Bibliography

At the right are the page numbers on which the sources are referred.

[ABV01] Rafael Accorsi, David Basin, and Luca Viganò. Towards an awareness-based semantics for security protocol analysis. *Electronic Notes in Theoretical Computer Science*, 55(1), 2001. 71, 182

[ACKM04] Gustavo Alonso, Fabio Casati, Harumi Kuno, and Vijay Machiraju. *Web Services: Concepts, Architecture and Applications*. Springer Verlag, 2004. 88, 92

[AES03] Rakesh Agrawal, Alexandre Evfimievski, and Ramakrishnan Srikant. Information sharing across private databases. In *Proceedings of the 2003 ACM SIGMOD International Conference on Management of Data*, pages 86–97, New York, NY, USA, 2003. ACM Press. 114, 115

[AF90] Martín Abadi and Joan Feigenbaum. Secure circuit evaluation, a protocol based on hiding information from an oracle. *Journal of Cryptology*, 2(1):1–12, February 1990. 24

[AF04] Martín Abadi and Cédric Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, 2004. 102

[AG99] Martín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148(1):1–70, January 1999. 174

[AIR01] Bill Aiello, Yuval Ishai, and Omer Reingold. Priced oblivious transfer: How to sell digital goods. In Birgit Pfitzmann, editor, *Advances in Cryptology - EUROCRYPT 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 119–135, Berlin / Heidelberg, 2001. Springer. 22

[And93] Ross Anderson. The classification of hash functions. In *Proceedings of the IMA Conference in Cryptography and Coding*, 1993. 29, 33, 34, 36

[AR02] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *Journal of Cryptology*, 15(2):103–127, 2002. 18, 47, 66, 182

[AT91] Martín Abadi and Mark Tuttle. A semantics for a logic of authentication. In *Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing*, pages 201–216, Montreal, August 1991. 47, 66, 180

[AvdHdV01] Nesria Agray, Wiebe van der Hoek, and Erik P. de Vink. On BAN logics for industrial security protocols. In Barbara Dunin-Kęplicz and Edward Nawarecki, editors, *Proceedings of the Second International Workshop of Central and Eastern Europe on Multi-Agent Systems*, pages 29–36, Cracow, 2001. 44, 48, 66, 175

[AvH04] Grigoris Antoniou and Frank van Harmelen. *A Semantic Web Primer*. MIT Press, Cambridge, MA, 2004. 84

[Bac02] Adam Back. Hashcash - a denial of service counter-measure. Technical report, hashcash.org, August 2002. 43

[BAN88] Michael Burrows, Martín Abadi, and Roger Needham. Authentication: A practical study in belief and action. In M. Vardi, editor, *Proceedings of the Second Conference on Theoretical Aspects of Reasoning About Knowledge*, pages 325–342, 1988. 63, 179

[BAN89a] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. Technical Report 39, Digital Equipment Corporation Systems Research Center, February 28 1989. revised on February 22, 1990. 47, 55, 56, 57, 58, 61, 62, 63, 65, 179

[BAN89b] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *Proceedings of the Royal Society of London, Series A, Mathematical and Physical Sciences*, 426(1871):233–271, December 1989. 44, 47, 55, 56, 57, 58, 61, 62, 63, 65, 179

[BAN89c] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *ACM SIGOPS Operating Systems Review (Proceedings of the 12th ACM Symposium on Operating Systems Principles)*, 23(5):1–13, December 1989. 179

[BAN90a] Michael Burrows, Martín Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, February 1990. 179

[BAN90b] Michael Burrows, Martín Abadi, and Roger Needham. Rejoinder to Nessett. *ACM SIGOPS Operating Systems Review*, 24(2):39–40, April 1990. 182

[BAN94] Michael Burrows, Martín Abadi, and Roger Needham. A scope of a logic of authentication. appendix to DEC SRC research report 39, Digital Equipment Corporation Systems Research Center, May 13, 1994. 56, 179

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, October 1988. 113

[BCLL91] Gilles Brassard, Claude Crépeau, Sophie Laplante, and Christian Léger. Computationally convincing proofs of knowledge. In C. Choffrut and M. Jantzen, editors, *Proceedings of the 8th Annual Symposium on Theoretical Aspects of Computer Science*, pages 251–262, 1991.

[BDG88] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity*. Monographs on Theoretical Computer Science. Springer-Verlag, Berlin / Heidelberg, 1988. 20

[Ber04] Jules J. Berman. Zero-check, a zero-knowledge protocol for reconciling patient identities across institutions. *Archives of Pathology and Laboratory Medicine*, 128(3):344–346, 2004. 115, 187

[BFM88] Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications (extended abstract). In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 103–112, Chicago, Illinois, 2–4 1988. 105

[BG93] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge.

