

List of Publications

Christian Cachin

IBM Research
Zurich Research Laboratory
CH-8803 Rüschlikon, Switzerland
cca@zurich.ibm.com

August 16, 2010

Journal Papers

- [1] C. Cachin, I. Keidar, and A. Shraer, “Fork sequential consistency is blocking,” *Information Processing Letters*, vol. 109, pp. 360–364, Mar. 2009.
- [2] C. Cachin, K. Kursawe, and V. Shoup, “Random oracles in Constantinople: Practical asynchronous Byzantine agreement using cryptography,” *Journal of Cryptology*, vol. 18, no. 3, pp. 219–246, 2005. Preliminary version appears in *Proc. 19th ACM Symposium on Principles of Distributed Computing (PODC)*.
- [3] C. Cachin, “An information-theoretic model for steganography,” *Information and Computation*, vol. 192, pp. 41–56, July 2004. Parts of this paper appeared in *Proc. 2nd Workshop on Information Hiding*, Springer, 1998.
- [4] C. Cachin and U. Maurer, “Linking information reconciliation and privacy amplification,” *Journal of Cryptology*, vol. 10, no. 2, pp. 97–110, 1997. Preliminary version appears in *Proc. EUROCRYPT ’94*.
- [5] C. Cachin and H. J. Wiesmann, “PD recognition with knowledge-based preprocessing and neural networks,” *IEEE Transactions on Dielectrics and Electrical Insulation*, vol. 2, no. 4, pp. 578–589, 1995.
- [6] C. Cachin, “Pedagogical pattern selection strategies,” *Neural Networks*, vol. 7, no. 1, pp. 175–181, 1994.

Conference Papers

- [1] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket, “Venus: Verification for untrusted cloud storage,” in *Proc. Workshop on Cloud Computing Security*, ACM, 2010.

- [2] M. Björkqvist, C. Cachin, R. Haas, X.-Y. Hu, A. Kurmus, R. Pawlitzek, and M. Vukolić, “Design and implementation of a key-lifecycle management system,” in *Proc. Financial Cryptography and Data Security (FC 2010)* (R. Sion, ed.), vol. 6052 of *Lecture Notes in Computer Science*, pp. 160–174, Springer, 2010.
- [3] C. Cachin, I. Keidar, and A. Shraer, “Fail-aware untrusted storage,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 494–503, June 2009.
- [4] C. Cachin and N. Chandran, “A secure cryptographic token interface,” in *Proc. Computer Security Foundations Symposium (CSF-22)*, pp. 141–153, IEEE, July 2009.
- [5] C. Cachin and M. Geisler, “Integrity protection for revision control,” in *Proc. Applied Cryptography and Network Security (ACNS)* (M. Abdalla and D. Pointcheval, eds.), vol. 5536 of *Lecture Notes in Computer Science*, pp. 382–399, Springer, 2009.
- [6] C. Cachin, abhi shelat, and A. Shraer, “Efficient fork-linearizable access to untrusted shared memory,” in *Proc. 26th ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 129–138, Aug. 2007.
- [7] R. Pletka and C. Cachin, “Cryptographic security for a high-performance distributed file system,” in *Proc. 24th IEEE Conf. on Mass Storage Systems and Technologies (MSST)*, pp. 227–232, Sept. 2007. Extended version available as IBM Research Report RZ 3661.
- [8] H. V. Ramasamy and C. Cachin, “Parsimonious asynchronous Byzantine-fault-tolerant atomic broadcast,” in *Proc. OPODIS — 9th Intl. Conference on Principles of Distributed Systems* (J. H. Anderson, G. Prencipe, and R. Wattenhofer, eds.), no. 3974 in *Lecture Notes in Computer Science*, pp. 88–102, Springer, 2006.
- [9] M. Backes, C. Cachin, and A. Oprea, “Lazy revocation in cryptographic file systems,” in *Proc. 3rd Intl. IEEE Security in Storage Workshop (SISW)*, pp. 1–11, Dec. 2005.
- [10] M. Backes, C. Cachin, and A. Oprea, “Secure key-updating for lazy revocation,” in *Proc. 11th European Symposium On Research In Computer Security (ESORICS)* (D. Gollmann, J. Meier, and A. Sabelfeld, eds.), no. 4189 in *Lecture Notes in Computer Science*, pp. 327–346, Springer, 2006.
- [11] C. Cachin and S. Tessaro, “Optimal resilience for erasure-coded Byzantine distributed storage,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 115–124, 2006.
- [12] M. Backes and C. Cachin, “Public-key steganography with active attacks,” in *Proc. 2nd Theory of Cryptography Conference (TCC)* (J. Kilian, ed.), vol. 3378 of *Lecture Notes in Computer Science*, pp. 210–226, Springer, 2005.
- [13] C. Cachin and S. Tessaro, “Asynchronous verifiable information dispersal,” in *Proc. 24th Symposium on Reliable Distributed Systems (SRDS)*, pp. 191–202, Oct. 2005.
- [14] C. Cachin and R. Strobl, “Asynchronous group key exchange with failures,” in *Proc. 23rd ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 357–366, July 2004.
- [15] C. Cachin and A. Samar, “Secure distributed DNS,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 423–432, June 2004.

