Dr. Markku-Juhani O. Saarinen

Curriculum Vitae – September 3, 2021

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, I 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.

I was one of the main designers of the official RISC-V Cryptography Extensions, specifically the entropy source, constant-time feature, and AES/SM4 instructions [2, 3, 5].

For many years I've also worked on systems security, having been hired to audit sensitive corporate information systems, and also delivered penetration testing training.

Security Engineering. I mostly code in C and Python, and I'm a fan of Rust. Most of my hardware work is done in SystemVerilog. I can also work with many other tools and languages and write assembly for ARM, x86, RISC-V, and others. I use formal verification and model checking tools in both hardware and software work.

Cryptanalysis and Cryptographic Design. I have 20 years of experience in the design and analysis of real-life cryptoalgorithms and protocols. I am currently deeply involved with various PQC (Post-Quantum Cryptography) transition and standardization efforts.

I have also cryptanalyzed ("broken") many algorithms. Some of these results are confidential, but I have also published several, e.g. on PAES and HKC [11], Hummingbird-1 & 2 [18, 23], FORK-256 [29], FSB hash [30], and LILI-128 [36].

Research Output and Academic Involvement. I'm an active author, reviewer for IEEE, ACM, IACR journals, and serve in scientific committees (recently: CHES 2020, ASHES 2021). Citation metrics: 1700+ cites, h-index 25 (Google Scholar) or 400, h=12 (Scopus).
Scholar Profile – https://scholar.google.com/citations?user=2_oEFqYAAAAJ
Scopus Profile – https://www.scopus.com/authid/detail.uri?authorId=8548822000

Professional Experience

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

I was an early hire in this University of Oxford spin-out, where we design, analyze, and implement quantum-resistant cryptography. My work is mostly research engineering in cryptography, involving embedded C, Verilog, Python, oscilloscopes, formal verification, side-channel evaluation, development boards, patents, scientific collaboration. Highlights:

- Foundational software and hardware engineering in relation to the NIST PQC standardization project. Designed and implemented the initial RISC-V CPU cores and post-quantum cryptography coprocessor.
- Worked with industry partners in the RISC-V Crypto TG (Cryptography Task Group) to design RISC-V Instruction Set Extensions (ISEs). I'm the main designer of the entropy source and some of the cryptography instructions.

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

I had my own 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.

ITINERANT RESEARCHER IN CRYPTOGRAPHY 2013/05 - 2015/07
ERCIM Alain Bensoussan Fellowship, Post-Doc 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

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 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, 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 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).

Talks and Presentations

2021-09-03 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/

2021-09-02 ICMC 2021: *"PQC Modules: Requirement Specifications, Integration, and Testing."* ICMC21: International Cryptographic Module Conference. Bethesda, MD USA / Virtual. https://icmconference.org/

2021-04-23 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

2021-01-13 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/

2020-11-13 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/

2020-09-24 ICMC 2020: *"Mobile Energy Requirements of the Upcoming NIST Post-Quantum Cryptography Standards."* ICMC20: International Cryptographic Module Conference. Virtual. https://icmconference.org/

2020-09-03 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/

2020-08-23 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

2020-08-04 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. https://www.mobile-cloud.net/

2020-07-21 DAC 2020: *"A RISC-V Secure Element for PQC: Fantasy Chip Codesign Approach."* DAC 2020: 57th Design Automation Conference (IEEE, Designer Track). Virtual. https://www.dac.com/

2019-11-07 ETSI PQC 2019: *"Towards microjoule PQC: How does the post-quantum transition impact mobile device energy budgets?"* 7th ETSI/IQC Quantum Safe Cryptography Workshop. Seattle, US. https://www.etsi.org/events/1607-etsi-iqc-quantum-safe-cryptography-workshop-2019

2019-08-24 NIST PQC 2019: *"ROUND5-Update and Future Directions."* (with Oscar Garcia-Morchon.) Second (NIST) PQC Standardization Conference. UCSB, US. https://csrc.nist.gov/events/2019/second-pqc-standardization-conference

(.. Cutoff. See "publications" for earlier talks given in events with proceedings ..)

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

Current (PQShield) patent applications where I'm the inventor:

- Co-processor for cryptographic operations. (GB202002655D0), 2020.
- Cryptography using a cryptographic state. (WO2020188269A1), 2020.
- Random Number Generation. (Recently filed), 2020.

Selected Publications

[1] Markku-Juhani O. Saarinen. On entropy and bit patterns of ring oscillator jitter. Preprint, February 2021. URL: https://arxiv.org/abs/2102.02196.

[2] 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. URL: https://eprint.iacr.org/2020/866, doi:10.1145/3411504.3421212.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.