Knowledge extraction in the quantum random-oracle model

Don, J.W.

Bibliography

[ABCP22] Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen. *CSI-SharK: CSI-FiSh with Sharing-friendly Keys*. Cryptology ePrint Archive, Paper 2022/1189. https://eprint.iacr.org/2022/1189. 2022. URL: https://eprint.iacr.org/2022/1189.

[ABG+20] Amit Agarwal, James Bartusek, Vipul Goyal, Dakshita Khurana, and Giulio Malavolta. *Post-Quantum Multi-Party Computation*. 2020. arXiv: 2005.12904 [quant-ph].

[AE18] Jean-Philippe Aumasson and Guillaume Endignoux. "Improving Stateless Hash-Based Signatures". In: *Topics in Cryptology – CT-RSA 2018*. Ed. by Nigel P. Smart. Cham: Springer International Publishing, 2018, pp. 219–242. ISBN: 978-3-319-76953-0.

[AFLT12] Michel Abdalla, Pierre-Alain Fouque, Vadim Lyubashevsky, and Mehdi Tibouchi. "Tightly-Secure Signatures from Lossy Identification Schemes". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer, 2012, pp. 572–590. ISBN: 978-3-642-29011-4.

[AHU19] Andris Ambainis, Mike Hamburg, and Dominique Unruh. "Quantum Security Proofs Using Semi-classical Oracles". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 269–295. ISBN: 978-3-030-26951-7.

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. "Quantum-Access-Secure Message Authentication via Blind-Unforgeability". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Cham: Springer International Publishing, 2020, pp. 788–817. ISBN: 978-3-030-45727-3.

[ARU14] A. Ambainis, A. Rosmanis, and D. Unruh. "Quantum Attacks on Classical Proof Systems: The Hardness of Quantum Rewinding". In: *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*. Oct. 2014, pp. 474–483. DOI: 10.1109/FOCS.2014.57.

[BBB+18] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, and G. Maxwell. "Bulletproofs: Short Proofs for Confidential Transac-

tions and More". In: *2018 IEEE Symposium on Security and Privacy (SP)*. May 2018, pp. 315–334. DOI: 10.1109/SP.2018.00020.

[BBHT98] Michel Boyer, Gilles Brassard, Peter Høyer, and Alain Tapp. "Tight Bounds on Quantum Searching". In: *Fortschritte der Physik* 46.4-5 (1998), pp. 493–505.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. "Random Oracles in a Quantum World". In: *Advances in Cryptology – ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Berlin, Heidelberg: Springer, 2011, pp. 41–69. ISBN: 978-3-642-25385-0.

[BDK+21] Shi Bai, Leo Ducas, Eike Kiltz, Lepoint Tancrede, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehle. *CRYSTALS-Dilithium Algorithm Specifications and Supporting Documentation (Version 3.1)*. https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf, retrieved on 19.03.2023. 2021.

[Beu20] Ward Beullens. "Sigma Protocols for MQ, PKP and SIS, and Fishy Signature Schemes". In: *Advances in Cryptology – EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Cham: Springer International Publishing, 2020, pp. 183–211. ISBN: 978-3-030-45727-3.

[BG93] Mihir Bellare and Oded Goldreich. "On Defining Proofs of Knowledge". In: *Advances in Cryptology — CRYPTO' 92*. Ed. by Ernest F. Brickell. Berlin, Heidelberg: Springer, 1993, pp. 390–420. ISBN: 978-3-540-48071-6.

[BGKM23] Loïc Bidoux, Philippe Gaborit, Mukul Kulkarni, and Victor Mateu. "Code-based signatures from new proofs of knowledge for the syndrome decoding problem". In: *Designs, Codes and Cryptography* 91.2 (2023), pp. 497–544.

