Curriculum Vitae

Dr. Markku-Juhani O. Saarinen

October 6, 2018

E-mail: mjos@iki.fi Homepage: https://mjos.fi

Education

Ph.D. Information Security, 2009. Royal Holloway, University of London, UK

Thesis: "Cryptanalysis of Dedicated Cryptographic Hash Functions", under Prof. Keith Martin. I did my doctoral research with the RHUL Information Security Group (ISG).

M.Sc. Scientific Computing, (1999) 2005. University of Jyväskylä, Finland

Computer science with a large mathematics component. I didn't take a B.Sc degree in 1999, but after a pause continued to Master's, which was awarded *eximia cum laude*.

Background and Skill Profile

I got my first real job in 1997 when SSH Communications Security hired me – then a young maths undergraduate with programming skills – to work full time as a cryptographer. I have worked exclusively in technical INFOSEC and COMSEC ever since. I earned my graduate degrees mostly while doing consulting and engineering work in the security industry and I maintain strong links with the wider security research community.

Cryptography and Security Engineering. I design, implement, and audit cryptographic systems. As part of this work, I have cryptanalyzed ("broken") a number of cryptosystems. Most of these results are confidential, but I have also published some, e.g. on PAES and HKC [6], Hummingbird-1 & 2 [13, 18], FORK-256 [24], FSB hash [25], and LILI-128 [31].

The ROUND5 quantum-resistant public key encryption algorithm [1, 4] is my current research focus. It is a result of merging my HILA5 [5] algorithm with an another proposal, ROUND2. These are official candidates in the ongoing U.S. NIST Post-Quantum Cryptography (PQC) selection and standardization effort. See: https://mjos.fi/round5.

In programming work I now prefer C and Rust. I can also work with many other languages and write low-level assembler code for ARM, x86, and various embedded targets. I have also done FPGA engineering work, professionally audited broader information systems for security, and ran major penetration testing projects.

Research and Standardization. I hold some patents and I've written dozens of peer-reviewed academic publications on applied cryptography. My papers have been cited roughly 1200 times. See: https://scholar.google.com/citations?user=2_oEFqYAAAAJ.

I am currently a coauthor of both Russian and Chinese national cipher TLS specification drafts in IETF, a result of my rare exposure to non-US cryptographic algorithms. Some of my earlier IETF contributions are acknowledged by name in RFC 2451 (on IPSec ESP ciphers), RFCs 4250-4254 and 4419 (I was one of the original developers of SSH2), and RFC 7693 (which I wrote and edited, on hash function BLAKE2).

Professional Experience

PQSHIELD (Oxford, UK) 2018/09 -
Senior Cryptography Engineer

PQSHIELD Ltd. is a new spin-off of the University of Oxford Mathematical Institute, focusing on Post-Quantum Cryptography.

INDEPENDENT CONSULTANT (Cambridge, UK) 2018/02 - 2018/08

Major projects: Quantum resistant cryptographic algorithm design with Philips Research (Netherlands), resource-constrained IoT cryptography implementations with Teserakt AG (Switzerland), and cryptography standardization work with Ribose Inc (Hong Kong).

ARM (Cambridge, UK) 2017/10 - 2018/02
Senior Principal Security Engineer

Engineering work on mbedTLS and lightweight cryptographic implementations.

DARKMATTER (Abu Dhabi, UAE) 2016/09 - 2017/08
Principal Cryptographer

Worked closely with United Arab Emirates government bodies in sensitive information assurance projects. This was mainly cryptography and cryptanalytic consultancy related to design, implementation, and analysis of varied security technologies.

QUEEN'S UNIVERSITY BELFAST (Belfast, UK) 2015/08 - 2016/06
Research Fellow

EU H2020 SAFEcrypto Project. Designing and engineering future cryptographic primitives. Focus on Lattice-based and other quantum resistant cryptography.

ITINERANT RESEARCHER IN CRYPTOGRAPHY 2013/05 - 2015/07
Research grants and temporary post-doctoral positions

Tampere University of Technology, Finland	2015/05 - 2015/07
TÜBİTAK Gebze, Turkey	2015/03 - 2015/04
INRIA Paris-Rocquencourt, France	2014/11
NTNU Trondheim, Norway	2014/02 - 2015/10 and 2014/12 - 2015/02
Contract with Kudelski Security, Switzerland	2013/12
NTU Temasek Laboratories, Singapore	2013/05 - 2013/10

My research focus was on Authenticated Encryption algorithms and the NIST - sponsored CAESAR project. I designed the STRIBOB and WHIRLBOB algorithms. Software and hardware implementations of cryptographic work. Implementation of the BRUTUS cryptanalytic testing framework for the CAESAR Project.

