Cyber Security Section
DTU Compute
Technical University of Denmark
Richard Petersens Plads
2800 Kgs. Lyngby
☎ *+4553575781*
christianmajenz.info

Christian Majenz

List of publications

Overview

- Conference papers: 12
- Journal articles: 9
- Preprints: 6
- Citations: 686, H-index: 14
  (According to google scholar as of August 2, 2022)
- ORCiD: `https://orcid.org/0000-0002-1877-8385`
- **Cryptography:** Crypto (4x), Eurocrypt (6x), Asiacrypt, ITC, 5 preprints
- **Quantum information theory:** Nature Communcations, Physical Review letters (3x), Physical Review A (2x), 1 preprint
- **Mathematics of quantum computation:** Communications in Mathematical Physics, Quantum

(Some of) my articles can be found on arXiv.org, eprint and dblp.

Peer reviewed conference papers

1 Gorjan Alagic and Christian Majenz, *Quantum non-malleability and authentication*, Advances in Cryptology – Crypto 2017. Lecture Notes in Computer Science, vol 10402, Springer, Cham

2 Jelle Don, Serge Fehr, Christian Majenz and Christian Schaffner, *Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model*, Advances in Cryptology – Crypto 2019. Lecture Notes in Computer Science, vol 11693, Springer, Cham.

3 Jelle Don, Serge Fehr, Christian Majenz, *The Measure-and-Reprogram Technique 2.0: Multi-Round Fiat-Shamir and More*, Advances in Cryptology – Crypto 2020. Lecture Notes in Computer Science, vol 12172, Springer, Cham.

4 Alex B. Grilo, Kathrin Hövelmanns, Andreas Hülsing and Christian Majenz, *Tight adaptive reprogramming in the QROM*,Advances in Cryptology – ASIACRYPT 2021. Lecture Notes in Computer Science, vol 13090. Springer, Cham.

5 Gorjan Alagic, Tommaso Gagliardoni and Christian Majenz, *Unforgeable quantum encryption*, Advances in Cryptology – Eurocrypt 2018. Lecture Notes in Computer Science, vol 10822. Springer, Cham.

6 Yfke Dulek, Alex Grilo, Stacey Jeffery, Christian Majenz and Christian Schaffner, *Secure multi-party quantum computation with a dishonest majority*, Advances in Cryptology – Eurocrypt 2020. Lecture Notes in Computer Science, vol 12107. Springer, Cham.

7 Gorjan Alagic, Christian Majenz, Fang Song and Alexander C. Russell, *Quantum-secure message authentication via blind unforgeability*, Advances in Cryptology – Eurocrypt 2020. Lecture Notes in Computer Science, vol 12107. Springer, Cham.

8 Gorjan Alagic, Christian Majenz and Alexander Russell, *Efficient simulation of random states and random unitaries*, Advances in Cryptology – Eurocrypt 2020. Lecture Notes in Computer Science, vol 12107. Springer, Cham.

9 Gorjan Alagic, Chen Bai, Jonathan Katz and Christian Majenz, *Post-Quantum Security of the Even-Mansour Cipher*, Advances in Cryptology – Eurocrypt 2022. Lecture Notes in Computer Science, vol 12107. Springer, Cham.

10 Jelle Don, Serge Fehr, Christian Majenz, Christian Schaffner, *Online-Extractability in the Quantum Random-Oracle Model*, Advances in Cryptology – Eurocrypt 2022. Lecture Notes in Computer Science, vol 12107. Springer, Cham.

11 Jelle Don, Serge Fehr, Christian Majenz, Christian Schaffner, *Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM*, preprint arXiv:2202.13730, accepted for publication at Crypto 2022.

12 Christian Majenz, Chanelle Matadah Manfouo, Maris Ozols, *Quantum-access security of the Winternitz one-time signature scheme*, ITC 2021, eprint 2021/387

Peer reviewed journal articles

13 Rafael Chaves, Christian Majenz, and David Gross,*Information-theoretic implications of quantum causal structures*, Nature communications 6 (2015).

14 Matthias Christandl, Felix Leditzky, Christian Majenz, Gaeme Smith, Florian Speelmann, and Michael Walter, *Asymptotic performance of port-based teleportation*, Communications in Mathematical Physics 381, 379–451 (2021)

15 Cécilia Lancien and Christian Majenz, *Weak approximate unitary designs and applications to quantum encryption*, Quantum 4, p. 313

16 Gorjan Alagic, Tommaso Gagliardoni and Christian Majenz, *Can you sign a quantum state?*, Quantum 4, p. 603

17 Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl, *Catalytic decoupling of quantum information*, Physical review letters 118, no. 8 (2017).

18 Berta, Mario, Fernando GSL Brandão, Christian Majenz, and Mark M. Wilde. *Conditional Decoupling of Quantum Information.* Physical review letters 121, no. 4 (2018): 040504.

19 Mario Berta and Christian Majenz, *Disentanglement cost of quantum states.* Physical review letters 121, no. 19 (2018)

20 Christian Majenz, Tameem Albash, and Daniel Lidar, *Coarse graining can beat the rotating-wave approximation in quantum Markovian master equations*, Physical Review A 88.1 (2013): 012103.

21 Mario Berta, Fernando G. S. L. Brandao, Christian Majenz, and Mark M. Wilde, *Deconstruction and conditional erasure of quantum correlations*, Physical Review A 98(2018): 042320

Preprints under Review

22 Kathrin Hövelmanns, Andreas Hülsing and Christian Majenz, *Failing gracefully: Decryption failures and the Fujisaki-Okamoto transform*, preprint arXiv:2203.10182

23 Christian Majenz, Maris Ozols, Christian Schaffner, Mehrdad Tahmasbi, *Local simultaneous state discrimination*, preprint arXiv:2111.01209

24 Christian Majenz, Christian Schaffner, Mehrdad Tahmasbi, *Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding*, preprint arXiv:2103.14510

25 Andrea Coladangelo, Alexander Poremba and Christian Majenz, *Quantum copy-protection of compute-and-compare programs in the quantum random oracle model*, preprint arXiv:2009.13865

26 Jan Czajkowski, Christian Majenz, Christian Schaffner and Sebastian Zur, *Quantum lazy sampling and game-playing proofs for quantum indifferentiability*, preprint arXiv:1904.11477.

27 Christian Majenz, Christian Schaffner and Jeroen van Wier, *Non-malleability for quantum public-key encryption*, preprint arXiv:1905.05490.

Theses

28 Christian Majenz, *Entropy in Quantum Information Theory – Communication and Cryptography*, PhD thesis

29 Christian Majenz, *Constraints on Multipartite Quantum Entropies*, M.Sc. thesis

Meta

30 Yfke Dulek, Stacey Jeffery, Christian Majenz, Christian Schaffner, Florian Speelman and Ronald de Wolf, *A Guide for New Program Committee Members at Theoretical Computer Science Conferences*, (probably eternal) preprint arXiv:2105.02773