In E.F. Brickell, editor, *Advances in Cryptology - CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 390–420, Berlin, 1993. Springer-Verlag. 105

[BGG94] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. Incremental cryptography: the case of hashing and signing. In Y.G. Desmedt, editor, *Advances in Cryptology - CRYPTO '94*, volume 839 of *Lecture Notes in Computer Science*, Berlin, 1994. Springer-Verlag. . 38, 40, 45

[BGG95] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. Incremental cryptography with application to virus protection. In *Proceedings of the 27th Annual Symposium on the Theory of Computing*. ACM, 1995. 38, 45

[BGI+01] Boaz Barak, Oded Goldreich, Russell Impagliazzo, Steven Rudich, Amit Sahai, Salil Vadhan, and Ke Yan. On the (im)possibility of obfuscating programs. Technical Report TR01-057, Electronic Colloquium on Computational Complexity, 2001. 37

[BGR95] Mihir Bellare, Roch Guerin, and Phillip Rogaway. XOR MACs: New methods for message authentication using finite pseudorandom functions. In D. Coppersmith, editor, *Advances in Cryptology - CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 15–28, Berlin, 1995. Springer-Verlag. 39

[Bin92] Ken Binmore. *Fun and Games: a Text on Game Theory*. DC Heath & Company, Lexington, MA, 1992. 5

[BKK95] Pieter A. Boncz, Fred Kwakkel, and Martin L. Kersten. High performance support for OO traversals in Monet. In *Proceedings British National Conference on Databases (BNCOD96)*, volume 1094 of *Lecture Notes in Computer Science*, pages 152–169, Berlin, 1995. Springer-Verlag. 100

[BM94] Colin Boyd and Wenbo Mao. On a limitation of BAN logic. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 240–247, Berlin, 1994. Springer-Verlag. 182

[BM97] Mihir Bellare and Daniele Micciancio. A new paradigm for collision-free hashing: Incrementality at reduced cost. In W. Fumy, editor, *Advances in Cryptology- EUROCRYPT 97 Proceedings*, volume 1233. Springer-Verlag, 1997. 37, 38, 39

[Bon02] Pieter A. Boncz. *Monet: A Next-Generation DBMS Kernel For Query-Intensive Applications*. PhD thesis, Universiteit van Amsterdam, Amsterdam, The Netherlands, May 2002. 100

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the First Annual Conference on Computer and Communications Security*. ACM, 1993. 36

[BST01] Fabrice Boudot, Berry Schoenmakers, and Jacques Traoré. A fair and efficient solution to the socialist millionaires' problem. *Discrete Applied Mathematics*, 111(1-2):23–36, 2001. 107, 113, 114, 116

[CC04] Tim Churches and Peter Christen. Some methods for blindfolded record linkage. *BMC Medical Informatics and Decision Making*, 4(9), June 2004. 115, 187

[CD05a] Mika Cohen and Mads Dam. A completeness result for BAN logic. In *Prococeedings of Methods for Modalities 4*, Berlin, December 2005. 47, 66, 182

[CD05b] Mika Cohen and Mads Dam. Logical omniscience in the semantics of ban logics. In Andrei Sabelfeld, editor, *Proceedings of the Foundations of Computer Security '05 — FCS'05*, pages 121–132, Chicago, 2005. 47, 66, 182

[CGH98] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *Proceedings of 30th Annual ACM Symposium on the Theory of Computing*, pages 209–218. ACM, 1998. 37

[CGKS98] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. *Journal of the ACM*, 45(6):965–982, November 1998. 100

[CH06] Łukasz Chmielewski and Jaap-Henk Hoepman. Fuzzy private matching. in submission, 2006. 189

[Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, February 1981. 99

[Cha85] David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985. 99

[Cha92] David Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, 1992. 99

[CK85] George P. Copeland and Setrag N. Khoshafian. A decomposition storage model. In S.B. Navathe, editor, *Proceedings of the 1985 ACM SIGMOD International Conference on Management of Data, Austin*, pages 268–279, New York, NY, USA, 1985. ACM Press. 100

[CMR98] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In *Proceedings of the 30th Annual ACM Symposium on the Theory of Computing*, pages 131–140, Dallas, 1998. 43

[Cod70] Edgar F. Codd. A relational model of data for large shared data banks. *Communications of the ACM*, 13(6):377–387, 1970. 100

[CW79] J. Lawrence Carter and Mark N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979. 35

[Dam88] Ivan B. Damgård. Collision free hash functions and public key signature schemes. In D. Chaum and W.L. Price, editors, *Advances in Cryptology - EUROCRYPT '87*, volume 304 of *Lecture Notes in Computer Science*, pages 203–216, Berlin, 1988. Springer-Verlag. 42

[Dam90] Ivan B. Damgård. A design principle for hash functions. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 416–427, Berlin, 1990. Springer-Verlag. 38

[Dam97] Ivan B. Damgård. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. *Journal of Cryptology*, 10(3):163–

