6 Etappenweiser Ausbau der heutigen Kommunikationsnetze

In den Kapiteln 4 und 5 wurde nur die technisch-ökonomische Realisierbarkeit eines auch breitbandige Dienste ermöglichenden und hochzuverlässigen Kommunikationsnetzes mit (teilnehmer-)überprüfbarem Datenschutz berücksichtigt.

In diesem Kapitel wird ein **etappenweiser Ausbau** der heutigen Kommunikationsnetze zu einem preiswerten und zuverlässigen, zunächst schmalbandigen, später breitbandigen Kommunikationsnetz mit überprüfbarem Datenschutz beschrieben. Dieser Ausbau wird aus ökonomischen Gründen so gestaltet, daß die bereits getätigten Netzinvestitionen (Gebäude, Kabelkanäle, Kabel, Verstärker und Vermittlungsstellen der heutigen Netze) in vollem Umfang genutzt werden. Die Einführung der verschiedenen Dienste kann dabei etwa so schnell erfolgen wie geplant, und es wird stets mehr Datenschutz garantiert als sowohl in der Alternative der Beibehaltung des analogen Fernsprechnetzes als auch bei der Realisierung der in Abschnitt 1.1 beschriebenen Pläne.

Zuallererst muß der Teilnehmeranschluß digitalisiert und Ende-zu-Ende-Verschlüsselung eingeführt werden, was in Abschnitt 6.1 kurz beschrieben wird.

Danach wird in den Abschnitten 6.2 bis 6.4 beschrieben, wie durch alternative Anwendung der Grundverfahren von Kapitel 2 zunächst nur ein **schmalbandiges**, aber auch überprüfbar datengeschütztes Netz entsteht, dessen Nutzübertragungsleistung und Datenschutz mit jeder Ausbauetappe wächst.

In Abschnitt 6.5 wird danach die Gestaltung eines Datenschutz durch Anonymität garantierenden **breitbandigen** diensteintegrierenden Digitalnetzes, also eines möglichen **Endzieles** der Netzentwicklung, beschrieben.

In Abschnitt 6.6 wird beschrieben, inwieweit und wie teilnehmerüberprüfbarer Datenschutz zwischen Teilnehmern in verschieden weit ausgebauten Kommunikationsnetzen möglich ist.

Ähnlich wie sich zu Beginn von Kapitel 5 aus der in Abschnitt 2.6 hergeleiteten Einordnung der Verschlüsselung sowie der Grundverfahren zum Schutz der Verkehrs- und Interessensdaten in das ISO OSI Referenzmodell (Bild 29, 30) eine kanonische Einschränkung der zu betrachtenden Fehlertoleranzverfahren ergab, ergibt sich aus dieser Einordnung auch eine kanonische Einschränkung des bezüglich eines etappenweisen Ausbaus der heutigen Kommunikationsnetze primär zu Betrachtenden:

Von den heutigen Kommunikationsnetzen stellen vor allem die Leitungen sowohl einen schwer zu modifizierenden Teil der Kommunikationsnetze als auch einen beträchtlichen Wert dar. In eingeschränkter Weise gilt dies auch für die bereits installierten Übertragungs- und Vermittlungssysteme, in noch eingeschränkterer Weise für die Entwicklung von Übertragungs- und Vermittlungssystemen. Da es bezüglich Verschlüsselung außer der sowieso vorgesehenen Digitalisierung der Übertragungstechnik keiner Maßnahmen bedarf, ist also gemäß Bild 30 primär zu untersuchen, welche Leitungen

- Verteilung bzw. Kanalselektion (Verteilung),
- Puffern und Umschlüsseln (MIX-Netz),

- Schlüssel und Nachricht überlagern (DC-Netz) oder
- Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung (RING-, BAUM-Netz)

erlauben und ob und ggf. welche Änderungen oder Erweiterungen der bestehenden oder auch nur entwickelten Übertragungs- und Vermittlungstechnik nötig sind.

Die bei einer Realisierung der im folgenden beschriebenen Ausbauetappen auch festzulegende Signalisierung zwischen Teilnehmerstation und Netz, zwischen inneren Netzknoten sowie zwischen Teilnehmerstationen halte ich demgegenüber nur für sekundär interessant:

Einerseits ist sie vergleichsweise flexibel und leicht gestaltbar. Andererseits betrifft die Signalisierung zwischen Teilnehmerstation und Netz bei Verteilung sowie Puffern und Umschlüsseln nur die ohne Rücksicht auf Anonymität realisierbaren Schichten, und bei allen anderen Grundverfahren „nur“ (vgl. Kapitel 5) die Schichten, die die Anonymität erhalten müssen. Letzteres gilt auch für die Signalisierung zwischen Teilnehmerstationen. Die Signalisierung zwischen inneren Netzknoten ist bei allen Ausbauetappen für die Anonymität unkritisch.

6.1 Digitalisierung des Teilnehmeranschlusses und Ende-zu-Ende-Verschlüsselung

In Abschnitt 2.3 wurde beschrieben, wie die Nutzdaten durch Ende-zu-Ende-Verschlüsselung vor Abhörern von Leitungen und sogar den Vermittlungszentralen geschützt werden können. Da beides ohne Verschlüsselung nicht in überprüfbarer Weise möglich ist und Verschlüsselung ohne Digitalisierung des Teilnehmeranschlusses nicht effizient möglich ist, ist die Digitalisierung des Teilnehmeranschlusses ein notwendiger erster Schritt.

Da das dazu Notwendige in Kapitel 2, insbesondere in den Abschnitten 2.2, 2.3.1.2 und 2.6 gesagt wurde, sind hier nur noch ein paar ergänzende Hinweise angebracht:

- Ende-zu-Ende-Verschlüsselung und damit eine Digitalisierung des Teilnehmeranschlusses ist nicht nur zur Lösung des Datenschutzproblems, sondern auch zur Lösung des Sicherheitsproblems nötig, vgl. Abschnitte 1.2, 2.1 und 2.2.1.
- Soweit möglich, sollten die Vermittlungszentralen und Teilnehmeranschlußgeräte nicht frei speicherprogrammierbar, sondern mittels ROMs fest speicherprogrammiert oder in der Form überhaupt nicht programmierbarer Spezialschaltungen realisiert werden, vgl. Abschnitt 2.1.2. Die Forderung nach Digitalisierung bezieht sich also nicht auf die Vermittlung, sondern auf die Übertragung.
- Werden die bereits entwickelten, frei speicherprogrammierbaren Vermittlungszentralen eingesetzt, in denen Trojanische Pferde nicht ausgeschlossen werden können, so sollten die Telefonzellen an eine andere, möglichst noch elektro-mechanische, zumindest aber diversitär entworfene Vermittlungsstelle angeschlossen werden. Dann (und nur dann) können nicht nur die zu Beginn von Kapitel 5 erwähnten physischen Katastrophen oder externen aktiven Angriffe toleriert werden, sondern auch interne aktive Angriffe mittels Trojanischer Pferde (vgl. Abschnitt 2.1.2): ein Trojanisches Pferd kann nämlich nicht nur, wie schon oft erwähnt, die Netzbenutzer beobachten, sondern auch die Dienster-

bringung unterbinden. Bisherige Erfahrungen mit (physischen) Ausfällen von Ortsvermittlungsstellen zeigen, daß dies bereits heute eine schwerwiegende Beeinträchtigung des gesellschaftlichen Lebens im betroffenen Gebiet darstellt. Nimmt – wie allgemein angenommen – die Abhängigkeit von Kommunikationsnetzen zu, so würde eine Gesellschaft von allen am Entwurfsprozeß der Vermittlungszentralen direkt oder indirekt (vgl. Abschnitt 2.1.2) Beteiligten in hohem Maße erpreßbar.

6.2 Schmalbandiges diensteintegrierendes Digitalnetz mit MIX-Kaskaden

Ein schmalbandiges diensteintegrierendes Digitalnetz mit Schutz der Kommunikationsbeziehung durch **MIX-Kaskaden** (MIXe mit fester Durchlaufreihenfolge, was für den Schutz der Kommunikationsbeziehung günstig ist, vgl. Abschnitte 2.5.2.1 und 4.2.3.1) stellt die am schnellsten und vermutlich auch am preiswertesten flächendeckend vorzunehmende Modifikation der heutigen Fernmeldenetze beziehungsweise des für die nächste Zukunft geplanten ISDN dar. Dabei werden die bereits verlegten schmalbandigen Kupferdoppeladern wie geplant nach Austausch der Verstärker etc. digital betrieben, die Vermittlungszentralen können (bezüglich Datenschutz, vgl. letzten Hinweis von Abschnitt 6.1) beliebig modernisiert werden, aber ergänzend zu der Datenschutz vernachlässigenden Planung werden MIXe eingerichtet.

Damit die Nachrichten nicht mehrmals oder auf Umwegen durch das öffentliche Netz laufen müssen, sollte dies entweder bei allen Fernvermittlungsstellen (zur Zeit gibt es in der Bundesrepublik 473 [Schö_86]) oder bei der weitaus größeren Menge aller Ortsvermittlungsstellen (zur Zeit gibt es ca. 6200) geschehen. Um diese MIXe einfacher realisieren und nutzen zu können, sollte es sich bei jeder der gewählten Vermittlungsstellen um eine Gruppe von MIXen handeln, für die eine feste Durchlaufreihenfolge festgelegt ist, sogenannte MIX-Kaskaden, und jede Informationseinheit sollte nur eine (im Fall der Fernvermittlungsstellen) bzw. zwei (im Fall der Ortsvermittlungsstellen) solcher Kaskaden durchlaufen (Bild 76).

Bei der *Wahl der Länge der einzelnen Kaskaden* hat man zwischen Datenschutz und Praktikabilitätsgesichtspunkten abzuwägen. Um etwa Telefon als Dienst mit Realzeitanforderungen ohne spürbare Verzögerung abwickeln zu können, dürfen (selbst bei Schalten anonymer Kanäle vgl. Abschnitt 3.2.2.1) allerhöchstens 640 MIXe durchlaufen werden (vgl. Abschnitt 3.2.2.4 Szenario 2). Je weiter man von dieser Grenze entfernt bleibt, desto geringer dürften wegen der größeren zulässigen Verzögerungszeit pro MIX die Kosten jedes MIXes sein, und natürlich verringert eine geringere Zahl an MIXen sowieso die Gesamtkosten, die über die normalen Fernmeldegebühren auf alle Netzteilnehmer umgelegt werden sollten. Auch die Teilnehmerstationen können bei der Verwendung von weniger MIXen billiger werden, da sie vor dem Senden nicht so oft verschlüsseln müssen. Daneben erlaubt es eine geringe Zahl von MIXen pro Kaskade am ehesten, diese auf separaten Grundstücken von verschiedenen Organisationen (z. B. Parteien, Kirchen, Datenschutzbüros, ...) betreiben zu lassen, wie sich das für MIXe gehört, und dazu auch verschiedene Rechensysteme zu verwenden, um die durch Trojanische Pferde

drohende Gefahr zu verringern. Vom Datenschutz her könnte z. B. die Verwendung von 5 bis 10 MIXen pro Informationseinheit reichen, vgl. Abschnitt 5.3.4.

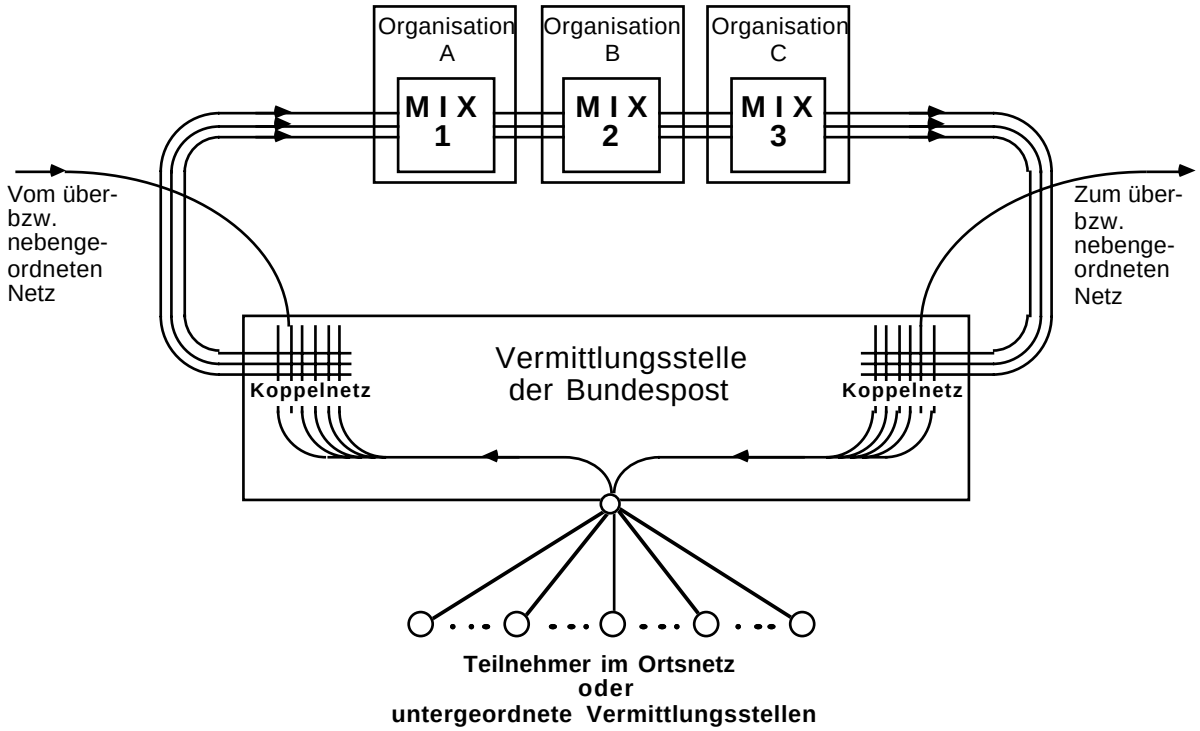

Bild 76: Vermittlungsstelle mit MIX-Kaskade

Bei dieser geringen Zahl von MIXen pro Informationseinheit kann es genügen, die MIXe *intern fehlertolerant* auszulegen, und bei Ausfall eines MIXes und damit seiner Kaskade dies allen Teilnehmerstationen mitzuteilen. Die Teilnehmerstationen unterlassen dann die dieser Kaskade entsprechenden Verschlüsselungen und die Vermittlungsstelle läßt die MIX-Kaskade aus. Bis zur Reparatur des MIXes muß dann entweder auf den Schutz der Kommunikationsbeziehung verzichtet oder eine andere Kaskade durchlaufen werden.

Eine Alternative wäre, den Teilnehmerstationen mitzuteilen, welcher MIX ausgefallen ist, so daß die Teilnehmerstationen nur die ihm entsprechende Verschlüsselung unterlassen. Da die MIXe räumlich benachbart sind, dürfte eine *übertragungstechnische Überbrückung* des ausgefallenen MIXes kein Problem sein – es sei denn, es handelt sich um eine Katastrophe (vgl. den Beginn von Kapitel 5).

Werden die MIX-Kaskaden bei den *Fernvermittlungsstellen* errichtet, um mit einer möglichst geringen Anzahl und damit minimalen Kosten sowie einer möglichst kurzen Einführungszeit bis zu einer effizienten flächendeckenden Datenschutzversorgung auszukommen, müssen aus Datenschutzgründen auch Ortsgespräche zumindest über eine Fernvermittlungsstelle geführt werden. Dadurch entsteht bereits eine nicht unwesentliche Mehrbelastung von Netzteilen, die nur für anteilige Benutzung durch die einzelnen Teilnehmer ausgelegt sind. Trotzdem ist der erreichbare Schutz der Kommunikationsbeziehung zumindest bei längeren Telefongesprächen

unbefriedigend: In Abschnitt 3.2.2.1 wurde darauf hingewiesen, daß jeder MIX die Kommunikationsbeziehung höchstens zwischen zusammen auf- und abgebauten Kanälen verbirgt. Können nun zum Teilnehmer nur sehr wenige Kanäle gleichzeitig unterhalten werden (beim geplanten ISDN sind es für den Privatkunden zwei), so muß er, wenn alle von aus Gründen des Schutzes der Kommunikationsbeziehung noch nicht abbaubaren Kanälen belegt sind, sich entweder in Geduld üben oder den Schutz der Kommunikationsbeziehung für sich und andere abschwächen, indem er einen Kanal „gewaltsam“ wiederbenutzt. Tun dies viele Teilnehmer, so untergräbt dies den Schutz der Kommunikationsbeziehung zumindest für sehr lange telefonierende Teilnehmer vollständig.

Werden die MIX-Kaskaden, um eine Belastung des Fernnetzes durch Ortsgespräche zu vermeiden, bei den *Ortsvermittlungsstellen* errichtet, so sind erheblich mehr erforderlich. Dafür kann in diesem Fall mittels des Verfahrens der **MIXe mit bedeutungslosen Zeitscheibenkanälen und Verteilung der Gesprächswünsche** [PfPW_88] nicht nur obiges Dilemma vermieden und damit die Kommunikationsbeziehung auch bei länger unterhaltenen Kanälen geschützt werden. Es wird sogar das Senden und Empfangen der Teilnehmerstationen geschützt, ohne daß es zu einer Belastung der Netzteile kommt, die nur für anteilige Benutzung durch die einzelnen Teilnehmer ausgelegt sind.

Nach Erkennen obigen Dilemmas könnte man zunächst erwägen, wieder auf das Schalten anonymer Kanäle zu verzichten bzw., da Paketvermittlung zu nicht erträglicher Verzögerung und Datenexpansion führt, Kanalstücke für so kurze Zeitscheiben getrennt zu vermitteln, daß Warten auf ihr Ende nicht stört. Allein hilft dies jedoch nichts, da ein Angreifer statistisch doch merkt, daß es sich um einen Kommunikationsdienst mit längerem, gleichmäßigem Informationsfluß oder notwendiger kurzer Verzögerungszeit handelt, weil sowohl Sender als auch Empfänger genau während der Dauer beispielsweise 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** unterhalten. Damit diese nicht ins Fernnetz gelangen, aber trotzdem nicht von bedeutungsvollen zu unterscheiden sind, müssen sie zwischen Teilnehmerstationen 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 Teilnehmerstationen 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 eine Kennzahl kennen muß. (Dies ist eine Anwendung des Verfahrens des anonymen Abrufs, vgl. Abschnitt 2.5.2.6, das hier ganz besonders effizient ist.)

Zusätzlich muß ein Signalisierungskanal zur Verfügung stehen, auf dem Gesprächswünsche übertragen werden können und die Kennzahlen 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 eigentlichen Kanal auf den Signalisierungskanal verlagert würde. Statt dessen können diese **Gesprächswünsche verteilt** werden, da ihr Informationsgehalt um Größenordnungen geringer ist als der der eigentlichen Fernsprechkanäle. Ein 8-kbit/s-Signalisierungskanal müßte beim derzeitigen Fernsprechverhalten, insbesondere bei Verwendung von Verfahren zur Vermeidung von erfolglosen Wahlwiederholungen, für etwa zehntausend Teilnehmer genügen.

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.

In [PfPW_89] ist das Verfahren der MIXe mit bedeutungslosen Zeitscheibenkanälen und Verteilung der Gesprächswünsche inkl. geeigneter Verfahren zur Vermeidung von erfolglosen Wahlwiederholungen ausführlicher beschrieben.

6.3 Schmalbandiges diensteintegrierendes Digitalnetz mit Verteilung auf Koaxialkabelbaumnetzen

Wo ein schmalbandiges ISDN vorhanden ist oder errichtet werden soll und mit dem **Koaxialkabelbaumnetz** zu ganz anderen Zwecken (Verteilung zusätzlicher Fernsehprogramme) im Teilnehmeranschlußbereich bereits ein breitbandiges Netz errichtet wurde, kann dieses genutzt werden, um auch andere Datenschutzmaßnahmen als MIXe anzuwenden. (Nach [ScS1_86] waren zur Jahresmitte 1986 etwa 20% der bundesdeutschen Haushalte an Breitbandkabelverteilnetze anschließbar, nach [Stan_87] waren es Ende 1986 26% und werden es Ende 1987 34% und Ende 1988 41% sein.)

Am einfachsten zu realisieren ist dabei **Verteilung zum Schutz des Empfängers**. Dazu muß man nur einen kleinen Teil der Bandbreite des Koaxialkabelbaumnetzes digitalisieren.

Wird bei dieser Maßnahme nur Ende-zu-Ende-verschlüsselt, so müssen die Teilnehmerstationen erheblich weniger oft verschlüsseln können als bei der Verwendung von MIXen. Können sie dies aber mindestens halb so oft wie bei der „reinen“ Verwendung von MIXen, so ergänzt sich diese Maßnahme auch gut mit evtl. vorhandenen MIXen in der Ortsvermittlungsstelle des Senders oder in einer Fernvermittlungsstelle.

Mit 32 Mbit/s können etwa 500 Teilnehmer gleichzeitig 64 kbit/s empfangen (z. B. beim Telefonieren), so daß selbst bei Verdopplung der „Telefon“nutzung [HuSW_83, Kais_82 Seite

46] auf maximal 20% gleichzeitig die Information für je 2500 Teilnehmer über ein Koaxialkabelbaumnetz verteilt werden kann. Da verteilte Kanäle ohne Abschwächung der Anonymität des Empfängers und damit auch ohne Abschwächung der Anonymität der Kommunikationsbeziehung zu einem beliebigen Zeitpunkt abgebaut werden können, löst dies zwar das in Abschnitt 6.2 beschriebene Dilemma beim Abbau von anonymen Kanälen durch MIXe.

Weitaus vorteilhafter kann es aber sein, die digitalisierte Bandbreite des Koaxialkabelbaumnetzes zumindest zu einem Teil als Signalisierungskanal beim Verfahren der *MIXe mit bedeutungslosen Zeitscheibenkanälen und Verteilung der Gesprächswünsche* einzusetzen. Ein 32 Mbit/s Signalisierungskanal müßte beim derzeitigen Fernsprechverhalten, insbesondere bei Verwendung von Verfahren zur Vermeidung von erfolglosen Wahlwiederholungen, für „Orts“netze mit 40 Millionen Teilnehmern genügen. Senden und Empfangen der Teilnehmerstationen können damit in (für praktische Zwecke) beliebig großen Ortsnetzen geschützt werden.

