[3] Brinckmann, H.: Rechtliche und politische Kontrolle einer neuen Infrastruktur. In: Gesellschaft für Rechts- und Verwaltungsinformatik (Hrsg.): Kommunikationstechnische Vernetzung. Rechtsprobleme, Kontrollchancen, Klienteninteressen. Darmstadt: Toeche-Mittler 1986, S. 25.

[4] Brinckmann, H.: Neue Netze – Neue Abhängigkeiten. Infrastruktur als Rahmenbedingung für Organisation von Arbeit. In: Schröder, K. T. (Hrsg.): Arbeit und Informationstechnik. GI-Fachtagung, Karlsruhe, Juli 1986, Proceedings. Informatik-Fachberichte 123. Berlin u. a.: Springer 1986, S. 61.

[5] Däubler, W.: Gestaltung neuer Technologien durch Recht?, Zeitschrift für Rechtspolitik 19, 42 (1986).

[6] Der Bundesminister für das Post- und Fernmeldewesen, Ref. 247: ISDN – die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen. Bonn: Selbstverlag 1984.

[7] Der Bundesminister für das Post- und Fernmeldewesen, Stab 202: Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur. Bonn: Selbstverlag 1984.

[8] Deutscher Bundestag, 10. Wahlperiode (Hrsg.): Große Anfrage der Fraktion DIE GRÜNEN: Ausbau der fernmeldetechnischen Infrastruktur I–III. Drucksachen 10/3334, 10/3335, 10/3336 des Deutschen Bundestages.

[9] Eurich, C.: Computerkinder. Reinbek: Rowohlt 1985.

[10] Fiedler, H.: Informationspolitik und Informationsrecht. In: Fischer, W., Mundhenke, E. (Hrsg.): Informationstechnik im öffentlichen Bereich. Baden-Baden: Nomos 1984, S. 88.

[11] Irmer, Th.: Die DBP auf dem Weg zum ISDN. In: Elias, D. (Hrsg.): Telekommunikation in der Bundesrepublik Deutschland 1982. Heidelberg/Hamburg: R. v. Decker's Verlag, G. Schenck 1982, S. 295.

[12] Kahl, P. (Hrsg.): ISDN – Das künftige Fernmeldenetz der Deutschen Bundespost. Heidelberg: R. v. Decker's Verlag, G. Schenck 1985.

[13] Klebe, Th., Roth, S. (Hrsg.): Information ohne Grenzen. Hamburg: VSA-Verlag 1987.

[14] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. April 1986 zum Entwurf einer Telekommunikationsordnung (TKO) vom November 1985. U. a. in: Der Berliner Datenschutzbeauftragte: Jahresbericht 1986. Berlin: Eigenverlag 1986, S. 32.

[15] Konferenz der Datenschutzbeauftragten des Bundes und der Länder: Entwurf einer Telekommunikationsordnung (E-TKO). Ergänzungen zur Entschließung der DSB-Konferenz vom 18. April 1986 aufgrund der Neufassung des Entwurfs vom April 1986. U. a. in: Der Berliner Datenschutzbeauftragte: Jahresbericht 1986, Berlin: Eigenverlag 1986, S. 33.

[16] Kubicek, H.: Zur sozialen Beherrschbarkeit integrierter Fernmeldenetze. In: Schröder K. T. (Hrsg.): Arbeit und Informationstechnik. GI-Fachtagung, Karlsruhe, Juli 1986, Proceedings. Informatik-Fachberichte 123. Berlin u. a.: Springer 1986, S. 324.

[17] Kubicek, H.: ISDN im Lichte von Demokratieprinzip und informationeller Selbstbestimmung, Datenschutz und Datensicherung 1/1987, 21.

[18] Kubicek, H., Rolf, A.: Mikropolis. Mit Computernetzen in die „Informationsgesellschaft", 2. Aufl. Hamburg: VSA-Verlag 1986.

[19] Mettler-Meibom, B.: Soziale Kosten in der Informationsgesellschaft, Überlegungen zu einer Kommunikationsökologie. Frankfurt/M.: S. Fischer 1987.

[20] Neumann, K.-H., Schnörig, Th.: Das ISDN – Ein Problemfeld aus volkswirtschaftlicher und gesellschaftspolitischer Sicht. In: Schwarz-Schilling, Chr. (Hrsg.): Jahrbuch der Deutschen Bundespost 1986. Bad Winsheim: Verlag für Wissenschaft und Leben Georg Heidecker 1986, S. 51.

[21] Pfitzmann, A., Pfitzmann, B., Waidner, M.: Technischer Datenschutz in dienstintegrierenden Digitalnetzen – Warum und wie?, Datenschutz und Datensicherung 3/1986, 178.

[22] Plank, K.-L.: Grundgedanken zur Gestaltung künftiger Fernmeldenetze. Heidelberg: R. v. Decker's Verlag, G. Schenck 1983.

[23] Rosenbrock, K. H.: ISDN – eine folgerichtige Weiterentwicklung des digitalen Fernsprechnetzes. In: Schwarz-Schilling, Chr. (Hrsg.): Jahrbuch der Deutschen Bundespost 1984. Bad Winsheim: Verlag für Wissenschaft und Leben Georg Heidecker 1984, S. 509.

[24] Scherer, J.: Telekommunikationsrecht und Telekommunikationspolitik. Baden-Baden: Nomos 1985.

[25] Schnöring, Th. (Hrsg.): Gesamtwirtschaftliche Effekte der Informations- und Kommunikationstechnologien. Berlin u. a.: Springer 1986.

[26] Schön, H.: ISDN und Ökonomie. In: Schwarz-Schilling, Chr. (Hrsg.): Jahrbuch der Deutschen Bundespost 1986. Bad Winsheim: Verlag Wissenschaft und Leben Georg Heidecker 1986, S. 9.

[27] Steinmüller, W.: Soziale Beherrschbarkeit offener Netze, ÖVD/Online 10/1985, 146.

[28] Volpert, W.: Zauberlehrlinge. Weinheim: Beltz 1985.

Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen*

Andreas Pfitzmann, Andreas Mann

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

In digitalen Kommunikationssystemen können die Nutzdaten effizient durch Ende-zu-Ende-Verschlüsselung geschützt werden.

Technisch weitaus aufwendiger und bezüglich Fehlertoleranz erheblich schwieriger ist der Schutz der aus den Vermittlungsdaten leicht berechenbaren Verkehrsdaten, wer wann wieviel mit wem kommuniziert. Verkehrsdaten werden wirkungsvoll und für den Netzbenutzer überprüfbar

* Dies ist eine Überarbeitung unseres Beitrags zur GI/NTG-Fachtagung „Kommunikation in Verteilten Systemen", die im Februar 1987 in Aachen stattfand.

nur dadurch geschützt, daß die Erfassung der Vermittlungsdaten unmöglich gemacht wird. Dies ist in idealer Weise dann der Fall, wenn die Benutzung eines Kommunikationssystems unbeobachtbar durch Unbeteiligte und den Netzbetreiber sowie anonym gegenüber dem Kommunikationspartner erfolgen kann. Um dies näherungsweise zu realisieren, wurden in den letzten Jahren drei Konzepte für Datenschutz garantierende Kommunikationssysteme vorgeschlagen. Alle drei garantieren im fehlerfreien Fall die Anonymität der Netzbenutzer voreinander und vor dem Netzbetreiber, es sei denn, die Netzbenutzer identifizieren sich explizit.

Da in einem realen Kommunikationssystem Fehler auftreten, wird untersucht, ob und wie diese unter Erhaltung der Anonymität der Netzbenutzer toleriert werden können. Es gilt, die Diskrepanz zwischen der Fehlertoleranz, die eine globale Sicht des Gesamtsystems erfordern kann, und der Anonymität, die nur eine lokale Sicht des Gesamtsystems durch die Stationen der Netzbenutzer und den Netzbetreiber erlaubt, aufzulösen. Die drei Konzepte werden so erweitert, daß sie Fehler tolerieren, aber weiterhin Anonymität gewähren. Dabei stellt sich heraus, daß entweder zwischen Fehlertoleranz und Anonymität abzuwägen ist oder auf kontinuierliche Nutzleistung im Fehlerfall verzichtet werden muß.

Notation

S	Sender einer Nachricht
E	Empfänger einer Nachricht
N	Nutznachricht, die S an E sendet
A	Antwort, die E an S sendet
N_i	Nachricht an MIX_i
R_i	Zufallszahl, die von MIX_i entfernt und weggeworfen wird
K_i, k_i	Schlüssel (für MIX_i) eines symmetrischen Kryptosystems – es gilt für alle Nachrichten N: $K_i^{-1}(K_i(N)) = N$ und $k_i^{-1}(k_i(N)) = N$
$ö_x$	öffentlicher Schlüssel eines asymmetrischen Kryptosystems einer Station x
p_x	privater Schlüssel eines asymmetrischen Kryptosystems einer Station x – es gilt für alle zusammengehörigen Schlüsselpaare p_x, $ö_x$ und Nachrichten N: $p_x(ö_x(N)) = N$
$L_{i\to j}$	Leitung von Station i zu Station j.

1 Einleitung

Heute betreibt die Deutsche Bundespost mehrere voneinander unabhängige Netze, z. B. Vermittlungsnetze wie das analoge Telefonnetz sowie das Integrierte Text- und Datennetz in digitaler Technik (IDN) und Verteilnetze wie die analogen lokalen Breitbandkabelverteilnetze. Aus Kosten- und Leistungsgründen plant die Post, im Laufe der nächsten Jahre (1988–2020) alle Dienste in *ein* Netz zu integrieren und dazu ab 1988 ein ISDN (Integrated Services Digital Network) und ab 1992 ein IBFN (Integriertes Breitband-Fernmeldenetz) einzuführen [ScSc_84, ScS1_84]. Über das IBFN sollen alle heutigen Dienste wie z. B. Telefon, Teletex, Btx, Fernsehen usw. sowie verbesserte und neue Dienste abgewickelt werden. Durch die geplante Sternstruktur und die Vermittlung aller Dienste wird jedoch jeder Netzbenutzer durch Abhören seiner Anschlußleitung und, schlimmer noch, durch Auswertung der im Vermittlungsrechner anfallenden Daten vollständig beobachtbar. Damit ist das Erstellen von Persönlichkeitsprofilen *aller* Benutzer durch die Post, Geheimdienste und sogar (mittels Trojanischer Pferde [PoKl_78]) durch Hersteller von Vermittlungsrechnern möglich [PfPW_86]. Da einerseits das Fernmeldemonopol und andererseits ein für die Zukunft noch verstärkt zu erwartender gesellschaftlicher Druck zur Benutzung der oben beschriebenen Fernmeldedienste besteht, resultiert ein *faktischer Benutzungszwang* des entstehenden Kommunikationssystems, so daß dessen Gestaltung grundrechtsrelevant ist. Das von der Post geplante Kommunikationssystem gewährt aus den oben geschilderten Gründen dem Benutzer nicht das „Recht auf informationelle Selbstbestimmung ... grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen" [Bund_83]. Wendet man das Volkszählungsurteil des Bundesverfassungsgerichts sinngemäß an, dürfte das entstehende Kommunikationssystem verfassungswidrig sein, da preiswerte, leistungsfähige und, wie im folgenden zu zeigen sein wird, zuverlässige technische Alternativen zur Gestaltung des Kommunikationssystems vorhanden sind, die massenhafte Einschränkung des Rechtes auf informationelle Selbstbestimmung also vollkommen unnötig und unbegründet ist.

Die Beobachtbarkeit personenbezogener Daten an der Anschlußleitung durch Angreifer ohne Zugriff auf die Vermittlungseinrichtungen läßt sich durch geeignete, d.h. auch das Vorhandensein von Übertragungsdaten verbergende Leitungs-Verschlüsselung (link-by-link encryption) [Denn_82] vermeiden. Ebenso können die Nutzdaten, d.h. die dem Kommunikationssystem zum Transport übergebenen Daten, durch Ende-zu-Ende-Verschlüsselung (end-to-end encryption) sehr wirkungsvoll vor unbefugter Kenntnisnahme geschützt und ihre Veränderung erkannt werden; damit dies auch in *offenen* Systemen und nicht nur in *geschlossenen Benutzergruppen* möglich ist, müssen allerdings asymmetrische Kryptosysteme und Schlüsselaustauschprotokolle standardisiert werden – ein zwar sehr dringendes, aber eher Organisations- als Forschungsproblem, so daß wir es nicht weiter behandeln werden. Es ist in [Riha_87, Rih1_87, Pfit_87, WaPP_87] ausführlich diskutiert.

