# Björn Tackmann, Ph. D.

## Curriculum Vitae

### Personal Information


| | | |
|---|---|---|
| position | Head of Research at DFINITY Foundation | |
| address | DFINITY Foundation<br>Genferstrasse 11<br>8002 Zürich<br>Switzerland | ✉ bjoern@dfinity.org |
| nationality | German, Swiss | |


### Work Experience

| | |
|---|---|
| 2019–... | Senior Researcher, Director of Research, Head of Research at DFINITY Foundation, Zürich, CH |
| 2016–2019 | Postdoctoral Researcher and Research Staff Member at IBM Research Zürich, CH |
| 2014–2016 | Postdoctoral Research Scholar in the Cryptography group of Prof. Mihir Bellare at UC San Diego, US |
| 2008–2014 | Research Assistant and Teaching Assistant in the Information Security and Cryptography group of Prof. Ueli Maurer at ETH Zürich, CH |
| 2007–2008 | Teaching Assistant for cryptography in the Cryptography and Security group of Prof. Müller-Quade at Karlsruhe Institute of Technology, DE |
| 2001–2008 | Software Developer at Consultico GmbH, DE<br>Development of web and client applications, responsible for server administration |

### Education

| | |
|---|---|
| 08/2014 | Ph. D. thesis: "A Theory of Secure Communication"<br>Awarded with the ETH Medal for outstanding Ph. D. theses<br>Advisor: Prof. Ueli Maurer, ETH Zürich, CH<br>Co-examiners: Prof. Mihir Bellare and Prof. Adrian Perrig<br>*ETH Zürich does not assign grades to doctoral theses and examinations.* |
| 07/2008 | M. sc. Mathematics, Karlsruhe Institute of Technology, DE, final grade 1.0<br>Majors: Algebra and Complex Analysis |
| 02/2008 | M. sc. Computer Science, Karlsruhe Institute of Technology, DE, final grade 1.0 *with distinction*<br>Majors: Cryptography and Operating Systems |
| 06/2000 | High school diploma, Grotefend Gymnasium Münden, DE, final grade 1.4<br>German grades: 1.0: very good, 2.0: good, 3.0: satisfactory, 4.0: sufficient, 5.0: failed |

### Awards and Fellowships

| | |
|---|---|
| 2014 | ETH Medal for outstanding Ph. D. theses, ETH Zürich, CH |
| 2014–2016 | Early Postdoc.Mobility Fellowship of the Swiss National Science Foundation (November 2014–October 2016, ∼$70'000) |

## Languages

| | |
|---|---|
| German | Native speaker |
| English | Excellent command |

## Activities

| | |
|---|---|
| 2015–2016 | Head Steward of the Postdoc Union at UC San Diego, US |
| 2010–2014 | Member of the board (President, Vice President) of the association of scientific staff at the Department of Computer Science, member of the Department Council, ETH Zürich, CH |
| 2003–2006 | Student representative in the Department Council of the Department of Computer Science, Karlsruhe Institute of Technology, DE |
| 2006 | Student representative in the senate, Karlsruhe Institute of Technology, DE |

## Teaching Experience

| | |
|---|---|
| winter 2016 | Co-instruction of "Transport Layer Security" course at UC San Diego with Prof. Hovav Shacham |
| 2009–2014 | Teaching assistance in "Cryptography" (Masters level) at ETH Zürich with Prof. Ueli Maurer, 5 years in a row, substitution of Prof. Maurer for classes on several occasions |
| spring 2009 | Teaching assistance in "Informationssicherheit" (information security, third-year Bachelors level) at ETH Zürich with Prof. Ueli Maurer |
| autumn 2008 | Teaching assistance in "Diskrete Mathematik" (discrete mathematics, first-year Bachelors level) at ETH Zürich with Prof. Ueli Maurer |
| spring 2008 | Teaching assistance in "Signale, Codes und Chiffren II" (signals, codes, and ciphers, part II, Masters level) at KIT with Dr. Willi Geiselmann |
| autumn 2007 | Teaching assistance in "Public-Key Kryptographie für Informationswirte" (public-key cryptography for business informatics, Bachelors level) at KIT with Dr. Willi Geiselmann |

## Student Supervision

| | |
|---|---|
| M.sc. | Daniel Jost: *A Constructive Analysis of IPSec* (10/2013–04/2014) |
| | Christian Badertscher: *Key Exchange Security in Constructive Cryptography* (04/2012–10/2012) |
| | Andreas Rüedlinger: *Restricted Types of Malleability in Encryption Schemes* (10/2010–04/2011) |
| B.sc. | Marco Nembrini: *Constructing Channels and Keys—A Classification* (02/2011–05/2011) |

