Christian Majenz

Curriculum Vitae

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

Academic

since 2023 **Associate Professor**, *Technical University of Denmark*, Lyngby, Denmark.

2021-2023 **Tenure-Track Assistant Professor**, *Technical University of Denmark*, Lyngby, Denmark.

2019-2021 **Postdoc**, *QuSoft/Centrum Wiskunde & Informatica*, Amsterdam, Netherlands.
funded by personal Veni grant

2017–2019 **Postdoc**, *QuSoft/University of Amsterdam*, Amsterdam, Netherlands.

2014–2017 **PhD student in Mathematics**, *University of Copenhagen*, Copenhagen, Denmark.
Advisor: Prof. Matthias Christandl

2011–2014 **M.Sc. in Physics**, *University of Freiburg*, Germany.
top grade (1.0 German scale). Advisor: Prof. David Gross

2008–2011 **B.Sc. in Physics**, *University of Freiburg*, Germany.
grade: 1.1 German scale. Advisor: Prof. Heinz-Peter Breuer

Long term visits

2017 **Visiting student researcher**, *California Institute of Technology*, Pasadena, CA, USA.
Visitor in the group of Prof. Fernando Brandão.

2012 **Visiting scholar**, *University of Southern California*, Los Angeles, CA, USA.
Visitor in the group of Prof. Daniel Lidar.

Teaching experience

2022-2023 (ongoing) **Teacher**, *Technical University of Denmark*, *Cryptography I* courses in Spring 2022 and 2023.
Introductory cryptography course covering block ciphers, modes of operation, RSA, Diffie-Hellman, El Gamal, Hash functions.

2022 **Teacher**, *Technical University of Denmark*, *Trends in Cybersecurity*.
Module on Quantum Computers and Quantum Cryptography, part of DTU's Master of Cyber Security (continuing education).

2022 **Teacher**, *Technical University of Denmark*, *Diskret Matematik*.
Discrete mathematics course for Bachelor of Engineering students (in Danish).

2021 **Teacher**, *Technical University of Denmark*, *Applied cryptography*.
Project-based course with the goal of giving the students a flavor of the security mindset (or "professional paranoia"), and convey how it needs to be used when designing cryptographic application from low-level building blocks like AES, SHA2/3, RSA, Diffie-Hellman etc.

2019-2020 **Course responsible, teacher**, *Amsterdam University College*, *Quantum information and quantum communication* courses in Spring 2019 and 2020.
Theme course, co-teaching with three other teachers, responsible for mathematical introduction to quantum information, quantum key distribution

2017-2018 **Teaching Assistant**, *University of Amsterdam*, *Introduction to modern cryptography* courses in fall 2017 and 2018.
This course was taught in flipped classroom style, the roles of the main teacher and the assistants were largely similar

2014-2016 **Teaching Assistant**, *University of Copenhagen*, *Quantum information theory* courses in winters 2014-2016.

2011-2013 **Teaching Assistant**, *University of Freiburg*, *Classical mechanics, Electrodynamics* and *Physics lab course for science students*.

Other professional experience

Research

2009-2011 **Research Assistant**, *Fraunhofer Institute for Solar Energy Systems, Department for Characterization and Development of Solar Cells*, Germany.

Industrial

2007 **Internship**, *BSR Solar Technologies*, Germany.

Students

since 2022 (ongoing) **Fabrizio Sisinni**, *Provable post-quantum security of key encapsulation*, PhD student.

since 2022 (ongoing) **Freja Elbro**, *Code-based cryptography*, PhD student.
supervision taken over from Lars Ramkilde Knudsen

2022 **Andreas Holm Jørgensen**, *Decryption errors in lattice-based encryption schemes*, M.Sc. Thesis.

2022 **Andreas Møller Jørgensen**, *Supersingular isogeny Diffie Hellman key exchange*, M.Sc. Thesis (Link).

2022 **Louise Noer Kolborg**, *Interactive Zero-knowledge Proofs used as Identity Authentication*, B.Sc. Thesis.

2021 **Alco Moerman**, *Are Matrix Action Key Exchanges post-quantum secure?*, B.Sc. Thesis, Mathematics.

