

LINDDUN – privacy enhancing solutions - References (step 6)

- [ABB+04] William Aiello, Steven M. Bellovin, Matt Blaze, Ran Canetti, John Ioannidis, Angelos D. Keromytis, and Omer Reingold. Just fast keying: Key agreement in a hostile internet. *ACM Transactions on Information and System Security (TISSEC)*, 7(2):242–273, 2004.
- [ABC+05] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In *Advances in Cryptology (CRYPTO'05)*, volume 3621 of LNCS, pages 205–222. Springer, 2005.
- [ACK+09] Claudio A. Ardagna, Jan Camenisch, Markulf Kohlweiss, Ronald Leenes, Gregory Neven, Bart Priem, Pierangela Samarati, Dieter Sommer, and Mario Verdicchio. Exploiting cryptography for privacy-enhanced access control: A result of the PRIME project. *Journal of Computer Security*, 2009.
- [AF04] Martín Abadia and Cédric Fournet. Private authentication. *Theoretical Computer Science*, 322(3):427–476, September 2004.
- [AP98] Ross Anderson and Fabien Petitcolas. On the limits of steganography. *IEEE Journal of Selected Areas in Communications*, 16:474–481, 1998.
- [Bac] André Bacard. Anonymous.to: Cypherpunk tutorial. <http://www.andrebacard.com/remail.html>.
- [BC93] Stefan Brands and David Chaum. Distance-bounding protocols (extended abstract). In *Advances in Cryptology (EUROCRYPT'93)*, volume 765 of LNCS, pages 344–359. Springer, 1993.
- [BFK00] Oliver Berthold, Hannes Federrath, and Stefan Köpsell. Web MIXes: A system for anonymous and unobservable Internet access. In *Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability*, LNCS, pages 115–129. Springer, 2000.
- [BGB04] Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM Workshop on Privacy in the Electronic Society*, pages 77–84. ACM New York, NY, USA, 2004.
- [BGS01] A. Back, I. Goldberg, and A. Shostack. Freedom systems 2.1 security issues and analysis. White paper, Zero Knowledge Systems, Inc., May 2001.
- [Cac98] Christian Cachin. On the foundations of oblivious transfer. In *Advances in Cryptology (EUROCRYPT'98)*, pages 361–374. Springer, LNCS 1403, 1998.
- [CD98] J. Camenisch and I. Damgård. Verifiable encryption and applications to group signatures and signature sharing. In *Technical Report RS-98-32, BRICS, Department of Computer Science, University of Aarhus*, Dec. 1998.
- [CF08] Barbara Carminati and Elena Ferrari. Privacy-aware collaborative access control in web-based social networks. In *Proceedings of the 22nd IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC2008)*, pages 81–96. Springer, 2008.
- [CGKS98] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Journal of the ACM*, pages 41–50, 1998.
- [Cha81] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.
- [Cha85] David Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.
- [Cha88] David Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[CL04] Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *Advances in Cryptology (CRYPTO'04)*, volume 3152 of LNCS, pages 56–72. Springer, 2004.

[CPHH02] Sebastian Clauß, Andreas Pfitzmann, Marit Hansen, and Els Van Herreweghen. Privacy-enhancing identity management. The IPTS Report 67, 8-16, September 2002.

[DBPP09] Mina Deng, Tiziano Bianchi, Alessandro Piva, and Bart Preneel. An efficient buyer-seller watermarking protocol based on composite signal representation. In *Proceedings of 11th ACM workshop on Multimedia and Security*, pages 9–18, 2009.

[DMS04] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[FG07] Caroline Fontaine and Fabien Galand. A survey of homomorphic encryption for non-specialists. *EURASIP Journal on Information Security*, pages 41–50, 2007.

[GMPT01] Christos K. Georgiadis, Ioannis Mavridis, George Pangalos, and Roshan K. Thomas. Flexible team-based access control using contexts. In *Proceedings of the Sixth ACM Symposium on Access Control Models and Technologies, SACMAT '01*, pages 21–27. ACM, 2001.

[GRS96] David M. Goldschlag, Michael G. Reed, and Paul F. Syverson. Hiding Routing Information. In *Proceedings of Information Hiding: First International Workshop*, volume 1174 of LNCS, pages 137–150. Springer, May 1996.