Technisch schwierig, d.h. ohne Berücksichtigung bereits bei der Planung des Kommunikationssystems praktisch unmöglich, ist der Schutz der Verkehrsdaten. Hierzu sind in der Literatur drei Konzepte veröffentlicht, wie Sender und Empfänger von Nachrichten oder zumindest die Beziehungen zwischen gesendeten und empfangenen Nachrichten unbeobachtbar bleiben können. Anders formuliert wird den Netzbenutzern die *Anonymität*, d.h. die Nicht-Personenbeziehbarkeit, zumindest der den Angreifer interessierenden Verkehrsereignisse garantiert (was im Gegensatz zur Unbeobachtbarkeit vor allen Unbeteiligten, also auch dem Netzbetreiber, die Abrechnung dann in keiner Weise erschwert). Diese Garantie bezieht sich nur auf Angriffe im bzw. mit Hilfe des Kommunikationssystems, die wegen ihres äußerst geringen Aufwands neben Individualüberwachung auch Massenüberwachung erlauben. Sie bezieht sich nicht auf die aufwendigen, dafür aber auch sehr viel weitergehenden klassischen Techniken zur Individualüberwachung: Richtmikrofone, Wanzen (miniaturisierte Abhörmikrofone), Observie-

rung durch Kameras oder direkt durch Menschen. Die drei Konzepte (in ihrer zeitlichen Entstehung) sind unter den folgenden Namen bekannt [PfPW_86, PfWa_86]:

MIX-Netz [Chau_81, Chau_84, Cha3_85, Pfi1_85]
RING-Netz [Pfit_83, Pfi1_83, Pfit_84, Höck_85, HöPf_85]
DC-Netz [Cha3_85, Cha8_85, Pfi1_85]

Das Konzept MIX-Netz besteht darin, daß ausgezeichnete Stationen im Netz, sogenannte MIXe, eine Menge von Nachrichten gleicher Länge sammeln und puffern, schon einmal bearbeitete Nachrichten ignorieren, die erstmals erhaltenen Nachrichten umschlüsseln und in einer zufälligen Reihenfolge ausgeben.

Das Konzept RING-Netz besteht darin, daß alle Stationen ringförmig verbunden werden, so daß jede alle Nachrichten empfängt und keine allein den Sender einer fremden Nachricht feststellen kann.

Das Konzept DC-Netz (Dining Cryptographers network [Cha3_85, Cha8_85 Referenz 2]) besteht darin, daß alle Stationen alle ihnen bekannten Schlüssel und ggf. zu sendenden Nachrichten überlagern (modulo 2 addieren) und nur das Ergebnis dieser lokalen Überlagerung ausgeben. Die Ausgaben aller Stationen werden global überlagert und das Ergebnis an alle Stationen verteilt. Da Schlüssel jeweils von einer Station generiert und genau einer anderen (vertraulich) mitgeteilt werden, heben sich beim globalen Überlagern alle Schlüssel auf, da sie jeweils genau zweimal modulo 2 addiert wurden. Nur die Summe aller gesendeten Nachrichten bleibt übrig (bei geeignetem Mehrfachzugriffsverfahren oftmals genau eine Nachricht).

Ausführlichere Erklärungen der Konzepte finden sich in den Kapiteln 3, 4 und 5, in denen dann auch die jeweils geeigneten Maßnahmen zur Fehlertoleranz beschrieben sind.

Die drei Konzepte unterscheiden sich insbesondere in ihrem jeweiligen *Angreifermodell* und der zugehörigen *Anonymitätsdefinition.*

Beim MIX- und DC-Netz wird der Angreifer als nahezu allmächtig angenommen. Er kann jederzeit alle Leitungen abhören, verfügt über sehr viel Rechnerleistung und kann an einigen Stellen Rechner besitzen oder mittels Trojanischer Pferde unterwandert haben, so daß er als normaler Netzbenutzer auftreten kann. Um die Anonymität der anderen Netzbenutzer trotz dieses starken Angreifers garantieren zukönnen, sind aufwendige kryptographische Mechanismen erforderlich, die sich insbesondere in den Kosten und der verminderten Nutzleistung des Gesamtsystems niederschlagen. Daher wurde mit dem RING-Netz ein preisgünstiges [Mann_85, Pfi1_85], leistungsfähiges [Bürl_85, Pfi1_85] Konzept vorgeschlagen, das auf Ringen und geeigneten Verfahren zum Mehrfachzugriff beruht. Dieses Konzept garantiert die Anonymität der Netzbenutzer jedoch nur gegenüber einem schwächeren Angreifer, der etwa nur eine Station, z.B. einen Protokollumsetzer (Gateway) zur Realisierung des in Abschnitt 7 erwähnten Vermittlungs-/Verteilnetzes, innerhalb des Ringes besitzt oder unterwandert hat. Dies ist dann sinnvoll, wenn vor allem Massenüberwachung ausgeschlossen und erst in zweiter Linie Individualüberwachung erschwert werden soll. Der Angreifer verfügt in diesem Fall über sehr viel Rechnerleistung, darf als Netzbenutzer auftreten und er darf eine beschränkte Auswahl an Leitungen abhören. Daß der Angreifer eine Station vollständig einkreist, indem er beide Leitungen abhört oder indem er die beiden Nachbarstationen der Station kontrolliert, wird jedoch durch die physische Leitungsführung, z.B. direkte Verkabelung von Wohnungen eines Mehrfamilienhauses, real sosehr erschwert, daß er mit dem gleichen Aufwand den beobachteten Teilnehmer mit den Techniken zur Individualüberwachung umfassender direkt beobachten könnte. Deshalb wird dies im Angreifermodell des RING-Netzes ausgeschlossen. Das Angreifermodell ist in Bild 1 graphisch dargestellt.

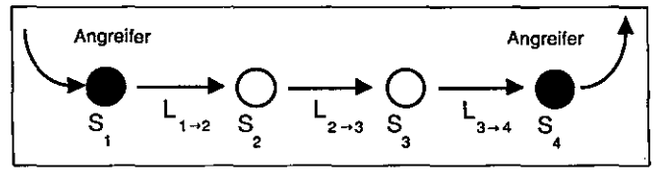

Bild 1 Stärkster zulässiger Angreifer beim RING-Netz kontrolliert die Stationen S_1 und S_4 bzw. die Leitungen $L_{1\to2}$ und $L_{3\to4}$.

Ebenso wie in ihrem jeweiligen Angreifermodell unterscheiden sich die drei Konzepte in der zugehörigen *Anonymitätsdefinition.*

Im MIX-Netz gilt eine *Kommunikationsbeziehung* als anonym, wenn es dem Angreifer nicht gelingt festzustellen, welcher Netzbenutzer mit welchem Netzbenutzer kommuniziert [Chau_81]. Jede von einem Netzbenutzer gesendete Nachricht sollte an jeden anderen Netzbenutzer gerichtet und jede von einem Netzbenutzer empfangene Nachricht von jedem Netzbenutzer gesendet worden sein können. Im RING- und DC-Netz wird nicht nur die Kommunikationsbeziehung, sondern bereits das *Senden* und *Empfangen* geschützt, d.h. jede Station sollte Sender einer gesendeten bzw. Empfänger einer empfangenen Nachricht sein können. Schutz des Sendens und Empfangens impliziert den Schutz der Kommunikationsbeziehung. Der Schutz des Empfangens geschieht durch Verteilung aller Nachrichten an alle Stationen und Verwendung von sogenannten *impliziten Adressen* [Waid_85, PfPW_86, PfWa_86], die zwar von der Station des intendierten Empfängers erkannt werden (was genügt, damit die Station diese Nachrichten weiter verarbeitet, anzeigt, etc.), im Gegensatz zu *expliziten Adressen* aber keinen Ort im Netz beschreiben, wodurch auch andere den Empfänger identifizieren könnten. Im RING-Netz kann ein Angreifer, der einige Stationen umzingelt hat, nur feststellen, daß eine oder mehrere von ihnen senden, nicht aber welche Nachricht von welcher Station genau gesendet wurde. Im DC-Netz gewinnt ein Angreifer, der Leitungen abhört und einige Stationen unterwandert hat, durch seine Beobachtungen keine zusätzliche Information über den Sender von Nachrichten, solange die Gruppe der Sender bezüglich der paarweise vertraulich ausgetauschten und beim Senden überlagerten Schlüssel zusammenhängt [Cha3_85].

Die stärkstmögliche Form von Anonymität wäre, daß eine Beobachtung dem Angreifer keine zusätzliche Information über den Sender bzw. Empfänger einer Nachricht liefert. (Ist der Angreifer selbst Sender oder Empfänger oder ist es jemand, der mit dem Angreifer kooperiert, so würde der Angreifer es sowieso erfahren, so daß er auch in diesen Fällen durch seine Beobachtung keine *zusätzliche* Information erhält.) Dies bedeutet nach [Shan_49], daß für alle Netzbenutzerpaare die Wahrscheinlichkeit, daß sie miteinander kommunizieren, für den Angreifer vor und nach seiner Beobachtung gleich ist.

Für das RING- und DC-Netz ist für das jeweilige Angreifermodell in [HöPf_85, Höck_85] bzw. [Cha3_85] bewiesen, daß die jeweils definierte Anonymität des Senders gegeben ist. Ein Beweis der Anonymität des Empfängers bei Verteilung ist trivial, er erfordert jedoch bei impliziter Adressierung durch Verschlüsselung zur Zeit nicht beweisbare aber nach Kräften validierte komplexitätstheoretische Annahmen. Dieselben Annahmen erfordert ein Beweis der Anonymität der Kommunikationsbeziehung bei Verwendung des

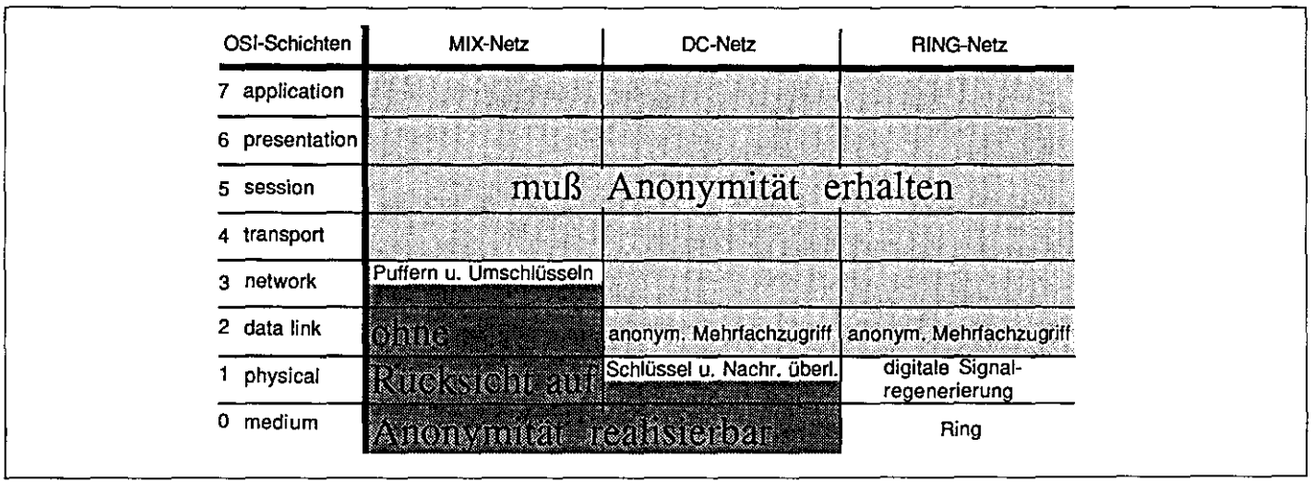

Bild 2 Einbettung der drei Konzepte in ein Kommunikationssystem. Die dunkel unterlegten Schichten können ohne Rücksicht auf die Unbeobachtbarkeit bzw. Anonymität realisiert werden, die hell hinterlegten Schichten müssen die durch die nicht hinterlegten Schichten geschaffene Unbeobachtbarkeit bzw. Anonymität erhalten.