194, July 1997. 43

[DBP96] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. RIPEMD160: A strengthened version of RIPEMD. In *Fast Software Encryption*, volume 1039 of *Lecture Notes in Computer Science*, pages 71–82, 1996. 38, 40

[DDMP03] Anupam Datta, Ante Derek, John C. Mitchell, and Dusko Pavlovic. Secure protocol composition. In *Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering*, pages 11–23, New York, NY, USA, 2003. ACM Press. 174

[Dek00] Anthony H. Dekker. C3PO: a tool for automatic sound cryptographic protocol analysis. In *Proceedings of the 13th IEEE Computer Security Foundations Workshop — CFSW-13*, pages 77–87. IEEE Computer Society Press, 2000. 47, 66, 180, 181

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6):644–654, 1976. 29, 42, 55

[DH05] AnHai Doan and Alon Y. Halevy. Semantic integration research in the database community: A brief survey. *AI Magazine*, 26(1):83–94, Spring 2005. 82, 84

[vD03] Hans P. van Ditmarsch. The russian cards problem. *Studia Logica*, 75:31–62, 2003. 107

[DMDH02] AnHai Doan, Jayant Madhavan, Pedro Domingos, and Alon Y. Halevy. Learning to map between ontologies on the semantic web. In *Proceedings of the 11th international conference on World Wide Web*, New York, NY, USA, 2002. ACM Press. 100

[DN93] Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In E.F. Brickell, editor, *Advances in Cryptology - CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 139–147, Berlin, 1993. Springer-Verlag. 43

[DPP94] Ivan B. Damgård, Torben Pedersen, and Birgit Pfitzmann. On the existence of statistically hiding bit commitment schemes and fail-stop signatures. In D.R. Stinson, editor, *Advances in Cryptology - CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 250–265, Berlin, 1994. Springer-Verlag. 43

[DQB95] Liliane Dusserre, Catherine Quantin, and Hocine Bouzelat. A one way public key cryptosystem for the linkage of nominal files in epidemiological studies. *Medinfo*, 8(1):644–647, 1995. 115, 187

[DY83] Danny Dolev and Andrew C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, March 1983. 23, 48

[EGL85] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, June 1985. 22

[ESAG02] Alexandre Evfimievski, Ramakrishnan Srikant, Rakesh Agrawal, and Johannes Gehrke. Privacy preserving mining of association rules. In *Proceedings of the 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*, July 2002. 99

[Fei73] Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, May 1973. 43

[FFS87] Uriel Feige, Amos Fiat, and Adi Shamir. Zero knowledge proofs of identity. In *Proceedings of the nineteenth annual ACM conference on Theory of computing*, pages 210–217, New York, NY, USA, June 1987. ACM Press.

[FFS88] Uriel Feige, Amos Fiat, and Adi Shamir. Zero-knowledge proofs of identity. *Journal of Cryptology*, 1(2):77–94, June 1988.

[FGR92] Joan Feigenbaum, Eric Grosse, and James A. Reeds. Cryptographic protection of membership lists. *Newsletter of the International Association for Cryptologic Research*, 9(1):16–20, 1992. 99, 112

[FHMV95] Ronald Fagin, Joseph Y. Halpern, Yoram Moses, and Moshe Y. Vardi. *Reasoning about Knowledge*. MIT Press, Cambridge, MA, 1995. 47, 175

[FKN94] Uriel Feige, Joe Kilian, and Moni Naor. A minimal model for secure computation. In *Proceedings of the Twentsixth Annual ACM Symposium on Theory of Computing*, pages 554–563. ACM Press, 1994. 24

[FLW91] Joan Feigenbaum, Mark Y. Liberman, and Rebecca N. Wright. Cryptographic protection of databases and software. In Joan Feigenbaum and Michael Merritt, editors, *Distributed Computing and Cryptography*, volume 2, pages 161–172, 1991. 99, 112

[FNP04] Michael J. Freedman, Kobbi Nissim, and Benny Pinkas. Efficient private matching and set intersection. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology - EUROCRYPT 2004*, volume 2037 of *Lecture Notes in Computer Science*, pages 1–19, Berlin, 2004. Springer-Verlag. 111, 114, 116, 188, 189

[FNS75] Horst Feistel, W.A. Notz, and J. Lynn Smith. Some cryptographic techniques for machine-to-machine data communications. *Proceedings of the IEEE*, 63(11):1545–1554, 1975. 43

[FNW96] Ronald Fagin, Moni Naor, and Peter Winkler. Comparing information without leaking it. *Communications of the ACM*, 39(5):77–85, 1996. 99, 106, 107, 114, 115, 172

[FS90] Uriel Feige and Adi Shamir. Witness indistinguishability and witness hiding protocols. In *Proceedings of the 22nd Annual Symposium on the Theory of Computing*, pages 416–426, New York City, 1990. ACM Press.

