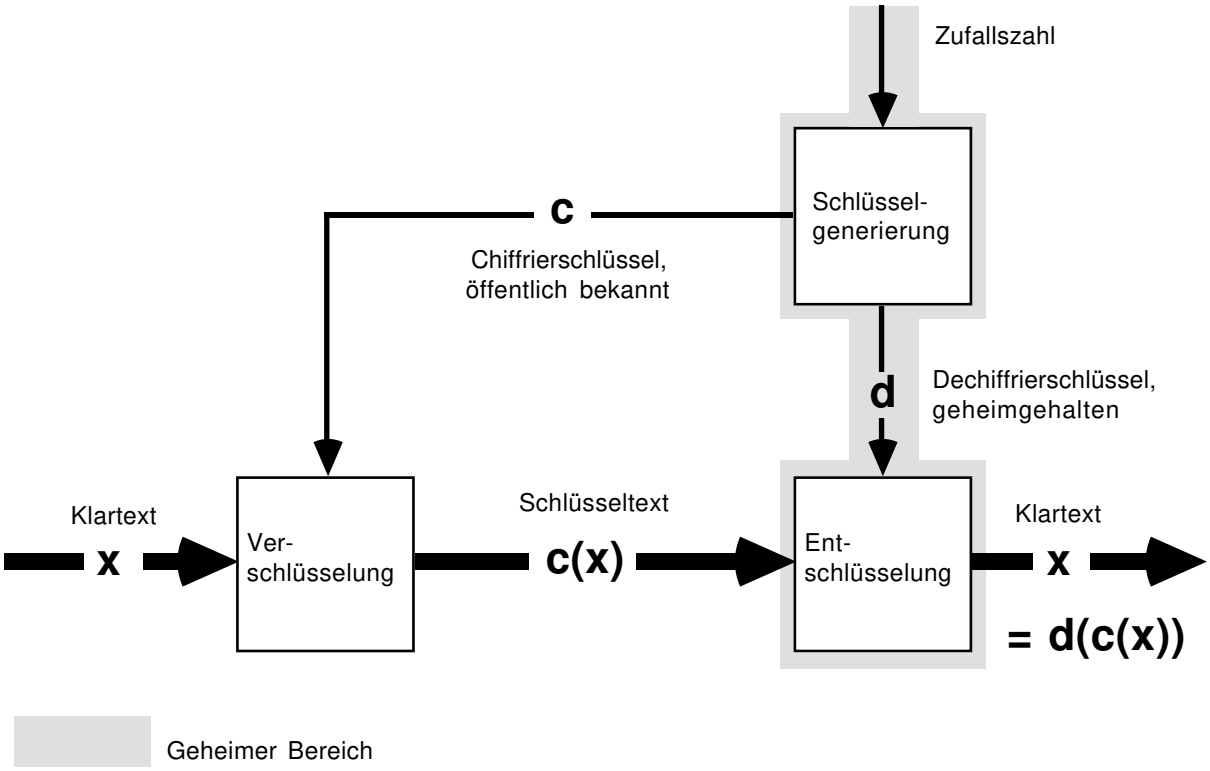


Abb. 5. Asymmetrisches Konzelationssystem

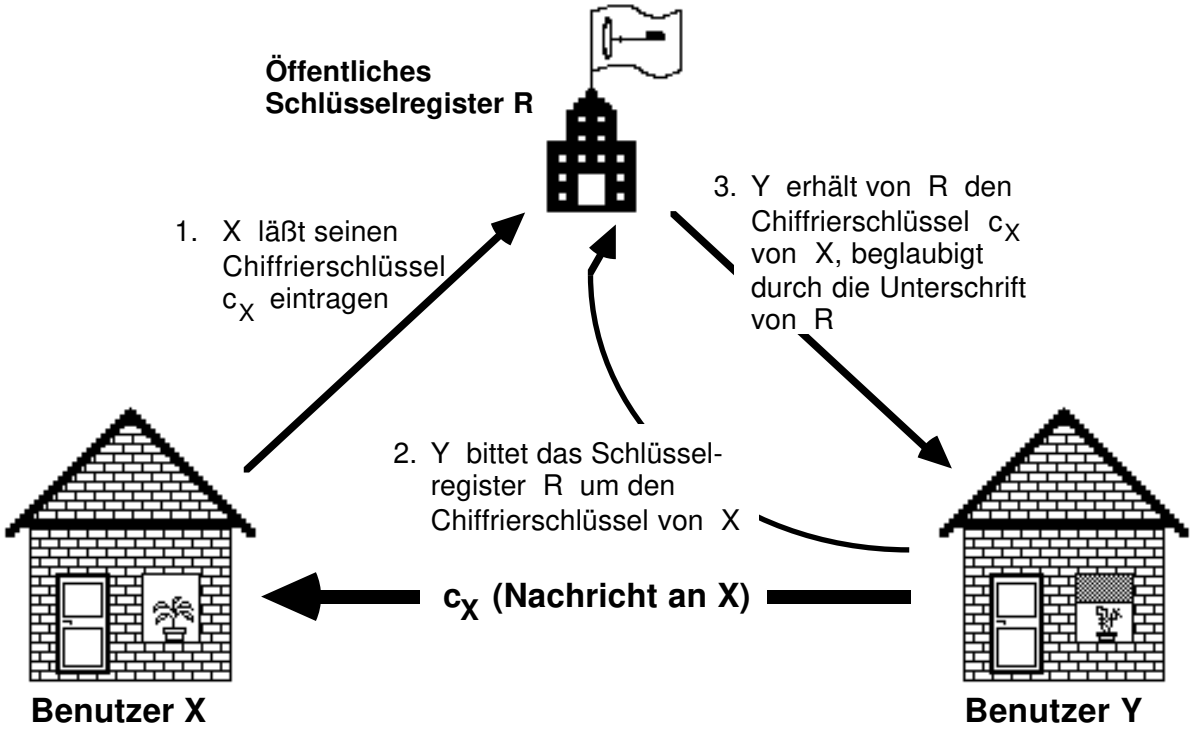


Abb. 6. Schlüsselverteilung bei asymmetrischem Konzelationssystem

1978 wurde mit RSA das erste und nach wie vor bekannteste asymmetrische Konzelationssystem (Ver- und Entschlüsselungsfunktion sowie Schlüsselgenerierungsfunktion entsprechend obigen Anforderungen) veröffentlicht [RSA_78, Denn_82, DaPr_89, Hors_85]. Seine Sicherheit beruht auf (teilweise unbewiesenen) Annahmen über den Lösungsaufwand zahlentheoretischer Probleme. Es wird allgemein vermutet, daß das Brechen von RSA, insbesondere das Ableiten des privaten aus dem öffentlichen Schlüssel, so schwer ist wie die Gewinnung der Primfaktoren einer gegebenen Zahl. Eine Faktorisierung beliebiger Zahlen, die aus sehr großen Primfaktoren zusammengesetzt sind, ist bisher, obwohl sich Mathematiker seit langer Zeit damit beschäftigen, praktisch unmöglich.

Die schnellste in der Forschungsliteratur angekündigte Implementierung von RSA erreicht 200 kbit/s bei einer (für die Sicherheit nötigen) Blocklänge von 660 bit [SeGo_86, Sedl_88].

Es sei angemerkt, daß es weniger bekannte asymmetrische Konzelationssysteme als RSA gibt, für die bewiesen wurde, daß selbst partielles Brechen für passive Angreifer so schwer wie Faktorisieren ist [BlGo_85]. Allerdings sind diese gegen aktive Angreifer unsicher. Ihre Verschlüsselungsgeschwindigkeit dürfte der von RSA ähneln. In [GoMT_82] ist ein in diesem Sinne vermutlich auch gegen aktive Angreifer sicheres, allerdings mehrphasiges Konzelationssystem beschrieben.

Leider gibt es zur Zeit weder praktikable symmetrische noch irgendwelche asymmetrischen Konzelationssysteme, deren Sicherheit ohne unbewiesene Annahmen über den Lösungsaufwand von Problemen bewiesen werden kann.

1.4.2 Verbindungs- und Ende-zu-Ende-Verschlüsselung

Für den Einsatz eines Konzelationssystems zum Schutz der Kommunikation hat man zwei Strategien zur Auswahl, die zwar beide sinnvoll sind, aber leider nicht sämtliche Probleme lösen:

Die erste Strategie besteht darin, alle Daten jeweils zwischen benachbarten Netzknoten, d.h. Teilnehmerstationen oder Vermittlungszentralen, zu verschlüsseln (**Verbindungs-Verschlüsselung**, link-by-link encryption). Dadurch erhält man durch das Abhören der Glasfaser keine Information mehr. Die Nachteile sind:

- In den Vermittlungszentralen liegen alle Daten unverschlüsselt vor, von allen oben genannten möglichen Angreifern werden also nur diejenigen ausgeschlossen, die die Glasfaser abhören.

  (Wir verwenden „**Angreifer**" als kurze Bezeichnung für jemanden, der versucht, sensitive Daten ohne Einwilligung der Betroffenen zu sammeln.)

- Auf der Glasfaser sollen mindestens 560 Mbit/s übertragen werden. Dies ist eher oberhalb dessen, was heute mit Kryptogeräten, die auf einem für halbwegs sicher gehaltenen Konzelationssystem beruhen und halbwegs preiswert sind, verschlüsselt werden kann (vgl. 1.4.1). Es wäre zumindest von Vorteil, wenn man Fernsehen als breitbandigen Dienst, bei dem es nicht um den Schutz von Inhalts-, sondern von Interessensdaten geht, nicht verschlüsseln müßte.

Die zweite Strategie ist, die Daten zwischen Teilnehmerstationen verschlüsselt zu übertragen (**Ende-zu-Ende-Verschlüsselung**, end-to-end encryption), damit sie in der Vermittlungszentrale nicht interpretiert werden können. Die Nachteile hiervon sind:

- Durch Ende-zu-Ende-Verschlüsselung können nur die Nutzdaten, nicht die Vermittlungsdaten geschützt werden. Verkehrsdaten (vgl. 1.2) lassen sich also weiterhin gewinnen.

- Vor jemandem, der die Nutzdaten schon vorher kannte und nun die Vermittlungsdaten erhält, sind damit auch die Interessensdaten (vgl. 1.2) ungeschützt.

  Insbesondere kann dieses Verfahren also nicht als Schutz vor der Post und anderen, die Zugriff auf Postrechner haben, dienen, wenn diese gleichzeitig Kommunikationspartner sind oder wenn sich die Nutzdaten in Form einer Datenbank in einem Postrechner (z.B. Bildschirmtext-Zentrale in Ulm) befinden. Die Nutzdaten können zwar in verschlüsselter Form in der Datenbank abge-

speichert werden, dies nützt jedoch nur etwas, wenn der Angreifer (Post bzw. andere mit Zugriff auf Postrechner) die zugehörigen Schlüssel nicht kennt und auch nicht in Erfahrung bringen kann. Letzteres erscheint außer bei kleinen geschlossenen Benutzergruppen unrealistisch, da der Angreifer in große geschlossene Benutzergruppen einen Strohmann einschleusen und bei offenen Benutzergruppen als normaler Nutzdateninteressent auftreten kann.

Daneben ist auch eine Zusammenarbeit von jemandem, der an Daten in der Vermittlungszentrale gelangen kann, und dem Kommunikationspartner denkbar. Dies könnte z.B. vom Geheimdienst ausgehen, der über die Post die Vermittlungsdaten erhält und Kommunikationspartner, z.B. Datenbanken, Zeitungsverlage, veranlaßt, ihm die Nutzdaten offenzulegen, aber auch vom Kommunikationspartner, der über Angestellte o.ä. Zugang zu den Vermittlungsdaten erhält.
Außerdem ist es trivialerweise sinnlos, sich mit Ende-zu-Ende-Verschlüsselung vor Kommunikationspartnern schützen zu wollen.

- Wie bei Verbindungs-Verschlüsselung ist es auch hier recht umständlich, auch Fernsehen verschlüsseln zu müssen, um die Interessensdaten vor den Angreifern in den Vermittlungszentralen zu schützen.

1.5 Was bleibt zu tun?

Durch Ende-zu-Ende-Verschlüsselung, wie in 1.4 beschrieben, können die Inhaltsdaten der Teilnehmer in beliebigen Netzen effizient geschützt werden.

Auch der Einsatz von Verschlüsselung erlaubt jedoch auf der heute üblichen und von der Deutschen Bundespost auch für die Zukunft geplanten Netzstruktur keinen ausreichenden und mit vernünftigem Aufwand **überprüfbaren** Datenschutz für Verkehrs- und Interessensdaten vor vielen möglichen Angreifern in den Vermittlungszentralen und Kommunikationspartnern.

In den folgenden Kapiteln wird untersucht, wie der noch fehlende Schutz durch andere Maßnahmen erreicht werden kann. Dabei muß darauf geachtet werden, daß nicht jemand, der bisher als möglicher Angreifer gar nicht auftrat, z.B. Nachbarn, plötzlich Beobachtungsmöglichkeiten erhält.

Technisch gesehen ist das Hauptziel, die Verkehrsdaten vor dem Betreiber der Vermittlungseinrichtungen zu schützen und sich auch gegenüber dem Kommunikationspartner nicht identifizieren zu müssen. Damit sind Verkehrs- und Interessensdaten nicht nur vor diesen geschützt, sondern (und das ohne zusätzliche Verschlüsselung von nicht personenbezogenen Nutzdaten wie Fernsehen) erst recht vor anderen Angreifern in den Vermittlungseinrichtungen oder Abhörern, da alle diese höchstens genausoviel Information erhalten können wie der Betreiber selbst.

In Kapitel 2 werden Grundverfahren hierzu mit einigen Überlegungen zu ihrer Implementierung dargestellt, und in Kapitel 3 wird untersucht, wie diese Verfahren für eine praktische Anwendung in öffentlichen Kommunikationsnetzen ergänzt werden müssen. Kapitel 4 enthält einige Bemerkungen über die Verwendung eines Datenschutz garantierenden Netzes.

Zum Schutz der Inhaltsdaten muß dabei zusätzlich Ende-zu-Ende-Verschlüsselung für sensitive Nutzdaten verwendet werden. Außerdem wird Kryptographie auch ein wichtiges Hilfsmittel der im folgenden zu untersuchenden Maßnahmen zum Schutz der Verkehrsdaten sein. Aus Leistungsgründen muß somit zumindest ein in Hardware implementiertes symmetrisches Konzelationssystem allen Teilnehmern zur Verfügung stehen.

Daher darf, obwohl dies ein eher politisches als wissenschaftliches Problem ist, nicht unerwähnt bleiben, daß eine **Normung** zumindest eines guten symmetrischen Konzelationssystems (und aus anderen Gründen auch anderer Kryptosysteme) dringend notwendig ist, soll das Kommunikationsnetz offen für alle Bürger sein. Andernfalls ist Datenschutz (ebenso wie Datensicherheit) nur innerhalb geschlossener Benutzergruppen, die sich jeweils auf ein Konzelationssystem geeinigt haben, erreichbar.

Dies ist zwar ein altbekanntes, aber dennoch ungelöstes organisatorisches Problem: International und national wurde zwar versucht, RSA und DES zu normen, doch wurden diese Versuche abgebrochen.

