A Complete Bibliography of Publications in the *Journal of Cryptographic Engineering*

Nelson H. F. Beebe
University of Utah
Department of Mathematics, 110 LCB
155 S 1400 E RM 233
Salt Lake City, UT 84112-0090
USA

Tel: +1 801 581 5254
FAX: +1 801 581 4148

E-mail: beebe@math.utah.edu, beebe@acm.org, beebe@computer.org (Internet)
WWW URL: https://www.math.utah.edu/~beebe/

08 August 2024
Version 1.26

Title word cross-reference

References

Koc:2011:IBC

[1] Çetin Kaya Koç. Introduction to the *Journal of Cryptographic Engineering*. *Journal of Cryptographic Engineering*, 1(1):1–3, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://cs.ucsb.edu/~koc/docs/j75.pdf; http://link.springer.com/article/10.1007/s13389-011-0007-x; http://link.springer.com/content/pdf/10.1007/s13389-011-0007-x.pdf.

Kocher:2011:IDP

[2] Paul Kocher, Joshua Jaffe, Benjamin

Jun, and Pankaj Rohatgi. Introduction to differential power analysis. *Journal of Cryptographic Engineering*, 1(1):5–27, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0006-y; http://link.springer.com/content/pdf/10.1007/s13389-011-0006-y.pdf.

Molter:2011:SPA

[3] H. Gregor Molter, Marc Stöttinger, Abdulhadi Shoufan, and Falko Strenzke. A simple power analysis attack on a McEliece cryptoprocessor. *Journal of Cryptographic Engineering*, 1(1):29–36, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0001-3.

Guneysu:2011:UHC

[4] Tim Güneysu. Utilizing hard cores of modern FPGA devices for high-performance cryptography. *Journal of Cryptographic Engineering*, 1(1):37–55, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0002-2.

Dominguez-Oviedo:2011:ALE

[5] Agustin Dominguez-Oviedo and M. Anwar Hasan. Algorithm-level error detection for Montgomery ladder-based ECSM. *Journal of Cryptographic Engineering*, 1(1):57–69, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0003-1.

Skorobogatov:2011:SMS

[6] Sergei Skorobogatov. Synchronization method for SCA and fault attacks. *Journal of Cryptographic Engineering*, 1(1):71–77, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0004-0.

Hocquet:2011:HPN

[7] Cédric Hocquet, Dina Kamel, Francesco Regazzoni, Jean-Didier Legat, Denis Flandre, David Bol, and François-Xavier Standaert. Harvesting the potential of nano-CMOS for lightweight cryptography: an ultra-low-voltage 65 nm AES coprocessor for passive RFID tags. *Journal of Cryptographic Engineering*, 1(1):79–86, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0005-z.

Anonymous:2011:HCa

[8] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 1(1):??, April 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Moreno:2011:SRB

[9] Carlos Moreno and M. Anwar Hasan. SPA-resistant binary exponentiation with optimal execution time. *Journal of Cryptographic Engineering*, 1(2):87–99, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0008-9.

Beuchat:2011:LAU

[10] Jean-Luc Beuchat, Eiji Okamoto, and Teppei Yamazaki. A low-area unified hardware architecture for the AES and the cryptographic hash function ECHO. *Journal of Cryptographic Engineering*, 1(2):101–121, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0009-8.

Doget:2011:USC

[11] Julien Doget, Emmanuel Prouff, Matthieu Rivain, and François-Xavier Standaert. Univariate side channel attacks and leakage modeling. *Journal of Cryptographic Engineering*, 1(2):123–144, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0010-2.

Whitnall:2011:FEF

[12] Carolyn Whitnall and Elisabeth Oswald. A fair evaluation framework for comparing side-channel distinguishers. *Journal of Cryptographic Engineering*, 1(2):145–160, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0011-1.

Goundar:2011:SMW

[13] Raveen R. Goundar, Marc Joye, Atsuko Miyaji, Matthieu Rivain, and Alexandre Venelli. Scalar multiplication on Weierstraß elliptic curves from co-Z arithmetic. *Journal of Cryptographic Engineering*, 1(2):161–176, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0012-0.

Anonymous:2011:HCb

[14] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 1(2):??, August 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Katzenbeisser:2011:RPL

[15] Stefan Katzenbeisser, Ünal Kocabaš, Vincent van der Leest, Ahmad-Reza Sadeghi, Geert-Jan Schrijen, and Christian Wachsmann. Recyclable PUFs: logically reconfigurable PUFs. *Journal of Cryptographic Engineering*, 1(3):177–186, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0016-9.