[FS03] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. Wiley, 2003. 19, 46

[Get63] Edmund L. Gettier. Is justified true belief knowledge? *Analysis*, 23:121–123, 1963. 105

[GH05] Flavio D. Garcia and Jaap-Henk Hoepman. Off-line karma: A decentralized currency for peer-to-peer and grid applications. In John Ioannidis, Angelos Keromytis, and Moti Yung, editors, *Applied Cryptography and Network Security: Third International Conference, ACNS 2005*, volume 3531 of *Lecture Notes in Computer Science*, pages 364–377, Berlin / Heidelberg, 2005. Springer. 43

[GK05] Michael Grüninger and Joseph B. Kopena. Semantic integration through invariants. *AI Magazine*, 26(1):11–20, Spring 2005. 82, 84

[GKSG91] Virgil D. Gligor, Rajashekar Kailar, Stuart G. Stubblebine, and Li Gong. Logics for cryptographic protocols — virtues and limitations. In *Proceedings of the IEEE Computer Security Foundations Workshop IV (CFSW IV)*, pages 219–226, Los Alamitos, 1991. IEEE Computer Society Press. 181

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 291–304, Providence, Rhode Island, 1985. 24, 25, 105

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proofs. *Journal of the ACM*, 38:691–729, 1991. 26

[GNY90] Li Gong, Roger Needham, and Raphael Yahalom. Reasoning about belief in cryptographic protocols. In Deborah Cooper and Teresa Lunt, editors, *Proceedings 1990 IEEE Symposium on Research in Security and Privacy*, pages 234–248, Los Angeles, 1990. IEEE Computer Society Press. 47, 50, 52, 66, 72, 75, 180, 183, 184, 186

[Gol02] Oded Goldreich. Zero-knowledge twenty years after its invention. Technical report, Department of Computer Science, Weizmann Institute of Science, 2002. 25, 26, 105

[GS91] Klaus Gaarder and Einar Snekkenes. Applying a formal analysis technique to the CCITT X.509 strong two-way authentication protocol. *Journal of Cryptology*, 3(2):81–98, January 1991. 181

[GSG99] Stefanos Gritzalis, Diomidis Spinellis, and Panagiotis Georgiadis. Security protocols over open networks and distributed systems: Formal methods for their analysis, design, and verification. *Computer Communications*, 22(8):697–709, May 1999. 48

[Gua98] Nicola Guarino. Formal ontology and information systems. In Nicola Guarino, editor, *Proceedings of the 1st International Conference on Formal Ontologies in Information Systems*, pages 3–15, Trento, Italy, June 1998. IOS Press. 100

[Gut01] Joshua D. Guttman. Key compromise, strand spaces, and the authentication tests. *Electronic Notes in Theoretical Computer Science*, 47:1–21, 2001. 49

[Gut02] Joshua D. Guttman. Security protocol design via authentication tests. In *Proceedings of the 15th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 92–103, Los Alamitos, 2002. IEEE Computer Society Press. 49

[Hei05] Dorothee Heisenberg. *Negotiating Privacy: The European Union, the United States and Personal Data Protection*. Lynne Rienner Publishers, 2005. 104

[Hel61] Joseph Heller. *Catch-22*. Simon & Schuster, 1961.

[Hid04] Jan-Willem Hiddink. Informatie als waardegoed. Master's thesis, Rijksuniversiteit Groningen, August 2004. 90

[HIM+04] Alon Y. Halevy, Zachary G. Ives, Jayant Madhavan, Peter Mork, Dan Suciu, and Igor Tatarinov. The Piazza peer data management system. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):787–798, July 2004. 88

[HM84] Joseph Y. Halpern and Yoram Moses. Knowledge and common knowledge in a distributed environment. In Tiko Kameda, Jayadev Misra, Joseph Peters, and Nicola Santoro, editors, *Proceedings of the Third Annual ACM Symposium on Principles of Distributed Computing*, pages 50–61. ACM, ACM Press, 1984. 56

[HM90] Joseph Y. Halpern and Yoram Moses. Knowledge and common knowledge in a distributed environment. *Journal of the ACM*, 37(3):549–587, 1990. 56

[Hoa69] C.A.R. (Tony) Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, October 1969. 52

[HPvdM03] Joseph Y. Halpern, Riccardo Pucella, and Ron van der Meyden. Revisiting the foundations of authentication logics. Manuscript, 2003. 66, 182

[HS06] Theo Hooghiemstra and Dirk Schravendeel. Burger service nummer werkt. *NRC Handelsblad*, page 7, June 27 2006. 15

[HT07] Marc Hooghe and Wouter Teepe. Party profiles on the web. *New Media & Society*, to appear, 2007. 10

[IN96] Russell Impagliazzo and Moni Naor. Efficient cryptographic schemes provably as secure as subset sum. *Journal of Cryptology*, 9(4):199–216, 1996. 39

[Jac04] Bart Jacobs. Semantics and logic for security protocols. Manuscript, September 2004. 181

