Benedikt Schmidt
Curriculum Vitae

Researcher
Edificio IMDEA Software
Campus Montegancedo UPM
28223-Pozuelo de Alarcón, Madrid
SPAIN
benedikt.schmidt@imdea.org
http://beschmi.net

1 Research Interests

The goal of my research is to build tools that help developers of cryptographic systems to increase the security and efficiency of their solutions. To achieve this, my research applies techniques from theorem proving, programming languages, and program verification to problems in information security and cryptography.

2 Education

- Ph.D., Computer Science

  ETH Zurich, Switzerland, December 2012.

  Dissertation title: Formal Analysis of Key Exchange Protocols and Physical Protocols

  Committee: David Basin (chair), Srdjan Capkun, Ralf Küsters

- M.S., Computer Science (Diplom Informatik)

  Universität Karlsruhe (TH), Germany, September 2007

3 Employment History

- Sep 2015 - IMDEA Software Institute

  Researcher

- Nov 2012 - Aug 2015 IMDEA Software Institute

  Postdoctoral Researcher

- Sep 2007 - Nov 2012 ETH Zurich

  Research Assistant

- Sep 2001 - Jan 2007 Computing Center of Universität Karlsruhe

  Programmer and System Administrator

- Sep 1999 - July 2000 National Service

4 Honors and Awards

- ETH Medal for outstanding dissertation, November 2013

5 Teaching

- **Lecturer: IACR Summer School on Computer Aided Cryptography**

  Summer 2015 (University of Maryland, College Park)

- **Lecturer: Joint EasyCrypt - F* - CryptoVerif School**

  Winter 2014 (Paris)

- **Lecturer: CERIST Autumn School on Cyber-Physical Systems**

  Fall 2013 (CERIST, Algiers)

- **Teaching assistant: Formal Methods and Functional Programming**

  Undergraduate Class

  Spring 2008, 2009, 2010, 2011, 2012 (ETH Zurich)

- **Teaching assistant: Computing tools for humanities and medical students**

  Undergraduate Class

  Fall 2010 (ETH Zurich)

- **Teaching assistant: Discrete Maths**

  Undergraduate Class

  Fall 2008 (ETH Zurich)

- **Teaching assistant: Linear Algebra**

  Undergraduate Class

  Fall 2007 (ETH Zurich)

6 Research Advising

- PhD Thesis Advising
  - Giuseppe Guagliardo, IMDEA, 2015 -
  - Miguel Ambrona, IMDEA, 2014 -
- Visiting PhD Students
  - Edvard Fagerholm, University of Pennsylvania, 2010-2015

    visiting IMDEA from October 2013 to November 2014

    Edvard received the Carlitz-Zippin price for Outstanding Ph.D. thesis
- Research Internships
  - Daniel Henry Mantilla, "Highly automated proofs for cryptographic constructions based on matrix assumptions", Ecole Polytechnique Paris, 2016, 3 months (ongoing)

- Charlie Jacomme, "Deducibility for pairing groups with applications to the automated search for cryptographic reductions", ENS Cachan, 2016, 3 months (ongoing)

- Daniel Henry Mantilla, "Extending the AutoGnP tool to the Random Oracle Model", Ecole Polytechnique Paris, 2015, 3 months

- Leo Stefanesco, "Formalizing the Forking Lemma in EasyCrypt", ENS Lyon, 2015, 3 months

- Simon Cancela Diaz, "Verifying assembly implementations of Curve25519", Universidad Complutense de Madrid, 2015, 8 months

- Martin Ceresa, ''Automating optimistic sampling transitions in EasyCrypt'', Universidad Nacional de Rosario, 2013, 6 months

- Google Summer of Code for the Darcs project

  - BSRK Aditya, Hyderabad, India, Summer 2012

    His work on patch index optimization got integrated into the next official release of Darcs.

    He successfully participated a second time in GSoc for Darcs in 2013.

7 Research Grants

- Fellowship from the EU FP7 Marie Curie Action AMAROUT (80000 EUR)

- Co-PI on the SynCrypt project funded by the US Office of Naval Research (ONR) and headed by Dan Boneh at Stanford University (900000 EUR for IMDEA). The other Co-PIs are Gilles Barthe (IMDEA), Andre Scedrov, and Steve Zdancewic (University of Pennsylvania).