6.4 Schmalbandiges diensteintegrierendes Digitalnetz durch anonymes Senden und Verteilung auf Koaxialkabelbaumnetzen

Will man auch das **Senden** statt auf dem üblichen schmalbandigen ISDN **geschützt auf dem Koaxialkabelbaumnetz** durchführen, so hat man die Wahl zwischen dem einfach zu realisierenden BAUM-Netz und dem wesentlich wirkungsvolleren, aber aufwendigeren DC-Netz.

Wie in Abschnitt 3.3.3 beschrieben, ist ein Baumnetz ohnehin eine für überlagerndes Senden geeignete Topologie. Für die ins Auge gefaßte Bandbreite von etwa 16 Mbit/s kann man zu recht hoffen, Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften in wenigen Jahren auf einem Chip implementiert kaufen zu können. Pseudozufallszahlengeneratoren von etwa dieser Geschwindigkeit, allerdings mit umstrittenen Sicherheitseigenschaften (DES), sind schon heute auf einem Chip erhältlich (vgl. Abschnitt 2.2.2.3).

Außerdem kann ein BAUM-Netz um überlagerndes Senden erweitert werden, vgl. Abschnitt 2.5.3.2. Hierzu muß sowohl eine Synchronisation der Teilnehmerstationen nachgerüstet werden (vgl. Abschnitt 4.2.4.2), als auch Schlüsselaustausch, -generierung und Überlagerung.

In allen drei in diesem Abschnitt genannten Fällen (BAUM-Netz, DC-Netz, um überlagerndes Senden erweitertes BAUM-Netz) entsteht damit in beschränkten Netzteilen ein **schmalbandiges Vermittlungs-/Verteilnetz**. Es sollte aber zumindest bei Realisierung der ersten Möglichkeit bei Diensten mit besonders geringen Leistungsanforderungen (z. B. elektronische Post) durch MIXe im Fernnetz ergänzt werden.

6.5 Ausbau zu einem breitbandigen diensteintegrierenden Digitalnetz

Der Ausbau dieses schmalbandigen zu einem **breitbandigen Vermittlungs-/Verteilnetz** sollte je nach Erschließungszustand und Besiedelungsstruktur des zu versorgenden Gebietes erfolgen (Bild 77).

Sind im zu versorgenden Gebiet schon Kabelkanäle vorhanden oder handelt es sich um ein ländliches Gebiet und sind inzwischen genügend schnelle Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften verfügbar, so dürfte es billiger sein, die Verkabelungsstruktur beizubehalten und die Verteilnetze mit überlagerndem Senden zu realisieren, selbst wenn die Pseudozufallszahlengeneratoren noch teuer sind, als die Verkabelungsstruktur zu ändern und RING-Netze als Verteilnetze einzusetzen. Sind im zu versorgenden Gebiet noch keine Kabelkanäle vorhanden und sind noch keine genügend schnellen Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften verfügbar, sollten RING-Netze als Verteilnetze realisiert werden. Trifft keine der obigen Bedingungen zu und besteht unmittelbarer Handlungsbedarf, so sollte trotz erhöhter Kosten ringförmig verkabelt und bei ländlichen Gebieten überlagerndes Senden später nachgerüstet werden.

Im Laufe der Zeit kann der Umfang der durch überlagerndes Senden realisierten Verteilnetze vergrößert werden. Bis die Bundesrepublik vielleicht in sehr ferner Zukunft über ein Verteilnetz mit allen Kommunikationsdiensten versorgt wird (vgl. Abschnitt 4.3), sollten für besonders sensitive und schmalbandige Dienste zur Erhöhung des Datenschutzes über das durch die Verteilnetze bzw. MIX-Kaskaden bei den Ortsvermittlungsstellen gegebene Maß hinaus MIX-Kaskaden bei den Fernvermittlungsstellen benutzt werden.

Dies und die beschriebenen Etappen sprechen dafür, MIX-Kaskaden zunächst bei den Ortsvermittlungsstellen und später entweder zusätzliche bei den Fernvermittlungsstellen zu errichten oder nach Umstellung eines Ortsnetzes von Kupferdoppeladern auf Glasfasern die der Ortsvermittlungsstelle zugeordnete MIX-Kaskade dann einer Fernvermittlungsstelle zuzuordnen. Insbesondere in Großstädten, deren Ortsnetz wegen der hohen Dichte an Anschlüssen, insbesondere Geschäftsanschlüssen, einerseits früh mit digitalen Ortsvermittlungsstellen und andererseits auch früh mit Glasfasern ausgebaut werden soll, kann dies ohne großen Aufwand geschehen, da Großstädte sowohl Orts- als auch Fernvermittlungsstellen besitzen.

Parallel zum beschriebenen Netzausbau bezüglich Nutzleistung muß er auch bezüglich Zuverlässigkeit erfolgen. Dabei werden die in Kapitel 5 beschriebenen Fehlertoleranz-Maßnahmen stetig an Gewicht gewinnen.

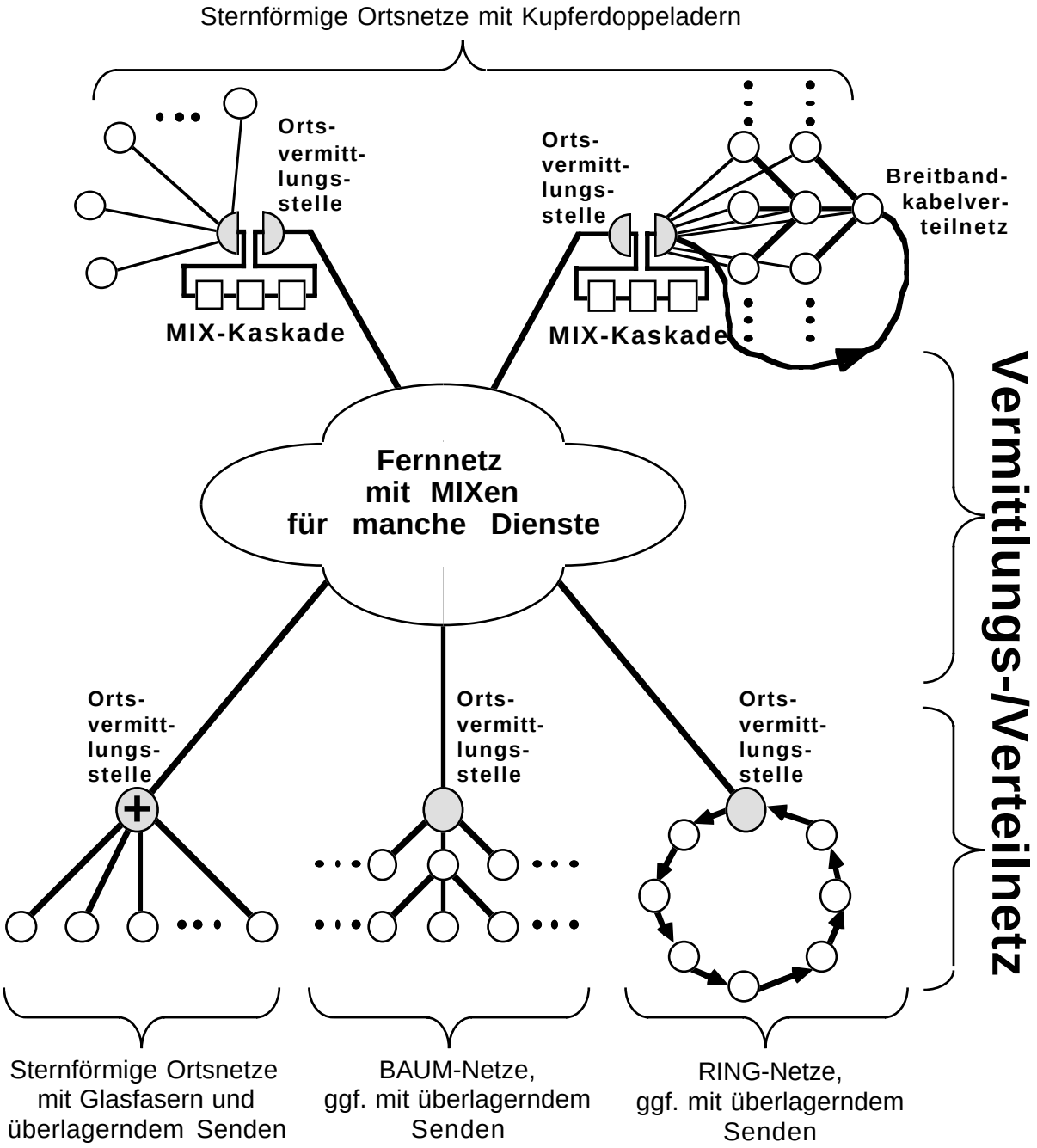

Bild 77: Integration verschiedener Datenschutzmaßnahmen in einem Netz

Zum Schluß sei erwähnt, daß weitgehend unklar ist, wie die *Kosten* bzw. *Effizienz* des beschriebenen Netzausbaus sich zu den des geplanten verhalten.

Selbst für den einfacheren Vergleichsfall, daß außer geräteinterner Fehlertoleranz keine vorgesehen wird, ist ein Vergleich schwierig: einerseits kosten zusätzliche MIXe sicherlich mehr als keine, andererseits könnte die Akzeptanz und damit Benutzung und damit Effizienz eines Kommunikationsnetzes mit MIXen höher sein als die eines ohne MIXe. Ich erwarte insbesondere deshalb eine höhere Effizienz, da etwa 80% der Kosten eines Kommunikationsnetzes

durch die Erdarbeiten bei der Kabelverlegung bestimmt und diese Kosten von der Realisierung der Datenschutzmaßnahmen völlig unabhängig sind. Bei der Ersetzung von Ortsvermittlungsstellen durch ein oder mehrere RING-Netze bei Errichtung eines breitbandigen diensteintegrierenden Digitalnetzes ist nicht einmal klar, wie sich bei neu zu erschließenden Gebieten die Kosten verhalten [Pfi1_85 Seite 33f, Pfi1_83, Bürl_85, Mann_85]:

- Ein RING-Netz mit *n* Stationen benötigt nur *n* Sender und Empfänger, während ein Vermittlungsnetz jeweils 2*n* benötigt. Zwar ist die erforderliche Bandbreite in einem RING-Netz höher, die Kosten der Sender und Empfänger dürften aber über weite Bandbreitenbereiche weitgehend unabhängig von der Bandbreite sein.
- Die gesamte Kabellänge eines RING-Netzes wächst proportional zur Quadratwurzel der Stationsanzahl in einem gegebenen Gebiet. Die gesamte Kabellänge eines Vermittlungsnetzes (Sternnetz ohne Konzentratoren) wächst proportional zur Stationsanzahl. Wie bei Sendern und Empfängern dürften auch bei Kabeln die Kosten über weite Bandbreitenbereiche weitgehend unabhängig von der Bandbreite sein. Die Länge der Kabelkanäle ist bei beiden Netzen näherungsweise gleich.
- Zumindest bezüglich Paket- und Nachrichtenvermittlung ist das Bitübertragungsnetz eines RING-Netzes ein breiterer Flaschenhals als eine übliche Vermittlungszentrale.

Bei geräteexterner Fehlertoleranz, insbesondere eines redundanten Übertragungssystems auch im Teilnehmeranschlußbereich ist ein Kostenvergleich noch schwieriger, zumal hierfür keine Planungen vorliegen.

In beiden Fällen wären weitergehende Untersuchungen wünschenswert. Leider sind sie wohl nur vom Netzbetreiber und dessen Lieferanten durchführbar, da an anderer Stelle die wirklichen Kosten aus politischen oder Wettbewerbsgründen nicht vorliegen.

6.6 Teilnehmerüberprüfbarer Datenschutz bei Kommunikation zwischen Teilnehmern in verschieden weit ausgebauten Kommunikationsnetzen

Als Schluß dieses Kapitels bleibt die Frage zu beantworten, inwieweit und wie teilnehmerüberprüfbarer Datenschutz zwischen Teilnehmern in verschieden weit ausgebauten Kommunikationsnetzen möglich ist.

Ist der Teilnehmeranschluß eines der Teilnehmer nicht digitalisiert, so kann mit ihm (außer für Kommunikationsdienste mit sehr geringen Durchsatzforderungen) nicht Ende-zu-Ende-verschlüsselt kommuniziert werden. Insbesondere bei längeren, d. h. über viele Vermittlungszentralen (oder gar Länder) geführten Verbindungen oder solchen, die über nicht Verbindungs-verschlüsselte Funk- oder Satellitenstrecken geführt sind, ist es lohnend, eine möglichst weite Strecke Ende-zu-„Ende“ zu verschlüsseln (Bild 78).

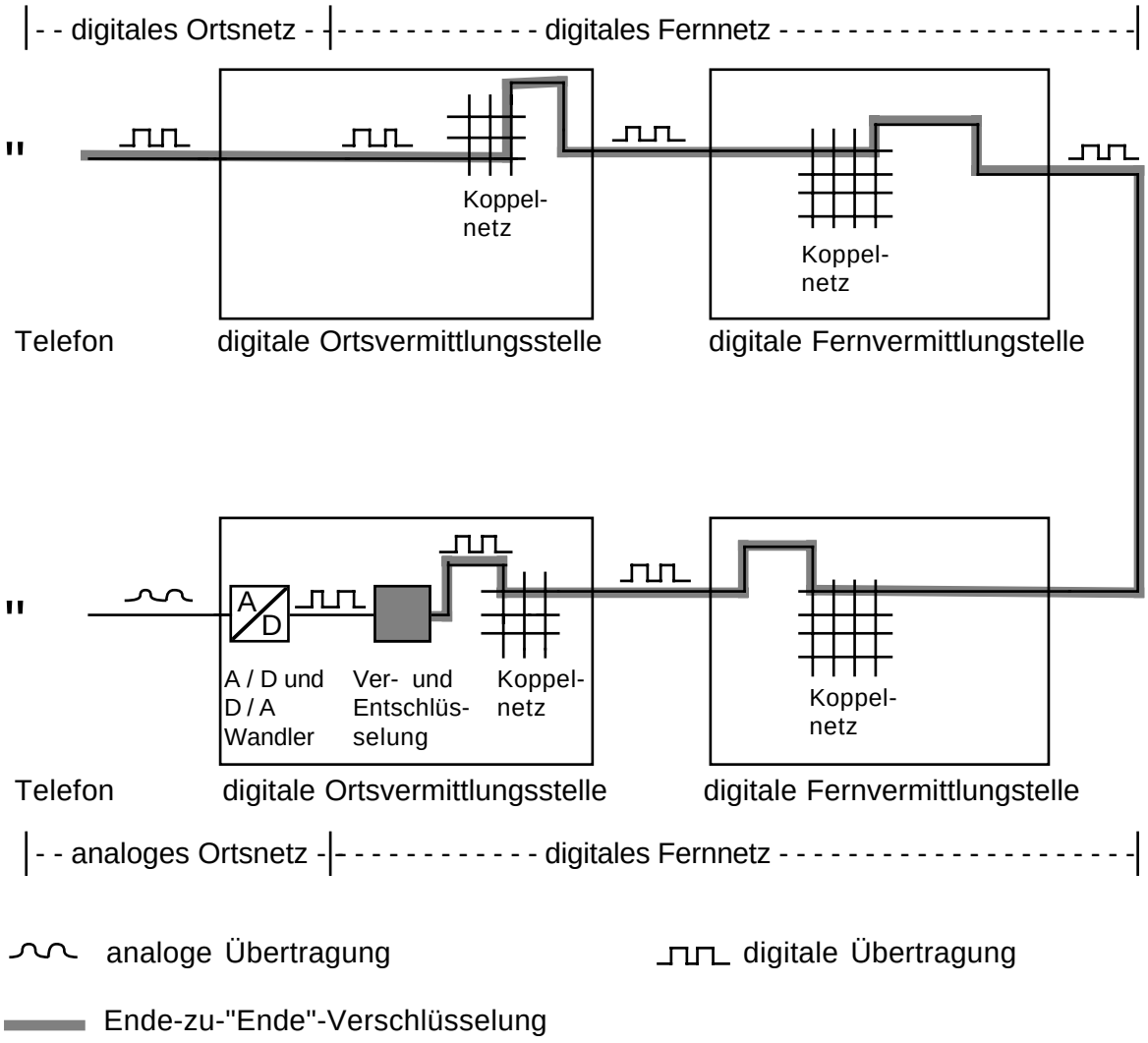

Bild 78: Ende-zu-„Ende“-Verschlüsselung zwischen einem Teilnehmer mit digitalisiertem und einem mit analogem Anschluß

Entsprechend wie bei Ende-zu-„Ende“-Verschlüsselung kann bezüglich MIXen verfahren werden, wenn der Anschlußbereich einer Teilnehmerstation entweder noch gar nicht digitalisiert ist oder die Teilnehmerstation die Zahl der Verschlüsselungen nicht bewältigen kann.

Die Realisierung von lokalen BAUM-, RING-, DC-Netzen oder Kombinationen schützt auch dann die Kommunikation der in diesen Netzen liegenden Stationen, wenn mit Stationen kommuniziert wird, die nicht in einem solchen Verteilnetz eines Vermittlungs-/Verteilnetzes liegen. Kann die Teilnehmerstation des Kommunikationspartners nach der Kontaktaufnahme nicht ständig neue offene implizite Adressen generieren, so muß die in diesen lokalen Verteilnetzen liegende Station dem Partner immer neue zusenden. Dies nützt natürlich nur dann viel, wenn zwischen beiden Partnern Ende-zu-Ende-verschlüsselt werden kann und wird.

7 Netzmanagement

In diesem Kapitel wird zunächst in Abschnitt 7.1 diskutiert, wer welche Teile des Kommunikationsnetzes (errichten sowie) betreiben und entsprechend die Verantwortung für die Dienstqualität übernehmen sollte.

Danach wird in Abschnitt 7.2 skizziert, wie eine Abrechnung der Kosten für die Benutzung des Kommunikationsnetzes mit dem Betreiber ohne Untergrabung des Datenschutzes sicher und komfortabel erfolgen kann.

Die Bezahlung von über das Kommunikationsnetz erbrachten (höheren) Diensten kann mittels eines beliebigen digitalen Zahlungssystems erfolgen, was in Abschnitt 8.1 erläutert wird. Digitale Zahlungssysteme stellen spezielle Transaktionsprotokolle dar, über die in Kapitel 8 ein kurzer Überblick gegeben wird.

7.1 Netzbetreiberschaft: Verantwortung für die Dienstqualität vs. Bedrohung durch Trojanische Pferde

Bezüglich Netzbetreiberschaft und Verantwortung für die Dienstqualität besteht folgendes Dilemma [Pfi1_85 Seite 129]:

Verwendet jeder eine beliebige **Teilnehmerstation** (was man sich bis hierher, da nichts anderes explizit gesagt wurde, vermutlich vorgestellt hat), so wird keine Organisation willens und in der Lage sein, die Verantwortung für die Dienstqualität, d. h. die von den Teilnehmern wahrnehmbare Nutzleistung und Zuverlässigkeit, zu übernehmen. Dies gilt zumindest dann, wenn fehlerhaftes Verhalten oder ungenügende Leistung einer Teilnehmerstation die Dienstqualität für andere Teilnehmer auch dann beeinträchtigen können, wenn diese anderen Teilnehmer nicht gerade mit dieser fehlerhaften oder ungenügend leistungsfähigen Teilnehmerstation kommunizieren wollen (weswegen ab Abschnitt 2.5 nicht mehr von Netzbenutzern, sondern von Netzteilnehmern gesprochen wurde). Ein solches „anarchisch-liberales“ Netzmanagement ist zwar für die (Teilnehmer-)Überprüfbarkeit des Datenschutzes optimal, wegen seiner unkalkulierbaren Dienstqualität aber nur für spezielle Anwendungen, keinesfalls aber für dienste-integrierende Kommunikationsnetze geeignet. Es kann natürlich auf einem beliebigen Kommunikationsnetz um den Preis geringer Kosten-Effizienz, geringer Nutzleistung, geringer Zuverlässigkeit und, vielleicht, großen Mißtrauens durch den Rest der Gesellschaft, was seine Teilnehmer wohl zu verbergen haben, errichtet und betrieben werden.

Entwirft, produziert, errichtet und betreibt eine Organisation andererseits sämtliche Netzkomponenten, insbesondere auch die Teilnehmerstationen, so wird diese Organisation zwar willens und in der Lage sein, die Verantwortung für die Dienstqualität zu übernehmen. Aber niemand, insbesondere kein Teilnehmer, kann ausschließen, daß Teile solch einer Organisation irgendwo Trojanische Pferde installieren, vgl. Abschnitt 2.1.2. Solch eine Organisation wäre also bezüglich (Sicherheit und) Datenschutz nicht kontrollierbar.

Da jede Schutzmaßnahme, die innerhalb des Kommunikationsnetzes angesiedelt ist, durch die Teilnehmerstationen realisiert (oder mit realisiert, z. B. MIXe) werden muß, ist es zur Verkleinerung dieses Dilemmas sinnvoll, die Teilnehmerstation bezüglich Entwurf, Produktion, Installation und Betreiberschaft geeignet in zwei Teile zu zerlegen: Das (bzw. die) Teilnehmerendgerät(e) und den Netzabschluß.

Zum **Teilnehmerendgerät** zählen dabei die Teile der Teilnehmerstation, die mit der Kommunikation mit anderen und der anderen Teilnehmerstationen nichts zu tun haben. Folglich kann das Teilnehmerendgerät ausschließlich unter der Kontrolle des einzelnen Teilnehmers stehen.

Zum **Netzabschluß** zählen all die Teile der Teilnehmerstation, die mit der Kommunikation mit anderen oder der anderen Teilnehmerstationen zu tun haben. Folglich ist der Betreiber des Kommunikationsnetzes für den Netzabschluß verantwortlich.

Beispielsweise wird von CCITT bei X.25 das Teilnehmerendgerät DTE (Data Terminal Equipment) und der Netzabschluß DCE (Data Circuit-terminating Equipment) genannt [Tane_81, Tane_88], bei ISDN heißt das Teilnehmerendgerät TE (Terminal Equipment) und der Netzabschluß NT (Network Termination) [ITG_87, Tane_88].