[Jac05] Bart Jacobs. Select before you collect. *Ars Aequi*, 54(12):1006–1009, December 2005. 6, 16

[JLS02] Stanislaw Jarecki, Patrick Lincoln, and Vitaly Shmatikov. Negotiated privacy (extended abstract). In *Proceedings of the International Symposium of Software Security (ISSS)*, pages 96–111, 2002. 99

[JY96] Markus Jakobsson and Moti Yung. Proving without knowing: On oblivious, agnostic and blindfolded provers. In N. Koblitz, editor, *Advances in Cryptology - CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 186–200, Berlin, 1996. Springer-Verlag. 107, 113, 114, 116

[KG91] Rajashekar Kailar and Virgil D. Gligor. On belief evolution in authentication protocols. In *Proceedings of the IEEE Computer Security Foundations Workshop IV (CFSW IV)*, pages 103–116, Los Alamitos, 1991. IEEE Computer Society Press. 181

[KM05] Aggelos Kiayias and Antonina Mitrofanova. Testing disjointness of private datasets. In *Proceedings of Financial Cryptography 2005*, 2005. 113, 114, 115

[KM06] Aggelos Kiayias and Antonina Mitrofanova. Syntax-driven private evaluation of quantified membership queries. In *Proceedings of Applied Cryptography and Network Security 2006*, 2006. 109, 111, 114, 115

[Koo03] Barteld Kooi. *Knowledge, Chance and Change*. PhD thesis, Institute for Logic, Language and Communication, 2003. xv

[KP98] Joe Kilian and Erez Petrank. Identity escrow. In H. Krawczyk, editor, *Advances in Cryptology - CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 169–185, Berlin, 1998. Springer-Verlag. 99

[KS92] Bala Kalyanasundaram and Georg Schnitger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992. 118, 188, 189

[KS04] Lea Kissner and Dawn Song. Private and threshold set-intersection. Technical Report CMU-CS-04-182, School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 2004. 111, 114, 116

[Kus97] Eyal Kushilevitz. *Communication Complexity*. Cambridge University Press, 1997. 21

[KW94] Volker Kessler and Gabriele Wedel. AUTLOG – an advanced logic of authentication. In *Proceedings of the 7th Computer Security Foundations Workshop (CSFW'94)*, pages 90–99, Los Alamitos, 1994. IEEE Computer Society Press. 47, 66, 180, 181

[Lip04] Helger Lipmaa. Verifiable homomorphic oblivious transfer and private equality test. In Chi Sung Liah, editor, *Advances in Cryptology - ASIACRYPT 2003*, Lecture Notes in Computer Science, pages 416–433, Berlin, 2004. Springer-Verlag. 22

[LLM05] Sven Laur, Helger Lipmaa, and Taneli Mielikäinen. Private itemset support counting. In Wenbo Mao, Javier Lopez, and Guilin Wang, editors, *Information and Communications Security: 7th International Conference, ICICS 2005*, volume 3783 of *Lecture Notes in Computer Science*, pages 97–111, Berlin / Heidelberg, December 2005. Springer-Verlag. 111, 114, 116

[Low96] Gavin Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In *Tools and Algorithms for the Construction and Analysis of Systems (TACAS)*, volume 1055, pages 147–166, Berlin, 1996. Springer-Verlag. 76, 181

[LP00] Yehuda Lindell and Benny Pinkas. Privacy preserving data mining. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 36–47, Berlin, 2000. Springer-Verlag. 98

[MB93] Wenbo Mao and Colin Boyd. Towards formal analysis of security protocols. In *Proceedings of the IEEE Computer Security Foundations Workshop VI (CFSW VI)*, pages 147–158, Los Alamitos, 1993. IEEE Computer Society Press. 181

[Mer90a] Ralph C. Merkle. A certified digital signature. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 218–238, Berlin, 1990. Springer-Verlag. 42

[Mer90b] Ralph C. Merkle. One way hash functions and DES. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 428–446, Berlin, 1990. Springer-Verlag. 38

[Mil75] Gary L. Miller. Riemann's hypothesis and tests for primality. In *Proceedings of seventh annual ACM symposium on Theory of computing*, pages 234–239, New York, NY, USA, 1975. ACM Press. 21

[MNPS04] Dahlia Malkhi, Noam Nisan, Benny Pinkas, and Yaron Sella. Fairplay — a secure two-party computation system. In *Proceedings of Usenix Security 2004*, 2004. 24

[Mom06] Laurens Mommers. Burger service nummer levert weinig service en veel risico's. *NRC Handelsblad*, page 7, May 30 2006. 15

[Moo05] Chris Mooney. *The Republican War on Science*. Basic Books, 2005. 5

[MV97a] Mastercard and Visa. *The SET Standard Book 1: Business Description, Version 1.0*. SETCO, May 31 1997. 66, 175

[MV97b] Mastercard and Visa. *The SET Standard Book 2: Programmer's Guide, Version 1.0*. SETCO, May 31 1997. 66, 175

