Sebastian Faust

Curriculum Vitae

Ruhr Univerität Bochum
Business: Universitätsstrasse 150, D-44780 Bochum
Private: Steinkuhlstr. 2, D-44799 Bochum
☎ *+49 (0)234 32 23265*
☎ *+49 (0)160 109 5858*
✉ *sebastian.faust@rub.de*

PROFESSIONAL EXPERIENCE

From Apr15 **Juniorprofessor in Cryptography**, *Department of Mathematics*, Ruhr-Universität Bochum, Germany.

Apr13–Mar15 **Postdoc in Cryptography and IT Security**, *Department of Computer Science*, EPFL, Switzerland, headed by Prof. Serge Vaudenay.

Funding: Marie Curie IEF fellowship: ∼ 200.000 EUR.

May11–Mar13 **Postdoc in Cryptography**, *Department of Computer Science*, Aarhus University, Denmark, headed by Prof. Ivan Damgård and Prof. Jesper Buus Nielsen.

Jan11–Apr11 **Postdoc in Cryptography and IT Security**, *Department of Electrical Engineering*, KU Leuven, Belgium, headed by Prof. Bart Preneel.

Aug06–Dec10 **PhD student**, *Department of Electrical Engineering*, KU Leuven, Belgium, headed by Prof. Bart Preneel.

Funding: Microsoft Research European PhD fellowship: ∼ 100.000 EUR.

Research visits: Fall 2008 & Summer 2009 Boston University and MIT (USA), Spring 2009 CWI Amsterdam (Netherlands)

. Jun05–Aug06 **Full time (freelancing) Consultant**, *SEB Bank AG, Frankfurt*, Germany.

1998–2003 **Part-time (freelancing) software engineer**, *Commerzbank AG, Siemens AG and GlaxoSmithKline.*

ACADEMIC DEGREES

December 10 **PhD in Engineering**, *Department of Electrical Engineering*, KU Leuven, Belgium.

Advisor: Prof. Bart Preneel and Dr. Gregory Neven.

PhD focus: My thesis was on the provable security of cryptographic implementations against side-channel leakage. In particular, I designed the first leakage resilient signature scheme and initiated the concept of computationally bounded leakage.

Sep. 05 **Master in Business Informatics ("Diplom in Wirtschaftsinformatik")**, *Universität Mannheim*, Germany.

Specialization: Cryptography, IT-security & Finance

Final grade: Total grade: 1.4. Grade of thesis: 1.0 supervised by Prof. Stefan Lucks.

April 1999 **Abitur**, *Ernst-Reuter Schule*, Bad Vilbel, Germany.

AWARDS

2015 **DFG Emmy Noether Programme**, *for project "Cryptography beyond the black-box model"*, acceptance rate approx. 20%.

2014 **Best paper award at Eurocrypt 2014**, *for publication "Unifying leakage models: from probing attacks to noisy leakage"*, (out of 197 submissions).

2013 **Marie Curie Fellowship 2013**, out of 6.500 submissions, acceptance rate $< 12.5\%$.

2013 **Invited to Journal of Cryptographic Engineering (1 out of 5 invitations) at CHES 2013**, *for publication "Masking vs. Multiparty Computation: How Large is the Gap for AES?"*, (out of 132 submissions).

2012 **Invited to Journal of Cryptology (1 out of 3 invitations) at Asiacrypt 2012**, *for publication "Theory and Practice of a leakage resilient masking scheme"*, (out of 247 submissions).

2007 **Microsoft Research PhD scholarship**, out of 120 submissions, acceptance rate $< 15\%$.

2005 **Travel award for Master thesis 2005**, *to attend autumn school in cryptography in Bertinoro, Italy.*

RESEARCH GRANTS AND FUNDING

DFG Emmy Noether Program, *2015-2020, Principal investigator*, Project name: "Cryptography beyond the black-box model", ca. 820.000 EUR.
Acceptance rate ca. 20%.

Partner of DFG Graduate school at Ruhr-Universität Bochum, *Project name: "New Challenges for cryptography in ubiquitous computing"*, my part: ca. 200.000 EUR.

Marie Curie FP7-2013 IEF fellowship, *2014-2015, Principal investigator*, Project name: "GAPS – Guiding Physical Security by Proofs", approx. 200.000 EUR.
6.500 applications and acceptance rate $< 12.5\%$.