HELP AG (Dubai, UAE) 2012/11 - 2013/05
Senior Security Specialist

Vulnerability assessment and penetration testing projects, security research. Development of the HAGRAT Remote Access Tool (RAT) and Command & Control system for simulating APT type adversaries in penetration exercises.

REVERE SECURITY (Addison TX, USA) 2010/11 - 2012/08
Research Fellow

Principal Investigator of a small DARPA-funded light-weight cryptography research project. Design and implementation of light-weight encryption methods for RFID and sensor networks. Lots of hands-on embedded software engineering.

ROYAL HOLLOWAY, UNIVERSITY OF LONDON (UK) 2005/10 - 2010/11
Postgraduate Student, Researcher, and Consultant

Doctoral studies with the Information Security Group (ISG), Royal Holloway, University of London. Graduated with a PhD in Information Security, November 2009.

Freelance consulting: Security audits and related consultancy as a part-time employee for Startups and NIXU Middle East in Saudi Arabia, Lebanon, Qatar, Kuwait and United Arab Emirates. PCI DSS audits or short pre-audits for NIXU in UAE, Lebanon, Kuwait.

NIXU Middle East (Dubai, UAE and Riyadh, KSA) 2004/09 - 2005/09
Senior Security Specialist

Penetration Testing and other security assessment projects for sensitive customers in Energy, Finance, Telecommunications, and Government sectors, mainly in Saudi Arabia. Running a Penetration Testing course for the technical staff of a large private customer. Design and implementation of large-scale original network monitoring, filtering, and intrusion detection solutions.

HELSINKI U. OF TECH. (Aalto University) (Espoo, Finland) 2002/02 - 2004/09
Research Assistant

Project manager in a cryptography research project funded by the Finnish Defence Forces. Unclassified research in cryptanalysis and cryptographic engineering. Teaching assistant (and occasional lecturer), Prof. H. Lipmaa's cryptography courses.

NOKIA CORPORATION (Helsinki, Finland) 2000/04 - 2002/02
Security Specialist

Specialist in cryptography and security protocols, analyzing the security of mobile devices and related technologies such as A5, Kasumi, TLS, WTLS, etc. Evaluated security products and services for Nokia Networks, Nokia Research, and Nokia Venturing.

SSH COMMUNICATIONS SECURITY (Espoo, Finland) 1997/06 - 1999/02
Cryptographer

I was one of the early employees and original developers of the SSH 2 protocol. I was also deeply involved in the IETF IPSec and NIST AES evaluation and specification processes. My SSH work is acknowledged by name in IETF specifications (RFCs 4250-4254, 4419).

Patents

[1] Markku-Juhani O. Saarinen. Method and apparatus for improved pseudo-random number generation. US Patent 7007050. Filed May 17, 2001. Granted February 28, 2006. https://www.google.com/patents/US7007050.

[2] Markku-Juhani O. Saarinen and Ville Ollikainen. Method and apparatus for implementing secure and selectively deniable file storage. US Patent 8555088. Filed March 16, 2009. Granted October 8, 2013. https://www.google.com/patents/US8555088

Selected Publications

[1] Markku-Juhani O. Saarinen, Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen, and Zhenfei Zhang. Shorter messages and faster post-quantum encryption with Round5 on Cortex M. In Begül Bilgin and Jean-Bernard Fischer, editors, *CARDIS 2018 – 17th Smart Card Research and Advanced Application Conference. Montpellier, France, November 12 - 14, 2018*, volume to appear of *Lecture Notes in Computer Science*. Springer. URL: https://eprint.iacr.org/2018/723.

[2] Markku-Juhani O. Saarinen. HILA5: On reliability, reconciliation, and error correction for Ring-LWE encryption. In Carlisle Adams and Jan Camenisch, editors, *Selected Areas in Cryptography – SAC 2017. 24th International Conference, Ottawa, ON, Canada, August 16 - 18, 2017*, volume 10719 of *Lecture Notes in Computer Science*, pages 192–212. Springer, 2018. doi:10.1007/978-3-319-72565-9_10.

[3] Markku-Juhani O. Saarinen. Arithmetic coding and blinding countermeasures for lattice signatures. *Journal of Cryptographic Engineering*, 8(1):71–84, April 2018. URL: http://rdcu.be/oHun, doi:10.1007/s13389-017-0149-6.

[4] Sauvik Bhattacharya, Oscar Garcia-Morchon, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. Round5: Compact and fast post-quantum public-key encryption. Cryptology ePrint Archive: Report 2018/725, August 2018. URL: https://eprint.iacr.org/2018/725.

