Compressed Σ-protocol theory

Attema, T.

BIBLIOGRAPHY

Bibliography

[AC20] Thomas Attema and Ronald Cramer. "Compressed Σ-Protocol Theory and Practical Application to Plug & Play Secure Algorithmics." In: *CRYPTO*. Vol. 12172. Lecture Notes in Computer Science. Springer, 2020, pp. 513–543 (Cited on pages 60, 107, 123, 148, 217).

[ACF21] Thomas Attema, Ronald Cramer, and Serge Fehr. "Compressing Proofs of k-out-of-n Partial Knowledge." In: *CRYPTO*. Vol. 12828. Lecture Notes in Computer Science. Springer, 2021, pp. 65–91 (Cited on pages 60, 108, 118).

[ACK21] Thomas Attema, Ronald Cramer, and Lisa Kohl. "A Compressed Σ-Protocol Theory for Lattices." In: *CRYPTO*. Vol. 12826. Lecture Notes in Computer Science. Springer, 2021, pp. 549–579 (Cited on pages 44, 60, 123, 148, 190).

[ACR21] Thomas Attema, Ronald Cramer, and Matthieu Rambaud. "Compressed Σ-Protocols for Bilinear Group Arithmetic Circuits and Application to Logarithmic Transparent Threshold Signatures." In: *ASIACRYPT*. Vol. 13093. Lecture Notes in Computer Science. Springer, 2021, pp. 526–556 (Cited on pages 123, 218, 227).

[ACX21] Thomas Attema, Ronald Cramer, and Chaoping Xing. "A Note on Short Invertible Ring Elements and Applications to Cyclotomic and Trinomials Number Fields." In: *Mathematical Cryptology* (2021), pp. 45–70 (Cited on pages 87, 137, 167).

[ADD+19] Ittai Abraham, Srinivas Devadas, Danny Dolev, Kartik Nayak, and Ling Ren. "Synchronous Byzantine Agreement with Expected $\mathcal{O}(1)$ Rounds, Expected $\mathcal{O}(n^2)$ Communication, and Optimal Resilience." In: *Financial Cryptography and Data Security (FC)*. Vol. 11598. Lecture Notes in Computer Science. Springer, 2019, pp. 320–334 (Cited on page 218).

[AF22] Thomas Attema and Serge Fehr. "Parallel Repetition of $(k_1, \ldots, k_\mu)$-Special-Sound Multi-Round Interactive Proofs." In: *CRYPTO*. Vol. 13507. Lecture Notes in Computer Science. Springer, 2022, pp. 415–443 (Cited on page 148).

[AFG+10] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. "Structure-Preserving Signatures and Commitments to Group Elements." In: *CRYPTO*. Vol. 6223. Lecture Notes in Computer Science. Springer, 2010, pp. 209–236 (Cited on page 125).

[AFG+16] Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo. "Structure-Preserving Signatures and Commitments to Group Elements." In: *Journal of Cryptology* 29.2 (2016), pp. 363–421 (Cited on page 227).

[AFK22] Thomas Attema, Serge Fehr, and Michael Klooß. "Fiat-Shamir Transformation of Multi-Round Interactive Proofs." In: *Theory of Cryptography Conference (TCC)*. Vol. 13747. Lecture Notes in Computer Science. Springer, 2022, pp. 113–142 (Cited on pages 148, 190, 211).

[AHI+17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. "Ligero: Lightweight Sublinear Arguments without a Trusted Setup." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2017, pp. 2087–2104 (Cited on page 187).

[Ajt96] Miklós Ajtai. "Generating Hard Instances of Lattice Problems (Extended Abstract)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1996, pp. 99–108 (Cited on pages 37, 136).

[AL21] Martin R. Albrecht and Russell W. F. Lai. "Subtractive Sets over Cyclotomic Rings - Limits of Schnorr-Like Arguments over Lattices." In: *CRYPTO*. Vol. 12826. Lecture Notes in Computer Science. Springer, 2021, pp. 519–548 (Cited on pages 17, 150).

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. "Proof Verification and the Hardness of Approximation Problems." In: *Journal of the ACM* 45.3 (1998), pp. 501–555 (Cited on page 9).

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra*. Addison-Wesley-Longman, 1969. ISBN: 978-0-201-40751-8 (Cited on page 85).

[AMS19] Ittai Abraham, Dahlia Malkhi, and Alexander Spiegelman. "Asymptotically Optimal Validated Asynchronous Byzantine Agreement." In: *ACM Symposium on Principles of Distributed Computing (PODC)*. ACM, 2019, pp. 337–346 (Cited on page 218).

[APS15] Martin R. Albrecht, Rachel Player, and Sam Scott. "On the Concrete Hardness of Learning With Errors." In: *Journal of Mathematical Cryptology* 9.3 (2015), pp. 169–203 (Cited on page 38).