2020-2021 **Jilling Kingma**, *Chosen-Blinding unforgeability*, B.Sc. Thesis, Physics. (Link)

2019-2020 **Chanelle Matadah Manfouo**, *Blind-unforgeability of the Winternitz signature scheme*, Visiting student, M.Sc. Thesis for submission at the African Institute for Mathematical Sciences, Kigali, Rwanda.
co-supervision with Stacey Jeffery and Maris Ozols, resulted in this paper

2019-2020 **Laurens Ligthart**, *Linear Quantum Entropy Inequalities beyond Strong Subadditivity and their Applications*, M.Sc. Thesis, Physics.
co-supervision with Michael Walter (Link)

2018-2019 **Hunter McKnight**, *Quantum Shell Games: How to Classically Delegate the Preparation of Authenticated Quantum States*, M.Sc. Thesis for the Master of Logic.
co-supervised with Yfke Dulek, Alex Grilo and Christian Schaffner

2018-2019 **Sebastian Zur**, *The Compressed Oracle and Applications to Quantum Query Solvability*, M.Sc. Thesis, mathematics.
co-supervised with Jan Czajkowski and Christian Schaffner (Link)

2017-2018 **Jelle Don**, *Post-quantum Security of Fiat-Shamir Signatures*, M.Sc. Thesis for the Master of Logic.
co-supervised with Christian Schaffner, resulted in this paper

2017-2018 **Jeroen van Wier**, *Quantum Plaintext Non-Malleability*, M.Sc. Thesis for the Master of Logic.
co-supervised with Christian Schaffner, resulted in this preprint

Talks

Peer-reviewed contributed talks

Crypto and Eurocrypt are the most important and competitive conferences in cryptography, while QIP and QCrypt are the top conferences in theoretical quantum information science, and quantum cryptography, respectively. Where available, videos are linked.

* indicates delivery by a coauthor.

*12/2022 **Asiacrypt 2022**, Regent Hotel, Taipei, *Post-Quantum Security of the Even-Mansour Cipher*

08/2022 **Crypto 2022**, UCSB, Santa Barbara, *Efficient NIZKs and Signatures from Commit-and-Open Protocols in the QROM*

06/2022 **Eurocrypt 2022**, Clarion Hotel, Trondheim, *Post-Quantum Security of the Even-Mansour Cipher*

*06/2022 **Eurocrypt 2022**, Clarion Hotel, Trondheim, *Online Extractability in the Quantum Random Oracle Model*

*03/2022 **QIP 2022**, Pasadena Convention Center, Pasadena, *Post-Quantum Security of the Even-Mansour Cipher*

03/2022 **QIP 2022**, Pasadena Convention Center, Pasadena, *Online-Extractability in the Quantum Random-Oracle Model*

12/2021 **Asiacrypt 2021**, Online, *Tight adaptive reprogramming in the QROM* (video talk created together with Kathrin Hövelmanns)

*07/2021 **ITC 2021**, Online, *Quantum-Access Security of the Winternitz One-Time Signature Scheme*

*02/2021 **QIP 2021**, Online, *Quantum copy protection for compute-and-compare functions in the quantum random oracle model* (merged with *Secure Software Leasing Without Assumptions* by other authors)

02/2021 **QIP 2021**, Online, *Adaptive reprogramming in the QROM*

*08/2020 **Crypto 2020**, Online, *The measure-and-reprogram technique 2.0: Multi-round fiat-shamir and more*

08/2020 **QCrypt 2020**, Online, *Efficient simulation of random states and random unitaries*

*08/2020 **QCrypt 2020**, Online, *Secure Multi-party Quantum Computation with a Dishonest Majority*

05/2020 **Eurocrypt 2020**, Online, *Quantum-secure message authentication via blind-unforgeability*

05/2020 **Eurocrypt 2020**, Online, *Efficient simulation of random states and random unitaries*

*05/2020 **Eurocrypt 2020**, Online, *Secure Multi-party Quantum Computation with a Dishonest Majority*

01/2020 **QIP 2020, plenary talk**, Hilton Shenzhen Shekou Nanhai, Shenzhen, *Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model*