Microsoft Research European PhD scholar, *2007-2010, Principal investigator*, Project name: "Provable security at implementation-level", approx. 100.000 EUR.
120 applications and acceptance rate $< 15\%$.

COST Action IC 1306, *from April 2014, COST national coordinator for Switzerland in COST action "Cryptography for secure digital interaction".*

Microsoft-ETHZ-EPFL Joint Research Center MSJRC program, *Contributor to the proposal "Authenticated Encryption: Security Notions, Constructions and Applications" for a joint research center between Microsoft Research and ETHZ-EPFL*, approx. 210.00 CHF.

Other minor scholarships, *Several small travel scholarships (each approx. 3.000 EUR) for visiting the US in 2008/2009 from the Research Foundation Flanders (Belgium).*

PUBLICATIONS

Publications in cryptography use alphabetical order. The main venues are Asiacrypt, Crypto and Eurocrypt, where I have published **13 works** and won the prestigious **Best paper award** at Eurocrypt 2014. Moreover, I published results at more applied venues such as CHES and ACM CCS, which illustrate the versatility of my research. Most of my other results also appeared at top venues including, IACR TCC, IACR PKC, ICALP and PETS.

Conference Proceedings

[C32] Stefan Dziembowski and Sebastian Faust and François-Xavier Standaert: Private Circuits III: Hardware Trojan-Resilience via Testing Amplification. To appear at ACM CCS 2016.

[C31] Stefan Dziembowski and Sebastian Faust and Gottfried Herold and Anthony Journault and Daniel Masny and François-Xavier Standaert: Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems. To appear at IACR Crypto 2016.

[C30] Marcin Andrychowicz, Stefan Dziembowski and Sebastian Faust. Circuit Compilers with $O(1/\log(n))$ Leakage Rate. In 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2016. Springer Verlag, LNCS 9666, 586-615.

[C29] Sebastian Faust, Daniel Masny, Daniele Venturi. Chosen-Ciphertext Security from Subset Sum. In 19th International Conference on Practice and Theory in Public-Key Cryptography – IACR PKC 2016. Springer Verlag, LNCS 9614, 35-46.

[C28] Stefan Dziembowski, Sebastian Faust, Maciej Skorski. Optimal Amplification of Noisy Leakages. In 13th Theory of Cryptography Conference – IACR TCC 2016-A. Springer Verlag, LNCS 9563, 291-318.

[C27] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, Krzysztof Pietrzak: Proofs of Space. In 35th Annual Cryptology Conference – IACR Crypto 2015. Springer Verlag, LNCS 9216, 585-605.

[C26] Alexandre Duc, Sebastian Faust and François-Xavier Standaert: Making Masking Security Proofs Concrete (Or How to Evaluate the Security of any Leaking Device). In 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2015. Springer Verlag, LNCS 9056, 401-429.

[C25] Stefan Dziembowski, Sebastian Faust and Maciej Skorski: Noisy leakages revisited. In 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2015. Springer Verlag, LNCS 9057, 159-188.

[C24] Josep Balasch, Sebastian Faust and Benedikt Gierlichs: Inner Product masking revisited. In 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2015. Springer Verlag, LNCS 9056, 486-510.

[C23] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee and Daniele Venturi: The Chaining Lemma and its Application. In 8th International Conference on Information-Theoretic Security – ICITS 2015. Springer Verlag, LNCS 9063, 181-196.

[C22] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen and Daniele Venturi: A Tamper and Leakage Resilient von Neumann Architecture. In 18th International Conference on Practice and Theory in Public-Key Cryptography – IACR PKC 2015. Springer Verlag, LNCS 9020, 579-603.

[C21] Marcin Andrychowicz, Ivan Damgaard, Stefan Dziembowski, Sebastian Faust and Antigoni Polychroniadou: Efficient Leakage Resilient Circuit Compilers. In Topics in Cryptology – CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015. Springer Verlag, LNCS 9048, 311-329.

[C20] Alexandre Duc, Stefan Dziembowski and Sebastian Faust: Unifying Leakage Models: from probing attacks to noisy leakage. In 33th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2014. Springer Verlag, LNCS 8441, 423-440. (***Best paper award***).

[C19] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi and Daniel Wichs: Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits. In 33th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2014. Springer Verlag, LNCS 8441, 111-128.