Diese Situation wurde zumindest in den USA von der den Geheimdiensten nahestehenden National Security Agency (NSA) dazu ausgenutzt, zu versuchen, auch in nichtstaatlichen und nichtmilitärischen Bereichen indirekt vorzuschreiben, welche Kryptosysteme verwendet werden. Zum Einsatz kommen sollten dabei von der NSA selbst entwickelte Kryptosysteme, deren genaue Beschreibung aber geheimgehalten werden sollte und deren Güte damit mehr als fraglich gewesen wäre, ganz abgesehen von politischen Bedenken, einen „Großen Bruder" zu installieren [WaPP_87]. Ende 1987 ist die Verantwortung zur Standardisierung von Kryptosystemen allerdings zurück an das NBS, inzwischen in NIST umbenannt, übertragen worden [CACM6_87]. Allerdings gibt es inzwischen eine Gesetzesvorlage, die die Hersteller von Kryptogeräten und -systemen verpflichten würde, eine Möglichkeit zum Brechen einzubauen [Agne_91].

Es ist zu hoffen, daß im Fall des fortdauernden Mangels an Normen wenigstens die Deutsche Bundespost geeignete, öffentlich validierte Kryptosysteme für ihre Kommunikationsnetze standardisieren wird.

2 Grundverfahren zum Schutz der Verkehrsdaten

In diesem Kapitel werden grundlegende Verfahren zum Schutz von Verkehrs- und Interessensdaten vor Angreifern in Vermittlungszentralen und Kommunikationspartnern dargelegt.

Zunächst werden Schutzmaßnahmen dargestellt, die **außerhalb** des Netzes angesiedelt sind, d.h. die jeder Benutzer für sich trifft. Diese werden sich als nicht ausreichend erweisen.

Danach werden solche Schutzmaßnahmen dargestellt, die **innerhalb** des Netzes angesiedelt sind, d.h. die Benutzung des Netzes nicht verändern, jedoch den Transport innerhalb des Netzes. Dabei werden auch Erweiterungen zum Schalten von Kanälen und zur Fehlertoleranz erwähnt.

2.1 Schutz außerhalb des Netzes

Bei Schutzmaßnahmen außerhalb des Netzes sind Ziel- und Herkunftsadresse einer Nachricht weiterhin im Netz als Vermittlungsdaten sichtbar. Dazu sind natürlich die Zeit, zu der eine Nachricht im Netz ist, und zumindest für den Kommunikationspartner die Nutzdaten sichtbar. Man muß verhindern, daß daraus Schlüsse auf Verkehrs- und Interessensdaten gezogen werden können.

2.1.1 Öffentliche Anschlüsse

Herkunftsadresse und **Zieladresse** einer Nachricht werden weitgehend bedeutungslos, wenn man verschiedene öffentliche Anschlüsse benutzt, z.B. Telefonzellen. Dies gilt natürlich nur, wenn man sich nicht zu Zwecken der Zugangskontrolle oder der Zahlung von Gebühren identifizieren muß, d.h. anonym bleibt.

Die Anwendung und Wirkung dieser Maßnahme ist stark eingeschränkt: Wer etwa will in (Bild-) Telefonzellen fernsehen?

2.1.2 Zeitlich entkoppelte Verarbeitung

Die **Zeit**, zu der sich eine Nachricht im Netz befindet, wird weitgehend bedeutungslos, wenn man Teilnehmerstationen (z.B. Personal Computer) Informationen nicht erst dann anfordern läßt, wenn der Teilnehmer sie benötigt, sondern zu einem beliebigen Zeitpunkt vorher:

> *Will man eine Zeitung lesen, so kann die Teilnehmerstation sie bereits zum Erscheinungszeitpunkt oder einem Zeitpunkt mit besonders geringen Übertragungskosten (z.B. Nachttarif) anfordern und zum späteren Lesen abspeichern.*

Diese Schutzmaßnahme verhindert, daß der Netzbetreiber allein aus dem Vermittlungsdatum „Zeit" und Kontextwissen schließen kann, wer mit wem kommuniziert:

Wenn tagsüber eine Zeitung angefordert wird und 10 Leute als Anforderer in Frage kommen, von denen bekanntlich 9 in Tag- und einer in Nachtschicht arbeiten, wäre ohne zeitliche Entkopplung klar, daß sie der Nachtarbeiter liest.

Kann der Netzbetreiber auf andere Art erkennen, wer mit wem kommuniziert, so erschwert diese Maßnahme doch zumindest das Erstellen von Persönlichkeitsbildern über den Tagesablauf.

Natürlich greift diese Maßnahme nicht bei Kommunikationsformen mit Realzeitanforderungen.

2.1.3 Lokale Auswahl

Um Interessensdaten zu schützen, kann man Information in großen Einheiten anfordern und lokal auswählen (lassen), was einen wirklich interessiert:

Bestellt man sich statt eines bestimmten Zeitungsartikels mehrere Zeitungen verschiedener politischer Richtungen, so können aus der Bestellung keinerlei Rückschlüsse auf die Interessen und Meinungen des Bestellers gezogen werden. Zusätzlich ließe sich durch „intelligente" Teilnehmerstationen die Dienstleistung sogenannter Ausschnittbüros, die einem Kunden auf Wunsch zu einem bestimmten Thema Artikel aus mehreren Zeitungen zusammenstellen, jedem Teilnehmer bieten.

Durch die lokale Auswahl verschleiert man selbst gegenüber dem Kommunikationspartner, was einen wirklich interessiert.

Das Anfordern von großen Informationseinheiten vom Kommunikationspartner ist folglich als Schutz bei solchen Informationsarten sinnvoll, die unverschlüsselt übertragen werden oder bei denen Netzbetreiber und Kommunikationspartner identisch sind oder als zusammenarbeitend angenommen werden können.

In zukünftigen Netzen, in denen (zumindest für schmalbandiges Senden) reichlich Bandbreite zur Verfügung steht, verursacht diese Maßnahme bei Diensten, bei denen der Benutzer nur bereits bereitgestellte Information abruft, real beinahe keine Kosten. Es ist jedoch eine Frage des Abrechnungsmodus, ob dies auch dem Anwender dieser Maßnahme zugutekommt.

2.2 Schutz innerhalb des Netzes

Im Gegensatz zu den obengenannten Schutzmaßnahmen sollen in diesem Kapitel Maßnahmen vorgestellt werden, die die im Netz anfallenden Vermittlungsdaten selbst verringern.

Dadurch sollen – ohne die Netzbenutzung für den Teilnehmer zu ändern oder gar komplizierter zu machen, aber unter Beibehaltung der Möglichkeit, den erhaltenen Datenschutz selbst nachzuprüfen – Senden und Empfangen, zumindest aber die Kommunikationsbeziehungen zwischen Teilnehmern, vor möglichen Angreifern (bösen Nachbarn, dem Netzbetreiber, großen Organisationen und Konzernen usw.) verborgen werden, so daß das Erfassen von Verkehrs- oder Interessensdaten unmöglich wird.

Da Schutz vor einem allmächtigen Angreifer, der alle Leitungen, alle Vermittlungszentralen, alle Teilnehmerstationen außer der eigenen und den Kommunikationspartner kontrolliert, nicht möglich ist, sind alle folgenden Maßnahmen nur Annäherungen an den perfekten Schutz der Teilnehmer vor jedem möglichen Angreifer. Die Annäherung wird im allgemeinen durch Angabe des unterstellten **Angreifermodells** (Was wird von ihm kontrolliert; wie stark ist er maximal?) beschrieben.

Verbirgt ein Kommunikationsnetz Senden und Empfangen oder zumindest die Kommunikationsbeziehung vor dem unterstellten Angreifer, so nennen wir es **anonym** und sprechen dann von anonymer Kommunikation.

2.2.1 Schutz des Empfängers

Der Empfänger einer Information ist vor *passiven* Angreifern in perfekter Weise geschützt, wenn das Netz alle Informationen an alle Teilnehmer sendet (**Verteilung**, broadcast).

Dies verhindert jedoch nicht, daß ein *aktiver* Angreifer, der die Konsistenz der Verteilung der Information stört, den Empfänger zumindest teilweise identifizieren kann [Waid_90, WaPf_89]:

Hierzu nehme man an, daß der aktive Angreifer eine Nachricht *N* konstruieren kann, auf deren Erhalt die zu identifizierende (und z.B. unter einer impliziten Adresse, siehe unten, bekannte) Teilnehmerstation innerhalb einer gewissen Zeit antworten wird. Da die meisten Protokolle zumindest eine Quittung des Empfängers vorsehen, ist diese Annahme sicher sinnvoll. Der Angreifer sendet nun *N* und sorgt dafür, daß genau eine Teilnehmerstation *N* erhält. Erhält er eine Antwort, so war der Empfänger eben diese Teilnehmerstation. Kann der Angreifer seinen Angriff genügend oft wiederholen, so kann er den Empfänger stets vollständig identifizieren.

Kann der Angreifer den Empfänger mehrmals zum Senden einer Antwort veranlassen, so kann er ihn sogar wesentlich effizienter vollständig identifizieren: Statt durch lineare kann der Angreifer den Empfänger durch logarithmische Suche bestimmen. Hierzu erhält nur die „erste“ Hälfte aller Teilnehmerstationen *N*, die „zweite“ wird von der Verteilung ausgeschlossen. Erhält der Angreifer eine Antwort, so weiß er, daß der Empfänger sich in der ersten, ansonsten, daß er sich in der zweiten Hälfte befand. Iterativ kann er den Angriff nun immer auf die Menge der Teilnehmerstationen anwenden, in der sich der Empfänger befinden muß, bis diese Menge nach logarithmisch vielen Schritten nur noch ein einziges Element enthält.

Diese Angriffsart kann entweder durch analoge oder digitale Maßnahmen vereitelt werden.

Eine *analoge Maßnahme* könnte in der Verwendung eines Mediums bestehen, daß *Konsistenz der Verteilung garantiert*. Häufig wird *Funknetzen* diese Eigenschaft zugeschrieben. Da solche Eigenschaften schwer nachgewiesen werden können und Funknetze anfällig für Angriffe auf die Diensterbringung sowie in der verfügbaren Bandbreite beschränkt sind und da das elektromagnetische Spektrum im wesentlichen nur einmal genutzt werden kann, ist es wichtig, digitale Maßnahmen zur Verfügung zu haben.

Digitale Maßnahmen können inkonsistente Verteilung natürlich nur *erkennen*, nicht aber verhindern, denn ein sehr mächtiger Angreifer kann die Signalausbreitung zu einzelnen Teilnehmerstationen immer unterbrechen (z. B. durch Errichten Faradayscher Käfige oder – meist einfacher – Durchtrennen von Leitungen oder Beschädigen der Funkantenne). Die Erkennung inkonsistenter Verteilung kann entweder *kryptographisch* realisiert werden, indem Nachrichten mit Sequenznummern, Uhrzeit etc. versehen und von einer als bezüglich eines Angriffes auf die Verteilung als nichtkooperierend angenommenen Gruppe von Stationen digital unterschrieben werden [WaPf_89, PfPW_89], oder sie kann *informationstheoretisch* erreicht werden, indem das in Abschnitt 2.2.3.1 beschriebene überlagernde Senden durch geeignetes Einbeziehen der verteilten Nachrichten in die dortige Schlüsselgenerierung erweitert wird [Waid_90, LuPW_91].

Ist der Angreifer jedoch nicht in der Lage, die Kommunikation zwischen nicht angreifenden Teilnehmern zu verhindern, so gibt es Verfahren, die die Konsistenz der Verteilung sicherstellen (**Byzantinische Übereinstimmung**, [PeSL_80, Reis_87, WaPf_89, PfWa1_91]).

Will man Verteilung auch bei bisher vermittelten Diensten verwenden, so muß jede Teilnehmerstation anhand eines Merkmals (**implizite Adresse**) entscheiden können, welche Nachrichten wirklich für sie bestimmt sind.

Kann eine Adresse nur vom Empfänger ausgewertet werden, so spricht man von **verdeckter** Adressierung. Kann eine Adresse von jedem ausgewertet, d.h. auf Gleichheit mit anderen Adressen getestet werden, so nennt man dies **offene** Adressierung [Waid_85].

Die übliche Implementierung von verdeckter Adressierung verwendet Redundanz innerhalb des Nachrichteninhalts und ein asymmetrisches Konzelationssystem: Jede Nachricht wird mit dem öffentlichen Schlüssel des adressierten Teilnehmers verschlüsselt (wodurch gleichzeitig Ende-zu-Ende-verschlüsselt

wird). Nach der Entschlüsselung mit dem zugehörigen privaten Schlüssel kann die Teilnehmerstation des adressierten Teilnehmers anhand der Redundanz feststellen, daß die Nachricht für sie bestimmt ist. Da die Implementierungen asymmetrischer Konzelationssysteme langsam sind (vgl. 1.4.1) und jede Teilnehmerstation alle Nachrichten entschlüsseln muß, ist dieses Verfahren im allgemeinen viel zu aufwendig. Es kann durch Austausch eines geheimen Schlüssels und Verwendung eines schnelleren symmetrischen Konzelationssystems (statt eines asymmetrischen) nach Aufnahme der Kommunikationsbeziehung jedoch etwas effizienter gestaltet werden.

Offene Adressierung läßt sich einfacher realisieren, indem man z.B. Nachrichten mit einem Adreßfeld versieht und die Teilnehmer(stationen) beliebige Zahlen als Adressen erzeugen. Eine Teilnehmerstation muß dann nur bei allen erhaltenen Nachrichten dieses Adreßfeld mit ihren Adressen vergleichen.

Hinsichtlich der Adreßverwaltung kann man bei beiden Formen der impliziten Adressierung **öffentliche** und **private** Adressen unterscheiden: Öffentliche Adressen stehen in allgemein zugänglichen Adreßverzeichnissen (z.B. in einem „Telefonbuch") und dienen meist einer ersten Kontaktaufnahme. Private Adressen werden an einzelne Kommunikationspartner gegeben. Dies kann entweder außerhalb des Netzes oder innerhalb als Absenderangabe in Nachrichten geschehen.

Bei offener Adressierung, im Gegensatz zur verdeckten, kann das Netz Informationen über die Empfänger von Nachrichten gewinnen. Dies kann bei Verwendung privater Adressen geschehen, wenn man dieselbe Adresse mehrfach verwendet, weil dann erkennbar wird, daß diese Nachrichten an denselben Empfänger gerichtet sind. Die mehrmalige Verwendung muß also durch fortlaufendes Generieren und Mitübertragen oder durch Vereinbarung eines Generieralgorithmus (Pseudozufallszahlengenerator) vermieden werden. Bei Verwendung öffentlicher offener Adressen kann sogar festgestellt werden, unter welcher Bezeichnung der Empfänger im Adreßverzeichnis eingetragen ist. Die Verwendung solcher Adressen sollte also möglichst vermieden werden.

Die Datenschutz- und Aufwandseigenschaften der Kombinationen von Adressierungsart und Adreßverwaltung sind in Abb. 7 zusammengefaßt.

			Adreßverwaltung	
			öffentliche Adresse	private Adresse
Adressierungsart	implizite Adresse	verdeckt	sehr aufwendig, für Kontaktaufnahme nötig	aufwendig
		offen	abzuraten	nach Kontaktaufnahme ständig wechseln
	explizite Adresse		sehr abzuraten	sehr abzuraten

Abb. 7. Bewertung der Kombinationen von Adressierungsart und Adreßverwaltung

2.2.2 Schutz der Kommunikationsbeziehung

Statt außer dem Empfänger auch den Sender verborgen zu halten, kann man zunächst versuchen, nur deren Verbindung geheimzuhalten und so die Anonymität der Kommunikation herzustellen.

Diese Idee wird durch das Verfahren der **umcodierenden MIXe** verwirklicht [Chau_81].

