Curriculum Vitae

Prof. Dr. phil. nat. Marc Fischlin

Contact Data

Technische Universität Darmstadt
Chair for Cryptography and Complexity Theory
Department of Computer Science
Phone: +49 (0)6151 16 25730
E-mail: marc.fischlin@cryptoplexity.de

Education and Professional Experience

since 07/11	W3-Professor TU Darmstadt (funded through Heisenberg Program 07/11-06/16)
02/06 – 01/11	Emmy Noether Group Leader, TU Darmstadt
09/04 – 08/05	Post-Doc, ETH Zurich, Switzerland (Emmy Noether Program)
09/03 – 08/04	Post-Doc, UCSD, San Diego, USA (Emmy Noether Program)
06/02 – 08/03	Post-Doc, Fraunhofer Institute Secure IT, Darmstadt
07/97 – 12/01	PhD, Mathematics Department, J.W. Goethe-Universität (suspended for community service in 1998)
10/94 – 04/98	Study of Computer Science, J.W. Goethe-Universität in Frankfurt/Main
10/92 – 06/97	Study of Mathematics, J.W. Goethe-Universität in Frankfurt/Main

Awards

Fraunhofer SmartCard Award 2014.

Miscellaneous

Program committee member of more than 40 international cryptographic conferences, including the IACR flagship conferences Crypto (2009, 2012), Eurocrypt (2005, 2007, 2009, 2012), and Asiacrypt (2010, 2012, 2014). Program chair of Eurocrypt 2015 (incoming) and 2016 (outgoing), as well as CT-RSA 2009 and PKC 2012.

Grant reviewer for ERC, DFG, FWO, GIF, EPSRC, Humboldt Foundation, Finland Academy.

External PhD, Habilitation, and hiring committee member for ETH Zurich, ENS Paris, KTH Sweden, U Leuven, U Karlsruhe, and U Berlin.

Supervised PhD Students

Arno Mittelbach. Random Oracles in the Standard Model. 02/2012-12/2015.
Paul Baecher. Cryptographic Reductions: Classification and Applications to Ideal Models. 04/2010-10/2014.
Özgür Dagdelen. The Cryptographic Security of the German Electronic Identity Card. 06/2009-06/2013.
Christina Brzuska. On the Foundations of Key Exchange. 05/2010-10/2012.
Cristina Onete. Security Aspects of Distance-Bounding Protocols. 02/2009-07/2012.
Dominique Schröder. On the Complexity of Blind Signatures. 10/2006-11/2010.
Anja Lehmann. On the Security of Hash Function Combiners. 08/2006-03/2010.

Selected Projects and Research Grants

BMBF=Federal Ministry of Education and Research, BSI=Federal Office for Information Security, DFG=German Research Foundation

ongoing:

BSI (since 04/2016): Security Evaluation of Schnorr Signatures

DFG Collaborative Research Center (from 10/2014 on):
CROSSING – Cryptography-Based Security Solutions: Enabling Trust in New and Next Generation Computing Environments, Principal Investigator and Deputy Speaker.

DFG Research Training Group (from 10/2015 on):
Privacy and Trust for Mobile Users, Principal Investigator.

DFG project Security-Preserving Operations on Big Data (with Alex May, from 07/2014-06/2016):
Part of the Priority Program 1736 Algorithms for Big Data

EU COST Action 1306: Cryptography for Secure Digital Interaction (since 04/2014)
MC (Germany).

completed:

Bundesdruckerei GmbH (10/2015-02/2016): Expert Report on eIDAS systems.

DFG-Heisenberg FI 940/3-1 (07/2011-06/2016): Scrutinizing Black-Box Separations in (Quantum) Cryptography.

DFG FI 940/4-1 (02/2011-06/2016): Scrutinizing Black-Box Separations in (Quantum) Cryptography.

Giesecke&Devrient (12/2013-01/2014): Expert Report on ISO 29167.

BMBF ProtoTo (06/2011-05/2013):
Holistic Development of Security Protocols, with DFKI (Coordinator), Kobil Systems, Sirrix AG.

BSI (12/2010-12/2013): Security Proofs for Federal Identification Documents.

BMBF EC SPRIDE (10/2010-07/2016):
Competence Center for IT Security, Principal Investigator.

LOEWE Initiative State Hesse (07/2008-06/2016):
Center for Advanced Security Research Darmstadt (CASED), Principal Investigator.

DFG-Emmy Noether Group FI 940/2-1 (02/2006-01/2011): Minimizing Cryptographic Assumptions.

DFG-Emmy Noether FI 940/1-1 (09/2003-08/2005):
Praktikable und beweisbar sichere Kryptographische Protokolle.

Brief Description of the Chair for Cryptography and Complexity Theory

Our research area is complexity-based cryptography which investigates the relationship of (abstract or concrete) cryptographic problems, such as the security of complex cryptographic protocols built out of more fundamental cryptographic primitives. Our security proofs for the protocols of the new German identity card are a concrete example for our work.

Central to our research are the question of modelling (what does it mean to be secure?) and the notion of a reduction, originating from complexity theory and nowadays forming the common technique to conduct security proofs. We are interested in both the applications of these notions as well as the notions as a research topic themselves. This requires vivid interaction with related areas like complexity theory, IT security, number theory, or algorithmics.

We view ourselves as a research-oriented group which, in collaboration with national and international partners from research, industry and the public sector, enhances the areas of cryptography and IT security. Our actions are based on the Rules of Good Scientific Practice, as described for example by the German Research Foundation (DFG).

More information available at **`www.cryptoplexity.de`**

Publications

Author of more than 70 peer-reviewed publications in the area of cryptography and IT security. More than 2750 citations, H-index of 29 (according to Google scholar).

Selected Publications:

[1] Marc Fischlin, Felix Günther, Giorgia Azzurra Marson, Kenneth G. Paterson: Data Is a Stream: Security of Stream-Based Channels. CRYPTO 2015, Lecture Notes in Computer Science, 2015.

[2] Christina Brzuska, Marc Fischlin, Bogdan Warinschi, Stephen C. Williams: Composability of Bellare-Rogaway key exchange protocols. ACM Conference on Computer and Communications Security 2011, ACM.

[3] Mihir Bellare, Marc Fischlin, Adam O'Neill, Thomas Ristenpart: Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles. CRYPTO 2008, Lecture Notes in Computer Science, Springer.

[4] Ran Canetti, Marc Fischlin: Universally Composable Commitments. CRYPTO 2001, Lecture Notes in Computer Science, Springer.

[5] Marc Fischlin: Lower Bounds for the Signature Size of Incremental Schemes. FOCS 1997, IEEE.