Taverne:2011:SSM

[16] Jonathan Taverne, Armando Faz-Hernández, Diego F. Aranha, Francisco Rodríguez-Henríquez, Darrel Hankerson, and Julio López. Speeding scalar multiplication over binary elliptic curves using the new carry-less multiplication instruction. *Journal of Cryptographic Engineering*, 1(3):187–199, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0017-8.

Meloni:2011:HPG

[17] Nicolas Méloni, Christophe Negre, and M. Anwar Hasan. High performance GHASH and impacts of a class of unconventional bases. *Journal of Cryptographic Engineering*, 1

(3):201–218, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0013-z`.

Tunstall:2011:PCD

[18] Michael Tunstall. Practical complexity differential cryptanalysis and fault analysis of AES. *Journal of Cryptographic Engineering*, 1(3):219–230, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0018-7`.

Medwed:2011:EAS

[19] Marcel Medwed and François-Xavier Standaert. Extractors against side-channel attacks: weak or strong? *Journal of Cryptographic Engineering*, 1(3):231–241, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0014-y`.

Brier:2011:MFA

[20] Éric Brier, David Naccache, Phong Q. Nguyen, and Mehdi Tibouchi. Modulus fault attacks against RSA–CRT signatures. *Journal of Cryptographic Engineering*, 1(3):243–253, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0015-x`.

Anonymous:2011:HCc

[21] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 1(3): ??, November 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Dichtl:2011:NMB

[22] Markus Dichtl. A new method of black box power analysis and a fast algorithm for optimal key search. *Journal of Cryptographic Engineering*, 1(4):255–264, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0019-6`.

Endo:2011:CGC

[23] Sho Endo, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh. An on-chip glitchy-clock generator for testing fault injection attacks. *Journal of Cryptographic Engineering*, 1(4):265–270, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0022-y`.

Avanzi:2011:SCA

[24] Roberto Avanzi, Simon Hoerder, Dan Page, and Michael Tunstall. Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *Journal of Cryptographic Engineering*, 1(4):271–281, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0024-9`. See erratum [34].

Strenzke:2011:MAS

[25] Falko Strenzke. Message-aimed side channel and fault attacks against public key cryptosystems with homomorphic properties. *Journal of Cryptographic Engineering*, 1(4):283–292, December 2011. CODEN ???? ISSN 2190-8508

(print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0020-0.

Hospodar:2011:MLS

[26] Gabriel Hospodar, Benedikt Gierlichs, Elke De Mulder, Ingrid Verbauwhede, and Joos Vandewalle. Machine learning in side-channel analysis: a first study. *Journal of Cryptographic Engineering*, 1(4):293–302, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0023-x.

Lux:2011:TSD

[27] Alexander Lux and Artem Starostin. A tool for static detection of timing channels in Java. *Journal of Cryptographic Engineering*, 1(4):303–313, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0021-z.

Anonymous:2011:HCd

[28] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 1(4): ??, December 2011. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Grabher:2012:EMD

[29] P. Grabher, J. Großschädl, S. Hoerder, K. Järvinen, D. Page, S. Tillich, and M. Wójcik. An exploration of mechanisms for dynamic cryptographic instruction set extension. *Journal of Cryptographic Engineering*, 2(1):1–18, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-011-0025-8.

Gouvea:2012:ESI

[30] Conrado P. L. Gouvêa, Leonardo B. Oliveira, and Julio López. Efficient software implementation of public-key cryptography on sensor networks using the MSP430X microcontroller. *Journal of Cryptographic Engineering*, 2(1):19–29, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0029-z.

Gueron:2012:ESI

[31] Shay Gueron. Efficient software implementations of modular exponentiation. *Journal of Cryptographic Engineering*, 2(1):31–43, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0031-5.

Carlet:2012:AAS

[32] Claude Carlet, Jean-Charles Faugère, Christopher Goyet, and Guénaël Renault. Analysis of the algebraic side channel attack. *Journal of Cryptographic Engineering*, 2(1):45–62, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0028-0.

Elaabid:2012:PT

[33] M. Abdelaziz Elaabid and Sylvain Guilley. Portability of templates. *Journal of Cryptographic Engineering*, 2 (1):63–74, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0030-6.

Avanzi:2012:ESC

[34] Roberto Avanzi, Simon Hoerder, Dan Page, and Michael Tunstall. Erratum to: Side-channel attacks on the McEliece and Niederreiter public-key cryptosystems. *Journal of Cryptographic Engineering*, 2(1):75, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-011-0026-7; http://link.springer.com/content/pdf/10.1007/s13389-011-0026-7.pdf`. See [24].