Bei diesem von David Chaum 1981 für elektronische Post vorgeschlagenen Verfahren werden Nachrichten nicht notwendigerweise auf dem kürzesten Weg zum Empfänger geschickt, sondern über mehrere möglichst unabhängige, umcodierende und umsortierende Zwischenstationen, sogenannte MIXe, geleitet. Der Absender einer Nachricht verschlüsselt sie so mit Schlüsseln eines asymmetrischen Konzelationssystems, daß sie nacheinander von der von ihm gewählten Folge von MIXen mit deren zugehörigen privaten Schlüsseln entschlüsselt werden muß. Dadurch ändert sich das Erscheinungsbild der Nachricht auf jedem Stück ihres Weges, so daß ihr Weg (außer wenn alle MIXe, die sie durchläuft, zusammenarbeiten) nicht verfolgt werden kann.

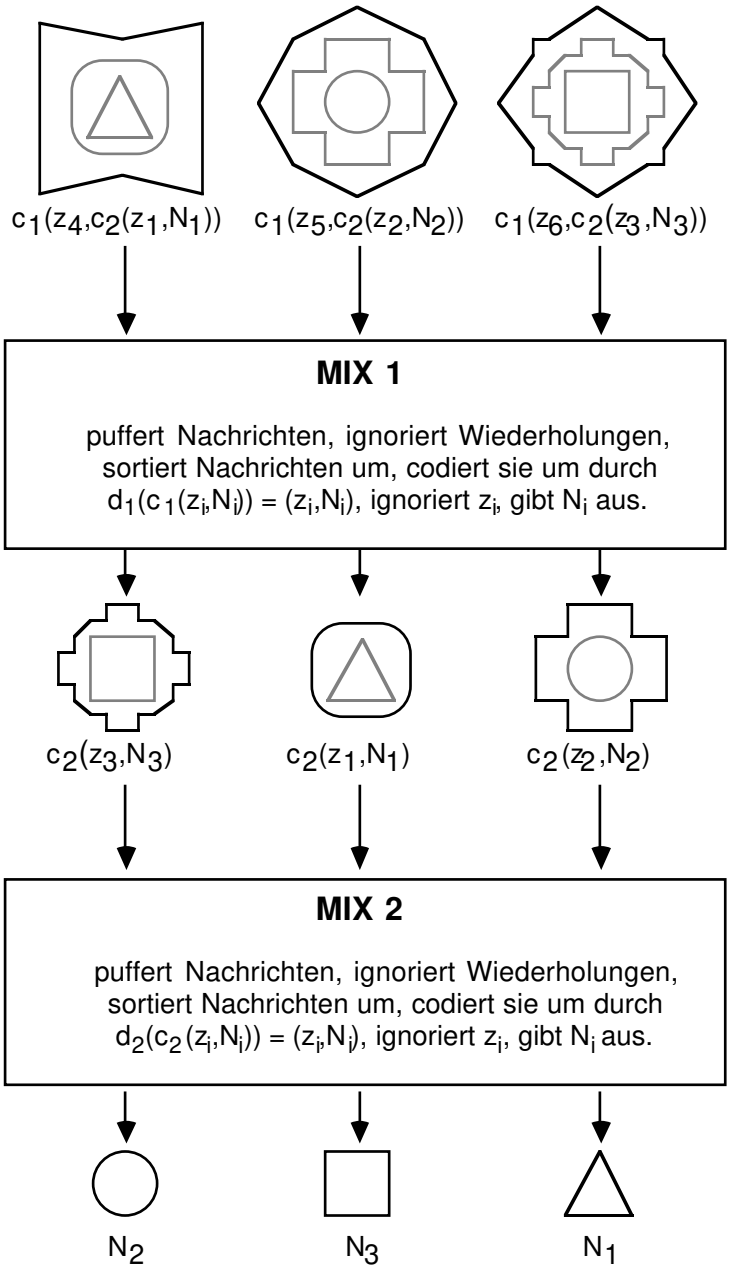


Abb. 8. MIXe verbergen den Zusammenhang zwischen ein- und auslaufenden Nachrichten. Es bezeichne c_j den öffentlichen, d_j den privaten Schlüssel von MIX_j; z_j sind zufällige Bitketten, N_j Nachrichten.

Um ein Verfolgen von Nachrichten nicht durch zeitliche Zusammenhänge oder ihre Längen zu ermöglichen, muß jeder MIX eine Reihe von Nachrichten gleicher Länge abwarten und dann diese umsortiert wieder ausgeben. Gegebenenfalls müssen Teilnehmer oder MIXe bedeutungslose Nachrichten erzeugen.

Um nicht über Nachrichtenhäufigkeiten Entsprechungen zwischen Ein- und Ausgabe des MIXes entstehen zu lassen, darf ein MIX (solange er sein Schlüsselpaar beibehält) nur unterschiedliche Eingabenachrichten bearbeiten. Erhält der MIX eine Eingabenachricht mehrmals, ignoriert er ihr wiederholtes Eintreffen.

Das Verfahren ist in Abb. 8 anhand zweier MIXe dargestellt. Es sei darauf hingewiesen, daß das zur Implementierung verwendete asymmetrische Konzelationssystem gegen sehr mächtige aktive Angreifer sicher sein muß (genauer: es muß sicher gegen Angriffe mit adaptiv gewähltem Schlüsseltext sein [Bött_89], was durch die bisher als relativ sicher bewiesenen asymmetrischen Konzelationssysteme leider nicht geleistet wird [GoMR_88]). So ist z.B. die direkte Implementierung mit RSA des in Abb. 8 dargestellten Verfahrens, in dem einfach vor jede Nachricht eine zufällige Bitkette gehängt wird, unsicher [PfPf_90]. Die Angriffe werden vermutlich erschwert, wenn die Zufallszahl zwischen die Nachricht eingestreut wird. Außerdem sollte man den Zufallszahlen noch Redundanz hinzufügen: Erhält ein MIX eine Nachricht, so mixt er sie nur dann, wenn das gewählte Redundanzprädikat erfüllt ist. Hinsichtlich der Sicherheit ist aber bisher kein solches Schema bewiesen und auch keines so gut untersucht wie die wichtigsten Kryptosysteme.

Weiter ist im Gegensatz zu allen anderen Verfahren in 2.2 eine Kommunikationsbeziehung stets nur unter all den Beziehungen verborgen, die gleichzeitig gemixt werden, nicht unter den Beziehungen aller, evtl. auch gerade inaktiven, anderen Teilnehmer. Dies hat zunächst den prinzipiellen Nachteil, daß ein Teilnehmer A bei einem aus mehreren Nachrichten bestehenden Kontakt mit einem Partner B bei jeder Nachricht unter einer anderen Teilnehmermenge verborgen ist, aus denen B den Durchschnitt bilden und so allmählich A deanonymisieren kann.

Ist das Verfahren sicher implementiert, so wäre die schlimmste Folge eines Angriffs auf einen MIX der Verlust einer Nachricht, nicht jedoch der Verlust der Anonymität. Dies gilt sogar dann, wenn bei Verwendung mehrerer MIXe alle anderen MIXe mit dem Angreifer zusammenarbeiten (bzw. fehlerhaft sind). Durch öffentlichen Zugriff auf die von MIXen gesendeten Nachrichten ist ein Verlust jedoch feststellbar und beweisbar. Zudem kann durch geeignete Fehlertoleranzmaßnahmen die Wahrscheinlichkeit des Verlustes von Nachrichten durch Fehler von MIXen beliebig vermindert werden [MaPf_87, Pfit_85, PfWa_85].

Wegen der Zeitverzögerung durch Umsortieren und Vergleichen der Nachrichten und des Zeitaufwandes für die Entschlüsselungen in einem asymmetrischen Konzelationssystem ist dieses Verfahren nicht für Anwendungen geeignet, die kurze Übertragungszeiten fordern.

Wandelt man es aber ab, so kann man **anonyme Kanäle** schalten, die z.B. den Realzeitanforderungen des Telefonverkehrs genügen könnten [Pfit_85]. Hierzu wird zum Kanalaufbau eine spezielle Nachricht nach dem oben beschriebenen Verfahren übertragen, die jedem gewählten MIX einen Schlüssel eines schnelleren symmetrischen Konzelationssystems übergibt, den dieser MIX von da an für die Entschlüsselung des Verkehrs auf diesem Kanal verwendet. Die Nutzdaten brauchen dann nicht mehr um zufällige Bitketten verlängert und bei Verwendung einer geeigneten Stromchiffre auch nicht auf Wiederholungen geprüft zu werden. Das Umcodieren schützt die Kommunikationsbeziehung eines Kanals natürlich nur unter denjenigen, die gleichzeitig mit ihm durch denselben MIX auf- und abgebaut werden. Durch Kombination mit anderen Grundverfahren kann dieses Verfahren noch verbessert werden (vgl. 3.1.2).

Will man allein durch umcodierende MIXe nicht nur Kommunikationsbeziehungen, sondern auch das Senden und Empfangen von Teilnehmerstationen schützen, muß jede Teilnehmerstation ein MIX sein. Dies erfordert bei geringer Verkehrsdichte große Wartezeiten auf mehrere Nachrichten bzw. auf Auf- oder Abbauwünsche für mehrere Kanäle. Bei hoher Verkehrsdichte erfordert es Teilnehmerstationen, die sehr viele Nachrichten und breitbandige Kanäle umcodieren und vermitteln können. Derartige Teilnehmerstationen sind sehr aufwendig und in überschaubarer Zukunft zu teuer.

2.2.3 Schutz des Senders

Der Sender einer Nachricht kann sich schützen, indem er **bedeutungslose Nachrichten** (dummy traffic) sendet. Werden diese mit nicht existenten impliziten Adressen versehen, können sie von allen Teilnehmerstationen weggeworfen werden. Werden auch bedeutungslose Nachrichten gesendet, kann das Netz nicht mehr entscheiden, wann genau und wieviele bedeutungsvolle Nachrichten ein Teilnehmer sendet [Chau_81].

Dieses Verfahren verursacht stets einen sehr hohen Aufwand und erfüllt zugleich nicht die Forderung nach Anonymität auch bei Angriffen, an denen sich der Empfänger bedeutungsvoller Nachrichten beteiligt.

Die beiden folgenden Verfahren haben diese Nachteile nicht; sie sind relativ effizient, und es ist bewiesen, daß der Sender selbst bei Identität oder Zusammenarbeit von Empfänger und Netzbetreiber anonym ist.

2.2.3.1 Überlagerndes Senden

In [Chau_88, Chau_87] gibt David Chaum folgende Möglichkeit zum anonymen Senden an:

Alle Teilnehmerstationen erzeugen für jedes zu sendende Nutzbit ein oder mehrere Schlüsselbits, von denen sie jedes genau einer anderen Teilnehmerstation auf einem (noch zu diskutierenden) Vertraulichkeit wahrenden Kanal zukommen lassen. Jede Teilnehmerstation **überlagert** (bildet die Summe modulo 2) lokal alle ihr bekannten Schlüsselbits und, sofern sie ein Nutzbit senden will, ihr Nutzbit. Jede Teilnehmerstation sendet das Ergebnis ihrer **lokalen** Überlagerung. Alle gesendeten Bits werden **global** überlagert und die entstehende Summe (modulo 2) aller Bits an alle Teilnehmerstationen verteilt.

Wollte keine senden, ist die Summe 0, da jedes Schlüsselbit genau zweimal addiert wurde. Wollte eine senden, ist die Summe gleich dem gesendeten Nutzbit (Abb. 9).

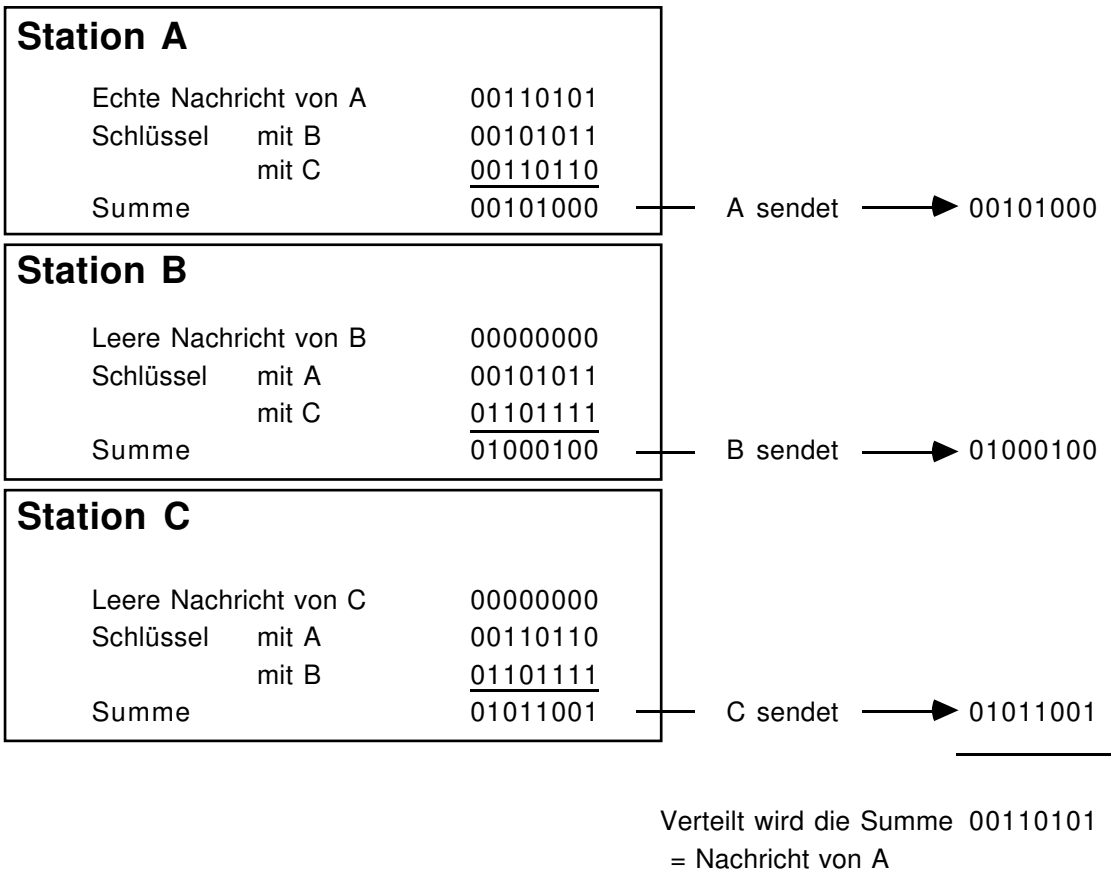


Abb. 9. Überlagerndes Senden

David Chaum beweist in [Chau_88], daß, solange eine Gruppe von Teilnehmerstationen Schlüssel nur in der beschriebenen Form weitergibt und solange diese Gruppe bezüglich der ausgetauschten Schlüssel zusammenhängend ist, andere an diesem Verfahren Beteiligte auch durch Zusammentragen all ihrer Information keine Information darüber erhalten, wer innerhalb der Gruppe sendet. „Bezüglich der ausgetauschten Schlüssel zusammenhängend" bedeutet, daß für je zwei beliebige Teilnehmerstationen T_0, T_1 der Gruppe es eine möglicherweise leere Folge von Teilnehmerstationen T_2 bis T_n der Gruppe gibt, so daß für $1 \le i \le n$ gilt: T_i hat mit $T_{(i+1) \bmod (n+1)}$ einen Schlüssel ausgetauscht.