[BHH+19] Nina Bindel, Mike Hamburg, Kathrin Hövelmanns, Andreas Hülsing, and Edoardo Persichetti. "Tighter Proofs of CCA Security in the Quantum Random Oracle Model". In: *Theory of Cryptography*. Ed. by Dennis Hofheinz and Alon Rosen. Cham: Springer International Publishing, 2019, pp. 61–90. ISBN: 978-3-030-36033-7.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. "Quantum cryptanalysis of hash and claw-free functions". In: *LATIN'98: The-*

oretical Informatics. Ed. by Cláudio L. Lucchesi and Arnaldo V. Moura. Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 163–169. ISBN: 978-3-540-69715-2.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. "CSI-FiSh: Efficient Isogeny Based Signatures Through Class Group Computations". In: *Advances in Cryptology – ASIACRYPT 2019*. Ed. by Steven D. Galbraith and Shiho Moriai. Cham: Springer International Publishing, 2019, pp. 227–247. ISBN: 978-3-030-34578-5.

[BLZ21] Jeremiah Blocki, Seunghoon Lee, and Samson Zhou. *On the Security of Proofs of Sequential Work in a Post-Quantum World*. 2021. arXiv: 2006.10972 [cs.CR].

[BMPS20] Jean-François Biasse, Giacomo Micheli, Edoardo Persichetti, and Paolo Santini. "LESS is More: Code-Based Signatures Without Syndromes". In: *Progress in Cryptology - AFRICACRYPT 2020*. Ed. by Abderrahmane Nitaj and Amr Youssef. Cham: Springer International Publishing, 2020, pp. 45–65. ISBN: 978-3-030-51938-4.

[BR93] Mihir Bellare and Phillip Rogaway. "Random oracles are practical: A paradigm for designing efficient protocols". In: *Proceedings of the 1st ACM conference on Computer and communications security*. ACM. 1993, pp. 62–73.

[BSK+21] Carsten Baum, Cyprien Delpech de Saint Guilhem, Daniel Kales, Emmanuela Orsini, Peter Scholl, and Greg Zaverucha. "Banquet: Short and Fast Signatures from AES". In: *Public-Key Cryptography – PKC 2021*. Ed. by Juan A. Garay. Cham: Springer International Publishing, 2021, pp. 266–297. ISBN: 978-3-030-75245-3.

[CDG+17] Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, and Greg Zaverucha. "Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. CCS '17. Dallas, Texas, USA: ACM, 2017, pp. 1825–1842. ISBN: 978-1-4503-4946-8. DOI: 10.1145/3133956.3133997.

[CDG+19] Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, et al. "The

picnic signature scheme". In: *Submission to NIST Post-Quantum Cryptography project* (2019).

[CDG+20] Melissa Chase, David Derler, Steven Goldfeder, Jonathan Katz, Vladimir Kolesnikov, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Xiao Wang, and Greg Zaverucha. *The Picnic Signature Scheme, Design Document v2.1.* 2020. URL: https://github.com/microsoft/Picnic/blob/master/spec/design-v2.2.pdf.

[CDS94] Ronald Cramer, Ivan Damgård, and Berry Schoenmakers. "Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols". In: *Advances in Cryptology — CRYPTO '94*. Ed. by Yvo G. Desmedt. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 174–187. ISBN: 978-3-540-48658-9.

[CFHL21] Kai-Min Chung, Serge Fehr, Yu-Hsuan Huang, and Tai-Ning Liao. "On the Compressed-Oracle Technique, and Post-Quantum Security of Proofs of Sequential Work". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and François-Xavier Standaert. Cham: Springer International Publishing, 2021, pp. 598–629. ISBN: 978-3-030-77886-6.

[CGH04] Ran Canetti, Oded Goldreich, and Shai Halevi. "The random oracle methodology, revisited". In: *Journal of the ACM* 51.4 (July 2004), pp. 557–594. ISSN: 00045411. DOI: 10.1145/1008731.1008734. arXiv: 0010019 [cs]. URL: http://arxiv.org/abs/cs/0010019.

[CGLQ20] Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. "Tight Quantum Time-Space Tradeoffs for Function Inversion". In: *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 673–684. DOI: 10.1109/FOCS46700.2020.00068.