[C18] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen and Daniele Venturi: Continuous Non-malleable Codes. In 11th Theory of Cryptography Conference – IACR TCC 2014. Springer Verlag, LNCS 8349, 465-488.

[C17] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee and Daniele Venturi: Bounded Tamper Resilience: How to go beyond the Algebraic Barrier. In 19th International Conference on the Theory and Application of Cryptology and Information Security – IACR Asiacrypt 2013. Springer Verlag, LNCS 8270, 140-160.

[C16] Vincent Grosso, François-Xavier Standaert and Sebastian Faust: Masking vs. Multiparty Computation: How Large is the Gap for AES? In 15th International Workshop on Cryptographic Hardware and Embedded Systems – IACR CHES 2013. Springer Verlag, LNCS 8086, 400-416. (***1 out of 5 invitations to Journal of Cryptographic Engineering***).

[C15] Sebastian Faust, Carmit Hazay and Daniele Venturi: Outsourced Pattern Matching. In 40th International Colloquium on Automata, Languages, and Programming – ICALP 2013. Springer Verlag, LNCS 7966, 545-556.

[C14] Josep Balasch, Sebastian Faust, Benedikt Gierlichs and Ingrid Verbauwhede: Theory and Practice of a Leakage Resilient Masking Scheme. In 18th International Conference on the Theory and Application of Cryptology and Information Security – IACR Asiacrypt 2012. Springer Verlag, LNCS 7658, 758-775. (***1 out of 3 invitations to Journal of Cryptology***).

[C13] Sebastian Faust, Carmit Hazay, Jesper Buus Nielsen, Peter Sebastian Nordholt and Angela Zottarel: Signature Schemes Secure against Hard-to-Invert Leakage. In 18th International Conference on the Theory and Application of Cryptology and Information Security – IACR Asiacrypt 2012. Springer Verlag, LNCS 7658, 98-115.

[C12] Sebastian Faust, Markulf Kohlweiss, Giorgia Azzurra Marson and Daniele Venturi: Fiat-Shamir Proofs are Simulation Sound. In Progress in Cryptology – INDOCRYPT 2012. Springer Verlag, LNCS 7668, 60-79.

[C11 Sebastian Faust, Krzysztof Pietrzak and Joachim Schipper: Practical Leakage-Resilient Symmetric Cryptography. In 14th International Workshop on Cryptographic Hardware and Embedded Systems – IACR CHES 2012. Springer Verlag, LNCS 7428, 213-232.

[C10] Ivan Damgård, Sebastian Faust and Carmit Hazay: Secure Two-Party Computation with Low Communication. In 9th Theory of Cryptography Conference – IACR TCC 2012. Springer Verlag, LNCS 7194, 54-74.

[C09] Stefan Dziembowski and Sebastian Faust: Leakage Resilient Circuits without Computational Assumptions. Stefan Dziembowski and Sebastian Faust. In 9th Theory of Cryptography Conference – IACR TCC 2012. Springer Verlag, LNCS 7194, 230-247.

[C08] Sebastian Faust, Krzysztof Pietrzak and Daniele Venturi: Tamper Resilient Circuits: How to Trade Leakage for Tamper-Resilience? In 38th International Colloquium on Automata, Languages, and Programming – ICALP 2011. Springer Verlag, LNCS 6755, 391-402.

[C07] Stefan Dziembowski and Sebastian Faust: Leakage Resilient Cryptography from the inner product extractor. In 17th International Conference on the Theory and Application of Cryptology and Information Security – IACR Asiacrypt 2011. Springer Verlag, LNCS 7073, 702-721.

[C06] Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer and Vinod Vaikuntanathan: Protecting Circuits from Leakage: the Computationally-Bounded and Noisy Cases. In 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques – IACR Eurocrypt 2010. Springer Verlag, LNCS 6110, 135-156.

[C05] Sebastian Faust, Krzysztof Pietrzak and Daniele Venturi: Leakage-Resilient Signatures. In 7th Theory of Cryptography Conference – IACR TCC 2010. Springer Verlag, LNCS 5978, 343-360.

[C04] Sebastian Faust, Emilia Kasper, Stefan Lucks: Efficient Simultaneous Broadcast. In 11th International Conference on Practice and Theory in Public-Key Cryptography – IACR PKC 2008. Springer Verlag, LNCS 4939, 180-196.

