Literature of the *research group on data security and privacy in distributed systems* at the Institut für Informatik, University of Hildesheim, and the Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe, and the Institut Theoretische Informatik, Technical University of Dresden 2.8.1994

Gray literature from Karlsruhe may be ordered by writing to:

Fakultätsbibliothek Informatik, Universität Karlsruhe, Postfach 6980, D-76128 Karlsruhe 1, Germany; Phone +49 721 608 3979; Fax +49 721 697760; e-mail Bibliothekarin_InfoBib@ira.uka.de

Documents you cannot obtain that way may be ordered by writing to:

Andreas Pfitzmann, Technische Universität Dresden, Fakultät Informatik, Institut Theoretische Informatik, D-01062 Dresden, Germany; Phone +49 351 4575 277; Fax +49 351 4575 255; e-mail pfitza@.de. tcs.inf.tu-dresden.de

or *Birgit Pfitzmann, Institut für Informatik, Universität Hildesheim, Marienburger Platz 22, D-31141 Hildesheim, Germany; Phone +49 5121 883 735; Fax +49 5121 883 732; e-mail pfitzb@informatik.uni-hildesheim*

or *Michael Waidner, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, Postfach 6980, D-76128 Karlsruhe, Germany, Phone +49 721 608 4024; Fax +49 721 370455; e-mail waidner@ira.uka.de.*

1 English

1.1 Untraceable Communication

Pfit_84 Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 Intern. Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, Zurich 1984, Proc. IEEE Catalog Nr. 84CH1998-4, 183-190.

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

PfWa_86 Andreas Pfitzmann, Michael Waidner: Networks without user observability -- design options; Eurocrypt '85, LNCS 219, Springer-Verlag, Berlin 1986, 245-253;

Revision in: Computers & Security 6/2 (1987) 158-166.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with very small Bandwidth Overhead; Proc. Kommunikation in verteilten Systemen, Feb. 1991 Mannheim, Informatik-Fachberichte 267, Springer-Verlag, Heidelberg 1991, 451-463;

Slightly extended in: Information Security, Proc. IFIP/Sec'91, Mai 1991, Brighton, D. T. Lindsay, W. L. Price (eds.), North-Holland, Amsterdam 1991, 245-258.

1.2 Theoretical Cryptography and Distributed Algorithms

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

PfPf_90 Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes; Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 373-381.

Waid_90 Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 302-319.

WaPf1_89 Michael Waidner, Birgit Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; Universität Karlsruhe 1989.

Abstract in: Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 690.

PfWa_90 Birgit Pfitzmann, Michael Waidner: Formal Aspects of Fail-stop Signatures; Interner Bericht 22/90 der Fakultät für Informatik, Universität Karlsruhe, Dezember 1990.

BlPW_91 Gerrit Bleumer, Birgit Pfitzmann, Michael Waidner: A Remark on a Signature Scheme where Forgery can be Proved; Eurocrypt '90, LNCS 473, Springer-Verlag, Berlin 1991, 441-445.

BaPW_91 Birgit Baum-Waidner, Birgit Pfitzmann, Michael Waidner: Unconditional Byzantine Agreement with Good Majority, STACS'91, LNCS 480, Springer-Verlag, Heidelberg 1991, 285-295.

ChHP_91 David Chaum, Eugène van Heijst, Birgit Pfitzmann: Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer; Interner Bericht 1/91, Fakultät für Informatik, Universität Karlsruhe, February 1991.

PfWa2_91 Birgit Pfitzmann, Michael Waidner: Fail-stop Signatures and their Application; SECURICOM 91; 9th Worldwide Congress on Computer and Communications Security and Protection, 20.-22. March 1991, Paris La Défense, 145-160.

Pfit8_91 Birgit Pfitzmann: Fail-stop Signatures; Principles and Applications; Proc. Compsec '91, 8th world conference on computer security, audit and control, Elsevier, Oxford 1991, 125-134.

ChHP_92 David Chaum, Eugène van Heijst, Birgit Pfitzmann: Cryptographically Strong Undeniable Signatures, Unconditionally Secure for the Signer (Extended abstract); Crypto '91, LNCS 576, Springer Verlag, Berlin 1992, 470-484. (In spite of identical titles, quite different from ChHP_91.)

