Erscheint in: Datenschutz und Datensicherung Stand vom 21.11.1989

Telefon-MIXe:

Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß*

Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner
Institut für Rechnerentwurf und Fehlertoleranz
Universität Karlsruhe, Postfach 6980, 7500 Karlsruhe

Zusammenfassung

In öffentlichen Kommunikationsnetzen, z.B. dem Fernsprechnetz oder dem ISDN, muß der Datenschutz der Teilnehmer sichergestellt werden. Dieser umfaßt nicht nur den Schutz von Nachrichteninhalten, sondern auch den Schutz des Kommunikationsverhaltens (wer kommuniziert wann, wieviel, mit welchem Dienst, mit wem?).

Insbesondere das ISDN ermöglicht diesen Schutz nur sehr unzureichend. Im folgenden wird daher eine praktikable, Daten umfassend schützende Alternative zum ISDN aufgezeigt.

Um mit den ISDN-Normen und bereits vorhandenen ISDN-Ortsnetzen kompatibel zu sein, wird die Digitalisierung der Übertragung auf den vorhandenen Teilnehmeranschlußleitungen und der Ausbau des Fernnetzes wie für das ISDN geplant bzw. bereits realisiert angenommen. Die Ortsvermittlungsstellen nebst angeschlossenen Netzabschlüssen können also schrittweise modernisiert und erweitert werden. Auch die Aufteilung des Basisanschlusses in zwei unabhängige 64-kbit/s-Vollduplexkanäle für die Nutzdatenübertragung und einen 16-kbit/s-Signalisierungskanal wird übernommen.

Als bereitzustellender Dienst wird lediglich die Schaffung von 64-kbit/s-Verbindungen zwischen Netzabschlüssen mit Aufbauzeiten im Bereich von 3 s betrachtet. Ebenfalls den 16-kbit/s-Signalisierungskanal nutzende schmalstbandige Dienste werden nur am Rande betrachtet.

Der Schutz des Nachrichteninhalts wird wie üblich durch Ende-zu-Ende-Verschlüsselung, der Schutz der Teilnehmer vor Beobachtung ihres Kommunikationsverhaltens durch eine Variante des MIX-Netzes, *Telefon-MIXe* genannt, realisiert.

Eine alsbaldige Entwicklung und Realisierung eines Datenschutz garantierenden ISDN erscheint daher technisch möglich.

Schlüsselwörter

Technischer Datenschutz, ISDN, Fernmeldenetze, MIX-Netz, Telefon-MIXe, Unbeobachtbarkeit, Verschlüsselung.

1 Einleitung

Alle öffentlichen leitungsgebundenen Fernmeldenetze für Zweiwegkommunikation der Deutschen Bundespost haben eine gemeinsame Grundstruktur: Jeweils eine größere Gruppe von Netzabschlüssen ist sternförmig mit einer lokalen Zentrale, einer Ortsvermittlungsstelle (OVSt) verbunden. Diese Sternnetze sind ihrerseits über evtl. mehrstufige Fernnetze miteinander verbunden. Nachrichten und Kanäle werden vermittelt. Diese Struktur soll auch für das digitale ISDN beibehalten werden, das auf den vorhandenen

---

* Ein Überblick über diese Arbeit wurde auf der 4. SAVE-Tagung, 19. - 21. April 1989, in Köln gegeben.

schmalbandigen Teilnehmeranschlußleitungen seinen Teilnehmern als ISDN-Basisanschluß zwei unabhängige 64-kbit/s-Vollduplexkanäle anbietet. Die notwendige Signalisierung erfolgt über einen getrennten 16-kbit/s-Vollduplexkanal, der allerdings auch für einige Dienste mit geringer Bandbreite, z.B. Fernwirken, genutzt werden kann.

Der Grundgedanke des ISDN ist, alle schmalbandigen Dienste zu integrieren, insbesondere also den allgemein verbreiteten Fernsprechdienst. Herkömmliche Fernsprechanschlüsse soll es zwar weiterhin geben, aber auch für diese wird die dem ISDN zugrundeliegende digitale Vermittlungstechnik und ab der OVSt die digitale Übertragungstechnik verwendet werden.

Damit stellt sich natürlich die Frage nach der Gewährleistung des *Datenschutzes* der Benutzer öffentlicher Fernmeldedienste.

Dieser ist durch verschiedene Gesetze zwar leidlich gefordert, die Einhaltung dieser Gesetze ist aber weder durch die Teilnehmer noch durch Kontrollorgane *überprüfbar*. Jedem Netzabschluß und damit meist jedem Teilnehmer ist eine Anschlußleitung exklusiv zugeordnet. Das Abhören einer solchen Leitung stellt kein ernsthaftes technisches Problem dar; eine Verschlüsselung der Daten ist nicht vorgesehen. Sogar wenn diese Daten zwischen den Endgeräten nur verschlüsselt übertragen würden, blieben doch die *Verkehrsdaten* (wer hat mit wem wann, wie lange und mittels welchem Dienst kommuniziert?) in den frei programmierbaren digitalen Vermittlungszentralen leicht erfaßbar (und werden zu Abrechnungszwecken zum Teil auch wirklich dort erfaßt).

Kaum jemand wird der Deutschen Bundespost unterstellen, sie wolle ihre Kunden beobachten. Aber kann man das auch für all die Personen und Organisationen ausschließen, die Zugang zu den Vermittlungsrechnern haben, oder die während des Herstellungsprozesses die Gelegenheit hatten, ein Trojanisches Pferd einzubauen, das ihnen im Betrieb sensitive Daten zukommen lassen könnte?

Alles bisher Gesagte gilt übrigens nicht nur für das ISDN, sondern für alle Netze mit vergleichbarer Struktur. Eingeschränkt gilt es sogar schon für das heutige vorwiegend noch analoge, aber ebenfalls vermittelnde Fernsprechnetz (vgl. zu dieser Diskussion [KuRo_86, Pfit_86, Kub1_87, PPfW_88]).

Auf eine genaue Auflistung aller Beobachtungsmöglichkeiten wie auch auf eine Begründung der Notwendigkeit des Datenschutzes soll nicht weiter eingegangen werden. Eine ausführliche Diskussion hierzu findet sich in [PfPW_88 § 1, Pfit_89 § 1].

Im folgenden soll vielmehr eine Lösung des Problems der unbeobachtbaren Kommunikation vorgestellt werden, die

- wie das ISDN auf den schmalbandigen Teilnehmeranschlußleitungen über den Netzabschluß zwei unabhängige 64-kbit/s-Vollduplexkanäle anbieten kann,
- das Fernnetz unverändert läßt, und
- einen schrittweisen Ausbau erlaubt, d.h. das Nebeneinander von analogen bzw. Standard-ISDN-Ortsvermittlungsstellen und den neuen, hier vorgeschlagenen.

Die eigentliche Übertragung wird gegenüber dem ISDN nicht verändert, d.h. es wird von einem Vollduplexkanal mit 144 kbit/s je Netzabschluß und bitsynchronem Betrieb ausgegangen.

Schmalstbandige Dienste, die im ISDN zusammen mit der Signalisierung über den 16-kbit/s-Signalisierungskanal abgewickelt werden könnten, werden im folgenden nur am Rande betrachtet.

Zur Realisierung Datenschutz garantierender Digitalnetze sind im wesentlichen drei Lösungskonzepte bekannt (und in [PfPW_88 § 2, Pfit_89 § 2.5] genauer beschrieben): das DC-Netz [Chau_88] mit den Verbesserungen in [Waid_89, WaPf_89, WaPf1_89], das Konzept der physikalischen Unbeobachtbarkeit [Pfi1_83, Pfit_89] und das MIX-Netz [Chau_81].

Die ersten beiden Konzepte erfordern, daß jeder Netzabschluß im *physikalischen* Sinne mindestens halb soviel sendet wie *alle* Netzabschlüsse zusammen im *logischen* Sinne senden. Auf den vorhandenen Teilnehmeranschlußleitungen sind daher diese Konzepte für Dienste, die einen wesentlichen Anteil der 64 kbit/s

benötigen, nicht realisierbar. (Wird ein (Teil-)netz neu aufgebaut, oder steht ein Breitbandkabelverteilnetz zur Verfügung, so ist die Errichtung eines der anderen Netze jedoch durchaus möglich und sinnvoll, vgl. [PfPW_88 § 3, Pfit_89 § 6].)

Ohne diese Forderung kommt nur das MIX-Netz aus, auf dem auch das hier vorgestellte Verfahren basiert.

In § 2 wird daher die hier benötigte Variante des MIX-Netzes dargestellt. Das für Einzelnachrichten entworfene MIX-Netz ist aber unter den ISDN-Annahmen für Fernsprechen nicht effizient genug. In § 3 wird dargestellt, wie durch MIX-Kanäle eine schnellere Übermittlung von Nachrichten ermöglicht wird. Die Auf- und Abbauzeitpunkte der MIX-Kanäle sind durch die Unbeobachtbarkeit allerdings eingeschränkt. Das Verfahren der **Telefon-MIXe** in § 4, in dem unbeobachtbare Verbindungen aus MIX-Kanälen in einzelnen Zeitscheiben zusammengesetzt werden, erfüllt alle Voraussetzungen für den Einsatz unter den oben genannten Bedingungen. In § 5 wird seine Leistungsfähigkeit abgeschätzt.

Im folgenden wird in Anlehnung an den für das ISDN üblichen Sprachgebrauch [ITG_87] unter einem **Netzabschluß** ein Gerät verstanden, das seinen Benutzern den o.g. Übermittlungsdienst zur Verfügung stellt. Hierzu muß der Netzabschluß zusätzlich zu seinen üblichen auch einen großen Teil der zur Gewährleistung der Unbeobachtbarkeit notwendigen Funktionen erbringen. Damit wird die Unbeobachtbarkeit eines Teilnehmers wesentlich von der Zuverlässigkeit und Sicherheit seines Netzabschlusses abhängen.

2 Grundkonzepte

Im folgenden werden die Grundkonzepte des hier vorgestellten Verfahrens dargestellt. § 2.1 führt die verwendeten kryptographischen Begriffe und Parameter ein. § 2.2 erklärt kurz die hier benötigte Variante des MIX-Netzes; Leser, die mit dem MIX-Netz bereits vertraut sind, seien lediglich auf Bild 2 hingewiesen.

2.1 Verschlüsselung

Verschlüsselung der Nutzdaten ist eine Grundvoraussetzung für Datenschutz garantierende Netze. Da hinreichend sichere und effizient implementierbare Kryptosysteme und Schlüsselverteilprotokolle bekannt sind, steht dem baldigen Einsatz von Ende-zu-Ende-Verschlüsselung in einem digitalen schmalbandigen Netz *technisch* nichts im Wege.

Auf eine genaue Diskussion soll hier verzichtet werden, für eine Darstellung der bekanntesten Kryptosysteme vgl. [Denn_82, Bras_88], zu ihrem Einsatz in Kommunikationsnetzen vgl. [VoKe_83]. Generelles zur Sicherheit von Kryptosystemen findet sich in [GoMT_82, Bras_88], Ausführlicheres zum Einsatz in Datenschutz garantierenden offenen Systemen in [WaPP_87, PfPW_88, Pfit_89 § 2.3].

Im folgenden werden ein **symmetrisches Kryptosystem** (*secret key cryptosystem*), betrieben als **Stromchiffre**, und ein **asymmetrisches Kryptosystem** (*public key cryptosystem*), betrieben als **Blockchiffre**, vorausgesetzt. Die Bezeichnungen für Schlüssel und Ver- und Entschlüsselungsfunktionen sind in Bild 1 zusammengefaßt.

Parameter	symmetrische Stromchiffre	asymmetrische Blockchiffre
Schlüssel: für jeden Index x	k_x	öffentlicher Chiffrierschlüssel: c_x geheimer Dechiffrierschlüssel: d_x
Verschlüsselung der Nachricht N	$k_x(N)$	$c_x(N)$
Entschlüsselung der Nachricht N	$k_x^{-1}(N)$	$d_x(N)$

Bild 1 Bezeichnungen für die benötigten Kryptosysteme

Symmetrische und asymmetrische Kryptosysteme haben jeweils entgegengesetzte Vor- und Nachteile:

Die *Schlüsselverteilung* ist bei asymmetrischen Kryptosystemen sehr einfach, da der Chiffrierschlüssel öffentlich bekannt und daher einem Teilnehmer (bzw. in Datenschutz garantierenden Netzen einem *Pseudonym* [Chau_81, Cha8_85, PWP_87, BüPf_87]) fest zugeordnet sein kann. In symmetrischen Kryptosystemen wird hingegen für jede Paarbeziehung ein eigener geheimer Schlüssel benötigt.

Umgekehrt sind sicher scheinende symmetrische Kryptosysteme sehr viel *effizienter* implementierbar als sicher scheinende asymmetrische (z.B. erlaubt das symmetrische DES bei gleichem Realisierungsaufwand eine mehr als 100 mal schnellere Ver- und Entschlüsselung als das asymmetrische RSA, vgl. § 5).

Die Vorteile beider werden in der **hybriden Verschlüsselung** vereint [Bras_88 § 4.7]: Will Teilnehmer S eine Nachricht N beliebiger Länge an Teilnehmer E senden und kennt dessen öffentlichen Chiffrierschlüssel c_E, so wählt S sich zuerst zufällig einen Schlüssel k_{SE} des symmetrischen Kryptosystems, teilt diesen E, verschlüsselt mit c_E, mit und benutzt k_{SE}, um die eigentliche Nachricht schnell (und fortlaufend) zu verschlüsseln. Die hybride Verschlüsselung werde mit $c_E^*(N)$ bezeichnet:

$$c_E^*(N) := c_E(k_{SE}), k_{SE}(N)$$

Neben den Verschlüsselungssystemen wird noch ein **Pseudozufallsbitfolgengenerator** (PZBFG), eine **Hashfunktion** und ein **digitales Signatursystem** benötigt [Denn_82, Bras_88].

2.2 MIX-Netz

Das MIX-Netz wurde 1981 von DAVID CHAUM vorgeschlagen [Chau_81]. Seine Grundidee ist, die Gestalt von Nachrichten auf ihrem Weg von den Sendern zu den Empfängern so zu ändern, daß ein Angreifer Nachrichten in ihren verschiedenen Gestalten nicht wiedererkennen kann. Damit wird die *Kommunikationsbeziehung* von Sender und Empfänger verborgen.

In diesem Abschnitt wird keiner der Originalvorschläge vorgestellt, sondern die im folgenden wirklich benötigte Variante des MIX-Netzes. In § 2.2.1 wird zunächst das Grundprinzip des MIX-Netzes näher erläutert, in § 2.2.2 wird beschrieben, wie sich die Teilfunktion der Änderung der Gestalt einer Nachricht mit Hilfe eines asymmetrischen Kryptosystems realisieren läßt, und in § 2.2.3, wie durch Verteilung der Empfänger einer Nachricht verborgen wird.

2.2.1 Grundprinzip des MIX-Netzes

Möchte A an B eine Nachricht N senden und soll die Beziehung zwischen A und B verborgen werden, so sendet A seine Nachricht über eine fest vorgegebene Folge $M_1, \ldots, M_m$ von m ausgezeichneten Stationen. Diese werden als **MIXe**, die Folge als **MIX-Kaskade** bezeichnet.

Der erste MIX M_1 faßt alle Nachrichten, die er in einem bestimmten Zeitraum erhalten hat, zu einem sogenannten **Eingabeschub** zusammen. Jede Nachricht des Schubs wird **umcodiert**, d.h. ihr Aussehen wird in einer Weise geändert, die für keinen möglichen Angreifer, außer für M_1, der die Umcodierung vornimmt, und denjenigen, der die Nachricht entsprechend vorbereitet hat, nachvollziehbar ist. Alle Ausgabenachrichten werden gegenüber der Reihenfolge im Eingabeschub (z.B. gemäß einer festen Ordnungsrelation) **umsortiert** und zu einem **Ausgabeschub** zusammengefaßt. Damit erhält ein Angreifer, der nicht von M_1 unterstützt wird, keine (zusätzliche) Information über die Zuordnung von nicht von ihm selbst vorbereiteten Nachrichten im Eingabeschub von M_1 zu Nachrichten im Ausgabeschub von M_1.

Das Verfahren wird durch jeden weiteren MIX wiederholt, d.h. der Ausgabeschub von M_i ist zugleich der Eingabeschub von M_{i+1}, $i = 1, \ldots, m\text{-}1$ (Bild 2). Bereits ein einziger nicht den Angreifer unterstützender MIX gewährleistet also die Unbeobachtbarkeit.

Das *Senden* von Nachrichten bleibt beobachtbar. Daher kann der Empfänger einer Nachricht N die möglichen Sender von N auf diejenigen Netzabschlüsse begrenzen, die zum entsprechenden Zeitpunkt überhaupt etwas gesendet haben. Diese Beobachtungsmöglichkeit wird beseitigt, indem *alle* Netzabschlüsse zu *jedem* möglichen Zeitpunkt *gleichviel* (notfalls bedeutungslose) Nachrichten zum Eingabeschub von M_1 beisteuern (*dummy-traffic* [Bara_64, Chau_81]).

2.2.2 Umcodierung

Die Umcodierung wird im wesentlichen durch ein *hybrides Kryptosystem* realisiert (Bild 2).