[Cha19] André Chailloux. *Tight quantum security of the Fiat-Shamir transform for commit-and-open identification schemes with applications to post-quantum signature schemes*. Cryptology ePrint Archive, Report 2019/699, version 1 Jul 2019. https://eprint.iacr.org/2019/699/20190701:091436. 2019.

[Cha21] André Chailloux. *Tight quantum security of the Fiat-Shamir transform for commit-and-open identification schemes with applications to post-quantum signature schemes*. Cryptology ePrint

Archive, Report 2019/699, version 16 Mar 2021. https://eprint.iacr.org/2019/699/20210316:124850. 2021.

[CHH+21] Kai-Min Chung, Yao-Ching Hsieh, Mi-Ying Huang, Yu-Hsuan Huang, Tanja Lange, and Bo-Yin Yang. *Isogeny-based Group Signatures and Accountable Ring Signatures in QROM*. Cryptology ePrint Archive, Paper 2021/1368. 2021. URL: https://eprint.iacr.org/2021/1368.

[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: *Advances in Cryptology – ASIACRYPT 2016*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 135–165. ISBN: 978-3-662-53890-6.

[CHR+18] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. "SOFIA: MQ-Based Signatures in the QROM". In: *Public-Key Cryptography – PKC 2018*. Ed. by Michel Abdalla and Ricardo Dahab. Cham: Springer International Publishing, 2018, pp. 3–33. ISBN: 978-3-319-76581-5.

[CHR+20] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. *MQDSS Specfications version 2.1*. https://repository.ubn.ru.nl/bitstream/handle/2066/236576/236576.pdf, retrieved on 16.03.2023. 2020.

[CMS19] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. "Succinct Arguments in the Quantum Random Oracle Model". In: *Theory of Cryptography*. Ed. by Dennis Hofheinz and Alon Rosen. Cham: Springer International Publishing, 2019, pp. 1–29. ISBN: 978-3-030-36033-7.

[CMSZ19] Jan Czajkowski, Christian Majenz, Christian Schaffner, and Sebastian Zur. *Quantum Lazy Sampling and Game-Playing Proofs for Quantum Indifferentiability*. Cryptology ePrint Archive, Report 2019/428. https://eprint.iacr.org/2019/428. 2019.

[Dam10] Ivan Damgard. *On Sigma-Protocols, Lecture notes, Faculty of Science Aarhus University, Department of Computer Science*. 2010. URL: http://www.cs.au.dk/~ivan/Sigma.pdf.

[DFG13] Özgür Dagdelen, Marc Fischlin, and Tommaso Gagliardoni. "The Fiat-Shamir Transformation in a Quantum World". In: *Advances in Cryptology - ASIACRYPT 2013*. Ed. by Kazue Sako and

Palash Sarkar. Berlin, Heidelberg: Springer, 2013, pp. 62–81. ISBN: 978-3-642-42045-0.

[DFM20] Jelle Don, Serge Fehr, and Christian Majenz. "The Measure-and-Reprogram Technique 2.0: Multi-round Fiat-Shamir and More". In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Cham: Springer International Publishing, 2020, pp. 602–631.

[DFMS19] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer International Publishing, 2019, pp. 356–383.

[DFMS22a] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Online-Extractability in the Quantum Random-Oracle Model". In: *Advances in Cryptology – EUROCRYPT 2022*. Ed. by Orr Dunkelman and Stefan Dziembowski. Cham: Springer International Publishing, 2022, pp. 677–706.

[DFMS22b] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. "Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM". In: *Advances in Cryptology – CRYPTO 2022*. Ed. by Yevgeniy Dodis and Thomas Shrimpton. Cham: Springer Nature Switzerland, 2022, pp. 729–757.

[DH76] W. Diffie and M. Hellman. "New directions in cryptography". In: *IEEE Transactions on Information Theory* 22.6 (1976), pp. 644–654. DOI: 10.1109/TIT.1976.1055638.

[DJ92] David Deutsch and Richard Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society of London Series A* 439.1907 (Dec. 1992), pp. 553–558. DOI: 10.1098/rspa.1992.0167.