PfWa_92 Birgit Pfitzmann, Michael Waidner: Unconditional Byzantine Agreement for any Number of Faulty Processors (Extended Abstract); STACS '92, LNCS 577, Springer-Verlag, Berlin 1992, 339-350.

PfWa_93 Birgit Pfitzmann, Michael Waidner: Attacks on protocols for server-aided RSA computation; Eurocrypt '92, LNCS 658, Springer-Verlag, Berlin 1993, 153-162.

PfWa5_92 Birgit Pfitzmann, Michael Waidner: Unconditionally Untraceable and Fault-tolerant Broadcast and Secret Ballot Election; Hildesheimer Informatik-Berichte (Mai 1992), Institut für Informatik, Universität Hildesheim.

HePP_93 Eugène van Heijst, Torben Pedersen, Birgit Pfitzmann: New Constructions of Fail-Stop Signatures and Lower Bounds; Crypto '92, LNCS 740, Springer-Verlag, Berlin 1993, 15-30.

Pfit5_93 Birgit Pfitzmann: Sorting Out Signature Schemes — and some Theory of Secure Reactive Systems; Hildesheimer Informatik-Berichte 4/93 (Mai 1993), Institut für Informatik, Universität Hildesheim.

Pfit4_93 Birgit Pfitzmann: Sorting Out Signature Schemes; 1st ACM Conference on Computer and Communications Security, 3.-5.11.1993, Fairfax, acm press 1993, 74-85.

Pfit11_93 Birgit Pfitzmann: Fail-Stop Signature Schemes; submitted as a doctoral thesis, Institut für Informatik, Universität Hildesheim, 4.9.1993.

DaPP_94 Ivan B. Damgård, Torben P. Pedersen, Birgit Pfitzmann: On the Existence of Statistically Hiding Bit Commitment Schemes and Fail-Stop Signatures; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 250-265.

Pfit2_94 Birgit Pfitzmann: Breaking an Efficient Anonymous Channel; Eurocrypt 94 Preproceedings, Perugia, 339-348.

PfWa_94 Birgit Pfitzmann, Michael Waidner: A General Framework for Formal Notions of "Secure" System; Hildesheimer Informatik-Berichte 11/94 (April 1994), Institut für Informatik, Universität Hildesheim.

Pfit1_94 Birgit Pfitzmann: Fail-Stop Signatures Without Trees; Hildesheimer Informatik-Berichte 16/94 (Juni 1994), Institut für Informatik, Universität Hildesheim.

1.3 Payment Systems and Value Transfer

BüPf_86 Holger Bürk, Andreas Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Pre-prints of Fourth Intern. Conf. and Exhibition on Computer Security: "Information Security: The Challenge", Monte Carlo, 2.-4. Dec. 1986, A. Grissonnanche (ed.), 1986, 250-263;

Final Proc.: "Security and Protection in Information Systems", IFIP/Sec. '86, A. Grissonnanche (ed.), North-Holland, 1989, 225-237.

BüPf_87 Holger Bürk, Andreas Pfitzmann: Value Transfer Systems Enabling Security and Unobservability; Interner Bericht 2/87, Fakultät für Informatik, Universität Karlsruhe 1987.

BüPf_89 Holger Bürk, Andreas Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

WaPf2_89 Michael Waidner, Birgit Pfitzmann: Loss-tolerant Electronic Wallet; Proceedings Smart Card 2000, Amsterdam, 4.-6. October 1989; North-Holland, Amsterdam 1991, 127-150.

BüPf_90 Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

WaPf_90 Michael Waidner, Birgit Pfitzmann: Loss-Tolerance for Electronic Wallets; FTCS 20, 26-28th June 1990, Newcastle upon Tyne (UK), 140-147.

PfWa2_92 Birgit Pfitzmann, Michael Waidner: How to Break and Repair a "Provably Secure" Untraceable Payment System; Crypto '91, LNCS 576, Springer Verlag, Berlin 1992, 338-350.

BBCM_94 Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Stig Mjølsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmaker, Luc Vallée, Michael Waidner: Digital Payment Systems in the ESPRIT Project CAFE; Securicom 94, Paris, 1.-3.6.1994.

BBCM1_94 Jean-Paul Boly, Antoon Bosselaers, Ronald Cramer, Rolf Michelsen, Stig Mjølsnes, Frank Muller, Torben Pedersen, Birgit Pfitzmann, Peter de Rooij, Berry Schoenmakers, Matthias Schunter, Luc Vallée, Michael Waidner: The ESPRIT Project CAFE — High Security Digital Payment Systems; will be published in: Proc. ESORICS 94, Brighton, November 1994.