Jeder MIX M_i, $i > 1$, wählt sich ein Schlüsselpaar (c_i, d_i) des asymmetrischen Kryptosystems und gibt c_i öffentlich bekannt. MIX M_1 tauscht mit jedem Netzabschluß A einen Schlüssel k_{1A} des symmetrischen Kryptosystems aus. Alle zu übermittelnden Nachrichten werden durch Auffüllen bzw. Aufspalten auf dieselbe Länge gebracht.

Angenommen, ein Teilnehmer möchte über seinen Netzabschluß A die (bereits Ende-zu-Ende-verschlüsselte) Nachricht N an den Netzabschluß B eines anderen Teilnehmers senden, und zusätzlich (warum, wird wenige Zeilen später klar werden) jedem MIX M_i gewisse Daten D_i zukommen lassen. Dann bildet er nacheinander die m+1 Nachrichten

$$\begin{aligned} N_{m+1} &:= N \\ N_i &:= c_i^*(D_i, N_{i+1}) \text{ für } i = m, m\text{-}1, \ldots, 2, \\ N_1 &:= k_{1A}(D_1, N_2) \end{aligned} \qquad (1)$$

und sendet N_1 an M_1. N_1 wird als **MIX-Eingabenachricht** bezeichnet.

Jeder M_i erhält von M_{i-1} bzw. von A die Nachricht N_i; die Umcodierung von N_i besteht in der Entschlüsselung mit k_{1A} bzw. d_i und dem Beseitigen von D_i.

(Für M_1 könnte natürlich statt des symmetrischen ebenfalls das hybride Kryptosystem verwendet werden, was jedoch den Aufwand zur Bildung von N_1 nur unnötig erhöhen und die Sicherheit in gewissen Fällen verschlechtern würde.)

Die Verschlüsselungen $c_i^*(.)$ in (1) müssen *indeterministisch* sein, damit ein Angreifer nicht einfach die Nachrichten des Ausgabeschubs gemäß (1) neu verschlüsseln und durch Vergleich mit den Nachrichten des zugehörigen Eingabeschubs die MIXe überbrücken kann.

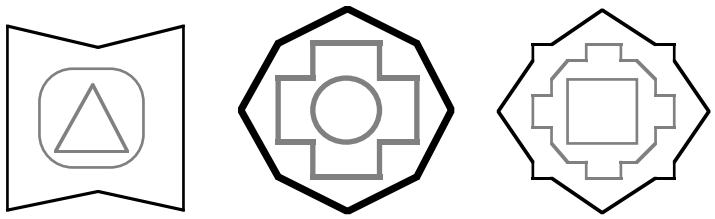
Die Entschlüsselungsfunktion jedes MIXes ist zwangsläufig *deterministisch*. Würde eine Nachricht N_i zweimal von M_i gemixt, so erschiene daher auch N_{i+1} zweimal als Ausgabe von M_i. Durch Wiederholung von N_i und Vergleich der Ausgabeschübe könnte also ein Angreifer leicht N_i mit N_{i+1} in Verbindung bringen. Genauer genügt hierzu schon die Wiederholung des ersten Blockes einer Nachricht.

Wiederholungen von Nachrichten in verschiedenen Schüben können durch den Schub eindeutig charakterisierende Zeitstempel ausgeschlossen werden, die den MIXen in den (siehe, eben dafür notwendigen) D_i vom Sender mitgeteilt werden. Nachrichten mit ungültigen Zeitstempeln werden ignoriert.

Schwerer zu vermeiden sind Wiederholungen im selben Schub. Daher müssen innerhalb eines Schubes die MIXe Nachrichten mit gleichen Anfangsblöcken ignorieren.

Ebenfalls zu verhindern ist, daß der Angreifer durch Manipulationen an einer Nachricht N_i (z.B. Verdoppeln einzelner Blöcke) für ihn erkennbare Muster in der zugehörigen Nachricht N_{i+1} erzeugen kann. Eine Stromchiffre, die dies garantiert, ist die Pseudo-Vernamchiffre, d.h. man erzeugt zur Verschlüsselung einer Nachricht N eine pseudozufällige Bitfolge der Länge $|N|$ (z.B. aus einer Blockchiffre im OFB-Modus) und bildet das bitweise exklusive Oder der Nachricht N und der Bitfolge [Denn_82]. Die Pseudo-Vernamchiffre erzeugt bei bitsynchroner Übertragung keine Fortpflanzung von Übertragungsfehlern und ist daher für das Folgende besonders geeignet.

Damit die Umcodierung sicher ist, sollte das asymmetrische Kryptosystem gegen aktive Angriffe sicher sein.

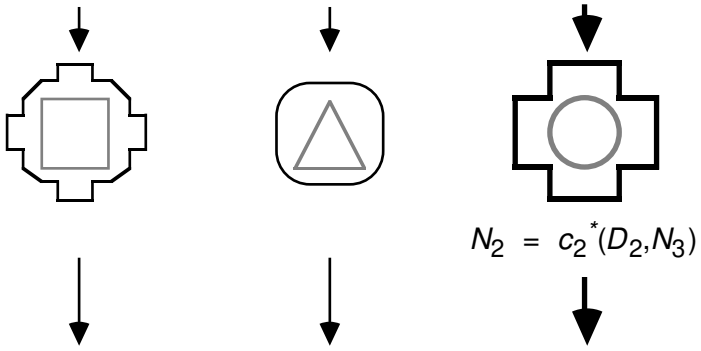


$N_1 = k_{1A}(D_1, c_2^*(D_2, N_3))$

MIX M_1

Faßt Nachrichten zu Eingabeschub zusammen, codiert sie um und gibt sie sortiert wieder aus: M_1

- erhält $N_1 = k_{1A}(D_1, N_2)$
- entschlüsselt N_1 mit k_{1A}, erhält die für ihn bestimmten Daten D_1 und die für ihn unlesbare Nachricht $N_2 = c_2^*(D_2, N_3)$ für M_2
- wertet D_1 aus und ordnet N_2 in seinen Ausgabeschub ein
- gibt den Ausgabeschub aus.

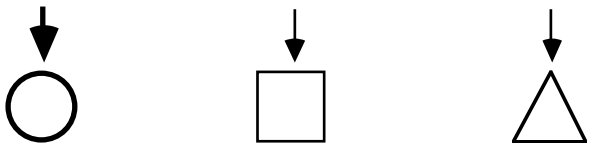


$N_2 = c_2^*(D_2, N_3)$

MIX M_2

Faßt Nachrichten zu Eingabeschub zusammen, ignoriert Wiederholungen, codiert die neuen Nachrichten um und gibt sie sortiert wieder aus: M_2

- erhält $N_2 = c_2^*(D_2, N_3)$
- entschlüsselt N_2 mit d_2, erhält die für ihn bestimmten Daten D_2 und die für ihn unlesbare Nachricht N_3 für den Empfänger
- wertet D_2 aus und ordnet N_3 in seinen Ausgabeschub ein
- verteilt den Ausgabeschub.



N_3

Bild 2 MIX-Prinzip am Beispiel einer Kaskade mit zwei MIXen und einem Schub von drei Nachrichten.

2.2.3 Verteilung und implizite Adressierung

Zum Schutz des Empfängers vor Beobachtung durch den Sender (der ja die Nachricht N_{m+1} kennt, die der Empfänger erhalten soll) wird der Ausgabeschub von M_m an alle Netzabschlüsse **verteilt**. Damit wird zugleich unbeobachtbar, wann jemand überhaupt eine Nachricht empfängt. Um unnötigen Aufwand zu vermeiden, werden bedeutungslose Nachrichten vom Sender für M_m erkennbar (z.B. in D_m) als bedeutungslos gekennzeichnet und vor der Verteilung von M_m ausgesondert; bis zu M_m müssen sie jedoch von echten Nachrichten ununterscheidbar sein.

Die Verteilung muß *zuverlässig* sein: Angenommen, die Nachricht N von A an X wird nicht korrekt verteilt, sondern nur einem Netzabschluß B zugestellt. Erhält A auf N Antwort, so war $B=X$, sonst (was meist durch Zeitschranken entscheidbar ist) war $B\neq X$, und A kann die Suche nach X fortsetzen [Waid_89, WaPf_89].

Dies kann durch **Rückmeldungen** der Netzabschlüsse an die MIXe verhindert werden: Jeder Netzabschluß sendet eine Signatur der erhaltenen Nachrichten an alle MIXe zurück. Damit diese nicht zu lang wird, sollte nur ein Hashwert der Nachrichten signiert werden. (Die üblichen Übereinstimmungsprotokolle [PeSL_80] sind, da hier von einem Sternnetz mit möglicherweise angreifender Zentrale ausgegangen werden soll, nicht anwendbar.)

Stimmen die Hashwerte nicht überein oder fehlt die Signatur eines Netzabschlusses, so muß, wenn der Schutz perfekt sein soll, sofort die Kommunikation im gesamten MIX-Netz unterbrochen werden. Damit kann das gesamte MIX-Netz allerdings durch jeden angreifenden Teilnehmer oder fehlerhaften Netzabschluß nachhaltig gestört werden. Aus praktischen Gründen wird daher der Schutz eingeschränkt und nach einem Protest eines Teilnehmers nicht die gesamte Kommunikation im MIX-Netz unterbrochen, sondern anhand signierter Nachrichten festgestellt, ob der Protest berechtigt war; ggf. wird der Angreifer verfolgt. Dazu muß in gewissen Abständen auch die Verteilzentrale eine Signatur der von ihr verteilten Nachrichten senden.

Im Fall, daß ein Teilnehmer behauptet, gar keine korrekt signierten Nachrichten empfangen zu haben, ist es jedoch leider prinzipiell nicht möglich, im nachhinein zu entscheiden, ob dies an ihm bzw. seinem Netzabschluß, an der Verteilzentrale oder einem aktiven Angriff auf der Teilnehmeranschlußleitung lag.

In einer an alle verteilten Nachricht darf der Sender den Empfänger natürlich nicht explizit angeben, sondern er muß diesen **implizit adressieren** [PfPW_88 § 2.2.1, Pfit_89 § 2.5.1].

Dies geschieht zweckmäßigerweise zusammen mit der Ende-zu-Ende-Verschlüsselung: zu jedem Pseudonym X wird ein Schlüssel c_X öffentlich bekanntgegeben. Der Sender A bestimmt seine dem Empfänger X mitzuteilende Nachricht und füllt sie ggf. auf eine Standardlänge auf. Sodann codiert er den ersten und gemäß der hybriden Verschlüsselung asymmetrisch zu verschlüsselnden Block seiner Nachricht redundant (z.B. durch einen fehlererkennenden Code). Die entstandene Nachricht sei N'. Der Sender A bestimmt schließlich die Nachricht N (d.h. die Nachricht N_{m+1} in § 2.2.2 (1)) als $c_X^*(N')$. Der Empfänger entschlüsselt probeweise alle verteilten Nachrichten N_{m+1} mit den zu seinen Pseudonymen gehörenden Schlüsseln und erkennt anhand der von A hinzugefügten Redundanz im ersten Block die für ihn bestimmten Nachrichten (im obigen Beispiel sind es genau diejenigen, die gültige Codewörter darstellen). Diese Adressierung wird **verdeckte implizite Adressierung** genannt.

Kennen sich A und X bereits aus einer früheren Kommunikationsbeziehung und möchte X von A wiedererkannt werden, so kann A auch **offene implizite Adressierung** verwenden: hierzu muß X zuvor A ein Kennzeichen a_{AX} (z.B. eine Folge von 100 Bits) als *offene Adresse* und einen Schlüssel k_{AX} des symmetrischen Kryptosystems mitgeteilt haben. Die Nachricht N' von A wird als $N = a_{AX}, k_{AX}(N')$ übertragen, und X erkennt sie als für ihn bestimmt durch Vergleich der Adresse a_{AX} mit all seinen offenen Adressen. (Um einem Außenstehenden keine Verkettung von verschiedenen offen implizit adressierten Nachrichten von A an X zu ermöglichen, sollten A und X die Adresse a_{AX} nur einmal verwenden. Sie

können sich aber leicht mit Hilfe eines Pseudozufallsbitfolgengenerators aus einer Adresse beliebig viele nacheinander verwendbare und in keiner offensichtlichen Beziehung zueinander stehende Adressen erzeugen. Der Schlüssel k_{AX} kann für alle Adressen derselbe sein.)

Es sei erwähnt, daß der Schutz des Empfängers vor dem Sender statt durch Verteilung der Nachrichten auch durch *anonyme Rückadressen* [Chau_81, Pfit_89 § 2.5.2] erreicht werden kann. Die Grundidee ist, die Verschlüsselungsstruktur der MIX-Eingabenachrichten vom Empfänger so vorherbestimmen zu lassen, daß der Sender ohne Hilfe aller MIXe diese Struktur nicht erkennen kann. Damit kann der Sender seine Nachricht nicht mehr bis zum Empfänger verfolgen. (Um wiederum den Sender vor Beobachtung durch den Empfänger zu schützen, werden beide Verschlüsselungsstrukturen kombiniert.)

Gleichwohl sich die Verteilung im folgenden als Hauptengpaß des Verfahrens der Telefon-MIXe herausstellen wird, sind anonyme Rückadressen hier dennoch nicht sinnvoll anwendbar, da sie die Unbeobachtbarkeit stark einschränken:

Möchte *A* an *B* eine Nachricht senden, so muß *A* hierzu eine Rückadresse von *B* kennen. Hinsichtlich ihrer Verkettbarkeit sind Rückadressen aber den offenen impliziten Adressen vergleichbar, d.h. die MIXe können erkennen, ob zwei Nachrichten mit derselben Rückadresse versehen sind. Das Empfangen an sich ist ebenfalls beobachtbar, d.h. es ist feststellbar, wieviele Nachrichten ein Teilnehmer überhaupt empfängt. Durch längeres Beobachten und Ausschließen von Möglichkeiten könnte ein Angreifer damit sogar die Zuordnung von häufiger verwendbaren Rückadressen zu Teilnehmern herausfinden.

In Kombination mit Verteilung und daher ohne Unbeobachtbarkeitseinbuße wird im folgenden ein ähnliches Konzept für MIX-Kanäle (§ 3) verwendet.

2.2.4 Bewertung der erreichten Unbeobachtbarkeit

Das MIX-Netz garantiert die Unbeobachtbarkeit nur unter gewissen Einschränkungen und kann zudem eine ganze Reihe von Beobachtungsmöglichkeiten im praktischen Sinne überhaupt nicht ausschließen.

2.2.4.1 Bedingungen für die Unbeobachtbarkeit

Ein **intuitives Maß** für die Unbeobachtbarkeit ist durch die Anzahl der nicht vom Angreifer kontrollierten Teilnehmer gegeben, denn nur unter diesen kann ein braver Teilnehmer vor dem Angreifer verborgen sein.

Im folgenden kann man in etwa von 5000 Teilnehmern je MIX-Netz ausgehen (vgl. § 5).

Die **implizite Adressierung** muß die Verkettung von Nachrichten sicher verbergen. Sollen Kontaktaufnahmen zwischen Teilnehmern möglich sein, die nicht bereits zuvor einen geheimen Schlüssel ausgetauscht haben, so ist die implizite Adressierung ein ebenso asymmetrisches Problem wie die asymmetrische Verschlüsselung und kann daher wie diese nur komplexitätstheoretisch sicher sein [PfWa_86, Pfit_89 § 2.5.1].

Ein komplexitätstheoretisch unbeschränkter Angreifer könnte also bereits anhand der (asymmetrischen) verdeckten impliziten Adressierung Teilnehmer deanonymisieren.

Im **MIX-Netz** schließlich muß wenigstens ein MIX existieren, der die Zuordnung seiner Eingaben und Ausgaben geheimhält und dessen Umcodierung vom Angreifer nicht gebrochen werden kann. Da die Umcodierungsfunktionen der MIXe M_i, $i > 1$, asymmetrische Kryptosysteme voraussetzen, ist das MIX-Netz damit i. allg. ebenfalls nur komplexitätstheoretisch sicher.

Ein komplexitätstheoretisch unbeschränkter Angreifer könnte also alle bis auf den ersten MIX (falls dieser ein perfektes symmetrisches Kryptosystem verwendet) überbrücken.

Die komplexitätstheoretische Sicherheit der impliziten Adressierung und des MIX-Netzes gilt i. allg. aber als völlig ausreichend, da ein realer Angreifer ja in der Tat in seiner Speicher- und Rechenkapazität beschränkt ist.

Im komplexitätstheoretischen Sinne *beweisbar sichere* implizite Adressierungsschemata oder MIX-Netze sind allerdings nicht bekannt. Dies liegt im wesentlichen daran, daß bereits keine asymmetrischen Kryptosysteme, die im *beweisbaren* Sinne gegen aktive Angriffe sicher sind, bekannt sind.

Ein Mechanismus, der die Möglichkeit aktiver Angriffe ausschließt und daher die Verwendung nur gegen passive Angreifer sicherer asymmetrischer Kryptosysteme erlaubt, ist in [GoMT_82] beschrieben, seine Anwendung auf MIXe in [Bött_89 § 3.3.1]. Das Brechen des gesamten Kryptosystems ist im besten Falle beweisbar äquivalent einem als schwer bekannten Problem, z.B. der effizienten Faktorisierung sehr großer Zahlen. Dasselbe gilt für das in [GaHY_89] angekündigte und wie [GoMT_82] mehrere Phasen benötigende Kryptosystem. Im selben Sinne beweisbar sicher sollte das in [BlFM_88] angekündigte *einphasige* Kryptosystem sein. Dies konnte jedoch leider nicht bewiesen werden [BeMi_89].