[AS92] Sanjeev Arora and Shmuel Safra. "Probabilistic Checking of Proofs; A New Characterization of NP." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1992, pp. 2–13 (Cited on page 9).

[Bab85] László Babai. "Trading Group Theory for Randomness." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1985, pp. 421–429 (Cited on pages 8, 255, 263).

[BBB+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell. "Bulletproofs: Short Proofs for Confidential Transactions and More." In: *IEEE Symposium on Security and Privacy (S&P)*. IEEE Computer Society, 2018, pp. 315–334 (Cited on pages 11, 17, 59, 62, 89, 132, 187, 256, 264).

[BBC+18] Carsten Baum, Jonathan Bootle, Andrea Cerulli, Rafaël del Pino, Jens Groth, and Vadim Lyubashevsky. "Sub-Linear Lattice-Based Zero-Knowledge Arguments for Arithmetic Circuits." In: *CRYPTO*. Vol. 10992. Lecture Notes in Computer Science. Springer, 2018, pp. 669–699 (Cited on page 136).

[BCC+16] Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit. "Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting." In: *EUROCRYPT*. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 327–357 (Cited on pages 11, 17, 59, 62, 132, 150, 167, 187, 256, 264).

[BCK+14] Fabrice Benhamouda, Jan Camenisch, Stephan Krenn, Vadim Lyubashevsky, and Gregory Neven. "Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures." In: *ASIACRYPT*. Vol. 8873. Lecture Notes in Computer Science. Springer, 2014, pp. 551–572 (Cited on page 134).

[BCP+14] Nir Bitansky, Ran Canetti, Omer Paneth, and Alon Rosen. "On the Existence of Extractable One-Way Functions." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 2014, pp. 505–514 (Cited on pages 15, 128).

[BCR+19] Eli Ben-Sasson, Alessandro Chiesa, Michael Riabzev, Nicholas Spooner, Madars Virza, and Nicholas P. Ward. "Aurora: Transparent Succinct Arguments for R1CS." In: *EUROCRYPT*. Vol. 11476. Lecture Notes in Computer Science. Springer, 2019, pp. 103–128 (Cited on page 187).

[BCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. "Interactive Oracle Proofs." In: *Theory of Cryptography Conference (TCC)*. Vol. 9986. Lecture Notes in Computer Science. 2016, pp. 31–60 (Cited on pages 187, 188).

[BDL+18] Carsten Baum, Ivan Damgård, Vadim Lyubashevsky, Sabine Oechsner, and Chris Peikert. "More Efficient Commitments from Structured Lattice Assumptions." In: *International Conference on Security and Cryptography for Networks (SCN)*. Vol. 11035. Lecture Notes in Computer Science. Springer, 2018, pp. 368–385 (Cited on pages 136, 137).

[Bel53] Giovan Battista Bellaso. *La Cifra del Sig.* Venice (Italy), 1553 (Cited on page 4).

[BFS20] Benedikt Bünz, Ben Fisch, and Alan Szepieniec. "Transparent SNARKs from DARK Compilers." In: *EUROCRYPT*. Vol. 12105. Lecture Notes in Computer Science. Springer, 2020, pp. 677–706 (Cited on pages 17, 36, 132, 136).

[BG92] Mihir Bellare and Oded Goldreich. "On Defining Proofs of Knowledge." In: *CRYPTO*. Vol. 740. Lecture Notes in Computer Science. Springer, 1992, pp. 390–420 (Cited on pages 10, 42).

[BGG90] Mihir Bellare, Oded Goldreich, and Shafi Goldwasser. "Randomness in Interactive Proofs." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1990, pp. 563–572 (Cited on page 169).

[BGM+05] Lucas Ballard, Matthew Green, Breno de Medeiros, and Fabian Monrose. "Correlation-Resistant Storage via Keyword-Searchable Encryption." In: *IACR Cryptology ePrint Archive* (2005). IACR ePrint: 2005/417 (Cited on page 35).

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation (Extended Abstract)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1988, pp. 1–10 (Cited on page 7).

[BHR+21] Alexander R. Block, Justin Holmgren, Alon Rosen, Ron D. Rothblum, and Pratik Soni. "Time- and Space-Efficient Arguments from Groups of Unknown Order." In: *CRYPTO*. Vol. 12828. Lecture Notes in Computer Science. Springer, 2021, pp. 123–152 (Cited on pages 36, 132, 136).

[BIN97] Mihir Bellare, Russell Impagliazzo, and Moni Naor. "Does Parallel Repetition Lower the Error in Computationally Sound Protocols?" In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1997, pp. 374–383 (Cited on pages 17, 18, 167).

[BKL+15] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. "Efficient Zero-Knowledge Proofs for Commitments from Learning with Errors over Rings." In: *European Symposium on Research in Computer Security (ESORICS)*. Vol. 9326. Lecture Notes in Computer Science. Springer, 2015, pp. 305–325 (Cited on page 136).