[DKL+18a] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018.1 (Feb. 2018), pp. 238–268. DOI: 10.13154/tches.v2018.i1.238-268. URL: https://tches.iacr.org/index.php/TCHES/article/view/839.

[DKL+18b] Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. "CRYSTALS-

Dilithium: A Lattice-Based Digital Signature Scheme". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018.1 (Feb. 2018), pp. 238–268. DOI: 10.13154/tches.v2018.i1.238-268. URL: https://tches.iacr.org/index.php/TCHES/article/view/839.

[DKR+21] Christoph Dobraunig, Daniel Kales, Christian Rechberger, Markus Schofnegger, and Greg Zaverucha. *Shorter Signatures Based on Tailor-Made Minimalist Symmetric-Key Crypto*. Cryptology ePrint Archive, Report 2021/692. https://ia.cr/2021/692. 2021.

[Ell87] James Ellis. *The history of Non-Secret Encryption*. 1987. URL: https://cryptocellar.org/cesg/ellis.pdf.

[ES15] Edward Eaton and Fang Song. "Making Existential-unforgeable Signatures Strongly Unforgeable in the Quantum Random-oracle Model". In: *10th Conference on the Theory of Quantum Computation, Communication and Cryptography*. 2015, p. 147.

[Feh18] Serge Fehr. "Classical Proofs for the Quantum Collapsing Property of Classical Hash Functions". In: *Theory of Cryptography Conference - TCC2018, volume 11240 of Lecture Notes in Computer Science* (2018), pp. 315–338. eprint: 2018/887.

[Feh22] Serge Fehr. *Multipartite Quantum Systems*. University Lecture Notes. 2022. URL: https://homepages.cwi.nl/~fehr/QC2022/Ch2.pdf.

[Fis05] Marc Fischlin. "Communication-Efficient Non-interactive Proofs of Knowledge with Online Extractors". In: *Advances in Cryptology – CRYPTO 2005*. Ed. by Victor Shoup. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 152–168. ISBN: 978-3-540-31870-5.

[FJ20] Patrick Fischlin Marc and Harasser and Christian Janson. "Signatures from Sequential-OR Proofs". In: *Advances in Cryptology - EUROCRYPT 2020*. Ed. by Anne Canteaut and Yuval Ishai. Vol. 12107. Lecture Notes in Computer Science. Springer, 2020, pp. 212–244. DOI: 10.1007/978-3-030-45727-3_8.

[FKMV12] Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson, and Daniele Venturi. "On the Non-malleability of the Fiat-Shamir Transform". In: *Indocrypt 2012*. Vol. 7668 LNCS. 2012, pp. 60–79. ISBN: 9783642349300. DOI: 10.1007/978-3-642-34931-7_5.

[FO99] Eiichiro Fujisaki and Tatsuaki Okamoto. "How to Enhance the Security of Public-Key Encryption at Minimum Cost". In: *Public Key Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 53–68. ISBN: 978-3-540-49162-0.

[FS87] Amos Fiat and Adi Shamir. "How To Prove Yourself: Practical Solutions to Identification and Signature Problems". In: *Advances in Cryptology — CRYPTO' 86*. Ed. by Andrew M. Odlyzko. Berlin, Heidelberg: Springer, 1987, pp. 186–194. ISBN: 978-3-540-47721-1.

[GHHM21] Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing, and Christian Majenz. "Tight Adaptive Reprogramming in the QROM". In: *Advances in Cryptology – ASIACRYPT 2021*. Ed. by Mehdi Tibouchi and Huaxiong Wang. Cham: Springer International Publishing, 2021, pp. 637–667. ISBN: 978-3-030-92062-3.

[GMO16] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. "ZKBoo: Faster Zero-Knowledge for Boolean Circuits". In: *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, 2016, pp. 1069–1083. ISBN: 978-1-931971-32-4. URL: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/giacomelli.