1.4 Implementation Issues

PfAß_90 Andreas Pfitzmann, Ralf Aßmann: Efficient Software Implementations of (Generalized) DES; Proc. SECURICOM 90, Paris, March 1990, 139-158.

Revision with more details and an even more efficient implementation: Interner Bericht 18/90, Fakultät für Informatik, Universität Karlsruhe, May 1990.

PfAß_93 Andreas Pfitzmann, Ralf Aßmann: Efficient Software Implementations of (Generalized) DES; Computers & Security 12/5 (1993) 477-500.

1.5 Health Care Informatics

PfPf1_90 Andreas Pfitzmann, Birgit Pfitzmann: Security in Medical Networks; Data Protection and Confidentiality in Health Informatics – Handling Health Data in Europe in the Future, Edited by the Commission of the European Communities DG XIII/F AIM, Proc. of the AIM Working Conference, Brussels, 19-21 March 1990, IOS Press, Amsterdam 1991, 231-248.

PfPf_92 Andreas Pfitzmann, Birgit Pfitzmann: Technical Aspects of Data Protection in Health Care Informatics; Advances in Medical Informatics, J. Noothoven van Goor and J. P. Christensen (Eds.), IOS Press, Amsterdam 1992, 368-386.

Bleu3_93 Gerrit Bleumer: Specification of a prototype for secure communication: SECURE Talk (Doc: SP08 - 03 (20-03-1993)); Deliverable Nr. 12 of EC Project AIM.SEISMED(A2033), 20.03.1993.

Almå_93 Gaute Almås: A Study on Security Services of Medical Applications; Diplomarbeit, Institut für Informatik, Universität Hildesheim, April 1993 (with Svein J. Knapskog).

Bleu4_93 Gerrit Bleumer: Report on the presentation of the prototype for secure communication: SECURE Talk (Doc: SEISMED (A2033) / Del.-no. 15,17 / SP08.05 / HILD / gb / 15-12-1993); Deliverable Nr. 15+17 of EC Project AIM.SEISMED(A2033), 15.12.1993.

BlHü_93 Gerrit Bleumer, Henrik Hüne: Prototype for encryption: SECURE Talk - User Manual (Doc: SEISMED (A2033) / Del.-no. 16 / SP08.06 / HILD / gb / 15-12-1993); Deliverable Nr. 16 of EC Project AIM.SEISMED(A2033), 15.12.1993.

Bleu1_94 Gerrit Bleumer: Security for Decentralised Health Information Systems; in: B. Barber, A.R. Bakker, S. Bengtsson (ed.): Caring for Health Information — Safety, Security, Secrecy; Elsevier Science, Amsterdam 1994, 139-146.

Bleu2_94 Gerrit Bleumer: Security for Decentralised Health Information Systems; International Journal of Biomedical Computing 35/? (Feb. 1994) 139-145.

Bleu3_94 Gerrit Bleumer: Guideline on Cryptographic Mechanisms; Deliverable Nr. 29 of EC Project AIM.SEISMED(A2033), 1.6.1994.

BiBl_94 Joachim Biskup, Gerrit Bleumer: Reflections on Security of Database and Datatransfer Systems in Health Care; Hildesheimer Informatik-Berichte 10/94 (April 1994), Institut für Informatik, Universität Hildesheim.

Also accepted for: Proceedings of the 13th World Computer Congress, IFIP Congress 1994.

1.6 Security Criteria

Pfit2_90 Andreas Pfitzmann: Statement of Observations concerning the Draft of the Information Technology Security Evaluation Criteria (ITSEC) Version 1, 02 May 1990; Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe, Sept. 3, 1990.

Pfit2_91 Andreas Pfitzmann: Statement of Observations concerning the Draft of the Information Technology Security Evaluation Criteria (ITSEC) Version 1.1, 10 January 1991; Institut für Rechnerentwurf und Fehlertoleranz, University of Karlsruhe, March 29, 1991.

Pfit10_91 Andreas Pfitzmann: Statement of Observations concerning the Information Technology Security Evaluation Criteria (ITSEC) Version 1.2, 28 June 1991; Institut für Informatik, University of Hildesheim, Germany, November 29, 1991; except the cover letter, published in ACM SIGSAC Review 10/1 (1992) 44-53.