Das überlagernde Senden läßt sich unter Wahrung der Sicherheit dahingehend verallgemeinern, daß die Überlagerung, d.h. sukzessive Addition von Nachrichten und Schlüsseln, statt modulo 2 innerhalb einer beliebigen abelschen Gruppe, also z. B. modulo einer beliebigen natürlichen Zahl $g \ge 2$, stattfindet. Statt jeden Schlüssel zweimal zu addieren und damit „auszulöschen", muß hier natürlich jeder Schlüssel einmal addiert und einmal subtrahiert werden [Pfit_90].

Natürlich kann es geschehen, daß mehrere Teilnehmerstationen gleichzeitig senden wollen.

Dies ist ein übliches und wohluntersuchtes Problem bei Verteilkanälen mit Mehrfachzugriff, zu dessen Lösung es eine große Zahl von Zugriffsverfahren gibt. Man darf aber nur solche verwenden, die die Anonymität des Senders wahren. Daneben sollten sie bei zu erwartender Verkehrsverteilung den zur Verfügung stehenden Kanal günstig nutzen. Beispiele anonymer Zugriffsverfahren sind das einfache, aber nicht sehr effiziente Verfahren slotted ALOHA und eine für Kanäle mit großer Verzögerungszeit entworfene, effiziente Reservierungstechnik [Chau_88, Tane_81 Seite 272].

Im Gegensatz zu den üblichen (analogen) Übertragungs-Kollisionen handelt es sich bei überlagerndem Senden um **digitale Überlagerungs-Kollisionen**, bei denen das Kollisionsergebnis wohldefiniert ist (eben als die Summe aller Nutznachrichten) und daher zur Auflösung von Kollisionen verwendet werden kann.

Das in [Pfit_90] vorgeschlagene (und auch in [Waid_90] beschriebene) **überlagernde Empfangen** verwendet, daß jeder, der die Summe von n Nachrichten und beliebige n-1 der Summanden kennt, auch die n-te Nachricht berechnen kann. Dies wird mittels Kollisionsauflösungsalgorithmen [Mass_81, Li_87] dazu verwendet, um die n Nachrichten in lediglich n Sendungen zu übertragen (wobei jede Sendung auch einige Kontrollinformation enthalten muß). Es wird das verallgemeinerte überlagernde Senden mit einem hinreichend großen Restklassenring als Nachrichtenraum verwendet, um sowohl die Anzahl kollidierender Nachrichten als auch deren Summe (in $\mathbb{Z}$) zu erhalten. Hieraus kann jeder den „Durchschnitt" (ebenfalls in $\mathbb{Z}$) der gesendeten Nachrichten berechnen. Jeder Sender entscheidet anhand der Lage seiner Nachricht zum Durchschnitt, ob er sich der ersten oder zweiten Gruppe anschließt. In jeder der beiden Gruppen wird dieses Verfahren ggf. rekursiv wiederholt. Offensichtlich ist der Berechnungsaufwand des Protokolls äußerst gering.

Das in [BoBo_90] vorgeschlagene Verfahren verwendet, daß in einem endlichen Körper aus den Summen der ersten n Potenzen von n verschiedenen Elementen ein Polynom berechnet werden kann, dessen Nullstellen gerade die n verschiedenen Elemente sind. Die n Potenzsummen können durch verallgemeinertes überlagerndes Senden mit einem endlichen Körper als Nachrichtenraum berechnet werden. Durch Faktorisieren des Polynoms kann dann jeder die eigentlichen Nachrichten berechnen. Da Faktorisieren von Polynomen relativ aufwendig ist [Rab1_80], ist der Berechnungsaufwand dieses Kollisionsauflösungsverfahrens sehr hoch. Dafür verwendet es etwas weniger Kontrollinformation als das oben skizzierte überlagernde Empfangen.

Beide Verfahren nutzen die Bandbreite erheblich besser als übliche Zugriffsverfahren.

Man kann effizient Kanäle schalten, indem man vereinbart, daß ein Teilnehmer nach kollisionsfreier Sendung einer Nachricht den zuvor bzw. damit reservierten Anteil der Bandbreite zyklisch weiterbenutzen darf und andere Teilnehmer in diesem Anteil erst wieder senden dürfen, wenn er einmal nicht benutzt wurde.

Nach erfolgreicher Reservierung eines Kanals zwischen zwei Stationen kann dieser leicht ohne zusätzlichen Aufwand als Duplexkanal verwendet werden, indem stets beide Stationen ihre Nachtricht senden und von der empfangenen Nachricht ihre eigene subtrahieren.

Durch Angriffe oder Fehler der am überlagernden Senden beteiligten Teilnehmer kann die Anonymität nicht ernstlich gefährdet werden, wohl aber kann die Nachrichtenübertragung nachhaltig und zunächst unidentifizierbar verhindert werden. Maßnahmen, fehlerhafte oder angreifende Teilnehmer zu lokalisieren und auszugrenzen, sind in [MaPf_87, Pfit_90] bzw. [Chau_88, WaPf_89, PfWa1_91] beschrieben, ein Verfahren zur Maskierung von Störungen in [EcNi_89, Nied_87]. Letzteres basiert auf der Verwendung mehrerer Netze mit überlagerndem Senden, wobei jeder Teilnehmer in allen Netzen empfangen, aber nicht in allen senden und damit auch nicht in allen stören kann. Werden aus Aufwandsgründen alle Netze mit überlagerndem Senden z.B. durch Zeitmultiplex auf einem einzigen Digitalnetz realisiert, so kann der Schutz gegen unerlaubtes Senden realisiert werden, indem eine zentrale Instanz die Überlagerung aller Einzelnachrichten übernimmt und dabei stets nur die Nachrichten der Teilnehmer überlagert, die im gerade aktuellen Zeitschlitz senden durften.

Der Einsatz des überlagernden Sendens ist sehr aufwendig, weil man große Mengen an Schlüsseln vertraulich austauschen muß: Für jedes Paar von Teilnehmerstationen, das Schlüssel miteinander austauscht, benötigt man dazu einen die Vertraulichkeit wahrenden Kanal mit derselben Bandbreite, wie sie das Netz allen Benutzern zusammen zum anonymen Austausch ihrer Nachrichten bereitstellt.

Diesen Aufwand beim Schlüsselaustausch kann man reduzieren, indem man Pseudozufallszahlengeneratoren verwendet. Man muß dann nur relativ kurze Schlüssel geheim austauschen und kann aus diesen sehr lange Schlüssel, die äußeren Betrachtern zufällig erscheinen, erzeugen. Das Verfahren ist dann nicht mehr **informationstheoretisch**, sondern nur noch **kryptographisch** mehr oder weniger sicher.

Ein Pseudozufallszahlengenerator heißt **kryptographisch stark**, wenn bewiesen werden kann, daß durch das Brechen zugleich ein effizienter Algorithmus zur Lösung eines wohluntersuchten, aber bislang nicht effizient lösbaren mathematischen Problems angegeben werden kann. Ein solcher Beweis wurde bisher leider nur für vergleichsweise ineffiziente Generatoren erbracht. So ist das Brechen des in [VaVa_85] beschriebenen Generators äquivalent zur Faktorisierung; die Geschwindigkeit dürfte bei geeigneter Implementierung der von RSA ähneln (vgl. 1.4.1).

Ohne einen vergleichbaren Sicherheitsbeweis lassen sich z.B. durch Modifikation von DES entsprechend schnellere und „praktisch" sichere Generatoren gewinnen (vgl. 1.4.1). Noch schneller als diese sind auf rückgekoppelten Schieberegistern basierende Generatoren, die in ihren konkreten Ausprägungen jedoch häufig gebrochen werden und daher für den praktischen Einsatz nicht empfehlenswert sind.

David Chaum schlägt in [Chau_88] vor, das überlagernde Senden auf einem Ring zu implementieren. Dadurch wird einem Angreifer das Brechen von schnellen (und vielleicht leicht brechbaren) Pseudozufallszahlengeneratoren erschwert, weil er die Ausgaben von aufeinanderfolgenden Teilnehmerstationen im Ring nur durch sehr aufwendige physikalische Maßnahmen, also realistischerweise nicht erfährt (vgl. 2.2.3.2).

Bei dieser Implementierung kreist jedes Bit einmal zum Zwecke des Sendens durch sukzessives Überlagern und einmal zum Zwecke des Empfangens um den Ring.

Da diese Implementierung im Mittel nur den vierfachen Übertragungsaufwand verursacht wie ein übliches Sendeverfahren auf einem Ring, während eine Implementierung auf einem sternförmigen Netz den *N*-fachen Übertragungsaufwand gegenüber einem gewöhnlichen Sendeverfahren auf einem Stern verursacht, wirkt sie recht effizient.

Da aber die Übertragungsmenge auf jeder einzelnen Leitung, also die geforderte Bandbreite, bei allen Implementierungen gleich ist, kann die Implementierung auf einem Stern (oder allgemeiner: Baum) trotzdem effizienter sein. Die Implementierung eines Kanals ist um so besser, je kürzer die Verzögerungszeit ist, also die Zeit, die zwischen Sendeversuch und der Rückmeldung, ob eine Überlagerungs-Kollision auftrat, verstreicht. Für dieses Verfahren können die Knoten von Stern- und Baumnetzen wesentlich

einfacher als übliche Vermittlungszentralen sein und so entworfen werden, daß die Summe der Schaltzeiten nur logarithmisch mit der Teilnehmeranzahl wächst. Die reine Laufzeit wächst ungefähr mit der Wurzel der Teilnehmeranzahl, während beide bei Ringnetzen stets proportional zur Teilnehmeranzahl wachsen [Pfit_85].

Es sei angemerkt, daß überlagerndes Senden mit der Erweiterung in [Waid_90, WaPf_89, LuPW_91] auch zum, selbst gegen stärkstmögliche aktive Angreifer, **anonymen Empfangen** genutzt werden kann, vgl. auch § 2.2.1.

2.2.3.2 RING-Netz

Das aufwendige Generieren, ggf. Verteilen und Überlagern von Schlüsseln und Nutzdaten im vorherigen Abschnitt ist nötig, weil dort davon ausgegangen wird, daß ein Angreifer die Ausgänge und Eingänge aller Teilnehmerstationen abhört.

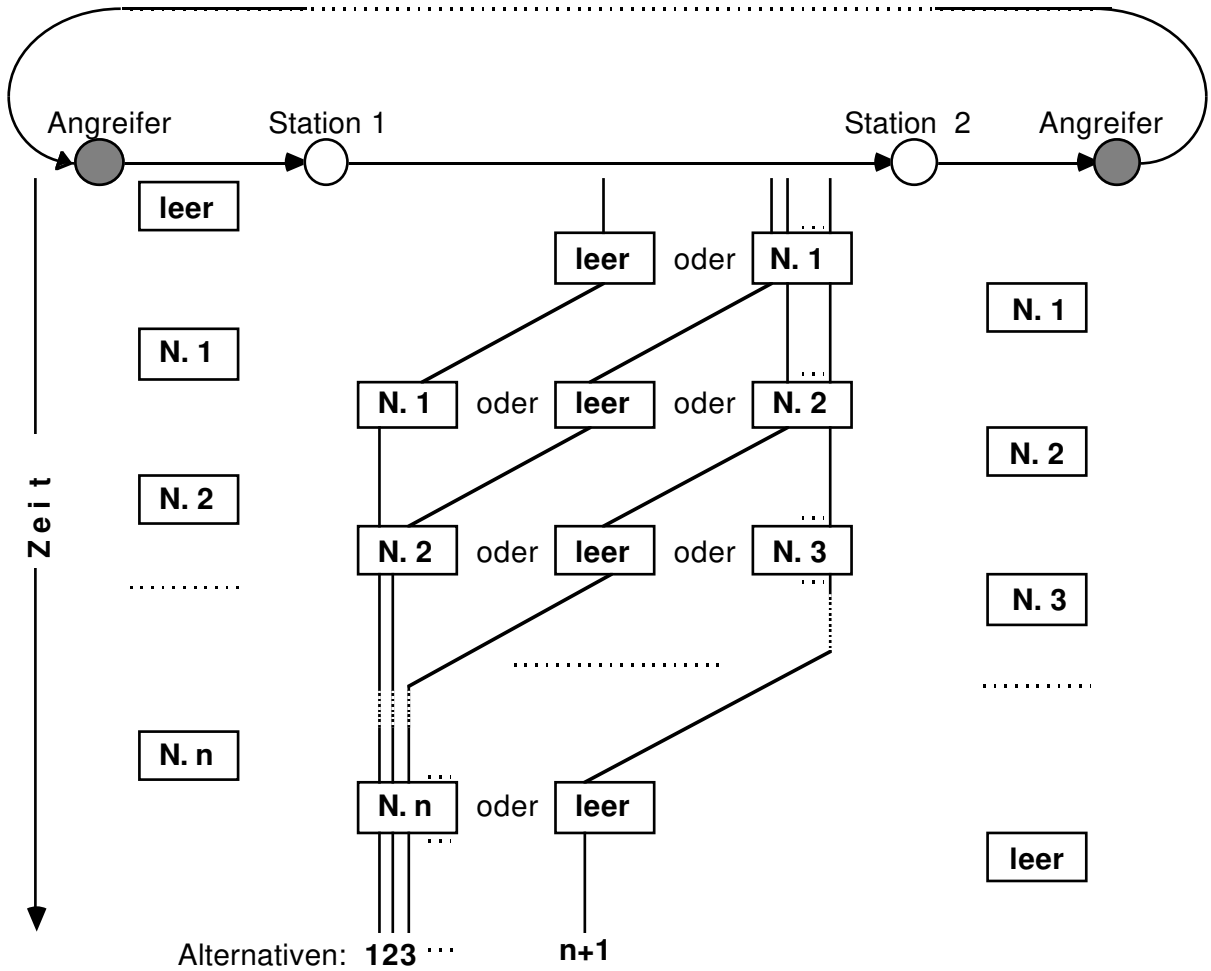
Die Idee für ein weit weniger aufwendiges Verfahren, das RING-Netz, besteht darin, das Netz bereits physikalisch so zu gestalten, daß es für einen Angreifer nicht einfacher ist, alle Ein- und Ausgänge einer Teilnehmerstation abzuhören, als den Teilnehmer bzw. die Teilnehmerstation direkt zu beobachten (vgl. 1.4).

Die praktischste Möglichkeit hierzu ist, die Teilnehmerstationen ringförmig anzuordnen, wie dies im Bereich lokaler Netze seit langem praktiziert wird. Um hier das Senden einer Station zu überwachen, müssen entweder ihre beiden Nachbarn zusammenarbeiten, oder die Leitungen müssen abgehört werden. Durch bauliche Maßnahmen, z.B. direkte Verkabelung von Wohnungen in Mehrfamilienhäusern sowie direkte Verkabelung aneinandergrenzender privater Grundstücke [Pfit_83 Seite 18], kann man erreichen, daß letzteres ebenso aufwendige physikalische Maßnahmen erfordert wie das direkte Abhören des Teilnehmers oder der Teilnehmerstation innerhalb der Wohnung. Damit verspricht es keinen zusätzlichen Vorteil. Versuchen die zwei Ringnachbarn eines Teilnehmers, diesen ohne Auftrag Dritter (d.h. hier ohne Zusammenarbeit mit großen Kommunikationspartnern) zu beobachten, so erfahren sie beinahe nichts, da alle ausgehenden Nachrichten verschlüsselt und die Adressen bei geeigneter Verwendung impliziter Adressierung für sie nicht interpretierbar sind.

Zu erwarten sind also im wesentlichen Angreifer, die nur eine Gruppe von vielen zusammenhängenden Stationen eingekreist haben. Sie können durch Vergleich der ein- und auslaufenden Bitmuster nur feststellen, welche davon von den Mitgliedern dieser Gruppe gesendet bzw. vom Ring entfernt wurden, nicht aber von welchem Mitglied genau.