[GMR85] S Goldwasser, S Micali, and C Rackoff. "The Knowledge Complexity of Interactive Proof-Systems". In: *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*. STOC '85. Providence, Rhode Island, USA: Association for Computing Machinery, 1985, pp. 291–304. ISBN: 0897911512. DOI: 10.1145/22145.22178. URL: https://doi.org/10.1145/22145.22178.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. "Proofs That Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems". In: *J. ACM* 38.3 (July 1991), pp. 690–728. ISSN: 0004-5411. DOI: 10.1145/116825.116852. URL: https://doi.org/10.1145/116825.116852.

[GPS22] Shay Gueron, Edoardo Persichetti, and Paolo Santini. "Designing a Practical Code-Based Signature Scheme from Zero-Knowledge Proofs with Trusted Setup". In: *Cryptography* 6.1 (2022). ISSN: 2410-387X. URL: https://www.mdpi.com/2410-387X/6/1/5.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. "A Modular Analysis of the Fujisaki-Okamoto Transformation". In: *Theory*

of Cryptography. Ed. by Yael Kalai and Leonid Reyzin. Cham: Springer International Publishing, 2017, pp. 341–371. ISBN: 978-3-319-70500-2.

[HM21] Yassine Hamoudi and Frédéric Magniez. "Quantum Time-Space Tradeoff for Finding Multiple Collision Pairs". In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Ed. by Min-Hsiu Hsieh. Vol. 197. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2021, 1:1–1:21. ISBN: 978-3-95977-198-6. DOI: 10.4230/LIPIcs.TQC.2021.1. URL: https://drops.dagstuhl.de/opus/volltexte/2021/13996.

[IKOS07a] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. "Zero-Knowledge from Secure Multiparty Computation". In: *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '07. San Diego, California, USA: Association for Computing Machinery, 2007, pp. 21–30. ISBN: 9781595936318. DOI: 10.1145/1250790.1250794. URL: https://doi.org/10.1145/1250790.1250794.

[IKOS07b] Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, and Amit Sahai. "Zero-knowledge from secure multiparty computation". In: *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing - STOC '07* (2007), p. 21. ISSN: 07378017. URL: http://portal.acm.org/citation.cfm?doid=1250790.1250794.

[Ker83] Auguste Kerckhoffs. "La cryptographie militaire". In: *Journal des sciences militaires* IX.Jan. (1883), pp. 5–83. URL: http://www.petitcolas.net/fabien/kerckhoffs/.

[KKPP20] Shuichi Katsumata, Kris Kwiatkowski, Federico Pintore, and Thomas Prest. "Scalable Ciphertext Compression Techniques for Post-quantum KEMs and Their Applications". In: *Advances in Cryptology – ASIACRYPT 2020*. Ed. by Shiho Moriai and Huaxiong Wang. Cham: Springer International Publishing, 2020, pp. 289–320. ISBN: 978-3-030-64837-4.

[KKW18] Jonathan Katz, Vladimir Kolesnikov, and Xiao Wang. "Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: Association for Computing Ma-

chinery, 2018, pp. 525–537. ISBN: 9781450356930. URL: https://doi.org/10.1145/3243734.3243805.

[KLS18] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. "A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model". In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Cham: Springer, 2018, pp. 552–586. ISBN: 978-3-319-78372-7.

[KM15] Neal Koblitz and Alfred J. Menezes. "The random oracle model: a twenty-year retrospective". In: *Designs, Codes and Cryptography* 77 (2015), pp. 587–610. DOI: 10.1007/s10623-015-0094-2.

[KZ20] Daniel Kales and Greg Zaverucha. "Improving the Performance of the Picnic Signature Scheme". English. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.4 (Sept. 2020). CHES 2020 : 2020 Annual Conference on Cryptographic Hardware and Embedded Systems ; Conference date: 14-09-2020 Through 17-09-2020, pp. 154–188. ISSN: 2569-2925. DOI: https://doi.org/10.13154/tches.v2020.i4.154-188.

[LWW04] Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. "Linkable Spontaneous Anonymous Group Signature for Ad Hoc Groups". In: *Information Security and Privacy*. Ed. by Huaxiong Wang, Josef Pieprzyk, and Vijay Varadharajan. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004, pp. 325–335. ISBN: 978-3-540-27800-9.