Es gibt jedoch *praktisch sichere* (d.h. trotz vieler Anstrengungen bis heute ungebrochene) Kryptosysteme (z.B. das in § 5.1.3 unterstellte und auf RSA basierende), so daß auch dieser Mangel eher von theoretischem Interesse ist.

2.2.4.2 Nicht ausgeschlossene Angriffe

Aus praktischen Gründen kann im MIX-Netz eine ganze Klasse von aktiven Angriffen nicht ausgeschlossen werden:

Angenommen, der Angreifer sendet eine Nachricht N an einen ihm unbekannten Teilnehmer X und weiß, daß X auf den Erhalt von N innerhalb einer begrenzten Zeit durch Senden einer Nachricht N' an den Angreifer antworten kann.

Der aktive Angriff besteht nun darin, daß der Angreifer einen Teilnehmer Y so stört, daß er, falls er mit X identisch ist, eben nicht auf den Erhalt von N reagieren könnte. Reagiert X trotz dieser Störung von Y, so ist zwangsläufig $X \neq Y$. Ansonsten hängt die Wahrscheinlichkeit für $X=Y$ natürlich davon ab, wie wahrscheinlich es überhaupt ist, daß X auf die Nachricht N des Angreifers reagiert.

(Durch Wiederholen des Angriffs und Stören mehrerer Teilnehmer kann der Angreifer den Teilnehmer X im günstigsten Fall in in der Teilnehmerzahl logarithmisch vielen Schritten identifizieren.)

Ein Beispiel für einen solchen Angriff wurde schon in § 2.2.3 gegeben, wo angenommen wurde, daß der Angreifer durch Manipulation des Verteilnetzes verhindern kann, daß Y die Nachricht N erhält. Denselben Erfolg hat der Angreifer natürlich, wenn er statt dessen Y im fraglichen Zeitraum am Senden seiner MIX-Eingabenachrichten hindern kann.

Diese Angriffe lassen sich *theoretisch* vereiteln, indem dafür gesorgt wird, daß ein solcher Angriffsversuch zum sofortigen Abbruch der Kommunikation im gesamten Netz führt. Der Angreifer erhält durch seinen Angriff dann keine Information mehr.

Aus Leistungs- und Zuverlässigkeitsgründen erscheint diese Möglichkeit für das MIX-Netz aber nicht anwendbar. (Entsprechende Techniken für das DC-Netz (vgl. § 1) sind in [Waid_89, WaPf_89, WaPf1_89] beschrieben.)

Für praktische Belange wird man sich daher wie in § 2.2.3 damit zufrieden geben müssen, daß ein Angriff der ersten Art zumindest erkannt und der Angreifer wenn möglich entdeckt werden kann. (Letzteres ist leider nicht immer möglich; insbesondere ist darauf zu achten, daß nicht statt des Angreifers ein braver Teilnehmer für schuldig erklärt wird.)

Eine weitere Möglichkeit, obigen Angriff zu realisieren, ergibt sich aus der Ausnutzung der Betriebsmittelknappheit: Das MIX-Netz hat im wesentlichen dort seinen Sinn, wo die Bandbreite der Teilnehmeranschlußleitungen stark begrenzt ist. In einem solchen Netz kann der Angreifer aber Y immer dadurch stören, daß er die gesamte für Y verfügbare Bandbreite blockiert, d.h. an Y soviele Nachrichten sendet, daß Y unmöglich weitere empfangen oder alle Antworten senden kann.

Auch dieser Angriff kann *theoretisch* vereitelt werden, indem die Überlastung eines Betriebsmittels durch eine vorweggenommene statische Aufteilung verhindert wird [Pfit_89 § 2.6]. Offensichtlich ist dies bei knappen Kommunikationsmitteln aber wenig praktikabel, so daß auch dieser Angriff hier nicht ausgeschlossen wird. Solange die Kommunikationsmittel eines Teilnehmers ausreichen, um alle externen Dienstanfragen zu berücksichtigen, weiß er zumindest, daß er durch diesen Angriff nicht bedroht wurde.

3 Schnellere Übermittlung durch MIX-Kanäle

Das in § 2.2 erläuterte MIX-Netz ist im wesentlichen zur unbeobachtbaren Übermittlung einzelner Nachrichten gedacht. Das MIX-Netz ist prinzipiell aber auch für Kanäle geeignet.

Im folgenden wird gezeigt, wie für Kanäle die Verzögerung durch die MIX-Operation verringert und die Verteilung aller Nachrichten (d.h. Kanäle) vermieden werden kann. Die sich so ergebenden MIX-Kanäle sind zwar unter den „ISDN-Annahmen" (vgl. § 1) nicht direkt einsetzbar, bilden jedoch das Grundverfahren der durchaus einsetzbaren Zeitscheibenkanäle (vgl. § 4).

In gewisser Weise realisiert bereits die hybride Verschlüsselung Simplexkanäle:

Der Hauptteil jeder Nachricht N_i ist lediglich mit einer symmetrischen *Stromchiffre* verschlüsselt. Da geeignete Stromchiffren Ver- und Entschlüsselungsgeschwindigkeiten im Mbit/s-Bereich haben und jedes Bit sofort zu ver- bzw. entschlüsseln erlauben, wird die Übermittlung dieses Hauptteiles praktisch nicht verzögert.

Der Anfang jeder Nachricht N_i, $i > 1$, wird jedoch merklich verzögert: Der erste Block der Nachricht ist asymmetrisch verschlüsselt. Zur Entschlüsselung muß meist der Empfang des gesamten ersten Blockes abgewartet werden, und die eigentliche Entschlüsselung ist bei Verwendung heutiger asymmetrischer Kryptosysteme vergleichsweise langsam. Hinzu kommt der Aufwand zur Umsortierung und für den Test auf Wiederholung von Nachrichtenanfängen.

Daher wird der langsame Kanalaufbau von der eigentlichen Nachrichtenübermittlung getrennt [Pfi1_85 § 2.1.2] und durch eigenständige Signalisierungsnachrichten realisiert.

Hierdurch wird eine Aufteilung der verfügbaren Bandbreite des Teilnehmeranschlusses in beiden Richtungen in jeweils einen Signalisierungsanteil für den Kanalaufbau und einen Datenanteil für die eigentliche Nachrichtenübermittlung vorgenommen. Die Art der Aufteilung ist für das folgende Verfahren irrelevant, doch wird in diesem Abschnitt der Einfachheit halber die im ISDN verwendete statische Aufteilung in einen Signalisierungskanal und mehrere Datenkanäle übernommen.

Zum Kanalaufbau wird gemäß § 2.2.2 (1) über den Signalisierungskanal eine MIX-Eingabenachricht N_1, genannt **Kanalaufbaunachricht**, gesendet, die den MIXen lediglich die für den symmetrischen Teil der hybriden Verschlüsselung benötigten Schlüssel k_i, $i > 1$, mitteilt. Folglich wird sie von M_m nicht verteilt. Der Einheitlichkeit halber sei mit k_1 im folgenden der Schlüssel k_{1A} abgekürzt, den der Sender A mit M_1 fest vereinbart hat.

Jeder MIX merkt sich die Zuordnung der Kanalaufbaunachricht vom Eingabe- zum Ausgabeschub. Jeder Kanalaufbaunachricht ist nun entsprechend ihrer Position im Eingabeschub von M_i ein Eingabekanal von M_i zugeordnet. Die Zuordnung der Kanalaufbaunachrichten vom Eingabe- zum Ausgabeschub von M_i definiert zugleich auch eine Vermittlung der Eingabekanäle von M_i auf die Ausgabekanäle von M_i, z.B. bei Frequenzmultiplex eine Zuordnung von Eingabe- zu Ausgabefrequenzen. Damit ist durch das Mixen der Kanalaufbaunachricht ein Kanal durch alle MIXe definiert, auf dem nun die eigentliche Nachricht übermittelt werden könnte.

Die Verteilung aller Kanäle an alle Netzabschlüsse wie in § 2.2.3 erscheint wenig sinnvoll, da davon ausgegangen wird, daß jeder Netzabschluß nur einige wenige, im ISDN meist zwei Kanäle empfangen

kann. Das Problem der Unbeobachtbarkeit des Empfängers vor dem Sender wird daher auf eine etwas andere Art gelöst, ähnlich den anonymen Rückadressen in [Chau_81].

Das Problem wird zunächst umgangen, indem der Empfänger dem Sender gleichgestellt wird: ein Kanal kann als **Sendekanal** oder als **Empfangskanal** genutzt werden.

Ein **Sendekanal** ist das genaue (d.h. oben suggerierte) Analogon zur hybriden Verschlüsselung: der Sender baut den Kanal auf, verschlüsselt den Informationsstrom N fortlaufend als $k_1(k_2(\ldots k_m(N)\ldots))$ und überträgt ihn an M_1. M_1 entschlüsselt fortlaufend mit k_1 und gibt den Nachrichtenstrom auf demselben Wege wie die zugehörige Kanalaufbaunachricht an M_2 weiter. Alle MIXe verfahren ebenso, d.h. M_m bildet am Ende den Klartextstrom N.

Ein **Empfangskanal** ist ein „rückwärts" betriebener Sendekanal: Der *Empfänger* baut den Kanal auf (mit derselben Art von Kanalaufbaunachricht). M_m erhält vom *Sender* den nicht speziell für die MIXe codierten (aber natürlich Ende-zu-Ende-verschlüsselten) Informationsstrom N, verschlüsselt ihn mit k_m und leitet $k_m(N)$ „zurück" an M_{m-1}. Alle MIXe verfahren ebenso, d.h. M_1 gibt am Ende den verschlüsselten Strom $k_1(\ldots k_m(N)\ldots)$ aus. Da der Empfänger alle Schlüssel k_i kennt, kann er hieraus N bestimmen.

Sende- und Empfangskanäle sind hinsichtlich ihrer Unbeobachtbarkeit völlig *symmetrisch*: Ebenso wie der Sender gefahrlos direkt seinen Sendekanal nutzen kann, ohne dadurch vom Empfänger identifiziert werden zu können, ist der Empfänger eines Empfangskanals vor Identifizierung durch den Sender geschützt. Hingegen ist der Empfänger eines Sendekanals durch den Sender und der Sender eines Empfangskanals durch den Empfänger beobachtbar.

Um nun beide Vorteile zu vereinen und beide Nachteile auszuschließen, werden die eigentlichen **MIX-Kanäle** als *Verknüpfungen* von Sende- und Empfangskanälen gebildet (Bild 3a-c): Der Sender baut einen Sendekanal auf, der bei M_m endet, und der Empfänger einen Empfangskanal, der bei M_m anfängt. M_m leitet den Informationsstrom, der auf dem Sendekanal eintrifft, auf den Empfangskanal um.

Die zu verknüpfenden Kanäle werden durch ein gemeinsames **Kanalkennzeichen** bezeichnet, das M_m übereinstimmend in beiden Kanalaufbaunachrichten erhält. Es muß natürlich beiden Partnern bekannt sein, und da man kaum von statischen und außerhalb des Netzes geknüpften Beziehungen ausgehen kann, muß es vom rufenden Partner R gewählt und mit dem üblichen Schema dem gerufenen Partner G in einer **Kanalwunschnachricht** mitgeteilt werden (sinnvollerweise zusammen mit einem Schlüssel zur Ende-zu-Ende-Verschlüsselung und der Angabe, ob R zu senden oder zu empfangen gedenkt). In Bild 3a wurde willkürlich R als Sender und G als Empfänger des MIX-Kanals angenommen. Es ist natürlich möglich, die Kanalwunschnachricht und die Kanalaufbaunachricht des Rufenden zu einer einzigen Signalisierungsnachricht zusammenzufassen.

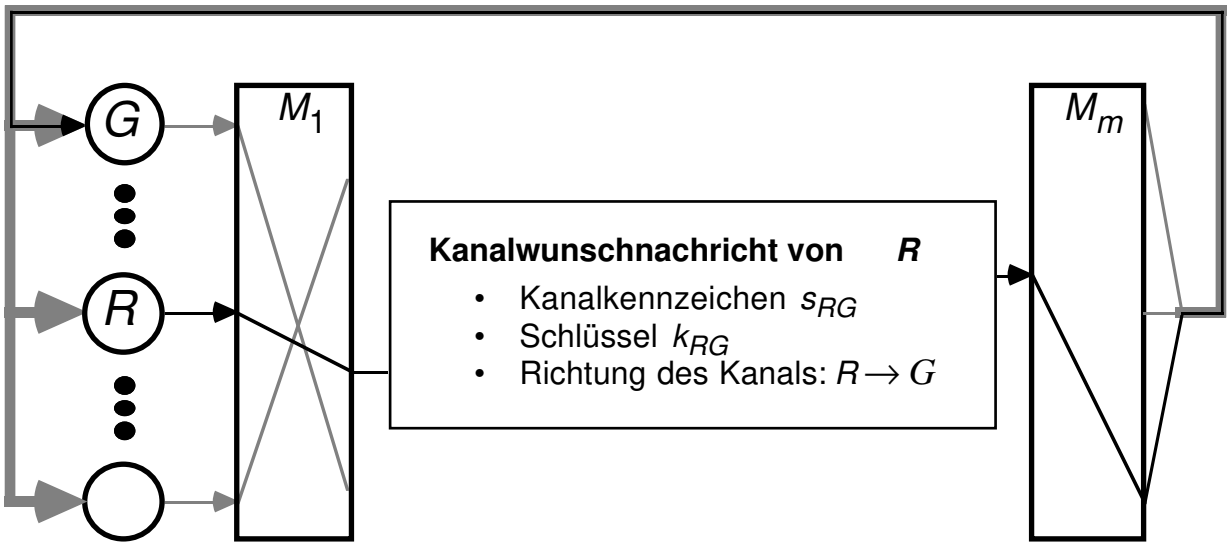


Bild 3a Der Netzabschluß *R* des rufenden Teilnehmers sendet über den Signalisierungskanal an den Netzabschluß *G* des gerufenen Teilnehmers eine Kanalwunschnachricht. Die Nachricht wird wie in Bild 2 dargestellt gemixt, der Ausgabeschub von M_m wird an alle Netzabschlüsse verteilt. *R* beabsichtigt zu senden.

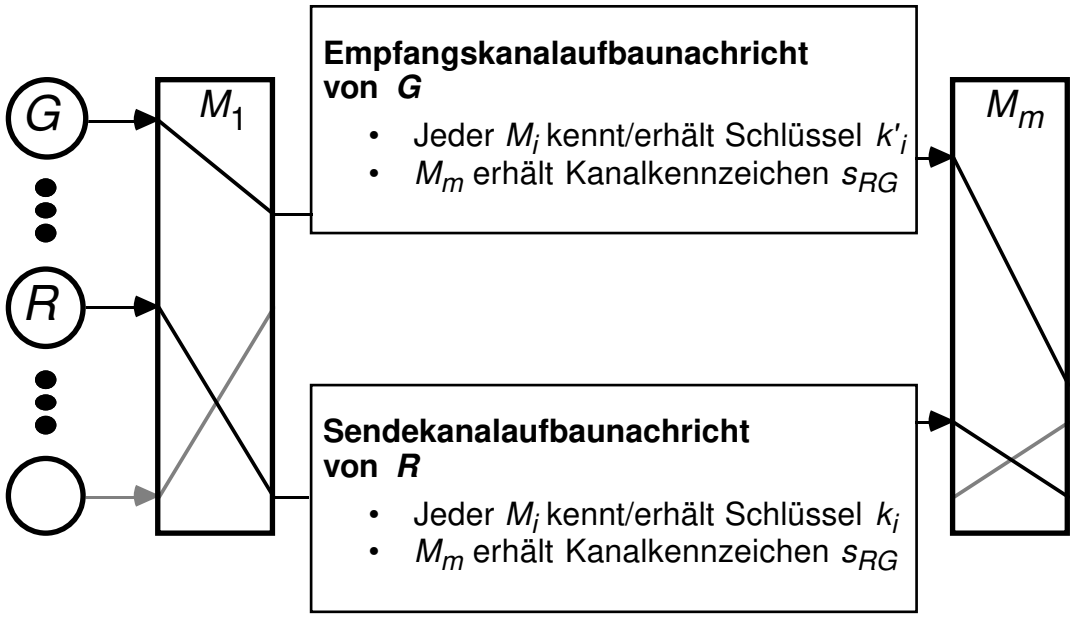


Bild 3b Beide Netzabschlüsse bauen nun einen Kanal auf. Die Kanalaufbaunachrichten werden über den Signalisierungskanal übertragen und wie in Bild 2 dargestellt gemixt, aber nicht verteilt. Die MIXe merken sich die Zuordnung der Kanalaufbaunachrichten von Eingabe- zu Ausgabeschüben, M_m verknüpft anhand des gemeinsamen Kanalkennzeichens s_{RG} den Sendekanal von *R* mit dem Empfangskanal von *G*.