Voraussetzung hierfür ist natürlich, daß Sender oder Empfänger sich nicht anhand analoger Charakteristika erkennen lassen, wozu geeignete Signalregenierungsverfahren notwendig sind [Pfit_90].

Ein Angreifer hat allerdings nicht nur die Möglichkeit, ein- und auslaufende Bitmuster zu vergleichen, sondern kann auch seine Kenntnis des Ringzugriffsverfahrens verwenden, um Schlüsse zu ziehen, wer gerade senden darf. Man kann aber zeigen, daß bei geeigneten Ringzugriffsverfahren ein Angreifer, der eine Station nicht direkt eingekreist hat, tatsächlich das Senden dieser Station nie feststellen kann [HöPf_85, Höck_85]. Geeignet und effizient sind gewisse bekannte Verfahren (slotted ring, token ring), die dahingehend abgewandelt wurden, daß Senderecht zeitlich unbefristet vergeben wird und jede Nachricht einmal ganz um den Ring läuft, d.h. nicht vom Empfänger, sondern erst vom Sender wieder vom Ring entfernt wird (Abb. 10). Da durch sie bereits Verteilung realisiert ist, wird neben dem Sender auch der Empfänger geschützt.



Effiziente Ringzugriffsverfahren (token, slotted) reichen das Senderecht von Station zu Station weiter. Wenn ein Angreifer 2 Stationen umzingelt hat, die nach Erhalt des Senderechts insgesamt n Nachrichten senden und dann das Senderecht weiterreichen, gibt es n+1 Alternativen, welche Station welche Nachricht (N.) gesendet haben kann. Für jede Nachricht gibt es mindestens eine Alternative, bei der Station i (i=1,2) die Nachricht sendet.

Das Beispiel kann auf g umzingelte Stationen verallgemeinert werden. Es gibt $\binom{n+g-1}{n}$ Alternativen und zumindest eine Alternative für jede Nachricht, bei der Station i (i=1,2,…,g) die Nachricht sendet.

Abb. 10. Ein anonymes Zugriffsverfahren für RING-Netze garantiert: Ein Angreifer, der eine Folge von Stationen umzingelt hat, kann nicht entscheiden, welche was sendet.

Sowohl das Senden von Nachrichten als auch das Schalten von Kanälen ist mit Hilfe dieser Zugriffsverfahren möglich. Bei Duplexkanälen kann man aber ohne große Anonymitätseinbußen auch wieder darauf verzichten, daß alle Information einmal ganz um den Ring läuft. Statt dessen nimmt der Empfänger die Information vom Ring und ersetzt sie sofort durch Information in Gegenrichtung. Dadurch ist die Kapazität des Rings doppelt so gut nutzbar.

Auch beim RING-Netz ist durch Angriffe oder Fehler in Stationen oder auf Leitungen zwar nicht die Anonymität, aber die Funktionsfähigkeit des gesamten Netzes gefährdet. Zur Fehlertoleranz müssen daher redundante Leitungen vorgesehen werden (braided ring), wobei bei der Rekonfiguration zur Erhaltung der Anonymität nicht nur logisch, sondern auch physikalisch stets wieder ein Ring entstehen sollte [Mann_85, MaPf_87].

3 Einsatz der Grundverfahren in einem flächendeckenden Kommunikationsnetz

In Kapitel 2.2 wurden die bekannten Grundverfahren beschrieben, die es den Teilnehmern eines Kommunikationsnetzes ermöglichen, anonym voreinander wie auch vor dem Netz Nachrichten auszutauschen. Dieses Kapitel soll nun unter Hinzunahme von Leistungs- und Kostenüberlegungen den praktischen Einsatz dieser Lösungsansätze behandeln.

Hierzu werden zunächst die technischen Grenzen der Grundverfahren aus heutiger Sicht angegeben. Sodann wird diskutiert, welche Möglichkeiten sich hieraus zur raschen Einführung eines flächendeckenden Datenschutz garantierenden Kommunikationsnetzes ergeben, insbesondere die Notwendigkeit einer hierarchischen Aufteilung des Netzes. Einige Gedanken zu den Netzabschlüssen und zur Abrechnung der Netzbenutzung schließen das Kapitel ab.

3.1 Grenzen für den praktischen Einsatz der Grundverfahren

Wirkungsvoller Schutz der Inhaltsdaten und alle in Abschnitt 2.2 aufgeführten Maßnahmen außer reiner Verteilung setzen ein Digitalnetz, insbesondere **digitale Teilnehmeranschlüsse**, voraus. Als Basis der folgenden Überlegungen wird daher angenommen, daß jeder Netzteilnehmer

- nach einer Übergangsphase mindestens einen **schmalbandigen** Duplexkanal mit 64 kbit/s, z.B. zum Fernsprechen, zur Verfügung haben und
- entsprechend der Postplanung in weiterer Zukunft einen **breitbandigen** Duplexkanal erhalten können soll. Um über diesen qualitativ hochwertiges Bildfernsprechen zu ermöglichen, muß er nach dem heutigen Stand der Technik mindestens 34 Mbit/s übertragen können [Möhr_87, KrNa_85].

Ende-zu-Ende-Verschlüsselung zum **Schutz der Inhaltsdaten** (ohne den Schutz der Verkehrsdaten oft sinnlos wäre) stellt, wie in Abschnitt 1.4 diskutiert, in beiden Fällen zum jeweiligen Einführungszeitpunkt ein praktisch lösbares Problem dar, sofern die heutigen Sicherheitseinschätzungen zutreffen.

Im folgenden sollen die Grenzen der einzelnen Verfahren zum **Schutz der Verkehrsdaten** aus 2.2 betrachtet werden (die natürlich auch von der Menge an Bauteilen abhängen, die man einzusetzen bereit ist). Hinsichtlich der verlangten Aufbau- und Antwortzeiten und des maximalen Nutzungsgrads werden im wesentlichen die für Fernsprechen üblichen Werte angenommen. Die Größe der Gruppen, innerhalb derer die Verfahren durchgeführt werden, ist noch zu bestimmen.

3.1.1 Verteilung

Der Empfänger einer Nachricht kann gemäß 2.2.1 geschützt werden, indem diese an alle Teilnehmer oder zumindest eine hinreichend große Gruppe zuverlässig verteilt wird.

Grundvoraussetzung hierfür ist, daß die **Bandbreite** des Übertragungskanals in Richtung jedes Teilnehmers ausreicht, um das, was alle gleichzeitig aktiven Teilnehmer seiner Gruppe empfangen sollen, zu übertragen. Die für das Fernsprechnetz üblichen Kupferdoppeladern erfüllen diese Forderung nur sehr unzureichend, so daß breitbandigere Medien eingesetzt werden müssen.

Nach dem heutigen Stand der Technik lassen sich auf Lichtwellenleitern Übertragungsgeschwindigkeiten von einigen Gbit/s erreichen [Midw_85, BeEn_85]. Damit ist die Anzahl der über eine Glasfaser gleichzeitig verteilbaren schmalbandigen Kanäle auf einige zehntausend, die breitbandiger auf etwa hundert begrenzt. Die Gruppen, innerhalb derer Teilnehmer anonym sind, können nur um einen kleinen Faktor größer sein, beispielsweise 10 bei einer maximalen Dienstnutzung von 10% (nach [Kais_82]) und der Beschränkung auf eine Glasfaser pro Teilnehmer. Für die Zukunft wird allerdings noch eine Erhöhung der Übertragungsgeschwindigkeit um den Faktor tausend erwartet [Midw_85, GPBK_88].

Es sei jedoch erwähnt, daß obige Begrenzungen nicht für Dienste der **Massenkommunikation** gelten müssen: Hörfunk, Fernsehen und evtl. auch Tageszeitungen (als besserer Videotext) können und

sollten auch in Zukunft netzweit als echte Verteildienste angeboten werden. Bei Bedarf könnte die Information verschlüsselt übertragen und der verwendete Schlüssel in einer Datenschutz garantierenden Weise zum Verkauf angeboten werden. Dabei kann ohne weiteres ein nicht sehr sicheres, dafür aber schnelles und billiges Kryptosystem verwendet werden, da dieser Verkäuferschutz sowieso leicht zu unterlaufen ist, indem ein legaler Käufer den Schlüssel weitergibt.

Ein zweiter möglicher Engpaß ist die **Adreßerkennung** für öffentliche verdeckte implizite Adressen (vgl. Abb. 7), die auf dem probeweisen Entschlüsseln von Adressen in einem asymmetrischen Kryptosystem beruht. Dies beansprucht je Adresse derzeit mindestens 3 ms (vgl. 1.4.1). Der während dieser relativ langen Zeit empfangene Verkehr muß entweder gepuffert werden, oder die Adressierung muß über einen Signalisierungskanal rechtzeitig vor Übertragung der eigentlichen Daten erfolgen. Der Durchsatz hingegen scheint derzeit kein Problem zu sein, denn werden z.B. die Teilnehmer in der Hauptverkehrsstunde im Mittel alle 15 Minuten angerufen (nach [Siem_88]), so kann ein Chip die Adressen von 300000 Teilnehmern entschlüsseln. Die anderen Formen impliziter Adressierung sind sowieso unkritisch.

3.1.2 Umcodierende MIXe

Durch Verwendung umcodierender MIXe wird gemäß 2.2.2 die Kommunikationsbeziehung zwischen Sender und Empfänger geschützt, wobei aber noch einmal erwähnt sei, daß die kryptographische Sicherheit dieses Verfahrens von allen vorgestellten am zweifelhaftesten ist.

Der Vorteil dieses Grundverfahrens gegenüber allen übrigen ist dafür, daß es, jedenfalls wenn man anonyme Kanäle (vgl. 2.2.2) schaltet, die benötigte **Bandbreite**, zumindest der Teilnehmeranschlußleitungen, gegenüber einem nicht anonymen Netz fast nicht erhöht. Insbesondere ist es daher als einziges mit den derzeitigen Kupferdoppeladern denkbar.

Die wesentlichste technische Beschränkung des Verfahrens ergibt sich durch die **Verzögerungszeiten.**

Wären die MIXe im Netz verstreut und könnten die Teilnehmer beliebige verwenden, so würde fast alle Information das Netz viele Male durchlaufen. Dies (und damit neben der Verzögerung die zusätzliche Belastung des Fernnetzes) kann vermieden werden, indem an geeigneten Stellen, z.B. bei Fern- oder Ortsvermittlungsstellen, jeweils eine direkt miteinander verbundene Gruppe von MIXen, eine sog. **MIX-Kaskade**, eingerichtet wird und jede Nachricht ein oder zwei in festgelegter Reihenfolge durchläuft (Abb. 11). Zur Gewährleistung des Datenschutzes könnte unseres Erachtens eine Kaskadenlänge von 5 bis 10 MIXen ausreichen.

Die durch das Umcodieren, Umsortieren und Vergleichen der Einzel- und Kanalaufbaunachrichten entstehende Verzögerung stellt bei so wenigen MIXen kein Problem dar, wenn die Vergleichsnachrichten im Hauptspeicher gehalten werden können. Letzteres könnte allerdings sehr große Speicher erfordern, weil die (durch die Schlüssel der MIXe und evtl. Zeitstempel gegebene) Klasse der erlaubten Nachrichten nicht sehr oft wechseln darf, denn ein Teil der Kanalaufbaunachrichten muß wegen dessen Anonymität vom Empfänger erzeugt sein, der nicht genau voraussagen kann, wann sie verwendet werden [Chau_81, Pfit_90].

Hinzu kommt aber die Verzögerung dadurch, daß stets **genug zu mixende Nachrichten** vorhanden sein müssen. Für einzelne, zeitunkritische Nachrichten, z.B. elektronische Post, stellt dies kein Problem dar, da einfach einige Zeit gesammelt werden kann. Für zwar eilige, aber einzelne Nachrichten kann durch Erzeugung bedeutungsloser Nachrichten das Verkehrsaufkommen entsprechend gesteigert werden. Mit dem Schalten von Kanälen müßte jedoch auf eine so große Zahl von Aufbauwünschen gewartet werden, daß aus den gleichzeitig aufgebauten Kanälen genügend große Teilgruppen gleichzeitig wieder abgebaut werden können. Dabei müßte auch die Wartezeit der Teilnehmer auf das Abbauen, zumindest bei schmalbandigen Teilnehmeranschlußleitungen, innerhalb der tolerierbaren Kanalaufbauzeit bleiben, da in der Zeit der Anschluß blockiert wäre. Ohne Zuhilfenahme anderer Verfahren scheint dieses Problem zumindest nicht ohne Datenschutzeinbußen für ungewöhnlich lange telefonierende Teilnehmer lösbar.

Man könnte zunächst erwägen, wieder auf das Schalten anonymer Kanäle zu verzichten bzw., da Paketvermittlung zu nicht erträglicher Verzögerung und Datenexpansion führen würde, Kanalstücke für so kurze Zeitscheiben getrennt zu vermitteln, daß Warten auf ihr Ende nicht stört. Allein hilft dies jedoch nichts, da man statistisch doch merkt, daß es sich um Kanäle handelt, weil sowohl Sender als auch Empfänger genau während der Dauer eines Gesprächs fortlaufend Zeitscheibenkanäle unterhalten.

Letzteres kann aber vermieden werden, wenn die Teilnehmer zwischen den Gesprächen auf den Teilnehmeranschlußleitungen, die ihnen ja exklusiv zugeordnet sind, ständig bedeutungslose Zeitscheibenkanäle senden und empfangen. Damit diese nicht ins Fernnetz gelangen, aber trotzdem nicht von bedeutungsvollen zu unterscheiden sind, müssen sie zwischen Teilnehmer und Ortsvermittlungsstellen, wo sie enden, eine MIX-Kaskade durchlaufen. Die Information auf den Empfangskanälen wird dabei von der Ortsvermittlungsstelle erzeugt, im Falle des Ausbleibens springt aber jeder MIX mit eigener Information ein. Man kann den Datenschutz sogar noch verbessern, indem die Teilnehmer im Normalfall auf den bedeutungslosen Kanälen an sich selbst senden, da diese dann von Ortsgesprächen nicht mehr zu unterscheiden sind.

Die Koordination zwischen dem Empfangen bedeutungsloser Zeitscheibenkanäle von sich selbst und bedeutungsvoller von einem Partner wird zweckmäßig so geregelt, daß jeder nicht nur seinen Sende-, sondern auch seinen Empfangskanal durch die MIX-Kaskade seines Ortsnetzes selbst aufbaut und ggf. ein Partner als Adresse ein Anschlußkennzeichen davon kennen muß.

Zusätzlich muß ein Signalisierungskanal zur Verfügung stehen, auf dem Gesprächswünsche übertragen werden können und die Adreßkennzeichen für die eigentlichen Kanäle vereinbart werden. Die Empfänger der Gesprächswünsche können nicht auf die gleiche Art geschützt werden, weil damit das Problem, den Kanal für echte Nachrichten von bedeutungslosen freizubekommen, nur vom Hauptkanal auf den Signalisierungskanal verlagert würde. Statt dessen können diese **Gesprächswünsche verteilt** werden, da ihr Informationsgehalt um Größenordnungen geringer ist als der der eigentlichen Fernsprechkanäle. Nutzung von 6-kbit/s des Signalisierungskanals müßte beim derzeitigen Fernsprechverhalten, insbesondere bei Verwendung von Verfahren zur Vermeidung von erfolglosen Wahlwiederholungen, für mindestens fünftausend Teilnehmer genügen.

