

## Informatik-Fachberichte 234

---

Herausgeber: W. Brauer  
im Auftrag der Gesellschaft für Informatik (GI)

Andreas Pfitzmann

# Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz



Springer-Verlag  
Berlin Heidelberg New York  
London Paris Tokyo Hong Kong

**Autor**

Andreas Pfitzmann  
Universität Karlsruhe  
Institut für Rechnerentwurf und Fehlertoleranz  
Postfach 6980, D-7500 Karlsruhe 1

CR Subject Classifications (1987): C.2, D.4.6, E.3, H.4.3, K.4.1

ISBN-13: 978-3-540-52327-7

e-ISBN-13: 978-3-642-75544-6

DOI: 10.1007/978-3-642-75544-6

CIP-Titelaufnahme der Deutschen Bibliothek.

Pfitzmann, Andreas:

Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz / Andreas Pfitzmann. - Berlin; Heidelberg; New York; London; Paris; Tokyo; Hong Kong: Springer, 1990

(Informatik-Fachberichte; 234)

NE: GT

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der Fassung vom 24. Juni 1985 zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

© Springer-Verlag Berlin Heidelberg 1990

2145/3140 - 543210 - Gedruckt auf säurefreiem Papier

# Vorwort

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

Deshalb wird in dieser Arbeit untersucht, wie sensitive Daten vor illegalen und legalen Netzbenutzern, dem Betreiber des Netzes und den Herstellern der Vermittlungszentralen sowie ihren Mitarbeitern geschützt werden können. Manche Vermittlungsdaten, z. B. die genauen Netzadressen der Teilnehmer, müssen auch vor Kommunikationspartnern, etwa Datenbanken, geschützt werden, damit sie nicht als Personenkenneichen verwendbar werden.

Bei der heute üblichen und von der Deutschen Bundespost auch für die Zukunft, nämlich für das **diensteintegrierende** Digitalnetz (ISDN), geplanten Netzstruktur erlauben auch juristische Datenschutzvorschriften und Verschlüsselung allein keinen ausreichenden und mit vernünftigem Aufwand **überprüfbar**en Datenschutz. Die Nutzdaten können zwar durch Ende-zu-Ende-Verschlüsselung in Digitalnetzen effizient, überprüfbar und umfassend geschützt werden. Bei der im Teilnehmeranschlußbereich üblichen vollvermittelten Sternstruktur der Kommunikationsnetze erlauben diese Maßnahmen jedoch keinen überprüfbar Schutz der Vermittlungsdaten vor dem Betreiber des Netzes. Werden – wie vorgesehen – komplexe und zusätzlich frei speicherprogrammierbare Vermittlungszentralen verwendet, die für „Trojanische Pferde“ anfällig sind, können vor ihren Herstellern, deren Mitarbeitern und damit grundsätzlich auch fremden Geheimdiensten die Vermittlungsdaten ebenfalls nicht überprüfbar geschützt werden. Derart strukturierte öffentliche Vermittlungsnetze – insbesondere also das geplante ISDN – gewähren ihrem Benutzer nicht das im Volkszählungsurteil des Bundesverfassungsgerichts vom Dezember 1983 formulierte „Recht auf informationelle Selbstbestimmung ...“, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Zusammen mit dem faktischen Benutzungszwang, der durch immer stärkere Nutzung und das Fernmeldemonopol verursacht wird, wirft dies die Frage auf, ob die Beibehaltung dieser Netzstruktur verfassungsrechtlich zulässig ist.

