Curriculum Vitae – Philipp Jovanovic

September 8, 2018

Personal Information

EPFL – IC – DEDIS	Phone: +41 (0)21 69 36628
BC 263, Station 14	Email: philipp.jovanovic@epfl.ch
CH-1015, Lausanne	Web: https://philipp.jovanovic.io
Switzerland	Google Scholar: p-KBDi8AAAAJ

Education

Dr. rer. nat. Cryptology 2011 – 2015
Faculty of Computer Science and Mathematics
University of Passau, Germany
Thesis title: Analysis and Design of Symmetric Cryptographic Algorithms
Advisors: Martin Kreuzer and Ilia Polian
Graduated with distinction (summa cum laude)
University award for best dissertation in computer science and mathematics

First State Examination for Computer Science and Mathematics 2005 – 2010
Faculty of Computer Science and Mathematics
University of Passau, Germany
Thesis title: Algebraic Attacks Using SAT-Solvers
Advisor: Martin Kreuzer

Employment History

Postdoctoral Researcher 2015 –
School of Computer and Communication Sciences
École polytechnique fédérale de Lausanne (EPFL), Switzerland
Research topics: scalability and security of decentralized and distributed systems, applied cryptography, blockchain technology, cryptocurrencies
Advisor: Bryan Ford

Research Assistant 2011 – 2015
Faculty of Computer Science and Mathematics
University of Passau, Germany
Research topics: analysis and design of authenticated encryption algorithms, side-channel attacks on cryptographic hardware, smart grid security
Advisors: Martin Kreuzer and Ilia Polian

Other Positions and Memberships

Co-founder of Sockpuppet Technologies, Inc.	2018 –
Scientific Advisor at DFINITY – The Decentralized Cloud	2017 –
Member at the Initiative for Cryptocurrencies and Contracts (IC3)	2017 –
Member at the Swiss Fintech Innovations (SFTI) Association Advisory Board	2017 –
Member at the Chaos Computer Club (CCC)	2015 –
Visiting Researcher at DTU's Cryptology Research Group, Copenhagen, Denmark	July 2014

Awards

Distinguished paper award, IEEE Security and Privacy Symposium	2018
Appreciation for Exceptional Performance, École polytechnique fédérale de Lausanne	2016
Best Dissertation in Mathematics and Computer Science, University of Passau	2016
Student travel award, 22nd International Workshop on Fast Software Encryption	2015
Appreciation for Exceptional Performance, University of Passau	2012

Teaching Activities

Exercises

Computer Architecture	SS12, SS13, SS14, SS15
Technical Computer Science	WS11/12, WS12/13, WS14/15, WS15/16
Sensors and Actuators	WS13/14

Seminars

Cryptology	WS11/12, WS12/13, WS13/14, WS13/15
E-learning	SS11, WS11/12, SS12, WS12/13, SS13
Mathematical Computer Programming	SS14

Supervision

Bachelor and Master Theses	SS13, WS13/14, WS14/15
Summer@EPFL interns	2016 –

Topics: lattices, pairings, decentralized randomness, etc.

SS: summer semester; WS: winter semester

Outreach Activities

Technology Blogging

Guest post at Hacking, Distributed on ByzCoin – Securely Scaling Blockchains	2016
Personal blog	2014 –

Technology Consulting

Ocean Protocol Foundation, topic: cryptocurrencies and blockchain technology	2018
Cryptography and blockchain trainings at Troopers, Black Hat Europe, Google Zurich, etc.	2017 –

Scientific Service Activities

Conference and Workshop Program Committees

PoPETs, FC	2019
BITCOIN, BTA, CryBlock, BlockSEA	2018
CCS	2017

Conference and Workshop Reviewing

SAC, IOLTS, Latincrypt, CHES	2015
SAC, Latincrypt, FSE	2014
SECRYPT	2013
Inscrypt	2012

Journal Reviewing

Journal of Computer Science and Technology, IET Information Security	2012

Event Organization

EPFL/ETHZ Blockchain Summer School	2017
IRGC Workshop on Governing Risks and Benefits of Distributed Ledger Technology Applications	2017
EPFL Summer Research Institute on Security and Privacy	2016 – 2018

Invited Talks (Selected)