MIX-Netzes. Alle Beweise betreffen nur den fehlerfreien Fall, d.h. den Betrieb des Netzes, solange keine Fehler auftreten.

Des weiteren unterscheiden sich die drei Konzepte wesentlich in ihrer *Einbettung in ein Kommunikationssystem* [Pfi1_85]. Dies läßt sich an einem durch die Benutzt-Relation definierten Schichtenmodell veranschaulichen (Bild 2 zeigt die Schichten des ISO-OSI-Modells [DaZi_83]).

Dabei zerfällt das Kommunikationssystem im wesentlichen in drei Teile: Die am tiefsten liegenden Schichten, die ohne Rücksicht auf die Unbeobachtbarkeit bzw. Anonymität realisiert werden können, darüber liegende Schichten, die Unbeobachtbarkeit bzw. Anonymität schaffen, und nochmals darüberliegende Schichten, die die Unbeobachtbarkeit bzw. Anonymität erhalten müssen. Die mittleren Schichten nennen wir *Datenschutz-Schichten*. Beim MIX- und DC-Netz handelt es sich um eigenständige und heutzutage in Kommunikationssystemen nicht anzutreffende Algorithmen, d.h. um jeweils eine eigene Teilschicht (sublayer), die in ein Kommunikationssystem eingefügt wird. Das RING-Netz garantiert durch seine Topologie, eben Ringe, und digitale Signalregenerierung die Anonymität des Senders. Ohne digitale Signalregenerierung könnte ein Angreifer analoge Signal-Charakteristika benutzen, um die Entfernung des Senders zu ermitteln.

Es sei angemerkt, daß MIX-, DC- und RING-Netz Konzepte, d.h. virtuelle Kommunikationsnetze darstellen und deshalb in beliebigen höheren Schichten implementiert werden können [Pfi1_85]. Bei Implementierung in höheren Schichten erhält man zwar ein ineffizientes Netz, da manche Funktionen mehrfach implementiert und ausgeführt werden müssen und auch das RING-Netz dann aufwendige kryptographische Mechanismen erfordert, nämlich Verbindungs-Verschlüsselung zur Simulation der Unbeobachtbarkeit der Ring-Leitungen. Man erhält jedoch die Möglichkeit, Datenschutz ohne Kooperation des Netzbetreibers zumindest für Dienste mit geringen Leistungsanforderungen und unter vermutlich hohen Übertragungskosten zu realisieren.

Um die durch die Teilschicht „Schlüssel und Nachrichten überlagern" des DC-Netzes bzw. durch die Schichten „Ring" und „digitale Signalregenerierung" bereitgestellten Kanäle mit Mehrfachzugriff effizient zu nutzen, sind Protokolle zum *anonymen Mehrfachzugriff* nötig. Diese sind in Bild 2 gesondert eingezeichnet, da sie zum Betrieb des Netzes unbedingt notwendig sind. Durch die Forderung des Erhalts der Unbeobachtbarkeit bzw. Anonymität des Senders sind diese Protokolle in ihren Möglichkeiten besonders eingeschränkt und wegen der trotzdem zu leistenden Koordination aller Beteiligten, d.h. von jeweils mehr als zwei Parteien, schwieriger zu entwerfen und fehlertolerant zu machen als die der darüber liegenden Schichten.

Unbefriedigend bezüglich der praktischen Anwendbarkeit aller drei Konzepte ist die ausschließliche Betrachtung des fehlerfreien Falls. Im folgenden wird daher diskutiert, wie die drei Konzepte so erweitert werden können, daß Fehler tolerierbar sind. Die Problematik liegt darin, genug Information für die Fehlertoleranz bereitzustellen, ohne dadurch die Anonymität der Netzbenutzer zu gefährden. Beispielsweise wären explizite Sender- und Empfänger-Adressen in jeder Nachricht für die Fehlertoleranz vorteilhaft (fehlertolerante Wegsuche), würden jedoch sofort Sender und Empfänger jeder Nachricht identifizieren.

Die Auswirkungen von Fehlern lassen sich gut in dem Schichtenmodell von Bild 2 betrachten, in dem eine Schicht die Dienste tieferliegender Schichten benutzt und den höherliegenden Schichten ihre Dienste zur Verfügung stellt. Einerseits kann ein Fehler, der in einer Schicht auftritt, in dieser Schicht selbst oder in der nächsthöheren Schicht toleriert werden. Der Fehler kann auch zu einem Fehler in der nächsthöheren Schicht führen, welcher dann ebenfalls toleriert werden muß. Andererseits werden Systeme so gebaut, daß ein Fehler, der in einer Schicht auftritt, nie zu einem Fehler in der nächsttieferen Schicht führt.

Zwei wesentliche Sachverhalte motivieren diese Arbeit. Sollen anonyme Netze in der Praxis eingesetzt werden, so müssen einerseits harte *Verfügbarkeitsanforderungen* berücksichtigt werden. Andererseits sind alle drei Konzepte, wie sie bisher beschrieben wurden, *Seriensysteme* im Sinne der Zuverlässigkeit, d.h. fällt nur ein MIX aus, gehen alle Nachrichten, die über ihn laufen, verloren, fällt nur eine Station im RING-Netz oder DC-Netz aus, kann in diesen Netzen überhaupt nicht mehr kommuniziert werden [Pfi1_85]. Beides zusammen erfordert Maßnahmen zur *Fehlertoleranz*. In den Kapiteln 3, 4 und 5 werden wir die drei Konzepte einzeln behandeln. Zunächst wird jeweils das Grundkonzept noch einmal ausführlicher vorgestellt und die Serieneigenschaft hervorgehoben. Sodann werden mögliche Fehlertoleranz-Maßnahmen vorgestellt. Diese Gliederung erlaubt es dem Leser, jeden der drei Abschnitte gesondert zu lesen. Dadurch soll eine bessere Verständlichkeit, insbeson-

dere des Ineinandergreifens aller Fehlertoleranz-Maßnahmen in je einem Netz erreicht werden. In den Kapiteln 2 und 6 gehen wir auf einige Gemeinsamkeiten der Konzepte bzw. der für sie geeigneten Fehlertoleranz-Maßnahmen ein.

2 Gemeinsamkeiten der drei Konzepte

In allen drei Konzepten werden Nachrichten (N) zwischen Sender (S) und Empfänger (E) verschlüsselt übertragen, d.h. *Ende-zu-Ende-Verschlüsselung* wird eingesetzt. Damit wird verhindert, daß ein Angreifer fremde Nachrichten liest und evtl. aus den Nachrichteninhalten Informationen gewinnt. Aus Gründen der Fehlertoleranz bietet es sich an, Ende-zu-Ende-Protokolle zu verwenden, um Fehler in der Nachrichtenübertragung entdecken und ggf. beheben zu können; außerdem dienen diese Protokolle auch der Sicherheit (Schutz vor Erfolg von Angriffen). Durch Sequenznummern, Zeitstempel, fehlererkennende Codes u.ä. lassen sich Übertragungsfehler erkennen, um eine Wiederholung der Nachrichtenübertragung zu initiieren. Gleichzeitig lassen sich auch aktive Angriffe, z.B. das Wiederholen alter, ehemals gültiger Nachrichten erkennen (vgl. Kapitel 6). Damit die Protokollinformationen keine Anhaltspunkte über Sender bzw. Empfänger von Nachrichten liefern, sollten sie vernünftigerweise selbst unter der Ende-zu-Ende-Verschlüsselung „versteckt" werden. Dies wiederum impliziert, daß das verwendete Kryptosystem gegen Angriffe mit bekanntem Klartext sicher sein muß. Ansonsten könnte die starre Struktur der Nachrichten dazu verwendet werden, das Kryptosystem zu brechen. Die oben erwähnten Ende-zu-Ende-Protokolle sind nicht in der Lage, alle Fehler zu tolerieren bzw. so zu tolerieren, daß die Anonymität der Netzbenutzer gewährleistet bleibt, sondern sie helfen lediglich bei der Fehlerklasse der transienten Fehler (sporadisches Fehlerauftreten), sofern das Kommunikationssystem selbst intakt bleibt. Diese Fehlerklasse umfaßt beispielsweise verfälschte Nachrichten, einzelne verlorene oder verdoppelte Nachrichten u.ä.

Bei allen drei Konzepten kann man zur Leistungssteigerung *anonyme Kanäle* schalten [Pfi1_85]. Fehler in diesen Kanälen lassen sich mit denselben Maßnahmen wie bei einzelnen Nachrichten tolerieren. Die erforderlichen Zusatzinformationen müssen dann für die Dauer eines Kanals gespeichert werden. Im folgenden werden wir die Kanäle daher nicht mehr weiter betrachten.

3 Fehlertolerantes MIX-Netz

Die Grundidee des MIX-Netzes ist folgende: Nachrichten werden über eine Folge von ausgezeichneten Stationen, sogenannten MIXen übertragen. Jeder MIX sammelt und puffert eine Menge von Nachrichten gleicher Länge, ignoriert schon einmal bearbeitete Nachrichten, schlüsselt die erstmals erhaltenen Nachrichten um und gibt sie in einer zufälligen Reihenfolge aus (besser als eine zufällige Reihenfolge ist eine von vornherein vorgegebene, z.B. alphabetische Reihenfolge, da so der verborgene Kanal (hidden channel) der „zufälligen" Reihenfolge für ein eventuell im jeweiligen MIX vorhandenes Trojanisches Pferd geschlossen wird und, da auch die Anzahl der jeweils gleichzeitig zu mixenden Nachrichten sowie die Zeitverhältnisse exakt vorgegeben werden können, damit keinerlei Möglichkeiten zu bestehen braucht, über die ein eventuell vorhandenes Trojanisches Pferd einem nicht empfangsberechtigten Empfänger Information zukommen lassen kann [PoKl_78, Denn_82 Seite 281]). Für einen Angreifer, der nur die Ein- und Ausgangsleitungen eines MIXes, nicht aber die Vorgänge im MIX selbst beobachtet, ist kein Zusammenhang zwischen ein- und auslaufenden Nachrichten derselben gesammelten und gepufferten Menge mehr sichtbar. Dadurch, daß eine Nachricht durch mehrere MIXe läuft, kann kein einzelner MIX die Anonymität der *Kommunikationsbeziehung* gefährden. Lediglich der gemeinsame Angriff aller MIXe auf dem Weg einer Nachricht kann den Sender *und* Empfänger dieser Nachricht identifizieren. Diese Eigenschaft wird durch die in Bild 3 graphisch dargestellte und im folgenden Text formal definierte aufwendige Verschlüsselungsstruktur erreicht, bei der die eigentliche Nutznachricht vom Sender so oft sukzessive so „eingepackt" (verschlüsselt) wird, daß jeweils nur einer der MIXe die äußerste Verpackung entfernen, sie also eine Verpackungsschicht weit „auspacken" (entschlüsseln) kann.

Zwischen MIXen können Nachrichten normal vermittelt werden, ggf. auch von den MIXen selbst.