[MV97c] Mastercard and Visa. *The SET Standard Book 3: Formal Protocol Definitions, Version 1.0*. SETCO, May 31 1997. 66, 175

[MvdH95] John-Jules Ch. Meyer and Wiebe van der Hoek. *Epistemic Logic for AI and Computer Science*. Cambridge University Press, 1995. 47, 175

[Nat92] National Institute of Standards and Technology (NIST). Proposed federal information processing standard for secure hash standard. *Federal Register*, 57(21):3747–3749, 1992. 40

[Nat02] National Institute of Standards and Technology (NIST). Secure hash standard. *Federal Information Processing Standards*, 180(2):1–71, 2002. 30, 40

[Nat04] National Institute of Standards and Technology (NIST). Secure hash standard, change notice 1. *Federal Information Processing Standards*, 180(2):72–79, 2004. 40

[Nes90] Dan M. Nessett. A Critique of the Burrows, Abadi and Needham Logic. *ACM SIGOPS Operating Systems Review*, 24(2):35–38, April 1990. 47, 66, 181

[NNR99] Moni Naor, Yael Naor, and Omer Reingold. Applied kid cryptography or how to convince your children you are not cheating. *Journal of Craptology*, 0(1), 1999. 26

[NP99] Moni Naor and Benny Pinkas. Oblivious transfer and polynomial evaluation. In *Proceedings of the Thirty-First Annual ACM Symposium on the Theory of Computing*, pages 245–254, New York, 1999. ACM Press. 112, 114, 116

[NPW02] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer-Verlag, 2002. 181

[NY89] Moni Naor and Moti Yung. Universal one-way hash functions and their cryptographic applications. In *Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing. (May 15–17 1989: Seattle, WA, USA)*, pages 33–43, New York, 1989. ACM Press. 35

[Oka93] Tatsuaki Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In E.F. Brickell, editor, *Advances in Cryptology - CRYPTO '92*, volume 740 of *Lecture Notes*

in Computer Science, pages 31–53, Berlin, 1993. Springer-Verlag. 34

[vO93] Paul C. van Oorschot. Extending cryptographic logics of belief to key agreement protocols (extended abstract). In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 232–243, New York, November 1993. ACM Press. 47, 66, 180

[OR94] Martin J. Osborne and Ariel Rubinstein. *A Course in Game Theory*. MIT Press, Cambridge, MA, 1994. 5

[ORSvH95] Sam Owre, John Rushby, Natarajan Shankar, and Friedrich von Henke. Formal verification for fault-tolerant architectures: Prolegomena to the design of PVS. *IEEE Transactions on Software Engineering*, 21(2):107–125, February 1995. 181

[Orw49] George Orwell. *Nineteen Eighty-Four*. Secker & Warburg, London, 1949.

[OYGB04] Christine M. O'Keefe, Ming Yung, Lifang Gu, and Rohan Baxter. Privacy-preserving data linkage protocols. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 94–102, New York, NY, USA, 2004. ACM Press. 115

[Pre93] Bart Preneel. *Analysis and Design of Cryptographic Hash Functions*. PhD thesis, Katholieke Universiteit Leuven, January 1993. 29

[Pre98] Bart Preneel. Cryptographic primitives for information authentication – state of the art. In Bart Preneel and Vincent Rijmen, editors, *State of the Art and Evolution of Computer Security and Industrial Cryptography*, volume 1528 of *Lecture Notes in Computer Science*, pages 50–105, Berlin, 1998. Springer-Verlag. 29

[Pre05] Bart Preneel. Hash functions: past, present and future. Invited Lecture at ASIACRYPT 2005, December 2005. 36

[PvO95] Bart Preneel and Paul C. van Oorschot. MDx-MAC and building fast MACs from hash functions. In D. Coppersmith, editor, *Advances in Cryptology - CRYPTO '95*, volume 963 of *Lecture Notes in Computer Science*, pages 1–14, Berlin, 1995. Springer-Verlag. 128

[QAD00] Catherine Quantin, François-André Allaert, and Liliane Dusserre. Anonymous statistical methods versus cryptographic methods in epidemiology. *International Journal of Medical Informatics*, 60(2):177–183, November 2000. 115, 187

[QBA+98a] Catherine Quantin, Hocine Bouzelat, François-André Allaert, Anne-Marie Benhamiche, Jean Faivre, and Liliane Dusserre. Automatic record hash coding and linkage for epidemiological follow-up data confidentiality. *Methods of Information in Medicine*, 37(3):271–277, September 1998. 115, 187

[QBA+98b] Catherine Quantin, Hocine Bouzelat, François-André Allaert, Anne-Marie Benhamiche, Jean Faivre, and Liliane Dusserre. How to ensure data security of an epidemiological follow-up:quality assessment of an anonymous record linkage procedure. *International Journal of Medical Informatics*, 49(1):117–122, March 1998. 115, 187