EcoCloud Annual Conference	2018
Binary District Conference on Blockchain for Payment Processing	2018
EPFL/SBB Data Science and Mobility Conference	2018
Bitcoin Wednesday Community Meetup	2017
Cybersecurity With the Best Conference	2017
dotSecurity.io – The Security Conference for Developers	2017
IRGC Conference on Cybersecurity Risks in the Internet of Things	2016
SPEED-B Conference	2016
Tech Talk at Google Zurich	2015

Refereed Journal Publications

2. Philipp Jovanovic, Atul Luykx, Bart Mennink, Yu Sasaki, and Kan Yasuda. Beyond Conventional Security in Sponge-Based Authenticated Encryption Modes. *Journal of Cryptology*, pages 1–46, 2018
1. Philipp Jovanovic and Martin Kreuzer. Algebraic Attacks using SAT-Solvers. *Groups — Complexity — Cryptology*, 2:247–259, 2010

Refereed Conference Publications

15. Stevens Le Blond, Alejandro Cuevas, Juan Ramón Troncoso-Pastoriza, Philipp Jovanovic, Bryan Ford, and Jean-Pierre Hubaux. On Enforcing the Digital Immunity of a Large Humanitarian Organisation. In *IEEE Security and Privacy*, 2018. **Distinguished paper award**
14. Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ewa Syta, and Bryan Ford. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In *IEEE Security and Privacy*, 2018
13. Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Justin Cappos, and Bryan Ford. Chainiac: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds. In *USENIX Security Symposium*, 2017
12. Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris-Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford. Scalable Bias-Resistant Distributed Randomness. In *IEEE Security and Privacy*, 2017
11. Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing. In *USENIX Security Symposium*, 2016
10. Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning. In *IEEE Symposium on Security and Privacy*, 2016
9. Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves. Improved Masking for Tweakable Blockciphers with Applications to Authenticated Encryption. In *Advances in Cryptology — EUROCRYPT*, 2016
8. Christof Beierle, Philipp Jovanovic, Martin M. Lauridsen, Gregor Leander, and Christian Rechberger. Analyzing Permutations for AES-like Ciphers: Understanding ShiftRows. In *Topics in Cryptology — CT-RSA*, 2015
7. Philipp Jovanovic and Samuel Neves. Practical Cryptanalysis of the Open Smart Grid Protocol. In *Fast Software Encryption — FSE*, 2015
6. Philipp Jovanovic and Ilia Polian. Fault-based Attacks on the Bel-T Block Cipher Family. In *Design, Automation and Test in Europe — DATE*, 2015
5. Philipp Jovanovic, Atul Luykx, and Bart Mennink. Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes. In *Advances in Cryptology — ASIACRYPT*, 2014
4. Raghavan Kumar, Philipp Jovanovic, Wayne Burleson, and Ilia Polian. Parametric Trojans for Fault-Injection Attacks on Cryptographic Hardware. In *IEEE Fault Diagnosis and Tolerance in Cryptography — FDTC*, 2014
3. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. Analysis of NORX: Investigating Differential and Rotational Properties. In *Progress in Cryptology — Latincrypt*, 2014

2. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. NORX: Parallel and Scalable AEAD. In *European Symposium on Research in Computer Security — ESORICS*, 2014

1. Raghavan Kumar, Philipp Jovanovic, and Ilia Polian. Precise Fault-Injections using Voltage and Temperature Manipulation for Differential Cryptanalysis. In *IEEE International On-Line Testing Symposium — IOLTS*, 2014

Refereed Workshop Publications

7. Maria Borge, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, Linus Gasser, and Bryan Ford. Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies. In *IEEE Security and Privacy on the Blockchain*, 2017

6. Hanno Böck, Aaron Zauner, Sean Devlin, Juraj Somorovsky, and Philipp Jovanovic. Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. In *USENIX Workshop on Offensive Technologies — WOOT*, 2016

5. Eleftherios Kokoris-Kogias, Linus Gasser, Ismail Khoffi, Philipp Jovanovic, Nicolas Gailly, and Bryan Ford. Managing Identities Using Blockchains and CoSi. In *Hot Topics in Privacy Enhancing Technologies — HotPETs*, 2016

4. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. NORX8 and NORX16: Authenticated Encryption for Low-End Systems. In *Trustworthy Manufacturing and Utilization of Secure Devices — TRUDEVICE*, 2015

3. Philipp Jovanovic, Martin Kreuzer, and Ilia Polian. Multi-Stage Fault Attacks on Block Ciphers. In *14th Workshop on RTL and High Level Testing — WRTLT*, 2013

2. Philipp Jovanovic, Martin Kreuzer, and Ilia Polian. An Algebraic Fault Attack on the LED Block Cipher. In *Third International Conference on Symbolic Computation and Cryptography — SCC*, 2012

1. Philipp Jovanovic, Martin Kreuzer, and Ilia Polian. A Fault Attack on the LED Block Cipher. In *International Workshop on Constructive Side-Channel Analysis and Secure Design — COSADE*, 2012

Technical Reports and Other Publications

1. Eleftherios Kokoris-Kogias, Enis Ceyhun Alp, Sandra Deepthy Siby, Nicolas Gailly, Linus Gasser, Philipp Jovanovic, Ewa Syta, and Bryan Ford. Calypso: Auditable Sharing of Private Data over Blockchains. Cryptology ePrint Archive, Report 2018/209, 2018

Coverage in Popular Media

- Chainiac: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds
  - New tool can help prevent government-mandated backdoors in software, Swiss researchers say; cyberscoop, J.M. Porup, July 25, 2017
- Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing
  - Researchers Suggest New Method to Scale Bitcoin to Paypal Levels of Transactions; CCN, Andrew Quentson, November 11, 2016
  - ByzCoin – An Innovative Solution; EPFL press release, Jeremy Hottinger and Inka Sayed, December 13, 2016
- Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS
  - "Forbidden attack" makes dozens of HTTPS Visa sites vulnerable to tampering; Ars Technica, Dan Goodin, May 26, 2016
  - Gefahr durch doppelte Nonces; Golem, Hanno Böck, May 20, 2016
  - Pwnie award nomination in the category best cryptographic attack 2016
- Keeping Authorities "Honest or Bust" with Decentralized Witness Cosigning
  - How Apple Could Fed-Proof Its Software Update System; MIT Technology Review, Tom Simonite, March 11, 2016
  - Cothority to Apple: Let's make secret backdoors impossible; Ars Technica, J.M. Porup, March 10, 2016

  - Using distributed code-signatures to make it much harder to order secret backdoors; BoingBoing, Cory Doctorow, March 10, 2016
  - Cothority offers to help Apple security with distributed cosigning; MacNN, MacNN Staff, March 10, 2016
  - Co-thority statt Authority: Viele-Augen-Prinzip für Zertifikate; Heise, Monika Emert, November 11, 2015
- Practical Cryptanalysis of the Open Smart Grid Protocol
  - Who Can Hijack Your Smart Meter? Weak Security Threatens Energy Grid; Uni Passau press release, May 13, 2015
  - Amateurs Produce Amateur Cryptography; Schneier on Security, Bruce Schneier, May 12, 2015
  - Verschlüsselte OSGP-Kommunikation von Smart Metern leicht belauschbar; Heise, Dennis Schirrmacher, May 12, 2015
  - Smart Grid consortium rolled its own crypto, which is always, always a bad idea; BoingBoing, Cory Doctorow, May 9, 2015
  - Weak Homegrown Crypto Dooms Open Smart Grid Protocol; threatpost, Michael Mimoso, May 7, 2015
- Miscellaneous
  - Interview on blockchain applications; Binary District Journal, Joseph Young, February 10, 2018
  - Interview on NORX, IoT Security, and Blockchain; InfoQ, Matthieu Bolla, May 22, 2017
  - Report on dotSecurity 2017; D2SI, Antoine Jacoutot, April 26, 2017

Software Artifacts Publicly Released

DRAND	Distributed randomness beacon daemon	2018
Cothority	Scalable collective authority framework	2015
Kyber	Advanced elliptic curve cryptography library	2015
MEM-AEAD	Authenticated encryption via Masked Even-Mansour (MEM)	2015
NORX	Parallel and scalable authenticated encryption	2014
DFA-AES	Differential fault analysis framework for AES	2013