Will S die Nachricht N an E senden und wählt die Folge der MIXe MIX_n, MIX_{n-1},..., MIX_1, so verschlüsselt er N wie folgt:

$$\ddot{o}_n(R_n,MIX_{n-1},\ddot{o}_{n-1}(R_{n-1},\ldots,$$
$$MIX_1,\ddot{o}_1(R_1,E,\ddot{o}_E(R_0,N))\ldots))$$

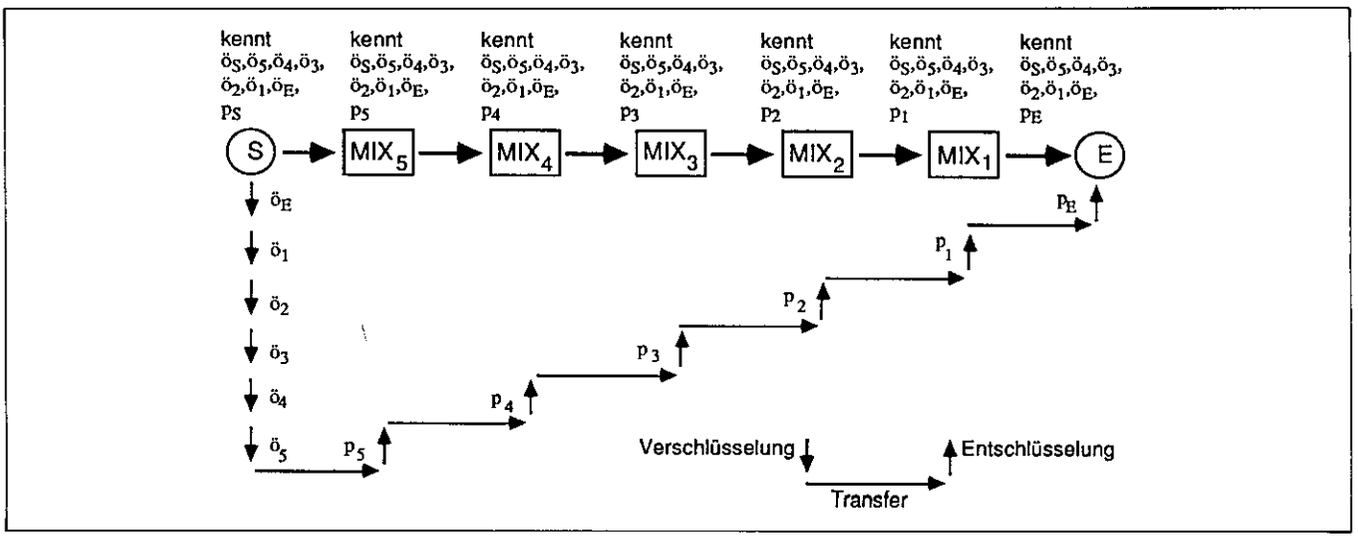

Bild 3 Transfer- und Verschlüsselungsstruktur der Nachrichten im MIX-Netz

Empfängt MIX_n diese Nachricht, so wendet er p_n darauf an und erhält die Zufallszahl R_n, die er wegwirft (da sie ihren Zweck, andere daran zu hindern, die von ihm ausgegebenen Nachrichten einfach mit seinem öffentlichen Schlüssel $ö_n$ zu verschlüsseln und so seine Eingabenachrichten zu erhalten, erfüllt hat), und die Adresse des nächsten Empfängers MIX_{n-1} der weiterzuleitenden Nachricht $ö_{n-1}(R_{n-1},...,MIX_1,ö_1(R_1,E,ö_E(R_0,N))...)$. Schließlich erhält der Empfänger $ö_E(R_0,N)$, wendet darauf p_E an, wirft R_0 weg und empfängt so die Nutznachricht N.

Damit E eine Antwort A an S senden kann, ohne S zu kennen, muß S eine anonyme Rückadresse an E senden. Die anonyme Rückadresse wird wie die gerade beschriebene Hinnachricht gebildet, enthält aber keine eigentliche Nutznachricht, sondern als innersten Teil die Adresse von S. Da E seine Antwort A nicht in diese mit vielen Verpackungsschichten versehene, genauer aus ihnen bestehende Adresse „hineinstecken" kann, wird sie zusammen, d.h. etwa konkateniert, mit der Antwort in Richtung von S übertragen, wobei dabei die anonyme Rückadresse von den entsprechenden MIXen jeweils eine Verpackungsschicht weit „ausgepackt" (entschlüsselt) und die begleitende Antwort jeweils mit einer Verpackungsschicht „eingepackt" (verschlüsselt) wird. S kann zur Bildung der anonymen Rückadresse die gleiche oder eine andere Folge von MIXen verwenden als bei der normalen Hinnachricht. Bei Bezeichnung der MIXe mit $MIX_1,...,MIX_{m-1}, MIX_m$ wird die anonyme Rückadresse folgendermaßen gebildet:

$$MIX_1,ö_1(K_1,MIX_2,ö_2(K_2,...,MIX_m,ö_m(K_m,S)...))$$

E sendet von dieser Adresse $ö_1(K_1,MIX_2,ö_2(K_2,...,MIX_m,ö_m(K_m,S)...))$ zusammen mit der eigentlichen Nachricht $ö_S(R_0,A)$ an MIX_1. Dieser wendet auf die anonyme Rückadresse seinen privaten Schlüssel p_1 an und findet K_1 (das sowohl verhindert, daß MIX_1 durch Verschlüsseln seiner Ausgabe konkateniert mit seinem Namen mit seinem öffentlichen Schlüssel überbrückt werden kann, als auch als Schlüssel eines symmetrischen Kryptosystems zum Verschlüsseln des eigentlichen Nachrichtenteiles dient), MIX_2 als nächste Adresse sowie $ö_2(K_2,...,MIX_m,ö_m(K_m, S)...)$. MIX_1 sendet dann $ö_2(K_2,...,MIX_m,ö_m(K_m, S)...)$ und $K_1(ö_S(R_0,A))$ an MIX_2. Kommt die Antwort schließlich bei S an, so hat sie folgendes Aussehen:

$$K_m(K_{m-1}(...K_1(ö_S(R_0,A))...))$$

Da nur S alle K_i ($i=m,...,1$) und p_S kennt, kann nur er A lesen. Es sei angemerkt, daß statt $ö_S$ von E auch ein geheimer Schlüssel K_0 verwendet werden kann, der ihm dann als Bestandteil der Rückadresse mitgeteilt werden muß und es erlaubt, R_0 genauso einzusparen, wie dies bei den Verschlüsselungen mit $K_1,...,K_m$ geschah. Bei Verwendung eines üblichen asymmetrischen Kryptosystems, das bei gegebenem öffentlichen Schlüssel ausschließlich Einheiten fester Länge, sogenannte Blöcke, verschlüsselt, ist diese Einsparung wesentlich. Andernfalls wächst die Nachrichtenlänge exponentiell mit der Anzahl der verwendeten MIXe, da aus dem oben dargelegten Grund in jedem Block je eine Zufallszahl von etwa 100 bit Länge enthalten sein muß, so daß die Nachrichtenlänge mit jedem MIX um den Faktor

$$\text{Blocklänge}/(\text{Blocklänge} - 100 \text{ bit})$$

wächst. Verwendet man ein bei gegebenem öffentlichen Schlüssel nur Blöcke fester Länge verschlüsselndes asymmetrisches Kryptosystem, wird man also für praktische Zwecke auch für Hinnachrichten ein Schema verwenden, das (bis auf einen Block) den Rest der Nachricht mit einem (symmetrischen) Kryptosystem, das Einheiten beliebiger Länge verschlüsseln kann, verschlüsselt [Chau_81 Seite 87, Pfi1_85]. Oder aber man verwendet ein (heute noch unübliches) asymmetrisches Kryptosystem, das bereits auch bei gegebenem öffentlichen Schlüssel Einheiten beliebiger Länge verschlüsseln kann. In [BlGo_85] ist solch ein asymmetrisches Kryptosystem beschrieben, das (intern) genauso wie eben beschrieben aus zwei Kryptosystemen aufgebaut ist, für das aber in dieser Zusammensetzung noch weitere wünschenswerte Sicherheitseigenschaften bewiesen werden konnten. Soweit die Verschlüsselungsstruktur.

Man erkennt deutlich die Serieneigenschaft. Fällt nur ein MIX auf dem Weg zwischen S und E aus, so kann die Nachricht nicht weiter übertragen werden. Wie schon aus Bild 2 ersichtlich, basiert das MIX-Netz auf einem in den Schichten 0 (medium), 1 (physical) und 2 (data link) beliebig realisierten Kommunikationssystem. Das impliziert, daß diese Schichten des Kommunikationssystems konventionelle Fehlertoleranz-Maßnahmen verwenden können, ohne dadurch die Anonymität der Netzbenutzer zu gefährden. Transiente sowie permanente Fehler in diesen Schichten können also von diesen selbst toleriert werden. Transiente Fehler in den MIXen werden von den Ende-zu-Ende-Protokollen zwischen Sender S und Empfänger E erkannt und durch wiederholtes Senden toleriert. (Zur Leistungssteigerung ist auch eine weitere Zwischenstufe mit MIX-zu-MIX-Protokollen möglich.) Es bleiben somit nur noch die permanenten Fehler in MIXen. Diese Fehler sind mit den üblichen Techniken zu erkennen bzw. zu lokalisieren, z.B. der Ausfall eines MIXes durch Zeitschranken bzw. die Diagnose, welcher MIX ausfiel, durch das Ausbleiben eines zyklisch zu gebenden Lebenssignals (I'm alive message). Die permanenten Ausfälle von MIXen erfordern darüber hinaus geeignete Methoden zur Fehlerbehebung. Prinzipiell gibt es drei Möglichkeiten [Pfi1_85].

Zum einen (Ende-zu-Ende-Protokoll) versucht der Sender eine Wiederholung der Nachrichtenübertragung auf einem anderen Weg (Bild 4), d.h. über eine disjunkte MIX-Folge (in der Begriffswelt der Fehlertoleranz [EcGM_83, gekürzt auch in BeEG_86]: *dynamisch aktivierte Redundanz*). Diese Lösung ist einfach, aber (wie dynamisch aktivierte Redundanz generell) langsam, da das Ende-zu-Ende-Protokoll zuerst den Fehler erkennen (i.allg. durch Zeitschranken) und dann eine zweite Übertragung einleiten muß, möglicherweise ohne zu wissen, welcher MIX defekt ist. Bei Rückadressen ist dieses Verfahren dann sehr aufwendig, wenn keine zeitliche Beziehung zwischen N und A besteht, wie dies z.B. bei elektronischer Post (electronic mail) der Fall ist. E kann, falls seine eine Rückadresse ausfällt (wenigstens ein MIX in dieser Folge ist defekt), keine Nachrichtenübertragung auf einem anderen Weg versuchen. Dies gilt auch, wenn immer zwei oder mehr Rückadressen (*statisch erzeugte Redundanz*) ausgetauscht werden und in jeder Folge ein MIX defekt ist. Der ursprüngliche Sender S (genauer: seine Teilnehmerstation) müßte also, solange er von E keine Antwort erhielt, E (genauer: seiner Teilnehmerstation) immer wieder neue Rückadressen mitteilen, was in den meisten Fällen völlig überflüssig ist, da E lediglich bisher noch keine Zeit fand, eine Antwort zu formulieren. Diese erste Möglichkeit der Fehlertoleranz läuft auf ein alle Stationen involvierendes Zwei-Phasen-Konzept (vgl. Kap. 4) hinaus. In der einen Phase werden Nachrichten anonym übertragen, in der anderen werden Fehler toleriert, z.B. dadurch daß nach jedem Ausfall eines MIXes alle Sender allen Empfängern neue anonyme Rückadressen zukommen lassen, in denen der ausgefallene MIX nicht benötigt wird (in der Begriffswelt der Fehlertoleranz: *dynamisch erzeugte,* dynamisch aktivierte *Redundanz*). Da in MIX-Netzen ohne Verteilung aller jeweils „letzten" Nachrichten an alle Stationen aus Gründen der gegenseitigen Anonymität von Sender und

Empfänger alle Adressen anonyme Rückadressen sein müssen [Pfi1_85], erfordert diese Neuverteilung in ihnen zwingend eine Indirektionsstufe in Form von nichtanonymen Stellen zur Neuverteilung der Adressen: nach Ausfall eines MIXes wird dies allen Stationen mitgeteilt und jede sendet den nichtanonymen Stellen zur Adreßverteilung mit dem zuerst beschriebenen Schema über die noch intakten MIXe eine Liste der unbrauchbar gewordenen Adressen, jeweils eine Ersatzadresse und eventuell noch weitere Adressen, da diese ja je nur einmal verwendet werden können und also von Zeit zu Zeit sowieso nachgeliefert werden müssen. In MIX-Netzen mit Verteilung aller jeweils „letzten" Nachrichten an alle Stationen sind anonyme Rückadressen überflüssig, da durch Verteilung und normale implizite Adressen der Empfänger vollständig geschützt ist. Also müssen in solchen MIX-Netzen auch nach Ausfall von MIXen keine neuen Adressen ausgetauscht werden. Eine Liste der ausgefallenen MIXe sollte natürlich an alle Stationen verteilt werden, damit sie diese MIXe für das zuerst beschriebene Verschlüsselungsschema nicht verwenden. Eine im Fehlerfall Zeit sparende Variation dieser Möglichkeit der Ende-zu-Ende-Protokolle mit statisch oder dynamisch aktivierter Redundanz besteht darin, jeden Nachrichtentransfer parallel über mehrere disjunkte MIX-Folgen auszuführen (statisch oder dynamisch erzeugte, *statisch aktivierte Redundanz*). Nachteil aller Ende-zu-Ende-Protokolle ist, daß statistische Angriffe über Nachrichtensenderaten bei MIX-Netzen ohne Verteilung bei individueller Wahl der Zeitschranken bzw. der Anzahl der parallel auszuführenden Nachrichtentransfers stark erleichtert werden.