Anonymous:2012:HCa

[35] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 2(1): ??, May 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Bernstein:2012:HSH

[36] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. *Journal of Cryptographic Engineering*, 2(2):77–89, September 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0027-1; http://link.springer.com/content/pdf/10.1007/s13389-012-0027-1.pdf`.

Hasan:2012:SMS

[37] M. Anwar Hasan and Christophe Negre. Sequential multiplier with sublinear gate complexity. *Journal of Cryptographic Engineering*, 2(2):91–97, September 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0035-1`.

Yen:2012:MEA

[38] Sung-Ming Yen, Chien-Ning Chen, and SangJae Moon. Multi-exponentiation algorithm based on binary GCD computation and its application to side-channel countermeasure. *Journal of Cryptographic Engineering*, 2(2):99–110, September 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0032-4`.

Roche:2012:HOG

[39] Thomas Roche and Emmanuel Prouff. Higher-order glitch free implementation of the AES using Secure Multi–Party Computation protocols. *Journal of Cryptographic Engineering*, 2(2):111–127, September 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0033-3`.

Bringer:2012:PAA

[40] Julien Bringer, Hervé Chabanne, and Thanh Ha Le. Protecting AES against side-channel analysis using wire-tap codes. *Journal of Cryptographic Engineering*, 2(2):129–141, September 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0034-2`.

Anonymous:2012:HCb

[41] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 2(2): ??, September 2012. CODEN ????

ISSN 2190-8508 (print), 2190-8516 (electronic).

Kasper:2012:SCB

[42] Markus Kasper, Amir Moradi, Georg T. Becker, Oliver Mischke, Tim Güneysu, Christof Paar, and Wayne Burleson. Side channels as building blocks. *Journal of Cryptographic Engineering*, 2(3): 143–159, October 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0040-4`.

Mather:2012:PSC

[43] Luke Mather and Elisabeth Oswald. Pinpointing side-channel information leaks in web applications. *Journal of Cryptographic Engineering*, 2(3):161–177, October 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0036-0`.

Trujillo-Olaya:2012:APV

[44] Vladimir Trujillo-Olaya, Timothy Sherwood, and Çetin Kaya Koç. Analysis of performance versus security in hardware realizations of small elliptic curves for lightweight applications. *Journal of Cryptographic Engineering*, 2(3):179–188, October 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0039-x`.

Shariati:2012:AEE

[45] Saloomeh Shariati, François-Xavier Standaert, Laurent Jacques, and Benoit Macq. Analysis and experimental evaluation of image-based PUFs. *Journal of Cryptographic Engineering*, 2(3):189–206, October 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0041-3`.

Anonymous:2012:HCc

[46] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 2(3):??, October 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Rolt:2012:SAS

[47] Jean Da Rolt, Amitabh Das, Santosh Ghosh, Giorgio Di Natale, Marie-Lise Flottes, Bruno Rouzeyre, and Ingrid Verbauwhede. Scan attacks on side-channel and fault attack resistant public-key implementations. *Journal of Cryptographic Engineering*, 2(4):207–219, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0045-z`.

Baldwin:2012:CES

[48] Brian Baldwin, Raveen R. Goundar, Mark Hamilton, and William P. Marnane. Co-Z ECC scalar multiplications for hardware, software and hardware-software co-design on embedded systems. *Journal of Cryptographic Engineering*, 2(4):221–240, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0042-2`.

Gueron:2012:PMS

[49] Shay Gueron and Vlad Krasnov. Parallelizing message schedules to accel-

erate the computations of hash functions. *Journal of Cryptographic Engineering*, 2(4):241–253, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0037-z`.

Koeberl:2012:PDA

[50] Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik, Marcin Wójcik, and Wei Wu. A practical device authentication scheme using SRAM PUFs. *Journal of Cryptographic Engineering*, 2(4):255–269, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-012-0043-1`.

Anonymous:2012:HCd

[51] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 2(4): ??, November 2012. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Prouff:2013:ICS

[52] Emmanuel Prouff and Patrick Schaumont. Introduction to the CHES 2012 special issue. *Journal of Cryptographic Engineering*, 3(1):1, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0055-5; http://link.springer.com/content/pdf/10.1007/s13389-013-0055-5.pdf`.

Schlosser:2013:SPE

[53] Alexander Schlösser, Dmitry Nedospasov, Juliane Krämer, Susanna Orlic, and Jean-Pierre Seifert. Simple photonic emission analysis of AES. *Journal of Cryptographic Engineering*, 3 (1):3–15, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0053-7`.