[5] Markku-Juhani O. Saarinen. Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography. In *IoTPTS '17: Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security. Abu Dhabi, United Arab Emirates – April 02, 2017*, pages 15–22. ACM, April 2017. doi:10.1145/3055245.3055254.

[6] Markku-Juhani O. Saarinen. The Brutus automatic cryptanalytic framework. *Journal of Cryptographic Engineering*, 6(1):75–82, April 2016. doi:10.1007/s13389-015-0114-1.

[7] Markku-Juhani O. Saarinen and Billy B. Brumley. WHIRLBOB, the Whirlpool based variant of STRIBOB. In Sonja Buchegger and Mads Dam, editors, *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings*, volume 9417 of *Lecture Notes in Computer Science*, pages 106–122. Springer, October 2015. doi:10.1007/978-3-319-26502-5_8.

[8] Markku-Juhani O. Saarinen and Jean-Philippe Aumasson. The BLAKE2 cryptographic hash and message authentication code (MAC). Internet Engineering Task Force RFC 7693, November 2015. doi:10.17487/RFC7693.

[9] Markku-Juhani O. Saarinen. StriBob: authenticated encryption from GOST R 34.11-2012 LPS permutation. *Mat. Vopr. Kriptogr.*, 6(2):67–68, 2015. URL: http://mi.mathnet.ru/eng/mvk146.

[10] Markku-Juhani O. Saarinen. Simple AEAD hardware interface (SÆHI) in a SoC: Implementing an on-chip Keyak/WhirlBob coprocessor. In *TrustEd '14: Proceedings of the 4th International Workshop on Trustworthy Embedded Devices*, pages 51–56. ACM, 2014. doi:10.1145/2666141.2666144.

[11] Markku-Juhani O. Saarinen. CBEAM: Efficient authenticated encryption from feebly one-way ϕ functions. In Josh Benaloh, editor, *Topics in Cryptology – CT-RSA*

2014: The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings, volume 8366 of *Lecture Notes in Computer Science*, pages 251–269. Springer, 2014. doi:10.1007/978-3-319-04852-9_13.

[12] Markku-Juhani O. Saarinen. Beyond modes: Building a secure record protocol from a cryptographic sponge permutation. In Josh Benaloh, editor, *Topics in Cryptology – CT-RSA 2014: The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings*, volume 8366 of *Lecture Notes in Computer Science*, pages 270–285. Springer, 2014. doi:10.1007/978-3-319-04852-9_14.

[13] Markku-Juhani O. Saarinen. Related-key attacks against full Hummingbird-2. In Shiho Moriai, editor, *Fast Software Encryption: 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 467–482. Springer, 2013. doi:10.1007/978-3-662-43933-3_24.

[14] Markku-Juhani O. Saarinen. Developing a grey hat C2 and RAT for APT security training and assessment. In *GreHack 2013 Hacking Conference, 15 November 2013, Grenoble, France*, 2013. Preprint privately available.

[15] Markku-Juhani O. Saarinen and D. Engels. A Do-It-All-Cipher for RFID: Design Requirements (Extended Abstract). DIAC 2012 Workshop, 05-06 July 2012, Stockholm SE. IACR ePrint 2012/317, June 2012. URL: https://eprint.iacr.org/2012/317.

[16] Markku-Juhani O. Saarinen. The BlueJay ultra-lightweight hybrid cryptosystem. In *TrustED: 2012 IEEE Symposium on Security and Privacy Workshops*, pages 27–32. IEEE, May 2012. doi:10.1109/SPW.2012.11.

[17] Markku-Juhani O. Saarinen. Cycling attacks on GCM, GHASH and other polynomial MACs and hashes. In Anne Canteaut, editor, *Fast Software Encryption: 19th International Workshop, FSE 2012, Washington, DC, USA, March 19-21, 2012. Revised Selected Papers*, volume 7549 of *Lecture Notes in Computer Science*, pages 216–225. Springer, 2012. doi:10.1007/978-3-642-34047-5_13.

[18] Markku-Juhani O. Saarinen. Cryptanalysis of hummingbird-1. In Antoine Joux, editor, *Fast Software Encryption: 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 328–341. Springer, 2011. doi:10.1007/978-3-642-21702-9_19.

[19] Markku-Juhani O. Saarinen. Cryptographic analysis of all 4×4 - bit s-boxes. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography: 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 118–133. Springer, 2011. doi:10.1007/978-3-642-28496-0_7.

[20] Daniel Engels, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith. The Hummingbird-2 lightweight authenticated encryption algorithm. In Ari Juels and Christof Paar, editors, *RFID. Security and Privacy: 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26-28, 2011, Revised Selected Papers*, volume 7055 of *Lecture Notes in Computer Science*, pages 19–31. Springer, 2011. doi:10.1007/978-3-642-25286-0_2.