✈ DFINITY Foundation
Genferstrasse 11
8002 Zürich
Switzerland

✉ bjoern@dfinity.org
✻ April 13, 1980 in Kassel, DE

## Service to the Research Community

I was member of the organizing committee of TCC 2010. I co-organized the workshop PENCIL that was affiliated with Eurocrypt 2018. I am co-organizing the workshop CTB that is affiliated with Eurocrypt 2024.
I served as associate editor of IET Information Security.
I participated in program committees of:

- ACM CCS 2018
- Eurocrypt 2018
- Crypto 2019

Reviewer for international conferences on cryptography and theoretical computer science:

- Africacrypt
- Asiacrypt
- CANS
- COCOON
- CRYPTO
- CT-RSA
- Eurocrypt
- ICITS
- ISIT
- PKC
- SCN
- TCC

Reviewer for journals:

- Journal of the ACM
- Journal of Cryptology
- IEEE Transactions on Information Theory
- Theoretical Computer Science
- International Journal of Communication Systems
- IEEE Transactions on Dependable and Secure Computing

✈ DFINITY Foundation
Genferstrasse 11
8002 Zürich
Switzerland

✉ bjoern@dfinity.org
✻ April 13, 1980 in Kassel, DE

## Conference Publications

30. Dmytro Bogatov, Angelo De Caro, Kaoutar Elkhiyaoui, and Björn Tackmann. Anonymous Transactions with Revocation and Auditing in Hyperledger Fabric. In *Cryptology and Network Security*, 2021.

29. Christian Badertscher, Ran Canetti, Julia Hesse, Björn Tackmann, and Vassilis Zikas. Universal composition with global subroutines: Capturing global setup within plain UC. In **Theory of Cryptography—TCC**, 2020.

28. Elli Androulaki, Jan Camenisch, Angelo De Caro, Maria Dubovitskaya, Kaoutar Elkhiyaoui, Björn Tackmann. Privacy-preserving auditable token payments in a permissioned blockchain system. In *ACM Conference on Advances in Financial Technologies*, 2020.

27. Mihir Bellare, Ruth Ng, and Björn Tackmann. Nonces are noticed: AEAD revisited. In **CRYPTO**, 2019.

26. Sergiu Costea, Marios O Choudary, Doru Gucea, Björn Tackmann, and Costin Raiciu. Secure Opportunistic Multipath Key Exchange. In **ACM CCS**, 2018.

25. Christian Badertscher, Ueli Maurer, and Björn Tackmann. On Composable Security for Digital Signatures. In *Public-Key Cryptography*, 2018.

24. Christian Cachin, Esha Ghosh, Dimitris Papadopoulos, and Björn Tackmann. Stateful Multi-Client Verifiable Computation. In *Applied Cryptography and Network Security*, 2018.

23. Anja Lehmann und Björn Tackmann. Updatable Encryption with Post-Compromise Security. In **EUROCRYPT**, 2018.

22. Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann Per-session security: Password-based cryptography revisited. In *ESORICS*, 2017.

21. Björn Tackmann. Secure event tickets on a blockchain. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, 2017.

20. Joël Alwen and Björn Tackmann. Moderately hard functions: Definition, instantiations, and applications. In **Theory of Cryptography—TCC**, 2017.

19. Mihir Bellare and Björn Tackmann. The Multi-User Security of Authenticated Encryption: AES-GCM in TLS 1.3. In **CRYPTO**, 2016.

18. Mihir Bellare and Björn Tackmann. Nonce-Based Cryptography: Retaining Security when Randomness Fails. In **EUROCRYPT**, 2016.

17. Sandro Coretti, Yevgeniy Dodis, Björn Tackmann, and Daniele Venturi. Non-Malleable Encryption: Simpler, Shorter, Stronger. In **Theory of Cryptography—TCC**, 2016.

16. Christopher Portmann, Renato Renner, Christian Matt, Ueli Maurer, and Björn Tackmann. Causal Boxes: Quantum Information-Processing Systems Closed under Composition. In *Quantum Information Processing—QIP*, 2016.

15. Juan Garay, Björn Tackmann, and Vassilis Zikas. Fair Distributed Computation of Reactive Functions. In *International Symposium on Distributed Computing*, 2015.

14. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi. (De-)Constructing TLS 1.3. In *Indocrypt*, 2015.

