Dr. Markku-Juhani O. Saarinen

Curriculum Vitae – March 1, 2024

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

Contents

1 Education 1

2 Background and Skill Profile 1

3 Professional Experience 2

4 Academic/Professional Service (2020-) 4

5 Academic Bibliography 5

6 Recent Talks and Presentations (2020-) 9

7 Patents and Published (Pending) Applications 11

1 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, I continued to Master's, which was awarded *eximia cum laude*.

2 Background and Skill Profile

Keywords: Post-Quantum Cryptography, Embedded C, Verilog, Python, Formal Verification, Side-Channel Security, Entropy Sources, RISC-V, Patents, Intellectual Property.

Applied Cryptography. 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 and editor of the SSH2 specifications. I have worked exclusively in technical INFOSEC and COMSEC ever since.

I have over two decades of experience in designing and analyzing real-life cryptoalgorithms and protocols. I am currently deeply involved with various PQC (Post-Quantum Cryptography) transition and standardization efforts.

Research Output and Academic Involvement. I am currently the Program Co-Chair of PQCrypto 2024, and Artifact Chair of CHES 2024. I'm an active author, and reviewer for IEEE, ACM, and IACR journals, and serve on several academic program committees.

Metrics: Google Scholar: 2199 cites, h-index 25 (https://scholar.google.com/citations?user=2_oEFqYAAAAJ) Scopus: 546 cites, h-index 14 (https://www.scopus.com/authid/detail.uri?authorId=8548822000).

Security Engineering. I mostly code in Assembler, C, and Python, and I'm a fan of Rust. Most of my hardware work is done in SystemVerilog. I can build full-system FPGA prototypes. I'm familiar with formal verification and model checking. I've created various power/emission leakage models and tools for side-channel security work.

I am currently the chair of the RISC-V PQC Task Group at RISC-V International (https://riscv.org). I was one of the main designers of the RISC-V Scalar Cryptography Extensions that were ratified in November 2021; specifically, the entropy source (Zkr), constant-time execution (Zkt), and 32-bit AES/SM4 instructions [10, 11, 13].

I architected PQShield's first commercial PQC Hardware modules that provide side-channel secure Kyber and Dilithium services. I designed and prototyped the system on FPGA, devised masking countermeasures, wrote much of the core firmware, and helped validate and adapt the implementation into commercial products (including ASIC silicon).

Consulting. 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. As a consultant in 2004- I was hired to assess the security of large corporate and governmental information systems and also delivered penetration testing training.

For these roles, I've held CISSP-ISSAP, PCI DSS QSAp, and UK NCSC IA Architect (CCP) certs. I re-certified as a CISSP in June 2022 (active CISSP # 61970.)

3 Professional Experience

TAMPERE UNIVERSITY (Tampere, Finland) 2023/01 -
Professor of Practice, Information Security

I'm a Professor of Practice (työelämäprofessori) at Tampere University, associated with the Network and Information Security Group (NISEC) and the SoC Hub Research Centre. This "industrial-academic" advisory and research role focuses on applied cryptography and hardware/software security engineering. As a part of this, I supervise Ph.D. students and M.Sc. Thesis workers.

PQSHIELD (Oxford, UK) 2018/09 -
Staff Cryptography Architect (Part-Time from 2023)

I was the first employee in this University of Oxford spin-out, where we designed, analyzed, and implemented Post-Quantum Cryptography (PQC). I worked mostly on the design of side-channel-resistant PQC hardware and software. Highlights:

- Architected and prototyped PQShield's first side-channel secure Post-Quantum Cryptography coprocessor, which became a successful semiconductor IP product.
- Worked with industry partners in the RISC-V Crypto TG (CETG, Cryptography Task Group) to design RISC-V Instruction Set Extensions (ISEs). I was the principal designer of the RISC-V entropy source (Zkr), constant-time (Zkt) extensions, as well as many symmetric cipher instructions.

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

I had my little consultancy for a while – before signing the PQShield full-time contract. My main projects and customer engagements: 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). References are available upon request.

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

Engineering work on mbedTLS and lightweight cryptographic implementations. I also authored the HILA5 first-round NIST Post-Quantum Cryptography candidate.

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 the 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.

POST-DOC CRYPTOGRAPHY RESEARCHER 2013/05 - 2015/07
ERCIM Alain Bensoussan Fellowship, Other Research Grants

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

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 APTtype adversaries in penetration exercises.