8 Publications

Journal Publications

1. **Formal Reasoning about Physical Properties of Security Protocols**
   ACM Transactions on Information and System Security (TISSEC), Volume 14, Number 2, 2012
   David Basin, Srdjan Capkun, Patrick Schaller, Benedikt Schmidt

2. **Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds**
   PKC2015 Special Issue of IET Information Security (to appear)

Refereed Conference Publications

S&P 2016 **3. Key Confirmation in Key Exchange: A Formal Treatment and Implications for TLS 1.3**
Proceedings of the 37th IEEE Symposium on Security & Privacy (S&P), May 2016
Marc Fischlin, Felix Günther, Benedikt Schmidt, Bogdan Warinschi

EC 2016 **4. Automated Unboundd Analysis of Cryptographic Constructions in the Generic Group Model**
Proceedings of Advances in Cryptology - EUROCRYPT, May 2016
Miguel Ambrona, Gilles Barthe, Benedikt Schmidt

CCS 2015 **5. Automated Proofs of Pairing-Based Cryptography**
Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS), October 2015
Gilles Barthe, Benjamin Grégoire, Benedikt Schmidt

EC 2015 **6. Mind the Gap: Modular Machine-Checked Proofs of One-Round Key Exchange Protocols**
Proceedings of Advances in Cryptology - EUROCRYPT, May 2015
Gilles Barthe, Juan-Manuel Crespo, Yassine Lakhnech, Benedikt Schmidt

PKC 2015 **7. Strongly-Optimal Structure Preserving Signatures from Type II Pairings: Synthesis and Lower Bounds**
Proceedings of Public-Key Cryptography (PKC), March 2015
Gilles Barthe, Edvard Fagerholm, Dario Fiore,
Andre Scedrov, Benedikt Schmidt, and Mehdi Tibouchi

Crypto 2014 **8. Automated Analysis of Cryptographic Assumptions in Generic Group Models**
Proceedings of Advances in Cryptology - CRYPTO, August 2014
Gilles Barthe, Edvard Fagerholm, Dario Fiore,
John Mitchell, Andre Scedrov, Benedikt Schmidt

CSF 2014 **9. Certified Synthesis of Efficient Batch Verifiers**
Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF), July 2014
Joseph A. Akinyele, Gilles Barthe, Benjamin Grégoire,
Benedikt Schmidt, Pierre-Yves Strub

S&P 2014 **10. Automated Verification of Group Key Agreement Protocols**
Proceedings of the 35th IEEE Symposium on Security & Privacy (S&P), May 2014
Benedikt Schmidt, Ralf Sasse, Cas Cremers, David Basin

CCS 2013 **11. Fully Automated Analysis of Padding-Based Encryption in the Computational Model**
Proceedings of the 20th ACM Conference on Computer and Communications Security (CCS), October 2013
Gilles Barthe, Juan Manuel Crespo, Benjamin Grégoire, César Kunz,
Yassine Lakhnech, Benedikt Schmidt, and Santiago Zanella-Béguelin

CAV 2013 **12. The Tamarin Prover for the Symbolic Analysis of Security Protocols (Tool Paper)**
Proceedings of Computer Aided Verification (CAV), June 2013
Simon Meier, Benedikt Schmidt, Cas Cremers, David Basin

CSF 2012 **13. Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties**
Proceedings of 25th IEEE Computer Security Foundations Symposium (CSF), July 2012
Benedikt Schmidt, Simon Meier, Cas Cremers, David Basin

S&P 2012 **14. Distance Hijacking Attacks on Distance Bounding Protocols**
Proceedings of 33rd IEEE Symposium on Security & Privacy (S&P), May 2012
Cas Cremers, Kasper Rasmussen, Benedikt Schmidt, Srdjan Capkun

CSF 2010 **15. Impossibility Results for Secret Establishment**
Proceedings of the 23nd IEEE Computer Security Foundations Symposium (CSF), July 2010
Benedikt Schmidt, Patrick Schaller, and David Basin