Das vollständige, **Telefon-MIXe** genannte Verfahren ist in [PfPW_89, PfPW_91] ausführlich beschrieben.

Die Kombination der MIXe mit bedeutungslosen Zeitscheibenkanälen und Verteilung der Gesprächswünsche löst zugleich zwei weitere Probleme: Zum einen wechseln die Gruppen, in denen die Teilnehmer anonym sind, nicht mehr. Zum anderen sind nun die einzigen Adressen, die lange gültig sein müssen, die impliziten der Gesprächswünsche, jedoch keine mehr, die durch MIXe führen. Dadurch können die MIXe in allen Kanalaufbaunachrichten Zeitstempel verlangen, was den Aufwand beim Prüfen der Nachrichten auf Wiederholungen drastisch reduziert.

Neben die technischen treten beim Verfahren der umcodierenden MIXe in besonderem Maße organisatorisch-politische Probleme. Grundannahme ist ja die Existenz hinreichend vieler **unabhängiger Betreiber** der MIXe. Die Anforderungen an diese sind hoch: einerseits sollte jeder Teilnehmer in der ihm zugeordneten Kaskade mindestens einen MIX seines Vertrauens finden; andererseits sind sie gegenüber der Post als eigentlichem Netzbetreiber zu einem guten Teil für die Dienstqualität (Verzögerungszeiten, Fehlerrate) verantwortlich.

Außerdem ist nicht garantiert, daß der Betreiber die alleinige Macht über seinen MIX hat, da MIXe als komplexe Systeme praktisch unauffindbare Trojanische Pferde enthalten könnten. Daher sollten MIXe verschiedener Betreiber auch unabhängige Entwerfer und Hersteller haben. Auch dieses Problem wird aber verringert, wenn die MIXe selbst keinerlei Vermittlungsfunktion haben und mittels bedeutungsloser Zeitscheibenkanäle konstant ausgelastet werden, da beides einen regulären, prüfbaren Entwurf erleichtert und die Möglichkeiten für verdeckte Kanäle einschränkt.

3.1.3 Überlagerndes Senden

Wird zum Schutz des Senders überlagerndes Senden gemäß 2.2.3.1 verwendet, so erfordert dies, daß die **Bandbreite** des Übertragungskanals jedes Teilnehmers ausreicht, um die Sendekanäle aller gleichzeitig aktiven Teilnehmer seiner Teilnehmergruppe zu übertragen. Dies ist fast die duale Situation zur Verteilung (hinzu kommt etwas Kontrollinformation, dafür senden private Teilnehmer kein Fernsehen). Hinsichtlich der notwendigen Übertragungsmedien und Teilnehmergruppengrößen gilt daher das bereits dort Gesagte. Sinnvollerweise wird man bei überlagerndem Senden immer auch Verteilung verwenden.

Die weiteren Grenzen des Verfahrens sind im wesentlichen durch die Schlüsselerzeugung gegeben.

Um allen Teilnehmern Unbeobachtbarkeit zu garantieren, muß im Mittel jeder mindestens zwei Schlüssel ausgetauscht haben; besser sind aber wesentlich mehr, z.B. zehn, um eine Partitionierung des Schlüsselgraphen nicht gar zu einfach zu machen (vgl. 2.2.3.1). Mit welchen anderen Teilnehmern ein Teilnehmer Schlüssel austauscht (z.B. mit einigen von ihm selbst ausgesuchten Wahlpartnern im Bekanntenkreis und, um das Eingliedern neuer Teilnehmer zu erleichtern, einigen ihm zugeteilten Partnern) und ob er auch mehr Schlüssel als gefordert austauschen darf, soll hier nicht weiter behandelt werden.

Um den Schlüsselaustausch effizient zu halten, werden **Pseudzufallsbitfolgengeneratoren** (kurz Generatoren genannt) verwendet (vgl. 2.2.3.1). Eine direkte Erzeugung des Ergebnisses der Überlagerung aller Schlüssel eines Teilnehmers mit den dort genannten, einigermaßen sicheren Generatoren ist nicht sinnvoll bzw. möglich, so daß jeder Teilnehmer für jeden ausgetauschten Schlüssel einen eigenen Generator benötigt.

Will man pro Schlüssel nur einen Generator einsetzen, so muß dessen Geschwindigkeit der Bandbreite des Übertragungskanals des Teilnehmers entsprechen, d.h. er muß zur Überlagerung dessen reichen, was alle gleichzeitig aktiven Teilnehmer seiner Teilnehmergruppe senden wollen. Damit ist das Verfahren für breitbandige Dienste offenbar noch nicht einsetzbar. Für schmalbandige Dienste würde diese Forderung die Anzahl der möglichen Teilnehmer bei Einsatz der derzeitigen kryptographisch sicheren Generatoren auf wenige zehn, bei Einsatz der schnelleren DES-ähnlichen Generatoren auf wenige tausend beschränken.

Da zur fehlerfreien Ausführung des Verfahrens alle Sender korrekt arbeiten müssen, wird die Anzahl der Teilnehmer am Verfahren auch durch die geforderte hohe **Zuverlässigkeit** begrenzt. Genauere Abschätzungen hierfür sind erst bei Kenntnis der Implementierungen möglich.

3.1.4 RING-Netz

Da ein RING-Netz zum Schutz des Senders gemäß 2.2.3.2 automatisch auch einen Verteilkanal realisiert, gilt für die **Bandbreite** dasselbe wie in 3.1.3. Ringstrukturen mit entsprechender Bandbreite sind im Laborstadium verfügbar [BeEn_85]. Kommerziell gibt es Ring-Netze mit 500 Teilnehmern ([Ross_87]: optischer Token-Ring, Leitungslänge maximal 100 km, Übertragungsrate 100 Mbit/s).

Auch die **Verzögerungszeit** und die zu fordernde **Zuverlässigkeit** lassen RING-Netze mit mehr als 10000 Teilnehmern kaum sinnvoll erscheinen.

Erste Übertragungsleistungs- und Zuverlässigkeitsuntersuchungen [Bürl_85, Mann_85] für Ringe mit den für Datenschutz modifizierten Zugriffs- und Fehlertoleranzverfahren (vgl. 2.2.3.2) lassen für sie bei moderater Größe ein etwa gleichgroßes Leistung/Kosten-Verhältnis wie für die üblichen reinen Vermittlungsnetze erwarten.

Um das **Angreifermodell** realistisch zu machen, muß der Zugriff auf die Leitungen, wie in 2.2.3.2 erläutert, durch bauliche Maßnahmen verhindert werden. Dies heißt zugleich, daß ein Ring im wesentlichen immer sofort vollständig aufgebaut werden muß.

Vertraut man nicht auf die Sicherheit längerer Kabelkanäle, so folgt weiterhin, daß RING-Netze nur in dicht bebauten Gebieten sinnvoll sind.

Außerdem ist man, sofern zumindest die Bandbreite eines benutzten Dienstes zu erkennen ist, nur unter den Teilnehmern an Diensten derselben Bandbreite innerhalb desselben Ringes geschützt. (Im Gegensatz dazu können die anderen Grundverfahren in der Einführungsphase eines Dienstes auch in Gruppen von räumlich voneinander entfernten Teilnehmern durchgeführt werden.) Will man schon

während der Einführungsphase des breitbandigen Netzes auf diesem nicht nur für schmalbandige, sondern auch für breitbandige Dienste Datenschutz garantieren, so muß also innerhalb eines RING-Netzes sogleich ein großer Teil der Teilnehmer an diesen teilnehmen (oder breitbandige Kanäle müssen als Summe vieler schmalbandiger geschaltet werden, was aber Möglichkeiten für statistische Angriffe läßt).

Ein RING-Netz verlangt im Gegensatz zu den anderen Grundverfahren eine neue Topologie der **Kabelkanäle**. Da die Kosten zusätzlicher Erdarbeiten u.ä. die von Pseudozufallszahlengeneratoren oder MIXen überwiegen dürften, ist es wohl nur dort kostengünstig, wo sowieso neue Kabelkanäle angelegt werden müssen, d.h. im wesentlichen in Neubaugebieten [Pfit_83, Mann_85].

3.2 Gestaltungsmöglichkeiten eines flächendeckenden, Datenschutz garantierenden offenen Kommunikationsnetzes

3.2.1 Hierarchisierung

Die Diskussion in 3.1 ergab, daß alle Verfahren außer MIXen mit heutiger Technologie höchstens in Gruppen von einigen hundert bis zehntausend Teilnehmern durchgeführt werden können. (Es sei jedoch daran erinnert, daß Massenkommunikation ohne Rückkanal, also z.B. Fernsehen, sich problemlos durch Verteilen in beliebig großen Netzen schützen läßt.)

Um mit diesen trotzdem ein Netz von der Größe des geplanten ISDN zu realisieren, müssen die Teilnehmer des ISDN in passende kleinere **Anonymitätsgruppen** eingeteilt werden, die jeweils ein Datenschutz garantierendes Teilnetz des umfassenderen Netzes bilden. Die Kommunikation zwischen den Teilnetzen kann durch ein beliebiges Netz realisiert werden. Das Netz wird also hierarchisch aufgeteilt, und entsprechend werden die Teilnehmer hierarchisch durch eine Adresse ihrer Anonymitätsgruppe im umfassenden Netz und durch eine implizite Adresse innerhalb derselben adressiert. Das Senden und Empfangen einer solchen Gruppe als Ganzes ist dann je nach dem umfassenden Netz beobachtbar, die Mitglieder der Gruppe bleiben jedoch untereinander verborgen.

Dabei erscheint es am sinnvollsten, die Gruppeneinteilung fest vorzugeben und durch die Netztopologie zu unterstützen. Für manche Situationen (wenig oder schmalstbandiger Verkehr) können jedoch zur Erhöhung der Anonymität mehrere Gruppen zu größeren zusammengefaßt werden. Die Alternative, die Anonymitätsgruppen dynamisch, evtl. je nach momentanem Wunsch der Teilnehmer, zu bilden, wäre (außer bei MIXen) höchstens bei Verteilung realisierbar. Dies würde aber die Adressierung und Vermittlung erschweren und die Gefahr beinhalten, daß Teilnehmer sich bei mehrfachem Kontakt mit demselben Partner innerhalb verschiedener Gruppen verbergen, aus denen der Partner den Durchschnitt bilden kann.

Im einfachsten Fall ergibt sich als Netzorganisation also eine zweistufige Hierarchie (**Vermittlungs-/Verteilnetz**, vgl. Abb. 11), die beim ISDN der bereits bestehenden in Fern- und Ortsnetze entspricht. Die obere Hierarchiestufe bleibt ein Vermittlungsnetz, die untere realisiert die Anonymitätsgruppen (evtl. mehrere pro Ortsnetz) und besteht aus Verteilnetzen, möglichst mit überlagerndem Senden oder als RING-Netze.

Die Alternative, auch auf der oberen Hierarchiestufe, also unter den Protokollumsetzern zwischen Vermittlungsnetz und den einzelnen Anonymitätsgruppen, eines der Grundverfahren anzuwenden (z.B. ein Verteil-/Verteilnetz), hätte die Probleme, daß der Verkehr zwischen diesen sehr breitbandig ist und man den Protokollumsetzern vertrauen müßte. Zusätzlich MIXe im Fernnetz sind jedoch sinnvoll.

3.2.2 Schrittweiser Netzausbau

Um ausgehend vom heutigen Fernsprechnetz zu einem Datenschutz garantierenden Netz zu gelangen, müssen ökonomisch vertretbare Einführungsstrategien entwickelt werden. Dies heißt im wesentlichen, daß bereits getätigte Investitionen der Post gut ausgenutzt und Neuinvestitionen den finanziellen Rahmen der heutigen Planung nicht allzusehr überschreiten sollten.

Die Einteilung der folgenden Abschnitte orientiert sich an den verwendeten Teilnehmeranschlußleitungen, da deren Austausch teurer zu sein scheint als die Einführung der anderen benötigten Hilfsmittel und damit die Ausbauetappen bestimmen dürfte.

3.2.2.1 Bei Kupferdoppeladern: MIX-Kaskaden

Hier sind selbstverständlich nur schmalbandige Dienste, also vor allem Fernsprechen, zu behandeln.

Wie in 3.1 festgestellt, sind MIXe das einzige in diesem Fall erfolgversprechende Grundverfahren, und die beste Realisierungsform ist nach 3.1.2 das bereits mit der Bandbreite des von der Post geplanten ISDN realisierbare Verfahren der Telefon-MIXe [PfPW_89].

Eine günstigere Realisierung der MIXe und bessere Möglichkeiten zu ihrer späteren Weiterverwendung ergäben sich bei ihrer Errichtung im Fernnetz, wozu aber im Fernnetz und für die Signalisierungskanäle auf den Teilnehmeranschlußleitungen etwas mehr Bandbreite benötigt würde.

3.2.2.2 Verwendung von Koaxialkabelbaumnetzen

Koaxialkabelbaumnetze lassen sich nicht nur zur Verteilung bei Massenkommunikationsdiensten nutzen, auch schmalbandige Individualkommunikation kann darauf bereits nach dem heutigen Stand der Technik durch **Verteilung** und **überlagerndes Senden** geschützt werden.

Dazu muß ein kleiner Teil der Bandbreite digitalisiert und die Verstärker müssen zur Verstärkung in beiden Richtungen erweitert oder ausgetauscht werden. Beides ist im Bereich lokaler Netze seit langem üblich (vgl. WANGNET [Czaa_82, Elek_82]). Digitalisiert man (wie bei WANGNET) 16 Mbit/s in beiden Richtungen, so können etwa 250 Teilnehmer gleichzeitig einen Duplexkanal von 64 kbit/s unterhalten. Bei einer maximalen Telefonnutzung von 10% ergäbe dies beispielsweise eine mögliche Gruppengröße von 2500 Teilnehmern. Da jede Teilnehmerstation auf jeden der Kanäle zugreifen kann und im Durchschnitt erheblich weniger Teilnehmer gleichzeitig „telefonieren", können meist sogar etliche Teilnehmer je einige 64-kbit/s-Kanäle gleichzeitig nutzen.

Zur Realisierung des überlagernden Sendens müssen die Verstärker natürlich um die Additionsfunktion in Richtung der Wurzel des Baumes erweitert werden. Das eigentliche Überlagerungsergebnis kann von der Wurzel des Baumes direkt an das Vermittlungsnetz weitergegeben werden; zumindest die Kontrollinformation für das Zugriffsverfahren (sinnvollerweise eine Version des überlagernden Empfangens) muß jedoch von der Wurzel an die Blätter verteilt werden.

16 Mbit/s ist auch etwa das, was derzeit mit DES-ähnlichen Generatoren überlagert werden kann. Sie können später gemäß dem Stand der Technik gegen sicherere ausgetauscht werden.

Selbst bei Verzicht auf die Überlagerung von Schlüsseln bietet ein Baumnetz bereits einen gewissen physischen Schutz gegen Beobachtung, ähnlich dem RING-Netz. Das implizierte Angreifermodell ist allerdings etwas unrealistischer als das des RING-Netzes.

Eine Kombination mit MIX-Kaskaden im Fernnetz für wesentlich größere Anonymitätsgruppen erscheint sinnvoll.

3.2.2.3 Glasfasern

Bei jeder Neuverkabelung sollten Monomode-Glasfasern verwendet werden. In Neubaugebieten bietet es sich zusätzlich an, sie zur Erhöhung der physischen Unbeobachtbarkeit ringförmig zu verlegen.

Für **schmalbandige** Dienste kann auf den Glasfasern, fast unabhängig von der Topologie, in Anonymitätsgruppen von einigen hundert bis zehntausend Teilnehmern verteilt und überlagernd gesendet werden.