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

Principal Investigator of a small DARPA-funded lightweight cryptography research project. Design and implementation of lightweight 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, in November 2009.

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

4 Academic/Professional Service (2020-)

- PQCrypto 2024 (Program Co-Chair)
- IACR CHES 2024 (Artifact Chair, Program Committee)
- ASHES 2023 (Program Committee)
- TASER 2023 Workshop (Program Committee)
- IACR CHES 2023 (Program Committee)
- RISC-V Summit 2022 (Program Committee)
- IEEE AsianHOST2022 (Program Committee)
- ASHES 2022 (Program Committee)
- ASHES 2021 (Program Committee)
- IACR CHES 2020 (Program Committee)

5 Academic Bibliography

[1] Markku-Juhani O. Saarinen. Accelerating SLH-DSA by two orders of magnitude with a single hash unit. Fifth NIST PQC Standardization Conference, April 10-12, 2024, Rockville, Maryland. Updated version, IACR ePrint Report 2024/367, 2024. URL: https://eprint.iacr.org/2024/367.

[2] Rafael del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani Saarinen. Threshold raccoon: Practical threshold signatures from standard lattice assumptions. In *Advances in Cryptology EUROCRYPT 2024 – 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland on May 26-30, 2024*. Springer, April 2024. To appear. Full version is available as IACR ePrint Report 2024/184. URL: https://eprint.iacr.org/2024/184.

[3] Markku-Juhani O. Saarinen and Mélissa Rossi. Mask compression: High-order masking on memory-constrained devices. In *Selected Areas in Cryptography – SAC 2023 – 30th International Conference, Fredericton, Canada, August 1418, 2023, Revised Selected Papers*, volume 14201 of *Lecture Notes in Computer Science*, pages 65–81. Springer, 2023. URL: https://eprint.iacr.org/2023/1117, doi:doi.org/10.1007/978-3-031-53368-6_4.

[4] Markku-Juhani O. Saarinen. Wrapq: Side-channel secure key management for post-quantum cryptography. In Thomas Johansson and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 14th International Workshop, PQCrypto 2023, College Park, MD, USA, August 16-18, 2023, Proceedings*, volume 14154 of *Lecture Notes in Computer Science*, pages 637–657. Springer, 2023. URL: https://eprint.iacr.org/2022/1499, doi:10.1007/978-3-031-40003-2_23.

[5] Rafaël del Pino, Thomas Prest, Mélissa Rossi, and Markku-Juhani O. Saarinen. High-order masking of lattice signatures in quasilinear time. In *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, 22-25 May 2023*, pages 1168–1185. IEEE, May 2023. doi:10.1109/SP46215.2023.10179342.

[6] Markku-Juhani O. Saarinen, G. Richard Newell, and Ben Marshall. Development of the RISC-V entropy source interface. *Journal of Cryptographic Engineering*, January 2022. URL: https://rdcu.be/cEp7a, doi:10.1007/s13389-021-00275-6.

[7] Markku-Juhani O. Saarinen. WiP: Applicability of ISO standard side-channel leakage tests to NIST post-quantum cryptography. In *IEEE International Symposium on Hardware Oriented Security and Trust (HOST). June 27–30, 2022 Washington DC, USA*, pages 69–72. IEEE, August 2022. URL: https://eprint.iacr.org/2022/229, doi:10.1109/HOST54066.2022.9839849.

[8] Markku-Juhani O. Saarinen. SP 800-22 and GM/T 0005-2012 tests: Clearly obsolete, possibly harmful. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 31–37. IEEE, June 2022. URL: https://eprint.iacr.org/2022/169, doi:10.1109/EuroSPW55150.2022.00011.

[9] Markku-Juhani O. Saarinen. On entropy and bit patterns of ring oscillator jitter. In *Asian Hardware Oriented Security and Trust Symposium, AsianHOST 2021, Shanghai, China, December 16-18, 2021*, pages 1–6. IEEE, 2021. URL: https://arxiv.org/abs/2102.02196, doi:10.1109/AsianHOST53231.2021.9699508.

[10] Markku-Juhani O. Saarinen, G. Richard Newell, and Ben Marshall. Building a modern TRNG: An entropy source interface for RISC-V. In *4th Workshop on Attacks and Solutions in Hardware Security (ASHES20), November 13, 2020, Virtual Event, USA.*, pages 93–102. ACM, November 2020. doi:10.1145/3411504.3421212.