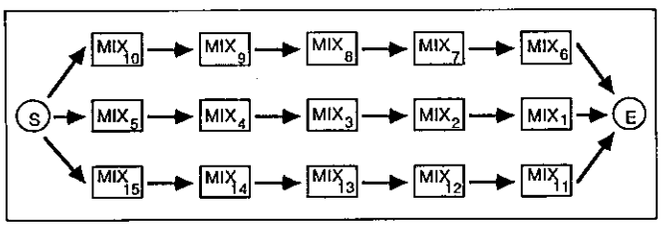

Bild 4 Zwei zusätzliche alternative Wege über disjunkte MIX-Folgen.

Eine zweite Möglichkeit (MIX-zu-MIX-Protokoll) besteht darin, daß der geheime Schlüssel des ausgefallenen MIXes einem oder mehreren anderen MIXen, die z.B. von derselben Organisation betrieben werden, bekannt ist (Bild 5) oder von vielen MIXen, die z.B. von sich gegenseitig mißtrauenden Organisationen betrieben werden, durch Verwendung eines Schwellwertschemas [Sham_79] rekonstruiert werden kann [Pfi1_85]. In der Begriffswelt der Fehlertoleranz ausgedrückt handelt es sich also um *statisch erzeugte, dynamisch aktivierte Parallel-Redundanz*. Bei dieser wie auch bei der dritten Möglichkeit muß darauf geachtet werden, daß trotz Ausfall eines MIXes und der Übernahme seiner Funktion durch einen anderen keine Nachricht mehrfach bearbeitet wird, da andernfalls die durch diese Verschlüsselung zu erreichende Anonymität der Kommunikationsbeziehung nicht garantiert wird und ein geschickter Angreifer ansonsten durch Herbeiführen von Fehlern oder deren Simulieren bei mehreren MIXen die Anonymität der Kommunikationsbeziehung insgesamt verhindern könnte [Pfi1_85].

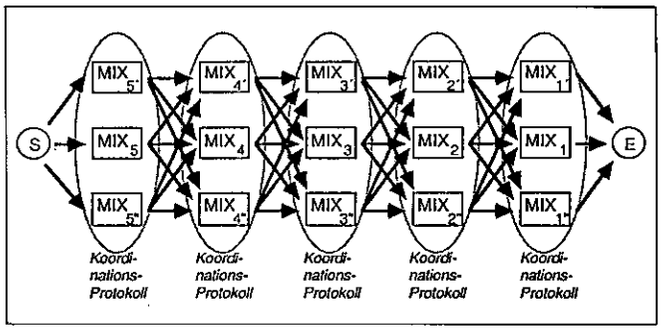

Bild 5 MIX_i kann alternativ von MIX_i' oder MIX_i'' ersetzt werden (i = 1, 2, 3, 4, 5).

Die dritte Möglichkeit (MIX-zu-MIX-Protokoll) sieht eine *fehlertolerante anonyme Verschlüsselungsstruktur* vor, die die in Bild 6 gezeigten Entschlüsselungs- und damit Weiterleitmöglichkeiten eröffnet [Pfi1_85].

Der Sender bildet nacheinander die Nachrichten N_0 bis N_n und sendet N_n an MIX_n.

$$N_0 = \ddot{o}_E(R_0,N)$$
$$N_1 = \ddot{o}_1(R_1,k_1,E),\ k_1(N_o)$$
$$N_i = \ddot{o}_i(R_i,k_i,MIX_{i-1},k_{i-1},MIX_{i-2}),\ k_i(N_{i-1})$$
$$\text{für } i = 2,\ldots,n$$

MIX_n entschlüsselt mit p_n den ersten Teil der Nachricht und erfährt dadurch k_n, den nächsten MIX, k_{n-1} und den übernächsten MIX (Ist MIX_n defekt, so bildet S nur die Nachricht N_{n-1} und sendet sie an MIX_{n-1}). MIX_n entschlüsselt mit k_n den zweiten Teil und erhält N_{n-1}, das er, wenn MIX_{n-1} intakt ist, an ihn weiterleitet. Ist dagegen MIX_{n-1} ausgefallen, so entfernt MIX_n den vorderen Teil von N_{n-1} und entschlüsselt mit k_{n-1} den Rest und erhält N_{n-2}. Sodann sendet MIX_n N_{n-2} an MIX_{n-2}.

Entsprechend läßt sich auch eine *fehlertolerante anonyme Rückadresse* $(N_1,k_1,K_1,MIX_1,MIX_2)$ konstruieren:

$$N_n = \ddot{o}_n(R_n,K_n,S)$$
$$N_{n-1} = \ddot{o}_{n-1}(R_{n-1},k_{n-1},K_{n-1},MIX_n,K_n,S),\ k_{n-1}(N_n)$$
$$N_i = \ddot{o}_i(R_i,k_i,K_i,MIX_{i+1},k_{i+1},K_{i+1},MIX_{i+2}),\ k_i(N_{i+1}) \quad \text{für } i = 1,\ldots,n-2$$

Sendet E die Antwort A an S, so sendet E, sofern MIX_1 intakt ist, N_1 und $\ddot{o}_S(R_0,A)$ an MIX_1. Dieser entschlüsselt den ersten Teil von N_1 mit p_1 und erfährt k_1, K_1, den nächsten MIX, k_2, K_2 und den übernächsten MIX. MIX_1 entschlüsselt den zweiten Teil von N_1 mit k_1 und prüft, ob MIX_2 intakt ist. Wenn ja, so sendet er $N_2,K_1(\ddot{o}_S(R_0,A))$ an MIX_2. Ist dagegen MIX_2 defekt, so wirft MIX_1 den ersten Teil von N_2 weg und entschlüsselt den zweiten Teil von N_2 mit k_2. Sodann sendet MIX_1 $N_3,K_2(K_1(\ddot{o}_S(R_0,A)))$ an MIX_3. Hier wird mit K_1 und K_2 verschlüsselt, damit S nicht zu erfahren braucht, welche MIXe ausgefallen sind. Andernfalls müßte S alle Möglichkeiten weggelassener Verschlüsselungen ausprobieren ($\approx 2^n$) oder es müßte S mitgeteilt werden, welche Schlüssel auszulassen sind. Dies könnte z.B. dadurch geschehen, daß nach jeder Verschlüsselung der Nachricht Redundanz hinzugefügt wird. Dies erlaubt beim Entschlüsseln festzustellen, ob ein Schlüssel weggelassen werden muß, und senkt so den Aufwand auf $\approx 2 \cdot n$. Ist andererseits bereits MIX_1 ausgefallen, so entschlüsselt E mit k_1 $k_1(N_2)$ und sendet direkt N_2 und $K_1(\ddot{o}_S(R_0,A))$ an MIX_2. Die nächsten MIXe verfahren analog.

Mit dieser fehlertoleranten anonymen Verschlüsselungsstruktur und Rückadresse ist es gelungen, Ausfälle einzelner MIXe zu tolerieren. Der Ausfall zweier benachbarter MIXe ist mit den obigen Schemata nicht tolerierbar. Sollte dies erforderlich sein, so lassen sie sich leicht auf d erreichbare MIXe erweitern [Pfi1_85]. Man erkennt drei weitere Varianten.

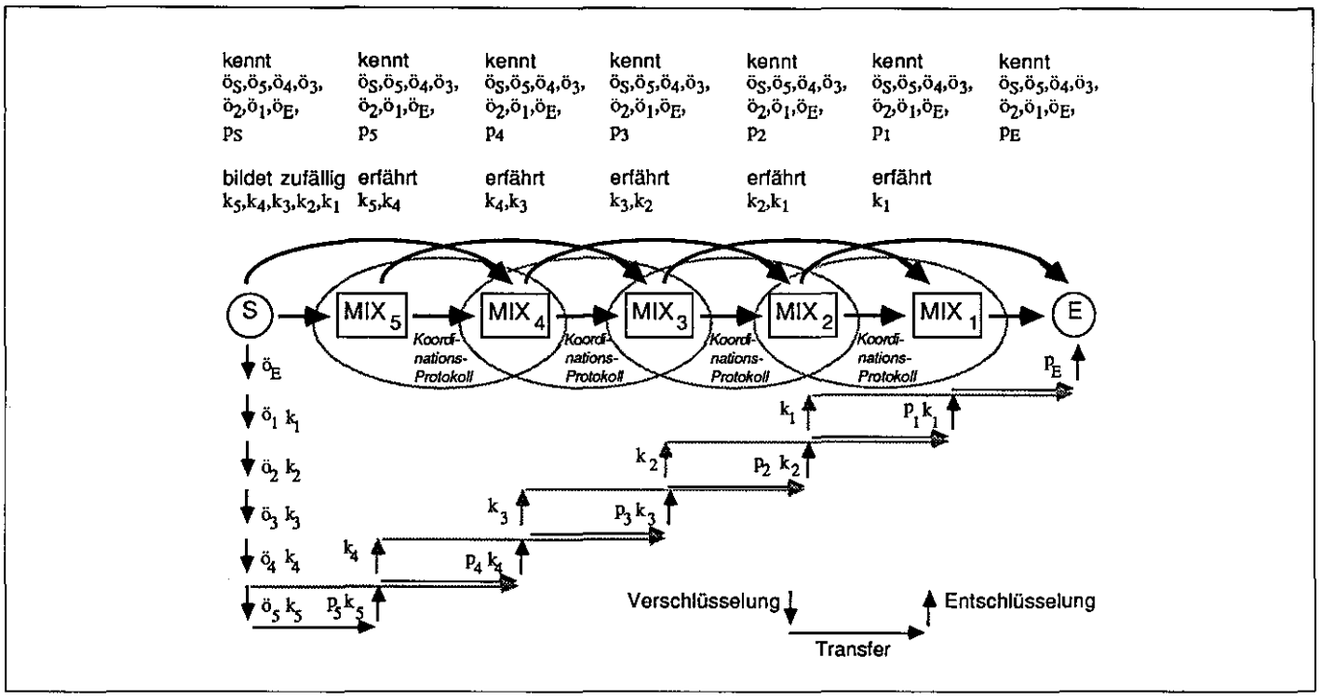

Bild 6 Jeweils ein MIX kann ausgelassen werden.

Zum einen können die Zufallszahlen bis auf R_0 weggelassen werden. Die zufälligen Schlüssel k_i und K_i verhindern bereits das Erraten der verschlüsselten Nachricht. Die Zufallszahlen können aber auch im Falle der Verwendung eines bei gegebenem öffentlichen Schlüssel nur Einheiten fester Länge verschlüsselnden Kryptosystems dazu verwendet werden, die Nachrichten auf ganzzahlige Vielfache der Blocklänge aufzufüllen. Die Blocklänge kann (z.B. bei RSA) von dem Schlüssel (Länge des Modulus) der betreffenden Instanz abhängen.

Des weiteren kann $k_i = K_i$ gewählt und folglich eines von beiden in der Nachricht weggelassen werden.

Zuletzt kann aus Leistungsgründen im fehlerfreien Fall MIX_i immer direkt an MIX_{i-2} (Weg von S→E) bzw. an MIX_{i+2} (Weg von E→S) senden. Dadurch wird jede Nachricht nur n/2-mal übertragen. Die Anonymität wird dadurch in keiner Weise beeinträchtigt, da der Angreifer ohnehin immer einen MIX auslassen könnte, sofern er MIXe auf dem Weg der Nachricht kontrolliert. Es sei hier noch einmal angemerkt, daß ein Koordinations-Protokoll zwischen MIXen dafür sorgen muß, daß jede Entschlüsselung von den MIXen, die der Angreifer nicht kontrolliert, insgesamt höchstens einmal ausgeführt wird. Dieses Koordinations-Protokoll ist für die gerade geschilderte Variante (Auslassen von MIXen wenn immer möglich) leider aufwendiger als bei der vorherigen Variante (Auslassen nur von defekten MIXen). Es kann also nur bei Kenntnis der Verteilung der Nachrichtenlängen an der Schichtgrenze zwischen den Schichten 4 (transport) und 3 (network) sowie der Eigenschaften der Schichten 0 (medium), 1 (physical) und 2 (data link) entschieden werden, welche Variante die günstigere ist.