[QQQ+90] Jean-Jacques Quisquater, Myriam Quisquater, Muriel Quisquater, Michaël Quisquater, Louis Guillou, Marie Annick Guillou, Gaïd Guil-

lou, Anna Guillou, Gwenolé Guillou, Soazig Guillou, and Tom Berson. How to explain zero-knowledge protocols to your children. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, pages 628–631, Berlin, 1990. Springer-Verlag. 26

[Rab78] Michael O. Rabin. Digitalized signatures. In R.A. DeMillo, R.J. Lipton, D.P. Dobkin, and A.K. Jones, editors, *Foundations of Secure Computation*, pages 155–166. Academic Press, New York, 1978. 42

[Rab80] Michael O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128–138, February 1980. 21

[Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical Report TR-81, Aiken Computation Laboratory, Harvard University, 1981. 22

[Raz92] Alexander A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106(2):385–390, December 1992. 118, 188

[RB01] Erhard Rahm and Philip A. Bernstein. A survey of approaches to automatic schema matching. *VLDB Journal: Very Large Data Bases*, 10(4):334–350, 2001. 82

[RCF04] Pradeep Ravikumar, William W. Cohen, and Stephen E. Fienberg. A secure protocol for computing string distance metrics. In *Proceedings of the Workshop on Privacy and Security Aspects of Data Mining*, pages 40–46, November 2004. 115

[Rei95] Raymond Reiter. On specifying database updates. *Journal of Logic Programming*, 25(1):53–91, 1995. 88

[Riv92] Ronald L. Rivest. The MD5 message-digest algorithm. Technical Report RFC 1321, IETF Network Working Group, 1992. 40

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978. 96, 183, 185

[SC01] Paul Syverson and Iliano Cervesato. The logic of authentication protocols. In R. Focardi and R. Gorrieri, editors, *Foundations of Security Analysis and Design: Tutorial Lectures*, number 2171 in Lecture Notes in Computer Science, pages 63–136. Springer-Verlag, 2001. 48, 54

[Sch96] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, New York, 1996. 19, 43, 56

[Sch98] Claus Peter Schnorr. The black-box model for cryptographic primitives. *Journal of Cryptology*, 11(2):125–140, March 1998. 37

[Sin99] Simon Singh. *The Code Book*. Doubleday Books, 1999. 19

[SOL06] SOLV, Mosho client care & communications. *SOLV FIVE+*. SOLV Attorneys, May 2006. 15

[Spa05] Karin Spaink. *Medische geheimen*. Nijgh & Van Ditmar, 2005. 16

[Sus06] Ron Suskind. *The One Percent Doctrine*. Simon & Schuster, 2006. 5

[SvO94] Paul Syverson and Paul C. van Oorschot. On unifying some cryptographic protocol logics. In *Proceedings of the 1994 IEEE Computer Society Symposium on Research in Security and Privacy*, pages 14–28. IEEE Com-

puter Society Press, May 1994. 47, 51, 66, 180

[SvO96] Paul Syverson and Paul C. van Oorschot. A unified cryptographic protocol logic. Report 5540-227, Center for High Assurance Computer Systems, Naval Research Laboratory (NRL CHACS), 1996. 47, 66, 180

[SWP00] Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *IEEE Symposium on Security and Privacy*, pages 44–55, 2000. 100

[Syv91] Paul Syverson. The value of semantics for the analysis of cryptographic protocols. In *Proceedings of the IEEE Computer Security Foundations Workshop IV (CFSW IV)*, pages 228–229, Los Alamitos, 1991. IEEE Computer Society Press. 180

[Syv93] Paul Syverson. Adding time to a logic of authentication. In *Proceedings of the First ACM Conference on Computer and Communications Security*, pages 97–101, New York, November 1993. ACM Press. 181

[Syv00] Paul Syverson. Towards a strand semantics for authentication logic. In Stephen Brookes, Achim Jung, Michael Mislove, and Andre Scedrov, editors, *Electronic Notes in Theoretical Computer Science*, 20, 2000. 66, 181

[Tee99] Wouter Teepe. Privacy-gerichte workflowanalyse, een verkenning aan de hand van color-x. Master's thesis, Rijksuniversiteit Groningen, December 1999. 10

[Tee04] Wouter Teepe. New protocols for proving knowledge of arbitrary secrets while not giving them away. In Sieuwert van Otterloo, Peter McBurney, Wiebe van der Hoek, and Michael Wooldridge, editors, *Proceedings of the First Knowledge and Games Workshop*, pages 99–116, Liverpool, July 2004. Department of Computer Science, University of Liverpool. 10

[Tee05a] Wouter Teepe. Een classificatie van persoonlijke partijprofielen een analyse vanuit de kennistechnologie. *Samenleving en Politiek*, pages 2–12, March 2005. 10