Nach dieser Problemanalyse werden zunächst die zur Abhilfe geeigneten bekannten Grundverfahren – sie machen **Datenschutz** weitgehend sogar **teilnehmerüberprüfbar** – zusammen mit einigen Überlegungen zu ihrer effizienten Realisierung dargestellt. In reiner Form sind sie beim in den nächsten zwei Jahrzehnten zu erwartenden Stand der Technik nur als Spezialnetze für geringe Teilnehmerzahlen oder Leistungsanforderungen zu vertretbaren, aber bezogen auf die Kommunikationsleistung hohen Kosten realisierbar. Um die bezüglich Teilnehmerzahl, Zuverlässigkeit und Verkehrslast hohen Anforderungen eines diensteintegrierenden Kommunikationsnetzes zu erfüllen und damit teilnehmerüberprüfbar Datenschutz auch in offenen Kommunikationsnetzen – durch die Dienstintegration sogar preiswert – zur Verfügung stellen zu können, werden die Grundverfahren durch Implementierung verschieden geschützter Verkehrsklassen, hierarchische Unterteilung des Kommunikationsnetzes sowie mit Datenschutz verträgliche Fehlertoleranztechniken praktikabel gemacht. Anschließend wird gezeigt, wie diese praktikablen Grundverfahren zur (ausgehend von den heutigen Kommunikationsnetzen) evolutionären Gestaltung eines Datenschutz garantierenden offenen, zunächst schmalbandigen, später breitbandigen diensteintegrierenden Digitalnetzes verwendet werden können. Überlegungen zur Netzbetreiberschaft und Verantwortung für die Dienstqualität sowie

zur datenschutzgerechten Abrechnung der Netznutzung schließen die Betrachtung diensteintegrierender Kommunikationsnetze im engeren Sinne ab.

Um einen Ausblick auf die Nutzung solcher Kommunikationsnetze zu geben, skizziere ich, wie die wichtigsten Transaktionsprotokolle, nämlich solche für *Zahlungen*, *Warentransfer* (d. h. digitale Ware gegen Geld) und *Dokumente* (z. B. Nachweis einer Qualifikation), und *statistische Erhebungen* so gestaltet werden können, daß teilnehmerüberprüfbarer Datenschutz und Rechtssicherheit gewährleistet werden. Um die Anwendbarkeit der Verfahren für teilnehmerüberprüfbarer Datenschutz in diensteintegrierenden Kommunikationsnetzen auf andere Problemstellungen zu demonstrieren, gebe ich einen Ausblick auf eine datenschutzgerechte Gestaltung von *öffentlichem mobilem Funk* (z. B. Autotelefon, Verkehrsleitsysteme) und *Fernwirken* (TEMEX) sowie auf eine Lösung des *Einschränkungsproblems* in verteilten Systemen, d. h. die Frage, wie ein Programm, das ein „Trojanisches Pferd“ enthält, daran gehindert werden kann, Information über verdeckte Kanäle weiterzugeben.

## Danksagung

Diese von der Fakultät für Informatik der Universität Karlsruhe (Technische Hochschule) genehmigte Dissertation entstand am Institut für Rechnerentwurf und Fehlertoleranz (früher: Institut für Informatik IV). Sie wurde der Fakultät am 20. Mai 1988 vom Autor zur Erlangung des akademischen Grades eines Doktors der Naturwissenschaften vorgelegt. Die mündliche Prüfung fand am 1. Februar 1989 statt.

Prof. Dr.-Ing. *Winfried Görke* übernahm das Referat, Prof. Dr. *Otto Spaniol* (RWTH Aachen) nach intensiven und sehr anregenden Gesprächen, der Lektüre der bis dahin geschriebenen Arbeiten und einem in Aachen gehaltenen Kolloquiumsvortrag das Korreferat. Als dritter Gutachter wurde Prof. Dr.-Ing. *Paul J. Kühn* (Univ. Stuttgart) bestimmt. Für die viele investierte Zeit danke ich ihnen sehr.