Sofern es einen Netzbetreiber geben und dieser für die Dienstqualität verantwortlich sein soll, so sollte aus Gründen der Überprüfbarkeit (der Sicherheit und) des Datenschutzes der Funktionsumfang der Netzabschlüsse möglichst klein sein, damit ihr Entwurf, ihre Produktion, ihre Installation und ihr Betrieb möglichst rigoros öffentlich überprüft werden können. Damit sollte es auch bezüglich der Überprüfbarkeit von Datenschutz akzeptabel sein, daß ein oder wenige Lieferanten die Netzabschlüsse liefern, und die Qualität ihrer Produkte vom Netzbetreiber anerkannt wird. Die Lieferanten haben ihre Entwürfe inkl. aller Entwurfshilfsmittel und Entwurfskriterien zu veröffentlichen. Konsumenten- oder Bürgervereinigungen wie beispielsweise die „Stiftung Warentest“ sollten in den Netzabschlüssen (wie auch in den Teilnehmerendgeräten) kontinuierlich nach Trojanischen Pferden suchen. Dies ist hauptsächlich zu Beginn aufwendig, wenn die Entwurfshilfsmittel und vor allem die Entwürfe überprüft werden müssen. Die Kontrolle der unveränderten Produktion dürfte wesentlich einfacher sein.

Netzabschlüsse dürften nur wenige integrierte digitale Schaltkreise und analoge Sender- und Empfänger-Bausteine umfassen. Entsprechend sollte Wartung bzw. Reparatur (und anschließende Überprüfung) selten sein. Insbesondere besteht keine Notwendigkeit für *Fernwartung*, d. h. die Fähigkeit des Herstellers oder Netzbetreibers, die Software des Netzabschlusses per Zugriff über das Kommunikationsnetz modifizieren zu können, wie dies bei den heutigen Vermittlungszentralen vorgesehen (und wegen bei der Auslieferung noch nicht gefundenen, geschweige denn korrigierten Entwurfsfehlern oder einer großen Zahl möglicher Hardwareausfälle) wohl auch nötig ist. Wie in Abschnitt 1.2 erläutert wurde, können Hersteller mittels Fernwartung Trojanische Pferde beliebig installieren und die von ihnen eingebauten beliebig beseitigen. Dies gilt dann nicht, wenn Fernwartung nur in der sehr eingeschränkten Form der *Fernabfrage* möglich ist: Hierbei können per Zugriff über das Kommunikationsnetz keine Programme modifiziert, sondern nur vor Ort vorhandene Diagnoseprogramme gestartet und ihre Ergebnisse entgegengenommen werden. Der Zweck der Fernabfrage ist, daß ein Wartungstechniker gezielt Ersatzteile mitnehmen kann. Sicherzustellen, daß Fernwartung auf Fernabfrage

beschränkt ist, ist allerdings das bereits in den Abschnitten 1.2 und 2.1.2 dargestellte Problem des Ausschließens Trojanischer Pferde.

In den folgenden Unterabschnitten wird beschrieben, welchen Funktionsumfang die Netzabschlüsse bei den verschiedenen Grundverfahren zum Schutz der Verkehrs- und Interessensdaten aufweisen müssen.

7.1.1 Ende-zu-Ende-Verschlüsselung und Verteilung

Da eine Teilnehmerstation bei fehlerhafter Ende-zu-Ende-Ver- bzw. -Entschlüsselung, fehlerhafter Generierung oder Erkennung impliziter Adressen oder fehlerhaftem Empfang verteilter Informationseinheiten nur die Dienstqualität ihres Teilnehmers und die seiner direkten Kommunikationspartner beeinträchtigt, kann all dies im Teilnehmerendgerät abgewickelt werden.

7.1.2 MIX-Netz

Werden MIXe von normalen Netzteilnehmern betrieben, so umfaßt der Netzabschluß eine (kleine) Vermittlungszentrale und eine größere Zahl von sehr leistungsfähigen Ver- und Entschlüsselungsgeräten sowie alle Maßnahmen zur Fehlertoleranz. Wie in Abschnitt 2.5.2.7 erwähnt, kann dann versucht werden, mittels MIXen nicht nur die Kommunikationsbeziehung, sondern auch das Senden und Empfangen von Teilnehmerstationen zu schützen. Neben den aus Abschnitt 3.2.2.4 ersichtlichen Schwierigkeiten, daß dann entweder sehr viele bedeutungslose Informationseinheiten erzeugt oder lange Wartezeiten hingenommen werden müssen, sei darauf hingewiesen, daß dieser sehr umfangreiche Netzabschluß das Senden und Empfangen (nicht aber die Kommunikationsbeziehungen) einer Teilnehmerstation kanonischerweise beobachten kann. Der geschilderte Versuch ist also nicht nur sehr aufwendig und unkomfortabel, sondern sein Erfolg auch höchst ungewiß.

Die Vermittlungsfunktion der MIXe kann zwar weitgehend eliminiert werden, indem die MIXe jeweils in fester Reihenfolge durchlaufen werden müssen (vgl. Abschnitte 2.5.2.1 und 4.2.3.1). Aber auch für den Rest kann Wartung oder Reparatur öfter nötig sein als dies für in privaten Räumen untergebrachte Geräte akzeptabel, geschweige denn wünschenswert ist.

Die Wartungs- und Reparatur-Situation ist völlig unproblematisch, sofern, wie beispielsweise in Abschnitt 6.2 beschrieben, normale Teilnehmerstationen nicht als MIX fungieren.

Da beim MIX-Netz die Dienstqualität Unbeteiligter durch „Fehler“ anderer Teilnehmer, die keine MIX-Funktion realisieren oder deren MIX-Funktion vom Fehler nicht betroffen ist, nicht beeinträchtigt wird, kann die den einzelnen Teilnehmer schützende Maßnahme, nämlich das mehrfache Ver- und Entschlüsseln, ausschließlich im Teilnehmerendgerät stattfinden. Mit dem in Abschnitt 6.2 beschriebenen Verfahren der MIXe mit bedeutungslosen Zeitscheibenkanälen und Verteilung der Gesprächswünsche kann also Senden und Empfangen mit erheblich besserer Aussicht auf Erfolg geschützt werden als mit dem in Abschnitt 2.5.2.7 beschriebenen Verfahren, bei dem jede Teilnehmerstation als MIX fungiert.

Für den Fall eines umfangreichen öffentlichen MIX-Netzes ist es noch wichtiger als bei lokalen oder Spezialnetzen, daß die kryptographische Stärke der verwendeten Kryptosysteme auch für diesen Anwendungszweck öffentlich bewiesen oder zumindest validiert ist (vgl. Abschnitte 2.2.2.2 und 2.5.2.8). Mir sind keine Beweise für praktisch einsetzbare MIX-Netze mit mehr als einem MIX pro Kommunikationsbeziehung zum Schutz des Senders- oder Empfängers bekannt, vgl. [Bött_89].

7.1.3 DC-Netz

Der Netzabschluß des DC-Netzes muß neben dem physischen Netzanschluß die Pseudozufallszahlengenerierung, das Zugriffsverfahren und auch alle vorgesehenen Fehlertoleranz-Maßnahmen umfassen. Denn sofern diese Funktionen bei einem Teilnehmer Leistungs- oder Zuverlässigkeitsmängel aufweisen, sind auch alle anderen Teilnehmer des DC-Netzes betroffen.

Ist im Netzabschluß vom Netzbetreiber oder dem Hersteller ein Trojanisches Pferd untergebracht, so kann dieses also das Senden der betroffenen Station registrieren, wodurch die Schutzwirkung des überlagernden Sendens vollständig verloren geht. Das Problem Trojanischer Pferde wurde somit von den Vermittlungszentralen auf die Netzabschlüsse verlagert. Dennoch ist, wie in Abschnitt 7.1 bereits begründet, die Situation hier erheblich besser, da Netzabschlüsse um einige Größenordnungen einfacher als Vermittlungsrechner sind und damit eine Prüfung auf Trojanische Pferde viel leichter möglich und wegen seltenerer Wartung bzw. Reparatur auch weniger häufig durchzuführen ist.

Bei modularem Aufbau des Netzabschlusses gemäß der Schichtung von Bild 30 sind zusätzlich die Module, die den physischen Netzanschluß darstellen (Medium und untere Teilschicht der Schicht 1), gemäß dem Angreifermodells des DC-Netzes bezüglich Datenschutz unkritisch. Hier darf, wer immer will, passiv angreifen. Selbst aktive Angriffe in diesen Modulen schwächen bei geeigneter Implementierung (vgl. die Anmerkungen in den Abschnitten 2.5.1 und 2.5.3.1.2) nicht die Anonymität ab, sondern verhindern nur die Diensterbringung. Geeignete Protokolle zur Fehler- bzw. Angriffsdiagnose sind in den Abschnitten 5.4 und 5.8 sowie [WaPf_89, WaPf1_89] beschrieben.

Für den Fall eines umfangreichen öffentlichen DC-Netzes mit einem Netzbetreiber ist es noch wichtiger als bei lokalen oder Spezialnetzen, daß die kryptographische Stärke der Pseudozufallszahlengenerierung öffentlich bewiesen oder zumindest validiert ist (vgl. Abschnitt 2.2.2.2). Anderenfalls kann die Pseudozufallszahlengenerierung eine verborgene Falltür (trapdoor) enthalten, die es dem Netzbetreiber oder -entwerfer ermöglicht, das Senden der Teilnehmerstationen zu beobachten. Oder die Pseudozufallszahlengenerierung wird einige Monate oder Jahre, nachdem sie für dieses umfangreiche DC-Netz ein De-facto-Standard geworden und nur noch unter sehr hohen Kosten zu ändern ist, gebrochen.

7.1.4 RING- und BAUM-Netz

Der Netzabschluß des RING- bzw. BAUM-Netzes muß neben dem physischen Netzanschluß mit digitaler Signalregenerierung, das Zugriffsverfahren und auch alle vorgesehenen Fehlertole-

ranz-Maßnahmen umfassen. Denn sofern diese Funktionen bei einem Teilnehmer Leistungs- oder Zuverlässigkeitsmängel aufweisen, sind auch alle anderen Teilnehmer des RING- bzw. BAUM-Netzes betroffen.

Ist im Netzabschluß vom Netzbetreiber oder dem Hersteller ein Trojanisches Pferd untergebracht, so kann dieses also das Senden der betroffenen Station registrieren, wodurch die Schutzwirkung von Übertragungstopologie und digitaler Signalregenerierung für die Sender vollständig verloren geht. Wie beim DC-Netz wurde somit das Problem Trojanischer Pferde von den Vermittlungszentralen auf die Netzabschlüsse verlagert. Wie in Abschnitt 7.1.3 ist aber die Situation dadurch erheblich besser geworden, denn der Netzabschluß des RING- bzw. BAUM-Netzes besitzt einen noch kleineren Funktionsumfang. Es sei noch erwähnt, daß es beim RING- oder BAUM-Netz zwar insgesamt nur geringeren Schutz des Senders als beim DC-Netz gibt – dafür sind aber, da die Beweise ohne irgendwelche unbewiesenen Annahmen geführt werden konnten, keine negativen Überraschungen möglich!

7.1.5 Kombinationen sowie heterogene Netze

Werden – wie etwa in Abschnitt 2.5.3.2 beschrieben – mehrere Grundverfahren zum Schutz der Verkehrs- und Interessensdaten kombiniert, so ist es bezüglich der Überprüfbarkeit des Datenschutzes günstig, nicht einen Netzabschluß mit der Vereinigungsmenge aller notwendigen Funktionen zu realisieren, sondern eine Kaskadierung der für die einzelnen Verfahren nötigen Netzabschlüsse entsprechend der Schichtung gemäß Abschnitt 2.6 vorzunehmen. Dann kann ein in einem vom Teilnehmerendgerät weit entfernter, einer niedrigen Schicht entsprechender Netzabschluß mit Trojanischem Pferd das Kommunikationsverhalten einer Teilnehmerstation nur wenig beobachten.

Entsprechendes gilt für die in Abschnitt 4.2 beschrieben heterogenen Kommunikationsnetze. Bei ihnen kann es beispielsweise durchaus lohnend sein, einen Teil der Bandbreite „anarchisch-liberal“ zu verwalten, vgl. Abschnitt 7.1.

7.1.6 Verbundene, insbesondere hierarchische Netze

Werden die Übergänge zwischen den Netzen bzw. Netzebenen und ggf. die von allen Teilnetzen hin und wieder benötigten oberen Netzebenen so realisiert, daß eine Gruppe von Betreibern die Verantwortung für die Dienstqualität dieser Netzteile übernehmen kann, so können die restlichen Netzteile beliebig realisiert werden. Netzbetreiberschaft und Verantwortung für die Dienstqualität können also in unterschiedlichen Netzteilen so gut wie unabhängig voneinander geregelt werden.

7.2 Abrechnung

Bei einem offenen Kommunikationsnetz muß ggf. eine komfortable und sichere Abrechnung der Kosten für die Netzbenutzung mit dem Netzbetreiber möglich sein. Bei der Organisation der Abrechnung muß darauf geachtet werden, daß durch Abrechnungsdaten die Anonymität, Unbeobachtbarkeit und Unverkettbarkeit im Kommunikationsnetz nicht verloren geht.

Prinzipiell hat man dabei zwei Möglichkeiten: **Individuelle** Abrechnung nach Einzelnutzung (oder auch für Abonnements u. ä.) mit Verfahren, bei denen der bezahlende Teilnehmer anonym ist oder **generelle**, d. h. von allen Netzteilnehmern zu leistende, pauschale Bezahlung, die nicht anonym erfolgen muß, da dabei keine interessanten Abrechnungsdaten entstehen.

Für individuelle Abrechnung können entweder
- nicht manipulierbare Zähler [Pfi1_83 Seite 36f] oder
- anonyme digitale Zahlungssysteme (siehe Abschnitt 8.1),

verwendet werden.

Die **nicht manipulierbaren Zähler** werden zweckmäßigerweise im Netzabschluß untergebracht. Sie entsprechen in ihrer Funktion den heutigen Elektrizitätszählern, nur daß sie über das Kommunikationsnetz ausgelesen werden können. Sind die Zähler technisch so gestaltet, daß dieses Auslesen nur in großen Zeitintervallen, z. B. alle Monate einmal, geschehen kann, so geben diese Zähler nur sehr wenig personenbezogene Information ab, so daß zwischen Netzbetreiber und Teilnehmern über deren Zählerstände nichtanonym abgerechnet werden kann.

Hauptvorteil dieser Lösung ist, daß im Kommunikationsnetz so gut wie kein Aufwand für Abrechnungszwecke getrieben werden muß. Hauptnachteile sind, daß ein Umgehen des Zählers durch Umgehen des Netzabschlusses genauso verhindert oder zumindest entdeckt werden muß wie eine Manipulation am Zählerstand. Beide Nachteile sind allerdings nicht sehr schwerwiegend, da (im Gegensatz zu allgemein verwendeten Zahlungsmitteln, vgl. Abschnitt 8.1) mit diesen Zählern nur die Bezahlung einer einzigen Dienstleistung von – zumindest bei Privatleuten – üblicherweise eher geringfügigem Wert möglich ist. Auch heute sind Briefmarken wesentlich leichter zu fälschen als Geldscheine.

Bei Verwendung von anonymen digitalen Zahlungssystemen müssen die genauen Abrechnungsprotokolle so entworfen werden, daß von vornherein niemand betrügen kann, da bei ihnen die Anonymität, Unbeobachtbarkeit und Unverkettbarkeit eine nachträgliche Strafverfolgung generell be- oder gar verhindert [WaPf_85, PWP_87, BüPf_86]. Dies ist beim Abrechnungsproblem der Netznutzung sehr einfach zu erreichen: der ersten aller verkettbaren Informationseinheiten wird jeweils ein digitales, d. h. durch eine binäre Nachricht repräsentiertes Zahlungsmittel vorangestellt. Den Wert dieser „**digitalen Briefmarke**“ läßt sich der Netzbetreiber gutschreiben, bevor er die verkettbaren Informationseinheiten weiterbefördert.

Selbst bei lokaler Kommunikation in DC-, RING-2-f- bzw. BAUM-Netzen kann der Netzbetreiber unfrankierte Nachrichten unterdrücken, wenn er die globale Überlagerung durchführt, den Schlüssel überlagert bzw. die Wurzel des Baumes kontrolliert. Beim RING-Netz kann er

dies nicht immer. Allerdings kann bei zwei Ringteilnehmern *A* und *B* entweder nur *A* unentgeltlich an *B* senden oder *B* an *A*. Kosten in einem Übertragungsrahmen realisierte Duplex-Kanäle genauso viel wie ein ebenfalls in einem Übertragungsrahmen realisierter Simplex-Kanal, so kann zumindest bei Diensten, die einen Duplex-Kanal erfordern, eine Dienstleistung nicht ohne Bezahlung erlangt werden, vgl. Abschnitt 3.1.4.3.

Hauptvorteil dieses Verfahrens der „digitalen Briefmarken“ ist, daß es ohne nicht umgehbare und nicht manipulierbare Zähler auskommt und bei einem „guten“ anonymen Zahlungssystem keinerlei personenbezogene Information anfällt. Hauptnachteil ist der nötige Kommunikationsaufwand. Um ihn erträglich zu halten und insbesondere die Verzögerungszeit kurz, sollte der Netzbetreiber die Funktion der Bank im digitalen Zahlungssystem übernehmen, vgl. Abschnitt 8.1.

Wünscht der Teilnehmer einen Einzelgebührennachweis, so kann ihm (und nur ihm!) dies je nach Funktionsverteilung entweder das Teilnehmerendgerät oder der Netzabschluß erstellen.

Durch Verwendung von generellen Pauschalen vermeidet man alle Probleme bezüglich Betrugssicherheit und fast den gesamten Aufwand des Abrechnungsverfahrens.

Sobald genügend Bandbreite zur Verfügung steht, ist z. B. eine pauschale Gebühr an den Netzbetreiber für schmalbandiges Senden und Fernsehempfang möglich.

8 Nutzung von Kommunikationsnetzen mit teilnehmerüberprüfbarem Datenschutz

Auf einem Anonymität, Unbeobachtbarkeit und Unverkettbarkeit anbietenden Kommunikationsnetz sind beliebige, auch nicht anonyme Kommunikationsformen ohne Leistungseinbuße realisierbar.

Fast alle Verfahren, sich über ein Netz einander zu erkennen zu geben (d. h. sich zu identifizieren) oder seine Autorisation nachzuweisen (d. h. sich zu authentizieren), machen bereits heute keinen Gebrauch davon, daß das sendende oder empfangende Endgerät oder gar der es gerade benutzende Teilnehmer dem Kommunikationsnetz gegenüber identifizierbar ist. Zum Beispiel erkennt man Telefonpartner an ihrer Stimme und Sprechweise sowie ihrem Wissen, Briefpartner an ihrer (Unter-)Schrift. Fortschritte der Sprachsynthese machen die Erkennung von Telefonpartnern an ihrer Sprechweise und Stimme [Diff_82], Fortschritte in der Mustererkennung und Robotik die Erkennung anhand einer (Unter-)Schrift jedoch immer unzuverlässiger. Da es für beides jedoch digitale Entsprechungen gibt (digitale Signatursysteme, vgl. Abschnitt 2.2.1.2.2), können übliche Identifikations- und Authentikationsprotokolle weiterverwendet werden [DaPr_84].

Deren routinemäßiger Einsatz bei allen Diensten, wo dies wünschenswert ist, ist preiswert und praktisch ohne Manipulationsmöglichkeit möglich – sogenannte (externe) „Hacker“ sind also kein Thema. Insbesondere ist es sowohl unsinnig als auch weitgehend erfolglos, mangelhafte Identifikations- oder Autorisationsprüfung in Teilnehmerendgeräten (z. B. Rechenzentren, Datenbanken etc.) durch globale Beobachtung und Protokollierung im offenen Kommunikationsnetz ausgleichen zu wollen: dann gehen „Hacker“ eben durch ausländische Kommunikationsnetze und von der „Hackergemeinde“ betriebene MIXe und hinterher ist nichts beweisbar. (Die in [BfD_88 Seite 41] erhobene Forderung, „daß entweder durch geeignete technische und organisatorische Vorkehrungen ‚anonyme Anzeigen‘ verhindert werden, oder aber daß zumindest der verursachende Btx-Anschluß ermittelt und dem Betroffenen benannt werden kann, damit diesem ermöglicht wird, seine Rechte wahrzunehmen.“ ist also sowohl unnötig – vgl. Abschnitt 8.3 und Pseudonyme allgemein in [Chau_81, Cha8_85, PWP_87] – als auch nicht durchführbar.)

Nach diesem Beispiel der anonymen oder eine falsche Benutzeridentität vortäuschenden Belästigung von Rechnern noch eins von Personen: Fühlt sich beispielsweise ein Teilnehmer durch nächtliche anonyme Anrufe belästigt, so kann er seine Teilnehmerstation instruieren, Anrufe zwischen beispielsweise 21.00 und 8.00 Uhr ihm nur dann zu signalisieren, nachdem sich der Anrufer dem Teilnehmerendgerät gegenüber identifiziert und dieses die Identifikation gespeichert hat. Ängstliche Gemüter können diesen „digitalen Kommunikationsleibwächter“ natürlich rund um die Uhr in Betrieb lassen. Analog kann jeder Netzteilnehmer den Personenkreis, für den man während gewisser Zeiten erreichbar ist, einschränken.

Für manche Dienste kann es interessant sein, daß es sogar Möglichkeiten gibt, daß sich Teilnehmer *gleichzeitig* identifizieren [Gol2_83, Gol1_85].

Nach diesen Bemerkungen zur expliziten Aufgabe der Anonymität, die bei manchen Diensten gesellschaftlich wünschenswert, rechtlich vorgeschrieben oder ins Belieben der Teilnehmer gestellt sein mag, wird in den folgenden Unterabschnitten für vier wichtige „Teletransaktionen“ skizziert, wie diese in voller Anonymität ohne Verlust an Sicherheit möglich sind.

8.1 Digitale Zahlungssysteme

Ein Zahlungssystem heißt *digital*, wenn Teilnehmer über ein Kommunikationsnetz Geld transferieren können. Dabei muß Geld, da ein physischer Transport materieller Zahlungsmittel per Definition ausgeschlossen ist, mittels digitaler Nachrichten transferiert werden. Da diese Nachrichten beliebig dupliziert werden können, die Geldmenge dadurch aber nicht (unkontrolliert) vermehrt werden können soll, darf nur das erste Eintreffen einer solchen Nachricht einen Geldzugang bewirken.