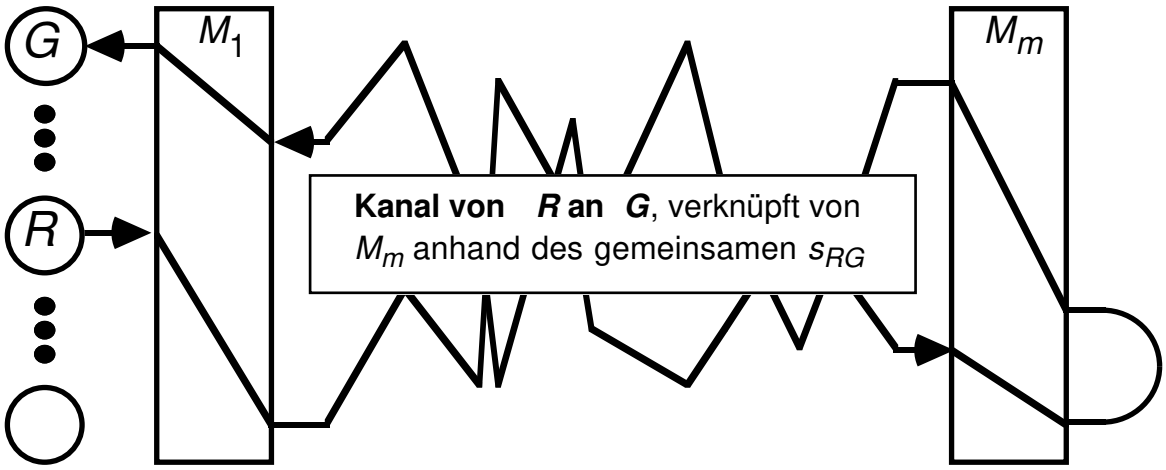


Bild 3c *R* sendet auf seinem Datenkanal Daten *N* verschlüsselt als $k_1(\ldots k_m(N)\ldots)$ an M_1. Der Kanal wird von M_1 über die weiteren MIXe bis zu M_m wie die Sendekanalaufbaunachricht in Bild 3b weitergeleitet und dabei werden die Daten entschlüsselt. M_m verschlüsselt *N* mit k'_m. Der Kanal wird zurückgeleitet und dabei werden die Daten verschlüsselt, *G* erhält über seinen Datenkanal $k'_1(\ldots k'_m(N)\ldots)$.

Kanalwunschnachrichten, Sende- und Empfangskanalaufbaunachrichten stellen die drei Typen von Signalisierungsnachrichten des Verfahrens dar. Die Übermittlung aller Signalisierungsnachrichten erfolgt nach dem Grundschema aus § 2, außer daß die Sende- und Empfangskanalaufbaunachrichten nicht verteilt werden.

Da die Größe der Eingabeschübe den Aufwand der einzelnen MIXe entscheidend beeinflußt, ist es sinnvoll, die Nachrichten der drei verschiedenen Typen getrennt zu mixen. Die Unbeobachtbarkeit wird dadurch nicht eingeschränkt.

Zur Vermeidung von Wiederholungen müssen entweder die Zeitstempel der MIX-Eingabenachrichten sowohl den Schub als auch den Nachrichtentyp eindeutig charakterisieren, oder aber die MIXe müssen für die verschiedenen Nachrichtentypen verschiedene Schlüssel zur Umcodierung verwenden. Die Angabe des Nachrichtentyps verursacht für die Netzabschlüsse zwar weniger Synchronisationsaufwand, andererseits wird aber ohnehin von einem streng synchronen Betrieb ausgegangen, und der Signalisierungskanal stellt den Hauptengpaß des Verfahrens dar. Daher wird im folgenden stets von der zweiten Möglichkeit ausgegangen.

Wie im Grundschema wird das Problem der Beobachtbarkeit des Sendens auf einem Sendekanal gelöst, indem jeder Netzabschluß jederzeit gleichviele Sendekanäle (notfalls Scheinsendekanäle) unterhält.

Ohne Verteilung ist nun natürlich das tatsächliche Empfangen von einem Empfangskanal beobachtbar. Daher muß jeder Netzabschluß jederzeit auch gleichviele Empfangskanäle (notfalls Scheinempfangskanäle) unterhalten.

Die gleiche Länge aller Kanäle wird durch die MIXe garantiert: wird auf einem Sende- oder Empfangskanal nichts übertragen, so überbrückt jeder MIX M_i dieses Fehlen durch bedeutungslose Daten.

Hierdurch wird insbesondere verhindert, daß der Sender den Empfänger identifiziert, indem er auf dem Sendekanal keine Information überträgt und der Empfänger nichts erhält. Dies ist der Grund, weshalb hier, anders als in [Pfi1_85], der Empfänger selbst seinen Empfangskanal aufbaut.

Zugleich wird verhindert, daß Scheinempfangskanäle durch Fehlen von Daten auffallen.

Ein **Duplexkanal** wird durch zwei gegenlaufende Simplexkanäle eingerichtet. Beide Kanäle könnten vom Rufenden mit derselben Kanalaufbaunachricht aufgebaut werden. Dies spart zwar Übertragungskapazität,

wird sich aber im folgenden als hinderlich herausstellen, so daß schon jetzt von zwei völlig getrennten MIX-Kanälen ausgegangen werden soll. Allerdings genügt eine gemeinsame Kanalwunschnachricht.

Im vorigen Absatz wurde beschrieben, wie ein aktiver Angriff eines Senders auf den zugehörigen Empfänger verhindert werden kann. Da aber der in § 2.2.4.2 beschriebene aktive Angriff eines Empfängers auf den zugehörigen Sender nicht verhindert werden kann und auch für MIX-Kanäle möglich ist, könnte man argumentieren, daß diese Maßnahme für Duplexkanäle völlig sinnlos ist, da der Angreifer seinen Partner ja wahlweise als Sender oder als Empfänger angreifen kann.

Aus praktischen Gründen ist die Verhinderung des Angriffs auf den Empfänger aber dennoch sinnvoll, da er sehr viel einfacher durchzuführen wäre als der Angriff auf den Sender: statt, wie in § 2.2.4.2 beschrieben, Senden aktiv zu stören, muß der Angreifer lediglich alle Empfangskanäle beobachten können. Zudem gelingt der Angriff auf den Empfänger sofort, während der Angriff auf den Sender lediglich einen Test darstellt, der dann logarithmisch in der Senderanzahl oft wiederholt werden muß, um den Sender wirklich zu finden.

Da für die eigentlichen MIX-Kanäle die üblicherweise aufwendigsten MIX-Aufgaben, nämlich die Sortierung von Nachrichten und die Kontrolle auf Wiederholungen, entfallen, d.h. lediglich eine einfache Umcodierung und Vermittlung von Eingangs- auf Ausgangskanäle erfolgt, kann der Aufwand der MIXe zur Verwaltung der MIX-Kanäle vernachlässigt werden. Die Umcodierung der Daten mit der symmetrischen Stromchiffre fällt, da sie mit einer sehr viel höheren Rate erfolgen kann als die Übertragung (vgl. § 5), kaum ins Gewicht.

In dieser Form könnte das Verfahren jedoch unter den „ISDN-Annahmen" (vgl. § 1) noch nicht direkt eingesetzt werden. Neben der üblichen Überlegung, daß das Verfahren nicht homogen für alle Netzabschlüsse auf einmal, sondern nur innerhalb gewisser Anonymitätsgruppen durchgeführt werden könnte, gibt es nämlich noch ein schwerwiegendes Problem. Wie für die Nachrichten in § 2.2 gilt auch für MIX-Kanäle:

- Jeder Netzabschluß muß für jeden Kanalwunscheingabeschub von M_1 gleich viele Kanalwunschnachrichten und Sende- und Empfangskanalaufbaunachrichten beisteuern, und entsprechend gleich viele Sende- und Empfangskanäle unterhalten.
- Nachrichten eines Schubes müssen gleich lang sein, was hier insbesondere heißt, daß gleichzeitig aufgebaute Kanäle auch *gleichzeitig* wieder abgebaut werden müssen.

Dies würde vor allem bedeuten, daß jeder Netzabschluß mit dem Abbau eines Kanals, sogar eines Scheinkanals, warten müßte, bis der längste gleichzeitig aufgebaute Kanal beendet wäre. Da dem Teilnehmer nur zwei 64-kbit/s-Kanäle zur Verfügung stehen, wäre dies unzumutbar.

Diese Einschränkung wird durch das Verfahren des folgenden Kapitels beseitigt.

4 Telefon-MIXe

Das folgende Verfahren, **Telefon-MIXe** genannt, erlaubt den Teilnehmern das Unterhalten **unbeobachtbarer Verbindungen**, d.h. unbeobachtbarer Ende-zu-Ende-Kanäle, die, im Gegensatz zu den MIX-Kanälen, beliebig lange andauern und von jedem der Partner nahezu jederzeit abgebaut werden können.

Es wird im wesentlichen nur die Verbindung zwischen den Netzabschlüssen der Teilnehmer betrachtet, die darauf aufbauende Verbindung zwischen den Endgeräten bzw. den i. allg. menschlichen Teilnehmern selbst wird nur dort betrachtet, wo sie sich von der Situation im ISDN unterscheidet. Über einen ISDN-Basisanschluß kann ein Teilnehmer gleichzeitig zwei 64-kbit/s-Duplexverbindungen unterhalten.

Im Gegensatz zu bisher soll hier gleich ein hierarchisches Netz mit Ortsnetzen und Fernnetz betrachtet werden.

In §§ 4.1-4.2 wird das Grundprinzip der Telefon-MIXe, die Verwendung von Zeitscheibenkanälen, dargestellt. In §§ 4.3-4.4 wird der Auf- und Abbau von Verbindungen behandelt. In § 4.5 werden die Abrechnung der Netzbenutzung, in § 4.6 Verbindungen zwischen OVSt'n mit MIX-Kaskade und herkömmlichen OVSt'n und in § 4.7 die Zuverlässigkeit betrachtet.

4.1 Grundprinzip der Zeitscheibenkanäle

Beide am Ende von § 3 für MIX-Kanäle genannten Probleme werden gelöst, indem beliebig lange andauernde Verbindungen auf mehrere kurze (≈ 1 s) und unmittelbar aufeinanderfolgende MIX-Kanäle, genannt **Zeitscheibenkanäle**, aufgeteilt werden. Mit jeder neuen Zeitscheibe hat jeder Teilnehmer die Möglichkeit, eine neue Verbindung einzurichten oder eine bestehende abzubrechen.

Jeder Zeitscheibenkanal habe die Zeitdauer z. Die Einteilung in Zeitscheiben erfolgt synchron für alle Teilnehmer des gesamten Netzes. Wie in § 3 besteht ein Zeitscheibenduplexkanal aus einem Sende- und einem Empfangskanal, die mit **ZS-Kanal** und **ZE-Kanal** abgekürzt werden. Für jede Zeitscheibe baut ein Netzabschluß eine konstante Anzahl von ZS- und ZE-Kanälen auf (d.h. hier jeweils ein Paar je 64-kbit/s-Kanal).

Eine reale Verbindung wird durch eine **Verbindungswunschnachricht** eingeleitet, die, wie oben die Kanalwunschnachricht, der Netzabschluß R des rufenden Teilnehmers an den Netzabschluß G des gerufenen Teilnehmers sendet. Im Idealfall, d.h. wenn G den Wunsch sofort akzeptiert und beide sich an ihr Protokoll halten, verknüpfen R und G ab einer vorherbestimmten Zeitscheibe ihre ZS- und ZE-Kanäle, bis einer von beiden den Abbruch signalisiert und sie wieder synchron ihre ZS- und ZE-Kanäle trennen. (Weitere Kanalwunschnachrichten für die einzelnen Zeitscheibenkanäle werden bei geeigneter Verbindungswunschnachricht nicht benötigt, vgl. § 4.3.)

Solange ein Netzabschluß keine reale Verbindung unterhält, sendet er zufällige Daten an sich selbst, d.h. sein ZS-Kanal ist direkt mit seinem ZE-Kanal verbunden. Da bedeutungsvolle Daten Ende-zu-Ende-verschlüsselt sind, also Außenstehenden ebenfalls zufällig erscheinen, sind zufällige Daten von einem wirklichen Ende-zu-Ende-Kanal nicht zu unterscheiden. (Alternativ könnte man Scheinkanäle auch wie in § 3 „offen“ lassen, d.h. mit keinem passenden Gegenstück verknüpfen. Dann könnte M_m sie aber von wirklichen Kanälen unterscheiden. Dies ist auch der Grund, die beiden Teile eines Duplexkanals einzeln aufzubauen.)

Die notwendige Signalisierung erfolgt im wesentlichen wie in § 3 über einen eigenen Signalisierungskanal, der in dem nicht für Datenkanäle genutzten Anteil der verfügbaren Bandbreite untergebracht werden muß, beim ISDN-Basisanschluß also in den in beiden Richtungen verbliebenen 16 kbit/s. Dieser Signalisierungskanal wird der Hauptengpaß des Verfahrens sein, da über ihn die Verbindungswunsch- und die ZE- und ZS-Kanalaufbaunachrichten übertragen und erstere sogar verteilt werden müssen.

Im Gegensatz zum ISDN findet daher der Teil der Signalisierung, der nach Aufbau der Verbindung zwischen den Anschlüssen noch notwendig ist, innerhalb des Datenkanals statt, allerdings nur soviel, daß der Datenkanal transparent bleibt. Die Signalisierung zum Zwecke des Verbindungsaufbaus findet jedoch ausschließlich im Signalisierungskanal statt.

Da für die Telefon-MIXe die schmalbandigen Teilnehmeranschlußleitungen und das Fernnetz unverändert gelassen werden sollen, kann das Verfahren nur im *lokalen Bereich* eingesetzt werden, d.h. jeder OVSt wird jeweils eine MIX-Kaskade von m MIXen zugeordnet.

Die Aufgabenverteilung zwischen OVSt und MIXen ist recht einfach: Die MIXe sind ausschließlich für die MIX-Funktionen zuständig, alle übrigen Aufgaben werden von der OVSt erfüllt. Funktional kann man sich eine solche OVSt zweigeteilt vorstellen: Die eine Hälfte übernimmt die Kommunikation zwischen dem ersten MIX der Kaskade und den Teilnehmern, insbesondere auch die Aufgaben der Verteilzentrale in

§ 2.2.3. Die andere Hälfte übernimmt die Kommunikation zwischen dem letzten MIX der Kaskade und dem Fernnetz (sowie einige Umsetzungsaufgaben, vgl. § 4.6).

In großen Ortsnetzen (mit mehr als 5000 Teilnehmern) wird es wegen der beschränkten Bandbreite des Teilnehmeranschlusses notwendig sein, die Teilnehmer ein für allemal logisch (d.h. ohne neue OVSt oder MIXe) in mehrere Anonymitätsgruppen einzuteilen, so daß Mixen und Verteilung immer nur innerhalb einer Anonymitätsgruppe stattfinden.

Der durch die Scheinsende- und Scheinempfangskanäle entstehende zusätzliche Kommunikationsaufwand stört hier nicht, da er nur die Teilnehmeranschlußleitung des Teilnehmers selbst betrifft, die diesem exklusiv zugeordnet ist und in derselben Zeit andernfalls ungenutzt wäre.

Im folgenden soll gleich der allgemeine Fall betrachtet werden, daß R und G möglicherweise zu verschiedenen OVSt'n gehören. Sei hierzu $MR_1, \ldots, MR_m$ die MIX-Kaskade von R, $MG_1, \ldots, MG_m$ die von G (Bild 4).

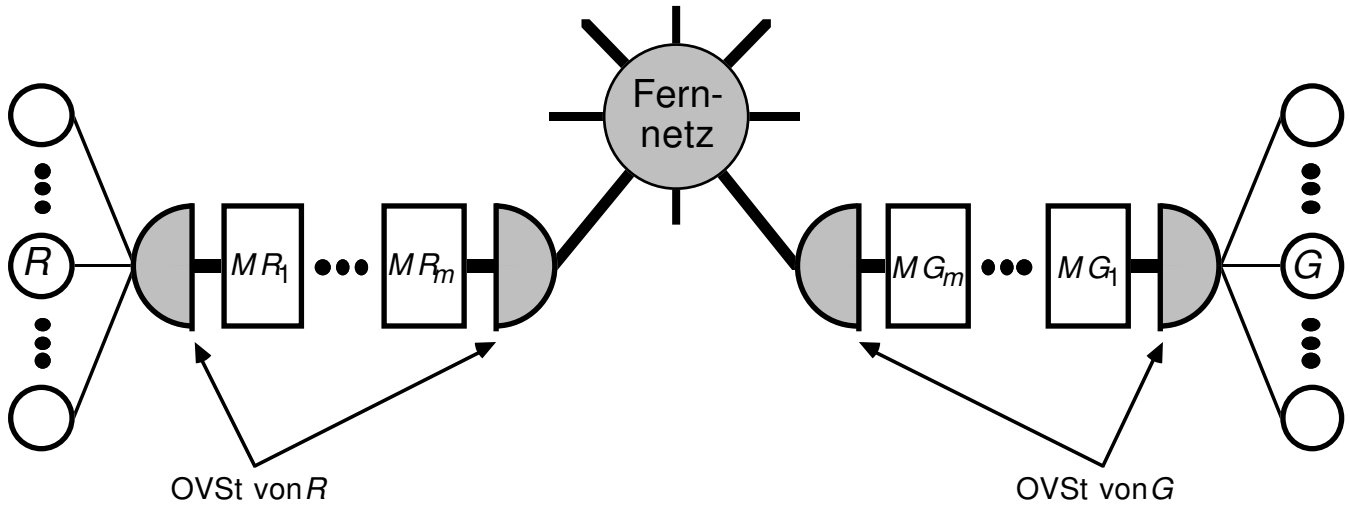


Bild 4 Netzabschlüsse des rufenden und des gerufenen Teilnehmers mit jeweiliger OVSt (aufgespalten in die zwei Funktionshälften) und zugeordneter MIX-Kaskade.