Ruhrmair:2013:PUP

[54] Ulrich Rührmair and Marten van Dijk. On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols. *Journal of Cryptographic Engineering*, 3(1):17–28, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0052-8`.

Heyse:2013:CBC

[55] Stefan Heyse and Tim Güneysu. Code-based cryptography on reconfigurable hardware: tweaking Niederreiter encryption for performance. *Journal of Cryptographic Engineering*, 3(1):29–43, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0056-4`.

Gerard:2013:UOL

[56] Benoît Gérard and François-Xavier Standaert. Unified and optimized linear collision attacks and their application in a non-profiled setting: extended version. *Journal of Cryptographic Engineering*, 3(1):45–58, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0051-9`.

Fouque:2013:ARC

[57] Pierre-Alain Fouque, Nicolas Guillermin, Delphine Leresteux, Mehdi Tibouchi, and Jean-Christophe Zapalowicz. Attacking RSA–CRT signatures with faults on Montgomery multiplication. *Journal of Cryptographic Engineering*, 3(1):59–72, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0050-x.

Anonymous:2013:HCa

[58] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 3(1):??, April 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Ali:2013:DFA

[59] Sk Subidh Ali, Debdeep Mukhopadhyay, and Michael Tunstall. Differential fault analysis of AES: towards reaching its limits. *Journal of Cryptographic Engineering*, 3(2):73–97, June 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0046-y.

Montminy:2013:ICD

[60] David P. Montminy, Rusty O. Baldwin, Michael A. Temple, and Eric D. Laspe. Improving cross-device attacks using zero-mean unit-variance normalization. *Journal of Cryptographic Engineering*, 3(2):99–110, June 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0038-y.

Akinyele:2013:CFR

[61] Joseph A. Akinyele, Christina Garman, Ian Miers, Matthew W. Pagano, Michael Rushanan, Matthew Green, and Aviel D. Rubin. Charm: a framework for rapidly prototyping cryptosystems. *Journal of Cryptographic Engineering*, 3(2):111–128, June 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0057-3.

Kurdziel:2013:MPO

[62] Michael T. Kurdziel, Marcin Lukowiak, and Michael A. Sanfilippo. Minimizing performance overhead in memory encryption. *Journal of Cryptographic Engineering*, 3(2):129–138, June 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0047-5.

Anonymous:2013:HCb

[63] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 3(2):??, June 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Mohamed:2013:IAS

[64] Mohamed Saied Emam Mohamed, Stanislav Bulygin, Michael Zohner, Annelie Heuser, Michael Walter, and Johannes Buchmann. Improved algebraic side-channel attack on AES. *Journal of Cryptographic Engineering*, 3(3):139–156, September 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0059-1.

Christofi:2013:FVC

[65] Maria Christofi, Boutheina Chetali, Louis Goubin, and David Vigilant. Formal verification of a CRT–RSA implementation against fault attacks. *Journal of Cryptographic Engineering*, 3(3):157–167, September 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0049-3.

Briais:2013:FST

[66] Sébastien Briais, Jean-Luc Danger, and Sylvain Guilley. A formal study of two physical countermeasures against side channel attacks. *Journal of Cryptographic Engineering*, 3(3):169–180, September 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0054-6.

Brown:2013:TTC

[67] Mark Brown. Toward a taxonomy of communications security models. *Journal of Cryptographic Engineering*, 3(3):181–195, September 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0058-2.

Anonymous:2013:HCc

[68] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 3(3): ??, September 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Yamamoto:2013:VEP

[69] Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko Takenaka, and Kouichi Itoh. Variety enhancement of PUF responses using the locations of random outputting RS latches. *Journal of Cryptographic Engineering*, 3(4):197–211, November 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-012-0044-0; http://link.springer.com/content/pdf/10.1007/s13389-012-0044-0.pdf.

Bhasin:2013:CHA

[70] Shivam Bhasin, Sylvain Guilley, Annelie Heuser, and Jean-Luc Danger. From cryptography to hardware: analyzing and protecting embedded Xilinx BRAM for cryptographic applications. *Journal of Cryptographic Engineering*, 3(4):213–225, November 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0048-4.

Kamal:2013:SHI

[71] Abdel Alim Kamal and Amr M. Youssef. Strengthening hardware implementations of NTRUEncrypt against fault analysis attacks. *Journal of Cryptographic Engineering*, 3(4):227–240, November 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0061-7.

Danger:2013:SSC

[72] Jean-Luc Danger, Sylvain Guilley, Philippe Hoogvorst, Cédric Murdica,

and David Naccache. A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards. *Journal of Cryptographic Engineering*, 3(4):241–265, November 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0062-6`.