Die für eine Klassifikation der digitalen Zahlungssysteme relevante Frage ist, ob dieses erste Eintreffen von einer zentralen Instanz (Gerät, Mitarbeiter) des Zahlungssystembetreibers (etwa einer Bank) oder einem der Obhut eines normalen Teilnehmers anheimgestellten Gerät geprüft wird. (Die eher theoretische Möglichkeit, eine absolute Mehrheit der am Zahlungssystem Beteiligten über das erste Eintreffen entscheiden zu lassen, wird im folgenden nicht extra behandelt, sondern als verteilte Implementierung einer zentralen Instanz betrachtet.) Während der Zahlungssystembetreiber ein klares Interesse hat, daß sich die Geldmenge nicht zu seinen Ungunsten vermehrt, dürfte der einzelne Teilnehmer durchaus ein Interesse daran haben, daß sein Gerät eine Nachricht mehrmals „akzeptiert“. Deshalb muß in diesem letzteren Fall das Teilnehmergerät vor diesem *manipulationssicher* sein. Gibt es solche Geräte (was mir gemäß dem in Abschnitt 2.1.2 Gesagten zumindest für solche mit Chipkartenabmessungen mehr als zweifelhaft erscheint) und werden sie verwendet, so kann das Zahlungssystem *autonome Zahlungen* der Teilnehmergeräte zwischeneinander zulassen, ohne daß dies die Sicherheit des Zahlungssystems gefährdet. Ohne solche Geräte kann die Deckung einer Zahlung im allgemeinen Fall nur durch Nachfragen beim Zahlungssystembetreiber überprüft werden – autonome Zahlungen sind dann nicht sicher möglich.

Damit nicht durch aktive Angriffe im Kommunikationsnetz unbefugt Zahlungsvorgänge ausgelöst oder befugt ausgelöste bezüglich Betrag oder Zeitpunkt manipuliert werden können, benötigen alle digitalen Zahlungssysteme die Verwendung eines *sicheren symmetrischen Kryptosystems* oder (asymmetrischen) *Signatursystems*. Ersteres genügt nur dann, wenn auch manipulationssichere Geräte verwendet werden. Letzteres ist dann nötig, wenn das Zahlungssystem die Rechtssicherheit zwischen Zahlungssystembetreiber und Teilnehmer waren soll. Darunter wird verstanden, daß auch der Betreiber des Zahlungssystems dem Teilnehmer keine Transaktion unterschieben, d. h. fälschlich und unwiderlegbar behaupten kann, der Teilnehmer habe einen Geldtransfer veranlaßt, einen Geldtranfer anderer Höhe veranlaßt oder einen niedrigeren Kontostand.

All diese Forderungen und Voraussetzungen sind vollkommen unabhängig davon, ob das digitale Zahlungssystem Anonymität von Zahlungsempfänger und Zahlendem voreinander, Unbeobachtbarkeit durch an der Zahlung nicht direkt Beteiligte (insbesondere den Zahlungssystembetreiber) und Unverkettbarkeit von Zahlungen anbieten soll oder nicht. Zur Erreichung von Anonymität, Unbeobachtbarkeit und Unverkettbarkeit gibt es drei Grundkonzepte:

- *manipulationssichere autonome Zähler* [Pfi1_83, Pfit_84, MaRS_84],
- *informationstheoretisch unverkettbare Umformung digitaler Zahlungsmittel durch die Teilnehmer*, wobei die Sicherheit gegen Vermehrung der Geldmenge bei effizienten Implementierungen bisher (nur) so sicher wie RSA als das vom Zahlungssystembetreiber dann zu verwendende Signatursystem ist [Chau_83, Cha1_84, Cha8_85, Chau_87, Chau_89], während sehr aufwendige Implementierungen die Verwendung eines beliebigen Signatursystems zulassen [BrCC_87], und
- *anonym übertragbare Standardwerte* [BüPf_87] (die anonymen Nummernkonten [Pfi1_83, Pfit_84] bzw. Standardwertkonten [BüPf_86, Bürk_86] sind Spezialfälle).

In [PWP_87, BüPf_87] wird eine Übersicht über digitale Zahlungssysteme gegeben und gezeigt, wie diese Grundkonzepte auch kombiniert werden können, so daß Anonymität, Unbeobachtbarkeit und Unverkettbarkeit voll erreichen werden. Wie bei Kommunikationsnetzen kann natürlich auch bei Zahlungssystemen auf diese Eigenschaften ohne Leistungseinbuße verzichtet werden, wenn immer dies vorgeschrieben ist oder von den Teilnehmern gewünscht wird.

Da die Anonymität, Unbeobachtbarkeit und Unverkettbarkeit eine nachträgliche Strafverfolgung be- oder gar verhindert, müssen die genauen Zahlungsprotokolle bei solchen Zahlungssystemen so entworfen werden, daß von vornherein niemand betrügen kann. Dies ist bereits geschehen [WaPf_85, PWP_87, BüPf_86].

Es ist bemerkenswert, daß der Verlust manipulationssicherer Teilnehmergeräte für autonome Zahlungen, der normalerweise den Verlust allen Geldes in diesen „elektronischen Brieftaschen“ (electronic wallets, [EvGY_84, Even_89]) bewirkt, mit geeigneten Methoden der Fehlertoleranz ohne Geld- und sogar ohne Anonymitätsverlust toleriert werden kann [WaPf_87, WaP1_87].

8.2 Warentransfer

Beim Transfer von Waren über ein Kommunikationsnetz gibt es folgendes, von der Anonymität unabhängiges, aber durch sie eskaliertes Problem: wer seinen Wert (Ware oder Geld) dem anderen als erster schickt, kann nicht sicher sein, daß er vom anderen dessen Wert auch zugeschickt bekommt. Ein Warentransferprotokoll heiße *betrugssicher*, wenn es verhindert, daß demjenigen, der seinen Wert zuerst sendet, dadurch ein Nachteil entsteht.

Um nicht nur einen anonymen, unbeobachtbaren und unverkettbaren Transfer von Geld, sondern auch unter den gleichen Bedingungen einen betrugssicheren Transfer von Waren,

z. B. Austausch Geld gegen Datenbankauskunft, zu ermöglichen, gibt es zwei (gegensätzliche) Konzepte:

- Entweder gibt es nichtanonyme einzelne [Herd_85] oder Ketten von [Chau_81 Seite 86] Instanzen, die im Betrugsfall die Anonymität aufheben, oder
- es wird ein nichtanonymer aktiver Treuhänder eingeschaltet, der den (möglicherweise) völlig anonymen Partnern Betrugssicherheit garantiert und von ihnen vollständig kontrolliert werden kann [Pfi1_83 Seite 32f, WaPf_85, Waid_85].

Aus den in [PWP_87, BüPf_86, BüPf_87] diskutierten Gründen ist das zweite Konzept vorteilhafter.

Bei individueller Bezahlung von Informationsdiensten von hinreichend allgemeinem Interesse gibt es ein von der Anonymität weitgehend unabhängiges ungelöstes (und ohne einen allgegenwärtigen großen Bruder wohl auch unlösbares) Problem: Da die Übertragung von Information in Zukunft sehr schnell und billig sein wird, kann man bei Diensten von hinreichend allgemeinem Interesse (z. B. Zeitungen) die Abrechnung mit dem Diensterbringer für die Dienstbereitstellung, die für ihn nicht billiger sein wird als bisher, umgehen, indem man Information im Kommunikationsnetz kopiert und weiterverteilt.

Dies gilt sogar für Information, die nicht im Kommunikationsnetz angeboten wird. Alles, was ein Mensch sehen oder hören kann, kann er digital kopieren bzw. aufnehmen und dann über das Kommunikationsnetz verteilen, z. B. gedruckte Zeitungen, Bücher oder Schallplatten. Dies verschärft das bisherige Urheberrechtsproblem mit Kopierern und Musikkassetten. Außerdem ist das Urheberrechtsproblem bezüglich für den Menschen sicht- oder hörbarer Werke schwerer zu lösen als das des Softwareschutzes, denn hier muß lediglich das Ergebnis eines Programmes wahrnehmbar sein, während man das Programm als solches oder Teile davon in einen sicheren Hardware-Modul einschließen kann.

Wollte man jedoch, um das obige Problem des Weiterkopierens zu umgehen, auch für die gesamte Nutzung von Informationsdiensten von hinreichend allgemeinem Interesse eine generelle Pauschale erheben, so müßte man ein Verfahren finden, nach dem die von einer GEZ-ähnlichen Organisation eingezogenen Gebühren „gerecht“ auf die verschiedenen Anbieter verteilt würden.

Dieses müßte die unterschiedlichen, von der Qualität, nicht aber von der Nachfrage abhängigen Bereitstellungskosten der Anbieter von Diensten berücksichtigen, ohne jedoch Meinungszensur zu betreiben oder bestehende Märkte festzuschreiben und damit letztendlich den Informationspluralismus zu gefährden. Ein solches Verfahren ist mir nicht bekannt.

8.3 Dokumente

Auch bei vielen Kommunikationsarten, bei denen man heute namentlich auftreten muß (z. B. Bürger bei Ämtern), kann man die Möglichkeit zur anonymen Kommunikation nutzen und unter verschiedenen Pseudonymen auftreten, wenn man ein Verfahren hat, um Dokumente, die auf eines dieser Pseudonyme lauten, in sicherer und anonymer Weise auf ein anderes eigenes Pseudonym umzuformen.

In [Cha1_84, Cha8_85, Chau_87, ChEv_87] sind effiziente Verfahren beschrieben, bei denen die Umformung der Dokumente informationstheoretisch unverkettbar erfolgt, und bei denen die Sicherheit gegen das Fälschen von Dokumenten (nur) so sicher wie RSA als das zu verwendende Signatursystem ist. Aus [Cha1_87, BrCC_87] können sehr aufwendige Implementierungen abgeleitet werden, die die Verwendung eines beliebigen Signatursystems zulassen. Zur Zeit wird nach effizienten Verfahren geforscht, die die Beschränkung auf die Sicherheit von RSA nicht mehr haben [Bura_88, Waid_88, WaPf_89, WaPf1_89].

Da David Chaum in seinen Veröffentlichungen nicht explizit darauf hinweist, sei hier betont, daß es natürlich durch rein kryptographische Methoden unmöglich ist zu verhindern, daß jemand ein vollkommen anonym erworbenes Dokument einem anderen überläßt (und es sogar hinfort selbst nicht mehr verwendet), was etwa beim Führerschein sicherlich nicht im Sinne der Verkehrssicherheit wäre. Aber auch hier ist keine namentliche Identifikation der Person nötig, sondern eine Verkettung des Dokumentes mit körperlichen Merkmalen der Person völlig hinreichend. Sind die pro Dokumententyp verwendeten körperlichen Merkmale (außer über den Körper des Besitzers der Dokumente) nicht verkettbar, so ist dem Datenschutz hier sicher Genüge getan.

8.4 Statistische Erhebungen

Mittels Anonymität, Unbeobachtbarkeit und Unverkettbarkeit anbietenden Kommunikationsnetzen können statistische Erhebungen tatsächlich anonym durchgeführt werden. Hierbei sollten die Teilnehmerstationen vom Teilnehmer zu dessen Bequemlichkeit nur möglichst wenige Daten erfragen, aber auch diese wenigen Daten nicht als ganzes, d. h. als Maxi-Datensatz, weitergeben, da damit meist eine *Reidentifikation* sehr leicht durchgeführt werden kann. Stattdessen sollte die Teilnehmerstation aus diesen wenigen erfragten Daten sehr viele Mini-Datensätze erzeugen und diese in anonymer und unverkettbarer Weise an das statistische Amt schicken. Diese Mini-Datensätze werden so generiert, daß sie dem statistischen Amt die Berechnung aller vor der statistischen Erhebung vereinbarten Statistiken ermöglichen. Sie ermöglichen nicht beliebige andere Statistiken, so daß das Zweckbindungsgebot (teilnehmer-)überprüfbar eingehalten wird.

Mit den in Abschnitt 8.3 zitierten Mechanismen kann sichergestellt werden, daß jeder an der statistischen Erhebung genau einmal teilnimmt.

9 Anwendung beschriebener Verfahren auf verwandte Probleme

In diesem Kapitel wird kurz skizziert, welche anderen Probleme mit den bisher entwickelten Verfahren auch gelöst werden können. Diese Skizze erhebt natürlich keinen Anspruch auf Vollständigkeit.

9.1 Öffentlicher mobiler Funk

Als Ergänzung des in den bisherigen Kapiteln behandelten Ausbaus der offenen Kommunikationsnetze zwischen ortsfesten, durch Leitungen verbundenen Teilnehmerstationen erfolgt ein Ausbau der offenen Funknetze zwischen mobilen Teilnehmerstationen [Alke_88]. Deshalb soll hier kurz skizziert werden, wie die hierbei auftretenden Datenschutzprobleme gelöst oder zumindest erträglich klein gehalten werden können.

Die Unterschiede zu den bisherigen Kapiteln sind, daß

- Übertragungsbandbreite bei Funknetzen sehr knapp ist und *bleiben wird*, da das elektromagnetische Spektrum im freien Raum „nur einmal“ vorhanden ist.
- nicht nur (technisch gesehen) die Nutzdaten und Vermittlungsdaten bzw. (inhaltlich gesehen) die Inhaltsdaten, Interessensdaten und Verkehrsdaten einen Personenbezug aufweisen und deshalb ggf. geschützt werden müssen, sondern auch der *momentane Ort* der mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers.

Wie in Abschnitt 2.5.3.2 erläutert wurde, ist es zumindest bezüglich technisch versierter Angreifer unrealistisch zu fordern, daß Signale, die von verschiedenen Stationen gesendet werden, nicht unterschieden werden können: Wegen der analogen Charakteristika des Senders und ihrer bei jedem Produktionsprozeß unvermeidbaren Streuung wäre dies praktisch und wegen der Änderung des Signals bei seiner Ausbreitung (Dispersion) bei kontinuierlichem Senden auch theoretisch nicht erfüllbar.

Ich gehe im folgenden deshalb davon aus, daß eine mobile Teilnehmerstation immer identifizierbar ist, wenn sie sendet (auch wenn Hochfrequenztechniker das Funksystem so auslegen sollten, daß Identifikation und Peilung der mobilen Teilnehmerstationen möglichst schwierig ist, und obwohl bei manchen Anwendungen dem Angreifer unbekannte, die Signalausbreitung beeinflussende Umgebungen eine Identifikation praktisch sehr erschweren). Im Gegensatz dazu gehe ich im folgenden davon aus, daß Teilnehmerstationen so ausgelegt werden können, daß sie nicht identifizierbar und peilbar sind, wenn sie nur (passiv) empfangen.

Wegen dem auch durch Außenstehende sehr leicht abhörbaren Funkverkehr ist neben der immer notwendigen Ende-zu-Ende-Verschlüsselung auch Verbindungs-Verschlüsselung zwischen der mobilen Teilnehmerstation und der (aus ihrer Sicht) ersten ortsfesten Station ange-

bracht, sofern die Protokollinformation der Schichten 1 bis 3 des ISO OSI Referenzmodells (vgl. Abschnitt 2.6) irgendeinen Personenbezug aufweist.

Wegen der Knappheit der Übertragungsbandbreite und einer ansonsten jederzeit möglichen Identifikation und Peilung der mobilen Teilnehmerstation sind die in Abschnitt 2.5.3 beschriebenen Möglichkeiten zum Schutz des Senders („bedeutungslose Nachrichten", „überlagerndes Senden", „Unbeobachtbarkeit angrenzender Leitungen und Station sowie digitale Signalregenerierung") sowohl nicht anwendbar als auch nicht empfehlenswert.

Da damit alle Maßnahmen zum Schutz der Verkehrs- und Interessensdaten im ortsfesten Teil des Kommunikationsnetzes abgewickelt werden müssen, bietet sich folgendes Vorgehen an:

Sofern die Codierung der Nutzdaten in mobilen genauso wie in ortsfesten Teilnehmerstationen erfolgt, kann das Verfahren der umcodierenden MIXe (Abschnitt 2.5.2) direkt angewendet werden, sofern die mobilen Teilnehmerstationen über genügend Verschlüsselungskapazität verfügen.

Ist die Codierung der Nutzdaten in mobilen Teilnehmerstationen anders als in ortsfesten, um beispielsweise Übertragungsbandbreite zu sparen (16 kbit/s oder 32 kbit/s Sprachkanal statt 64 kbit/s), so könnte der Empfänger und das Kommunikationsnetz dies zur Verkettung verwenden. In diesem Fall sollte, zumindest solange mobile Teilnehmerstationen nur einen sehr kleinen Teil aller Teilnehmerstationen darstellen, von der mobilen Teilnehmerstation ein Verbindungsverschlüsselter Kanal zu einer ortsfesten Teilnehmerstation (möglichst des gleichen Teilnehmers) hergestellt, das Signal dort an die übliche Signalcodierung angepaßt und von dort mit den üblichen Verfahren zum Schutz der Verkehrs- und Interessensdaten weiterübertragen werden. Entsprechendes gilt, wenn zwar die Codierung der Nutzdaten in mobilen genauso wie in ortsfesten Teilnehmerstationen erfolgt, die mobilen Teilnehmerstationen aber nicht über genügend Verschlüsselungskapazität verfügen.

Eine gerade nur (passiv) empfangende mobile Teilnehmerstation sollte (auch bei Zellularfunksystemen) vom Kommunikationsnetz nicht lokalisiert werden können. Liegt für sie ein Verbindungswunsch oder eine lange Nachricht vor, so sollte eine entsprechende implizite Adresse im ganzen Funknetz verteilt werden, worauf sich die mobile Teilnehmerstation (aktiv) meldet und dadurch lokalisierbar ist. Da Adressen nur wenige Bytes umfassen müssen, ist der Aufwand für diese Datenschutzmaßnahme gering – falls dies nicht sogar zu einer Aufwandssenkung führt, da die Verwaltung eines Zellularfunksystems erheblich vereinfacht wird.

Zum Schluß sei nochmals daran erinnert, daß die mobilen Teilnehmerstationen aus den zu Beginn von Kapitel 5 (im Zusammenhang mit Katastrophentoleranzverfahren) und in Abschnitt 6.1 genannten Gründen so konzipiert werden sollten, daß sie in Katastrophensituationen weitgehend ohne den ortsfesten Teil des Kommunikationsnetzes in der näheren Umgebung auskommen und zusätzliche, normalerweise für Unterhaltung (Rundfunk) verwendete Frequenzen nach Erhalt einer „Freigabenachricht" für Notrufe verwenden können.

Das über öffentlichen mobilen Funk Gesagte ist bei der Gestaltung von **Verkehrsleitsystemen** zu beachten: Es ist bezüglich Datenschutz unkritisch, Informationen an Fahrzeuge zu verteilen, es ist sehr kritisch, wenn Fahrzeuge Informationen dauernd oder sehr oft senden müssen, wie dies im Projekt PROMETHEUS [FO_87, Walk_87] vorgesehen ist.

Aus den in Abschnitt 2.1 dargelegten Gründen sollten Verkehrsleitsysteme aus Datenschutzgründen zusätzlich so entworfen werden, daß Sensoren zwar Fahrzeuge erkennen, aber weder Fahrzeugtypen noch gar Fahrzeugexemplare unterscheiden können – anderenfalls entstehen Bewegungsbilder, die genausowenig geschützt werden können, wie die im Rest der Arbeit behandelten Vermittlungsdaten.

9.2 Fernwirken (TEMEX)

Die Datenschutzproblematik des Fernwirkens (TEMEX) wird bezüglich des Fernablesens von Zählern jeder Art praktisch vollständig beseitigt, wenn dies Ablesen nur in gewissen Mindestabständen erfolgen kann, wie dies in Abschnitt 7.2 für nicht manipulierbare Abrechnungszähler beschrieben und begründet ist. Sowohl aus Gründen des Datenschutzes vor Unbeteiligten als auch aus Gründen der Authentifikation erfolgt die Übertragung des Ableseergebnisses Ende-zu-Ende-verschlüsselt.

Dieses von mir erstmals 1983 vorgeschlagene Vorgehen [Pfi1_83 Seite 36] ist dem in [Pete_87] beschriebenen in der Weise überlegen, daß die vorbeugende Verhinderung einer unerlaubten Handlung immer besser als die nachträgliche Entdeckung und Bestrafung ist.

9.3 Einschränkungsproblem (confinement problem)

Butler Lampson beschreibt in [Lamp_73] das Einschränkungsproblem (confinement problem), d. h. das Problem, wie ein Programm bei seiner Ausführung so eingeschränkt werden kann, daß es Information, die ihm zur Ausführung seiner Aufgabe zur Verfügung gestellt wird, nicht an jemand weitergeben kann, der zum Erhalt der Information nicht befugt ist. Mit anderen Worten: Wenn schon nicht feststellbar ist, ob ein Programm ein Trojanisches Pferd enthält, kann dann wenigstens der Schaden durch ein potentiell vorhandenes Trojanisches Pferd verhindert oder zumindest begrenzt werden (vgl. Abschnitt 2.1.2) ?

In [RuRa_83, RuR1_83] diskutieren John Rushby und Brian Randell eine partielle Lösung des Einschränkungsproblems in einem verteilten System. Ihre Lösung verwendet *vertrauenswürdige Netzschnittstellen* (Trustworthy Network Interface Units = TNIUs), um, wo nötig, Isolation zu erzwingen. Diese vertrauenswürdigen Netzschnittstellen kontrollieren allen Nachrichtenverkehr zwischen den als nicht vertrauenswürdig angenommenen Wirtsrechnern (hosts) über das als nicht vertrauenswürdig angenommene lokale Netz. Rushby und Randell merken in [RuRa_83 Seite 60] an, daß ein Programm, das Information an Unbefugte weitergeben will, die Ziel-Adressen der von ihm gesendeten Nachrichten modulieren kann. Da Adressen in Rushbys und Randells lokalem Netz nicht verschlüsselt werden, können sie von einem Angreifer, der das lokale Netz abhört, leicht interpretiert werden. (Entsprechendes würde gelten, wenn die Adressen von den vertrauenswürdigen Netzschnittstellen einfach mit einer deterministischen Blockchiffre zum Zwecke der Konzelation verschlüsselt würden, denn auch dann könnte ein

Angreifer Adressen auf Gleichheit testen, vgl. Abschnitt 2.2.2.1.) Die einzige Gegenmaßnahme, die Rushbys und Randell vorschlagen, ist zufällig adressierter bedeutungsloser Nachrichtenverkehr (vgl. Abschnitt 2.5.3) zwischen den vertrauenswürdigen Netzschnittstellen. Aber dies ist nur eine sehr unbefriedigende Lösung, da der verborgene Kanal (covert channel) dadurch nur verrauscht wird und dieses „Verrauschen“ zudem beträchtliche Nutzleistungseinbußen des lokalen Netzes verursacht.