- [16] C. Cachin, “An asynchronous protocol for distributed computation of RSA inverses and its applications,” in *Proc. 22nd ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 153–162, July 2003.
- [17] M. Backes, C. Cachin, and R. Strobl, “Proactive secure message transmission in asynchronous networks,” in *Proc. 22nd ACM Symposium on Principles of Distributed Computing (PODC)*, pp. 223–232, July 2003.
- [18] M. Backes and C. Cachin, “Reliable broadcast in a computational hybrid model with Byzantine faults, crashes, and recoveries,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 37–46, June 2003.
- [19] C. Cachin, “Modeling complexity in secure distributed computing,” in *Future Directions in Distributed Computing* (A. Schiper, A. A. Shvartsman, H. Weatherspoon, and B. Y. Zhao, eds.), vol. 2584 of *Lecture Notes in Computer Science*, pp. 57–61, Springer, 2003.
- [20] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl, “Asynchronous verifiable secret sharing and proactive cryptosystems,” in *Proc. 9th ACM Conference on Computer and Communications Security (CCS)*, pp. 88–97, 2002.
- [21] C. Cachin and J. A. Poritz, “Secure intrusion-tolerant replication on the Internet,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 167–176, June 2002.
- [22] C. Cachin, K. Kursawe, F. Petzold, and V. Shoup, “Secure and efficient asynchronous broadcast protocols (extended abstract),” in *Advances in Cryptology: CRYPTO 2001* (J. Kilian, ed.), vol. 2139 of *Lecture Notes in Computer Science*, pp. 524–541, Springer, 2001. Full version available as Cryptology ePrint Archive, Report 2001/006, <http://eprint.iacr.org/>.
- [23] C. Cachin, “Distributing trust on the Internet,” in *Proc. Intl. Conference on Dependable Systems and Networks (DSN)*, pp. 183–192, June 2001.
- [24] J. Algesheimer, C. Cachin, J. Camenisch, and G. Karjoth, “Cryptographic security for mobile code,” in *Proc. IEEE Symposium on Security and Privacy*, pp. 2–11, May 2001.
- [25] C. Cachin and J. Camenisch, “Optimistic fair secure computation,” in *Advances in Cryptology: CRYPTO 2000* (M. Bellare, ed.), vol. 1880 of *Lecture Notes in Computer Science*, pp. 94–112, Springer, 2000.
- [26] C. Cachin, J. Camenisch, J. Kilian, and J. Müller, “One-round secure computation and secure autonomous mobile agents,” in *Proc. 27th International Colloquium on Automata, Languages and Programming (ICALP)* (U. Montanari, J. P. Rolim, and E. Welzl, eds.), vol. 1853 of *Lecture Notes in Computer Science*, pp. 512–523, Springer, 2000.
- [27] C. Cachin, “Efficient private bidding and auctions with an oblivious third party,” in *Proc. 6th ACM Conference on Computer and Communications Security*, pp. 120–127, 1999.
- [28] C. Cachin, S. Micali, and M. Stadler, “Computationally private information retrieval with polylogarithmic communication,” in *Advances in Cryptology: EUROCRYPT ’99* (J. Stern, ed.), vol. 1592 of *Lecture Notes in Computer Science*, pp. 402–414, Springer, 1999.

- [29] C. Cachin, C. Crépeau, and J. Marcil, “Oblivious transfer with a memory-bounded receiver,” in *Proc. 39th IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 493–502, 1998.
- [30] C. Cachin, “An information-theoretic model for steganography,” in *Information Hiding, 2nd International Workshop* (D. Aucsmith, ed.), vol. 1525 of *Lecture Notes in Computer Science*, pp. 306–318, Springer, 1998. Revised version appears in *Information and Computation*, 2004.
- [31] C. Cachin, “On the foundations of oblivious transfer,” in *Advances in Cryptology: EUROCRYPT ’98* (K. Nyberg, ed.), vol. 1403 of *Lecture Notes in Computer Science*, pp. 361–374, Springer, 1998.
- [32] C. Cachin and U. Maurer, “Unconditional security against memory-bounded adversaries,” in *Advances in Cryptology: CRYPTO ’97* (B. Kaliski, ed.), vol. 1294 of *Lecture Notes in Computer Science*, pp. 292–306, Springer, 1997.
- [33] C. Cachin, “Smooth entropy and Rényi entropy,” in *Advances in Cryptology: EUROCRYPT ’97* (W. Fumy, ed.), vol. 1233 of *Lecture Notes in Computer Science*, pp. 193–208, Springer, 1997.
- [34] C. Cachin, “On-line secret sharing,” in *Cryptography and Coding: 5th IMA Conference, Cirencester, UK* (C. Boyd, ed.), vol. 1025 of *Lecture Notes in Computer Science*, pp. 190–198, Springer, 1995.
- [35] M. Rauterberg and C. Cachin, “Locating the primary attention focus of the user,” in *Vienna Conference on Human Computer Interaction* (T. Grechenig and M. Tscheligi, eds.), vol. 733 of *Lecture Notes in Computer Science*, pp. 129–140, Springer, 1993.