[11] Markku-Juhani O. Saarinen. Mobile energy requirements of the upcoming NIST post-quantum cryptography standards. In *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pages 23–30. IEEE, April 2020. URL: https://arxiv.org/abs/1912.00916, doi:10.1109/MobileCloud48802.2020.00012.

[12] Markku-Juhani O. Saarinen. A lightweight ISA extension for AES and SM4. In *First International Workshop on Secure RISC-V Architecture Design Exploration (SECRISC-V'20)*. IEEE, August 2020. URL: https://arxiv.org/abs/2002.07041.

[13] Ben Marshall, G. Richard Newell, Dan Page, Markku-Juhani O. Saarinen, and Claire Wolf. The design of scalar AES instruction set extensions for RISC-V. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(1):109–136, December 2020. doi:10.46586/tches.v2021.i1.109-136.

[14] Hayo Baan, Sauvik Bhattacharya, Scott R. Fluhrer, Óscar García-Morchón, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O. Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. Round5: Compact and fast post-quantum public-key encryption. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 83–102. Springer, 2019. doi:10.1007/978-3-030-25510-7_5.

[15] Markku-Juhani O. Saarinen, Sauvik Bhattacharya, Óscar García-Morchón, 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, *Smart Card Research and Advanced Applications, 17th International Conference, CARDIS 2018, Montpellier, France, November 12-14, 2018, Revised Selected Papers*, volume 11389 of *Lecture Notes in Computer Science*, pages 95–110. Springer, 2018. doi:10.1007/978-3-030-15462-2_7.

[16] 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.

[17] Markku-Juhani Olavi Saarinen. Ring-LWE ciphertext compression and error correction: Tools for lightweight post-quantum cryptography. In Richard Chow and Gökay Saldamli, editors, *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, IoTPTS@AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2, 2017*, pages 15–22. ACM, 2017. doi:10.1145/3055245.3055254.

[18] 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, Revised Selected Papers*, volume 10719 of *Lecture Notes in Computer Science*, pages 192–212. Springer, 2017. doi:10.1007/978-3-319-72565-9_10.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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. URL: http://grehack.org/files/2013/GreHack_2013_proceedings-separate_files/3-accepted_papers/3.1_Markku_Juhani_O_Saarinen-Developing_a_Grey_Hat_C2_and_RAT_for_APT_Security_Training_and_Assessment.pdf.

[28] Markku-Juhani O. Saarinen and Daniel 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

6 Recent Talks and Presentations (2020-)

2023-Nov-08 RISC-V Summit: *"Benchmarking RISC-V Post-Quantum Crypto."* Talk at RISC-V Summit 2023, Santa Clara, CA, USA. https://events.linuxfoundation.org/riscv-summit/

2023-Nov-01 ICCC: *"Post-Quantum vs. AVA_VAN."* Talk at the International Common Criteria Conference, Washington DC, USA. https://iccconference.org/

2023-Aug-18 PQCrypto 2023: *"WrapQ: Side-Channel Secure Key Management for Post-Quantum Cryptography."* Paper at 14th International Conference on Post-Quantum Cryptography, College Park, MD, USA. https://pqcrypto2023.umiacs.io/

2023-Aug-16 SAC 2023: *"Mask Compression: High-Order Masking on Memory-Constrained Devices."* Paper at 30th Selected Areas in Cryptography, SAC 2023, University of New Brunswick, Canada. https://sac-workshop.github.io/sac-2023

2023-Jun-29 RISC-V Tech Sessions: *"RISC-V Cryptography and Hardware Security."* Webinar organized by RISC-V International. https://sites.google.com/riscv.org/riscv-technical-sessions/

2023-Jun-05 RISC-V Summit Europe: *"Cryptographic Extenions (Update)."* Technical Working Group presentation at RISC-V Summit Europe 2023, Barcelona, Spain. https://riscv-europe.org/

2023-May-22 IEEE S&P: *"High-Order Masking of Lattice Signatures in Quasilinear Time."* Paper at 44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA. Joint work with Rafaël del Pino, Thomas Prest, and Mélissa Rossi. https://sp2023.ieee-security.org/