Wie in [Pfi1_85 Seite 134] beschrieben, kann dieser verborgene Kanal vollkommen eliminiert werden, wenn auf dem lokalen Netz Verteilung verwendet wird (was üblicherweise sowieso der Fall ist) und die vertrauenswürdigen Netzschnittstellen die von den Programmen bzw. Wirtsrechnern generierten Adressen in verdeckte oder nur einmal verwendete offene implizite Adressen umsetzen, vgl. Abschnitt 2.5.1.

Verwenden die vertrauenswürdigen Netzschnittstellen (außerdem) ein Verfahren zum Schutz des Senders, so schließen sie (außerdem) den verborgenen Kanal, welches Programm bzw. welcher Wirtsrechner wie häufig Nachrichten sendet, zum größten Teil, ohne die Fähigkeit zur dynamischen Aufteilung der Bandbreite aufzugeben. Eine statische Aufteilung der Bandbreite (jede vertrauenswürdige Netzschnittstelle sendet unabhängig davon, ob sie etwas zu senden hat, mit einer festen Rate) scheint der Preis dafür zu sein, diesen verborgenen Kanal vollständig zu schließen und damit zu eliminieren [Pfi1_85 Seite 134].

Verwandte Themen werden in [McMo_86, Coh2_87 Seite 223 bis 226] angesprochen.

9.4 Hocheffizienter Mehrfachzugriff

Das DC-Netz arbeitet mit den in Abschnitt 3.1.2 beschriebenen Mehrfachzugriffsverfahren so effizient, daß sein Einsatz zumindest im lokalen Bereich auch für Zwecke, bei denen es nicht auf Senderanonymität ankommt, zweckmäßig erscheint. Für Pakete und kurze Nachrichten sind besonders die in Abschnitt 3.1.2.3.2 ausführlich beschriebenen Kollisionsauflösungsalgorithmen mit globalem überlagerndem Empfangen interessant, für Kanäle die Anwendung von paarweisem überlagerndem Empfangen (Abschnitt 3.1.2.5).

Schlüsselerzeugung und synchronisierte Überlagerung können, wenn es auf Senderanonymität nicht ankommt, natürlich weggelassen werden. Dann ist die Übertragung führender Nullen, wie dies in Abschnitt 3.1.2.3.2, insbesondere Bild 35, beschrieben und begründet wurde, überflüssig. Wird z. B. die globale Überlagerung von einer Zentrale durchgeführt, so wird dann zur Zentrale weniger Bandbreite benötigt als von ihr weg.

Auch ist bei Verzicht auf die Überlagerung von Schlüsseln in Erwägung zu ziehen, inwieweit die Synchronität zwischen den am überlagernden Senden Beteiligten aufgegeben werden kann: etwa könnte es genügen, wenn alle Beteiligten unsynchronisiert, aber in etwa phasenstabil senden und die modulo-Addierer für die globale Überlagerung erst eine für die Addition der Zeichen nötige, lokale Synchronität herstellen. Bei solch einer Implementierung könnte dann auch die in Abschnitt 3.1.2 ausgeklammerte Klasse der asynchronen Mehrfachzugriffsverfahren Bedeutung erlangen.

10 Ausblick

Die Verwendung nicht Datenschutz durch Anonymität, Unbeobachtbarkeit und Unverkettbarkeit anbietender offener Kommunikationsnetze gefährdet dauerhaft die Rechte aller Teilnehmer, Privatpersonen wie auch Unternehmen.

Wie in den Abschnitten bis 2.3 einschließlich begründet, ist der Einsatz geeigneter kryptographischer Verfahren notwendig und hinreichend für einen überprüfbaren Schutz der Nutz- bzw. Inhaltsdaten – allerdings sind kryptographische Verfahren nur in Kommunikationsnetzen mit digitaler Übertragungstechnik effizient einsetzbar. Die weltweit vorangetriebene Umstellung von analoger auf digitale Übertragungstechnik ist also ein notwendiger erster Schritt, vgl. Abschnitt 6.1.

Eine nachträgliche Einführung eines überprüfbaren Schutzes der Verkehrs- und Interessensdaten ist allerdings selbst bei Verwendung digitaler Übertragungstechnik technisch schier unmöglich. Dieses Problem ist bei diensteintegrierenden Kommunikationsnetzen besonders schwerwiegend.

Das Problem, die Verkehrs- und Interessensdaten zu schützen, ist daher in gewissem Sinne dringlicher als die Probleme des Schutzes der Nutzdaten und der Authentifikation, mit denen sich die öffentliche Diskussion zur Zeit hauptsächlich beschäftigt: Diese lassen sich auf Digitalnetzen beliebiger Struktur notfalls im nachhinein durch kryptographische Verfahren lösen (falls hierfür die notwendigen Normen oder zumindest De-facto-Standards vorliegen, was leider noch nicht der Fall ist, vgl. Abschnitt 2.2.2.4); eine willentliche Selbstidentifikation, ein unfälschbarer Autorisationsnachweis sowie ein Schutz vor unerwünschten anonymen Anrufen ist stets möglich (Kapitel 8).

Der Schutz der Verkehrs- und Interessensdaten muß hingegen bereits beim Entwurf berücksichtigt werden. Denn offene diensteintegrierende Kommunikationsnetze, die auch Interessens- und Verkehrsdaten (vgl. Abschnitt 1.2) in überprüfbarer Weise schützen und ihren Benutzern nennenswert viel Sendebandbreite zur Verfügung stellen, benötigen auf jeden Fall eine passende physische Netzstruktur:

Ohne Verteilnetze im Teilnehmeranschlußbereich scheint ein effizienter Schutz der Empfänger unmöglich zu sein. Dies bedeutet, daß hier Leitungen mit sehr hoher Bandbreite benötigt werden. Verwendet man RING- oder BAUM-Netze zum Schutz des Senders, so ist zusätzlich die Topologie des Kommunikationsnetzes (Ringe oder Bäume im Teilnehmeranschlußbereich) vorgegeben.

Riskiert man den Einsatz von MIXen, obwohl keine im Sinne von Abschnitt 2.2.2.2 bewiesenen einschrittigen Implementierungen bekannt sind (vgl. Abschnitt 2.5.2.8), so müssen nur die Verbindungswünsche verteilt werden. Jede Teilnehmerstation muß dann so viele Zeitscheibenkanäle unterhalten, wie sie maximal gleichzeitig verwenden will, vgl. Abschnitt 6.2.

Datenschutz durch Anonymität, Unbeobachtbarkeit und Unverkettbarkeit anbietende offene Kommunikationsnetze sind realisierbar – ihre Kosten sind aber noch weniger bekannt als die der geplanten. Soweit ich aus den mir bekannten Aufwandsbetrachtungen und Kostenschätzungen auf die Mehrkosten für teilnehmerüberprüfbaren Datenschutz schließen kann, sind die mit dem technischen Fortschritt laufend fallenden Mehrkosten bereits heute vertretbar. Bei manchen

Verfahren erwarte ich sogar ein etwa gleich großes Leistung/Kosten-Verhältnis wie für die üblichen reinen Vermittlungsnetze, vgl. Abschnitt 4.3.1.1.1. Deshalb halte ich eine etappenweise Einführung eines breitbandigen diensteintegrierenden Digitalnetzes mit teilnehmerüberprüfbarem Datenschutz mit der Zwischenstufe eines Datenschutz garantierenden schmalbandigen diensteintegrierenden Digitalnetzes für mit in etwa der gleichen Geschwindigkeit möglich wie die Einführung der geplanten Netze.

Leider ist mir über Aufwand, Kosten und mögliche Einführungsgeschwindigkeit nicht mehr als das in dieser Arbeit Wiedergegebene bekannt. Die für einen genauen Aufwandsvergleich notwendigen Pilotimplementierungen signifikanten Umfangs sind einer kleinen, in der Informatik und nicht in der Nachrichtentechnik angesiedelten Forschungsgruppe nicht möglich. Ich hoffe, daß Netzbetreiber (z. B. DBP), Hersteller und nachrichtentechnisch ausgerichtete Forschungsgruppen in näherer Zukunft Pilotimplementierungen durchführen. Die für qualifiziertere Aussagen nötigen genauen Werte, wie sich heutzutage Aufwand in realen Kosten niederschlägt und welche Verschiebung in der überschaubaren Zukunft von Netzbetreibern (z. B. DBP) oder Herstellern erwartet wird, waren nicht zu erhalten. Entsprechendes gilt für Prognosen möglicher Einführungsgeschwindigkeiten.

Da die juristische und technische Situation in verschiedenen Ländern signifikant unterschiedlich ist, kann nicht von einer weltweiten und schon gar nicht von einer homogenen und gleichzeitigen Realisierung von Kommunikationsnetzen ausgegangen werden. Trotzdem darf die Realisierung von teilnehmerüberprüfbarem Datenschutz in manchen Ländern internationale Kommunikation nicht erschweren und der Datenschutz sollte für die Teilnehmer in diesen Ländern auch bei internationaler Kommunikation möglichst erhalten bleiben. All dies ist mit den in Abschnitt 6.6 beschriebenen Ideen erreichbar.

Aus dieser informatischen Arbeit ergeben sich für die Bundesrepublik Deutschland mindestens zwei juristische Fragen:

Wie gezeigt wurde, stellt die Realisierung der derzeitigen Pläne der DBP *technisch* gesehen einen unnötigen Eingriff in das informationelle Selbstbestimmungsrecht des durch das Fernmeldemonopol faktisch zur Benutzung gezwungenen Bürgers dar. Ist dieser Eingriff bei sinngemäßer Anwendung des Volkszählungsurteils des Bundesverfassungsgerichts und unter Abwägung auch außertechnischer Sachverhalte verfassungsrechtlich zulässig?

Die technische Entwicklung der automatischen Sprecher- und Spracherkennung macht Ende-zu-Ende-Verschlüsselung immer notwendiger. Diese ist aber über den analogen Teilnehmeranschluß nicht ohne gravierenden Verständlichkeitsverlust von Sprache möglich. Ist unter Abwägung auch außertechnischer Sachverhalte das von Herbert Kubicek vorgeschlagene Beibehalten des heutigen Fernsprechnetzes verfassungsrechtlich zulässig?

Anhang: Modifikationen von DES

Für den mit DES vertrauten Leser werden hier 4 *verallgemeinernde* Modifikationen von DES beschrieben, die alle bisher an der Sicherheit von DES geäußerte Kritik berücksichtigen. Es wird begründet, warum diese Verallgemeinerungen von DES mindestens so sicher wie DES sind. Effiziente Implementierungen werden skizziert.

Vermeidung der Schlüsselexpansion (key expansion, [Hell_82 Seite 131]): Statt in 16 Runden jeweils 48 der 56 Schlüsselbits zu verwenden, verwende man für jede Runde jeweils 48 „neue“ Schlüsselbits, so daß die Gesamtschlüssellänge statt 56 Bit dann 16•48 Bit = 768 Bit beträgt [Morr_78 Seite 13] (das so verallgemeinerte DES wird in [LuR1_86, LuRa_88] „modified DES“ bzw. abgekürzt „MDES“ genannt).

Trivialerweise ist das durch diese Verallgemeinerung entstehende Kryptosystem abwärtskompatibel mit DES, indem die 768 Schlüsselbits so gewählt werden, daß sie jeweils den von DES ausgehend vom 56 Bit Schlüssel in der betreffenden Runde verwendeten 48 Bit entsprechen [Ber1_83]. Aus dem gleichen Grund ist diese Verallgemeinerung im folgenden Sinne mindestens so sicher wie DES: kann die Verallgemeinerung von einem Angreifer bei beliebigen Schlüsseln gebrochen werden, insbesondere also bei allen DES entsprechenden Schlüsseln, so kann der Angreifer DES bei beliebigen Schlüsseln brechen. Dies sagt natürlich nichts über einen Angreifer aus, der die Verallgemeinerung nur bei fast allen (im schlimmsten Fall allen 2^{768}-2^{56} nicht DES entsprechenden) Schlüsseln brechen kann. Da die Verallgemeinerung von DES aber keinerlei vom Schlüssel abhängige zusätzliche Struktur einführt, die Schlüsselexpansion in der mir bekannten Literatur nicht als für die kryptographische Stärke von DES wesentlich betrachtet wird und die Struktur von DES die kryptologisch am besten öffentlich untersuchte ist und dabei (wie in Abschnitt 2.2.2.2 erwähnt) kein Ansatz zu einem wesentlich effizienteren Brechen als durch vollständiges Durchprobieren aller Schlüssel gefunden wurde, ist dies sehr, sehr unwahrscheinlich.

Die gerade spezifizierte Modifikation von DES macht sowohl Software-Implementierungen [Aßma_88] als auch MDES-Chips [BeFG_89] nicht komplizierter und langsamer, sondern eher etwas einfacher und schneller. Die Produktionskosten eines MDES-Chips dürften also etwas geringer als die eines DES-Chips sein.

Variable Substitutions- und Permutationsboxen: Eine zur gerade besprochenen orthogonale, aber etwas aufwendigere Verallgemeinerung ist, Implementierungen von DES so zu modifizieren, daß die Substitutions- und Permutationsboxen vom Anwender festgelegt werden können, ihre Werte also Bestandteil des entsprechend verlängerten Schlüssels würden.

Bei einer Hardware-Implementierung müßten für jede der 8 Substitutionsboxen statt 2^6•4 Bit ROMs dann 2^6•4 Bit RAMs verwendet werden. Diese 2048 Bit könnten direkt Bestandteil des Schlüssels sein und müßten in jedem Fall vor dem Ver- bzw. Entschlüsselungsvorgang eingelesen und für die Dauer der Ver- bzw. Entschlüsselung gespeichert werden.

Macht man die Werte aller Permutationsboxen variabel und wählt eine für eine schnelle Realisierung geeignete redundante Codierung, so werden 48•$\lceil \mathrm{ld}\ 32 \rceil$ = 48•5 Bit für die Permutation E und 32•$\lceil \mathrm{ld}\ 32 \rceil$ = 32•5 Bit für die Permutation P, zusammen also 400 Bit, als Codierung

benötigt. Diese 400 Bit müßten ebenfalls vor dem Verschlüsselungsvorgang eingelesen werden und auch sie könnten direkt Bestandteil des Schlüssels sein.

Da sich bisher geäußerte Kritik vor allem auf die Substitutionsboxen bezieht [DaPr_84 Seite 70 bis 76], genügt es vermutlich, nur diese variabel zu machen, so daß dann höchstens 2048 Bit als zusätzliche Schlüsselbits benötigt werden. Auch hier ist natürlich die Abwärtskompatibilität und die „beweisbare“ Steigerung der Sicherheit gegeben. Diesmal ist bezüglich des Beweises aber etwas Skepsis angebracht, da – wie die Diskussion über die Substitutionsboxen zeigt – die Sicherheit von ihrer Wahl abhängt. Allerdings ist die Wahrscheinlichkeit, bei zufälliger Wahl gute Substitutionsboxen zu definieren, vermutlich überwältigend groß [CaMa_86 Seite 93] – der konservative Anwender mag sich natürlich auch mit einer Permutation der Substitutionsboxen zufriedengeben, indem er die Originalwerte an andere Stellen einliest.

Die gerade beschriebenen Verallgemeinerungen machen Software-Implementierungen zwar etwas umfangreicher, senken aber bei geschickter Implementierung die Verschlüsselungsleistung nicht [Aßma_88]. Leider macht die gerade beschriebene Modifikation von DES-Chips sie nicht nur etwas komplizierter, sondern auch langsamer: Erstens ist die Verzögerungszeit durch RAMs üblicherweise etwas größer als die durch ROMs. Zweitens vergrößert der Verdrahtungsaufwand variabler Permutationen die benötigte Chip-Fläche und dadurch die Laufzeiten. Die Verschlüsselungsleistung der modifizierten Chips ist also bei Einsatz variabler Substitutions- und/oder Permutationsboxen etwas geringer, ihre Produktionskosten dürften sich jedoch in keinem Fall in nennenswerter Weise erhöhen.

Komposition von DES und verallgemeinertem DES: Genügen einem die bei den vorherigen zwei Punkten erwähnten „Beweise“ nicht, so kann man erst 16 Runden gemäß DES und danach weitere 16 Runden mit den vorher erwähnten Verallgemeinerungen verschlüsseln. Werden die Schlüssel für die Verschlüsselung gemäß DES und die gemäß der Verallgemeinerung unabhängig gewählt, so ist das durch Komposition entstehende Kryptosystem nun mindestens so sicher wie DES. Leider ist die Verschlüsselungseffizienz der Komposition nur etwa halb so groß wie die von DES – aber auch dies ist bei der Leistungsfähigkeit und den Kosten heutiger Chips überhaupt kein Problem.

Zusätzliche Runden: Bei Vermeidung der Schlüsselexpansion kann die Anzahl der Runden beliebig erhöht werden. Das entstehende Kryptosystem ist (bei Vermeidung der Schlüsselexpansion) mindestens so sicher wie das mit weniger Runden. Die Verschlüsselungsleistung ist in etwa umgekehrt proportional zur Rundenzahl.

Der *Mehraufwand* dieser vier verallgemeinernden Modifikationen von jeweils einigen hundert zusätzlichen Schlüsselbits, die ja ausgetauscht und zumindest für kurze Zeit gespeichert werden müssen, mag zur Zeit der Definition von DES erheblich gewesen sein. Heutzutage und erst recht für die Zukunft ist er es nicht:

Einerseits ist die Übertragungsgeschwindigkeit und Speicherkapazität inzwischen um mehrere Größenordnungen gewachsen, was als Rechtfertigung allein schon genügt.

Andererseits werden zunehmend **hybride Konzelationssysteme** eingesetzt, d. h. ein asymmetrisches (und möglicherweise ineffizientes) Konzelationssystem wird zum Austausch eines Schlüssels eines symmetrischen (und möglicherweise viel effizienteren) Konzelationssystems verwendet. Mit dem symmetrischen Konzelationssystem werden dann die Nachrichten

verschlüsselt. Da alle mir bekannten sicheren asymmetrischen Konzelationssysteme die Eigenschaft haben, daß es genau oder zumindest fast gleich viel Rechen-, Übertragungs- und Speicheraufwand verursacht, gleichgültig ob der Schlüssel des symmetrischen Konzelationssystems einige zehn oder einige hundert Bit lang ist, stellt die Erfindung der asymmetrischen Konzelationssysteme, die erst nach der Definition von DES stattfand, eine zusätzliche Rechtfertigung für die obigen verallgemeinernden Modifikationen dar.

In [VHVD_88] werden teilweise andere *Modifikationen* von DES befürwortet und es wird angestrebt, durch einen modularen Entwurf von DES-Chips Modifikationen des Entwurfs und damit eine kürzere Entwicklungszeit für effiziente Implementierungen von DES-Modifikationen zu erreichen. Da bei letzterem Ansatz aber alle betroffenen Partner bei jeder DES-Modifikation jeweils ein neues Chip oder gar Gerät kaufen müßten, ist dieser Ansatz für diensteintegrierende Kommunikationsnetze nur schwer durchführbar und damit bei weitem nicht so ökonomisch wie der von mir vorgeschlagene Ansatz einer festen, dafür aber beliebige *Verallgemeinerungen* unterstützenden Implementierung.

Literatur

Abbr_84 C. R. Abbruscato: Data Encryption Equipment; IEEE Communications Magazine Vol. 22, No. 9, September 1984, Seite 15 bis 21.

AbJe_87 Marshall D. Abrams, Albert B. Jeng: Network Security: Protocol Reference Model and the Trusted Computer System Evaluation Criteria; IEEE Network, The Magazine of Computer Communications, Vol. 1, No. 2, April 1987, Seite 24 bis 33.

Adam_86 John A. Adam: Counting the weapons; 1. Part of Special report Verification: Peacekeeping by technical means; IEEE Spectrum Vol. 23, Nu. 7, July 1986, Seite 46 bis 56.

Adam_87 John Adam: French commercial satellite Spot furnishes data on earth's resources; The Institute, News Supplementum to IEEE Spectrum April 1987, Seite 11.

Alba_83 A. Albanese: Star Network With Collision-Avoidance Circuits; The Bell System Technical Journal (BSTJ) Vol. 62, Nu. 3, March 1983, Seite 631 bis 638.

AlFi_77 Marcelo Alonso, Edward J. Finn: Physik; Deutsche Übersetzung von Anneliese Schimpl, Herausgegeben von Wolfgang Muschik; Inter European Editions, Amsterdam, 1977.

Alke_88 Horst Alke: DATENSCHUTZBEHÖRDEN: Alles registriert – nur beim Autotelefon? Registrierung durch die DBP beim normalen Telefon; Vollspeicherung beim Autotelefondienst; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Vieweg & Sohn, Wiesbaden, 1/88, Heft 1, Januar 1988, Seite 4 bis 5.

AlSc_83 Bowen Alpern, Fred B. Schneider: Key exchange Using 'Keyless Cryptography'; Information Processing Letters Vol. 16, 26 February 1983, Seite 79 bis 81.

Amst_83 Stanford R. Amstutz: Burst Switching -- An Introduction; IEEE Communications Magazine Vol. 21, No. 8, November 1983, Seite 36 bis 42.

Ande_84 T. Anderson: Can Design Faults be Tolerated?; Proceedings Fehlertolerierende Rechensysteme, 2. GI/NTG/GMR-Fachtagung Bonn, September 1984, K.-E. Großpietsch und M. Dal Cin (Hrsg.), Informatik-Fachberichte IFB 84, Springer-Verlag Heidelberg, 1984, Seite 426 bis 433.

AnLe_81 T. Anderson, P. A. Lee: Fault Tolerance - Principles and Practice; Prentice Hall, Englewood Cliffs, New Jersey, 1981.

ApSP_87 Theodore K. Apostolopoulos, Efstathios D. Sykas, Emmanuel N. Protonotarios: Analysis of a New Retransmission Control Algorithm for Slotted CSMA/CD LAN's; IEEE Transactions on Computers Vol. C-36, Nu. 6, June 1987, Seite 692 bis 701.

Aßma_88 Ralf Aßmann: Effiziente MC 68000 Assembler-Implementierung von verallgemeinertem DES; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Juli 1988; erweitert und umgewandelt in die Diplomarbeit "Effiziente Software-Implementierung von verallgemeinertem DES", Abgabe Februar 1989.

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

Ath1_86 Tom Athanasiou: Encryption: Technology, Privacy, and National Security; Technology Review, Cambridge, Mass., Aug./Sept. 1986, Seite 57 bis 66.