[Lyu09] Vadim Lyubashevsky. "Fiat-Shamir with Aborts: Applications to Lattice and Factoring-Based Signatures". In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Berlin, Heidelberg: Springer, 2009, pp. 598–616. ISBN: 978-3-642-10366-7.

[Lyu12] Vadim Lyubashevsky. "Lattice Signatures without Trapdoors". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer, 2012, pp. 738–755. ISBN: 978-3-642-29011-4.

[LZ19a] Qipeng Liu and Mark Zhandry. "On Finding Quantum Multi-collisions". In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 189–218. ISBN: 978-3-030-17659-4.

[LZ19b] Qipeng Liu and Mark Zhandry. "Revisiting Post-quantum Fiat-Shamir". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Cham: Springer In-

ternational Publishing, 2019, pp. 326–355. ISBN: 978-3-030-26951-7.

[Mer78] Ralph C. Merkle. "Secure Communications over Insecure Channels". In: *Commun. ACM* 21.4 (Apr. 1978), pp. 294–299. ISSN: 0001-0782. URL: https://doi.org/10.1145/359460.359473.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 10th. New York, NY, USA: Cambridge University Press, 2011. ISBN: 1107002176, 9781107002173.

[Pas03] Rafael Pass. "On Deniability in the Common Reference String and Random Oracle Model". In: *Advances in Cryptology - CRYPTO 2003*. Ed. by Dan Boneh. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 316–337. ISBN: 978-3-540-45146-4.

[Pas04] Rafael Pass. "Alternative variants of zero-knowledge proofs". PhD thesis. KTH Stockholm, 2004.

[PS96] David Pointcheval and Jacques Stern. "Security Proofs for Signature Schemes". In: *LNCS* 1070 (1996), pp. 387–398. URL: https://www.di.ens.fr/%7B~%7Dpointche/Documents/Papers/1996%7B%5C_%7Deurocrypt.pdf.

[RCB22] Prasanna Ravi, Anupam Chattopadhyay, and Shivam Bhasin. "Security and Quantum Computing: An Overview". In: *2022 IEEE 23rd Latin American Test Symposium (LATS)*. 2022, pp. 1–6. DOI: 10.1109/LATS57337.2022.9936966.

[RSA78] R. L. Adleman Rivest, A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Commun. ACM* 21.2 (Feb. 1978), pp. 120–126. ISSN: 0001-0782. URL: https://doi.org/10.1145/359340.359342.

[Sho94] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[Sim97] Daniel R. Simon. "On the Power of Quantum Computation". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1474–1483. DOI: 10.1137/S0097539796298637.

[SSH11] Koichi Sakumoto, Taizo Shirai, and Harunaga Hiwatari. "Public-Key Identification Schemes Based on Multivariate Quadratic Polynomials". In: *Advances in Cryptology – CRYPTO 2011*. Ed.

by Phillip Rogaway. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 706–723. ISBN: 978-3-642-22792-9.

[TDJ+22] Gang Tang, Dung Hoang Duong, Antoine Joux, Thomas Plantard, Youming Qiao, and Willy Susilo. "Practical Post-Quantum Signature Schemes from Isomorphism Problems of Trilinear Forms". In: *Advances in Cryptology – EUROCRYPT 2022*. Ed. by Orr Dunkelman and Stefan Dziembowski. Cham: Springer International Publishing, 2022, pp. 582–612. ISBN: 978-3-031-07082-2.

[TU16] Ehsan Ebrahimi Targhi and Dominique Unruh. "Post-Quantum Security of the Fujisaki-Okamoto and OAEP Transforms". In: *Theory of Cryptography*. Ed. by Martin Hirt and Adam Smith. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 192–216. ISBN: 978-3-662-53644-5.