[BL02] Boaz Barak and Yehuda Lindell. "Strict Polynomial-Time in Simulation and Extraction." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 2002, pp. 484–493 (Cited on pages 147, 151, 191).

[BLN+20] Jonathan Bootle, Vadim Lyubashevsky, Ngoc Khanh Nguyen, and Gregor Seiler. "A Non-PCP Approach to Succinct Quantum-Safe Zero-Knowledge." In: *CRYPTO*. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 441–469 (Cited on pages 17, 190).

[BLS01] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing." In: *ASIACRYPT*. Vol. 2248. Lecture Notes in Computer Science. Springer, 2001, pp. 514–532 (Cited on pages 227, 230, 232).

[BLS04] Dan Boneh, Ben Lynn, and Hovav Shacham. "Short Signatures from the Weil Pairing." In: *Journal of Cryptology* 17.4 (2004), pp. 297–319 (Cited on pages 227, 230, 232).

[Blu81] Manuel Blum. "Coin Flipping by Telephone." In: *CRYPTO*. UC Santa Barbara, Department of Electrical and Computer Engineering (ECE) Report No 82-04, 1981, pp. 11–15 (Cited on page 7).

[BN06] Mihir Bellare and Gregory Neven. "Multi-Signatures in the Plain Public-Key Model and a General Forking Lemma." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2006, pp. 390–399 (Cited on pages 151, 191).

[Bol03] Alexandra Boldyreva. "Threshold Signatures, Multisignatures and Blind Signatures Based on the Gap-Diffie-Hellman-Group Signature Scheme." In: *Practice and Theory of Public-Key Cryptography (PKC)*. Vol. 2567. Lecture Notes in Computer Science. Springer, 2003, pp. 31–46 (Cited on pages 228, 229).

[Bon98] Dan Boneh. "The Decision Diffie-Hellman Problem." In: *Algorithmic Number Theory Symposium (ANTS)*. Vol. 1423. Lecture Notes in Computer Science. Springer, 1998, pp. 48–63 (Cited on page 35).

[BP97] Niko Baric and Birgit Pfitzmann. "Collision-Free Accumulators and Fail-Stop Signature Schemes without Trees." In: *EUROCRYPT*. Vol. 1233. Lecture Notes in Computer Science. Springer, 1997, pp. 480–494 (Cited on page 36).

[BR93] Mihir Bellare and Phillip Rogaway. "Random Oracles are Practical: A Paradigm for Designing Efficient Protocols." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 1993, pp. 62–73 (Cited on page 47).

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. "Multiparty Unconditionally Secure Protocols (Extended Abstract)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1988, pp. 11–19 (Cited on page 7).

[CCH+19] Ran Canetti, Yilei Chen, Justin Holmgren, Alex Lombardi, Guy N. Rothblum, Ron D. Rothblum, and Daniel Wichs. "Fiat-Shamir: From Practice to Theory." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 2019, pp. 1082–1090 (Cited on pages 19, 188).

[CD98] Ronald Cramer and Ivan Damgård. "Zero-Knowledge Proofs for Finite Field Arithmetic; or: Can Zero-Knowledge be for Free?" In: *CRYPTO*. Vol. 1462. Lecture Notes in Computer Science. Springer, 1998, pp. 424–441 (Cited on pages 10, 11, 60, 61, 255, 263).

[CDG87] David Chaum, Ivan Damgård, and Jeroen van de Graaf. "Multiparty Computations Ensuring Privacy of Each Party's Input and Correctness of the Result." In: *CRYPTO*. Vol. 293. Lecture Notes in Computer Science. Springer, 1987, pp. 87–119 (Cited on page 7).

[CDM00] Ronald Cramer, Ivan Damgård, and Ueli M. Maurer. "General Secure Multi-party Computation from any Linear Secret-Sharing Scheme." In: *EUROCRYPT*. Vol. 1807. Lecture Notes in Computer Science. Springer, 2000, pp. 316–334 (Cited on pages 107, 256, 264).

[CDN15] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015. ISBN: 9781107043053 (Cited on pages 31, 52, 53, 109, 119, 256, 264).

[CDP12] Ronald Cramer, Ivan Damgård, and Valerio Pastro. "On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations." In: *International Conference on Information Theoretic Security (ICITS)*. Vol. 7412. Lecture Notes in Computer Science. Springer, 2012, pp. 62–79 (Cited on pages 13, 14, 107–110, 112, 218, 256, 264).

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols." In: *CRYPTO*. Vol. 839. Lecture Notes in Computer Science. Springer, 1994, pp. 174–187 (Cited on pages 10, 15, 107, 114–116, 119).

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. "The Random Oracle Methodology, Revisited." In: *Journal of the ACM* 51.4 (2004), pp. 557–594 (Cited on page 19).