Atha_86 Tom Athanasiou: Encryption and the dossier society; Processed World.

ATM_88 Asynchron durch die Glasfasern; Funkschau 1/1989, 30. Dezember 1988, Seite 52 bis 53.

Aviz_85 Algirdas Avizienis: The N-Version Approach to Fault-Tolerant Software; IEEE Transactions on Software Engineering Vol. SE-11, No. 12, December 1985, Seite 1491 bis 1501.

AvLa_86 A. Avizienis, J.-C. Laprie: Dependable Computing: From Concepts to Design Diversity; Proceedings of the IEEE Vol. 74, No. 5, May 1986, Seite 629 bis 638.

Baac_85 Clemens Baack: Optische Nachrichtentechnik und Integrierte Optik - Basistechnologie eines zukünftigen Breitband-ISDN; Telecommunications, Veröffentlichungen des Münchner Kreis, Band 11, W. Kaiser (ed.), in Zusammenarbeit mit der NTG, Springer-Verlag Heidelberg, 1985, Seite 352 bis 367.

BaBr_85 E. E. Basch, T. G. Brown: Introduction to Coherent Optical Fiber Transmission; IEEE Communications Magazine Vol. 23, No. 5, May 1985, Seite 23 bis 30.

BaCh_89 Ralph Ballart, Yau-Chau Ching: SONET: Now It's the Standard Optical Network; IEEE Communications Magazine Vol. 27, No. 3, March 1989, Seite 8 bis 15.

Bake_85 Richard H. Baker: The Computer Security Handbook; TAB Professional and Reference Books, TAB BOOKS Inc., P.O. Box 40, Blue Ridge Summit, PA 17214; 1985.

Bara_64 Paul Baran: On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations; Memorandum RM-3765-PR, August 1964, The Rand Corporation, 1700 Main St, Santa Monica, California, 90406 Reprinted in: Lance J. Hoffman (ed.): Security and Privacy in Computer Systems; Melville Publishing Company, Los Angeles, California, 1973, Seite 99 bis 123;.

BaSa_85 R. J. S. Bates, L. A. Sauer: Jitter accommodation in token-passing ring LANs; IBM Journal on Research and Development Vol. 29, No. 6, November 1985, Seite 580 bis 587.

Bauc_83 Helmut Bauch: BIGFON - die Übertragungstechnik; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 57 bis 62.

BaWe_83 Helmut Bauch, Karl Weinhardt: Communication in the Subscriber Area of Optical Broadband Networks; Optical Communications, A Telecommunications Review, SIEMENS, John Wiley & Sons Limited (Title of German original edition: telcom report Nachrichtenübertragung mit Licht), 1983, Seite 140 bis 146.

BCKK_83 Werner Bux, Felix H. Closs, Karl Kuemmerle, Heinz J. Keller, Hans R. Mueller: Architecture and Design of a Reliable Token-Ring Network; IEEE Journal on Selected Areas in Communications Vol. SAC-1, No. 5, November 1983, Seite 756 bis 765.

BeB2_88 Pierre Beauchemin, Gilles Brassard: A Generalization of Hellman's Extension to Shannon's Approach to Cryptography; Journal of Cryptology Vol. 1, No. 2, 1988, Seite 129 bis 131.

BeEG_86 F. Belli, K. Echtle, W. Görke: Methoden und Modelle der Fehlertoleranz; Informatik Spektrum Band 9, Heft 2, April 1986, Seite 68 bis 81.

BeEn_85 Larry A. Bergman, Sverre T. Eng: A Synchronous Fiber Optic Ring Local Area Network for Multigigabit/s Mixed-Traffic Communication; IEEE Journal on Selected Areas in Communications Vol. SAC-3, No. 6, November 1985, Seite 842 bis 848.

BeFG_89 Wilfried Beller, Jürgen Frößl, Thomas Giesler: Spezifikation und Implementierung eines erweiterten DES-Algorithmus als VENUS-Standardzellenchip; Studien-

arbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe (Betreuer: Oliver Haberl, Thomas Kropf), 1989.

Ber1_83 Thomas A. Berson: Long Key Variants of DES; Crypto 82, Plenum Press, New York 1983, Seite 311 bis 313.

BfD_85 Siebter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Dr. Baumann); gemäß Par. 19 Absatz 2 Satz 2 Bundesdatenschutzgesetz dem Deutschen Bundestag vorgelegt zum 1. Januar 1985; auch als Bundestags-Drucksache 10/2777 veröffentlicht.

BfD_86 Achter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Dr. Baumann); gemäß Par. 19 Absatz 2 Satz 2 Bundesdatenschutzgesetz dem Deutschen Bundestag vorgelegt zum 1. Januar 1986; auch als Bundestags-Drucksache 10/4690 veröffentlicht.

BfD_87 Neunter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Dr. Baumann); gemäß Par. 19 Absatz 2 Satz 2 Bundesdatenschutzgesetz dem Deutschen Bundestag vorgelegt zum 1. Januar 1987; auch als Bundestags-Drucksache 10/6816 veröffentlicht.

BfD_88 Zehnter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz (Dr. Baumann); gemäß Par. 19 Absatz 2 Satz 2 Bundesdatenschutzgesetz dem Deutschen Bundestag vorgelegt zum 1. Januar 1988; auch als Bundestags-Drucksache 11/1693 veröffentlicht.

BGJK_81 P. Berger, G. Grugelke, G. Jensen, J. Kratzsch, R. Kreibich, H. Pichlmayer, J. P. Spohn: Datenschutz bei rechnerunterstützten Telekommunikationssystemen; Bundesministerium für Forschung und Technologie Forschungsbericht DV 81-006 (BMFT-FB-DV 81-006), Institut für Zukunftsforschung GmbH Berlin, September 1981.

BlFM_88 Manuel Blum, Paul Feldman, Silvio Micali: Non-interactive zero-knowledge and its applications (extended abstract); 20th Symposium on Theory of Computing 1988, ACM, New York, Seite 103 bis 112.

BlGo_85 Manuel Blum, Shafi Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; Advances in Cryptology, Proc. of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 1984, Univ. of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 289 bis 299.

BlMi_84 Manuel Blum, Silvio Micali: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits; SIAM J. Comput. Vol. 13, No. 4, November 1984, Seite 850 bis 864.

BMTW_84 Toby Berger, Nader Mehravari, Don Towsley, Jack Wolf: Random Multiple-Access Communication and Group Testing; IEEE Transactions on Communications Vol. COM-32, Nu. 7, July 1984, Seite 769 bis 779.

Bock_86 Peter Bocker: ISDN, Das diensteintegrierende digitale Nachrichtennetz; Konzept, Verfahren, Systeme; In Zusammenarbeit mit G. Arndt, V. Frantzen, O. Fundneider, L. Hagenhaus, L. Schweizer Springer-Verlag Heidelberg 1986.

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

Bra2_83 Ewald Braun: BIGFON Brings the Optical Waveguide into the Subscriber Area; Optical Communications, A Telecommunications Review, SIEMENS, John Wiley & Sons Limited (Title of German original edition: telcom report Nachrichtenübertragung mit Licht), 1983, Seite 136 bis 139.

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

Brau_82 Ewald Braun: BIGFON - der Start für die Kommunikationstechnik der Zukunft; telcom report Band 5, Heft 2, 1982, Seite 123 bis 129.

Brau_83 Ewald Braun: BIGFON - Erprobung der optischen Breitbandübertragung im Ortsnetz; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 52 bis 53.

Brau_84 Ewald Braun: Systemversuch BIGFON gestartet; telcom report, SIEMENS, Band 7, Heft 1, 1984, Seite 9 bis 11.

Brau_87 E. Braun: BIGFON; Informatik-Spektrum Band 10, Heft 4, August 1987, Seite 216 bis 217.

BrCC_87 Gilles Brassard, David Chaum, Claude Crépeau: Minimum Disclosure Proofs of Knowledge; July 1987; received 5.2.1988.

Bric_85 Ernest F. Brickell: Breaking Iterated Knapsacks; Advances in Cryptology, Proceedings of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 19-22, 1984, University of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 342 bis 358.

BrLY_88 E. F. Brickell, P. J. Lee, Y. Yacobi: Secure audio teleconference; Proceedings of Crypto ´87, Carl Pomerance (ed.), Lecture Notes in Computer Science 293, Springer-Verlag, Berlin 1988, Seite 418 bis 426.

BrMo_83 Ewald Braun, Karl Heinz Moehrmann: Optical Communications in Short-Haul and Long-Haul Wideband Communication Networks; Optical Communications, A Telecommunications Review, SIEMENS, John Wiley & Sons Limited (Title of German original edition: telcom report Nachrichtenübertragung mit Licht), 1983, Seite 202 bis 205.

BrS1_86 Ewald Braun, Erhard Steiner: Überwachung und zusätzliche Dienste der Digitalübertragungssysteme für Lichtwellenleiter; SIEMENS telcom report 4/86, 9. Jahrgang Juli/August 1986, Seite 240 bis 245.

BrS2_86 Ewald Braun, Baldur Stummer: Grundausrüstung der Digitalübertragungssysteme für Lichtwellenleiter; SIEMENS telcom report 4/86, 9. Jahrgang Juli/August 1986, Seite 232 bis 239.

Bund_83 Bundesverfassungsgericht: Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 - 1 BvR 209/83 u. a.; DuD Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg&Sohn Verlagsgesellschaft Braunschweig, Heft 4, Oktober 1984, Seite 258 bis 281.

BüPf_86 Holger Bürk, Andreas Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Pre-prints of the Fourth Intern. Conference and Exhibition on Computer Security: Information Security: The Challenge, Monte Carlo, Dezember 1986, A. Grissonnanche (ed.), 1986, Seite 250 bis 263.

BüPf_87 Holger Bürk, Andreas Pfitzmann: Value Transfer Systems Enabling Security and Unobservability; Interner Bericht 2/87, Fakultät für Informatik, Universität Karlsruhe 1987; erscheint gekürzt in Computers & Security, North-Holland.

Bura_88 Axel Burandt: Informationstheoretisch unverkettbare Beglaubigung von Pseudonymen mit beliebigen Signatursystemen; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Mai 1988.

Bürk_86 Holger Bürk: Digitale Zahlungssysteme und betrugssicherer, anonymer Wertetransfer; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, April 1986.

Bürl_84 Gabriele Bürle: Leistungsvergleich von Sternnetz und Schieberegister-Ringnetz; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, 1984.

Bürl_85 Gabriele Bürle: Leistungsbewertung von Vermittlungs-/Verteilnetzen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, Mai 1985.

CACM6_87 General News and Notes: Computer Security Act Stresses Encryption Standard; Communications of the ACM, Vol. 30, Nu. 6, June 1987, Seite 572.

CaMa_86 John M. Carroll, Stephen Martin: Cryptographic Requirements for Secure Data Communications; IFIP/Sec. '86, Pre-prints of the Fourth Intern. Conference and Exhibition on Computer Security: Information Security: The Challenge, Monte Carlo, 2. - 4. Dezember 1986, A. Grissonnanche (ed.), 1986, Seite 90 bis 98.

Cha1_84 David Chaum: A New Paradigm for Individuals in the Information Age; Proceedings of the 1984 Symposium on Security and Privacy, IEEE, April 29 - May 2 1984, Oakland, California, Seite 99 bis 103.

Cha1_87 David Chaum: Demonstrating that a Public Predicate can be Satisfied Without Revealing Any Information About How; Advances in Cryptology – CRYPTO '86; Proceedings; August 11-15, 1986, University of California, Santa Barbara; A. M. Odlyzko (Ed.), Lecture Notes in Computer Science LNCS 263, Springer-Verlag Berlin, 1987, Seite 195 bis 199.

Cha3_85 David Chaum: The Dining Cryptographers Problem. Unconditional Sender Anonymity; Draft, received May 13, 1985.

Cha3_87 David Chaum: Security without Identification: Card Computers to make Big Brother Obsolete; Draft, received 24.6.1987.

Cha8_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM Vol. 28, Nu. 10, October 1985, Seite 1030 bis 1044.

Chau_81 David L. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM Vol. 24, Nu. 2, February 1981, Seite 84 bis 88.

Chau_83 David Chaum: Blind Signatures for untraceable payments; Advances in Cryptology, Proc. of Crypto 82, A Workshop on the Theory and Application of Cryptographic Techniques, August 1982, Univ. of California, Santa Barbara, D. Chaum, R. Rivest, A. Sherman (eds.), Plenum Press, New York, 1983, Seite 199 bis 203.

Chau_84 David Chaum: Design Concepts for Tamper Responding Systems; Advances in Cryptology, Proc. of Crypto 83, A Workshop on the Theory and Application of Cryptographic Techniques, August 1983, Univ. of California, Santa Barbara, Edited by David Chaum, Plenum Press, New York, 1984, Seite 387 bis 392.

Chau_87 David Chaum: Sicherheit ohne Identifizierung; Scheckkartencomputer, die den Großen Bruder der Vergangenheit angehören lassen; Informatik-Spektrum, Springer-Verlag, Heidelberg, 1987, Seite 262 bis 277; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Vieweg, Wiesbaden, Heft 1, Januar 1988, Seite 26 bis 41.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology, Springer-Verlag, Heidelberg, Vol. 1, Nu. 1, 1988, Seite 65 bis 75.

Chau_89 David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; SMART CARD 2000: The Future of IC Cards; Proc. of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. Oktober 1987, Seite 69 bis 93.

ChEv_86 David Chaum, Jan-Hendrik Evertse: Cryptanalysis of DES with a Reduced Number of Rounds; Sequences of Linear Factors in Block Ciphers; Advances in Cryptology, Proceedings of Crypto 85, A Conference on the Theory and Application of Cryptographic Techniques, August 18-22, 1985, University of California, Santa Barbara, Edited by Hugh C. Williams, Lecture Notes in Computer Science LNCS 218, Springer-Verlag Heidelberg, 1986, Seite 192 bis 211.

ChEv_87 David Chaum, Jan-Hendrik Evertse: A secure and privacy-protecting protocol for transmitting personal information between organizations; Advances in Cryptology – CRYPTO '86; Proceedings; August 11-15, 1986, University of California, Santa Barbara; A. M. Odlyzko (Ed.), Lecture Notes in Computer Science LNCS 263, Springer-Verlag Berlin, 1987, Seite 118 bis 167.

CoBD_86 Peter Cochrane, Rodney Brooks, Ronald Dawes: A High-Reliability 565 Mbit/s Trunk Transmission System; IEEE Journal on Selected Areas in Communications Vol. SAC-4, No. 9, December 1986, Seite 1396 bis 1403.

Coh2_87 Fred Cohen: Design and Administration of Distributed and Hierarchical Information Networks Under Partial Orderings; Computers & Security, North-Holland, Vol. 6, Nu. 3, June 1987, Seite 219 bis 228.

Cohe_84 Fred Cohen: Computer Viruses, Theory and Experiments; Proceedings of the 7th National Computer Security Conference, 1984, National Bureau of Standards, Gaithersburg, MD; USA, Seite 240 bis 263.

Cohe_87 Fred Cohen: Computer Viruses; Theory and Experiments; Computers & Security, North-Holland, Vol. 6, Nu. 1, February 1987, Seite 22 bis 35.

Czaa_82 Franz R. Czaak: Konzepte eines lokalen Netzwerks; Kommunikationstechnologien, Neue Medien in Bildungswesen, Wirtschaft und Verwaltung, Helmut Schauer, Michael J. Tauber (eds.), Schriftenreihe der Österreichischen Computer Gesellschaft Band 17, R. Oldenbourg Wien München 1982, Seite 341 bis 359.

Dail_84 Daily Telegraph: Meinungsumfrage; wiedergegeben in: Das Jahr im Bild 1984, 26. Jahrgang, Carlsen Verlag GmbH, Reinbek bei Hamburg, ISBN 3-551-45084-6, Seite 21.

DaPa_83 D. W. Davies, G. I. Parkin: The Average Cycle Size of the Key Stream in Output Feedback Encipherment; Cryptography; Proc. Burg Feuerstein 1982, Thomas Beth (Ed.); LNCS 149, Springer-Verlag, Heidelberg, 1983, Seite 263 bis 279.

DaPr_84 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, Chichester, New York, 1984.

DeDe_77 Dorothy E. Denning, Peter J. Denning: Certification of Programs for Secure Information Flow; Communications of the ACM Vol. 20, Nu. 7, July 1977, Seite 504 bis 513.

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

Denn_84 Dorothy E. Denning: Digital Signatures with RSA and Other Public-Key Cryptosystems; Communications of the ACM, Vol. 27, No. 4, April 1984, Seite 388 bis 392.

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

DeVG_84 Y. Desmedt, J. Vandewalle, R. Govaerts: Fast authentication using public key schemes; 1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6-8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog no. 84CH1998-4, Seite 191 bis 197.

Diff_82 Whitfield Diffie: Cryptographic Technology: Fifteen Years Forecast; acm SIGACT NEWS Vol. 14, Nu. 4, Fall-Winter 1982, Seite 38 bis 57.

DiH1_76 Whitfield Diffie, Martin E. Hellman: Multiuser cryptographic techniques; AFIPS conference proceedings Vol. 45, 1976 National Computer Conference, June 7-10, New York City, New York, Seite 109 bis 112.

DiH2_76 W. Diffie, M. E. Hellman: A Critique of the Proposed Data Encryption Standard; Communications of the ACM, Vol. 19, No. 3, March 1976, Seite 164 bis 165.

DiHe_76 W. Diffie, M. E. Hellman: New Directions in Cryptography; IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, Seite 644 bis 654.

DiHe_77 W. Diffie, M. E. Hellman: Exhaustive Cryptanalysis of the NBS Data Encryption Standard; Computer, IEEE, Vol. 10, Nu. 6, June 1977, Seite 74 bis 84.

DiHe_79 W. Diffie, M. E. Hellman: Privacy and Authentication: An Introduction to Cryptography; Proc. of the IEEE, Vol. 67, No. 3, March 1979, Seite 397 bis 427.

DINISO8372_87 DIN ISO 8372: Informationsverarbeitung – Betriebsarten für einen 64-bit-Blockschlüsselungsalgorithmus;

DuD_86 DuD AKTUELL; DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 1, Februar 1986, Seite 54 bis 56.

DuD4_87 DuD REPORT: Kompromißlose Datensicherheit und hohe Speicherleistung; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Heft 4, April 1987, Seite 204 bis 205.

DuDR_87 DuD REPORT: Kryptographie für die US-Privatwirtschaft, Exportbeschränkungen; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Vieweg & Sohn, Wiesbaden, 1/87, Heft 1, Januar 1987, Seite 53.

EcGM_83 Klaus Echtle, Winfried Görke, Michael Marhöfer: Zur Begriffsbildung bei der Beschreibung von Fehlertoleranz-Verfahren; Universität Karlsruhe, Fakultät für Informatik, Institut für Informatik IV, Interner Bericht Nr. 6/83 Mai 1983.

Eck_85 Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?; Computers & Security Vol. 4, Nu. 4, December 1985, Seite 269 bis 286.

ECMA89_85 ECMA European Computer Manufacturers Association: Standard ECMA-89; Local Area Networks Token Ring Technique; 2 nd Edition - March 1985 nearly identical with: ANSI/IEEE Std 802.5-1985, ISO/DP 8802/5 Local Area Networks, Token Ring Access Method, Approved December 13, 1984 IEEE Standards Board, Approved March 19, 1985 American National Standards Institute.

ECMA93_87 ECMA European Computer Manufacturers Association: Standard ECMA-93; Distributed Application for Message Interchange (MIDA); Second Edition - July 1987.

ECMATR42_87 ECMA European Computer Manufacturers Association: TR/42; Framework for Distributed Office Application; July 1987.

EcPf_85 Klaus Echtle, Andreas Pfitzmann: Software-Maßnahmen zur Fehlertoleranz; Skriptum zur Vorlesung, Institut für Informatik IV, Universität Karlsruhe, Wintersemester 1984/85.

Elek_82 Elektronik Sonderheft Nr. 50, Daten-Kommunikation; 8. Teil Einführung in die Datenfernverarbeitung, Lokale Netzwerke - die Basis für integrierte Informations-Systeme; Franzis-Verlag GmbH, Karlstr. 37 - 41, 8000 München 2, ISSN 0170-0898, 1982, Seite 69 bis 77.

EMMT_78 W. F. Ehrsam, S. M. Matyas, C. H. Meyer, W. L. Tuchman: A cryptographic key management scheme for implementing the Data Encryption Standard; IBM Systems Journal Vol. 17, No. 2, 1978, Seite 106 bis 125.

Even_89 Shimon Even: Secure Off-Line Electronic Fund Transfer Between Nontrusting Parties; SMART CARD 2000: The Future of IC Cards; Proc. of the IFIP WG 11.6 International Conference; Laxenburg (Austria), 19.-20. Oktober 1987, Seite 57 bis 66.

EvGY_84 S. Even, O. Goldreich, Y. Yacobi: Electronic Wallet; 1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6-8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog no. 84CH1998-4, Seite 199 bis 201.

FaLa_75 David J. Farber, Kenneth C. Larson: Network Security Via Dynamic Process Renaming; Fourth Data Communications Symposium, 7-9 October 1975, Quebec City, Canada, Seite 8-13 bis 8-18.

FeNS_75 Horst Feistel, William A. Notz, J. Lynn Smith: Some Cryptographic Techniques for Machine-to-Machine Data Communications; Proceedings of the IEEE Vol. 63, No. 11, November 1975, Seite 1545 bis 1554.

FO_87 FO: Ein Fall für Prometheus; ADAC motorwelt April 1987, Seite 50 bis 53.

Folt_87 Hal Folts: Open Systems Standards; IEEE Network, The Magazine of Computer Communications, Vol. 1, No. 2, April 1987, Seite 45 bis 46.

Free_88 Robert P. Freese: Optical disks become erasable; IEEE spectrum, Vol. 25, Nu. 2, February 1988, Seite 41 bis 45.

Freu_87 Johannes Freudenmann: Entwicklung von Kommunikationssoftware auf der Basis der Transformationstechnik; Kommunikation in Verteilten Systemen; GI/NTG-Fachtagung, Aachen, Februar 1987, Informatik-Fachberichte Band 130, N. Gerner und O. Spaniol (Hrsg.), Springer-Verlag, Heidelberg, Seite 725 bis 737.

Gall_85 Robert G. Gallager: A Perspective on Multiaccess Channels; IEEE Transactions on Information Theory Vol. IT-31, Nu. 2, March 1985, Seite 124 bis 142.