Der Sonderfall, daß einer der beiden Netzabschlüsse an eine OVSt *ohne* MIX-Kaskade angeschlossen ist, wird in § 4.6 behandelt.

4.2 Aufbau der Zeitscheibenkanäle

Zeitscheibenkanäle zeichnen sich gegenüber den MIX-Kanälen in § 3 lediglich durch ihre vorgegebene Dauer sowie vorgegebene Anfangszeitpunkte aus, so daß hier nichts prinzipiell Neues zu sagen ist. Zu beachten ist lediglich der Einfluß des Fernnetzes auf das Nachrichtenformat und den Beginn der Zeitscheiben.

Sind R und G nicht an dieselbe OVSt angeschlossen, so müssen die MIXe MR_m und MG_m die Funktion des letzten MIXes M_m in § 3 gemeinsam erbringen:

Ein ZS-Kanal z.B. von R an G wird von MR_m über die OVSt von R, das Fernnetz und die OVSt von G an MG_m übermittelt, der ihn in den passenden ZE-Kanal von G einleiten muß. Um dies zu ermöglichen, muß R in seiner ZS-Kanalaufbaunachricht MR_m zusätzlich die OVSt von G mitteilen.

Da die Verbindung zwischen R und G aus sehr vielen Zeitscheibenkanälen besteht, ist es sinnvoll, den zur Übermittlung notwendigen Kanal im Fernnetz zwischen den OVSt'n von R und G für die gesamte

Verbindung zu nutzen. Der Zusammenhang der verschiedenen Zeitscheibenkanäle der Verbindung muß dabei für die MIXe MR_m und MG_m bzw. die OVSt'n nicht explizit hergestellt werden; es genügt, daß der Kanal im Fernnetz erst dann abgebaut wird, wenn erstmalig *kein* Zeitscheibenkanal zwischen den OVSt'n von *R* und *G* zu übermitteln ist.

Wie üblich muß eine MIX-Kaskade mit dem Beginn der ZE-Kanäle der aktuellen Zeitscheibe warten, bis die Anfänge aller entsprechenden ZS-Kanäle eingetroffen sind.

MG_m bzw. MR_m muß daher die schnell eintreffenden, aus demselben Ortsnetz stammenden ZS-Kanäle solange zwischenpuffern, bis ZS-Kanäle von überall aus dem Fernnetz Zeit hatten einzutreffen. (Bei einer maximalen Laufzeit von 0,2 s im Fernnetz wären dies 12,8 kbit je lokalem 64-kbit/s-Simplexkanal.)

In Bild 5 sind die von den MIXen benötigten Daten für den Kanalaufbau zusammengefaßt. Die Schlüssel des symmetrischen Kryptosystems werden durch die hybride Verschlüsselung übergeben, die restlichen Daten in den D_i-Feldern der Kanalaufbaunachricht. Das Feld „Gebührenmarke" wird in § 4.5 erklärt.

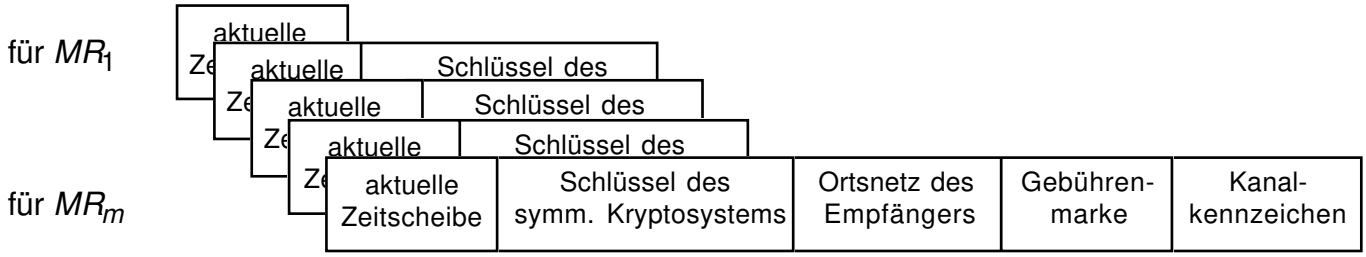


Bild 5a Von den MIXen MR_i benötigte Daten für den ZS-Kanalaufbau.

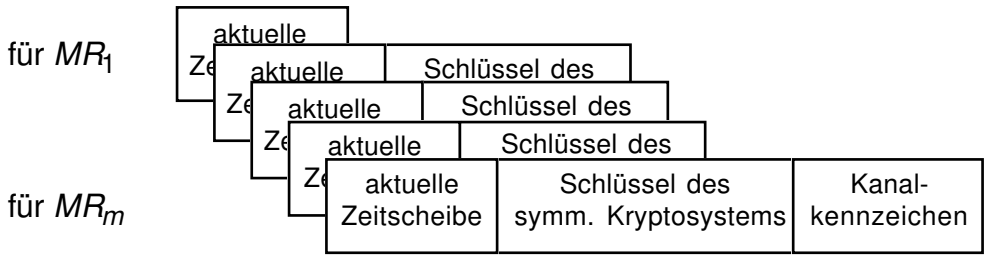


Bild 5b Von den MIXen MR_i benötigte Daten für den ZE-Kanalaufbau.

4.3 Aufbau einer unbeobachtbaren Verbindung

Zum Aufbau einer unbeobachtbaren Verbindung sendet der Netzabschluß *R* des rufenden Teilnehmers über seinen Signalisierungskanal eine **Verbindungswunschnachricht**. Die Nachricht wird mit dem Schema aus § 2.2 übermittelt, d.h. sie wird von der Kaskade MR_1, …, MR_m gemixt, ggf. über das Fernnetz zur OVSt des Empfängers übermittelt und dort an alle Teilnehmeranschlüsse verteilt.

Da mit jeder neuen Zeitscheibe jeder Teilnehmer die Möglichkeit haben soll, eine neue Verbindung einzurichten, müssen auch Verbindungswunschnachrichten einmal pro Zeitscheibe gemixt werden. Im folgenden wird angenommen, daß jeder Netzabschluß pro Zeitscheibe und Datenkanal genau eine, ggf. bedeutungslose, solche Nachricht beisteuert.

Der Netzabschluß *G* des Gerufenen muß die Nummer t_0 der ersten Zeitscheibe erfahren, ab der die Verbindung bestehen soll.

Die Kanalwunschnachrichten der einzelnen Zeitscheibenkanäle (hier zwei je Zeitscheibe) werden alle zusammengefaßt und in die Verbindungswunschnachricht integriert:

- G erhält das feste Ortsnetzkennzeichen von R.
- Die Kanalkennzeichen der Zeitscheibenkanäle werden systematisch mit einem Pseudozufallsbitfolgengenerator (PZBFG) erzeugt, wozu R an G einen Startwert s_{RG} des PZBFG schickt.

  Bezeichnet $s_{RG}(x)$ das x-te aus s_{RG} abgeleitete Kennzeichen, so wird für die Zeitscheibe $(t_0 + t)$, $t = 0, 1, \ldots$, in Richtung $R \rightarrow G$ das Kennzeichen $s_{RG}(2 \bullet t+1)$ und in Richtung $G \rightarrow R$ das Kennzeichen $s_{RG}(2 \bullet t+2)$ verwendet.
- R und G verwenden für alle Zeitscheibenkanäle einen einzigen Schlüssel k_{RG} zur Ende-zu-Ende-Verschlüsselung (was außer R und G aber niemand feststellen kann, also auch nichts schadet). Auch k_{RG} kann aus s_{RG} abgeleitet werden.

Alternativ könnte man auch einen von s_{RG} unabhängigen Schlüssel k_{RG} mitschicken, oder für die beiden Richtungen $R \rightarrow G$ und $G \rightarrow R$ zwei getrennte Startwerte des PZBFG verwenden. Dies würde aber die von der OVSt von G zu *verteilende* Verbindungswunschnachricht nur unnötig verlängern.

Im korrekten Fall baut R ab Zeitscheibe t_0 nun wie angekündigt einen ZS- und ZE-Kanal mit den oben angegebenen aus s_{RG} abgeleiteten Kennzeichen auf.

Im Idealfall wird der Kanal zwischen den Anschlüssen R und G geschaltet, indem G ebenfalls ab t_0 seinen ZS- und ZE-Kanal passend aufbaut (Bild 6).

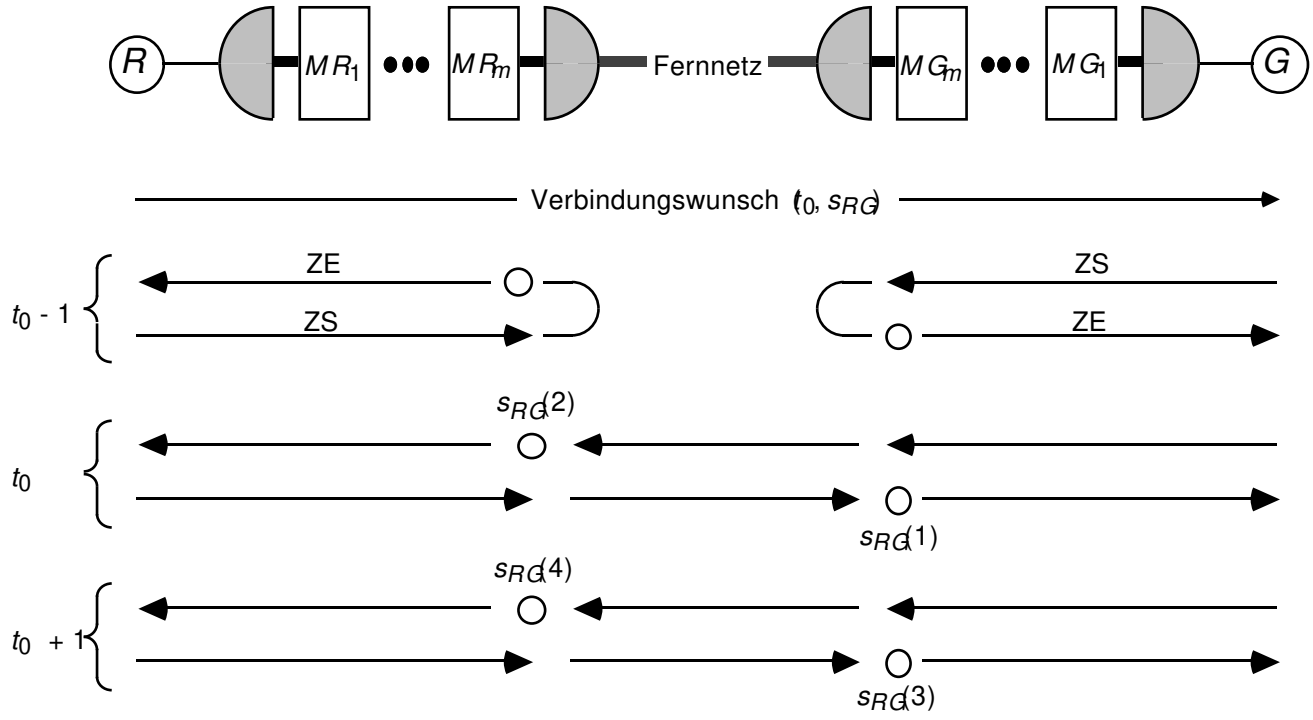


Bild 6 Verbindungsaufbau im einfachsten Fall. Das Senden der Startnachrichten, d.h. der eigentliche Beginn der Verbindung, wurde nicht dargestellt.

Im Gegensatz zum ISDN, wo die gesamte Signalisierung außerhalb des 64-kbit/s-Datenkanals erfolgt, erscheint es hier zur Entlastung des Signalisierungskanals sinnvoller, wie im analogen Fernsprechnetz die weitere Signalisierung für den Verbindungsaufbau im noch ungenutzten Datenkanal vorzunehmen:

Über diesen Datenkanal wird zunächst das Zustandekommen der Verbindung von G durch eine **Startnachricht** an R signalisiert, der sein noch bestehendes Interesse an der Verbindung ggf. ebenfalls mit

einer Startnachricht an *G* signalisiert. (Damit nicht durch das Auffüllen eines partnerlosen ZE-Kanals durch einen MIX zufällig eine Startnachricht entsteht, müssen diese hinreichend lang gewählt sein.)

Daran anschließend kann die Verbindung zwischen den Endgeräten hergestellt werden, d.h. für den Fernsprechdienst könnte nun das Telefon des Gerufenen anfangen zu klingeln, das Telefon des Rufenden könnte anfangen, Freizeichen von sich zu geben. Die notwendige Signalisierung für den Übergang von „Warten auf Partner" zu „Partner am Apparat" u.ä. erfolgt wiederum über den noch ungenutzten Datenkanal.

Bauen *R* und *G* ihre Zeitscheibenkanäle nicht synchron auf, z.B. weil *G* keinen ungenutzten Datenkanal zur Verfügung hat, so schadet dies der Unbeobachtbarkeit nichts, da ja ein fehlender ZS-Kanal durch wenigstens einen der MIXe aufgefüllt wird. ZS-Kanäle ohne passenden ZE-Kanal werden vom letzten MIX des beabsichtigten Empfängers ignoriert.

Damit kann der Verbindungsaufbau völlig asynchron erfolgen. Hierzu muß *G* alle eingegangenen Verbindungswünsche zumindest für eine bestimmte Zeit speichern.

Ist *G* besetzt (d.h. ist er bereits vollständig mit echten Verbindungen ausgelastet, die der Teilnehmer auch nicht abbrechen will) oder nicht empfangsbereit, so kann der rufende Teilnehmer seinen Netzabschluß *R* im Prinzip beliebig lange auf *G* warten lassen. Um aber zu vermeiden, daß *G*, nachdem *R* seinen Wunsch längst aufgegeben hat, sinnlos einen Kanal durchs Fernnetz zur OVSt von *R* aufbauen läßt, wird die maximale Wartezeit von *R* durch eine Zeitschranke beschränkt. Kann der rufende Teilnehmer diese Schranke beliebig wählen und sie in der Verbindungswunschnachricht *G* mitteilen, so entfällt damit die im Verfahren der Telefon-MIXe den Signalisierungkanal arg belastende Wahlwiederholung durch dauerndes Senden von Verbindungswunschnachrichten. Bei längeren Zeitschranken muß hierzu nicht unbedingt der Teilnehmer persönlich am Endgerät warten, sondern es ist denkbar, ihm das Zustandekommen der Verbindung zwischen den Anschlüssen wiederum durch ein Klingelzeichen anzuzeigen.

Wartet *R* trotzdem nicht, d.h. bricht den Verbindungsaufbau ab, und baut *G* später seine Kanalhälfte doch noch auf, so bleibt die Startnachricht von *R* natürlich aus und *G* bricht den Verbindungsaufbau ebenfalls ab.

Wartet *G* sehr lange, bevor er den Verbindungswunsch von *R* befriedigt, so muß er, um die aktuellen Kennzeichen erzeugen zu können, zuerst alle vorangegangenen erzeugen. Statt der linearen Anordnung der Kennzeichen kann man diese aber auch baumförmig so anordnen (die genaue Konstruktion ist in [GoGM_86] beschrieben), daß sich jedes Kennzeichen $s_{RG}(x)$ statt in $|x|$ Schritten in $\log(|x|)$ Schritten erzeugen läßt [GoGM_86]. Steht ausreichend Speicherplatz zur Verfügung, um jeweils einen Zweig des Baumes vollständig abzuspeichern, so sind zur sequentiellen Erzeugung im Mittel weniger als zwei Schritte erforderlich, d.h. im Normalfall verdoppelt sich der Aufwand.

Wartet einer der beiden Anschlüsse auf den anderen und sind sie nicht beide an dieselbe OVSt angeschlossen, so würde im obigen Schema das Fernnetz durch noch ungenutzte Datenkanäle unnötig belastet. Dies kann mit einer geringen Einbuße an Unbeobachtbarkeit vermieden werden, wenn man den jeweils letzten MIXen bzw. den OVSt'n ermöglicht, die Zusammengehörigkeit aller Zeitscheibenkanäle einer Verbindung innerhalb des Fernnetzes zu erkennen.

Hierzu verwenden *R* und *G* für alle ZE- und ZS-Kanäle ihrer Verbindung im Falle eines Ferngesprächs ein *gemeinsames* Kennzeichen.

Der (nicht sehr große) Nachteil ist, daß dadurch die genaue Dauer der einzelnen Ferngespräche erkennbar wird. Bestehen zwischen zwei bestimmten OVSt'n innerhalb eines längeren Zeitraums nur wenige Verbindungen, so ist dies aber auch im bisher beschriebenen Verfahren der Fall: ein Angreifer kann mit hoher Wahrscheinlichkeit annehmen, daß alle unmittelbar aufeinanderfolgenden Zeitscheibenkanäle zwischen diesen beiden OVSt'n genau einer Verbindung entsprechen.