[CHK+10] Sanjit Chatterjee, Darrel Hankerson, Edward Knapp, and Alfred Menezes. "Comparing Two Pairing-Based Aggregate Signature Schemes." In: *Designs, Codes and Cryptography* 55.2-3 (2010), pp. 141–167 (Cited on page 231).

[CHR+16] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. "From 5-Pass MQ-Based Identification to MQ-Based Signatures." In: *ASIACRYPT*. Vol. 10032. Lecture Notes in Computer Science. 2016, pp. 135–165 (Cited on page 172).

[Chu36] Alonzo Church. "An Unsolvable Problem of Elementary Number Theory." In: *American Journal of Mathematics* 58.2 (1936), pp. 345–363 (Cited on page 4).

[CKS00] Christian Cachin, Klaus Kursawe, and Victor Shoup. "Random Oracles in Constantipole: Practical Asynchronous Byzantine Agreement using Cryptography (Extended Abstract)." In: *ACM Symposium on Principles of Distributed Computing (PODC)*. ACM, 2000, pp. 123–132 (Cited on page 218).

[CKS05] Christian Cachin, Klaus Kursawe, and Victor Shoup. "Random Oracles in Constantinople: Practical Asynchronous Byzantine Agreement using Cryptography." In: *Journal of Cryptology* 18.3 (2005), pp. 219–246 (Cited on page 218).

[CL10] Kai-Min Chung and Feng-Hao Liu. "Parallel Repetition Theorems for Interactive Arguments." In: *Theory of Cryptography Conference (TCC)*. Vol. 5978. Lecture Notes in Computer Science. Springer, 2010, pp. 19–36 (Cited on pages 18, 167).

[CMS19] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. "Succinct Arguments in the Quantum Random Oracle Model." In: *Theory of Cryptography Conference (TCC)*. Vol. 11892. Lecture Notes in Computer Science. Springer, 2019, pp. 1–29 (Cited on page 188).

[Coo71] Stephen A. Cook. "The Complexity of Theorem-Proving Procedures." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1971, pp. 151–158 (Cited on page 8).

[CP15] Kai-Min Chung and Rafael Pass. "Tight Parallel Repetition Theorems for Public-Coin Arguments using KL-Divergence." In: *Theory of Cryptography Conference (TCC)*. Vol. 9015. Lecture Notes in Computer Science. Springer, 2015, pp. 229–246 (Cited on pages 18, 167–170).

[CR79] Stephen A. Cook and Robert A. Reckhow. "The Relative Efficiency of Propositional Proof Systems." In: *Journal of Symbolic Logic* 44.1 (1979), pp. 36–50 (Cited on page 8).

[Cra96] Ronald Cramer. "Modular Design of Secure yet Practical Cryptographic Protocols." PhD thesis. CWI and University of Amsterdam, 1996 (Cited on pages 10, 16, 42, 59–61, 149, 151, 152, 255, 257, 263, 265).

[Dam10] Ivan Damgård. *On Σ-Protocols*. Lecture Notes, Aarhus University, Department of Computer Science. 2010 (Cited on page 149).

[Dam93] Ivan Damgård. "Interactive Hashing can Simplify Zero-Knowledge Protocol Design without Computational Assumptions (Extended Abstract)." In: *CRYPTO*. Vol. 773. Lecture Notes in Computer Science. Springer, 1993, pp. 100–109 (Cited on page 45).

[DF02] Ivan Damgård and Eiichiro Fujisaki. "A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order." In: *ASIACRYPT*. Vol. 2501. Lecture Notes in Computer Science. Springer, 2002, pp. 125–142 (Cited on page 132).

[DFM+19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model." In: *CRYPTO*. Vol. 11693. Lecture Notes in Computer Science. Springer, 2019, pp. 356–383 (Cited on page 50).

[DGO+95] Ivan Damgård, Oded Goldreich, Tatsuaki Okamoto, and Avi Wigderson. "Honest Verifier vs Dishonest Verifier in Public Coin Zero-Knowledge Proofs." In: *CRYPTO*. Vol. 963. Lecture Notes in Computer Science. Springer, 1995, pp. 325–338 (Cited on page 45).

[DH76] Whitfield Diffie and Martin E. Hellman. "New Directions in Cryptography." In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654 (Cited on page 6).

[Din07] Irit Dinur. "The PCP Theorem by Gap Amplification." In: *Journal of the ACM* 54.3 (2007), 12–es (Cited on page 9).

[DJM+12] Yevgeniy Dodis, Abhishek Jain, Tal Moran, and Daniel Wichs. "Counterexamples to Hardness Amplification Beyond Negligible." In: *Theory of Cryptography Conference (TCC)*. Vol. 7194. Lecture Notes in Computer Science. Springer, 2012, pp. 476–493 (Cited on pages 168, 170).

[DKL+18] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme." In: *Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 2018.1 (2018), pp. 238–268 (Cited on page 140).