GiLB_85 David K. Gifford, John M. Lucassen, Stephen T. Berlin: The Application of Digital Broadcast Communication to Large Scale Information Systems; IEEE Journal on Selected Areas in Communications Vol. SAC-3, Nu. 3, May 1985, Seite 457 bis 467.

Gins_85 Hans J. Ginsburg: Computer, nein danke; Mit dem Vormarsch der neuen Technik wächst die Angst um den Job; DIE ZEIT Nr. 23, 31. Mai 1985, Seite 27 bis 28.

Goel_86 Ted Goeltz: Why not DES?; Computers & Security, North-Holland, Vol. 5, 1986, Seite 24 bis 27.

GoGM_84 Oded Goldreich, Shafi Goldwasser, Silvio Micali: How to Construct Random Functions (Extended Abstract); 25th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, October 24-26, 1984, Seite 464 bis 479.

GöKü_85 E. Göldner, P. J. Kühn: Integration of Voice and Data in the Local Area; First Intern. Conference on Data Communications in the ISDN Era, Tel-Aviv University, March 1985, Y. Perry (ed.), North Holland, IFIP 1985, Seite 103 bis 117.

Gol1_85 Oded Goldreich: On Concurrent Identification Protocols; Advances in Cryptology, Proceedings of EUROCRYPT 84, A Workshop on the Theory and Application of Cryptographic Techniques, April 9-11, 1984, Paris, France, Edited by T. Beth, N. Cot and I. Ingemarsson, Lecture Notes in Computer Science LNCS 209, Springer-Verlag Heidelberg, 1985, Seite 387 bis 396.

Gol1_87 Oded Goldreich: Two Remarks Concerning the Goldwasser-Micali-Rivest Signature Scheme; Advances in Cryptology – CRYPTO '86; Proceedings; August, 1986, Univ. of California, Santa Barbara; A. M. Odlyzko (Ed.), Lecture Notes in Computer Science LNCS 263, Springer-Verlag Berlin, 1987, Seite 104 bis 110.

Gol2_83 Oded Goldreich: On Concurrent Identification Protocols; Laboratory for Computer Science, Massachusetts Institute of Technology, MIT/LCS/TM-250, December 1983.

Gold_84 J. Goldberg: The Problem of Confidence in Fault-Tolerant Computer Design; GI-NTG-Fachtagung Architektur und Betrieb von Rechensystemen, Universität Karlsruhe, 26. - 28.3.1984, Informatik-Fachberichte Band 78, Springer-Verlag Heidelberg, Seite 347 bis 361.

Göld_85 Ernst-Heinrich Göldner: An Integrated Circuit/Packet Switching Local Area Network - Performance Analysis and Comparison of Strategies; 11th International Teletraffic Congress (ITC), Kyoto, Japan, September 1985.

GoMi_84 Shafi Goldwasser, Silvio Micali: Probabilistic Encryption; Journal of Computer and System Sciences Vol. 28, 1984, Seite 270 bis 299.

GoMR_84 Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Paradoxical Solution to the Signature Problem; 25th Annual Symposium on Foundations of Computer Science, IEEE Computer Society, October 24-26, 1984, Seite 441 bis 448.

GoMR_88 Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. Vol. 17, Nu. 2, April 1988, Seite 281 bis 308.

GoMT_82 Shafi Goldwasser, Silvio Micali, Po 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, Seite 134 bis 144.

GrFL_87 Albert G. Greenberg, Philippe Flajolet, Richard E. Ladner: Estimating the Multiplicities of Conflicts to Speed Their Resolution in Multiple Access Channels; Journal of the Association for Computing Machinery Vol. 34, No. 2, April 1987, Seite 289 bis 325.

Harb_86 Reb Harbinger: Geheime Nachrichtentechnik; - Im Kampf um die Information -; geheim-schriftliche- micro-fotographische- krypto-chemische- elektronische-steganografische- geheim-postalische- ... und andere Nachrichtenwaffen + Handbuch für den privaten Nachrichten-Schutz; Privatstudie, im Selbstverlag,

Copyright by Reb Harbinger, Urmanuskript in Englisch, Photoprinted in Switzerland, Vertrieb: Utilisation Est., Postadresse: PF 856, FL-9490 Vaduz, Vertragsdruck in der BR Deutschland.

HarM_85 Michael A. Harrison: Theoretical Issues Concerning Protection in Operating Systems; Advances in Computers, Edited by Marshall C. Yovits, Vol. 24, 1985, Seite 61 bis 100.

HeFi_80 Clayton L. Henderson, Allan M. Fine: Motion, Intrusion and Tamper Detection for Surveillance and Containment; Sandia Laboratories, Albuquerque, New Mexico 87185; SAND79-0792, Printed March 1980.

HeKW_85 Franz-Peter Heider, Detlef Kraus, Michael Welschenbach: Mathematische Methoden der Kryptoanalyse; DuD-Fachbeiträge 8, Vieweg, Braunschweig, 1985.

Hell_77 Martin E. Hellman: An Extension of the Shannon Theory Approach to Cryptography; IEEE Transactions on Information Theory Band IT-23, No. 3, May 1977, Seite 289 bis 294.

Hell_82 Martin E. Hellman: Cryptographic Key Size Issues; digest of papers compcon spring 1982, February 22-25, Seite 130 bis 131.

Hell_87 Martin E. Hellman: Commercial Encryption; IEEE Network, The Magazine of Computer Communications, Vol. 1, No. 2, April 1987, Seite 6 bis 10.

Herd_85 Siegfried Herda: Authenticity, Anonymity and Security in OSIS. An Open System for Information Services; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P.P.Spies, Informatik-Fachberichte Band 113, Springer-Verlag Berlin Heidelberg New-York Tokyo 1985, Seite 35 bis 50.

Hig1_86 Harold Joseph Highland: Random Bits&Bytes; The DES Revisited; Computers & Security, North-Holland, Vol. 5, Nu. 4, December 1986, Seite 281 bis 282.

Hig1_87 Harold Joseph Highland: Random Bits&Bytes; The Charade of Computer Security; Computers & Security, North-Holland, Vol. 6, Nu. 2, April 1987, Seite 108 bis 109.

High_87 Harold Joseph Highland: Random Bits&Bytes; The DES Revisited - Part II; Computers & Security, North-Holland, Vol. 6, Nu. 2, April 1987, Seite 100 bis 101.

Höck_85 Gunter Höckel: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, August 1985.

Hoff_87 Frank Hoffmeister: Ein Ansatz zur Abwehr von Computerviren; Organisation und Betrieb der verteilten Datenverarbeitung, 7. GI-Fachgespräch über Rechenzentren, München, März 1987, Informatik-Fachberichte (IFB) Band 134, Herausgegeben von F. Peischl, Seite 101 bis 110.

Home_?? Homer: Ilias; Diogenes Taschenbuch detebe 20779, übersetzt aus dem Altgriechischen von H. Voß; Diogenes Verlag, Zürich 1980.

HöPf_85 Gunter Höckel, Andreas Pfitzmann: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P.P.Spies, Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg 1985, Seite 113 bis 127.

Hor1_86 John Horgan: Encoding experts fault NSA security programs; The Institute, IEEE, Vol. 10, Nu. 9, September 1986, Seite 1, 2.

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

Horg_85 John Horgan: Thwarting the information thieves; IEEE Spectrum Vol. 22, Nu. 7, July 1985, Seite 30 bis 41.

Horg_86 John Horgan: NSA explains encryption program to IEEE Privacy Subcommittee; The Institute, IEEE, Vol. 10, Nu. 9, September 1986, Seite 2.

Hors_85 Patrick Horster: Kryptologie; Reihe Informatik/47, Herausgegeben von K. H. Böhling, U. Kulisch, H. Maurer, Bibliographisches Institut, Mannheim, 1985.

HuSW_83 Daniel E. Huber, Walter Steinlin, Peter J. Wild: SILK: An Implementation of a Buffer Insertion Ring; IEEE Journal on Selected Areas in Communications Vol. SAC-1, No. 5, November 1983, Seite 766 bis 774.

IBM_87 IBM: Keine Angst vor Computern; Die Einstellung der deutschen Bevölkerung zum Computer wird immer positiver; IBM Nachrichten 37. Jahrgang, Heft 288, April 1987, Seite 72 bis 73.

IEEE_87 IEEE: Apple opens its architecture with Macintosh II; Computer, IEEE, Vol. 20, No. 4, April 1987, Seite 92.

Inge_84 Ingemar Ingemarsson: Critique of the Security of Public-key Systems; 1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6-8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog no. 84CH1998-4, Seite 171 bis 173.

ISO7498SA_86 ISO: IS 7498 Addendum to the Basic Reference Model for OSI - Security Architecture (proposal); ISO TC 97/SC 21 N, proposed 1986-01-30.

ISO7498-2_87 ISO: Information processing systems – Open Systems Interconnection Reference Model – Part 2: Security architecture; DRAFT INTERNATIONAL STANDARD ISO/DIS 7498-2; ISO TC 97, Submitted on 1987-06-18.

ITG_87 ITG 1.6/01 Empfehlung 1987: ISDN-Begriffe; ntz Band 40, Heft 11, November 1987, Seite 814 bis 819.

Josh_85 Sunil P. Joshi: Making the LAN Connection with a Fiber Optic Standard; Computer Design September 1, 1985, Seite 64 bis 69.

Jung_87 Achim Jung: Implementing the RSA Cryptosystem; Computers & Security, North-Holland, Vol. 6, No. 4, 1987, Seite 342 bis 350.

Jurg_86 Ronald K. Jurgen: The Specialties; IEEE spectrum Vol. 23, No. 1, January 1986, Seite 86.

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

KaR1_86 Burton S. Kaliski, Ronald L. Rivest, Alan T. Sherman: Is DES a Pure Cipher? (Results of More Cycling Experiments on DES); (Preliminary Abstract); Advances in Cryptology, Proceedings of Crypto 85, A Conference on the Theory and Application of Cryptographic Techniques, August, 1985, Univ. of California, Santa Barbara, Edited by Hugh C. Williams, Lecture Notes in Computer Science LNCS 218, Springer-Verlag Heidelberg, 1986, Seite 212 bis 226.

Karg_77 Paul A. Karger: Non-Discretionary Access Control for Decentralized Computing Systems; Master Thesis, Massachusetts Institute of Technology, Laboratory for Computer Science, 545 Technology Square, Cambridge, Massachusetts 02139, May 1977, Report MIT/LCS/TR-179.

KaRS_86 Burton S. Kaliski, Ronald L. Rivest, Alan T. Sherman: Is the Data Encryption Standard a Group? (Preliminary Abstract); Eurocrypt 85, April 1985, Linz, Austria, Proc. edited by Franz Pichler, Lecture Notes in Computer Science LNCS 219, Springer-Verlag, Heidelberg, 1986, Seite 81 bis 95.

KaRS_88 Burton S. Kaliski, Ronald L. Rivest, Alan T. Sherman: Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES); Journal of Cryptology, Springer-Verlag, Heidelberg, Vol. 1, Nu. 1, 1988, Seite 3 bis 36.

KeMM_83 Heinz J. Keller, Heinrich Meyr, Hans R. Müller: Transmission Design Criteria for a Synchronous Token Ring; IEEE Journal on Selected Areas in Communications Vol. SAC-1, No. 5, November 1983, Seite 721 bis 733.

Ken1_81 Stephen T. Kent: Security Requirements and Protocols for a Broadcast Scenario; IEEE Transactions on Communications Vol. COM-29, No. 6, June 1981, Seite 778 bis 786.

Kent_80 Stephen Thomas Kent: Protecting Externally Supplied Software in Small Computers; PhD-Thesis, Massachusetts Institute of Technology, Laboratory for Computer Science, 545 Technology Square, Cambridge, Massachusetts 02139, September 1980, Report MIT/LCS/TR-255.

KlKl_83 P. Klein, G. Kleinke: BIGFON - Endgeräte und ihre Leistungsmerkmale; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 69 bis 77.

Kola_85 Gina Kolata: NSA to Provide Secret Codes; Science Vol. 230, October 1985, Seite 45 bis 46.

Kran_86 Evangelos Kranakis: Primality and Cryptography; Wiley-Teubner Series in Computer Science; B. G. Teubner Stuttgart, John Wiley & Sons, Chichester, 1986.

Krat_84 Herbert Krath: Stand und weiterer Ausbau der Breitbandverteilnetze; telematica 84, Juni 1984, Stuttgart, Kongreßband Teil 2 Breitbandkommunikation, W. Kaiser (Hrsg.), VDE-Verlag GmbH, Neue Mediengesellschaft Ulm mbH, Seite 3 bis 17.

Kub1_87 Herbert Kubicek: Für fernmeldetechnische Alternativen zum ISDN; PIK, Praxis der Informationsverarbeitung und Kommunikation, 10. Jahrgang 1987, April-Juni, Carl Hanser Verlag, München, Seite 87 bis 92.

Kub2_86 Herbert Kubicek: Zur sozialen Beherrschbarkeit integrierter Fernmeldenetze; GI-Fachtagung Arbeit und Informationstechnik, Juli 1986, Karlsruhe, Informatik-Fachberichte 123, Klaus Theo Schröder (Hrsg.), Springer-Verlag, Heidelberg, Seite 325 bis 350 unverändert nachgedruckt in: Kommunikation in Verteilten Systemen; GI/NTG-Fachtagung, Aachen, Februar 1987, Informatik-Fachberichte Band 130, herausgegeben von N. Gerner und O. Spaniol, Seite 787 bis 812.

KuRo_86 Herbert Kubicek, Arno Rolf: Mikropolis; Mit Computernetzen in die Informationsgesellschaft; 2. Auflage, VSA-Verlag, Hamburg 1986.

Lamp_73 Butler W. Lampson: A Note on the Confinement Problem; Communications of the ACM Vol. 16, Nu. 10, October 1973, Seite 613 bis 615.

Lang_84 Klaus Lange: Das Image des Computers in der Bevölkerung; GMD-Studien Nr. 80, März 1984, GMD, Schloß Birlinghoven, D-5205 St. Augustin 1.

Leuz_83 Ruth Leuze: Datenschutz für unsere Bürger; 4. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz 1983; Herausgegeben von der Landesbeauftragten für den Datenschutz Dr. Ruth Leuze, Marienstraße 12, 7000 Stuttgart.

Leuz_84 Ruth Leuze: Datenschutz für unsere Bürger; 5. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz 1984; Herausgegeben von der Landesbeauftragten für den Datenschutz Dr. Ruth Leuze, Marienstraße 12, 7000 Stuttgart.

Leuz_87 Ruth Leuze: Datenschutz für unsere Bürger; 8. Tätigkeitsbericht der Landesbeauftragten für den Datenschutz 1987; Herausgegeben von der Landesbeauftragten für den Datenschutz Dr. Ruth Leuze, Marienstraße 12, 7000 Stuttgart.

Li_87 Victor O. K. Li: Multiple Access Communications Networks; IEEE Communications Magazine Vol. 25, No. 6, June 1987, Seite 41 bis 48.

LiFl_83 John O. Limb, Lois E. Flamm: A Distributed Local Area Network Packet Protocol for Combined Voice and Data Transmission; IEEE Journal on Selected Areas in Communications Vol. SAC-1, No. 5, November 1983, Seite 926 bis 934.

LiHe_87 Richard A. Linke, Paul S. Henry: Coherent optical detection: a thousand calls on one circuit; IEEE spectrum Vol. 24, No. 2, February 1987, Seite 52 bis 57;.

Lipn_75 Steven B. Lipner: A Comment on the Confinement Problem; Proc. of the Fifth Symposium on Operating Systems Principles, November 1975, The University of Texas at Austin, Operating Systems Review Vol. 9, No. 5, Seite 192 bis 196.

Loep_85 Keith Loepere: Resolving Covert Channels Within a B2 Class Secure System; acm Operating Systems Review Vol. 19, Nu. 3, July 1985, Seite 9 bis 28.

LuR1_86 Michael Luby, Charles Rackoff: Pseudo-random Permutation Generators and Cryptographic Composition; Proceedings of the 18th Annual ACM Symposium on Theory of Computing, Berkeley, California, May 28-30, 1986, Seite 356 bis 363.

LuRa_86 Michael Luby, Charles Rackoff: How to Construct Pseudo-random Permutations from Pseudo-random Functions; Advances in Cryptology, Proc. of Crypto 85, A Conference on the Theory and Application of Cryptographic Techniques, August 1985, Univ. of California, Santa Barbara, Hugh C. Williams (Ed.), Lecture Notes in Computer Science LNCS 218, Springer-Verlag Heidelberg, 1986, Seite 447.

LuRa_88 Michael Luby, Charles Rackoff: How to Construct Pseudorandom Permutations from Pseudorandom Functions; SIAM Journal on Computing Vol. 17, No. 2, April 1988, Seite 373 bis 386.

Lutz_88 Karl Anton Lutz: ATM ermöglicht unterschiedliche Bitraten im einheitlichen Breitbandnetz; telcom report Siemens Aktiengesellschaft, Band 11, Heft 6, 1988, Seite 210 bis 213.

Mann_85 Andreas Mann: Fehlertoleranz und Datenschutz in Ringnetzen; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, Oktober 1985.

MaPf_87 Andreas Mann, Andreas Pfitzmann: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen; Kommunikation in Verteilten Systemen; GI/NTG-Fachtagung, Aachen, Februar 1987, Informatik-Fachberichte Band 130, N. Gerner und O. Spaniol (Hrsg.), Springer-Verlag, Heidelberg, Seite 16 bis 30; überarbeitete und erweiterte Fassung in DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Friedr. Vieweg & Sohn, Wiesbaden, Heft 8, August 1987, Seite 393 bis 405.

Marc_88 Eckhard Marchel: Leistungsbewertung von überlagerndem Empfangen bei Mehrfachzugriffsverfahren mittels Kollisionsauflösung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, April 1988.

MaRS_84 H. A. Maurer, N. Rozsenich, I. Sebestyen: Videotex without "Big Brother"; IIG, Universität Graz, Bericht F128, January 1984; erscheint in Electronic Publishing Review, Oxford, 1984.

Mass_81 James L. Massey: Collision-Resolution Algorithms and Random-Access Communications; Multi-User Communication Systems; G. Longo (Ed.); CISM Courses and Lectures No. 265, Springer-Verlag Wien, New York, 1981, Seite 73 bis 137.

MaYa_86 Jon W. Mark, Oliver W. W. Yang: Design and Analysis of a Metropolitan Area Network: A Two-Center Tree Net; Computer Networking Symposium, IEEE, November 17-18, 1986, Washington, DC, Seite 46 bis 54.

McLi_85 R. W. McLintock: Overview of International Standards for Transmission Impairments Affecting Digital Telecommunications Networks; Computer Networks and ISDN Systems Vol. 9, Nu. 5, May 1985, Seite 339 bis 344.

McMo_86 John McHugh, Andrew P. Moore: A Security Policy and Formal Top Level Specification for a Multi-Level Secure Local Area Network; Proceedings of the 1986 IEEE Symposium on Security and Privacy, April 7-9, 1986, Oakland, California, Seite 34 bis 39.

MeMa_82 Carl H. Meyer, Stephen M. Matyas: Cryptography – A New Dimension in Computer Data Security; (3rd printing) John Wiley & Sons, 1982.

Merr_83 Michael John Merritt: Cryptographic Protocols; Ph. D. Dissertation, School of Information and Computer Science, Georgia Institute of Technology, Feb. 1983.

MeSt_88 Willi Meier, Othmar Staffelbach: Fast Correlation Attacks on Stream Ciphers; Eurocrypt '88, LNCS 330, Springer-Verlag, Berlin 1988, Seite 301 bis 314.

Morr_78 Robert Morris: The Data Encryption Standard – Retrospective and Prospects; IEEE Communications Society Magazine Vol. 16, No. 6, Nov. 1978, Seite 11 bis 14.

MüSc_83 Christian Müller-Schloer: A Microprocessor-based Cryptoprocessor; IEEE Micro Vol. 3, No. 5, October 1983, Seite 5 bis 15.

NBS_87 NBS Journal of Research: Computer Security: A New Focus at the National Bureau of Standards; Computers & Security, North-Holland, Vol. 6, Nu. 2, April 1987, Seite 102 bis 103.

NePi_86 David B. Newman, Raymond L. Pickholtz: Cryptography in the Private Sector; IEEE Communications Magazine Vol. 24, No. 8, August 1986, Seite 7 bis 10.

NeSc_87 R. M. Needham, M. D. Schroeder: Authentication Revisited; acm Operating Systems Review Vol. 21, Nu. 1, January 1987, Seite 7.

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

Orwe_49 George Orwell: 1984; A Novel by George Orwell, A Signet Classic, New American Library, Times Mirror, New York, 1983.

OtRe_87 Dave Otway, Owen Rees: Efficient and Timely Mutual Authentication; acm Operating Systems Review Vol. 21, Nu. 1, January 1987, Seite 8 bis 10.

Papa_84 Petros Papadimitriou: Kürzeste Ringstrukturen und Kostenvergleich zu Sternstrukturen bei Kommunikationsnetzen; Studienarbeit am Institut für Informatik IV, Universität Karlsruhe, Dezember 1984.

Papa_86 Stavros Papastavridis: Upper and Lower Bounds for the Reliability of a Consecutive-k-out-of-n:F System; IEEE Transactions on Reliability Vol. R-35, Nu. 5, December 1986, Seite 607 bis 610.

Perr_84 Tekla Perry: Readers comment on computers' effect on privacy; The Institute, IEEE, April 1984, Seite 3.

Pete_87 Ulrich v. Petersdorff: Weltneuheit beim Berliner TEMEX-Versuch: Erprobung eines »intelligenten« Wasserzählers; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme, Friedr. Vieweg & Sohn, Braunschweig, Heft 12, Dezember 1987, Seite 575.

Pfi1_83 Andreas Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 18/83, Dezember 1983.

Pfi1_85 Andreas Pfitzmann: How to implement ISDNs without user observability - Some remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 14/85.

Pfi1_87 Andreas Pfitzmann: IFIP/Sec'86: Tagung über Rechnersicherheit; Computer und Recht, 3. Jahrgang, Heft 2, Februar 1987, Seite 141 bis 142.

Pfi2_87 Andreas Pfitzmann: Experten warnen vor der Geheimhaltung von Kryptosystemen; Computer und Recht, 3. Jahrgang, Heft 4, April 1987, Seite 272.

Pfit_83 A. Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; GI '83, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 411 bis 418.