GePR_92 Michael Gehrke, Andreas Pfitzmann, Kai Rannenberg: Information Technology Security Evaluation Criteria (ITSEC) – a Contribution to Vulnerability?; Education and Society, R. Aiken (ed.), Proc. 12th IFIP World Computer Congress 1992, Information Processing 92, Vol. II, Elsevier Science Publishers B.V. (North-Holland), 1992, 579-587.

Pfit3_92 Andreas Pfitzmann: Statement of Observations concerning the Information Technology Security Evaluation Manual (ITSEM) Version 0.2, 2 April 1992; Institut für Informatik, University of Hildesheim, Germany, May 28, 1992.

1.7 Miscellaneous

2 Deutsch

2.1 Datenschutz garantierende Kommunikationsnetze

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

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

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

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

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

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

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

HöPf_85 Gunter Höckel, Andreas Pfitzmann: Untersuchung der Datenschutzeigenschaften von Ringzugriffsmechanismen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Berlin 1985, 113-127.

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

PfPW_86 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Warum und wie?; Datenschutz und Datensicherung DuD /3 (1986) 178-191.

MaPf_87 Andreas Mann, Andreas Pfitzmann: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen; Kommunikation in Verteilten Systemen, GI/NTG-Fachtagung, Aachen 1987, IFB 130, Springer-Verlag, Heidelberg 1987, 16-30;

Überarbeitung in: Datenschutz und Datensicherung DuD /8 (1987) 393-405.

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

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

PfPW_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Garantierter Datenschutz für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß durch Telefon-MIXe; Tagungsband 3 der 4. SAVE-Tagung, 19.-21. April 1989, Köln, 1417-1447.

PfPW1_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64 + 16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung DuD /12 (1989) 605-622.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990.

PfPW2_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze; Teletech NRW, Landesinitiative Telekommunikation des Ministeriums für Wirtschaft, Mittelstand und Technologie des Landes Nordrhein-Westfalen; März 1991, Vortragsausarbeitung Nr. 2, Präsentation auf CeBIT'91.

Überarbeitungen in: Dokumentation des Fachseminars „Programm-Manipulationen in Netzen“, SYSTEMS 91, München; Hrsg. Deutsche Informatik-Akademie, Bonn, Oktober 1991.

und: Vernetzte Systeme und Sicherheit der Informationsverarbeitung, Deutsche Informatik Akademie, Begleitunterlage zu einem Tutorium der GI-Jahrestagung 1992, Karlsruhe, 75-120.

und: Dokumentation Fachseminar Sicherheit in Netzen, 21. Okt. 1993, SYSTEMS 93, München, 75-121.

LuPW_91 Jörg Lukat, Andreas Pfitzmann, Michael Waidner: Effizientere fail-stop Schlüsselerzeugung für das DC-Netz; Datenschutz und Datensicherung DuD 15/2 (1991) 71-75.

PfWa4_92 Andreas Pfitzmann, Michael Waidner: Netze mit unbeobachtbarer Kommunikation; Symposium „Datenschutz: Komfort und Freiheit des Kunden in der Telekommunikation“, 2. Sept. 1991, Materialien zum Datenschutz 15, Herausgeber: Berliner Datenschutzbeauftragter, Hildegardstr. 28/29, 1000 Berlin 31, Mai 1992, 209-235. (Leicht überarbeitete Übersetzung von [PfWa_86].)

Pfit8_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung DuD 17/8 (1993) 451-463.

2.2 Theoretische Kryptographie und verteilte Algorithmen

Pfi1_88 Birgit Pfitzmann: Vergleich der algebraischen und kryptographischen Modellierung von Kryptoprotokollen; Studienarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1988.

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

Pfit1_89 Birgit Pfitzmann: Für den Unterzeichner sichere digitale Signaturen und ihre Anwendung; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1989.

Bleu_90 Gerrit Bleumer: Vertrauenswürdige Schlüssel für ein Signatursystem, dessen Brechen beweisbar ist; Studienarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1990.

PfWa_91 Birgit Pfitzmann, Michael Waidner: Fail-stop-Signaturen und ihre Anwendung; Proc. of the GI-Fachtagung Verläßliche Informationssysteme (VIS'91), March 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 289-301.