Den Anstoß zu dieser Arbeit verdanke ich Dipl.-Ing. *Peter Mahnkopf*, der am 31. Januar 1983 im Informatik-Kolloquium der Karlsruher Fakultät voller Begeisterung über „Neue bildschirmorientierte Telekommunikationsformen – eine Darstellung der neuen Medien“ vortrug und auf meine Frage, ob er jemals über die durch das von ihm angepriesene BIGFON-Konzept (Vermittlung von allen Diensten, auch von Fernsehen) verursachten Datenschutz-Probleme und deren technische Lösung nachgedacht habe, klar antwortete: „Nein, und ich kenne auch niemand, der bisher darüber nachgedacht hat.“ Dies und die durch die damals bevorstehende Volkszählung verursachte, sehr lebhaft Diskussions über Datenschutz brachten mich dazu, mich nicht nur um Fehlertoleranz, sondern nebenbei auch etwas um Datenschutz zu kümmern. Darin bestärkt wurde ich dadurch, daß Dr. *Ruth Leuze* im Sommersemester 1983 in Karlsruhe eine vielbesuchte und eindrucksvolle Vorlesung über (juristischen) „Datenschutz“ hielt. Dankenswerterweise verschwieg sie nicht, wie wenig sie und ihre Mitarbeiter von technischem Datenschutz verstünden und wie dringend erforderlich originäre Lösungen in diesem Bereich seien.

Ich danke Prof. Dr.-Ing. *Winfried Görke* für die mir gewährte Freiheit, in seiner bisher ausschließlich mit Zuverlässigkeit elektronischer Geräte, Fehlerdiagnose und Fehlertoleranz beschäftigten Arbeitsgruppe mich zunächst „nebenbei“, und wie sich durch das lebhaft Echo nach und nach ergab, später „hauptsächlich“ mit Technischem Datenschutz zu beschäftigen. Es war sehr angenehm, mit ihm und meinen Kollegen, insbesondere Dr. *Klaus Echte*, über ein für uns alle neues Gebiet zu diskutieren und gemeinsam manches zu lernen.

Für meine Themenentscheidung fundierende Gespräche und menschliche Begleitung danke ich Dr. *Klaus Dittrich*, Dr. *Hermann Härtig* und Prof. Dr.-Ing. *Detlef Schmid*.

Zahlreiche Studenten haben durch fruchtbare Zusammenarbeit diese Arbeit gefördert: *Gabriele Bürle* durch Arbeiten über vergleichende Leistungsbewertung zwischen Ringnetzen mit verschiedenen Zugriffsverfahren und Sternnetzen, *Michael Waidner* durch eine grundlegende Arbeit über die Anonymitätserhaltung von Ringzugriffsverfahren sowie durch eine erste wichtige Systematisierung der Datenschutzmaßnahmen in Kommunikationsnetzen, *Gunter Höckel* durch eine mustergültige und weitgehend abschließende Arbeit über die Anonymitätserhaltung von Ringzugriffsverfahren, *Andreas Mann* durch Entwicklung und Bewertung von Datenschutz erhaltenden Fehlertoleranzmaßnahmen in Ringnetzen, *Holger Bürk* durch Programmieren der Formeln in Abschnitt 5.3.4, *Axel Burandt* durch Erfinden eines originellen Codes, *Eckhard Marchel* durch eine sehr sorgfältige Leistungsbewertung von überlagerndem Empfangen bei Mehrfachzugriffsverfahren mittels Kollisionsauflösung, *Arnold Niedermaier* durch die Bewertung von Zuverlässigkeit und Senderanonymität einer fehlertoleranten Kommunikationsstruktur für das DC-Netz, *Manfred Böttger* durch sorgfältige Untersuchungen zur Sicherheit von asymmetrischen Kryptosystemen und MIX-Implementierungen gegen aktive Angriffe und *Ralf Aßmann* durch die bei weitem effizienteste Implementierung von verallgemeinertem DES sowie das zuverlässige Realisieren, Integrieren und Pflegen von Programmen zur komfortableren Textbearbeitung und Literaturstellenverwaltung. *Manfred Böttger* und *Dirk Fox* lasen Teile dieser Arbeit; ihre Kritik führte zu zahlreichen Verbesserungen der Darstellung.

