

# 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	Signatursysteme.....	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
3	Effiziente Realisierung der Grundverfahren innerhalb des Kommunikationsnetzes zum Schutz der Verkehrs- und Interessensdaten.....	115
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 überlagerndes 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