Für **breitbandige** Kommunikation ist diese Kombination zur Zeit jedoch kaum realisierbar. Verteilung zum Schutz des Empfängers ist aber innerhalb von Gruppen von wenigen hundert Teilnehmern bereits möglich. Zumindest wenn sie keine RING-Netze bilden, sollten die kleinen Verteilnetze so organisiert werden, daß sie leicht um überlagerndes Senden erweitert werden können.

Für schmal- und breitbandige Dienste gleichermaßen ist zusätzlicher Schutz durch MIX-Kaskaden möglich, die jeweils den Verkehr aus mehreren Verteilnetzen zusammen mixen. Während der Einführung neuer breitbandiger Dienste kann es sinnvoll sein, eine MIX-Kaskade für einen größeren Einzugsbereich als im Endausbau zu verwenden.

Ein Datenschutz garantierendes Netz in einer mittleren Ausbaustufe ist in Abb. 11 dargestellt.

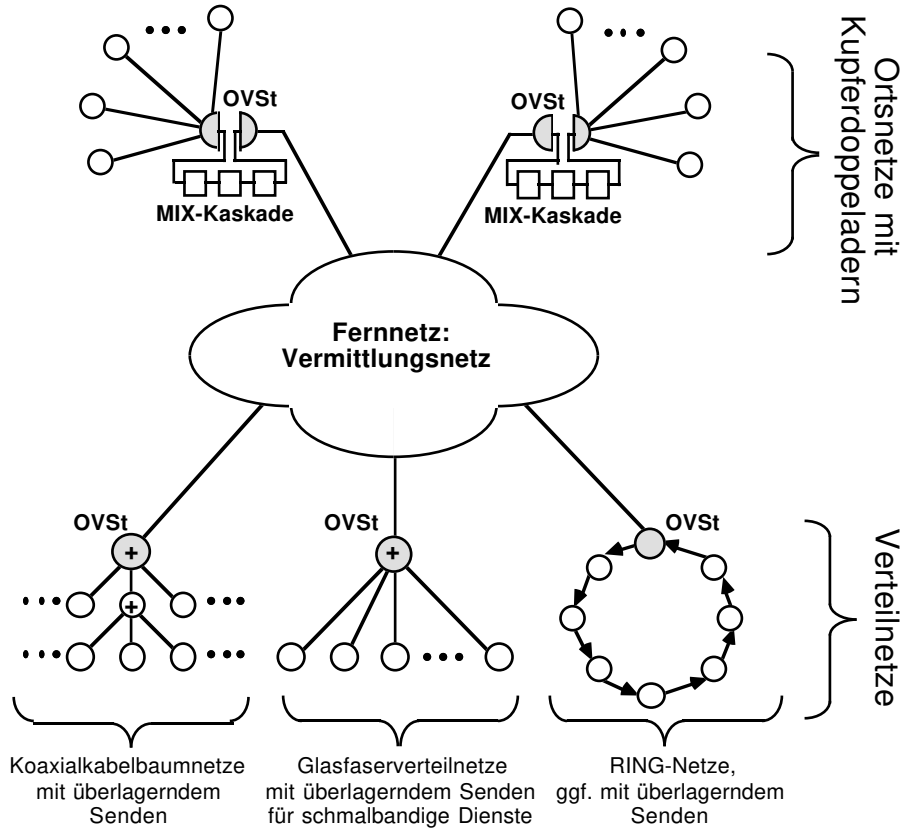


Abb. 11. Integration verschiedener Datenschutzmaßnahmen in einem Netz

3.3 Netzabschluß

Jede Schutzmaßnahme, die innerhalb des Netzes angesiedelt ist, muß durch die Teilnehmerstationen und deren Netzabschlüsse mit realisiert werden. Zur **Teilnehmerstation** zählt man dabei die Teile, die ausschließlich unter Kontrolle der Teilnehmer stehen, während das, wofür die Post verantwortlich ist, zum **Netzabschluß** gerechnet wird.

Sofern die Post weiterhin für die Dienstqualität verantwortlich sein soll, bedeutet dies, daß

- bei Verwendung des RING-Netzes neben dem Netzanschluß auch das Zugriffsverfahren und
- beim überlagernden Senden zusätzlich noch die Pseudozufallszahlenerzeugung

zum Netzabschluß gehören. Wenn diese nämlich bei einem Teilnehmer Leistungs- oder Zuverlässigkeitsmängel aufweisen, sind auch alle anderen Teilnehmer desselben Verteilnetzes betroffen. Wäre im Netzabschluß von der Post oder dem Hersteller ein „Trojanisches Pferd" untergebracht, so könnte dieses also das Senden der betroffenen Station registrieren. Man hat somit dieses Problem von den Vermittlungszentralen auf die Netzabschlüsse verlagert. Dennoch ist die Situation hier besser:

- Netzabschlüsse sind um einige Größenordnungen einfacher als Vermittlungsrechner, so daß eine Prüfung auf „Trojanische Pferde" möglich ist.
- Sie müssen nicht so häufig gewartet werden und können auch nicht so leicht ausgetauscht werden, so daß Kontrollen auf „Trojanische Pferde" nur selten nötig sind.

Um „Trojanische Pferde" ausschließen zu können, müßte man die Netzabschlüsse unter öffentlicher Kontrolle nach geprüften Entwürfen herstellen.

Günstiger als beim RING-Netz und überlagerndem Senden ist die Situation beim MIX-Netz, sofern normale Teilnehmerstationen nicht als MIX fungieren. Da bei ihm die Dienstqualität Unbeteiligter durch „Fehler" anderer Teilnehmer nicht beeinträchtigt wird, kann hier die Datenschutzmaßnahme, nämlich das mehrfache Ver- und Entschlüsseln, ausschließlich in der Teilnehmerstation stattfinden.

3.4 Abrechnung

Ein offenes Kommunikationsnetz muß die Abrechnung der Kosten für die Netzbenutzung mit dem Netzbetreiber ermöglichen. Bei der Organisation der Abrechnung muß einerseits darauf geachtet werden, daß durch Abrechnungsdaten die Anonymität im Netz nicht verloren geht; andererseits müssen die Abrechnungsprotokolle so entworfen werden, daß von vornherein niemand betrügen kann, da die Anonymität eine nachträgliche Strafverfolgung be- oder gar verhindert [WaPf_85, PWP_87].

Zur Abrechnung hat man prinzipiell zwei Möglichkeiten: Abrechnung nach Einzelnutzung oder von allen Netzteilnehmern zu leistende, pauschale Bezahlung.

Eine **Pauschalabrechnung** wird praktikabel, sobald genügend Bandbreite zur Verfügung steht und muß nicht anonym erfolgen, da dabei keine interessanten Abrechnungsdaten entstehen.

Zur **Einzelabrechnung** können entweder **unmanipulierbare Zähler** in den Teilnehmerstationen verwendet werden, die lokal die Gebühren aufsummieren [Pfit_83], oder es kann jeder vom Netz zu übertragenden Nachricht ein digitaler Scheck beigelegt werden, der die Übertragungsgebühren abdeckt (also eine **„digitale Briefmarke"**). Für letzteres gibt es anonyme kryptographische Geldtransfersysteme, die ein Nachbilden herkömmlicher Schecks erlauben [BüPf_86, BüPf_89, Chau_87, Chau_89, PWP_87].

4 Nutzung eines Datenschutz garantierenden Kommunikationsnetzes

Auf einem Datenschutz garantierenden Netz sind beliebige, insbesondere auch alle herkömmlichen nicht anonymen Kommunikationsformen realisierbar.

Fast alle Verfahren, sich über ein Netz einander zu erkennen zu geben (d.h. sich zu **authentisieren**), machen bereits heute keinen Gebrauch davon, daß man dem Netz gegenüber identifizierbar ist. Zum Beispiel erkennt man Telefonpartner an ihrer Stimme und Sprechweise sowie ihrem Wissen, Briefpartner an ihrer (Unter-)Schrift. Entsprechendes gilt für die üblichen Authentikationsprotokolle [DaPr_89], die im wesentlichen auf der Verwendung von Paßwörtern [Lamp_81] und dem Ersetzen der Unterschrift durch eine digitale Signatur [ChRo_91, FiSh_87, GoMR_88, PfWa_91, RSA_78] basieren.

Zahlreiche Anwendungen eines Netzes können jedoch auch in der durch das Kommunikationsnetz ermöglichten vollkommenen Anonymität abgewickelt werden, insbesondere solche, deren Entsprechungen auf herkömmlichen Medien ebenfalls anonym sind, z.B. der Empfang einer Fernsehsendung oder der Kauf einer Zeitung oder eines Lexikonartikels.

Das Problem hierbei ist, wie schon bei der Abrechnung, die Anonymität der Teilnehmer mit der heute (scheinbar) üblichen Rechtssicherheit zu verbinden. Ein allgemeiner Überblick über Lösungen hierzu, insbesondere für anonymen **digitalen Zahlungsverkehr** und darauf aufbauenden **anonymen Werteaustausch**, findet sich in [PWP_87, BüPf_86, BüPf_90]. (Ungelöst ist das, allerdings von der Anonymität unabhängige, Problem des Urheberschutzes: Einmal gekaufte Information kann vom Empfänger beliebig kopiert und an andere Interessierte über das Kommunikationsnetz ohne hohe Kosten weiterverteilt werden [PfPW_86].)

Ein wichtiges Prinzip der oben genannten Lösungen ist die Verwendung verschiedener **digitaler Pseudonyme** mit zugehörigen digitalen Signaturen, an die, wie heute an den Namen, verschiedene Rechte gebunden werden. Es ist dabei auch möglich, ein Recht eines Teilnehmers bzw. eine digital signierte Beglaubigung darüber anonym von einem Pseudonym des Teilnehmers auf ein anderes seiner Pseudonyme zu übertragen [Chau_84, Chau_87], was Möglichkeiten zur Nutzung der Anonymität auch bei manchen Kommunikationsarten eröffnet, bei denen man heute namentlich auftreten muß (z.B. Bürger bei Ämtern).

5 Resümee

Das informationelle Selbstbestimmungsrecht der Bürger, wie es vom BVG im Volkszählungsurteil formuliert wurde, und die in Abschnitt 1.2 aufgezeigten Möglichkeiten der Massenüberwachung, die ein diensteintegrierendes Digitalnetz wie das von der Deutschen Bundespost geplante ISDN bietet, stehen in krassem Widerspruch.

Dieser Widerspruch kann nur durch

- Vermeidung jeglicher nachrichtentechnisch unterstützter offener Kommunikationsnetze (auch des heutigen analogen Telefonnetzes) oder
- Verwendung Datenschutz garantierender Kommunikationsnetze

aufgelöst werden.

In dieser Arbeit wurden die technischen Möglichkeiten dargestellt, den zuletzt genannten Weg zu beschreiten:

Offene Kommunikationsnetze, die auch Verkehrs- und Interessensdaten in überprüfbarer Weise schützen, benötigen auf jeden Fall eine passende physische Netzstruktur: Ohne Verteilnetze im Teilnehmeranschlußbereich scheint ein effizienter Schutz des Empfängers unmöglich zu sein. Dies bedeutet, daß hier Leitungen mit hoher Bandbreite benötigt werden. Verwendet man RING-Netze zum Schutz des Senders, so ist zusätzlich die Topologie des Netzes (Ringe im Teilnehmeranschlußbereich) vorgegeben.

Die Erfordernisse des Schutzes der Verkehrs- und Interessensdaten müssen daher bereits beim Entwurf eines Netzes berücksichtigt werden, eine nachträgliche Einführung eines überprüfbaren Schutzes ist aus Kostengründen schier unmöglich.

Damit ist das Problem, diese Daten zu schützen, in gewissem Sinne dringlicher als die Probleme des Schutzes der Nutzdaten und der Authentikation: Diese lassen sich auf Digitalnetzen beliebiger Struktur notfalls im nachhinein durch kryptographische Verfahren (falls hierfür die notwendigen Standards vorliegen, was leider nicht der Fall ist, vgl. 1.5) lösen, eine willentliche Selbstidentifikation ist stets möglich.

Datenschutz garantierende Netze, die selbst die hohen Leistungsanforderungen an ein Integriertes Breitbandfernmeldenetz (IBFN) erfüllen, sind realisierbar. Die zusätzlichen Kosten sind vertretbar, bei manchen Verfahren ist sogar ein gleich großes Leistung/Kosten-Verhältnis wie für die derzeit geplanten Netze zu erwarten. Eine etappenweise Einführung mit der Zwischenstufe eines Datenschutz garantierenden schmalbandigen ISDN ist etwa mit der gleichen Geschwindigkeit möglich wie die der von der Post geplanten Netze.

Dank: Für ihre Kritik und Diskussionsbereitschaft danken wir Dr. Klaus Echtle, Prof. Winfried Görke, Prof. Herbert Kubicek, Michael Kühn und Prof. Detlef Schmid. Der Deutschen Forschungsgemeinschaft (DFG) danken wir für ihre freundliche Unterstützung.

6 Literatur

Fotokopien von Studien-, Diplomarbeiten sowie Interne Berichte der Universität Karlsruhe sind von der Fakultätsbibliothek Informatik, Universität Karlsruhe, Postfach 6980, W-7500 Karlsruhe 1, Tel. 0721/608-3979, erhältlich.

Abbr_84 C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine 22/9 (1984) 15-21

Agne_91 G. B. Agnew: Editor's Corner; IACR Newsletter, A Publication of the International Association for Cryptologic Research, 8/2 (1991) 1

Aßma_89 R. Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Univ. Karlsruhe, Februar 1989

AT&T_86 AT&T: Einchip-Prozessor zur Verschlüsselung digitaler Signale; Design & Elektronik, Markt & Technik, Ausgabe 21 vom 14. 10. 1986, 8-11

BeEn_85 L. A. Bergman, S. T. Eng: A Synchronous Fiber Optic Ring Local Area Network for Multigigabit/s Mixed-Traffic Communication; IEEE Journal on Selected Areas in Communications SAC-3/6 (1985) 842-848

BfD_85 R. Baumann: Siebter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz; Bundestags-Drucksache 10/2777, Bonn 1985

BiSh_90 E. Biham, A. Shamir: Differential Cryptanalysis of DES-like Cryptosystems; Journal of Cryptology 4/1 (1990) 3-72

BiSh4_91 E. Biham, A. Shamir: Differential Cryptanalysis of the Full 16-round DES; Technical Report Nr. 708, December 1991, Computer Science Department, Technion, Haifa, Israel

BlGo_85 M. Blum, S. Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Proc. of Crypto 84, LNCS 196, Springer-Verlag Heidelberg 1985, 289-299

BoBo_90 J. Bos, B. den Boer: Detection of Disrupters in the DC Protocol; Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 320-327

Bött_89 M. Böttger: Untersuchung der Sicherheit von asymmetrischen Kryptosystemen und MIX-Implementierungen gegen aktive Angriffe; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1989

Bras_88 G. Brassard: Modern Cryptology - A Tutorial; LNCS 325, Springer-Verlag, Berlin 1988

Brau_82 E. Braun: BIGFON - der Start für die Kommunikationstechnik der Zukunft; telcom report 5/2 (1982) 123-129

Brau_83 E. Braun: BIGFON - Erprobung der optischen Breitbandübertragung im Ortsnetz; telcom report 6/2 (1983) 52-53

Brau_87 E. Braun: BIGFON; Informatik-Spektrum 10/4 (1987) 216-217

Bund_83 Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 - 1 BvR 209/83 u. a.; in: Datenschutz und Datensicherung DuD 4 (1984) 258-281

BüPf_86 H. Bürk, A. Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Pre-Prints of the 4th International Conference on Computer Security, Monte Carlo 1986, A. Grissonnanche (ed.), 1986, 250-263

BüPf_89 H. Bürk, A. Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416

BüPf_90 H. Bürk, A. Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721

Bürl_85 G. Bürle: Leistungsbewertung von Vermittlungs-/Verteilnetzen; Diplomarbeit, Univ. Karlsruhe 1985

CACM6_87 General News and Notes: Computer Security Act Stresses Encryption Standard; Communications of the ACM 30/6 (1987) 572

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

Chau_84 D. Chaum: A New Paradigm for Individuals in the Information Age; Proc. of the 1984 Symposium on Security and Privacy, IEEE, Oakland 1984, 99-103

Chau_87 D. Chaum: Sicherheit ohne Identifizierung. Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum 10/5 (1987) 262-277; Datenschutz und Datensicherung DuD /1 (1988) 26-41; Übersetzungen einer Überarbeitung von: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044

Chau_88 D. Chaum: The dining cryptographers problem. Unconditional sender and recipient untraceability; Journal of Cryptology 1/1 (1988) 65-75

Chau_89 D. Chaum: Privacy Protected Payments – Unconditioned Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards, Proceedings of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. 10. 1987, North-Holland, Amsterdam 1989, 69-93.