[C03] George Danezis, Claudia Diaz, Sebastian Faust, Emilia Kasper, Carmela Troncoso and Bart Preneel: Efficient Negative Databases from Cryptographic Hash Functions. In 10th International Conference on Information Security ICS 2007. Springer Verlag, LNCS 4779, 423-436.

[C02] Markulf Kohlweiss, Sebastian Faust, Lothar Fritsch, Bartek Gedrojc and Bart Preneel: Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker. In 7th International Symposium on Privacy Enhancing Technologies – PETS 2007. Springer Verlag, LNCS 4776, 77-94.

[C01] Sebastian Faust, Emilia Kasper and Stefan Lucks: A Protocol for the Distributed Generation of Random Values and Some Applications. 1st Benelux Workshop on Information and System Security – WISSEC 2006, 11 pp.

Journals

[J04] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee and Daniele Venturi: Bounded Tamper Resilience: How to go beyond the Algebraic Barrier. To appear in Journal of Cryptology 2016.

[J03] Sebastian Faust, Carmit Hazay, Jesper Buus Nielsen, Peter Sebastian Nordholt and Angela Zottarel: Signature Schemes Secure against Hard-to-Invert Leakage. In Journal of Cryptology 29(2): 422-455 (2016).

[J02] Vincent Grosso, François-Xavier Standaert and Sebastian Faust: Masking vs. Multiparty Computation: How Large is the Gap for AES? In Journal of Cryptographic Engineering 4(1): (2014), 47-57.

[J01] Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer and Vinod Vaikuntanathan: Protecting Circuits from Leakage: the Computationally-Bounded and Noisy Cases. SIAM Journal on Computing 43(5): (2014), 1564-1614.

INDEXES

Google Scholar

Profile: `https://scholar.google.com/citations?user=ZJp1L-AAAAAJ`.

H-Index: 18.

Total # of citations: 877 (30/08/2016).

PROGRAM COMMITTEE MEMBERSHIP

2017 IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC) 2017

2016 IACR Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT) 2016

Conference on Security and Cryptography for Networks (SCN) 2016

IACR Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2016

ArcticCrypt 2016

2015 IACR Theory of Cryptography Conference (TCC) 2015

IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC) 2015

International Conference on Information-Theoretic Security (ICITS) 2015

2014 International Workshop on Security (IWSEC) 2014

Asian Workshop on Public Key Cryptography (ASIAPKC) 2014

2013 International Workshop on Security (IWSEC) 2013

Indocrypt 2013

2012 Latincrypt 2012

INDUSTRIAL EXPERIENCE

Co-founder As CTO of Pollux GmbH we raised 200.000 EUR seed funding and partnered with more than 500 local businesses in Germany.

1998–2006 Independent consultant for major banks, technology and pharmaceutical companies, including Commerzbank AG, SEB AG, Siemens AG and GlaxoSmithKline pharmaceutical.

STUDENT SUPERVISION

PhD Students **Clara Paglialonga**, *since February 2016, Department of Mathematics, Ruhr-Universität Bochum, Germany.*

Lisa Eckey, *since April 2016, Department of Mathematics, Ruhr-Universität Bochum, Germany.*

Kristina Hostakova, *from September 2016, Department of Mathematics, Ruhr-Universität Bochum, Germany.*

Master Students **Dragos Gilca**, *Advances in Random Number Generators*, Master of Science, School of Computer and Communication Science, EPFL Lausanne, February 2015.

Lisa Eckey, *Smart contracts for Bitcoin*, Master of Informationssicherheit, Department of Mathematics, Ruhr-Universität Bochum, Spring 2016.

Jonas Geilich, *Smart contracts for Ethereum*, Master of Mathematics, Department of Mathematics, Ruhr-Universität Bochum, Spring 2016.

Semester Students **Ludovic Barman**, *Bitcoins with fast payment processing*, School of Computer and Communication Science, EPFL Lausanne, January 2015.

Clément Doucet, *Tamper Resilient Cryptography*, School of Computer and Communication Science, EPFL Lausanne, June 2014.

Yijun Ying, *Leakage Resilient Fully Homomorphic Encryption*, School of Computer and Communication Science, EPFL Lausanne, January 2014.