Ganz besonders anregend waren Artikel von sowie Begegnungen und Telefonate mit Dr. *David Chaum*, der mich seit 1985 über seine Arbeiten auf dem laufenden hält und an unseren kritischen Anteil nimmt.

Prof. *Herbert Kubicek* habe ich für über den Datenschutz hinausgehende Diskussionen über ISDN zu danken, *Michael Kühn* für beharrliches Fragen, was im Datenschutzkontext denn mit den Breitbandkabelverteilnetzen anzufangen sei.

Ganz besonders danke ich meinen schärfsten, beharrlichsten, aber auch konstruktivsten Kritikern: Zuallererst meiner Frau *Birgit Pfitzmann*, dann dem Kollegen, mit dem ich die letzten Jahre am engsten zusammengearbeitet habe, Dipl.-Inform. *Michael Waidner*.

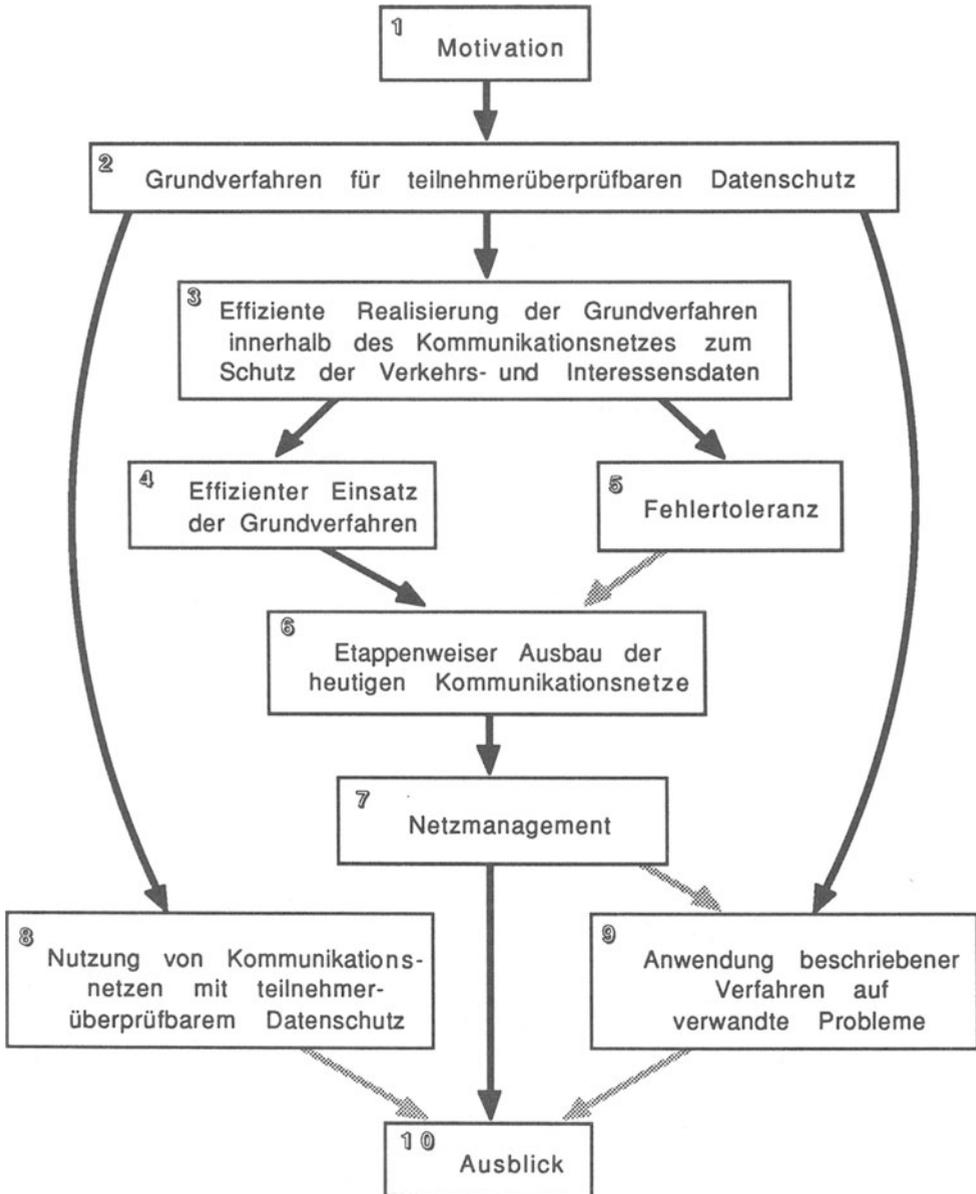
## Hinweise für den Leser

Literaturangaben mit Jahreszahl 89 wurden kurz vor Drucklegung und nur mit kurzem Hinweis auf ihren Inhalt nachträglich eingefügt. Entsprechendes gilt für alle Referenzen in Kapitel 8, das nur einen skizzenhaften Ausblick auf die Nutzung von Kommunikationsnetzen mit teilnehmerüberprüfbarem Datenschutz gibt. Alle anderen Referenzen stehen nach Sachverhalten, die für das Verständnis dieser Arbeit ausreichend ausführlich dargestellt sind. Dies gilt insbesondere für Arbeiten, deren Autor oder Koautor ich bin.

Diese Arbeit verdeutlicht einige der im fachlich sehr weit gespannten Bereich „Kommunikationsnetze“ vorhandenen technischen Gefahren und weist Möglichkeiten zu ihrer Abwendung mit den Mitteln der „Telematik“ (Telekommunikation und Informatik) nach. Sie bedient sich der in der Informatik üblichen Betrachtungsebenen und beschränkt sich auf sie. Das Erarbeiten und Darstellen von Lösungen setzt voraus, daß die zu lösenden Probleme klar und prägnant formuliert werden. Damit dies nicht mißverstanden wird: Wenn ich hervorhebe, daß jemand etwas tun *kann*, will ich damit nicht unterstellen, daß er es getan *hat* oder tun *wird*.

## VIII

Das folgende Diagramm stellt die inhaltliche Abhängigkeit der Kapitel dar. Ein schwarzer bzw. grauer Pfeil von Kapitel x zu Kapitel y bedeutet, daß das Verständnis von y das Verständnis von x voraussetzt bzw. durch es erleichtert wird.