[Tee05b] Wouter Teepe. Integrity and dissemination control in administrative applications through information designators. *International Journal of Computer Systems Science & Engineering*, 20(5):377–386, September 2005. 10

[Tee05c] Wouter Teepe. Wetenschap kan conflict met Amerika oplossen. *het Financieele Dagblad*, page 7, August 15 2005. 10

[Tee06a] Wouter Teepe. BAN logic is not 'sound', constructing epistemic logics for security is difficult. In Barbara Dunin-Kęplicz and Rineke Verbrugge, editors, *Proceedings of Formal Approaches to Multi-Agent Systems 2006*, pages 79–91, August 2006. 10

[Tee06b] Wouter Teepe. Proving possession of arbitrary secrets while not giving them away, new protocols and a proof in GNY logic. *Synthese*, 149(2):409–443, March 2006. 10

[TH05] Wouter Teepe and Marc Hooghe. Interactief internetgebruik in tijden van verkiezingskoorts een analyse van de gebruikers van "wij kiezen partij voor u" in 2003 en 2004. *Samenleving en Politiek*, pages 73–88, March 2005. 10

[THG98] F. Javier Thayer Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: Why is a security protocol correct? In *IEEE Symposium on Security and Privacy*, 1998. 174, 181

[THG99] F. Javier Thayer Fábrega, Jonathan C. Herzog, and Joshua D. Guttman. Strand spaces: Proving security protocols correct. *Journal of Computer Security*, 7(2-3):191–230, 1999. 174, 181

[Tom88] Martin Tompa. Zero knowledge interactive proofs of knowledge (a digest). In *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge*, pages 1–12, New York, NY, USA, 1988. ACM Press.

[Tsu92] Gene Tsudik. Message authentication with one-way hash functions. In *Proceedings of IEEE INFOCOM 1992*, pages 2055–2059, Los Angeles, 1992. IEEE Computer Society Press. 41

[TvdRO02] Wouter Teepe, Reind P. van de Riet, and Martin Olivier. Workflow analyzed for security and privacy in using databases. In Bhavani Thuraisingham, Reind P. van de Riet, Klaus R. Dittrich, and Zahir Tari, editors, *Data and Application Security, Development and Directions*, volume 73 of *IFIP International Federation for Information Processing*, pages 271–282, Boston, 2002. Springer. 10

[TvdRO03] Wouter Teepe, Reind P. van de Riet, and Martin Olivier. Workflow analyzed for security and privacy in using databases. *Journal of Computer Security*, 11(3):353–363, 2003. 10, 75, 99

[TW87] Martin Tompa and Heather Woll. Random self reducibility and zero knowledge interactive proofs of possession of information. In *Proceedings of the 28th IEEE Symposium on Foundations of Computer Science*, pages 472–482, 1987.

[UG96] Mike Uschold and Michael Grüninger. Ontologies: Principles, methods, and applications. *Knowledge Engineering Review*, 11(2):93–155, June 1996. 100

[WC81] Mark N. Wegman and J. Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981. 35, 115

[WK96] Gabriele Wedel and Volker Kessler. Formal semantics for authentication logics. In Elisa Bertino, Helmut Kurth, Giancarlo Martella, and Emilio Montolivo, editors, *Computer Security — ESORICS 96: 4th European Symposium on Research in Computer Security Rome*, number 1146 in Lecture Notes in Computer Science, pages 219–241, Berlin, 1996. Springer-Verlag. 47, 61, 66, 180, 181

[WSI03] Yodai Watanabe, Junji Shikata, and Hideki Imai. Equivalence between semantic security and indistinguishability against chosen ciphertext attacks. In Y. Desmedt, editor, *Public Key Cryptography - PKC 2003: 6th International Workshop on Practice and Theory in Public Key Cryptography*, volume 2567 of *Lecture Notes in Computer Science*, pages 71–84, Berlin, 2003. Springer-Verlag. 108

[WY05] Xiaoyun Wang and Hongbo Yu. How to break MD5 and other hash functions. In Ronald Cramer, editor, *Advances in Cryptology - EURO-*

CRYPT 2005, volume 3494 of *Lecture Notes in Computer Science*, pages 19–35, Berlin, 2005. Springer-Verlag. 40

[WYY05] Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu. Finding collisions in the full SHA-1. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 17–36, Berlin, 2005. Springer-Verlag. 40

[Yao79] Andrew C. Yao. Some complexity questions related to distributed computing. In *Proceedings of the eleventh annual ACM symposium on Theory of Computing*, pages 209–213, New York, NY, USA, 1979. ACM Press. 21

[Yao82] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science*, pages 160–164, Los Angeles, 1982. IEEE Computer Society Press. 23, 24, 107, 108

[Yao86] Andrew C. Yao. How to generate and exchange secrets. In *Proceedings of the 27th IEEE Symposium on Foundations of Computer Science*, pages 162–167, Los Angeles, 1986. IEEE Computer Society Press. 24, 108