Der Vorteil ist dafür, daß in diesem Fall der letzte MIX in der Kaskade des Senders bzw. die OVSt bedeutungslose Daten im Fernnetz unterdrücken können. Dazu werden die Startnachrichten von *R* und *G*

jeweils für MR_m bzw. MG_m erkennbar übermittelt. Erst bei Eintreffen der Startnachricht von G läßt MG_m den Kanal im Fernnetz aufbauen. Die ZE-Kanäle werden bis zum Eintreffen des richtigen ZS-Kanals wie üblich von MR_m bzw. MG_m mit bedeutungslosen Daten aufgefüllt.

Wird die Verbindung nicht sofort zur Übermittlung von Daten genutzt, etwa weil es im Fernsprechdienst nach dem Verbindungsaufbau zwischen den Endgeräten erst einige Zeit beim Gerufenen klingeln muß, bevor er den Hörer abnimmt, so können auch hier bedeutungslose Daten unterdrückt werden. Hierzu muß das Signal für „Verbindung zum *Teilnehmer* bereit“ den letzten MIXen MG_m bzw. MR_m wie schon die Startnachrichten über den Datenkanal im Klartext übermittelt werden.

Verbindungswunschnachrichten müssen im Ortsnetz des Empfängers *verteilt* werden. Damit ist es aber möglich, daß durch einen koordinierten Angriff vieler Teilnehmer ein bestimmtes Ortsnetz durch Verbindungswünsche überflutet wird, so daß die Verbindungswünsche anderer Teilnehmer nicht mehr verteilt werden können (*denial of service attack*). Dieser Angriff ist analog in jedem mehrstufigen Netz, also auch im ISDN, möglich. Da der Angreifer nichts Unzulässiges tut, kann der Angriff auch nicht verhindert, sondern höchstens erkannt oder in seiner Wirkung begrenzt werden.

Letzteres kann erreicht werden, indem man die Verbindungswunschnachrichten mit Prioritäten versieht, und jedem Teilnehmer lediglich eine begrenzte Anzahl von Verbindungswünschen höherer Prioritäten erlaubt. Die Verteilung der Verbindungswünsche erfolgt sortiert nach ihrer Priorität. Die Zuordnung von Prioritäten zu Verbindungswünschen erfolgt adaptiv durch den Netzabschluß: Jeder Verbindungswunsch erhält zunächst die geringste Priorität. Wird der Verbindungswunsch nicht beantwortet und nach einer gewissen Zeit wiederholt, so erhält er die nächsthöhere noch verfügbare Priorität.

Die Einhaltung der zulässigen Anzahl von Verbindungswünschen höherer Priorität je Teilnehmer wird von den OVSt'n anhand nur einmal gültiger „Berechtigungsmarken“ kontrolliert. Eine solche Berechtigungsmarke ist eine von der OVSt digital unterschriebene Nachricht, die die Priorität angibt. Jeder Teilnehmer erhält für jede höhere Priorität nur eine begrenzte Anzahl von Berechtigungsmarken je Zeiteinheit (z.B. Woche). Sie können in Zeiten geringer Netzauslastung durch die OVSt verschickt werden. Enthält ein Verbindungswunsch keine Berechtigungsmarke, so wird ihr die geringste Priorität zugeordnet.

Nun könnte allerdings die OVSt durch Vergleich der erhaltenen mit den ausgegebenen Berechtigungsmarken die Sender der Verbindungswünsche identifizieren. Um dies zu vermeiden, werden zur Unterzeichnung der Berechtigungsmarken **blind geleistete Unterschriften** [Cha8_85, Chau_89] verwendet. Diese erlauben es den Teilnehmern, jede von der OVSt unterschriebene Berechtigungsmarke genau einmal so umzuformen, daß sie nach wie vor von der OVSt unterschrieben ist, aber von dieser nicht mehr wiedererkannt werden kann.

Damit enthält eine Verbindungswunschnachricht für MR_i im Feld D_i

- einen aktuellen Zeitstempel (d.h. die Nummer der aktuellen Zeitscheibe)

und für MR_m zusätzlich

- den Hinweis, ob die Verbindungswunschnachricht bedeutungslos ist und ignoriert werden kann,
- das Ortsnetzkennzeichen des Empfängers,
- eine Berechtigungsmarke.

Die Bestandteile einer Verbindungswunschnachricht sind in Bild 7 zusammengefaßt.

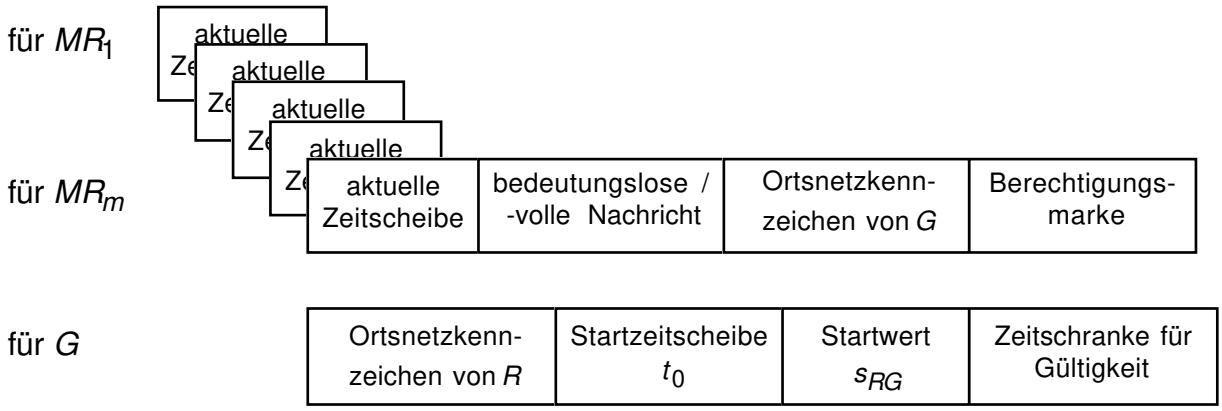


Bild 7 Verbindungswunschnachricht von R an G.

4.4 Abbau einer unbeobachtbaren Verbindung

Die Verbindung kann von jedem der beiden Partner geordnet abgebaut werden. Der Abbau erfolgt, indem die Partner ab einer bestimmten Zeitscheibe ihre ZS- und ZE-Kanäle nicht mehr miteinander verbinden, sondern wieder „kurzschließen“ oder für eine neue Verbindung nutzen.

Bei strikter Beibehaltung der Transparenz gibt es im wesentlichen zwei Möglichkeiten, wie einem Partner ermöglicht werden kann, dem anderen den Verbindungsabbauwunsch zu signalisieren.

Zum einen kann der abbauende Netzabschluß eine eigenständige Verbindungsabbaunachricht über den Signalisierungskanal an seinen Partner senden. Da der Signalisierungskanal aber ohnehin schon sehr belastet ist, scheint diese „natürliche“ Lösung nicht sehr sinnvoll.

Zum anderen kann man aber auch einen Teil des Signalisierungskanals, genauer 1 bit je Zeitscheibe, fest dem Datenkanal zuordnen, d.h. dieser 1-bit/z-Kanal würde zusammen mit dem Datenkanal über ZS- und ZE-Kanäle übermittelt. Der Verbindungsabbau könnte z.B. durch Übermittlung einer '1' auf diesem Kanal signalisiert werden.

4.5 Abrechnung der Netzbenutzung

Die bereits in [PfPW_88] genannten Möglichkeiten zur Abrechnung der Netz- und Dienstbenutzung ohne Identifikation der Teilnehmer sind natürlich auch hier anwendbar.

Für Gespräche innerhalb eines Ortsnetzes erscheint eine Abrechnung von Einzelgesprächen technisch sinnlos, da sie im Netz keinen zusätzlichen Aufwand verursachen. Zudem sind solche Gespräche völlig unbeobachtbar.

Soll dennoch eine benutzungsabhängige Abrechnung erfolgen, so kann diese unter Beibehaltung der völligen Unbeobachtbarkeit von Ortsgesprächen durch lokale Gebührenzähler bei den Teilnehmeranschlüssen selbst vorgenommen werden (die natürlich nur in fest vorgegebenen Intervallen, z.B. monatlich, vom Betreiber ausgelesen werden dürfen und können).

Wird die Unbeobachtbarkeit von Ortsgesprächen eingeschränkt, so können aber auch dieselben Abrechnungstechniken wie für das Fernnetz verwendet werden.

Zur Abrechnung von Verbindungen, die das Fernnetz benutzen (und erst damit echten Mehraufwand verursachen), können den entsprechenden Kanalaufbaunachrichten in den Daten für den jeweils letzten MIX Gebührenmarken (von derselben Art wie die Berechtigungsmarken in § 4.3) beigelegt werden. Kann eine OVSt den Zusammenhang aller Zeitscheibenkanäle eines Ferngesprächs erkennen (vgl. § 4.3), so ist es wie bisher möglich, daß erst bei Abnahme beider Hörer bezahlt werden muß, und es genügt, wenn z.B.

in den ZS-Kanalaufbaunachrichten bezahlt wird. Auch muß in diesem Fall nicht jede Zeitscheibe einzeln bezahlt werden.

In Bild 5 wurden die zur Abrechnung notwendigen Daten willkürlich den ZS-Kanalaufbaunachrichten zugeordnet. Für ZS-Kanäle, die nicht über das Fernnetz übermittelt werden müssen, ist das Feld für die Gebührenmarke leer, aber natürlich vorhanden.

Die Gebührenmarken können mit Hilfe eines die Unbeobachtbarkeit wahrenden digitalen Zahlungssystems [PWP_87, BüPf_87] jederzeit von den Teilnehmern bei deren OVSt eingekauft werden. Der notwendige Nachrichtenaustausch geschieht dabei über eine normale unbeobachtbare Verbindung.

Geht man davon aus, daß für eine Verbindung über das Fernnetz für alle Zeitscheibenkanäle ein gemeinsames Kennzeichen verwendet wird, so kann wahlweise der Rufende oder der Gerufene bezahlen: Wer die Verbindung bezahlen wird, kann in der Verbindungswunschnachricht vom Rufenden für den Gerufenen und MR_m angegeben werden. MR_m teilt MG_m mit, wer bezahlen soll. Nach Austausch der Startnachrichten, die das Zustandekommen der Verbindung zwischen den Endgeräten signalisiert, akzeptiert der letzte MIX des Zahlenden nur noch ZS-Kanalaufbaunachrichten mit gültiger Gebührenmarke und baut bei Fehlen der Marken die Verbindung ab.

Statt der jeweils letzten MIXe können natürlich auch die OVSt'n von *R* und *G* diese Abrechnung übernehmen, wenn sie von den MIXen die jeweils notwendigen Daten (Verbindungskennzeichen, Angabe wer bezahlt, Gebührenmarke) erhalten.

4.6 Verbindungen zwischen OVSt mit MIX-Kaskade und herkömmlicher OVSt

Für Verbindungen zwischen OVSt'n mit MIX-Kaskade und herkömmlichen OVSt'n muß der letzte MIX in der MIX-Kaskade der erweiterten OVSt die Rolle eines Umsetzers spielen.

Verfügt nur die OVSt von *R* über eine MIX-Kaskade, so teilt *R* dem MIX MR_m in einer speziellen Verbindungswunschnachricht die Rufnummer von *G* und all die Daten mit, die im normalen Schema *G* erhielte, d.h. den für die Verbindung verwendeten Startwert s_{RG} und die Nummer der ersten Zeitscheibe. MR_m baut über seine OVSt und das Fernnetz eine herkömmliche Verbindung zu *G* auf und verknüpft diese mit den Zeitscheibenkanälen von *R*.

Der rufende Teilnehmer ist nun ebenso unbeobachtbar wie im Fall, daß auch bei *G* eine MIX-Kaskade ist. Der gerufene Teilnehmer ist so beobachtbar wie heute und im ISDN.

Verfügt nur die OVSt von *G* über eine MIX-Kaskade, so stellt sich in erster Linie die Frage der geeigneten Adressierung.

Verwendet der rufende Teilnehmer eine Rufnummer im heutigen Sinne, so ist die Unbeobachtbarkeit des gerufenen Teilnehmers damit zwangsläufig verloren. Daher sollte man auch für solche Verbindungen implizite Adressen vorsehen.

Im folgenden wird sich herausstellen, daß eine Anonymitätsgruppe aus jeweils ungefähr 5000 Teilnehmern bestehen kann. Nimmt man an, daß jeder Teilnehmer ungefähr 50 verschiedene offene implizite Adressen verwendet (vgl. § 2.2.3), und daß, um Kollisionen zu verhindern, die Menge der möglichen Adressen ungefähr quadratisch in der Anzahl der benötigten sein soll, so kommt man auf einen Adreßraum von $6{,}25 \cdot 10^{10}$, d.h. eine offene implizite Adresse käme mit 11 Dezimalziffern aus. Hinzu kommt allerdings noch die Auswahl der Anonymitätsgruppe von *G*. Nimmt man an, daß das größte Ortsnetz sicher weniger als 50 000 000 Anschlüsse hat und jede Anonymitätsgruppe 5000 Teilnehmer, so kommt man mit 4 Dezimalziffern aus.

Damit liegt für solche Verbindungen folgendes Schema nahe: *R* wählt zunächst wie heute die Vorwahl des Ortsnetzes von *G* und stellt damit eine herkömmliche Verbindung zu MG_m her. Durch 15 weitere Dezimalziffern teilt er MG_m die implizite Adresse von *G* mit. MG_m spielt Stellvertreter und sendet *G* eine entsprechende Verbindungswunschnachricht. Nimmt *G* die Verbindung an, so verknüpft MG_m wie oben

die herkömmliche und die datenschützende Verbindungshälfte. Nimmt *G* die Verbindung nicht an, so kann MG_m zur Vermeidung von Wahlwiederholungen an *R* das Angebot zurücksenden, den Verbindungswunsch aufrecht zu erhalten und ihn bei Annahme des Wunsches durch *G* zurückzurufen.

Eine verdeckte implizite Adresse wird hingegen aus mindestens 200 Dezimalziffern bestehen und setzt zudem beim Rufenden gewisse kryptographische Fähigkeiten voraus: Der Rufende benötigt einen Rechner zur Speicherung von Schlüsseln und Berechnung von Adressen, und muß in der Lage sein, Daten von diesem Rechner an MG_m übermitteln zu können, sei es über das ISDN oder über das herkömmliche Fernsprechnetz mittels Modem oder Akustikkoppler. Die Übermittlung erfolgt innerhalb der Verbindung zwischen *R* und MG_m, d.h. nicht im Signalisierungskanal.

Es sei angemerkt, daß an einer OVSt, die eine MIX-Kaskade hat, auch herkömmliche Teilnehmeranschlüsse beibehalten werden können.

4.7 Zuverlässigkeit

Offensichtlich stellen die MIXe einer Kaskade hinsichtlich der Zuverlässigkeit ein *Seriensystem* dar. Hier würde es aber wohl genügen, jeden MIX intern fehlertolerant auszulegen. Falls trotzdem ein MIX ausfallen sollte, können die an diese OVSt angeschlossenen Netzabschlüsse in allen Nachrichten diesen MIX auslassen.

Es gibt auch sich über mehrere MIXe erstreckende Fehlertoleranzverfahren, vgl. [Pfi1_85 § 3.1, MaPf_87, Pfit_89 § 5.3]. Diese erhöhen aber den Aufwand, und das Problem der anonymen Rückadressen, das diese Verfahren vor allem nötig macht, tritt im hier beschriebenen Verfahren nicht auf.

Hinsichtlich der Sicherung vor Übertragungsfehlern ändert sich gegenüber dem ISDN nichts. Auch hier wird nur eine streng synchrone, aber ansonsten ungesicherte Übertragung angenommen.

Durch Verwendung einer synchronen Stromchiffre (Pseudo-Vernamchiffre) wird eine *zusätzliche* Ausbreitung von Bitverfälschungen auf den 64-kbit/s-Kanälen verhindert. Auf dem Signalisierungskanal wird die Verwendung entsprechender Protokolle, z.B. HDLC, zur Sicherung der Übertragung angenommen.

5 Aufwand

Im folgenden soll anhand einer sehr einfachen Leistungsabschätzung die Praktikabilität der in den vorhergehenden Abschnitten beschriebenen Telefon-MIXe demonstriert werden.

Es wird sich zeigen, daß bei Beschränkung auf $2 \cdot 64 + 16$ kbit/s Duplexkanäle für $m = 10$ MIXe ungefähr 5000 Netzabschlüsse an eine MIX-Kaskade angeschlossen werden können.

Als Hauptengpässe werden sich herausstellen

- die Übertragung der ZS- und ZE-Kanalaufbaunachrichten, Verbindungswunschnachrichten und Rückmeldungen von den Netzabschlüssen an die OVSt sowie
- die Verteilung der Verbindungswunschnachrichten an die Netzabschlüsse.

Beides muß über den 16-kbit/s-Signalisierungskanal erfolgen. Da ein Teil seiner Bandbreite für die Datensicherung verwendet werden muß und möglicherweise auch einige schmalbandigere Dienste über den Signalisierungskanal abgewickelt werden, soll im folgenden lediglich mit einer verfügbaren Bandbreite zur Signalisierung von $b = 12$ kbit/s in beiden Richtungen gerechnet werden.