[Unr12] Dominique Unruh. "Quantum Proofs of Knowledge". In: *Advances in Cryptology – EUROCRYPT 2012*. Ed. by David Pointcheval and Thomas Johansson. Berlin, Heidelberg: Springer, 2012, pp. 135–152. ISBN: 978-3-642-29011-4.

[Unr14a] Dominique Unruh. "Quantum Position Verification in the Random Oracle Model". In: *Advances in Cryptology – CRYPTO 2014*. Ed. by Juan A. Garay and Rosario Gennaro. Berlin, Heidelberg: Springer, 2014, pp. 1–18. ISBN: 978-3-662-44381-1.

[Unr14b] Dominique Unruh. "Revocable Quantum Timed-Release Encryption". In: *Advances in Cryptology – EUROCRYPT 2014*. Ed. by Phong Q. Nguyen and Elisabeth Oswald. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 129–146. ISBN: 978-3-642-55220-5.

[Unr15a] Dominique Unruh. *Computationally binding quantum commitments*. Cryptology ePrint Archive, Paper 2015/361. `https://eprint.iacr.org/2015/361`. 2015. URL: `https://eprint.iacr.org/2015/361`.

[Unr15b] Dominique Unruh. "Non-Interactive Zero-Knowledge Proofs in the Quantum Random Oracle Model". In: *Advances in Cryptology - EUROCRYPT 2015*. Ed. by Elisabeth Oswald and Marc Fischlin. Berlin, Heidelberg: Springer, 2015, pp. 755–784. ISBN: 978-3-662-46803-6.

[Unr16] Dominique Unruh. "Computationally Binding Quantum Commitments". In: *Advances in Cryptology – EUROCRYPT 2016*. Ed.

by Marc Fischlin and Jean-Sébastien Coron. Berlin, Heidelberg: Springer, 2016, pp. 497–527. ISBN: 978-3-662-49896-5.

[Unr17] Dominique Unruh. "Post-quantum Security of Fiat-Shamir". In: *Advances in Cryptology – ASIACRYPT 2017*. Ed. by Tsuyoshi Takagi and Thomas Peyrin. Cham: Springer, 2017, pp. 65–95. ISBN: 978-3-319-70694-8.

[Wik18] Douglas Wikström. *Special Soundness Revisited*. Cryptology ePrint Archive, Report 2018/1157. `https://ia.cr/2018/1157`. 2018.

[YZ21] Takashi Yamakawa and Mark Zhandry. "Classical vs Quantum Random Oracles". In: *Advances in Cryptology – EUROCRYPT 2021*. Ed. by Anne Canteaut and François-Xavier Standaert. Cham: Springer International Publishing, 2021, pp. 568–597. ISBN: 978-3-030-77886-6.

[Zha12] Mark Zhandry. "How to Construct Quantum Random Functions". In: *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*. IEEE, Oct. 2012, pp. 679–687. ISBN: 978-0-7695-4874-6. DOI: `10.1109/FOCS.2012.37`. URL: `https://eprint.iacr.org/2012/182.pdf`.

[Zha15a] Mark Zhandry. "A note on the quantum collision and set equality problems". In: *Quantum Information and Computation* 15.7-8 (2015), pp. 557–567.

[Zha15b] Mark Zhandry. "Secure identity-based encryption in the quantum random oracle model". In: *International Journal of Quantum Information* 13.04 (2015), p. 1550014.

[Zha19a] Mark Zhandry. "How to Record Quantum Queries, and Applications to Quantum Indifferentiability". In: *Advances in Cryptology – CRYPTO 2019*. Ed. by Alexandra Boldyreva and Daniele Micciancio. Full Version (1 March 2019): `https://eprint.iacr.org/2018/276/20190301:184107`. Cham: Springer International Publishing, 2019, pp. 239–268. ISBN: 978-3-030-26951-7.

[Zha19b] Mark Zhandry. "Quantum Lightning Never Strikes the Same State Twice". In: *Advances in Cryptology – EUROCRYPT 2019*. Ed. by Yuval Ishai and Vincent Rijmen. Cham: Springer International Publishing, 2019, pp. 408–438. ISBN: 978-3-030-17659-4.