PfWa1_91 Birgit Pfitzmann, Michael Waidner: Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit; Proc. of the GI-Fachtagung Verläßliche Informationssysteme (VIS'91), March 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 302-320.

Pfit7_91 Birgit Pfitzmann: Neu und sicher: Digitale Fail-stop-Signaturen; KES – Zeitschrift für Kommunikations- und EDV-Sicherheit 7/5 (1991) 321-326.

Schu_94 Matthias Schunter: Spezifikation von Geheimhaltungseigenschaften für reaktive kryptologische Systeme; Diplomarbeit am Institut für Informatik, Universität Hildesheim, Januar 1994.

Wilh_94 Jan-Peter Wilhelms: Effizienzuntersuchungen neuerer Fail-stop-Signaturschemata; Diplomarbeit am Institut für Informatik, Universität Hildesheim, Juni 1994.

2.3 Zahlungssysteme und Wertetransfer

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

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Berlin 1985, 128-141;

Überarbeitung in: Datenschutz und Datensicherung DuD /1 (1986) 16-22.

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

Bürk_87 Holger Bürk: Modellierung und Verifikation der Sicherheit und Lebendigkeit von Kryptoprotokollen; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, März 1987.

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;

WaPf_87 Michael Waidner, Birgit Pfitzmann: Verlusttolerante elektronische Brieftaschen; 3rd International Conference on Fault-Tolerant Computing-Systems, IFB 147, Springer-Verlag, Berlin 1987, 36-50; Überarbeitung in: Datenschutz und Datensicherung DuD /10 (1987) 487-497.

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

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

Wai1_88 Michael Waidner: Betrugssicherheit durch kryptographische Protokolle beim Wertetransfer über Kommunikationsnetze; Datenschutz und Datensicherung DuD /9 (1988) 448-459.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Waid_94 Michael Waidner: Das ESPRIT-Projekt "Conditional Access for Europe"; 4. GMD-SmartCard Workshop, Darmstadt, 8.-9.2.1994, Tagungsband (Hrsg. Bruno Struif).

und: Multicard '94, Elektronische Kartensysteme - Anspruch und Wirklichkeit, Kongreßdokument II, 23.-25. Februar 1994, Berlin, 236-249.

WaWe_94 Michael Waidner, Arnd Weber: Europäisches Industrie- und Forschungskonsortium entwickelt neuartiges Zahlungsverfahren; à la Card aktuell 5/94 (1994) 13-19.

und: erscheint in Datenschutzberater.

2.4 Implementierungen

Aßma_88 Ralf Aßmann: Effiziente Software-Implementierung von verallgemeinertem DES; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, Februar 1989.

Aßma_89 Ralf Aßmann: Assembler-Implementierung von modularer Langzahlarithmetik; Studienarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe 1989.

Fox_90 Dirk Fox: Implementierung digitaler Signatursysteme; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe Juni 1990.

Bött_90 Manfred Böttger: Realisierung des DC-Netz-Versuchs und einer einheitlichen Praktikums-Netzschnittstelle; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Juli 1990.

Luka_91 Jörg Lukat: Effizienzverbesserung und Implementierung einiger Verfahren zur fail-stop Schlüsselgenerierung im DC-Netz; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, Januar 1991.

Bleu_91 Gerrit Bleumer: Eine Praktikumsumgebung für Kryptoprotokolle sowie Erstellung der Versuche „Zahlentheoretische Algorithmen“ und „Asymmetrische Konzelationssysteme“; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1991.

Ort_91 Andreas Ort: Implementierung eines MIX-Netzes sowie Konzeption und Realisierung des MIX-Netz-Versuchs; Diplomarbeit, Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, März 1991.

FoPf_91 Dirk Fox, Birgit Pfitzmann: Effiziente Software-Implementierung des GMR-Signatursystems; Proc. GI-Fachtagung Verläßliche Informationssysteme (VIS'91), March 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 329-345.

Fox_91 Dirk Fox: Effiziente Softwareimplementierung asymmetrischer Kryptosysteme und der zugrundeliegenden modularen Langzahlarithmetik; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe April 1991.

Schm_91 Andreas Schmidt: Softwareimplementierung unbeobachtbarer und sicherer Zahlungssysteme in einer Versuchsumgebung; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe September 1991.

Hay_92 Friedgard Hay: Implementierung der Schlüsselinitialisierung für eine Ende-zu-Ende-Schutz-Anwendung; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1992.