[HBC+04] Marit Hansen, Peter Berlich, Jan Camenisch, Sebastian Clauß, Andreas Pfitzmann, and Michael Waidner. Privacy-enhancing identity management. *Information Security Technical Report (ISTR)*, 9(1):35–44, 2004.

[IBM] IBM. Enterprise Privacy Authorization Language (EPAL 1.2). W3C Member Submission, 10 November 2003.

[KM01] Darko Kirovski and Henrique Malvar. Robust covert communication over a public audio channel using spread spectrum. In *Information Hiding*, volume 2137 of LNCS, pages 354–368. Springer, 2001.

[LBW08] Heather Richter Lipford, Andrew Besmer, and Jason Watson. Understanding privacy settings in facebook with an audience view. In *UPSEC*. USENIX Association, 2008.

[LHDL04] Scott Lederer, Jason I. Hong, Anind K. Dey, and James A. Landay. Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, 8:440–454, 2004.

[MGKV06] Ashwin Machanavajjhala, Johannes Gehrke, Daniel Kifer, and Muthuramakrishnan Venkitasubramaniam. I-diversity: Privacy beyond k-anonymity. In *Proceedings of the 22nd International Conference on Data Engineering (ICDE'06)*, page 24, 2006.

[Mixa] Mixmaster. Mixmaster homepage. <http://mixmaster.sourceforge.net/>.

[Mixb] Mixminion. Mixminion official site. <http://mixminion.net/>.

[MNCM03] Ira Moskowitz, Richard E. Newman, Daniel P. Crepeau, and Allen R. Miller. Covert channels and anonymizing networks. In *In Workshop on Privacy in the Electronic Society*, pages 79–88. ACM, 2003.

[MOV97] Alfred J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography, 1997. <http://www.cacr.math.uwaterloo.ca/hac/>.

[Nao02] Moni Naor. Deniable ring authentication. In *Advances in Cryptology (CRYPTO'02)*, volume 2442 of LNCS, pages 481–498. Springer, 2002.

[NN01] Moni Naor and Kobbi Nissim. Communication preserving protocols for secure function evaluation. In *Proceedings of the Thirty-third Annual ACM Symposium on Theory of Computing (STOC '01)*, pages 590–599. ACM, 2001.

[oo] OASIS (oasis.open.org). XACML 3.0 - work in progress, retrieved 09-september-2009. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml#CURRENT.

- [OS05] Rafail Ostrovsky and William E. Skeith. Private searching on streaming data. In *Advances in Cryptology (CRYPTO'05)*, volume 3621 of LNCS, pages 223–240. Springer, 2005.
- [Pin02] B. Pinkas. Cryptographic techniques for privacy preserving data mining. *SIGKDD Explorations*, 4(2):12–19, 2002.
- [PK09] Sameer Patil and Alfred Kobsa. *Privacy Considerations in Awareness Systems: Designing with Privacy in Mind*, chapter 8, pages 187–206. Human–Computer Interaction Series. Springer, June 2009.
- [PPW91] Andreas Pfitzmann, Birgit Pfitzmann, and Michael Waidner. ISDNmixes: Untraceable communication with very small bandwidth overhead. In *Proceedings of the GI/ITG Conference on Communication in Distributed Systems*, pages 451–463, 1991.
- [Rab81] Michael O. Rabin. How to exchange secrets by oblivious transfer. Technical report TR-81, Aiken Computation Laboratory, Harvard University, 1981.
- [RR98] Michael Reiter and Aviel Rubin. Crowds: Anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1), June 1998.
- [STP09] Koen Simoons, Pim Tuyls, and Bart Preneel. Privacy weaknesses in biometric sketches. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, pages 188–203. IEEE Computer Society, 2009.
- [Swe02a] Latanya Sweeney. Achieving k-anonymity privacy protection using generalization and suppression. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):571–588, 2002.
- [Swe02b] Latanya Sweeney. k-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.
- [VBF+04] V.S. Verykios, E. Bertino, I.N. Fovino, L.P. Provenza, Y. Saygin, and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *ACM SIGMOD Record*, 3(1):50–57, Mar. 2004.
- [W3C] W3C. Platform for privacy preferences (p3p) project. <http://www.w3.org/P3P/>.
- [Yao82] Andrew Chi-Chih Yao. Protocols for secure computations. In *Proceedings of Twenty-third IEEE Symposium on Foundations of Computer Science*, pages 160–164, November 1982.