[DOT+21] Ivan Damgård, Claudio Orlandi, Akira Takahashi, and Mehdi Tibouchi. "Two-Round n-out-of-n and Multi-Signatures and Trapdoor Commitment from Lattices." In: *Practice and Theory of Public-Key Cryptography (PKC)*. Vol. 12710. Lecture Notes in Computer Science. Springer, 2021, pp. 99–130 (Cited on page 78).

[ElG84] Taher ElGamal. "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms." In: *CRYPTO*. Vol. 196. Lecture Notes in Computer Science. Springer, 1984, pp. 10–18 (Cited on page 126).

[ESS+19] Muhammed F. Esgin, Ron Steinfeld, Amin Sakzad, Joseph K. Liu, and Dongxi Liu. "Short Lattice-Based One-out-of-Many Proofs and Applications to Ring Signatures." In: *Applied Cryptography and Network Security (ACNS)*. Vol. 11464. Lecture Notes in Computer Science. Springer, 2019, pp. 67–88 (Cited on page 38).

[FFS88] Uriel Feige, Amos Fiat, and Adi Shamir. "Zero-Knowledge Proofs of Identity." In: *Journal of Cryptology* 1.2 (1988), pp. 77–94 (Cited on page 10).

[FO97] Eiichiro Fujisaki and Tatsuaki Okamoto. "Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations." In: *CRYPTO*. Vol. 1294. Lecture Notes in Computer Science. Springer, 1997, pp. 16–30 (Cited on page 132).

[FS86] Amos Fiat and Adi Shamir. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems." In: *CRYPTO*. Vol. 263. Lecture Notes in Computer Science. Springer, 1986, pp. 186–194 (Cited on pages 10, 12, 18, 45, 50, 61, 228).

[Gál95] Anna Gál. "Combinatorial Methods in Boolean Function Complexity." PhD thesis. University of Chicago, 1995 (Cited on page 119).

[Gen09] Craig Gentry. "Fully Homomorphic Encryption using Ideal Lattices." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 2009, pp. 169–178 (Cited on page 7).

[GH98] Oded Goldreich and Johan Håstad. "On the Complexity of Interactive Proofs with Bounded Communication." In: *Information Processing Letters* 67.4 (1998), pp. 205–214 (Cited on page 9).

[GK96] Oded Goldreich and Ariel Kahan. "How to Construct Constant-Round Zero-Knowledge Proof Systems for NP." In: *Journal of Cryptology* 9.3 (1996), pp. 167–190 (Cited on page 167).

[GM82] Shafi Goldwasser and Silvio Micali. "Probabilistic Encryption and How to Play Mental Poker Keeping Secret All Partial Information." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1982, pp. 365–377 (Cited on page 7).

[GMR85] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1985, pp. 291–304 (Cited on pages 8–10, 39, 255, 263).

[GMW86] Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design (Extended Abstract)." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1986, pp. 174–187 (Cited on pages 9, 11).

[GMW87] Oded Goldreich, Silvio Micali, and Avi Wigderson. "How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1987, pp. 218–229 (Cited on page 7).

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs that Yield Nothing But Their Validity for All Languages in NP Have Zero-Knowledge Proof Systems." In: *Journal of the ACM* 38.3 (1991), pp. 691–729 (Cited on page 9).

[Göd31] Kurt Gödel. "Über Formal Unentscheidbare Sätze der Principia Mathematica und Verwandter Systeme I." In: *Monatshefte für Mathematik und Physik* 38.1 (1931), pp. 173–198 (Cited on page 3).

[Gol01] Oded Goldreich. *The Foundations of Cryptography - Volume 1: Basic Techniques*. Cambridge University Press, 2001. ISBN: 0-521-79172-3 (Cited on page 167).

[Gol04] Oded Goldreich. *The Foundations of Cryptography - Volume 2: Basic Applications*. Cambridge University Press, 2004. ISBN: 0-521-83084-2 (Cited on pages 40–42, 164).

[Gol98] Oded Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Vol. 17. Algorithms and Combinatorics. Springer, 1998 (Cited on page 169).

[GPS08] Steven D. Galbraith, Kenneth G. Paterson, and Nigel P. Smart. "Pairings for Cryptographers." In: *Discrete Applied Mathematics* 156.16 (2008), pp. 3113–3121 (Cited on pages 36, 231).

[GQ88] Louis C. Guillou and Jean-Jacques Quisquater. "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory." In: *EUROCRYPT*. Vol. 330. Lecture Notes in Computer Science. Springer, 1988, pp. 123–128 (Cited on page 10).

[Gro03] Jens Groth. "A Verifiable Secret Shuffle of Homomorphic Encryptions." In: *Practice and Theory of Public-Key Cryptography (PKC)*. Vol. 2567. Lecture Notes in Computer Science. Springer, 2003, pp. 145–160 (Cited on page 74).