08/2019 **QCrypt 2019**, UQAM, Montréal, *Quantum lazy sampling and game-playing proofs for quantum indifferentiability*

*08/2019 **QCrypt 2019**, UQAM, Montréal, *Security of the Fiat-Shamir transformation in the quantum random-oracle model*

*08/2019 **QCrypt 2019**, UQAM, Montréal, *Non-malleability for quantum public-key encryption*

*08/2019 **Crypto 2019**, UCSB, Santa Barbara, *Security of the Fiat-Shamir transformation in the quantum random-oracle model*

01/2019 **QIP 2019**, CU Boulder, Boulder, *Asymptotic performance of port-based teleportation*

08/2018 **QCrypt 2018**, Shanghai International Conference Center, Shanghai, *Unforgeable quantum encryption*

08/2018 **QCrypt 2018**, Shanghai International Conference Center, Shanghai, *Quantum-secure message authentication via blind unforgeability*

*05/2018 **Eurocrypt 2018**, Dan Panorama Hotel, Tel Aviv, *Unforgeable quantum encryption*

09/2017 **AQIS 2017**, National University of Singapore, Singapore, *Quantum non-malleability and authentication*

*09/2017 **QCrypt 2017**, University of Cambridge, *Quantum non-malleability and authentication*

08/2017 **Crypto 2017**, University of California Santa Barbara, *Quantum non-malleability and authentication*

01/2017 **QIP 2017**, Seattle, *Catalytic decoupling and conditional erasure of correlations*

09/2016 **TQC 2016**, Free University of Berlin, *Catalytic decoupling*

*01/2015 **QIP 2015**, University of Sydney, *Information-theoretic implications of quantum causal structures*

Invited talks and lectures

12/2022 **Quantum crypptography course**, Ruhr University Bochum, *Guest lecture: The quantum-accessible random oracle model: challenges and techniques*

02/2020 **Workshop: Quantum Cryptanalysis of Post-Quantum Cryptography**, Simons institute for the Theory of Computing, Berkeley, *On Attacking Hash functions in Cryptographic schemes*

12/2019 **QSC junior day**, QuSoft, Amsterdam, *Introduction to quantum money*

09/2019 **Quantum Information for Developpers Summerschool**, ETH Zürich, *Quantum cryptography*

10/2018 **Crypto Working Group**, Technical University of Eindhoven, *Quantum-secure message authentication via blind-unforgeability*

09/2017 **Quantum Innovators in Mathematics and Computer Science Workshop**, Institute for Quantum Computing, Waterloo, *Quantum non-malleability and authentication – information theoretic security + a sneak preview*

07/2017 **Beyond IID Workshop**, National University of Singapore, Singapore, *Deconstruction and Conditional Erasure of Correlations*

07/2016 **Beyond IID Workshop**, Institut d'Estudis Catalans, Barcelona, *Catalytic decoupling*

12/2015 **Workshop on Quantum Nonlocality, Causal Structures, and Device-Independent Quantum Information**, National Cheng Kung University, Taiwan, *Information-theoretic implications of quantum causal structures*

12/2014 **Workshop on Quantum Metrology, Interaction, and Causal Structure**, Tsinghua University, *Information-theoretic implications of quantum causal structures*

Invited seminars and colloquia

12/2022 **Ruhr University of Bochum**, CASA distinguished lecture *How do quantum computers break crypto and what are we doing about it?*

11/2022 **Aarhus University**, Seminar of the Cryptography and Security group, *Post-quantum security of Fiat-Shamir signatures in the quantum random oracle model*

10/2020 **University of Copenhagen**, QMATH, Institute for Mathematical Sciences, *Quantum copy-protection of compute-and-compare programs in the quantum random oracle model*

10/2020 **Perimeter Institute**, *Weak approximate unitary designs and applications to quantum encryption*

07/2020 **University of Copenhagen**, QMATH, Institute for Mathematical Sciences, *Efficient simulation of random states and random unitaries*

01/2020 **University of Amsterdam**, Korteweg-de Vries institute for Mathematics, *Port-based teleportation and asymptotic representation theory*

12/2019 **University of Luxembourg**, Interdisciplinary Centre for Security, Reliability and Trust, *Can you sign a quantum state?*