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 Intern. Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 1984, Zurich, Switzerland, Proceedings IEEE Catalog no. 84CH1998-4, Seite 183 bis 190.

Pfit_85 A. Pfitzmann: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, P.P.Spies (Hrsg.), IFB 113, Springer-Verlag Heidelberg 1985, Seite 96 bis 112.

Pfit_86 A. Pfitzmann: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten?; DuD, Datenschutz und Datensicherung, Vieweg & Sohn, Wiesbaden, Heft 6, Dezember 1986, Seite 353 bis 359.

PfPf_89 Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes; Universität Karlsruhe 1989; erscheint in Proceedings of Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1989.

PfPW_87 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Technischer Datenschutz in offenen diensteintegrierenden Digitalnetzen; Tutorium: Kommunikation in Verteilten Systemen; 16. und 17. Februar 1987, RWTH Aachen, GI - Deutsche Informatik Akademie; herausgegeben von O. Spaniol, Seite 281 bis 312.

PfPW_88 A. Pfitzmann, B. Pfitzmann, M. Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik-Spektrum, Springer-Verlag, Heidelberg, Juni 1988, Seite 118 bis 142.

PfPW_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Garantierter Datenschutz für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß durch Telefon-MIXe; erscheint im Tagungsband der 4. SAVE-Tagung, 19.-21. April 1989, Köln; Überarbeitung und Erweiterung in DuD, Datenschutz und Datensicherung, Vieweg & Sohn, Wiesbaden.

PfWa_86 A. Pfitzmann, M. Waidner: Networks without user observability -- design options; Eurocrypt 85, A Workshop on the Theory and Application of Cryptographic Techniques, April 1985, Linz, Austria, Franz Pichler (ed.), Lecture Notes in Computer Science LNCS 219, Springer-Verlag, Heidelberg, 1986, Seite 245 bis 253; erweiterte Fassung „Networks without User Observability“ in Computers & Security, North-Holland, Vol. 6, Nu. 2, April 1987, Seite 158 bis 166.

Plum_82 Joan B. Plumstead: Inferring a Sequence Generated by a Linear Congruence; 23rd Annual Symposium on Foundations of Computer Science, November 3-5, 1982, Seite 153 bis 159.

PoGr_86 M. M. Pozzo, T. E. Gray: Computer Virus Containment in Untrusted Computing Environments; IFIP/Sec.'86, Pre-prints Fourth Intern. Conf. on Computer Security, Monte Carlo, Dez. 1986, A. Grissonnanche (ed.), 1986, Seite 118 bis 126.

PoGr_87 M. M. Pozzo, T. E. Gray: An Approach to Containing Computer Viruses; Computers & Security, North-Holland, Vol. 6, Nu. 4, Aug. 1987, Seite 321 bis 331.

PoKl_78 G. J. Popek, C. S. Kline: Issues in Kernel Design; Operating Systems, An Advanced Course, Lecture Notes in Computer Science LNCS 60, 1978; Springer Study Edition, 1979; Springer-Verlag, Heidelberg, Seite 209 bis 227.

PoST_88 Carl Pomerance, J. W. Smith, Randy Tuler: A pipeline architecture for factoring large integers with the Quadratic Sieve algorithm; SIAM J. Comput. Vol. 17, No. 2, 1988, Seite 387 bis 403.

PPfW_88 A. Pfitzmann, B. Pfitzmann, M. Waidner: Weitere Aspekte fernmeldetechnischer Alternativen zum ISDN; PIK, Band 11, Heft 1, 1988, Carl Hanser, München, Seite 5 bis 7.

Prei_88 Ralph J. Preiss: Classification of 'sensitive' information is once again in civilian hands; Computer, IEEE, Vol. 21, Nu. 3, March 1988, Seite 124.

Pric_88 W. L. Price: Standards for Data Security – A Change of Direction; Proceedings of Crypto ´87, Carl Pomerance (ed.), Lecture Notes in Computer Science 293, Springer-Verlag, Berlin 1988, Seite 3 bis 8.

PWP_87 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht (CR), Verlag Dr. Otto Schmidt KG, Köln, 3. Jahrgang, Okt., Nov., Dez. 1987, Hefte 10, 11, 12, Seiten 712 bis 717, 796 bis 803, 898 bis 904.

Rayc_85 Dipankar Raychaudhuri: Announced Retransmission Random Access Protocols; IEEE Transactions on Communications Vol. COM-33, No. 11, November 1985, Seite 1183 bis 1190.

REFE_83 Reference Manual for the Ada Programming Language; ANSI/MIL-STD-1815A-1983, February 17, 1983; Lecture Notes in Computer Science LNCS 155, Springer-Verlag, Heidelberg.

Rei1_86 Peter O'Reilly: Burst and Fast-Packet Switching: Performance Comparisons; IEEE INFOCOM '86, Fifth Annual Conference Computers and Communications Integration - Design, Analysis, Management, April 8-10, 1986, Miami, Florida, Seite 653 bis 666.

Rih1_87 Karl Rihaczek: Ein Kompromißvorschlag zur Datenverschlüsselung; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme; Vieweg & Sohn, Wiesbaden, Heft 6, Juni 1987, Seite 299 bis 303.

Riha_84 Karl Rihaczek: Datenverschlüsselung in Kommunikationssystemen; Möglichkeiten und Bedürfnisse; DuD-Fachbeiträge 6, Friedr. Vieweg & Sohn, Braunschweig, Wiesbaden, 1984.

Riha_85 Karl Rihaczek: Datenmißbrauch: Verhindern besser als verbieten; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, P.P.Spies (Hrsg.), Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg 1985, Seite 229 bis 236.

Riha_87 Karl Rihaczek: Datensicherheit amerikanisch; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme; Vieweg & Sohn, Wiesbaden, Heft 5, Mai 1987, Seite 240 bis 245.

RiSh_84 Ronald L. Rivest, Adi Shamir: How to Expose an Eavesdropper; Communications of the ACM, Vol. 27, No. 4, April 1984, Seite 393 bis 395.

Rive_87 R. L. Rivest: Network Control by Bayesian Broadcast; IEEE Transactions on Information Theory, Vol. IT-33, No. 3, May 1987, Seite 323 bis 328.

Roch_87 Edouard Y. Rocher: Information Outlet, ULAN versus ISDN; IEEE Communications Magazine Vol. 25, No. 4, April 1987, Seite 18 bis 32.

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, 11.-15. März 1985, Tagungsband 1, D. Heger, G. Krüger, O. Spaniol, W. Zorn (Hrsg.), Informatik-Fachberichte IFB 95, Springer-Verlag Heidelberg, Seite 202 bis 221.

Rose_86 R. Rosenberg: Slamming the door on data thieves; Can the NSA Create and Enforce a New Encryption Standard? Electronics February 3, 1986, Seite 27 bis 31.

Ross_86 Floyd E. Ross: FDDI - a Tutorial; IEEE Communications Magazine, Vol. 24, No. 5, May 1986, Seite 10 bis 17.

Ross_87 Floyd E. Ross: Rings are 'Round for Good!; IEEE network, The Magazine of Computer Communications, Vol. 1, No. 1, January 1987, Seite 31 bis 38.

RSA_78 R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM Vol. 21, No. 2, February 1978, Seite 120 bis 126.

Rue1_86 R. A. Rueppel: Correlation Immunity and the Summation Generator; Advances in Cryptology, Proceedings of Crypto 85, A Conference on the Theory and Application of Cryptographic Techniques, August 1985, Univ. of California, Santa Barbara, Edited by Hugh C. Williams, Lecture Notes in Computer Science LNCS 218, Springer-Verlag Heidelberg, 1986, Seite 260 bis 272.

Rue2_86 Rainer A. Rueppel: Analysis and Design of Stream Ciphers; Communications and Control Engineering Series, Editors: A. Fettweis, J. L. Massey, M. Thoma; Springer-Verlag, Heidelberg, 1986.

Rul1_87 Christoph Ruland: Datenschutz in Kommunikationssystemen; DATACOM Buchverlag, Pulheim, 1987.

RuR1_83 J. M. Rushby, B. Randell: A Distributed Secure System; Proceedings of the 1983 Symposium on Security and Privacy, IEEE, April 25 - 27 1983, Oakland, California, Seite 121 bis 126.

RuRa_83 John Rushby, Brian Randell: A Distributed Secure System; IEEE computer Vol. 16, Nu. 7, July 1983, Seite 55 bis 67.

Scha_83 Bernhard Schaffer: BIGFON - Vermittlungs- und Verteiltechnik; telcom report Siemens Aktiengesellschaft, Band 6, Heft 2, April 1983, Seite 63 bis 68.

Schl_87 Friedrich-Wilhelm Schlomann: Ost-Spionage: Der Griff auf die Datenverarbeitung; Datenschutz-Berater; Verlagsgruppe Handelsblatt, Düsseldorf, Nu. 5, 14. Mai 1987, Seite 8 bis 10.

Schö_84 Helmut Schön: Die Deutsche Bundespost auf ihrem Weg zum ISDN; The Deutsche Bundespost on its Way towards the ISDN; Zeitschrift für das Post- und Fernmeldewesen Heft 6 vom 27. Juni 1984.

Schö_86 Helmut Schön: ISDN und Ökonomie; Jahrbuch der Deutschen Bundespost 1986.

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

ScS1_86 Christian Schwarz-Schilling (ed.): Chance und Herausforderung der Telekommunikation in den 90er Jahren; Heft 4 aus der Schriftenreihe über Konzepte und neue Dienste der Telekommunikation des Bundesministers für das Post- und Fernmeldewesen, Bonn, 1986.

ScSc_83 Richard D. Schlichting, Fred B. Schneider: Fail-Stop Processors: An Approach to Designing Fault-Tolerant Computing Systems; acm TOCS Vol. 1, Nu. 3, August 1983, Seite 222 bis 238.

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

Sedl_88 Holger Sedlak: The RSA Cryptography Processor; Eurocrypt '87, Lecture Notes in Computer Science LNCS 304, Springer-Verlag, Heidelberg 1988, Seite 95 bis 105.

SeGo_86 Holger Sedlak, Ulrich Golze: Ein Public-Key-Code Kryptographie-Prozessor; Informationstechnik it, 28. Jahrgang, Heft 3/1986, Seite 157 bis 161.

Sha1_49 C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal Vol. 28, No. 4, October 1949, Seite 656 bis 715.

Sham_79 Adi Shamir: How to Share a Secret; CACM Vol. 22, Nu. 11, November 1979, Seite 612, 613.

Sham_84 Adi Shamir: A Polynomial-Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem; IEEE Transactions on Information Theory Vol. IT-30, Nu. 5, September 1984, Seite 699 bis 704.

Shan_48 C. E. Shannon: A Mathematical Theory of Communication; The Bell System Technical Journal Vol. 27, July/October 1948, Seite 379 bis 423 und 623 bis 656.

Shan_49 C. E. Shannon: Communication in the Presence of Noise; Proc. of the Institute of Radio Engineers, Band 37, Nummer 1, Januar 1949, Seite 10 bis 21; reprinted in Proceedings of the IEEE Vol. 72, No. 9, September 1984, Seite 1192 bis 1201.

Sie1_86 T. Siegenthaler: Design of Combiners to Prevent Divide and Conquer Attacks; Advances in Cryptology, Proceedings of Crypto 85, A Conference on the Theory and Application of Cryptographic Techniques, August, 1985, Univ. of California, Santa Barbara, Edited by Hugh C. Williams, Lecture Notes in Computer Science LNCS 218, Springer-Verlag Heidelberg, 1986, Seite 273 bis 279.

Sieg_84 T. Siegenthaler: Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications; IEEE Transactions on Information Theory Vol. IT-30, Nu. 5, September 1984, Seite 776 bis 780.

Sieg_85 T. Siegenthaler: Decrypting a Class of Stream Ciphers Using Ciphertext Only; IEEE Transactions on Computers Vol. C-34, Nu. 1, Jan. 1985, Seite 81 bis 85.

Sieg_86 T. Siegenthaler: Cryptanalysts Representation of Nonlinearly Filtered ML-Sequences; Eurocrypt 85, A Workshop on the Theory and Application of Cryptographic Techniques, April 1985, Linz, Austria, F. Pichler (ed.), Lecture Notes in Computer Science 219, Springer-Verlag, Heidelberg, 1986, Seite 103 bis 110.

SIEM_87 SIEMENS: Internationale Fernsprechstatistik 1987; Stand 1. Januar 1986; SIEMENS Aktiengesellschaft N ÖV Marketing, Postfach 70 00 73, D-8000 München 70, Mai 1987.

Simm_85 Gustavus J. Simmons: Authentication Theory/Coding Theory; Advances in Cryptology, Proc. of Crypto 84, August 19-22, 1984, University of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 411 bis 431.

Simm_86 Gustavus J. Simmons: The Practice of Authentication; Eurocrypt 85, A Workshop on the Theory and Application of Cryptographic Techniques, April 9-11, 1985, Johannes-Kepler-University, Linz, Austria, Proceedings edited by Franz Pichler, Lecture Notes in Computer Science LNCS 219, Springer-Verlag, Heidelberg, 1986, Seite 261 bis 272.

Simm_88 Gustavus J. Simmons: Message Authentication with Arbitration of Transmitter/Receiver Disputes; Eurocrypt '87, LNCS 304, Springer-Verlag, Heidelberg 1988, Seite 151 bis 165.

SiSw_82 Daniel P. Siewiorek, Robert S. Swarz: The Theory and Practice of Reliable System Design; Digital Press, Bedford, Massachusetts 01730, 1982.

Stan_85 I. W. Stanley: A Tutorial Review of Techniques for Coherent Optical Fiber Transmission Systems; IEEE Communications Magazine Vol. 23, No. 8, August 1985, Seite 37 bis 53.

Stan_87 Stand der Breitbandverkabelung; com, Siemens-Magazin für Computer & Communications 22. Jahrgang, 2/87, März/April 1987, Seite 2.

Steg_85 H. Stegmeier: Einfluß der VLSI auf Kommunikationssysteme; GI/NTG-Fachtagung Kommunikation in Verteilten Systemen, 11.-15. März 1985, Tagungsband 1, D. Heger, G. Krüger, O. Spaniol, W. Zorn (Hrsg.), Informatik-Fachberichte IFB 95, Springer-Verlag Heidelberg, Seite 663 bis 672.

Stin_88 D. R. Stinson: Some Constructions and Bounds for Authentication Codes; Journal of Cryptology, Springer-Verlag, Heidelberg, Vol. 1, Nu. 1, 1988, Seite 37 bis 51.

Stro_87 Norman C. Strole: The IBM token-ring network - A functional overview; IEEE network, The Magazine of Computer Communications, Vol. 1, No. 1, January 1987, Seite 23 bis 30.

Sumn_87 Eric E. Sumner: Technology Perspective; IEEE Network, The Magazine of Computer Communications, Vol. 1, No. 2, April 1987, Seite 41.

Surv_84 Survey finds EEs are more hopeful for technology's future, less concerned about privacy than general public; The Institute, IEEE, June 1984, Seite 1, 6.

SuSY_84 Tatsuya Suda, Mischa Schwartz, Yechiam Yemini: Protocol Architecture of a Tree Network with Collision Avoidance Switches; Links for the Future; Science, P. Dewilde and C. A. May (eds.); Proceedings of the International Conference on Communications - ICC '84, Amsterdam, The Netherlands, May 14-17, 1984, IEEE, Elsevier Science Publishers B. V. (North-Holland), Seite 423 bis 427.

SymG_84 Symposium der Hessischen Landesregierung: Informationsgesellschaft oder Überwachungsstaat - Strategien zur Wahrung der Freiheitsrechte im Computerzeitalter; Gutachten; 3. bis 5. September 1984 im Plenarsaal des Hessischen Landtages in Wiesbaden; Herausgegeben vom Hessendienst der Staatskanzlei, Postfach 3147, 6200 Wiesbaden;.

Sze_85 Daniel T. W. Sze: A Metropolitan Area Network; IEEE Journal on Selected Areas in Communications Vol. SAC-3, No. 6, November 1985, Seite 815 bis 824.

Tane_81 Andrew S. Tanenbaum: Computer Networks; Prentice-Hall, Englewood Cliffs, N. J., 1981.

Tane_88 Andrew S. Tanenbaum: Computer Networks; 2nd Edition, Prentice-Hall, Englewood Cliffs, N. J., 1988.

Tasa_83 Shuji Tasaka: Stability and Performance of the R-ALOHA Packet Broadcast System; IEEE Transactions on Computers, Vol. C-32, No. 8, August 1983, Seite 717 bis 726.

Thom_84 Ken Thompson: Reflections on Trusting Trust; Communications of the ACM, Vol. 27, No. 8, August 1984, Seite 761 bis 763.

Thom_87 Karl Thomas: Der Weg zur offenen Kommunikation; nachrichten elektronik+telematik net special ISDN – eine Idee wird Realität; Sondernummer Oktober 87, R. v. Decker's Verlag, Seite 10 bis 17.

Unge_84 Hans-Georg Unger: Trends in Optical Communications; Links for the Future; P. Dewilde and C. A. May (eds.); Proceedings of the International Conference on Communications - ICC '84, Amsterdam, The Netherlands, May 14-17, 1984, IEEE, Elsevier Science Publishers B. V. (North-Holland), Seite 153 bis 158.

VaVa_85 Umesh V. Vazirani, Vijay V. Vazirani: Efficient and Secure Pseudo-Random Number Generation (extended abstract); Advances in Cryptology, Proceedings of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 19-22, 1984, University of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 193 bis 202.

VHVD_88 I. Verbauwhede, F. Hoornaert, J. Vandewalle, H. De Man: Security Considerations in the Design and Implementation of a new DES chip; Eurocrypt '87, LNCS 304, Springer-Verlag, Heidelberg 1988, Seite 287 bis 300.

VoKe_83 V. L. Voydock, Stephen T. Kent: Security Mechanisms in High-Level Network Protocols; acm computing surveys Vol. 15, No. 2, June 1983, Seite 135 bis 171.

VoKe_85 Victor L. Voydock, Stephen T. Kent: Security in High-level Network Protocols; IEEE Communications Magazine Vol. 23, Nu. 7, July 1985, Seite 12 bis 24.

Waer_67 B.L. van der Waerden: Algebra II; Heidelberger Taschenbücher Band 23, Springer-Verlag Berlin, Heidelberg, New York 1967, 5. Auflage.

WaGo_84 William M. Waite, Gerhard Goos: Compiler Construction; Texts and Monographs in Computer Science, Springer-Verlag Heidelberg, 1984.

Waid_84 Michael Waidner: Datenschutz in Kommunikationsnetzen - Ein Modellierungsansatz; Studienarbeit am Institut für Informatik IV, Univ. Karlsruhe, Oktober 1984.

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

Waid_88 Michael Waidner: Betrugssicherheit durch kryptographische Protokolle beim Einsatz über Kommunikationsnetze; Arbeitsbericht über das DFG-Projekt Go 347/6-1; Interner Bericht 7/88 der Fakultät für Informatik, Universität Karlsruhe, April 1988.

Waid_89 Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Universität Karlsruhe 1989; erscheint in Proceedings of Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1989.

Walk_87 Bernhard Walke: Über Organisation und Leistungskenngrößen eines dezentral organisierten Funksystems; Kommunikation in Verteilten Systemen; GI/NTG-

Fachtagung, Aachen, Februar 1987, Informatik-Fachberichte Band 130, N. Gerner und O. Spaniol (Hrsg.), Springer-Verlag, Heidelberg, Seite 578 bis 591.

Wall_87 Paul Wallich: Putting speech recognizers to work; IEEE spectrum Vol. 24, Nu. 4, April 1987, Seite 55 bis 57.

WaP1_87 Michael Waidner, Birgit Pfitzmann: Anonyme und verlusttolerante elektronische Brieftaschen; Interner Bericht 1/87 der Fakultät für Informatik, Universität Karlsruhe 1987.

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; Proc. der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, P.P.Spies (Hrsg.), Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg 1985, Seite 128 bis 141; Überarbeitung in DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme, Vieweg & Sohn, Braunschweig, Heft 1, Februar 1986, Seite 16 bis 22.

WaPf_87 Michael Waidner, Birgit Pfitzmann: Verlusttolerante elektronische Brieftaschen; Proc. der 3rd International Conference on Fault-Tolerant Computing-Systems, 9. bis 11. September 1987, Bremerhaven, IFB 147, Springer-Verlag Heidelberg 1987, Seite 36 bis 50; überarbeitete Fassung in DuD 10 (1987) Seite 487 bis 497.

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

WaPf1_89 Michael Waidner, Birgit Pfitzmann: Serviceability in spite of Sender and Recipient Untraceability; Universität Karlsruhe 1989; erscheint in Proceedings of Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1989.

WaPP_87 Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; DuD, Datenschutz und Datensicherung, Recht und Sicherheit der Informations- und Kommunikationssysteme; Vieweg & Sohn, Wiesbaden, Heft 6, Juni 1987, Seite 293 bis 299.

Wein_87 Steve H. Weingart: Physical Security for the microABYSS System; Proc. 1987 IEEE Symp. on Security and Privacy, April 27-29, 1987, Oakland, California, Seite 52 bis 58.

WiHi_80 Deborah Williams, Harvey J. Hindin: Can software do encryption job?; Electronics July 3, 1980, Seite 102 bis 103.

Wil1_85 H. C. Williams: Some Public-Key Crypto-Functions as Intractable as Factorization; Cryptologia, Vol. 9, Nu. 3, July 1986, Seite 223 bis 237.

Will_85 H. C. Williams: Some Public-Key Crypto-Functions as Intractable as Factorization (Extended Abstract); Advances in Cryptology, Proc. of Crypto 84, A Workshop on the Theory and Application of Cryptographic Techniques, August 1984, Univ. of California, Santa Barbara, Edited by G. R. Blakley and David Chaum, Lecture Notes in Computer Science LNCS 196, Springer-Verlag Heidelberg, 1985, Seite 66 bis 70.

Yao1_82 Andrew C. Yao: Theory and Applications of Trapdoor Functions; 23rd Symposium on Foundations of Computer Science, November 3-5, 1982, Seite 80 bis 91.

ZaNi_87 M. Zafirovic-Vukotic, I. G. Niemegeers: An Evaluation of High Speed Local Area Network Access Mechanisms; Kommunikation in Verteilten Systemen; GI/NTG-Fachtagung, Aachen, Februar 1987, Informatik-Fachberichte Band 130, N. Gerner und O. Spaniol (Hrsg.), Springer-Verlag, Heidelberg, Seite 426 bis 440.

Bilderverzeichnis