Rieg_92 Ullrich Rieger: Implementierung einer dateiorientierten Ende-zu-Ende-Schutz-Anwendung; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe 1992.

OABB_92 Andreas Ort, Ralf Aßmann, Gerrit Bleumer, Manfred Böttger, Dirk Fox, Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Schutz in verteilten Systemen durch Kryptologie – Ein Praktikum im Informatik-Hauptstudium; Datenschutz und Datensicherung DuD 16/11 (1992) 571-579.

Ort_93 Andreas Ort: Das Mixnetz und seine Bedeutung für die Lehre; Datenschutz und Datensicherung DuD 17/1 (1993) 28-32.

Hamm_93 Charlie Hammerer: Vermittlung der Problematik des sicheren Schlüssel-Verteilens als Lehrprogramm; Datenschutz und Datensicherung DuD 17/1 (1993) 33-39.

Hess2_93 Dirk Hesse: Langzahlarithmetik mit kleinem Assemblerkern; Diplomarbeit am Institut für Informatik, Universität Hildesheim, 1993.

Hüne_94 Henrik Hüne: The Manual for SECURE Talk; Studienarbeit, Institut für Informatik, Universität Hildesheim, Dezember 1993.

Scha1_94 Axel Scharff: Konzeption und Implementierung einer Programmierschnittstelle für den Filetransfer in einem AppleTalk-Netz; Studienarbeit, Institut für Informatik, Universität Hildesheim, Januar 1994.

Schü_94 Ulrike Schütte: Konzeption und Implementierung von dateiorientierten, kryptograhischen Diensten in einer objektorientierten Umgebung; Studienarbeit, Institut für Informatik, Universität Hildesheim, Januar 1994.

Weis_94 Matthias Weise: Implementierung höherer zahlentheoretischer Algorithmen in C++; Studienarbeit, Institut für Informatik, Universität Hildesheim, Juni 1994.

2.5 Gesellschaftliche und juristische Aspekte

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

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

Pfi3_87 Andreas Pfitzmann: Anmerkungen aus Anlaß der 2. Auflage von Duncan Campbell, "The Unsinkable Aircraft Carrier"; Computer und Recht, 3. Jahrgang, Heft 8, August 1987, 560.

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

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

Pfit1_90 Andreas Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14/12 (1990) 620-627.

Pfit_91 Andreas Pfitzmann: Soziale Telekommunikationsgestaltung durch technischen Datenschutz oder durch Verzicht auf Netzintegration?; Soziale Gestaltung der Telekommunikation, Johann Welsch (Hrsg.), Dokumentation einer gemeinsamen Fachtagung des DGB und der Hans Böckler Stiftung, Düsseldorf, 7./8. Dez. 1989; Graue Reihe – Neue Folge 31, ISSN 0932-1586, 1991, 177-196.

Pfit5_91 Andreas Pfitzmann: Stellungnahme des Präsidiums-Arbeitskreises „Datenschutz und Datensicherung“ der Gesellschaft für Informatik e.V. (GI) zum „Entwurf (Stand 28.2.1991; BMPT, Referat 211) Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV)“ und der Öffentlichen

Anhörung des Bundestagsausschusses für Post und Telekommunikation am 5. März 1991; Datenschutz-Berater 14/5 (1991) 4-5.

Pfit6_91 Andreas Pfitzmann: Zur Verantwortung der Informatiker; Datenschutz-Berater 14/8-9 (1991) 2-7.

Mit aktualisierten Literaturhinweisen nachgedruckt in: Informatik Forum 7/1-2 (1993) 28-32.

Pfit9_91 Andreas Pfitzmann: Für rechtliche Regelungen relevante Eigenschaften der Informationstechnik und die daraus resultierenden Chancen und Gestaltungsmöglichkeiten, Diskurs-Protokoll zur Technikfolgenabschätzung der Informationstechnik III-4, Vorhaben "Rechtliche Beherrschung der Informationstechnik", Herausgeber: Dr. Reinhard Stransfeld, VDI/VDE-Technologiezentrum, Informationstechnik GmbH, Budapester Str. 40, W-1000 Berlin 30, Dezember 1991, 69-73.

Pfit2_93 Andreas Pfitzmann: Stellungnahme zum politischen Handlungsbedarf; in: Bernd Lutterbeck, Rudolf Wilhelm: Rechtsgüterschutz in der Informationsgesellschaft; TU Berlin, Forschungsberichte des Fachbereichs Informatik, Bericht 1993/5 (1993) 104-106.