2023-Apr-04 NIST PQC Seminar: *"Intro to Side-Channel Security of NIST PQC Standards."* U.S. National Institute of Standards and Technology / Information Technology Laboratory (Virtual.) https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline/pqc-seminars

2023-Feb-15 ETSI QSC9: *"PQC Side-Channel Leakage Assessments in the Semiconductor Industry."* Presentation at 9th ETSI/IQC Quantum Safe Cryptography Event. Sophia Antipolis, France. https://www.etsi.org/events/2117-2023-02-9th-etsi-iqc-quantum-safe-cryptography-workshop

2022-Dec-14 RISC-V Summit 2022: *"RISC-V Zkt: Portable Timing Attack Resistance (via Dynamic Taint Analysis)."* Invited talk at RISC-V Summit 2022. San Jose, CA. https://events.linuxfoundation.org/riscv-summit/

2022-Sep-18 TASER/CHES 2022: *"Verifying constant-time code with RISC-V Zkt and Dynamic Taint Analysis."* Invited talk at TASER (Topics in hArdware SEcurity and RISC-V), IACR CHES 2022. Leuven, Belgium. https://ches.iacr.org/

2022-Sep-15 ICMC 2022: *"Post-Quantum Crypto Side-Channel Tests and a CSP Walk-Through."* Presentation at ICMC 2022, International Cryptographic Module Conference. Washington DC, USA. https://icmconference.org

2022-Jun-28 HOST 2022: *"WiP: Applicability of ISO Standard Side-Channel Leakage Tests to NIST Post-Quantum Cryptography."* Paper in the Work-in-Progress Track at the IEEE International Symposium on Hardware Oriented Security and Trust. Washington DC, USA. http://www.hostsymposium.org/

2022-Jun-06 SSR 2022: *"SP 800-22 and GM/T 0005-2012 Tests: Clearly Obsolete, Possibly Harmful."* Paper at the Security Standardisation Research Conference – Workshop of IEEE Euro Security & Privacy. Genoa, Italy. https://ssr2022.com/

2022-May-30 CryptArchi 2022: *"Side-Channel Leakage Tests for Post-Quantum Crypto Modules."* Presentation at CryptArchi ("Cryptographic architectures embedded in logic devices"). Ile de Porquerolles, France. https://labh-curien.univ-st-etienne.fr/cryptarchi/workshop22/program.html

2022-May-23 ISO/IEC 19790 Day: *"Side-Channel Leakage Tests for Post-Quantum Crypto Modules."* Presentation at the ISO/IEC 19790 Cryptographic Module Day – held with the EU Cybersecurity Act Conference. Brussels, Belgium. https://cryptomod.org/

2022-Jan-25 CMUF Entropy WG: *"The RISC-V Entropy Source Interface."* Presentation at the Regular meeting of the Cryptographic Module User Forum (CMUF) Entropy Working Group (Virtual). https://cmuf.org/

2021-Dec-17 AsianHOST 2021: *"On Entropy and Bit Patterns of Ring Oscillator Jitter."* Asian Hardware Oriented Security and Trust Symposium (AsianHOST). Shanghai, China (Virtual). http://asianhost.org/

2021-Dec-14 HOST Summit 2021: *"Post-Quantum Cryptography: Are We Ready?"* Panel with Lily Chen (NIST), David McGrew (Cisco), Johanna Sepúlveda (Airbus and TuM), and Ingrid Verbauwhede (KU Leuven). IEEE HOST Summit 2021. Washington DC, USA (Virtual). http://www.hostsymposium.org/

2021-Nov-18 ECW PQC: *"Specifying and Testing PQC Hardware Modules."* European Cyber Week 2021 Workshop "Implementing post-quantum cryptography." Rennes, France (Live). https://en.european-cyber-week.eu/cryptographie-post-quantique

2021-Oct-06 Worcester Polytechnic Institute: *"Building and Testing Entropy Sources for Cryptography."* WPI ECE Graduate Seminar Lecture. Worcester, MD USA (Virtual). https://www.wpi.edu/news/calendar/events/ece-graduate-seminar-lecture-dr-markku-juhani-o-saarinen-senior-cryptography

2021-Sep-03 ICMC 2021: *"Building and Testing a Modern TRNG/RBG: The RISC-V Entropy Source Interface."* ICMC21: International Cryptographic Module Conference. Bethesda, MD USA (Virtual). https://icmconference.org/