Die Vorbereitung und Verarbeitung der Nachrichten durch die Netzabschlüsse, das Mixen und die eigentlichen Datenkanäle stellen demgegenüber ein geringeres Problem dar.

In § 5.1 werden zunächst einige Parameter zur Beschreibung der benötigten Kryptosysteme eingeführt und typische Werte angegeben. In § 5.2 wird die Dauer *z* einer Zeitscheibe abgeschätzt, und in § 5.3 die Anzahl

n der Netzabschlüsse, die an eine MIX-Kaskade angeschlossen werden können. In § 5.4 wird die Komplexität der von den Netzabschlüssen und MIXen je Zeitscheibe durchzuführenden Aufgaben betrachtet, und in § 5.5 schließlich die Verbindungsaufbauzeit abgeschätzt.

5.1 Parameter zur Beschreibung der benötigten Kryptosysteme

Die im folgenden verwendeten Parameter orientieren sich an den jeweils bekanntesten Vertretern der symmetrischen bzw. asymmetrischen Kryptosysteme, nämlich DES und RSA.

Wiederholt (vgl. § 2.2.2) und bekräftigt sei an dieser Stelle, daß die Sicherheit dieser Kryptosysteme und damit auch die jeder darauf basierenden MIX-Implementierung bislang noch nicht einmal relativ zu einem als schwer erachteten Problem, z.B. der Faktorisierung, *bewiesen* wurde.

Dieser Nachteil wird hier nur deshalb ignoriert, weil einerseits dasselbe auf alle praktikablen Kryptosysteme zutrifft, andererseits DES und RSA zumindest als praktisch gut untersucht und im öffentlichen Bereich als ungebrochen gelten.

Die Parameter und ihre angenommenen Werte sind in Bild 8 zusammengefaßt.

Parameter	symmetrische Stromchiffre	asymmetrische Blockchiffre
Schlüssellänge	$s_{sym} = 128$ bit	irrelevant
Blocklänge	$b_{sym} = \infty$	$b_{asym} = 660$ bit
Länge der Verschlüsselung von N	$\|N\|$	b_{asym} (falls $\|N\| \leq b_{asym}$)

Bild 8 Parameter der verwendeten Kryptosysteme.

5.1.1 Symmetrisches Kryptosystem

Für das Kryptosystem DES [Denn_82 § 2.6.2, Bras_88 § 3.4] wird in [Bras_88 § 3.4] für gute Hardwareimplementierungen eine Ver- und Entschlüsselungsgeschwindigkeit von 20 Mbit/s angegeben.

An der im mathematischen Sinne bislang unbewerteten kryptographischen Sicherheit von DES wurde seit seiner Veröffentlichung immer wieder Kritik geübt. Vereinfachte Varianten von DES wurden sogar schon effizient gebrochen. Jüngstes Beispiel ist ein nur auf Schlüsseltext basierender Angriff von ADI SHAMIR gegen DES mit 8 Runden [Dier_89]. Das angewandte Verfahren ist öffentlich nicht bekannt, so daß seine Anwendbarkeit auf DES mit wie üblich 16 Runden nicht beurteilt werden kann.

Durch Verwendung anderer Schlüsselexpansionsalgorithmen lassen sich aber leicht Varianten von DES mit vergrößertem Schlüsselraum angeben [Aßma_89, Ber1_83], die hoffentlich sicherer sind als DES selbst und für die ähnliche Geschwindigkeitswerte erreicht werden [BeFG_89].

Im folgenden wird daher von 128 bit Schlüssellänge statt 56 bit ausgegangen.

Für das hier vorgestellte Verfahren benötigt man eine synchrone Stromchiffre, d.h. das symmetrische Kryptosystem wird im OFB-Modus betrieben. Es entsteht keine Expansion durch Auffüllen von Blöcken oder ähnlichem.

5.1.2 Asymmetrisches Kryptosystem

Für das Kryptosystem RSA [RSA_78, Denn_82 § 2.7.2, Bras_88 § 4.4] wird in [Sedl_88] eine Hardwareimplementierung mit einer Ver- und Entschlüsselungsgeschwindigkeit von ca. 200 kbit/s bei einer

Moduluslänge von 660 bit angegeben. Letzteres erscheint für die Sicherheit von RSA zur Zeit als ausreichend.

Die Moduluslänge von RSA ist zugleich auch die Blocklänge. RSA verschlüsselt deterministisch, Klartextraum und Schlüsseltextraum sind identisch.

Neuere, probabilistisch verschlüsselnde asymmetrische Kryptosysteme haben die Eigenschaft, daß der Schlüsseltext stets länger ist als der Klartext.

Da RSA nicht zu dieser Klasse gehört, wird diese Längenexpansion im folgenden nicht berücksichtigt, was aber bei Bedarf leicht nachgeholt werden kann.

5.1.3 Hybride Verschlüsselung

Um Übertragungskapazität zu sparen, wird bei der hybriden Verschlüsselung stets ein möglichst großer Teil N' des Klartextes N in den ersten, asymmetrisch verschlüsselten, Block hineingezogen, d.h. es ist, wenn N'' der Rest von N ist,

$$c_E{}^*(N) := \begin{cases} c_E(N) & \text{falls } |N| \le b_{asym} \\ c_E(k_{SE},N'),\ k_{SE}(N'') & \text{sonst.} \end{cases} \qquad (2)$$

Zur Bestimmung der Länge von $c_E{}^*(N)$ ist zu beachten, daß zur Gewährleistung der Unbeobachtbarkeit die in § 2.2.2 (1) verwendete Verschlüsselung *indeterministisch* sein muß.

Bei Verwendung von RSA muß daher dessen Determinismus beseitigt werden, indem die Nachricht vor der Verschlüsselung indeterministisch codiert, d.h. im wesentlichen um eine Anzahl a zufällig gewählter Bits erweitert wird [Chau_81].

Die dadurch verursachte *Längenexpansion* kann sinnvoll genutzt werden, indem eben jene a zusätzlichen Bits als symmetrischer Schlüssel k_{SE} verwendet werden. Damit ist $a = s_{sym}$.

Die genaue Realisierung der „Erweiterung“ ist leider nicht trivial. So wurde gezeigt, daß speziell bei Verwendung von RSA die in [Chau_81] nahegelegte Codierung durch Voranstellen zufällig gewählter Bits ein unsicheres MIX-Netz ergibt [PfPf_89].

Ungebrochen ist jedoch folgende Erweiterung, von der im folgenden auch ausgegangen werden soll: vor der Verschlüsselung einer Nachricht wählt sich der Verschlüßler einen zufälligen, s_{sym} bit langen String und konkateniert ihn mit der Nachricht. Die so erweiterte Nachricht wird mit einer festen und möglichst wenig strukturerhaltenden Permutation π des Klartextraumes „verwürfelt“. Die Permutation π und ihre Inverse π^{-1} sind allgemein bekannt. (Sie könnten z.B. durch einen festen Schlüssel eines symmetrischen Kryptosystems beschrieben werden.) Beim Entschlüsseln wird umgekehrt verfahren, d.h. zunächst die inverse Permutation π^{-1} angewandt und dann der s_{sym} bit lange String entfernt.

Geht man von dieser Erweiterung aus, so ist

$$|c_E{}^*(N)| = \max\ \{\ b_{asym},\ |N| + s_{sym}\ \}. \qquad (3)$$

5.2 Minimale Dauer einer Zeitscheibe

Jeder Netzabschluß muß für jede Zeitscheibe und jeden ihm zur Verfügung stehenden 64-kbit/s-Datenkanal drei MIX-Eingabenachrichten (vgl. § 2.2.2 (1)) senden: eine ZS- und eine ZE-Kanalaufbaunachricht sowie eine Verbindungswunschnachricht. Deren Längen seien mit L_{ZS}, L_{ZE} bzw. L_V bezeichnet.

Die Länge einer Rückmeldung (vgl. § 2.2.3) wird mit L_R bezeichnet. Wird RSA als Signatursystem verwendet, so gilt im wesentlichen $L_R = b_{asym}$, was im folgenden auch angenommen werden soll. Da die Rückmeldungen ob ihrer kurzen Länge ohnehin kaum ins Gewicht fallen, wird angenommen, daß jeder Netzabschluß für jede Zeitscheibe eine Rückmeldung sendet.

Ein Netzabschluß muß also in der Lage sein, über seinen Signalisierungskanal in jeder Zeitscheibe $2 \bullet (L_{ZS} + L_{ZE} + L_V) + L_R$ bit zu übertragen, d.h. es muß gelten

$$z \geq \frac{2 \bullet (L_{ZS} + L_{ZE} + L_V) + L_R}{b} \quad . \tag{4}$$

Die Längen L_{ZS}, L_{ZE} und L_V sollen im folgenden abgeschätzt werden. In § 5.2.1 wird hierzu die Länge einer MIX-Eingabenachricht allgemein abgeschätzt, in § 5.2.2 werden die speziellen Werte in Gleichung (4) eingesetzt.

5.2.1 Länge einer MIX-Eingabenachricht

Gemäß § 2.2.2 (1) gilt

$$|N_1| \leq |D_1| + |N_2|$$

bzw. für $i = 2, \ldots, m$ gemäß § 5.1.3 (3)

$$|N_i| \;=\; \max \{\; b_{asym}, |D_i| + |N_{i+1}| + s_{sym} \}.$$

Da für $i < m$ die Nachricht N_{i+1} wenigstens aus einem asymmetrisch verschlüsselten Block besteht, gilt für $i < m$ stets $|N_{i+1}| \geq b_{asym}$. Damit folgt nach Auflösung der obigen rekursiven Gleichungen

$$|N_1| = \sum_{j=1}^{m-1} |D_j| + (m\text{-}2) \bullet s_{sym} + \max \{\; b_{asym}, |D_m| + |N_{m+1}| + s_{sym} \}. \tag{5}$$

Im folgenden soll stets von Gleichung (5) ausgegangen werden.

5.2.2 Abschätzung

Die Strukturen der drei interessierenden Nachrichtentypen sind in den Bildern 5 und 7 dargestellt. Den Feldern sind folgende Längen zugeordnet worden:

Bild 5,7:
- Zeitscheibennummer: 30 bit
- Ortsnetzkennzeichen: 22 bit

Bild 5:
- Gebührenmarke zur Bezahlung der Fernnetzbenutzung: 670 bit
- Kanalkennzeichen: 28 bit

Bild 7:
- Unterscheidung bedeutungslose Nachricht / bedeutungsvolle Nachricht: 1 bit
- Startwert s_{RG} des PZBFG: 128 bit
- Zeitschranke für Gültigkeit (d.h. das Warten von R auf G): 20 bit
- Berechtigungsmarke zur Angabe der Priorität eines Verbindungswunsches: 670 bit

Für die beiden Marken wurde jeweils angenommen, daß die Priorität der Berechtigungsmarke bzw. der Wert der Gebührenmarke nicht nur implizit in der Signatur (bei RSA: 660 bit) durch unterschiedliche Unterschriften, sondern auch explizit (in weiteren 10 bit) angegeben wird. Dies erspart der kontrollierenden OVSt das Durchprobieren aller möglichen Schlüssel zum Prüfen von Unterschriften.

Für eine ZS- oder ZE-Kanalaufbaunachricht gilt für $i = 1, \ldots, m\text{-}1$ jeweils $|D_i| = 30$ bit, da der Schlüssel des symmetrischen Kryptosystems bereits für die hybride Verschlüsselung gezählt wurde, und $|N_{m+1}| = 0$.

Für eine ZS-Kanalaufbaunachricht ist $|D_m| = 750$ bit, d.h. nach (5) $|N_m| = 750 \text{ bit} + s_{sym}$. Für eine ZE-Kanalaufbaunachricht ist $|D_m| = 58$ bit, d.h. nach (5) $|N_m| = b_{asym}$.

Damit folgt aus (5)

$$\begin{aligned} L_{ZS} &= (m\text{-}1) \bullet (30 \text{ bit} + s_{sym}) + 750 \text{ bit} \\ L_{ZE} &= (m\text{-}1) \bullet (30 \text{ bit} + s_{sym}) - s_{sym} + b_{asym}. \end{aligned} \tag{6}$$

Für eine Verbindungswunschnachricht gilt für $i = 1, \ldots, m\text{-}1$ jeweils $|D_i| = 30$ bit, und $|D_m| = 723$ bit. Nach (5) ist $|N_m| = 723 \text{ bit} + |N_{m+1}| + s_{sym}$. Umgekehrt reicht $|N_{m+1}| = b_{asym}$ aus, da der Empfänger lediglich 200 bit erhalten muß.

Damit ist

$$L_V = (m\text{-}1) \bullet (30 \text{ bit} + s_{sym}) + b_{asym} + 723 \text{ bit}. \tag{7}$$

Gemäß (6) und (7) ist

$$L_{ZS} + L_{ZE} + L_V = (m\text{-}1) \bullet 90 \text{ bit} + (3 \bullet m\text{-}4) \bullet s_{sym} + 2 \bullet b_{asym} + 1473 \text{ bit}. \tag{8}$$

Setzt man nun die angenommenen Werte für s_{sym}, b_{asym} (vgl. Bild 8) und $b = 12$ kbit/s in (4) ein, so erhält man

$$z \geq \frac{474 \text{ bit} \bullet m + 2191 \text{ bit}}{6000 \text{ bit/s}} + \frac{660 \text{ bit}}{12000 \text{ bit/s}} = 0{,}079 \text{ s} \bullet m + 0{,}4201\overline{6} \text{ s}, \tag{9}$$

wozu für $m = 10$ ein Wert $z \geq 1{,}22$ s hinreichend ist.

5.3 Maximale Anzahl der von einer MIX-Kaskade bedienbaren Netzabschlüsse

Die Anzahl n der von einer MIX-Kaskade bedienbaren Netzabschlüsse wird im wesentlichen durch die Verteilung der Verbindungswunschnachrichten begrenzt: jedem Netzabschluß steht anteilig lediglich ein Empfangskanal von b/n zur Verfügung.

Wie stark diese Begrenzung ist, hängt von der Verkehrsstatistik ab. Vereinfachend wird angenommen, daß das Verteilnetz ein M/D/1-System sei, wobei λ die maximale mittlere Rate sei, mit der jeder der n Teilnehmer Verbindungswünsche erhält. Als Wert wird $\lambda = 1/300$ 1/s angenommen, d.h. in Stoßzeiten im Mittel zwölf Verbindungswünsche je Teilnehmer und Stunde.

(Dieser Wert für λ ist sicher ausreichend, eher sogar zu hoch: Laut Fernsprechstatistik [Siem_87] wurden 1985 in der Bundesrepublik *im Mittel* weniger als 3,1 Gespräche je Hauptanschluß und *Tag* geführt. Vertraut man den Erwartungen von Siemens, so dürfte der Wert $\lambda = 1/300$ 1/s auch für Spitzenzeiten eher zu hoch sein: Laut [Siem_88] verarbeitet der leistungsfähigste Vermittlungsrechner von Siemens im Endausbau 4,8 Vermittlungsversuche je Teilnehmer und Stunde. Außerdem interessieren beim Verfahren der Telefon-MIXe für λ sogar nur die ankommenden Gespräche.)

Jede verteilte Verbindungswunschnachricht besteht aus genau einem asymmetrisch verschlüsselten Block (vgl. § 5.2.2) und hat daher die Länge b_{asym}, so daß maximal $\mu := b / b_{asym}$ Verbindungswunschnachrichten pro Sekunde verteilt werden können.

Ist T_v die mittlere Systemzeit, d.h. die Zeit, die ein Verbindungswunsch im Mittel benötigt, um bei den Netzabschlüssen einzutreffen, so gilt [Klei_75 § 5.5, insbesondere (5.74)] in Stoßzeiten im Mittel

$$T_v = \frac{2 \bullet \mu - n \bullet \lambda}{2 \bullet \mu \bullet (\mu - n \bullet \lambda)}. \tag{10}$$

Hieraus ergibt sich

$$n = \frac{\mu}{\lambda} \bullet \frac{\mu \bullet T_v - 1}{\mu \bullet T_v - 0{,}5}. \tag{11}$$

Für $\lambda = 1/300$ 1/s, $T_v \leq 0{,}5$ s, $b = 12$ kbit/s und $b_{asym} = 660$ bit ergibt dies $n \leq 5137$.

Speziell für Verbindungswunschnachrichten würde sich die Verwendung der in § 2.2.3 erklärten offenen impliziten Adressierung lohnen: da der gerufene Netzabschluß G den rufenden Netzabschluß R bereits anhand der offenen Adresse a_{RG} wiedererkennt, muß der Verbindungswunsch lediglich die Nummer der gewünschten Startzeitscheibe angeben. Alle anderen Angaben kann G „wiederverwenden“. Verwendet der rufende Teilnehmer nicht seinen eigenen Netzabschluß R, sondern ruft von einem anderen Ortsnetz aus an, so kann die Verbindung über R zu dem aktuell verwendeten Netzabschluß umgeleitet werden. Ist eine Adresse 100 bit lang, so ist ein Verbindungswunsch damit maximal 130 bit lang. Werden nur solche

Adressen verwendet, so ergibt sich mit $\mu = b$ / 130 bit gemäß (11) und obigen Werten eine Schranke von $n \leq 27389$.