# Inhaltsverzeichnis

1	Motivation .....	1
1.1	Heutige und geplante Kommunikationsnetze .....	1
1.2	Welche Beobachtungsmöglichkeiten bieten diese Netze?.....	3
1.3	Notwendigkeit vorbeugenden Datenschutzes als Gegenmaßnahme .....	9
1.4	Diskussion möglicher Einwände .....	10
2	Grundverfahren für teilnehmerüberprüfbaren Datenschutz.....	14
2.1	Informatische Problemstellung und Lösungsansätze.....	14
2.1.1	Informatische Problemstellung .....	14
2.1.2	Diskussion von Lösungsansätzen .....	16
2.2	Hilfsmittel aus der Kryptographie .....	19
2.2.1	Kryptosysteme und ihre Schlüsselverteilung.....	19
2.2.1.1	Symmetrische Kryptosysteme .....	21
2.2.1.2	Asymmetrische Kryptosysteme.....	24
2.2.1.2.1	Asymmetrische Konzelationssysteme .....	26
2.2.1.2.2	Signaturssysteme .....	28
2.2.2	Eigenschaften von Kryptosystemen .....	30
2.2.2.1	Betriebsarten: Blockchiffre, Stromchiffre .....	30
2.2.2.2	Sicherheit: informationstheoretisch, komplexitätstheoretisch .....	41
2.2.2.3	Realisierungsaufwand bzw. Verschlüsselungsleistung .....	47
2.2.2.4	Registrierung geheimer oder Standardisierung und Normung öffentlicher Kryptosysteme? .....	50
2.3	Einsatz und Grenzen von Verschlüsselung in Kommunikationsnetzen .....	53
2.3.1	Einsatz von Verschlüsselung in Kommunikationsnetzen .....	53
2.3.1.1	Verbindungs-Verschlüsselung .....	53
2.3.1.2	Ende-zu-Ende-Verschlüsselung .....	54
2.3.2	Grenzen von Verschlüsselung in Kommunikationsnetzen .....	57
2.4	Grundverfahren außerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten .....	59
2.4.1	Öffentliche Anschlüsse.....	59
2.4.2	Zeitlich entkoppelte Verarbeitung .....	60
2.4.3	Lokale Auswahl.....	61
2.5	Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten .....	62
2.5.1	Schutz des Empfängers (Verteilung) .....	63
2.5.2	Schutz der Kommunikationsbeziehung (MIX-Netz) .....	67
2.5.2.1	Grundsätzliche Überlegungen über Möglichkeiten und Grenzen des Umcodierens .....	68
2.5.2.2	Senderanonymität .....	70
2.5.2.3	Empfängeranonymität.....	73
2.5.2.4	Gegenseitige Anonymität .....	76
2.5.2.5	Längentreue Umcodierung .....	77
2.5.2.6	Effizientes Vermeiden wiederholten Umcodierens .....	85
2.5.2.7	Kurze Vorausschau .....	86
2.5.2.8	Notwendige Eigenschaften des asymmetrischen Konzelations- systems und Brechen der direkten RSA-Implementierung .....	87
2.5.3	Schutz des Senders .....	90
2.5.3.1	Überlagerndes Senden (DC-Netz) .....	92
2.5.3.1.1	Ein erster Überblick.....	92
2.5.3.1.2	Definition und Beweis der Senderanonymität .....	95

2.5.3.1.3	Überlagerndes Empfangen .....	98
2.5.3.1.4	Optimalität, Aufwand und Implementierungen .....	99
2.5.3.2	Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung .....	101