2021-Sep-02 ICMC 2021: *"PQC Modules: Requirement Specifications, Integration, and Testing."* ICMC21: International Cryptographic Module Conference. Bethesda, MD USA (Virtual). https://icmconference.org/

2021-Apr-23 Rennes: *"Post-Quantum Cryptography Hardware."* Séminaire de cryptographie, IRMAR / Université de Rennes 1. In collaboration with French MoD and DGA. Virtual. https://webmath.univ-rennes1.fr/crypto/2021/Saarinen

2021-Jan-13 RWC 2021: *"RISC-V Scalar Crypto."* (with B. Marshall.) RWC 2021: Real World Crypto Symposium. An IACR (International Association for Cryptologic Research) event (Virtual). https://rwc.iacr.org/2021/

2020-Nov-13 ASHES 2020: *"Building a Modern TRNG: An Entropy Source Interface for RISC-V."* (with G. R. Newell and B. Marshall.) ASHES 2020: Attacks and Solutions in Hardware Security, Workshop of ACM CCS 2020 (Virtual). http://ashesworkshop.org/

2020-Sep-24 ICMC 2020: *"Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards."* ICMC20: International Cryptographic Module Conference (Virtual). https://icmconference.org/

2020-Sep-03 RISC-V Global Forum: *"RISC-V True Random Number Generation: Probably Too Important to be Left to Chance."* RISC-V Global Forum 2020 (Virtual). https://riscv.org/proceedings/2020/09/risc-v-global-forum-proceedings/

2020-Aug-23 SECRISC-V 2020: *"A Lightweight ISA Extension for AES and SM4."* SECRISC-V'20: First International Workshop on Secure RISC-V Architecture Design Exploration (Virtual). https://ascslab.org/conferences/secriscv/index.html

2020-Aug-04 MobileCloud 2020: *"Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards."* MobileCloud 2020: 8th IEEE Intl. Conference on Mobile Cloud Computing, Services, and Engineering (Virtual).

7 Patents and Published (Pending) Applications

1. Markku-Juhani O. Saarinen. *"Method and apparatus for improved pseudo-random number generation."* U.S. Patent 7007050: Filed 2001-May-01, Granted 2006-Feb-28. https://patents.google.com/patent/US7007050B2

2. Markku-Juhani O. Saarinen and Ville Ollikainen. *"Method and apparatus for implementing secure and selectively deniable file storage."* U.S. Patent 8555088: Priority 2008-Sep-22. Granted 2013-Oct-08. https://patents.google.com/patent/US8555088B2

3. Markku-Juhani O. Saarinen. *"Cryptography using a cryptographic state."* U.S. US20220066741A1 Application: Priority 2019-Mar-18. Published 2022-Mar-03. https://patents.google.com/patent/US20220066741A1

4. Markku-Juhani O. Saarinen. *"Cryptographic architecture for cryptographic permutation."* U.S. US20220138349A1 Application: Filed 2020-Jul-15. Published 2022-May-05. https://patents.google.com/patent/US20220138349A1

5. Markku-Juhani O. Saarinen. *"Co-processor for cryptographic operations."* WIPO (PCT) WO2021032946A1 Application: Priority 2019-Aug-16, Published 2021-Feb-25. https://patents.google.com/patent/WO2021032946A1

6. Markku-Juhani O. Saarinen. *"Random Number Generation."* WIPO (PCT) WO2022112788A1 Application: Priority 2020-Nov-26. Published 2022-Jun-02. https://patents.google.com/patent/WO2022112788A1/

7. Markku-Juhani O. Saarinen. *"Cryptographic system for post-quantum cryptographic operations."* WIPO (PCT) WO2023285830A1 Application: Priority 2022-Jul-14. Published 2023-Jan-19. https://patents.google.com/patent/WO2023285830A1/

8. Markku-Juhani O. Saarinen. *"Secure processing system and method."* GB 2207808.3 Application: Priority 2022-May-26. Published 2022-Jul-13. https://patents.google.com/patent/GB202207808D0/

9. Markku-Juhani O. Saarinen. *"Method and apparatus for storing/recovering a plurality of secret shares."* GB 2211124.9 Application: Priority 2022-Jul-29. Published 2022-Sep-14. https://patents.google.com/patent/GB202211124D0/