2.6 Sicherheitskriterien

Pfit1_93 Andreas Pfitzmann: Leserbrief zu "Zur Diskussion der Sicherheitskriterien, speziell der ITSEC" (KES 92/6); KES /1 (1993) 49.

PfRa_93 Andreas Pfitzmann, Kai Rannenberg: Staatliche Initiativen und Dokumente zur IT-Sicherheit – Eine kritische Würdigung; Computer und Recht 9/3 (1993) 170-179.

2.7 Buchbesprechungen

Pfit4_91 Andreas Pfitzmann: Buchbesprechung: „Dietrich Cerny und Heinrich Kersten (Hrsg.), Sicherheitsaspekte in der Informationstechnik; Proceedings der 1. Deutschen Konferenz über Computersicherheit; Vieweg, Braunschweig 1991, ISBN 3-528-05157-4“; Datenschutz-Berater 14/5 (1991) 26.

Pfit6_93 Andreas Pfitzmann: Buchbesprechung von Jean-Claude Laprie (ed.): Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese; Springer-Verlag, Wien 1992; Datenschutz und Datensicherung DuD 17/9 (1993) 539-540.

Pfit7_93 Andreas Pfitzmann: Buchbesprechung: John F. Meyer, Richard D. Schlichting: Dependable Computing for Critical Applications 2; Springer-Verlag, Wien 1992, ISBN 3-211-82330-1, XIII+439 Seiten, DM 172,--; Datenschutz und Datensicherung DuD 17/8 (1993) 483-484.

Pfit9_93 Andreas Pfitzmann: Buchbesprechung: Harald Faust: Datenschutz und Arbeitsplatzrechner; Sicherheit in der Informationstechnik, Schriftenreihe Band 2, R. Oldenbourg Verlag, München 1991, ISBN 3-486-21883-2, 137 Seiten, DM 48,--; Datenschutz und Datensicherung DuD 17/10 (1993) 594.

Bleu_93 Gerrit Bleumer: Buchbesprechung: „Thomas Beth, Markus Frisch, Gustavus J. Simmons: Public-Key Cryptography: State of the Art and Future Directions”; Datenschutz und Datensicherung DuD 17/6 (1993) 372.

Bleu_94 Gerrit Bleumer: Buchbesprechung: S. Muftic, A. Patel, P. Sanders, R. Colon, Heijnskijk, U. Pulkinnen: Security Architecture for Open Distributed Systems; Datenschutz und Datensicherung DuD 18/1 (1994) 58-59.

2.8 Verschiedenes

Cles_88 Wolfgang Clesle: Schutz auch vor Herstellern und Betreibern von Informationssystemen; Diplomarbeit am Institut für Rechnerentwurf und Fehlertoleranz, Universität Karlsruhe, Juni 1988.

PfP1_89 Birgit Pfitzmann, Andreas Pfitzmann: Anmerkungen zu "Matthias Leclerc: Schlüsselmanagement durch Teilschlüssel, DuD 12/88"; Datenschutz und Datensicherung DuD /3 (1989) 116.

ClPf_91 Wolfgang Clesle, Andreas Pfitzmann: Rechnerkonzept mit digital signierten Schnittstellenprotokollen erlaubt individuelle Verantwortungszuweisung; Datenschutz-Berater 14/8-9 (1991) 8-38.

Pfit5_92 Andreas Pfitzmann: Informationsverarbeitung in Netzen – alte und neue Probleme der Sicherheit; Vernetzte Systeme und Sicherheit der Informationsverarbeitung, Deutsche Informatik Akademie, Begleitunterlage zu einem Tutorium der GI-Jahrestagung 1992, Karlsruhe, 13-38.

Nachgedruckt in: Dokumentation Fachseminar Sicherheit in Netzen, 21. Okt. 1993, SYSTEMS 93, München, 7-32

Kroh_92 Johannes Krohn: Verhinderung unerkannter anonymer Programmodifikation mittels digitaler Signaturen; Studienarbeit am Institut für Rechnerentwurf und Fehlertoleranz der Universität Karlsruhe, November 1992.

MöPS_94 Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist; Datenschutz und Datensicherung DuD 18/6 (1994) 318-326.