Curriculum Vitae

Björn Tackmann

Personal Information

Position:	Postdoctoral Research Scholar with Mihir Bellare, UC San Diego
Office address:	UC San Diego, Computer Science & Engineering EBU3b 9500 Gilman Drive La Jolla, CA 92093-0404 USA
E-Mail:	btackmann@eng.ucsd.edu
Homepage:	http://cseweb.ucsd.edu/∼btackmann/

Research and Practical Experience

	since	11/2014	Postdoctoral Research Scholar at UC San Diego
08/2008	to	10/2014	Research Assistant at ETH Zürich, Switzerland
04/2001	to	07/2008	Programmer at Consultico GmbH, Fuldabrück/Bochum Development of web and client applications in Perl, Java, Delphi, Administration of company's Linux-based web and mail server

Education

08/2008	to	10/2014	PhD Student at ETH Zürich, Department of Computer Science Cryptography and Information Security group, Prof. Ueli Maurer Thesis: *A Theory of Secure Communication* Co-examiners: Prof. Mihir Bellare (UCSD) Prof. Adrian Perrig (ETH Zürich)
04/2003	to	07/2008	Studies in Mathematics at Universität Karlsruhe (TH), "Diplom-Mathematiker" (equivalent to M.Sc.), final grade 1.0, 07/21/2008 Majors: Algebra and Complex Analysis
10/2001	to	02/2008	Studies in Informatics at Universität Karlsruhe (TH) Degree: "Diplom-Informatiker" (equivalent to M.Sc.), final grade 1.0, with distinction, 02/01/2008 Majors: Cryptography and System Architecture Thesis: *Security Properties and Mathematical Foundations of Key Agreement Protocols* Advisors: Jörn Müller-Quade (CS) and Stefan Kühnlein (Math)

German grades: 1.0: very good, 2.0: good, 3.0: satisfactory, 4.0: sufficient, 5.0: failed

Teaching Experience

08/2008	to	10/2014	Teaching assistant at ETH Zürich for courses: Discrete Mathematics (2008) Information Security (2009) Cryptography (2009, 2010, 2012, 2013, 2014)
10/2007	to	06/2008	Teaching assistant for two courses on cryptography at IAKS (now IKS), Universität Karlsruhe (TH)

Student Supervision

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

Service to the University

2015	Head steward of the postdoc union at UC San Diego
2010–2014	Representative of the scientific staff in the department conference at the CS department, ETH Zürich
2013	Faculty recruiting committee (CS), ETH Zürich
2010–2012	Member of the board (2010 vice-president, 2011 president) of the association of the scientific staff of the CS department, ETH Zürich
2003, 2006, 2007	Faculty recruiting committees (CS), Universität Karlsruhe (TH)
2006	Student representative in the senate of Universität Karlsruhe (TH)
2003–2006	Student representative in the faculty council ("Fakultätsrat") of the faculty of informatics ("Fakultät für Informatik"), Universität Karlsruhe (TH)

Service to the Research Community

Sub-reviewer for international conferences on cryptography:

Africacrypt	2009
Asiacrypt	2010, 2014, 2015
CANS	2014
COCOON	2014
CRYPTO	2009, 2012, 2014
CT-RSA	2009
Eurocrypt	2011, 2013, 2014, 2016
ICITS	2009, 2013
ISIT	2013
PKC	2011, 2016
SCN	2010, 2012
TCC	2012, 2013, 2014, 2015

Reviewer for Journal of the ACM, Journal of Cryptology, IEEE Transactions on Information Theory, and Theoretical Computer Science

Member of the organizing committee of TCC 2010

Awards and Funding

Early PostDoc.Mobility Fellowship, Swiss National Science Foundation. "Constructive Design of Secure Channels Protocols." November 2014—April 2016, $\approx$ \$70k.

ETH Medal for outstanding PhD thesis, December 2014

Seminar and Workshop Talks

Microsoft Research Cambridge, UK. "A Constructive Approache to Secure-Channel Protocols." December 2015.

IBM Research Zurich, Switzerland. "A Constructive Approache to Secure-Channel Protocols." December 2015.

NEC Research Heidelberg, Germany. "Secure Communication over the Internet: TLS and beyond." July 2015.

Sapienza University of Rome, Italy. "Unilaterally Authenticated Key Establishment—A Constructive Perspective." September 2014.

Key Exchange and Secure Channels Workshop, Bertinoro, Italy. "A Constructive Perspective on Secure Channels." June 2014.

University of California, Los Angeles, USA. "Constructive Cryptography—Introduction and Applications." October 2013.

University of California, San Diego, USA. "Constructive Cryptography—Introduction and Applications." October 2013.

Aarhus University, Denmark. "Constructive Cryptography—Introduction and Current Trends." May 2013.

Dagstuhl Workshop on Public-Key Encryption, Germany. "Integrity Notions for Encryption Schemes: A Constructive Perspective." September 2011.

AT&T Research Labs, Florham Park, USA. "The Malleability of Symmetric Encryption: Definition and Applications." August 2011.

University of Maryland, USA. "Integrity Notions for Encryption Schemes: A Constructive Perspective." August 2011.

ECRYPT MAYA Meeting, Salerno, Italy. "Integrity Notions for Encryption Schemes—Without any Oracles." July 2011.

Royal Holloway, University of London, UK. "Authenticate-then-Encrypt: A Constructive Perspective." March 2011.

Conference Publications

Sandro Coretti, Yevgeniy Dodis, Björn Tackmann, and Daniele Venturi. From Single-Bit to Multi-Bit Public-Key Encryption via Non-Malleable Codes. In *Theory of Cryptography—TCC*, 2016, to appear.

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, to appear.

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

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.

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.

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

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.

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

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.

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.

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

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.

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.

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

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

Ueli Maurer, Andreas Rüedlinger, and Björn Tackmann. Confidentiality and Integrity Revisited. In *Theory of Cryptography—TCC*, 2012.

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.

Book Chapter

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

NON-REFEREED PUBLICATIONS

Markulf Kohlweiss, Ueli Maurer, Cristina Onete, Björn Tackmann, and Daniele Venturi. (De-)-Constructing TLS. Cryptology ePrint Archive, Report 2014/020.

Sandro Coretti, Ueli Maurer, and Björn Tackmann. Key Exchange with Unilateral Authentication: Composable Security Definition and Modular Protocol Design. Cryptology ePrint Archive, Report 2013/555.