✈ DFINITY Foundation
Genferstrasse 11
8002 Zürich
Switzerland

✉ bjoern@dfinity.org
✻ April 13, 1980 in Kassel, DE

13. Juan Garay, Jonathan Katz, Björn Tackmann, and Vassilis Zikas. How Fair is You Protocol? A Utility-based Approach to Protocol Optimality. In **ACM Principles of Distributed Computing**, 2015.

12. Grégory Demai, Peter Gaži, Ueli Maurer, and Björn Tackmann. Query-Complexity Amplification for Random Oracles. In *International Conference on Information-Theoretic Security*, 2015.

11. Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway, and Björn Tackmann. Robust Authenticated Encrypton and the Limits of Symmetric Cryptography. In *IMA Workshop on Cryptography and Coding*, 2015.

10. Christian Badertscher, Christian Matt, Ueli Maurer, Phillip Rogaway, and Björn Tackmann. Augmented Secure Channels and the Goal of the TLS 1.3 Record Layer. In *International Conference on Provable Security*, 2015.

9. Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi. From Single-Bit to Multi-Bit Public-Key Encryption via Non-Malleable Codes. In **Theory of Cryptography—TCC**, 2015.

8. Grégory Demai, Peter Gaži, Ueli Maurer, and Björn Tackmann. Optimality of Non-Adaptive Strategies: The Case of Parallel Games. In *Information Theory Proceedings — ISIT*, 2014.

7. Sandro Coretti, Ueli Maurer, and Björn Tackmann. Constructing Confidential Channels from Authenticated Channels—Public-Key Encryption Revisited. In **Advances in Cryptology—ASIACRYPT**, 2013.

6. Juan Garay, Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Rational Protocol Design: Cryptography against Incentive-driven Adversaries. In **Foundations of Computer Science (FOCS)**, 2013.

5. Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi. Anonymity-Preserving Public-Key Encryption: A Constructive Approach. In *Privacy Enhancing Technologies (PETS)*, 2013.

4. Jonathan Katz, Ueli Maurer, Björn Tackmann, and Vassilis Zikas. Universally Composable Synchronous Computation. In **Theory of Cryptography—TCC**, 2013.

3. Ueli Maurer, and Björn Tackmann. Synchrony Amplification. In *Information Theory Proceedings — ISIT*, 2012.

2. Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann. Confidentiality and Integrity: A Constructive Perspective. In **Theory of Cryptography—TCC**, 2012.

1. Ueli Maurer and Björn Tackmann. On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption. In **ACM Conference on Computer and Communications Security (CCS)**, 2010.

## JOURNAL PUBLICATIONS

5. Christian Cachin, Angelo De Caro, Pedro Moreno-Sanchez, Björn Tackmann, and Marko Vukolič. The Transaction Graph for Modeling Blockchain Semantics. In *Cryptoeconomic Systems*, 2021.

4. Sandro Coretti, Yevgeniy Dodis, Ueli Maurer, Björn Tackmann, and Daniele Venturi. Non-malleable encryption: simpler, shorter, stronger. In *Journal of Cryptology*, 2020.

✈ DFINITY Foundation
Genferstrasse 11
8002 Zürich
Switzerland

✉ bjoern@dfinity.org
✻ April 13, 1980 in Kassel, DE

3. Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann. Per-session security: Password-based cryptography revisited. In *Journal of Computer Security*, 2019.

2. Christian Matt, Ueli Maurer, Christopher Portmann, Renato Renner, and Björn Tackmann. Toward an algebraic theory of systems. In *Theoretical Computer Science*, 2018.

1. Christopher Portmann, Renato Renner, Christian Matt, Ueli Maurer, and Björn Tackmann. Causal Boxes: Quantum Information-Processing Systems Closed under Composition. In *IEEE Transactions on Information Theory*, 2017.

## Book Chapters

2. Björn Tackmann and Ivan Visconti. Cryptographic Tools for Blockchains. Book chapter in *Principles of Blockchain Systems*, 2021.

1. Sandro Coretti, Ueli Maurer, and Björn Tackmann. A Constructive Perspective on Key Encapsulation. Book chapter in *Number Theory and Cryptography*, Springer LNCS 8260, 2013.

Conferences are the major publication channel in cryptography; publications are peer reviewed and appear as full papers online and/or printed in proceedings. Authors are generally ordered alphabetically. The up-to-date list of publications and citation statistics can be found on my Google scholar page, all papers are available as PDF on my personal web site.

✈ DFINITY Foundation
Genferstrasse 11
8002 Zürich
Switzerland

✉ bjoern@dfinity.org
✻ April 13, 1980 in Kassel, DE