2.5.3.2.1	Ringförmige Verkabelung (RING-Netz) .....	102
2.5.3.2.2	Kollisionen verhinderndes Baumnetz (BAUM-Netz)....	107
2.6	Einordnung in ein Schichtenmodell .....	108
<b>3</b>	<b>Effiziente Realisierung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten.....</b>	<b>115</b>
3.1	Anonymität erhaltende Schichten: effiziente implizite Adressierung und effizienter Mehrfachzugriff .....	116
3.1.1	Implizite Adressierung bei Verteilung nur in wenigen Kanälen .....	118
3.1.2	Mehrfachzugriff beim DC-Netz für Pakete, Nachrichten und Kanäle .....	119
3.1.2.1	Kriterien für die Erhaltung von Anonymität und Unverkettbarkeit ..	119
3.1.2.2	Klasseneinteilung von Anonymität und Unverkettbarkeit erhaltenden Mehrfachzugriffsverfahren .....	120
3.1.2.3	Beschreibung und ggf. Anpassung der in Klassen eingeteilten Mehrfachzugriffsverfahren .....	122
3.1.2.3.1	Direkte Übertragung, bei Kollision nochmaliges Senden nach zufälliger Zeitdauer (slotted ALOHA) .....	123
3.1.2.3.2	Direkte Übertragung, bei Kollision Kollisionsauflösung (splitting algorithm) .....	123
3.1.2.3.3	Direkte Übertragung, bei Kollision nochmaliges Senden nach zufälliger, aber angekündigter Zeitdauer (ARRA) .....	136
3.1.2.3.4	Direkte Übertragung, bei Erfolg Reservierung (R-ALOHA).....	136
3.1.2.3.5	Reservierungsschema (Roberts' scheme) .....	137
3.1.2.3.6	Verfahren für einen Kanal mit kurzer Verzögerungszeit .....	138
3.1.2.4	Eignung für das Senden von Paketen, Nachrichten und kontinuierlichen Informationsströmen (Kanäle) .....	140
3.1.2.5	Einsatz von paarweisem überlagernden Empfangen .....	140
3.1.2.6	(Anonyme) Konferenzschaltungen .....	141
3.1.2.7	Resümee .....	142
3.1.3	Mehrfachzugriff beim BAUM-Netz auch für Kanäle.....	142
3.1.4	Mehrfachzugriff beim RING-Netz .....	142
3.1.4.1	Angreifermodelle, grundlegende Begriffe und Beweismethoden....	143
3.1.4.2	Ein effizientes 2-anonymes Ringzugriffsverfahren.....	147
3.1.4.3	Effiziente Kanalvermittlung und Konferenzschaltung .....	148
3.1.4.4	Unkoordinierter Zugriff während des ersten und koordinierter Nichtzugriff während des zweiten Umlaufs.....	150
3.1.4.5	Klassifikation und Anonymitätseigenschaften der Ringzugriffsverfahren .....	154
3.2	Anonymität schaffende Schichten .....	156
3.2.1	Kanäle bei Verteilung .....	156
3.2.2	MIX-Netz.....	157
3.2.2.1	Schalten von Kanälen beim MIX-Netz .....	157
3.2.2.2	Längenwachstum der bisherigen Umcodierungsschemata .....	161
3.2.2.3	Minimal längenexpandierendes längentreues Umcodierungsschema	163
3.2.2.4	Anzahl der pro Kommunikationsbeziehung benutzbaren MIXe und ihr möglicher Anteil an der Gesamtheit aller Stationen .....	164
3.2.3	DC-Netz .....	173