12/2019 **University of Amsterdam**, Informatics Institute, *Cryptography for the quantum Internet – Elements of a "quantum TLS"*

04/2019 **Institut de Mathématique de Tulouse**, *The mathematical structure of port-based teleportation*

01/2019 **Texas A&M University**, Department of Computer Science and Engeneering, *Can you sign a quantum state?*

12/2018 **University of Cologne**, Institute for Theoretical Physics, *Asymptotic performance of port-based teleportation*

09/2018 **University of Copenhagen**, QMATH, Institute for Mathematical Sciences, *Asymptotic performance of port-based teleportation*

04/2018 **Portland State University**, Department of Computer Science, *Unforgeable Quantum Encryption*

04/2018 **University of Maryland**, QuICS, *Asymptotic Port-Based teleportation*

11/2017 **University of Copenhagen**, QMATH, Institute for Mathematical Sciences, *Unforgeable quantum encryption*

04/2017 **Masaryk University**, Faculty of Informatics, *Quantum non-malleability and authentication*

04/2017 **CWI Amsterdam**, *Quantum non-malleability and authentication*

11/2016 **ETH Zurich**, Institute for Theoretical Physics, *Quantum non-malleability and authentication*

11/2016 **Università della Svizzera italiana**, Faculty of Informatics, *Catalytic decoupling*

04/2016 **Free University of Berlin**, Department of Physics, *Catalytic decoupling*

03/2016 **University of Siegen**, Department of Physics, *Catalytic decoupling*

03/2016 **University of Cologne**, Institute for Theoretical Physics, *Catalytic decoupling*

Professional activities

Reviewer Horizon 2020 project “Scalable Oblivious Data Analytics”

PC member Eurocrypt, PKC, PQCrypto, SAC, ITC, QIP, QCrypt, TQC

Conference Referee STOC, FOCS, Crypto, Eurocrypt, Asiacrypt, ITC, TCC, SODA, SOSA, PKC, PQCrypto, QCrypt, TQC, QIP, AQIS

Journal Referee Journal of Cryptology, Journal of the ACM, Sicomp, IEEE Transactions on Information Theory, Entropy, Quantum Information and Computation, Quantum, Physical Review Letters, Journal of Mathematical Physics, Journal of Statistical Physics, Proceedings of the Royal Society, New Journal of Physics, Physical Review A, IEEE Access

Organizer Workshop "Quantum Techniques for Provable Security", affiliated event at Eurocrypt 2021; Weekly *Quantum Lunch* seminar, 2014-2015

Grants and Distinctions

2022 **DFF Sapere Aude grant**.
5.6 Mio. DKK

2022 **MSCA Doctoral Training Network "Quantum-Safe Internet"**.
DTU's share: ∼300k €

2019 **NWO Veni postdoc grant**.
300k €

2009-2014 **Fellow of the German National Academic Foundation**.
~10k €

Social and Outreach

11/2022 **Danish Society of Engineers (IDA)**, *Kryptografi i kvantecomputerens tidsalder (Cryptography in the age of quantum computing)*, Evening talk for a general audience of engineers.

06/2022 **Technical University of Denmark**, *Cryptography in a quantum computing world*, Talk during a visit of the National Cybercrime Center of the National Police of Denmark.

04/2019 **Het Sieraad, Amsterdam**, *Cryptography in the age of quantum computers*, part of "Awesome IT", a career orientation event for undergrads in the information sciences.

05/2018 **Café Checkpoint Charlie, Amsterdam**, *Cryptography in the age of quantum computers*, part of "Pint of Science", an international grass-roots organization aiming to bring science to a general audience by hosting scientific talks in an informal environment.

05/2016 **The Royal Danish Academy of Fine Arts**, School of Architecture, Design and Conservation, *Introduction to quantum mechanics and the 4th dimension for architects*, part of a student seminar course on the spaciality of time.

2009-2011 **University of Freiburg**, member of the Global Marshalplan Initiative student club.

2008 **Tamrat-el-Zeitoun**, Shfar'am, Israel, volunteer.

Languages

German	native speaker
English	proficient
Danish	proficient
Dutch	intermediate
French	basics