Die M/D/1-Annahme ist, wie erwähnt, natürlich etwas vereinfachend. Allerdings schadet dies hier fast nichts: Die Ankünfte sind näherungsweise „gedächtnislos“, da eine Wahlwiederholung durch Wiederholen der Verbindungswunschnachricht nicht notwendig ist. Die Bedienzeit ist tatsächlich deterministisch, bis auf seltene, aufgrund von Fehlern notwendige Wiederholungen. Die verfügbare Bandbreite braucht natürlich nicht statisch nach oben beschränkt zu werden. Zudem hat bei der hier gemachten Annahme von $T_v \gg 1/\mu$ die Wartezeit ohnehin nur einen recht geringen Einfluß auf n, d.h. (11) ist im wesentlichen die triviale Forderung $n \bullet \lambda \leq \mu$.

5.4 Berechnungsaufwand der Netzabschlüsse und MIXe

Der Berechnungsaufwand der Netzabschlüsse und MIXe besteht zu einem großen Teil aus dem Anwenden kryptographischer Operationen: Vorbereiten und Erkennen von impliziten Adressen, Vorbereiten und Verarbeiten von MIX-Eingabenachrichten, Signieren und Testen von Rückmeldungen, Ver- und Entschlüsseln von Datenkanälen.

Da aber die Verschlüsselungsraten beider Kryptosysteme erheblich höher sind als die Übertragungsraten, stellen diese Operationen kein Problem dar.

Der sonstige Aufwand der Netzabschlüsse, z.B. zur Verwaltung von Schlüsseln, impliziten Adressen usw., ist zu vernachlässigen.

Der sonstige Aufwand der MIXe besteht im wesentlichen aus dem Puffern und Umsortieren von Nachrichten sowie dem Testen von Zeitstempeln. Dies betrifft je Zeitscheibe 6 Eingabeschübe mit je n Nachrichten, also mit den Schranken aus § 5.3 weniger als 27389 Nachrichten. Dies sollte, zumindest mit spezieller Hardware, in 0,01 s pro MIX möglich sein. Man kann, um hier noch etwas Zeit zu sparen, auch die Verbindungswunschnachrichten so gestalten, daß sie zunächst einen Sendekanal zu MR_m bzw. der OVSt schalten, über den dann erst die zusätzlichen Daten für MR_m und G übermittelt werden. Dadurch kann der Teilnehmer die Entscheidung, ob und mit wem er eine echte Verbindung wünscht, etwas später treffen.

Generell ist zu beachten, daß die Nachrichten der verschiedenen Zeitscheiben von den MIXen pipelineartig verarbeitet werden können, also insbesondere die Zeitscheiben bei den verschiedenen MIXen zu verschiedenen Zeitpunkten beginnen können.

5.5 Verbindungsaufbauzeit

Die Verbindungsaufbauzeit setzt sich im wesentlichen zusammen aus

- dem Warten auf die Übermittlung des Verbindungswunsches durch die MIX-Kaskade des rufenden Netzabschlusses ($\leq z$),
- der Verzögerungszeit der MIX-Kaskade des rufenden Netzabschlusses ($m \bullet 0{,}01$ s),
- der Laufzeit im Fernnetz ($\leq 0{,}2$ s),
- dem Warten auf die Verteilung an den Empfänger (in Spitzenzeiten im Mittel T_v),
- dem Warten auf das Aufbauen des ZS-Kanals durch den gerufenen Netzabschluß ($\leq z$, sofern der gerufene Netzabschluß sofort antwortet), und schließlich
- der Verzögerungszeit der MIX-Kaskade des gerufenen Netzabschlusses ($m \bullet 0{,}01$ s).

Dies ergibt zusammen eine Zeit von $2 \bullet (z + m \bullet 0{,}01 \text{ s}) + T_v + 0{,}2$ s, bei den obigen Werten also ungefähr 3,34 s. Im Mittel wird die Zeit etwa halb so groß sein.

6 Zusammenfassender Ausblick

In den vorangehenden Abschnitten wurde das Konzept eines Datenschutz garantierenden Digitalnetzes unter der Randbedingung eines schmalbandigen Teilnehmeranschlusses entwickelt.

Hauptziel hierbei war, eine praktikable Alternative zum den Datenschutz seiner Teilnehmer nur unzureichend ermöglichenden ISDN aufzuzeigen.

Um mit den ISDN-Normen und bereits vorhandenen ISDN-Orts- und Fernnetzen kompatibel zu sein, wird die Digitalisierung der Übertragung auf den vorhandenen Teilnehmeranschlußleitungen und der Ausbau des Fernnetzes wie für das ISDN geplant bzw. bereits realisiert angenommen. Die Ortsvermittlungsstellen nebst angeschlossenen Netzabschlüssen können also schrittweise modernisiert und erweitert werden.

Auch die Aufteilung des Basisanschlusses in zwei unabhängige 64-kbit/s-Vollduplexkanäle für die Nutzdatenübertragung und einen 16-kbit/s-Signalisierungskanal wird übernommen. Im Gegensatz zum ISDN wird jedoch ein Teil der Signalisierung zur Herstellung der 64-kbit/s-Verbindung wie im heutigen Fernsprechnetz innerhalb der Verbindungen selbst vorgenommen, allerdings ohne die Transparenz einzuschränken.

Als bereitzustellender Dienst wurde lediglich die Schaffung von 64-kbit/s-Duplexverbindungen zwischen Netzabschlüssen mit Aufbauzeiten im Bereich von 3 s betrachtet.

Schmalstbandige, ebenfalls den 16-kbit/s-Signalisierungskanal nutzende Dienste wurden nur am Rande betrachtet. Deren Nachrichten könnten unbeobachtbar mit dem in § 2.2 beschriebenen Grundschema über den Signalisierungkanal übertragen werden, würden aber natürlich den für Signalisierung verfügbaren Anteil des Signalisierungskanals beschränken und damit zugleich die Aufbauzeit verlängern und die mögliche Anonymitätsgruppengröße verkleinern.

Der Schutz des Nachrichteninhalts wird wie üblich durch Ende-zu-Ende-Verschlüsselung, der Schutz der Teilnehmer vor Beobachtung ihres Kommunikationsverhaltens (wer kommuniziert wann, wieviel, mit welchem Dienst, mit wem?) durch eine Variante des MIX-Netzes [Chau_81], die Telefon-MIXe, realisiert.

Die Teilnehmer sind jeweils innerhalb einer Anonymitätsgruppe von ungefähr 5000 Teilnehmern unbeobachtbar, d.h. ein Angreifer kann Quelle und Senke eines Informationsstroms jeweils nur auf die Anonymitätsgruppe genau feststellen. Das Bestehen einer Verbindung zwischen verschiedenen Anonymitätsgruppen ist jedoch beobachtbar, Verbindungen innerhalb einer Anonymitätsgruppe sind völlig unbeobachtbar. Die Begrenzung der Größe der Anonymitätsgruppen rührt im wesentlichen von der Bandbreitenbeschränkung des Signalisierungskanals auf 16 kbit/s her.

Die Zuordnung der Teilnehmer zu Anonymitätsgruppen ist eindeutig und im wesentlichen bereits durch die Einteilung in Ortsnetze festgelegt, d.h. jeder OVSt entspricht eine oder mehrere solcher Anonymitäts-gruppen.

Jedes „neue“ Ortsvermittlungssystem besteht aus mehreren Teilen, nämlich den m sogenannten MIXen, $m \approx 10$, und der für die Kommunikation mit den Netzabschlüssen und die Verbindung zum Fernnetz zuständigen eigentlichen OVSt.

Diese Aufteilung muß sehr strikt verstanden werden: zur Gewährleistung der Unbeobachtbarkeit muß angenommen werden, daß in jedem Ortsnetz wenigstens einer der m MIXe korrekt arbeitet, d.h. die Beobachtung der Teilnehmer des Ortsnetzes verhindert. Aus diesem Grunde müssen die m MIXe eines Ortsvermittlungssystems räumlich voneinander und von der eigentlichen OVSt getrennt arbeiten, voneinander unabhängige Betreiber haben und zur Tolerierung Trojanischer Pferde auch von unterschiedlichen Entwerfern und Herstellern produziert worden sein. Als unabhängige MIX-Betreiber können z.B. mehrere voneinander unabhängige öffentlich-rechtliche Anstalten agieren, über deren Integrität

und Nichtzusammenarbeit ein öffentliches Gremium zu wachen hat. Diese MIX-Anstalten tragen natürlich auch einen Teil der Verantwortung für die Dienstqualität innerhalb eines Ortsnetzes.

Die organisatorische Schaffung solch öffentlich-rechtlicher MIX-Anstalten und der Entwurf und die Herstellung solch (m+1)-gliedriger Ortsvermittlungssysteme wurde in dieser Arbeit nicht betrachtet, stellt aber sicher die verbleibende Hauptaufgabe dar.

Im theoretischen Sinne kann der Schutz durch das hier vorgestellte Verfahren nicht perfekt sein:

Es werden kryptographische Techniken verwendet, die nur einem in seinen Berechnungsfähigkeiten *beschränkten* Angreifer standhalten (vgl. insbesondere die Diskussion am Ende von § 2.2.2), und der Angreifer darf höchstens m-1 MIXe je Ortsvermittlungssystem kontrollieren.

Zudem muß angenommen werden, daß innerhalb einer Anonymitätsgruppe eine hinreichend große Zahl von Netzabschlüssen nicht vom Angreifer kontrolliert wird, um überhaupt von Unbeobachtbarkeit im intuitiven Sinne sprechen zu können. Um auszuschließen, daß durch einen Hersteller in allen Endgeräten ein Trojanisches Pferd untergebracht ist, sollte auch hier den Teilnehmern die Auswahl unter vielen, unabhängig voneinander entworfenen und hergestellten Geräten möglich sein.

Zudem sind einige aktive Angriffe auf die Unbeobachtbarkeit nicht ausgeschlossen (vgl. § 2.2.4.2). Ihre Behandlung würde jedem Teilnehmer jederzeit erlauben, alle anderen Teilnehmer seiner Anonymitätsgruppe am Kommunizieren zu hindern, und erscheint daher nicht praktikabel.

Für praktische Zwecke erscheint der Schutz aber durchaus zufriedenstellend.

Eine Abrechnung der Netzbenutzung scheint nur für Verbindungen zwischen verschiedenen Ortsnetzen sinnvoll und ist auch leicht möglich (vgl. § 4.5).

Die bereits in [PfPW_88, Pfit_89 § 8] gemachten Bemerkungen zur Verwendung eines Datenschutz garantierenden Netzes für „höhere“ Dienste gelten natürlich auch hier.

Eine nachträgliche Identifikation auf höheren Ebenen ist, wo gewünscht, durch Anwendung kryptographischer Techniken stets möglich, für viele, auch rechtssicherheitskritische, Dienste aber gar nicht notwendig [PWP_87]. (Beispielsweise ist der Zweck der geplanten Möglichkeit, daß der Gerufene sich die Rufnummer des Anrufenden zeigen lassen kann, viel besser mit digitalen Signaturen auf einer höheren Ebene zu erreichen: Einerseits ist eine digitale Signatur viel aussagekräftiger als eine Rufnummer, z.B. bei vorher Unbekannten oder einem Anruf aus einer Telefonzelle; andererseits sollte diese Möglichkeit, zumindest bei Anrufen bei Informationsanbietern u.ä., die Ausnahme, nicht die Regel sein und ihre Nutzung durch den Anrufenden explizit ermöglicht werden müssen.)

Zum Schluß sei angemerkt, daß bei Aufgabe der Bandbreitenbegrenzung im Teilnehmeranschlußbereich andere und in mancherlei Hinsicht bessere Konzepte für Datenschutz garantierende Digitalnetze bekannt sind, insbesondere auch solche, die keine Aufteilung der Vermittlungssysteme in mehrere unabhängige Teile erfordern [PfPW_88, Pfit_89].

Ein Dankeschön

Für ihre Kritik und Diskussionsbereitschaft danken wir Manfred Böttger und Prof. Dr. Winfried Görke. Der Deutschen Forschungsgemeinschaft (DFG) danken wir für ihre freundliche Unterstützung, die diese Arbeit erst möglich gemacht hat.

Literatur

Aßma_89 Ralf Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1989.

Bara_64 Paul Baran: On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations; The Rand Corporation, Santa Monica 1964; nachgedruckt in: Lance J. Hoffman (ed.): Security and Privacy in Computer Systems; Melville, Los Angeles 1973, 99-123.

BeFG_89 Wilfried Beller, Jürgen Frößl, Thomas Giesler: Spezifikation und Implementierung eines erweiterten DES-Algorithmus als VENUS-Standardzellenchip; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1989.

BeMi_89 Mihir Bellare, Silvio Micali: Non–interactive Oblivious Transfer and Applications; Crypto '89, August 20-24 1989, Abstracts, 517-528.

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

BlFM_88 Manuel Blum, Paul Feldman, Silvio Micali: Non-interactive zero-knowledge and its applications (extended abstract); 20th STOC, ACM, New York 1988, 103-112.

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

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

BüPf_87 Holger Bürk, Andreas Pfitzmann: Value Transfer Systems Enabling Security and Unobservability; Interner Bericht 2/87, Fakultät für Informatik, Universität Karlsruhe 1987; Überarbeitung erscheint in zwei Teilen in Computers & Security, 1. Teil: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

Cha8_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; CACM 28/10 (1985) 1030-1044; deutsche Übersetzung: Informatik-Spektrum (1987) 262-277; DuD /1 (1988) 26-41.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM 24/2 (1981) 84-88.

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

Chau_89 David Chaum: Privacy Protected Payments – Unconditional Payer and/or Payee Untraceability; Smart Card 2000, Proc., North Holland, Amsterdam 1989, 69-93.

Denn_82 Dorothy Denning: Cryptography and Data Security; Addison-Wesley, Reading 1982, reprinted with corrections 1983.

Dier_89 Rüdiger Dierstein: DES-Algorithmus entschlüsselt?; Datenschutz-Berater 12/5 (1989) 3-5.

GaHY_89 Zvi Galil, Stuart Haber, Moti Yung: A Secure Public-Key Authentication Scheme; erscheint in: Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1989.

GoGM_86 Oded Goldreich, Shafi Goldwasser, Silvio Micali: How to construct random functions; JACM 33/4 (1986) 792-807.

GoMT_82 Shafi Goldwasser, Silvio Micali, Po Tong: Why and How to Establish a Private Code on a Public Network; 23rd FOCS, IEEE Computer Society, 1982, 134-144.

ITG_87 ITG-Empfehlungen: ISDN-Begriffe; ntz 40/11 (1987) 814-819.

Klei_75 Leonard Kleinrock: Queueing Systems - Volume I: Theory; Wiley, New York 1975.

Kub1_87 Herbert Kubicek: Für fernmeldetechnische Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 10/April-Juni (1987) 87-92.

KuRo_86 Herbert Kubicek, Arno Rolf: Mikropolis; Mit Computernetzen in die „Informationsgesellschaft“ (2. Aufl.), VSA-Verlag, Hamburg 1986.

MaPf_87 Andreas Mann, Andreas Pfitzmann: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen; Kommunikation in Verteilten Systemen, IFB 130, Springer-Verlag, Berlin 1987, 16-30; Überarbeitung in: DuD /8 (1987) 393-405.

PeSL_80 Marshall Pease, Robert Shostak, Leslie Lamport: Reaching Agreement in the Presence of Faults; JACM 27/2 (1980) 228-234.

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

Pfi1_85 Andreas Pfitzmann: How to implement ISDNs without user observability - Some remarks; Fakultät für Informatik, Interner Bericht 14/85, Universität Karlsruhe 1986.

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

Pfit_89 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe, Fakultät für Informatik, Dissertation, IFB 234, Springer-Verlag, Heidelberg 1989.

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

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze; DuD /3 (1986) 178-191; Überarbeitung in: Informatik-Spektrum 11/3 (1988) 118-142.

PfWa_86 Andreas Pfitzmann, Michael Waidner: Networks without user observability -- design options; Eurocrypt '85, LNCS 219, Springer-Verlag, Berlin 1986, 245-253; Überarbeitung in: Computers & Security 6/2 (1987) 158-166.

PPfW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Weitere Aspekte fernmeldetechnischer Alternativen zum ISDN; Praxis der Informationsverarbeitung und Kommunikation PIK 11/1 (1988) 5-7.

PWP_87 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht 3/10,11,12 (1987) 712-717, 796-803, 898-904.

RSA_78 Ronald L. Rivest, Adi Shamir, Leonard Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; CACM 21/2 (1978) 120-126, nachgedruckt in: CACM 26/1 (1983) 96-99.

Sedl_88 H. Sedlak: The RSA cryptography processor; Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin 1988, 95-105.

Siem_87 Internationale Fernsprechstatistik 1987, Stand 1. Januar 1986; SIEMENS AG, München 1987.

Siem_88 Kurz berichtet: Vermittlungsrechner CP 113 für ISDN; telcom report 11/2 (1988) 80.

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

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

WaPf1_89 Michael Waidner, Birgit Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; erscheint voraussichtlich in: Eurocrypt '89, LNCS, Springer-Verlag, Berlin 1989.

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

WaPP_87 Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; DuD /6 (1987) 293-299.