CSF 2009 **16. Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks**
Proceedings of the 22nd IEEE Computer Security Foundations Symposium (CSF), July 2009
Patrick Schaller, Benedikt Schmidt, David Basin, Srdjan Capkun

Invited Papers and Book Chapters

17. Computer-Aided Proofs in Cryptography: An Overview
All about Proofs, Proofs for All. Vol 55. Mathematical Logic and Foundations, 2015
Gilles Barthe, François Dupressoir, Benjamin Grégoire,
Benedikt Schmidt, and Pierre-Yves Strub

18. EasyCrypt: A Tutorial
Foundations of Security Analysis and Design VII. Vol. 8604, 2013
Gilles Barthe, François Dupressoir, Benjamin Grégoire, César Kunz,
Benedikt Schmidt, and Pierre-Yves Strub

19. Let's Get Physical: Models and Methods for Real-World Security Protocols
Proceedings of the 22st International Conference on Theorem Proving in Higher Order Logics (TPHOLS), August 2008
David Basin, Srdjan Capkun, Patrick Schaller, Benedikt Schmidt

Theses

20. Formal Analysis of Key Exchange Protocols and Physical Protocols
Ph.D. Thesis, ETH Zurich, December 2012

21. A Cryptographically Sound Proof of an Electronic Payment System in Isabelle/HOL
Diploma Thesis, Universität Karlsruhe (TH), September 2007

9 Invited Talks and Conference Talks

- **Automated Proofs of Pairing-Based Cryptography**
  - CCS, Denver, USA, October 2015
  - ETH Zurich, Switzerland, September 2015
- **Demo: Verifying Assembly Implementations of Elliptic Curve Cryptography**

  The Core Infrastructure Initiative (CII) 2015 meeting, Madrid, Spain, July 2015

- **Modular Machine-Checked Proofs of One-Round Key Exchange Protocols**
  - EuroCrypt, Sofia, Bulgaria, May 2015
  - SKECH@BiCi: Secure Key Exchange and Channel Protocols, Bertinoro, Italy, June 2014
- **Automated Analysis of Cryptographic Assumptions in Generic Group Models**
  - IACR Computer-Aided Crypto School, University of Maryland, College Park, USA, June 2015
  - Crypto, Santa Barbara, USA, August 2014
- **Fully Automated Analysis of Padding-Based Encryption in the Computational Model**
  - 1st Microsoft Research and IMDEA Software Institute Collaboration Workshop, Madrid, Spain, April 2014
  - CCS, Berlin, Germany, October 2013
  - University of Pennsylvania, Philadelphia, USA, May 2013
- **Attacks and Proofs for Channel Establishment and Key Exchange Protocols**
  Second Prometidos-CM Winter School, Madrid, Spain, December 2013
- **Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties**
  - CAV, Saint Petersburg, Russia, July 2013
  - CSF, Boston, USA, June 2012
  - Dagstuhl Seminar 11332 on Security and Rewriting, Dagstuhl, Germany, August 2011**9.1**
- **Impossibility Results for Secret Establishment**
  CSF, Edinburgh, UK, July 2010
- **Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks**
  - MICS Site Visit, EPFL, Lausanne, Switzerland, September 2009
  - CSF, Port Jefferson, USA, July 2009

10 Professional Activities

Program Committees

- EuroCrypt 2016
- FCS 2015

Journal Review

- Journal of Computer Security

- Journal of Automated Reasoning
- ACM Transactions on Computational Logic
- Foundations and Trends in Programming Languages
- IEEE/ACM Transactions on Networking
- Elsevier Computers & Security
- IEEE Transactions on Emerging Topics in Computing

External Reviewer

- ASIACCS 2008-2011, ESORICS 2008, CSF 2011, POST 2012, CCS 2012, S&P 2013, CSF 2013, LICS 2014, AfricaCrypt 2014, CONCUR 2014, SCN 2014, EuroCrypt 2015, Crypto 2015, etc.

Project Evaluation

- German Research Society (DFG), 2014
- Luxembourg National Research Fund (FNR), 2015

Schools

- Organised the IACR School on Computer-aided Cryptography at University of Maryland, June 2015

11 Languages

English, German (native), French