EXTERNAL PHD COMMITTEE MEMBER

2016 **Christian Hanser**, *External assessor of PhD thesis at TU Graz, Austria.*

2016 **Daniel Masny**, *External assessor of PhD thesis at Ruhr-University Bochum, Germany.*

Since 2014 **Anthony Journault**, *External member of PhD supervising committee at Université Catholique De Louvain, Belgium.*

TEACHING

Spring 2016 **Lecturer** of the seminar "Research oriented cryptography", Ruhr-Universität of Bochum, Department of Mathematics.

Fall 2015 **Lecturer** of the class "Randomness in Cryptography", Ruhr-Universität of Bochum, Department of Mathematics.

Spring 2015,2016 **Lecturer** of the class "Financial Cryptography", Ruhr-Universität of Bochum, Department of Mathematics.

Spring 2014 **Coordinator** for "Student seminars on Security protocols and applications", EPFL Lausanne, Switzerland, Department of Computer Science.

Spring 2012 **Co-lecturer** for "Cryptographic protocol theory", Aarhus University, Denmark, Department of Computer Science.

Spring 2008, 2009, 2010 **Teaching assistant** of exercises in Cryptography and Network Security (H05E1A), KU Leuven, Department of Engineering.

Spring 2007, 2008 **Teaching assistant** of P&O Multimedia and signal processing (H05H8A), KU Leuven, Department of Engineering.

SELECTED RECENT TALKS

Mar. 2016 Kryptographie jenseits des Black-box Modells, GIBU Schloss Dagstuhl, Germany.

Dec. 2015 Leakage Resilient Masking Schemes, IMDEA Madrid, Spain.

Nov. 2015 Leakage Resilient Masking Schemes, Bochum, Germany. **Invited speaker at 14th Smart Card Research and Advanced Application Conference**.

Nov. 2015 Building digital economy with smart contracts, Zug, Switzerland. Invited speaker at 8th Cyber Intelligence Event.

June 2015 Multiple lectures on practice-oriented provable security, Sibenik, Croatia. Summer school on real-world crypto and privacy.

May 2014 Unifying leakage models: from probing to noisy leakages, Copenhagen, Denmark. Eurocrypt 2014.

April 2014 Leakage Resilient Circuits, Paris, France. **Invited speaker at COSADE Workshop'14**.

Nov. 2013 Advances in Leakage Resilient Crypto in Okinawa, Japan. **Invited speaker at the IWSEC'13 conference**.

Nov. 2013 Advances in non-malleable codes in Tokyo, Japan at NTT and NICT Research center.

June 2013 Efficient Leakage Resilient Symmetric Crypto. Warsaw, Poland. Workshop on Leakage, Tampering and Viruses.

Oct. 2011 Leakage-Resilient Cryptography From the Inner-Product Extractor, Tsinghua University, Beijing. Aarhus-Tsinghua-University lecture series.

May 2011 Leakage-Resilient Cryptography for symmetric primitives, Albena, Bulgaria. Invited lecture at ECRYPT II summer school on Design and Security of Cryptographic Algorithms and Devices.

OTHER SCIENTIFIC ACTIVITIES

Organizer	Co-organizer of Workshop on Practice-orient provable security, Bochum, Germany, 22 – 24 April 2015.
	Co-organizer of Workshop on Leakage, Tampering and Viruses, Warsaw, Poland, 2 – 6 June 2013.
Sub-Reviews (last 2 years)	Crypto 2016, S&P Oakland 2016, TCC 2016, FSE 2016, Crypto 2015, ICALP 2015, Asiacrypt 2014, FOCS 2014, Crypto 2014, ACNS 2014, FSE 2014, Eurocrypt 2014, ITCS 2014, Asiacrypt 2013, Crypto 2013, ICALP 2013, CHES 2013, Journal of Cryptology
Grant reviews	Foundation for Polish Science, Netherlands Organisation for Scientific Research
Visits	CWI (Centrum Wiskunde & Informatica), Amsterdam, The Netherlands. Several visits between 2009–2010 of in total 6 months. Hosts: Prof. Ronald Cramer.
	La Sapienza University of Rome, Italy, January 2010. Host: Prof. Dr. Stefan Dziembowski.
	Boston University and MIT, Boston, USA. October – December 2008 and July – September 2009: Host: Prof. Dr. Leonid Reyzin & Dr. Eran Tromer.

OTHER

Languages	German (native), English (fully proficiency).
Programming	Experience in Java, C/C++, PHP, Perl, SQL.