[Gro05] Jens Groth. "A Verifiable Secret Shuffle of Homomorphic Encryptions." In: *IACR Cryptology ePrint Archive* (2005). IACR ePrint: 2005/246 (Cited on page 74).

[Gro10] Jens Groth. "Short Pairing-Based Non-Interactive Zero-Knowledge Arguments." In: *ASIACRYPT*. Vol. 6477. Lecture Notes in Computer Science. Springer, 2010, pp. 321–340 (Cited on pages 129, 131).

[GS86] Shafi Goldwasser and Michael Sipser. "Private Coins versus Public Coins in Interactive Proof Systems." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1986, pp. 59–68 (Cited on page 9).

[GT21] Ashrujit Ghoshal and Stefano Tessaro. "Tight State-Restoration Soundness in the Algebraic Group Model." In: *CRYPTO*. Vol. 12827. Lecture Notes in Computer Science. Springer, 2021, pp. 64–93 (Cited on pages 19, 188).

[Hai09] Iftach Haitner. "A Parallel Repetition Theorem for Any Interactive Argument." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 2009, pp. 241–250 (Cited on page 18).

[HBH+20] Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox. *Zcash Protocol Specification - Version 2020.1.7*. Aug. 30, 2020 (Cited on page 227).

[HKR19] Max Hoffmann, Michael Klooß, and Andy Rupp. "Efficient Zero-Knowledge Arguments in the Discrete Log Setting, Revisited." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2019, pp. 2093–2110 (Cited on pages 17, 150).

[HL10] Carmit Hazay and Yehuda Lindell. *Efficient Secure Two-Party Protocols - Techniques and Constructions*. Information Security and Cryptography. Springer, 2010. ISBN: 978-3-642-14302-1 (Cited on pages 41, 42, 149, 164).

[HM98] Shai Halevi and Silvio Micali. "More on Proofs of Knowledge." In: *IACR Cryptology ePrint Archive* (1998). IACR ePrint: 1998/015 (Cited on page 42).

[HPW+10] Johan Håstad, Rafael Pass, Douglas Wikström, and Krzysztof Pietrzak. "An Efficient Parallel Repetition Theorem." In: *Theory of Cryptography Conference (TCC)*. Vol. 5978. Lecture Notes in Computer Science. Springer, 2010, pp. 1–18 (Cited on pages 18, 167).

[ILL89] Russell Impagliazzo, Leonid A. Levin, and Michael Luby. "Pseudo-Random Generation from One-Way Functions (Extended Abstracts)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1989, pp. 12–24 (Cited on page 138).

[JT20] Joseph Jaeger and Stefano Tessaro. "Expected-Time Cryptography: Generic Techniques and Applications to Concrete Soundness." In: *Theory of Cryptography Conference (TCC)*. Vol. 12552. Lecture Notes in Computer Science. Springer, 2020, pp. 414–443 (Cited on pages 17, 150).

[Kas63] F.W. Kasiski. *Die Geheimschriften und die Dechiffrir-Kunst: Mit Besonderer Berücksichtigung der Deutschen und der Französischen Sprache*. E. S. Mittler und Sohn, 1863 (Cited on page 5).

[Kil92] Joe Kilian. "A Note on Efficient Zero-Knowledge Proofs and Arguments (Extended Abstract)." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 1992, pp. 723–732 (Cited on pages 9, 11).

[Lan02] Serge Lang. *Algebra*. 3rd ed. Graduate Texts in Mathematics. Originally published by Addison-Wesley (1993). Springer New York, NY, 2002. ISBN: 978-0-387-95385-4 (Cited on page 27).

[Lev73] Leonid Anatolevich Levin. "Universal Sequential Search Problems (in Russian)." In: *Problemy Peredachi Informatsii* 9.3 (1973), pp. 115–116 (Cited on page 8).

[Lin01] Yehuda Lindell. "Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation." In: *CRYPTO*. Vol. 2139. Lecture Notes in Computer Science. Springer, 2001, pp. 171–189 (Cited on page 167).

[Lin03] Yehuda Lindell. "Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation." In: *Journal of Cryptology* 16.3 (2003), pp. 143–184 (Cited on page 167).

[LL93] Arjen K. Lenstra and Hendrik W. Lenstra. *The Development of the Number Field Sieve*. Springer Berlin, Heidelberg, 1993. ISBN: 978-3-540-57013-4 (Cited on page 6).

[LM06] Vadim Lyubashevsky and Daniele Micciancio. "Generalized Compact Knapsacks are Collision Resistant." In: *International Colloquium on Automata, Languages, and Programming (ICALP)*. Vol. 4052. Lecture Notes in Computer Science. Springer, 2006, pp. 144–155 (Cited on page 37).

[LM18] Julian Loss and Tal Moran. "Combining Asynchronous and Synchronous Byzantine Agreement: The Best of Both Worlds." In: *IACR Cryptology ePrint Archive* (2018). IACR ePrint: 2018/235 (Cited on page 218).