ChRo_91 D. Chaum, S. Roijakkers: Unconditionally Secure Digital Signatures; Crypto '90, LNCS 537, Springer-Verlag, Berlin 1991, 206-214

Czaa_82 F. R. Czaak: Konzepte eines lokalen Netzwerks; Kommunikationstechnologien, Neue Medien in Bildungswesen, Wirtschaft und Verwaltung, H. Schauer, M. J. Tauber (Hrsg.), Schriftenreihe der Österreichischen Computer Gesellschaft Band 17, R. Oldenbourg Wien 1982, 341-359

DaPr_89 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; (2nd ed.) John Wiley & Sons, New York 1989

Denn_82 D. E. Denning: Cryptography and Data Security; Addison-Wesley, Reading 1982; Reprinted with corrections, January 1983

DES_77 Federal Information Processing Standards Publication 46 (FIPS PUB 46): Specification for the Data Encryption Standard; January 15, 1977

DiHe_76 W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory, IT-22/6 (1976) 644-654

Eck_85 W. van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?; Computers & Security 4/4 (1985) 269-286

EcNi_89 K. Echtle, A. Niedermaier: Eine senderanonyme fehlertolerante Kommunikationsstruktur; 4th GI-GMA-ITG-Fachtagung „Fehlertolerierende Rechensysteme“, IFB 214, Springer-Verlag, Berlin 1989, 283-295

Elek_82 Elektronik Sonderheft Nr. 50, „Daten-Kommunikation”; 8. Teil Einführung in die Datenfernverarbeitung, Lokale Netzwerke - die Basis für integrierte Informations-Systeme; Franzis-Verlag, München 1982, 69-77

FiSh_87 A. Fiat, A. Shamir: How to prove yourself: Practical solutions to identification and signature problems; Proc. of Crypto 86, LNCS 263, Springer-Verlag Heidelberg 1987, 186-194

GoMi_82 S. Goldwasser, S. Micali: Probabilistic Encryption & How to Play Mental Poker Keeping Secret All Partial Information; 14th Symposium on Theory of Computing (STOC) 1982, ACM, New York 1982, 365-377; Überarbeitung in: J. of Computer and System Sciences 28 (1984) 270-299

GoMR_88 S. Goldwasser, S. Micali, R. L. Rivest: A digital signature scheme secure against adaptive chosen-message attacks; SIAM J. Comput. 17/2 (1988) 281-308

GoMT_82 S. Goldwasser, S. Micali, P. Tong: Why and How to establish a Private Code On a Public Network; 23rd Annual Symposium on Foundations of Computer Science, November 3-5, 1982, 134-144

GPBK_88 B. Glance, K. Pollock, C. Burrus, B. Kasper, G. Eisenstein, L. Stulz: WDM Coherent Optical Star Network; Journal of Lightwave Technology 6/1 (1988) 67-72

Höck_85 G. Höckel: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Diplomarbeit, Univ. Karlsruhe 1985

HöPf_85 G. Höckel, A. Pfitzmann: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Proc. der 1. GI Fachtagung Datenschutz und Datensicherung, IFB 113, Springer-Verlag Heidelberg 1985, 113-127

Home_?? Homer: Illias

Horg_85 J. Horgan: Thwarting the information thieves; IEEE Spectrum 22/7 (1985) 30-41

Hors_85 P. Horster: Kryptologie; Reihe Informatik/47, Bibliographisches Institut, Mannheim 1985

Hor2_85 J. Horgan: Inventor seeks to warn Government of threat from laser-based bug; The Institute, IEEE, October (1985) 8

Inge_84 I. Ingemarsson: Critique of the Security of Public-key Systems; 1984 International Zurich Seminar on Digital Communications, IEEE 1984, 171-173

Kais_82 W. Kaiser: Interaktive Breitbandkommunikation – Nutzungsformen und Technik von Systemen mit Rückkanälen; Telecommunications, Veröffentlichungen des Münchner Kreis, Band 8, Springer-Verlag Heidelberg, 1982

KaRS_85 B. S. Kaliski, R. L. Rivest, A. T. Sherman: Is the Data Encryption Standard a Group?; Proc. of Eurocrypt 85, LNCS 219, Springer-Verlag Heidelberg 1986, 81-95; Überarbeitung in Journal of Cryptology 1/1 (1988) 3-36

KrNa_85 F. Kretz, D. Nasse: Digital Television: Transmission and Coding; Proceedings of the IEEE 73/4 (1985) 575-591

Kubi_87 H. Kubicek: Für fernmeldetechnische Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 10/2 (1987) 87-92

KuRo_86 H. Kubicek, A. Rolf: Mikropolis; Mit Computernetzen in die „Informationsgesellschaft"; 2. Auflage, VSA-Verlag Hamburg 1986

Lamp_81 L. Lamport: Password authentication with insecure communication; Communications of the ACM 24/11 (1981) 770-772

Leuz_83 R. Leuze: Datenschutz für unsere Bürger; 4. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz, 1983

Leuz_84 R. Leuze: Datenschutz für unsere Bürger; 5. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz, 1984

Li_87 V. O. K. Li: Multiple Access Communications Networks; IEEE Communications Magazine 25/6 (1987) 41-48

Loep_85 K. Loepere: Resolving covert channels within a B2 class secure system; ACM Operating Systems Review 19/3 (1985) 9-28

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

LuRa_86 M. Luby, C. Rackoff: Pseudo random permutation generators and cryptographic composition; Proc. 18th ACM Symposium on Theory of Computing, New York 1986, 356-363; Überarbeitung: How to construct pseudorandom permutations from pseudorandom functions; SIAM J. Comput. 17/2 (1988) 373-386.

Mann_85 A. Mann: Fehlertoleranz und Datenschutz in Ringnetzen; Diplomarbeit, Univ. Karlsruhe 1985

MaPf_87 A. Mann, A. Pfitzmann: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen; GI-NTG Fachtagung „Kommunikation in verteilten Systemen" 1987, IFB 130, Springer-Verlag Heidelberg 1987, 16-30; Überarbeitung in: Datenschutz und Datensicherung DuD 8 (1987) 393-405

Mass_81 J. L. Massey: Collision-Resolution Algorithms and Random-Access Communications; Multi-User Communication Systems; Edited by G. Longo; CISM Courses and Lectures No. 265; Springer-Verlag Wien, 1981, 73-137

Midw_85 J. E. Midwinter: Current Status of Optical Communications Technology; Journal of Lightwave Technology 3/5 (1985) 927-930

Möhr_87 K. H. Möhrmann: Codierung von Videosignalen für die digitale Übertragung; telcom report, Siemens, 10/6 (1987) 340-345

NeSc_87 R. M. Needham, M. D. Schroeder: Authentication Revisited; ACM Operating Systems Review 21/1 (1987) 7

Nied_87 A. Niedermaier: Bewertung von Zuverlässigkeit und Senderanonymität einer fehlertoleranten Kommunikationsstruktur; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1987

OtRe_87 D. Otway, O. Rees: Efficient and Timely Mutual Authentication; ACM Operating Systems Review 21/1 (1987) 8-10

PeSL_80 M. Pease, R. Shostak, Leslie Lamport: Reaching Agreement in the Presence of Faults; Journal of the ACM 27/2 (1980) 228-234

PfAß_90 A. Pfitzmann, R. Aßmann: More Efficient Software Implementations of (Generalized) DES; Interner Bericht 18/90, Fakultät für Informatik, Univ. Karlsruhe 1990

Pfit_83 A. Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Interner Bericht 18/83 der Fakultät für Informatik, Univ. Karlsruhe 1983

Pfit_85 A. Pfitzmann: How to implement ISDNs without user observability - Some remarks; Interner Bericht 14/85 der Fakultät für Informatik, Univ. Karlsruhe 1985

Pfit_86 A. Pfitzmann: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten?; Datenschutz und Datensicherung DuD 10/6 (1986) 353-359

Pfit_90 A. Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, Dissertation, IFB 234, Springer-Verlag, Heidelberg 1990

Pfit1_90 A. Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14/12 (1990) 620-627

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

PfPW_86 A. Pfitzmann, B. Pfitzmann, M. Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Warum und wie? Datenschutz und Datensicherung DuD 3 (1986) 178-191

PfPW_88 A. Pfitzmann, B. Pfitzmann, M. Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik-Spektrum 11/3 (1988) 118-142

PfPW_89 A. Pfitzmann, B. Pfitzmann, Michael Waidner: Garantierter Datenschutz für zwei 64-kbit/s-Duplexkanäle über den (2•64+16)-kbit/s-Teilnehmeranschluß durch Telefon-MIXe; 4. SAVE-Tagung, 19.-21. April 1989, Köln, 1417-1447; Überarbeitung und Erweiterung in: Datenschutz und Datensicherung 13/12 (1989) 605-622

PfPW_91 A. Pfitzmann, B. Pfitzmann, M. Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead; Proc. Kommunikation in verteilten Systemen, Feb. 1991 Mannheim, Informatik-Fachberichte 267, Springer-Verlag, Heidelberg 1991, 451-463; leicht erweitert in: Proc. IFIP/Sec'91, May 1991, Brighton, North-Holland, Amsterdam 1991, 245-258

PfWa_85 A. Pfitzmann, M. Waidner: Networks without user observability -- design options; Proc. of Eurocrypt 85, LNCS 219, Springer-Verlag Heidelberg 1986, 245-253; Überarbeitung in: Computers & Security 6/2 (1987) 158-166

PfWa_91 B. Pfitzmann, M. Waidner: Fail-stop-Signaturen und ihre Anwendung; Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 289-301

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

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, Edited by R. Bayer, R. M. Graham, G. Seegmüller; LNCS 60, Springer-Verlag Heidelberg 1978; Nachdruck als Springer Study Edition, Springer-Verlag Heidelberg 1979, 209-227

PPfW_87 A. Pfitzmann, B. Pfitzmann, M. Waidner: Weitere Aspekte fernmeldetechnischer Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 11/1 (1988) 5-7

PWP_87 B. Pfitzmann, M. Waidner, A. Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht CR Okt./Nov./Dez. (1987) 712-717, 796-803, 898-904; Überarbeitung und Erweiterung erschien in zwei Teilen in Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315

Rab1_80 M. O. Rabin: Probabilistic Algorithms in Finite Fields; SIAM J. Comput. 9/2 (1980) 273-280

Reis_87 R. Reischuk: Konsistenz und Fehlertoleranz in Verteilten Systemen - Das Problem der Byzantinischen Generäle; 17. GI Jahrestagung, IFB 156, Springer-Verlag, Berlin 1987, 65-81

RiSh_84 R. L. Rivest, A. Shamir: How to Expose an Eavesdropper; Communications of the ACM 27/4 (1984) 393-395

Rose_85 K. H. Rosenbrock: ISDN - Die folgerichtige Weiterentwicklung des digitalisierten Fernsprechnetzes für das künftige Dienstleistungsangebot der Deutschen Bundespost; GI/NTG-Fachtagung „Kommunikation in verteilten Systemen" 1985, IFB 95, Springer-Verlag Heidelberg 1985, 202-221

Ross_87 F. E. Ross: Rings are Round for Good!; IEEE Network 1/1 (1987) 31-38

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126

Schö_84 H. Schön: Die Deutsche Bundespost auf ihrem Weg zum ISDN; Zeitschrift für das Post- und Fernmeldewesen 6 (1984)

Schö_86 H. Schön: ISDN und Ökonomie; Jahrbuch der Deutschen Bundespost 1986, Verlag für Wissenschaft und Leben, Georg Heidecker, Bad Windsheim

ScSc_84 C. Schwarz-Schilling (Hrsg.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Der Bundesminister für das Post- und Fernmeldewesen, Stab 202, Bonn 1984

ScS1_84 C. Schwarz-Schilling (Hrsg.): ISDN - die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Der Bundesminister für das Post- und Fernmeldewesen, Bonn 1984

Sedl_88 H. Sedlak: The RSA Cryptography Processor; Proc. Eurocrypt '87, Amsterdam 1987, LNCS 304, Springer-Verlag Heidelberg 1988, 95-105

SeGo_86 H. Sedlak, U. Golze: Ein Public-Key-Code Kryptographie-Prozessor; Informationstechnik it 28/3 (1986) 157-161

Shan_49 C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal 28/4 (1949) 656-715

Siem_88 SIEMENS: Vermittlungsrechner CP 113 für ISDN, telcom report 11/2 (1988) 80

Steg_85 H. Stegmeier: Einfluß der VLSI auf Kommunikationssysteme; GI/NTG-Fachtagung „Kommunikation in verteilten Systemen" 1985, IFB 95, Springer-Verlag Heidelberg 1985, 663-672

Tane_81 A. S. Tanenbaum: Computer Networks; Prentice-Hall Englewood Cliffs 1981

Thom_84 K. Thompson: Reflections on Trusting Trust; Communications of the ACM 27/8 (1984) 761-763

Thom_87 K. Thomas: Der Weg zur offenen Kommunikation; nachrichten elektronik + telematik (net) special, Sondernummer Oktober 87 (1987) 10-17

VaVa_85 U. V. Vazirani, V. V. Vazirani: Efficient and Secure Pseudo-Random Number Generation (extended abstract); Proc. of Crypto 84, LNCS 196, Springer-Verlag Berlin 1985, 193-202

VoKe_83 V. L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; ACM computing surveys 15/2 (1983) 135-171

Waid_85 M. Waidner: Datenschutz und Betrugssicherheit garantierende Kommunikationsnetze. Systematisierung der Datenschutzmaßnahmen und Ansätze zur Verifikation der Betrugssicherheit; Diplomarbeit, Interner Bericht 19/85 der Fakultät für Informatik, Universität Karlsruhe 1985

Waid_90 M. Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 302-319

Wall_87 P. Wallich: Putting speech recognizers to work; IEEE Spectrum 24/4 (1987) 55-57

WaPf_85 M. Waidner, A. Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; Proc. der 1. GI Fachtagung Datenschutz und Datensicherung 1985, IFB 113, Springer-Verlag Heidelberg, 128-141; Überarbeitung in: Datenschutz und Datensicherung DuD 1 (1986) 16-22

WaPf_89 M. Waidner, B. Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks – Some Remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 5/89, März 1989

WaPP_87 M. Waidner, B. Pfitzmann, A. Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD 6 (1987) 293-299