Die Fehlertoleranz, die hier durch zusätzliche Information erreicht wurde (ein MIX kennt die nächsten zwei auf ihn folgenden MIXe und kann den nächsten überbrücken), schwächt auf der anderen Seite den Datenschutz ab. Reichen beim Vorschlag aus [Chau_81] n MIXe auf einem Weg, um hinreichend anonym zu sein, so müssen bei der fehlertoleranten Verschlüsselungsstruktur n' MIXe (mit $n' > n$) auf dem Weg liegen, um sicherzugehen, daß S und E dieser Nachricht unbeobachtet (anonym) bleiben. Ein quantitatives Bewertungsmodell hierfür ist in [Pfi1_85 Seite 91ff.] enthalten.

Es sei noch erwähnt, daß die Grundidee dieses Fehlertoleranzverfahrens dem geflochtenen Ring (braided ring) in Kapitel 5 entspricht. Im MIX-Netz wird dieses Fehlertoleranzverfahren zweckmäßigerweise in der Schicht 3 (network), im RING-Netz auf den Schichten 0 (medium) und 1 (physical) implementiert (siehe Bilder 2, 3, 6 und 8).

4 Fehlertolerantes DC-Netz

Die Grundidee des DC-Netzes ist folgende: Alle Stationen *überlagern* (addieren modulo 2) lokal alle ihnen bekannten Schlüssel und ggf. ihre zu sendende Nachricht bzw. andernfalls stattdessen Nullen. Die in Stationen durch lokale Überlagerung entstehenden Bitfolgen werden im Kommunikationssystem global überlagert und die dadurch entstehende Bitfolge an alle Stationen verteilt. Da jeder Schlüssel von einer Station generiert und genau einer weiteren Station vertraulich mitgeteilt wird, ist das Ergebnis der globalen Überlagerung die Summe (modulo 2) aller gesendeten Nachrichten, da jeder Schlüssel genau zweimal überlagert (modulo 2 addiert) wird. Es ist Aufgabe eines Verfahrens zum anonymen Mehrfachzugriff (siehe Bild 2), Kollisionen zwischen Nachrichten, die im allgemeinen einen Nachrichtenverlust bedeuten, möglichst zu vermeiden, ohne Hinweise auf den Sender zu liefern.

In der technischen Realisierung wird natürlich kein ganzer Schlüssel, der mindestens die Länge der Folge aller jemals zu sendenden Nachrichten haben muß, vertraulich ausgetauscht, sondern nur der Startwert für einen Pseudozufallsbitfolgengenerator (PZG). Im folgenden gehen wir immer von der Verwendung kryptographisch sicherer PZGs aus, d.h. selbst wenn Teilsequenzen der Bitsequenz bekannt sind, lassen sich mit vertretbarem Aufwand keine weiteren Bits mit einer Wahrscheinlichkeit größer 1/2 voraussagen [BlMi_84].

Das DC-Netz kann auf einer beliebigen Topologie realisiert werden [Cha3_85, PfPW_86], ein beliebiges Bitübertragungsnetz, das die OSI-Schicht 0 und die tiefere Teilschicht der Schicht 1 umfaßt, mit konventionellen Fehlertoleranz-Maßnahmen ist möglich. Anders als beim MIX-Netz (vgl. Bild 2) muß das Zugriffsverfahren zum Bitübertragungsnetz die Anonymität erhalten. Da das Bitübertragungsnetz (unabhängig von der Topologie) und das darauf aufbauende DC-Netz einem gemeinsamen Broadcast-Medium aller angeschlossenen Netzbenutzer entspricht, wird das Zugriffsverfahren aus den Klassen der ALOHA-Protokolle (unslotted sowie slotted ALOHA liefern keinerlei Information über den Sender), der anonymen Reservierungsverfahren, der anonymen CSMA/CD-Verfahren u.ä. sein [Pfi1_85 Seite 40ff.]. Ein Angreifer, der alle Leitungen beobachtet, aber keine Schlüssel kennt, kann nie auf den Sender bzw. Empfänger einer Nachricht rückschließen. Ein Sender ist dann identifizierbar, wenn alle anderen Netzbenutzer, mit denen er Schlüssel ausgetauscht hat, zusammenarbeiten und ihre Schlüssel offenlegen. Dieses Identifizieren von Netzbenutzern ist zum Aufdecken von Versuchen, die Diensterbringung zu verhindern, erforderlich (siehe Kapitel 6).

Die Serieneigenschaft des DC-Netzes besteht darin, daß alle PZGs und alle Modulo-2-Addierer fehlerfrei arbeiten müssen und die Synchronisation erhalten bleiben muß. Anders als beim MIX-Netz, bei dem Fehlertoleranz-Maßnahmen ständig im Hintergrund abgewickelt werden können, lassen sich beim DC-Netz zwei Phasen, später Modi genannt, klar voneinander trennen. Zunächst übertragen alle Netzbenutzer anonym Nachrichten. Tritt ein permanenter Fehler im Verfahren zum anonymen Mehrfachzugriff oder im DC-Netz auf, so kann kein Netzbenutzer Nachrichten übertragen, bis dieser Fehler durch Ausgliedern oder Reparatur der defekten Komponente(n) toleriert ist, es sei denn, man realisiert mehrere voneinander unabhängige DC-Netze (*statisch erzeugte Parallel-Redundanz*, die wiederum *statisch* oder *dynamisch aktiviert* werden kann). Die Realisierung mehrerer unabhängiger DC-Netze betrachten wir nicht vertieft, da sie keine besonderen Entwurfs-Schwierigkeiten aufwirft. Es sei lediglich angemerkt, daß es zweckmäßig sein dürfte, zwar jeder Station das Empfangen auf jedem der unabhängigen DC-Netze zu ermöglichen, das Senden jedoch nur auf relativ wenigen. Dadurch wird ein Angreifer, der nur wenige Stationen kontrolliert, daran gehindert, alle anderenfalls eben bezüglich des Angreifers nicht unabhängigen DC-Netze zu stören. [Nied_87] enthält eine Bewertung der Zuverlässigkeit und Senderanonymität solcherart konfigurierter DC-Netze.

Transiente wie auch permanente Fehler im Bitübertragungsnetz können durch gesonderte Fehlertoleranz-Maßnahmen in ihm selbst toleriert werden, oder führen andernfalls zu transienten bzw. permanenten Fehlern im DC-Netz. Die transienten Fehler im DC-Netz werden durch Ende-zu-Ende-Protokolle (vgl. Kapitel 2) toleriert. Es verbleiben somit die permanenten Fehler im DC-Netz (Ausfall von PZGs, von Modulo-2-Addierern, Verlust der Konsistenz oder Synchronisation der Schlüssel usw.). Diese sind, wenn einmal erkannt und lokalisiert, leicht zu beheben. Die entsprechenden Schlüssel (von defekten PZGs) werden nicht mehr überlagert, Addierer werden ausgetauscht, Schlüssel werden neu verteilt oder sie werden neu synchronisiert. Das Hauptproblem liegt also in der *Fehlererkennung* und *-lokalisierung*. Fehler lassen sich dadurch erkennen, daß jeder verschlüsselten Nachricht von ihrem Sender zusätzliche, allen Stationen zugängliche Redundanz zugefügt wird (z.B. ein bestimmtes Bitmuster am Beginn und ein CRC-Code am Ende der Nachricht). Dies kann immer geschehen, da die Redundanz nur einen Bruchteil der Nachrichtenlänge umfaßt, die nutzbare

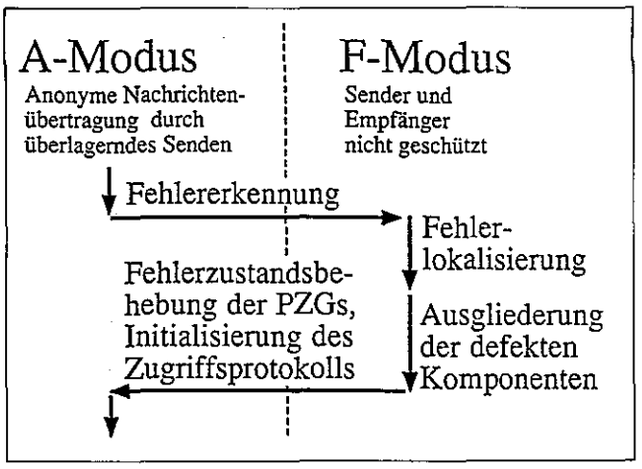

Bild 7 Fehlererkennung, -lokalisierung und -behebung beim DC-Netz.

Übertragungsleistung also kaum sinkt. Um einen Fehler lokalisieren zu können, wird aus dem die Anonymität garantierenden A-Modus in den F-Modus, in dem die Fehler lokalisiert und toleriert werden, geschaltet. In diesem Modus überträgt jeder PZG einige neu generierte und später zur Nachrichtenübertragung nicht mehr verwendete Bits seiner Zufallssequenz im Klartext, daher die Forderung nach kryptographisch sicheren PZGs. So können je zwei PZGs, die denselben Schlüssel generieren, gegenseitig getestet werden. Außerdem kann so die Synchronisation überprüft werden. Sodann werden von jeder Station bestimmte Daten übertragen, um die Modulo-2-Addierer zu testen. Beide Maßnahmen lassen sich so verbessern, daß sie logarithmischen Zeitaufwand (logarithmisch in der Zahl der aktiven PZGs bzw. logarithmisch in der Zahl der Modulo-2-Addierer) erfordern. Dies kann z.B. dadurch erreicht werden, daß zunächst die Hälfte aller Schlüsselpaare im Klartext überlagert wird. Dies ergibt Nullen, sofern alle betroffenen PZGs und die Modulo-2-Addierer intakt sind und die Synchronisation gegeben ist. Durch sukzessives Halbieren der Menge der gleichzeitig überlagerten Schlüsselpaare lassen sich Fehler schnell lokalisieren [Pfi1_85].

Mit dem Zurückschalten vom F-Modus in den A-Modus wird das Verfahren zum anonymen Mehrfachzugriff neu initialisiert, um Auswirkungen von Fehlern der Schicht 1 (physical) auf die Schicht 2 (data link) rückgängig zu machen. Alle gerade geschilderten Schritte sind in Bild 7 zusammengefaßt.

Es ist beachtenswert, daß bei dieser Realisierung die Anonymität trotz Fehlertoleranz nicht abgeschwächt wird. Durch das Einführen der zwei Modi und die Verwendung kryptographisch sicherer PZGs bleibt im A-Modus die Anonymität jederzeit in ihrem ursprünglichen Umfang garantiert.

5 Fehlertolerantes RING-Netz

Bei diesem Konzept wird die Anonymität der Netzbenutzer durch Ringe sowie digitale Signalregenerierung garantiert (Bild 2), also durch (im Bereich lokaler Netze) durchaus übliche Verfahren, während MIX- und DC-Netz aufwendige zusätzliche Verfahren benötigen, die zweckmäßigerweise in Teilschichten (sublayers) der Schicht 3 (network) bzw. 1 (physical) implementiert werden. Spezielle Verfahren zum

Mehrfachzugriff [Höck_85, HöPf_85] erhalten diese Anonymität durch verteiltes und anonymes Abfragen (polling) [Pfil_85 Seite 43]. Eine Station ist als Sender bzw. Empfänger einer Nachricht nur dann ohne ihr Mitwirken identifizierbar, wenn ihre Eingangs- und Ausgangsleitungen abgehört werden. Ein Angreifer, der bis auf zwei Stationen sowie die dazwischenliegende Leitung den ganzen Ring beobachtet, kann bei den besten Verfahren zum anonymen Mehrfachzugriff nie beweisen, welche der eingekreisten Stationen eine Nachricht gesendet bzw. empfangen hat (vgl. Bild 1). Allgemeiner gilt: Garantiert das Zugriffsverfahren *n-Anonymität* [Höck_85], so kann kein Angreifer, der n Stationen beobachtet (ohne die dazwischenliegenden Leitungen abzuhören), auf den Sender bzw. Empfänger einer Nachricht rückschließen.