[LMR19] Russell W. F. Lai, Giulio Malavolta, and Viktoria Ronge. "Succinct Arguments for Bilinear Group Arithmetic: Practical Structure-Preserving Cryptography." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2019, pp. 2057–2074 (Cited on pages 125–127, 226, 227).

[LS15] Adeline Langlois and Damien Stehlé. "Worst-Case to Average-Case Reductions for Module Lattices." In: *Designs, Codes and Cryptography* 75.3 (2015), pp. 565–599 (Cited on page 37).

[LS18] Vadim Lyubashevsky and Gregor Seiler. "Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-Based Zero-Knowledge Proofs." In: *EUROCRYPT*. Vol. 10820. Lecture Notes in Computer Science. Springer, 2018, pp. 204–224 (Cited on pages 87, 137, 167).

[Lyu09] Vadim Lyubashevsky. "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures." In: *ASIACRYPT*. Vol. 5912. Lecture Notes in Computer Science. Springer, 2009, pp. 598–616 (Cited on page 74).

[Lyu12] Vadim Lyubashevsky. "Lattice Signatures without Trapdoors." In: *EUROCRYPT*. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 738–755 (Cited on page 74).

[MBK+19] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. "Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings." In: *ACM Conference on Computer and Communications Security (CCS)*. ACM, 2019, pp. 2111–2128 (Cited on page 17).

[MR09] Daniele Micciancio and Oded Regev. "Lattice-Based Cryptography." In: *Post-Quantum Cryptography*. Springer Berlin Heidelberg, 2009, pp. 147–191 (Cited on page 38).

[MV03] Daniele Micciancio and Salil P. Vadhan. "Statistical Zero-Knowledge Proofs with Efficient Provers: Lattice Problems and More." In: *CRYPTO*. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 282–298 (Cited on page 10).

[Nao03] Moni Naor. "On Cryptographic Assumptions and Challenges." In: *CRYPTO*. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 96–109 (Cited on pages 15, 128).

[Oka92] Tatsuaki Okamoto. "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes." In: *CRYPTO*. Vol. 740. Lecture Notes in Computer Science. Springer, 1992, pp. 31–53 (Cited on page 10).

[OVY93] Rafail Ostrovsky, Ramarathnam Venkatesan, and Moti Yung. "Interactive Hashing Simplifies Zero-Knowledge Protocol Design." In: *EUROCRYPT*. Vol. 765. Lecture Notes in Computer Science. Springer, 1993, pp. 267–273 (Cited on page 45).

[OW93] Rafail Ostrovsky and Avi Wigderson. "One-Way Fuctions are Essential for Non-Trivial Zero-Knowledge." In: *Israel Symposium on Theory of Computing Systems (ISTCS)*. IEEE Computer Society, 1993, pp. 3–17 (Cited on page 9).

[Ped91] Torben P. Pedersen. "Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing." In: *CRYPTO*. Vol. 576. Lecture Notes in Computer Science. Springer, 1991, pp. 129–140 (Cited on pages 123, 124).

[PLS19] Rafaël del Pino, Vadim Lyubashevsky, and Gregor Seiler. "Short Discrete Log Proofs for FHE and Ring-LWE Ciphertexts." In: *Practice and Theory of Public-Key Cryptography (PKC)*. Vol. 11442. Lecture Notes in Computer Science. Springer, 2019, pp. 344–373 (Cited on pages 17, 150).

[PR06] Chris Peikert and Alon Rosen. "Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices." In: *Theory of Cryptography Conference (TCC)*. Vol. 3876. Lecture Notes in Computer Science. Springer, 2006, pp. 145–166 (Cited on page 37).

[PS96] David Pointcheval and Jacques Stern. "Security Proofs for Signature Schemes." In: *EUROCRYPT*. Vol. 1070. Lecture Notes in Computer Science. Springer, 1996, pp. 387–398 (Cited on page 191).

[PV07] Rafael Pass and Muthuramakrishnan Venkitasubramaniam. "An Efficient Parallel Repetition Theorem for Arthur-Merlin Games." In: *ACM Symposium on Theory of Computing (STOC)*. ACM, 2007, pp. 420–429 (Cited on page 18).

[PV12] Rafael Pass and Muthuramakrishnan Venkitasubramaniam. "A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs." In: *ACM Transactions on Compututation Theory (TOCT)* 4.4 (2012), 10:1–10:22 (Cited on page 18).

[PW07] Krzysztof Pietrzak and Douglas Wikström. "Parallel Repetition of Computationally Sound Protocols Revisited." In: *Theory of Cryptography Conference (TCC)*. Vol. 4392. Lecture Notes in Computer Science. Springer, 2007, pp. 86–102 (Cited on pages 17, 167).

[RAD78] Ronald L. Rivest, Len Adleman, and Michael L. Dertouzos. "On Data Banks and Privacy Homomorphisms." In: *Foundations of Secure Computation* 4.11 (1978), pp. 169–180 (Cited on page 7).