3.2.4	RING-Netz.....	178
3.2.5	BAUM-Netz.....	181
3.3	Ohne Rücksicht auf Anonymität realisierbare Schichten.....	183
3.3.1	Verteilung.....	183
3.3.2	MIX-Netz.....	183
3.3.3	Übertragungstopologie und Multiplexbildung beim DC-Netz.....	184
4	Effizienter Einsatz der Grundverfahren.....	187
4.1	Vergleich der bzw. Probleme mit den Grundverfahren.....	187
4.2	Heterogene Kommunikationsnetze: verschieden geschützte Verkehrsklassen in einem Netz.....	189
4.2.1	Asymmetrische Kommunikationsnetze für Massenkommunikation.....	190
4.2.2	Aufwandsreduktion bei nicht sensitivem Verkehr im MIX-, DC-, RING- und BAUM-Netz.....	191
4.2.3	Verschieden sichere Realisierung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten....	193
4.2.3.1	Fest vorgegebene MIX-Kaskaden beim MIX-Netz.....	193
4.2.3.2	Verschieden sichere Schlüsselerzeugung beim DC-Netz.....	194
4.2.4	Kombination von Grundverfahren für besonders sensitiven Verkehr.....	194
4.2.4.1	MIX-Netz und Verteilung.....	194
4.2.4.2	Überlagerndes Senden auf RING- und BAUM-Netz.....	195
4.3	Hierarchische Kommunikationsnetze.....	195
4.3.1	Statisch feste Hierarchiegrenze.....	196
4.3.1.1	Eine Anonymitätsklasse bezüglich Hierarchiegrenze.....	196
4.3.1.1.1	Vermittlungs-/Verteilnetz.....	197
4.3.1.1.2	Verteil-/Verteilnetz.....	200
4.3.1.2	Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze.....	202
4.3.2	Dynamisch an Verkehrslast adaptierbare Hierarchiegrenze.....	202
4.3.2.1	Eine Anonymitätsklasse bezüglich Hierarchiegrenze.....	203
4.3.2.1.1	Dynamisch partitionierbares DC-Netz.....	204
4.3.2.1.2	Dynamisch adaptierbares Vermittlungs-/DC-Netz.....	206
4.3.2.1.3	Dynamisch adaptierbares DC-/DC-Netz.....	208
4.3.2.2	Mehrere Anonymitätsklassen bezüglich Hierarchiegrenze.....	209
5	Fehlertoleranz.....	210
5.1	Verschlüsselung.....	217
5.2	Verteilung.....	218
5.3	MIX-Netz.....	219
5.3.1	Verschiedene MIX-Folgen.....	220
5.3.2	Ersetzen von MIXen.....	222
5.3.2.1	Das Koordinations-Problem.....	223
5.3.2.2	MIXe mit Reserve-MIXen.....	225
5.3.2.3	Auslassen von MIXen.....	227
5.3.2.3.1	Nachrichten- und Adreßformate.....	227
5.3.2.3.2	Datenschutz-Kriterien.....	233
5.3.2.3.3	Auslassen von möglichst wenig MIXen.....	234
5.3.2.3.4	Auslassen von möglichst vielen MIXen.....	238
5.3.2.4	Verschlüsselung zwischen MIXen zur Verringerung der nötigen Koordinierung.....	240
5.3.3	Besonderheiten beim Schalten von Kanälen.....	243
5.3.4	Quantitative Bewertung.....	244
5.4	DC-Netz.....	254
5.5	RING-Netz.....	259