[21] Jean-Philippe Aumasson, María Naya-Plasencia, and Markku-Juhani O. Saarinen. Practical attack on 8 rounds of the lightweight block cipher KLEIN. In Daniel J.

Bernstein and Sanjit Chatterjee, editors, *Progress in Cryptology – INDOCRYPT 2011: 12th International Conference on Cryptology in India, Chennai, India, December 11-14, 2011. Proceedings*, volume 7107 of *Lecture Notes in Computer Science*, pages 134–145. Springer, 2011. doi:10.1007/978-3-642-25578-6_11.

[22] Markku-Juhani O. Saarinen. The PASSERINE public key encryption and authentication mechanism. In Tuomas Aura, Kimmo Järvinen, and Kaisa Nyberg, editors, *Information Security Technology for Applications: 15th Nordic Conference on Secure IT Systems, NordSec 2010, Espoo, Finland, October 27-29, 2010, Revised Selected Papers*, volume 7127 of *Lecture Notes in Computer Science*, pages 283–288. Springer, 2010. doi:10.1007/978-3-642-27937-9_20.

[23] Markku-Juhani O. Saarinen. Project twovault secure and selectively deniable data storage. In *Proc. ISCTURKEY 2008. December 25–27, 2008, Ankara, Turkey.*, pages 42–47. Information Association of Turkey, 2008.

[24] Markku-Juhani O. Saarinen. A meet-in-the-middle collision attack against the new FORK-256. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *Progress in Cryptology – INDOCRYPT 2007: 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007. Proceedings*, volume 4859 of *Lecture Notes in Computer Science*, pages 10–17. Springer, 2007. doi:10.1007/978-3-540-77026-8_2.

[25] Markku-Juhani O. Saarinen. Linearization attacks against syndrome based hashes. In K. Srinathan, C. Pandu Rangan, and Moti Yung, editors, *Progress in Cryptology – INDOCRYPT 2007: 8th International Conference on Cryptology in India, Chennai, India, December 9-13, 2007. Proceedings*, volume 4859 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 2007. doi:10.1007/978-3-540-77026-8_1.

[26] Markku-Juhani O. Saarinen. Security of VSH in the real world. In Rana Barua and Tanja Lange, editors, *Progress in Cryptology - INDOCRYPT 2006: 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006. Proceedings*, volume 4329 of *Lecture Notes in Computer Science*, pages 95–103. Springer, 2006. doi:10.1007/11941378_8.

[27] Markku-Juhani O. Saarinen. Chosen-IV statistical attacks against eSTREAM ciphers. In Manu Malek, Eduardo Fernández-Medina, and Javier Hernando, editors, *SECRYPT 2006, Proceedings of the International Conference on Security and Cryptography, Setúbal, Portugal, August 7-10, 2006*, pages 260–266. INSTICC Press, 2006.

[28] Kamel Bentahar, Dan Page, Markku-Juhani O. Saarinen, Joseph H. Silverman, and Nigel P. Smart. LASH. In *Second NIST Cryptographic Hash Workshop*, August 2006. URL: http://csrc.nist.gov/groups/ST/hash/documents/SAARINEN_lash4-1_ORIG.pdf.

[29] Markku-Juhani O. Saarinen. Encrypted watermarks and Linux laptop security. In Chae Hoon Lim and Moti Yung, editors, *Information Security Applications: 5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers*, volume 3325 of *Lecture Notes in Computer Science*, pages 27–38. Springer, 2004. doi:10.1007/978-3-540-31815-6_3.

[30] Markku-Juhani O. Saarinen. Cryptanalysis of block ciphers based on SHA-1 and MD5. In Thomas Johansson, editor, *Fast Software Encryption: 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003. Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 36–44. Springer, 2003. doi:10.1007/978-3-540-39887-5_4.

[31] Markku-Juhani O. Saarinen. A time-memory tradeoff attack against LILI-128. In Joan Daemen, , and Vincent Rijmen, editors, *Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers*, volume 2365 of *Lecture Notes in Computer Science*, pages 231–236. Springer, 2002. doi:10.1007/3-540-45661-9_18.

[32] Markku-Juhani O. Saarinen. Attacks against the WAP WTLS protocol. In Bart Preneel, editor, *Communications and Multimedia Security IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS99) September 2021, 1999, Leuven, Belgium*, volume 23 of *IFIP The International Federation for Information Processing*, pages 209–215. Kluwer / Sringer, 1999. doi:10.1007/978-0-387-35568-9_14.