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." In: *Communications of the ACM* 21.2 (1978), pp. 120–126 (Cited on page 6).

[Sch91] Claus-Peter Schnorr. "Efficient Signature Generation by Smart Cards." In: *Journal of Cryptology* 4.3 (1991), pp. 161–174 (Cited on page 10).

[Sha48a] Claude E. Shannon. "A Mathematical Theory of Communication." In: *Bell System Technical Journal* 27.3 (1948), pp. 379–423 (Cited on page 5).

[Sha48b] Claude E. Shannon. "A Mathematical Theory of Communication." In: *Bell System Technical Journal* 27.4 (1948), pp. 623–656 (Cited on page 5).

[Sha49] Claude E. Shannon. "Communication Theory of Secrecy Systems." In: *Bell System Technical Journal* 28.4 (1949), pp. 656–715 (Cited on page 5).

[Sha79] Adi Shamir. "How to Share a Secret." In: *Communications of the ACM* 22.11 (1979), pp. 612–613 (Cited on page 53).

[Sho00] Victor Shoup. "Practical Threshold Signatures." In: *EUROCRYPT*. Vol. 1807. Lecture Notes in Computer Science. Springer, 2000, pp. 207–220 (Cited on pages 218, 228).

[Sho94] Peter W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1994, pp. 124–134 (Cited on pages 5, 7, 36).

[SJM91] Gustavus J. Simmons, Wen-Ai Jackson, and Keith M. Martin. "The Geometry of Shared Secret Schemes." In: *Bulletin of the Institute of Combinatorics and its Applications* 1 (1991), pp. 71–88 (Cited on page 119).

[SRA81] Adi Shamir, Ronald L Rivest, and Leonard M Adleman. "Mental Poker." In: *The Mathematical Gardner*. Springer, 1981, pp. 37–43 (Cited on page 7).

[SSH11] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. "Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials." In: *CRYPTO*. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 706–723 (Cited on page 172).

[SV07] Nigel P. Smart and Frederik Vercauteren. "On Computable Isomorphisms in Efficient Asymmetric Pairing-Based Systems." In: *Discrete Applied Mathematics* 155.4 (2007), pp. 538–547 (Cited on page 230).

[SW05] Amit Sahai and Brent Waters. "Fuzzy Identity-Based Encryption." In: *EUROCRYPT*. Vol. 3494. Lecture Notes in Computer Science. Springer, 2005, pp. 457–473 (Cited on page 227).

[Tur36] Alan Mathison Turing. "On Computable Numbers, with an Application to the Entscheidungsproblem." In: *Proceedings of the London Mathematical Society* 42.2 (1936), pp. 230–265 (Cited on page 4).

[TW87] Martin Tompa and Heather Woll. "Random Self-Reducibility and Zero Knowledge Interactive Proofs of Possession of Information." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1987, pp. 472–482 (Cited on page 10).

[Unr12] Dominique Unruh. "Quantum Proofs of Knowledge." In: *EUROCRYPT*. Vol. 7237. Lecture Notes in Computer Science. Springer, 2012, pp. 135–152 (Cited on page 42).

[Unr17] Dominique Unruh. "Post-Quantum Security of Fiat-Shamir." In: *ASIACRYPT*. Vol. 10624. Lecture Notes in Computer Science. Springer, 2017, pp. 65–95 (Cited on page 50).

[Wes19] Benjamin Wesolowski. "Efficient Verifiable Delay Functions." In: *EUROCRYPT*. Vol. 11478. Lecture Notes in Computer Science. Springer, 2019, pp. 379–407 (Cited on pages 36, 136).

[Wig19] Avi Wigderson. *Mathematics and Computation*. Princeton University Press, 2019. ISBN: 978-0-691-18913-0 (Cited on page 11).

[Wik18] Douglas Wikström. "Special Soundness Revisited." In: *IACR Cryptology ePrint Archive* (2018). IACR ePrint: 2018/1157 (Cited on pages 150, 190).

[Wik21] Douglas Wikström. "Special Soundness in the Random Oracle Model." In: *IACR Cryptology ePrint Archive* (2021). IACR ePrint: 2021/1265 (Cited on page 190).

[Yao82] Andrew Chi-Chih Yao. "Protocols for Secure Computations (Extended Abstract)." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1982, pp. 160–164 (Cited on page 7).

[Yao86] Andrew Chi-Chih Yao. "How to Generate and Exchange Secrets (Extended Abstract)." In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. IEEE Computer Society, 1986, pp. 162–167 (Cited on page 7).

[YMR+19] Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan-Gueta, and Ittai Abraham. "HotStuff: BFT Consensus with Linearity and Responsiveness." In: *ACM Symposium on Principles of Distributed Computing (PODC)*. ACM, 2019, pp. 347–356 (Cited on page 218).