5.6	BAUM-Netz .....	264
5.7	Hierarchische Netze .....	266
5.8	Tolerierung aktiver Angriffe .....	267
5.9	Konzepte zur Realisierung von Fehlertoleranz und Anonymität .....	271
6	Etappenweiser Ausbau der heutigen Kommunikationsnetze .....	272
6.1	Digitalisierung des Teilnehmeranschlusses und Ende-zu-Ende-Verschlüsselung ...	273
6.2	Schmalbandiges diensteintegrierendes Digitalnetz mit MIX-Kaskaden .....	274
6.3	Schmalbandiges diensteintegrierendes Digitalnetz mit Verteilung auf Koaxialkabelbaumnetzen .....	277
6.4	Schmalbandiges diensteintegrierendes Digitalnetz durch anonymes Senden und Verteilung auf Koaxialkabelbaumnetzen .....	278
6.5	Ausbau zu einem breitbandigen diensteintegrierenden Digitalnetz .....	279
6.6	Teilnehmerüberprüfbarer Datenschutz bei Kommunikation zwischen Teilnehmern in verschieden weit ausgebauten Kommunikationsnetzen .....	281
7	Netzmanagement .....	283
7.1	Netzbetreiberschaft: Verantwortung für die Dienstqualität vs. Bedrohung durch Trojanische Pferde .....	283
7.1.1	Ende-zu-Ende-Verschlüsselung und Verteilung .....	285
7.1.2	MIX-Netz .....	285
7.1.3	DC-Netz .....	286
7.1.4	RING- und BAUM-Netz .....	286
7.1.5	Kombinationen sowie heterogene Netze .....	287
7.1.6	Verbundene, insbesondere hierarchische Netze .....	287
7.2	Abrechnung .....	288
8	Nutzung von Kommunikationsnetzen mit teilnehmerüberprüfbarem Datenschutz .....	290
8.1	Digitale Zahlungssysteme .....	291
8.2	Warentransfer .....	292
8.3	Dokumente .....	293
8.4	Statistische Erhebungen .....	294
9	Anwendung beschriebener Verfahren auf verwandte Probleme .....	295
9.1	Öffentlicher mobiler Funk .....	295
9.2	Fernwirken (TEMEX) .....	297
9.3	Einschränkungsproblem (confinement problem) .....	297
9.4	Hocheffizienter Mehrfachzugriff .....	298
10	Ausblick .....	299
	Anhang: Modifikationen von DES .....	301
	Literatur .....	304
	Bilderverzeichnis .....	325
	Stichwortverzeichnis (inkl. Abkürzungen) .....	328