Books and Book Chapters

- [1] C. Cachin, “State machine replication with Byzantine faults,” in *Replication: Theory and Practice* (B. Charron-Bost, F. Pedone, and A. Schiper, eds.), vol. 5959 of *Lecture Notes in Computer Science*, pp. 169–184, Springer, 2010.
- [2] L. Arge, C. Cachin, T. Jurdzinski, and A. Tarlecki, eds., *Proc. 34th International Colloquium on Automata, Languages and Programming (ICALP), Wroclaw, Poland, July 2007*, vol. 4596 of *Lecture Notes in Computer Science*, Springer, 2007.
- [3] C. Cachin and J. Camenisch, eds., *Advances in Cryptology — EUROCRYPT 2004*, vol. 3027 of *Lecture Notes in Computer Science*, Springer, 2004.
- [4] C. Cachin, “Digital steganography,” in *Encyclopedia of Cryptography and Security* (H. C. van Tilborg, ed.), Springer, 2005.

Other Publications

- [1] R. Kapitza, M. Schunter, C. Cachin, K. Stengel, and T. Distler, “Storyboard: Optimistic deterministic multithreading,” in *Proc. 6th Workshop on Hot Topics in System Dependability*, 2010.

- [2] C. Cachin, “From Byzantine-tolerant to intrusion-safe services.” Presented at Workshop on Theory and Practice of Byzantine Fault Tolerance (BFTW3), Sept. 2009.
- [3] C. Cachin, A. Kurmus, and M. Vukolić, “Strict access control in a key-management server.” Presented at 3rd International Workshop on Analysis of Security APIs, July 2009.
- [4] C. Cachin, “Rational protocols.” Presented at Workshop on Open Research Problems in Network Security (iNetSec 2009), Apr. 2009.
- [5] C. Cachin, I. Keidar, and A. Shraer, “Trusting the cloud,” *SIGACT News*, vol. 40, pp. 80–86, June 2009.
- [6] C. Cachin, I. Keidar, and A. Shraer, “Principles of untrusted storage: A new look at consistency conditions,” in *Proc. 27th ACM Symposium on Principles of Distributed Computing (PODC)*, p. 426, Aug. 2008.
- [7] C. Cachin, I. Keidar, and A. Shraer, “Improving efficiency and enhancing concurrency of untrusted storage,” in *Proc. 6th USENIX Conference on File and Storage Technologies (FAST), Work-in-Progress Report*, Feb. 2008.
- [8] C. Cachin, “Cryptographic methods for protecting storage systems.” Tutorial, presented at 6th USENIX Conference on File and Storage Technologies (FAST ’08), at 24th IEEE Conf. on Mass Storage Systems and Technologies (MSST 2007), and at 13th ACM Conference on Computer and Communications Security (CCS 2006), 2008.
- [9] P. Veríssimo, N. F. Neves, C. Cachin, J. Poritz, D. Powell, Y. Deswarte, R. Stroud, and I. Welch, “Intrusion-tolerant middleware,” *IEEE Security & Privacy Magazine*, vol. 4, pp. 88–102, July 2006.
- [10] C. Cachin and S. Tessaro, “Brief Announcement: Optimal resilience for erasure-coded Byzantine distributed storage,” in *Proc. 19th International Conference on Distributed Computing (DISC), Cracow, Poland* (P. Fraigniaud, ed.), vol. 3724 of *Lecture Notes in Computer Science*, pp. 497–498, Springer, 2005.
- [11] C. Cachin and S. Tessaro, “Brief Announcement: Asynchronous verifiable information dispersal,” in *Proc. 19th International Conference on Distributed Computing (DISC), September 26-29, 2005, Cracow, Poland* (P. Fraigniaud, ed.), vol. 3724 of *Lecture Notes in Computer Science*, pp. 503–504, Springer, 2005.
- [12] C. Cachin, “Hashing a source with an unknown probability distribution.” Manuscript (Abstract in Proc. 1998 IEEE International Symposium on Information Theory, Boston), 1998.
- [13] C. Cachin and U. Maurer, “Smoothing probability distributions and smooth entropy.” Manuscript (Abstract in Proc. 1997 IEEE International Symposium on Information Theory, Ulm), 1997.
- [14] C. Cachin, *Entropy Measures and Unconditional Security in Cryptography*, vol. 1 of *ETH Series in Information Security and Cryptography*. Konstanz, Germany: Hartung-Gorre Verlag, 1997. ISBN 3-89649-185-7 (Reprint of Ph.D. dissertation No. 12187, ETH Zürich, Ref. Prof. U. Maurer, Co-Ref. Prof. J.L. Massey).

- [15] C. Cachin and U. Maurer, “Sicherheit im Internet: Illusion oder Realität?,” *INFORMATIK / INFORMATIQUE*, vol. 2, no. 2, pp. 18–23, 1995.

Recent and Unpublished Work

- [1] C. Cachin, “Yet another visit to Paxos,” Research Report RZ 3754, IBM Research, Nov. 2009.