Bei diesem Konzept ist die Serieneigenschaft sofort ersichtlich. Durch das Zusammenspiel von Anonymität, Ring, digitaler Signalregenerierung und Verfahren zum anonymen Mehrfachzugriff sind spezielle Fehlertoleranz-Maßnahmen erforderlich. Transiente Fehler im Ring können nur übertragene Nachrichten betreffen; diese Fehler sind einfach und werden durch das Ende-zu-Ende-Protokoll (Kapitel 2) erkannt und behoben. Schwierig sind diejenigen transienten Fehler, die das Zugriffsverfahren betreffen. Man stelle sich z.B. vor, daß bei einem Token-Ring das Token zerstört wird. Dieser und ähnliche Fehler werden durch *indeterministische Protokolle* toleriert. Permanente Fehler im Ring führen immer zu einer *Ringrekonfigurierung* mit Neustart (Synchronisation,...) des Verfahrens zum anonymen Mehrfachzugriff. Da dieses Konzept auf den Schichten 0 (medium) und 1 (physical) angesiedelt ist, sind Fehler leicht zu erkennen und zu lokalisieren (Zeitschranken, Selbsttest sowie Fremdtest durch mehrere Instanzen, damit ein Angreifer, der wenige Stationen kontrolliert, nicht andere Stationen beliebig an- und abschalten kann, u.ä.). Problematisch ist die Fehlerbehebung, da für jede nachgewiesen werden muß, daß die Anonymität nicht verletzt wird. Zwei Ideen sind bei der Fehlertoleranz wichtig. Um transiente Fehler der zweiten Art (siehe oben) tolerieren zu können, führt man bewußt Indeterminismus ein. Dadurch kann in dem deterministischen Angreifermodell (der Angreifer muß beweisen, welche Station gesendet bzw. empfangen hat) kein Angreifer sichere Rückschlüsse ziehen. Da es bisher kein befriedigendes formales statistisches Angreifermodell gibt (darin gibt sich ein Angreifer zufrieden, wenn er z.B. mit 90 %iger Wahrscheinlichkeit den Sender bzw. Empfänger kennt), kann die Auswirkung des Indeterminismus nicht quantifiziert werden. Eine andere Art der Fehlertoleranz basiert auf der Idee, einigen wenigen, ausgezeichneten Stationen keine Anonymität zu garantieren. Diese Stationen können nach anderen Protokollen arbeiten als die Stationen von Netzbenutzern und dadurch gezielt Fehler tolerieren [Mann_85]. Daher spricht man von *asymmetrischen Protokollen*. Diese sind leichter zu implementieren und sehr viel leistungsfähiger, schwächen jedoch die Anonymität der Netzbenutzer ab. Garantiert das einfache Zugriffsverfahren n-Anonymität, so gewährleisten die modifizierten asymmetrischen Protokolle häufig nur noch die n+1- oder gar n+2-Anonymität. Um permanente Fehler im Ring tolerieren zu können, wird ein *geflochtener Ring* (braided ring, siehe Bild 8) verwendet. In ihm gibt es drei mögliche *Einzelfehler*, nämlich den Ausfall

- einer *Station* i: sie wird mit Leitung $L_{i-1 \to i+1}$ überbrückt (Bild 8, oben rechts).
- einer *inneren Leitung* $L_{i \to i+2}$: der äußere Ring bleibt intakt und wird solange ausschließlich benutzt, bis der Ausfall der Leitung behoben ist.
- einer *äußeren Leitung* $L_{i \to i+1}$: Station S_{i-1} sendet an die Stationen S_i und S_{i+1} (kopiert den Datenstrom auf

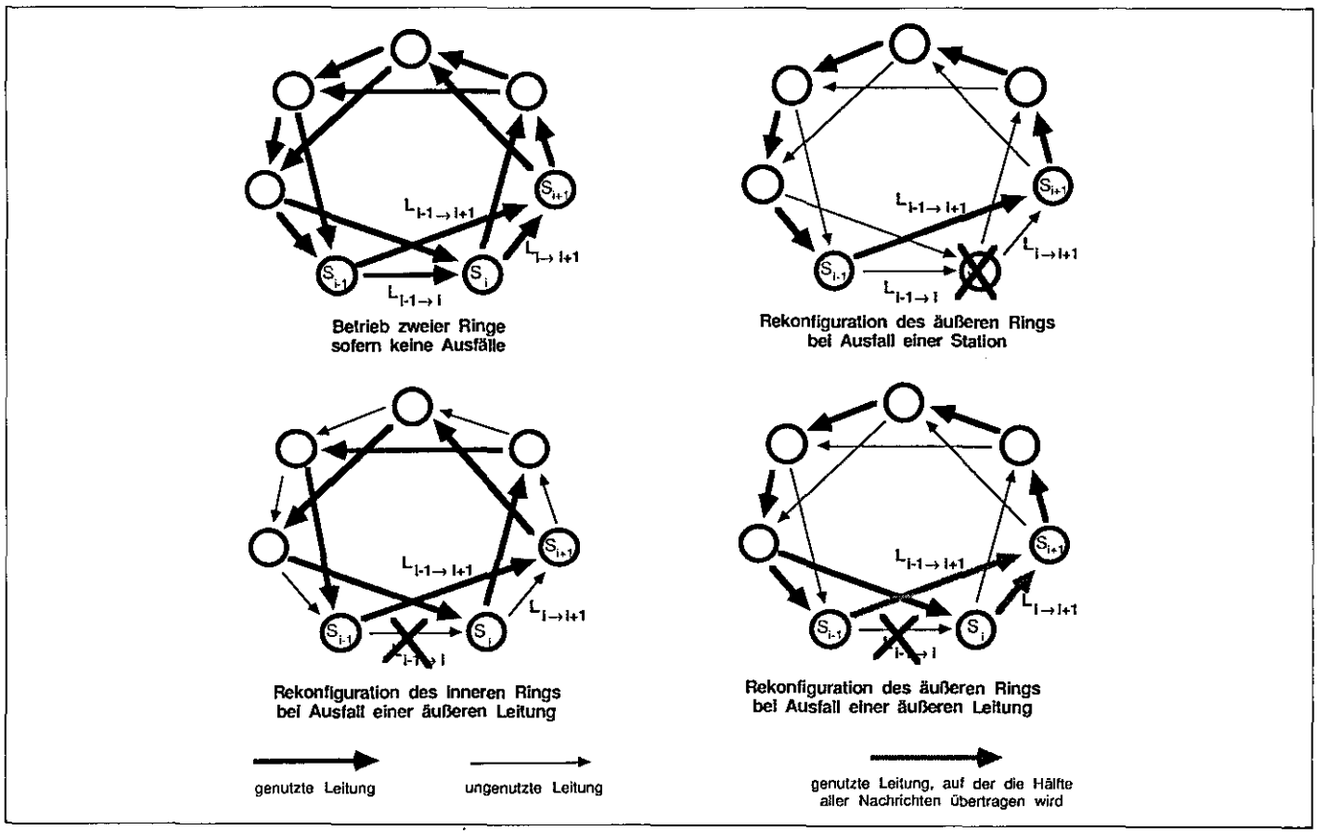

Bild 8 Geflochtener Ring kann bei Ausfällen von Stationen oder Leitungen so rekonfiguriert werden, daß die Anonymität der Netzbenutzer gewahrt bleibt.

zwei Leitungen). Station S_i sendet die Hälfte aller Nachrichten (z.B. alle Slots mit gerader Nummer, sofern i gerade) an Station S_{i+2}, Station S_{i+1} sendet die andere Hälfte (z.B. alle Slots mit ungerader Nummer, sofern i+1 ungerade) an Station S_{i+2}. S_{i+2} vereint die beiden (verzahnten) Datenströme wieder (Bild 8, unten rechts). Dies ist einer Rekonfigurierung des inneren Rings (Bild 8, unten links) vorzuziehen, da auf diese Weise ggf. noch Ausfälle von inneren Leitungen und Stationen toleriert werden können.

Basierend auf diesen drei Grundkonzepten zur Tolerierung des Ausfalls kann der Ring (auch bei den meisten Mehrfachfehlern) so rekonfiguriert werden, daß jede Station jederzeit in einem Datenstrom liegt, d.h. auf der ein- und der auslaufenden Leitung werden Nachrichten übertragen. Daher lassen sich die Beweise für die Anonymität aus dem fehlerfreien Fall direkt übernehmen. Dabei ist zu beachten, daß aus einem zulässigen Angreifer im fehlerfreien Fall bei bestimmten Ausfällen ein unzulässiger Angreifer (gemäß Angreifermodell) wird. Besitzt der Angreifer die Stationen S_1 und S_4 (vgl. Bild 1 und Bild 8 mit i=2) und fällt die Leitung $L_{3\to4}$ aus, so sendet Station S_2 sowohl an Station S_3 als auch an S_4. Damit ist Station S_2 durch den Angreifer eingekreist und daher beobachtbar. Es sei angemerkt, daß bei manchen Ausfällen sogar eine Station allein eine andere beobachten kann. Fällt S_1 so aus, daß sie auf ihren beiden Ausgangsleitungen dasselbe sendet, so kann die Station S_3 die Station S_2 alleine beobachten.

Eine genaue Beschreibung von Fehlertoleranz im RING-Netz, sowie viele Beispiele und Protokolle findet man in [Mann_85].

6 Verhinderung der Diensterbringung

In einem Kommunikationssystem kann jeder Fehler als Angriff angesehen werden. Die physikalischen Fehler bilden eine Untermenge aller möglichen (physikalischen, logischen, aktiven, passiven) Angriffe. Daher wurde in jedem der drei Konzepte nach einem Fehler so rekonfiguriert, daß unter allen Umständen die Anonymität gewahrt bleibt. Ein Angreifer kann jetzt soweit gehen, daß er ständig Fehler erzeugt, d.h. Nachrichten falsch umschlüsselt, fälschlicherweise nicht weiterüberträgt, eigene sendet wenn er es gemäß des Protokolls zum anonymen Mehrfachzugriff nicht darf oder Schlüssel falsch überlagert, um jede Diensterbringung zu unterbinden (*denial of service*). Dieses Problem kann auf zwei Arten gelöst werden. Zum einen wird nach jedem Fehler untersucht, ob eventuell ein aktiver Angriff und, wenn ja, durch wen vorliegt. Da die erforderlichen Maßnahmen sehr aufwendig sind und darüber hinaus u.U. den Sender bzw. Empfänger einer Nachricht identifizieren, ist es besser, erst auf Verdacht (anormale Fehlerrate u.ä.) die entsprechenden Maßnahmen einzuleiten. Um aktive Angriffe erkennen zu können, muß bei allen drei Konzepten *jede Station ihre Aktivitäten aufdecken*, d.h.

- beim MIX-Netz muß jeder MIX alle ein- und auslaufenden Nachrichten ab einem festgelegten Zeitpunkt offenlegen. Dann kann jeder prüfen, ob eine von ihm gesendete Nachricht von diesem MIX falsch ent- oder verschlüsselt oder gar ganz unterschlagen wurde. Um dies einer dritten Partei zu beweisen, müssen die Zusammenhänge der betroffenen Nachrichten aufgedeckt werden. Es ist jedoch nicht erforderlich, die Zusammenhänge aller Nachrichten zu offenbaren, so daß diese Maßnahme zwar hohen Aufwand verursacht, nicht aber die Anonymität unversehrt übertragener Nachrichten gefährdet;
- beim DC-Netz muß jede Station alle Schlüssel (nicht aber den Startwert des PZG) und ihre gesendeten Nachrichten ab einem bestimmten Zeitpunkt offenlegen;
- beim RING-Netz muß jede Station ihre gesendeten Nachrichten ab einem bestimmten Zeitpunkt offenlegen.

Es sei darauf hingewiesen, daß dazu beim DC- und insbesondere beim RING-Netz – auch falls keine „Fehler" auftreten – erheblicher zusätzlicher Aufwand zur Speicherung von Nachrichten nötig ist.

Sind aus verläßlicher Quelle die *Übertragungen auf allen Leitungen bekannt* (z.B. bei ausschließlicher Verwendung eines physischen Broadcast-Mediums – im Gegensatz zu mit Hilfe von Protokollen realisierten Verteilnetzen, beispielsweise Ringen mit Punkt-zu-Punkt-Leitungen), so kann der aktive Angreifer beim MIX-Netz sicher entdeckt werden. (Beim RING-Netz natürlich auch, aber hier besteht der Witz des Verfahrens gerade darin, daß niemand die Übertragungen auf allen Leitungen kennt.) Anders ist dies beim DC-Netz, da hier auch die einer Station bekannten Schlüssel bekannt sein müssen, um zu entscheiden, ob sie gesendet hat. Sind nicht alle Übertragungen auf Leitungen öffentlich bekannt, so kann derselbe Effekt dadurch erreicht werden, daß jede Station jede von ihr auf der Leitung gesendete Nachricht unterschreibt. Das Unterschreiben und Speichern von Unterschriften verursacht zwar einen erheblichen zusätzlichen Aufwand, erlaubt es aber, hinterher sicher festzustellen, was genau auf der Leitung übertragen wurde. (Ein Sonderfall liegt vor, wenn beide Stationen an einer Leitung Angreifer sind und gemeinsam lügen. Dann kann natürlich nicht festgestellt werden, was auf der Leitung übertragen wurde.) Sind nicht alle Übertragungen auf Leitungen bekannt und wird nicht jede Nachricht unterschrieben, so können im MIX- und RING-Netz sowie im DC-Netz (dort über strittige gesendete Nachrichten oder strittige Schlüssel) drei Gruppen von Stationen identifiziert werden, wovon die erste Gruppe weder beschuldigt wird noch beschuldigt, während zumindest eins von beiden bei der zweiten und dritten Gruppe der Fall ist. Eine von ihnen ist der aktive Angreifer. Die andere ist unschuldig, wird aber vom Angreifer beschuldigt. Dabei gehen wir davon aus, daß sich nur ein Angreifer im Netz befindet, der aber mehrere Stationen besitzen oder unterwandert haben kann, und Widersprüche nur in der Umgebung des Angreifers vorkommen. Der Angreifer hat nur dann eine Chance, nicht sofort ermittelt zu werden, wenn er wenige andere Stationen beschuldigt. Ansonsten spräche eine Mehrheit von zu Unrecht beschuldigten „ehrlichen" Stationen gegen ihn. In diesem nicht entscheidbaren Fall jeweils weniger sich gegenseitig beschuldigender Stationen wird man normal weiterarbeiten, aber vorher so rekonfigurieren, daß sich im Wiederholungsfall diese wenigen Stationen nicht mehr gegenseitig beschuldigen können. Dies wird beispielsweise dadurch erreicht, daß

- beim MIX-Netz andere Wege (Adressen) verwendet werden, d.h. jeder Sender bildet Adressen nur noch so, daß keine Nachricht diese beiden MIXe direkt hintereinander passiert.
- beim DC-Netz keine Schlüssel zwischen den beiden betroffenen Stationen mehr ausgetauscht werden (die vorhandenen Schlüssel werden entfernt). Eine Alternative wäre, daß jeweils beide Partner ihren gemeinsamen Schlüssel vor seiner Verwendung digital unterschreiben, so daß jeder Partner die Unterschrift des anderen hat. Dann kann bei gegenseitiger Beschuldigung von einem Dritten nach Vorlage der Unterschriften entschieden werden, welche Station im Unrecht ist.

- beim RING-Netz wird der Ring rekonfiguriert. Dies ist bei einer Realisierung als virtueller Ring, d.h. auf einem beliebigen Kommunikationssystem wird ein logischer Ring durch Verbindungs-Verschlüsselung zur Simulation der Unbeobachtbarkeit der Ring-Leitungen realisiert (was auf eine eigene Datenschutz-Schicht führt), sehr leicht möglich. Bei einer physikalischen Realisierung ist die Rekonfigurierung sehr aufwendig und daher kostenintensiv.

Ist ein Netzbenutzer mehrfach in einer Gruppe, die eine andere beschuldigt oder von ihr beschuldigt wird, so wird er als der aktive Angreifer angesehen und aus dem Kommunikationssystem ausgeschlossen. Dieses Verfahren ist nur dann praktikabel, wenn relativ wenige Netzbenutzer aktive Angreifer sind. Ansonsten könnten die aktiven Angreifer zusammenarbeiten und die korrekt kommunizierenden Stationen aus dem Kommunikationssystem ausschließen, wobei sie dann natürlich immer weniger Stationen zum Beobachten hätten.

7 Ausblick

In den Kapiteln 2 bis 6 wurde skizziert, wie die drei Vorschläge zur Realisierung anonymer Netze auf ihrer jeweiligen Schicht (siehe Kapitel 1) fehlertolerant gemacht werden können. Außerdem können sowohl passive als auch aktive Angreifer (bis hin zum Versuch jegliche Diensterbringung zu verhindern) entdeckt und damit die Folgen von Fehlern *und* aktiven Angriffen begrenzt werden.

Praktisch realisiert werden solche Netze für schmalbandige Dienste als MIX-Netz auf den im Teilnehmeranschlußbereich vorhandenen Kupferdoppeladern [Pfit_86] oder für Dienste mit hohen Übertragungsleistungsanforderungen auf im Teilnehmeranschlußbereich zu verlegenden Glasfasern. Letzteres geschieht zumindest in den nächsten Jahrzehnten zweckmäßigerweise in einem räumlich begrenzten Gebiet, wobei mehrere solche lokalen Netze über Protokollumsetzer (gateways) mit einem konventionellen Vermittlungsnetz verbunden werden. Man kommt dann zu sogenannten Vermittlungs-/Verteilnetzen [Pfit_83, Pfil_85, PfPW_86]. Die Anonymität eines Netzbenutzers kann dann nur lokal garantiert werden. Der Betreiber des Vermittlungsnetzes kann sehr wohl feststellen, wenn zwei Netzbenutzer aus verschiedenen lokalen Netzen miteinander kommunizieren – er weiß jedoch nicht welche beiden Netzbenutzer. Da das Vermittlungsnetz selbst keine Anonymität garantiert, können in ihm konventionelle Fehlertoleranz-Maßnahmen verwendet werden.

Somit bleibt festzustellen, daß anonyme Kommunikationssysteme bzgl. Leistung [Bürl_85, Pfil_85], Zuverlässigkeit [Mann_85, Pfil_85] und Kosten [Mann_85, Pfil_85] realisierbar sind. Über sie können sogar viele Rechtsgeschäfte, bei denen man heute namentlich auftreten muß, mit Hilfe geeigneter höherer Protokolle ohne Verlust an Sicherheit anonym abgewickelt werden [Cha8_85, BüPf_86, PPW_87, WaPf_85], wodurch Datenschutz auch bei diesen Rechtsgeschäften für den Teilnehmer überprüfbar wird.

Zum Schluß sei noch auf die interessante Frage nach einer *quantitativen Abwägung zwischen Fehlertoleranz* einerseits und *Anonymität* andererseits hingewiesen. Hier scheinen zwei grundlegend verschiedene Konzepte möglich zu sein. Zum einen wird eine gesonderte Phase zur Fehlertoleranz eingeführt. Dadurch wird eine globale Sicht des Gesamtsystems erreicht, die die Fehlertoleranz erleichtert (vgl. die Zusammenfassung zu Beginn des Textes). In der Regel ist eine solche Realisierung jedoch wegen abrupter Unterbrechung der Nutzleistung unerwünscht. Zum anderen kann die Fehlertoleranz aus Sicht des Netzbenutzers im Hintergrund, parallel zur anonymen Datenübertragung, ablaufen. Dies ist immer dann möglich, wenn Fehler ausgehend von einer lokalen Sicht des Gesamtsystems toleriert werden können. Solche die Anonymität abschwächende Maßnahmen wurden für das MIX-Netz (fehlertolerante Verschlüsselungsstruktur – nur der Zustand des benachbarten MIXes muß bekannt sein) und das RING-Netz (lokale Ringrekonfigurierung und indeterministische bzw. asymmetrische Protokolle) diskutiert und für das DC-Netz angedeutet. Bei ihm kann die durch Schicht 0 (medium) und die untere Teilschicht von Schicht 1 (physical) – Schichten gemäß ISO-OSI Modell – geschaffene Bandbreite des Kommunikationsnetzes z.B. durch Zeit-Multiplex, auf viele DC-Netze aufgeteilt werden, auf denen jeweils alle Stationen empfangen, aber nur ein Teil der Stationen senden können [Nied_87].

Wir danken Holger Bürk, Dr. Klaus Echtle, Prof. Winfried Görke und Michael Waidner für ihre Kritik und Verbesserungsvorschläge.

Stichwörter: Recht auf informationelle Selbstbestimmung, Technischer Datenschutz, überprüfbarer Datenschutz, (Un-)Beobachtbarkeit, Fehlertoleranz trotz Anonymität, Anonymitätsmodus, Fehlertoleranzmodus, Individualüberwachung, Massenüberwachung, Vermittlungssysteme, Fernmeldenetze, ISDN, IBFN, „Trojanische Pferde", Verkehrsanalyse, Nutzdaten, Vermittlungsdaten, Verkehrsdaten, Verschlüsselung, MIX-Netz, DC-Netz, RING-Netz, Vermittlungs-/Verteilnetz, Verhinderung der Diensterbringung, anonyme Kanäle, indeterministische Protokolle, asymmetrische Protokolle, Koordinationsprotokoll

Literatur

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

BlGo_85 Manuel Blum, Shafi Goldwasser: An Efficient Probabilistic Public-Key Encryption Scheme Which Hides All Partial Information; 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 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

Bund_83 Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 – 1 BvR 209/83 u.a.; „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Heft 4, Oktober 1984, Vieweg & Sohn, Wiesbaden, Seite 258 bis 281

BüPf_86 Holger Bürk, Andreas Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Proceedings of the Fourth International Conference and Exhibition on Computer Security, Monte Carlo, 2. bis 4. Dezember 1986, A. Grissonnanche (ed.), North-Holland, 1986

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

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

Chau_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

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

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

DaZi_83 John D. Day, Hubert Zimmermann: The OSI Reference Model; Proceedings of the IEEE Vol. 71, Nu. 12, December 1983, Seite 1334 bis 1340

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

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

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

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 Berlin Heidelberg New-York Tokyo 1985, Seite 113 bis 127

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

Nied_87 Arnold Niedermaier: Bewertung von Zuverlässigkeit und Senderanonymität einer fehlertoleranten Kommunikationsstruktur; Diplomarbeit am Institut für Informatik IV, Universität Karlsruhe, August 1987

Pfit_83 Andreas Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; GI '83 13. Jahrestagung der Gesellschaft für Informatik 3. bis 7. Oktober 1983, Universität Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 411 bis 418

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 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 183 bis 190

Pfit_85 Andreas Pfitzmann: Technischer Datenschutz in diensteintegrierenden Digitalnetzen — Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur; 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 96 bis 112

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

Pfit_87 Andreas Pfitzmann: Experten warnen vor der Geheimhaltung von Kryptosystemen; Computer und Recht, Verlag Dr. Otto Schmidt KG, Köln, 3. Jahrgang, Heft 4, April 1987, Seite 272

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

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

PfPW_86 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen — Warum und wie? Stark überarbeitete und erweiterte Fassung von [Pfit_85], erschien in „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Heft 3, Juni 1986, Seite 178 bis 191, Vieweg & Sohn, Wiesbaden

PfWa_86 Andreas Pfitzmann, Michael Waidner: Networks without user observability — design options; Eurocrypt 85, Lecture Notes in Computer Science LNCS 219, Franz Pichler (ed.), Springer-Verlag Heidelberg, 1986, Seite 245 bis 253; Überarbeitete und erweiterte Fassung erschien unter dem Titel „Networks without user observability" in Computers & Security, North-Holland, Vol. 6, Nu. 2, April 1987, Seite 158 bis 166

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

PPW_87 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; erscheint in Computer und Recht, Verlag Dr. Otto Schmidt KG, Köln

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

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

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

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

Sham_79 Adi Shamir: How to Share a Secret; Communications of the ACM Vol. 22, Nu. 11, November 1979, Seite 612 bis 613

Shan_49 C. E. Shannon: Communication Theory of Secrecy Systems; The Bell System Technical Journal Vol. 28, No. 4, October 1949, Seite 656 bis 715

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

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 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, Seite 128 bis 141; Überarbeitung erschien in „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg & Sohn, Braunschweig, Heft 1, Februar 1986, Seite 16 bis 22

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, Friedr. Vieweg & Sohn Verlagsgesellschaft Braunschweig, Heft 6, Juni 1987, Seite 293 bis 299