Anonymous:2013:HCd

[73] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 3(4): ??, November 2013. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Bertoni:2014:ICS

[74] Guido Bertoni and Jean-Sébastien Coron. Introduction to the CHES 2013 special issue. *Journal of Cryptographic Engineering*, 4(1):1, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0076-8; http://link.springer.com/content/pdf/10.1007/s13389-014-0076-8.pdf`.

Oliveira:2014:TFP

[75] Thomaz Oliveira, Julio López, Diego F. Aranha, and Francisco Rodríguez-Henríquez. Two is the fastest prime: lambda coordinates for binary elliptic curves. *Journal of Cryptographic Engineering*, 4(1):3–17, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0069-z`.

Becker:2014:SDL

[76] Georg T. Becker, Francesco Regazzoni, Christof Paar, and Wayne P. Burleson. Stealthy dopant-level hardware Trojans: extended version. *Journal of Cryptographic Engineering*, 4(1):19–31, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0068-0`.

DeMulder:2014:UBS

[77] Elke De Mulder, Michael Hutter, Mark E. Marson, and Peter Pearson. Using Bleichenbacher's solution to the hidden number problem to attack nonce leaks in 384-bit ECDSA: extended version. *Journal of Cryptographic Engineering*, 4(1):33–45, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0072-z`.

Grosso:2014:MVM

[78] Vincent Grosso, François-Xavier Standaert, and Sebastian Faust. Masking vs. multiparty computation: how large is the gap for AES? *Journal of Cryptographic Engineering*, 4(1):47–57, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0073-y`.

Sugawara:2014:MSC

[79] Takeshi Sugawara, Daisuke Suzuki, Minoru Saeki, Mitsuru Shiozaki, and Takeshi Fujino. On measurable side-channel leaks inside ASIC design primitives. *Journal of Cryptographic Engineering*, 4(1):59–73, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0078-6`.

Anonymous:2014:HCa

[80] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 4(1):??, April 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Almeida:2014:LPB

[81] Leonardo C. Almeida, Ewerton R. Andrade, Paulo S. L. M. Barreto, and Marcos A. Simplicio, Jr. Lyra: password-based key derivation with tunable memory and processing costs. *Journal of Cryptographic Engineering*, 4(2):75–89, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0063-5.

Negre:2014:EBP

[82] Chistophe Negre. Efficient binary polynomial multiplication based on optimized Karatsuba reconstruction. *Journal of Cryptographic Engineering*, 4 (2):91–106, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0066-2.

Carlet:2014:ASC

[83] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Emmanuel Prouff Houssem Maghrebi. Achieving side-channel high-order correlation immunity with leakage squeezing. *Journal of Cryptographic Engineering*, 4(2):107–121, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0067-1.

Biasi:2014:SEC

[84] Felipe P. Biasi, Paulo S. L. M. Barreto, Rafael Misoczki, and Wilson V. Ruggiero. Scaling efficient code-based cryptosystems for embedded platforms. *Journal of Cryptographic Engineering*, 4(2):123–134, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0070-1.

Paul:2014:DSC

[85] Goutam Paul and Anupam Chattopadhyay. Designing stream ciphers with scalable data-widths: a case study with HC-128. *Journal of Cryptographic Engineering*, 4(2):135–143, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0071-0.

Anonymous:2014:HCb

[86] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 4(2): ??, June 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Moro:2014:FVS

[87] N. Moro, K. Heydemann, E. Encrenaz, and B. Robisson. Formal verification of a software countermeasure against instruction skip attacks. *Journal of Cryptographic Engineering*, 4(3):145–156, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0077-7.

Belaid:2014:TFR

[88] Sonia Belaïd, Fabrizio De Santis, Johann Heyszl, Stefan Mangard, Marcel Medwed, Jørn-Marc Schmidt, François-Xavier Standaert, and Stefan Tillich. Towards fresh re-keying with leakage-resilient PRFs: cipher design principles and analysis. *Journal of Cryptographic Engineering*, 4(3):157–171, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0079-5`.

Rauzy:2014:FPC

[89] Pablo Rauzy and Sylvain Guilley. A formal proof of countermeasures against fault injection attacks on CRT–RSA. *Journal of Cryptographic Engineering*, 4(3):173–185, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-013-0065-3`.

Kamel:2014:ULI

[90] Dina Kamel, Mathieu Renauld, Denis Flandre, and François-Xavier Standaert. Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations. *Journal of Cryptographic Engineering*, 4(3):187–195, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0080-z`.

Tiran:2014:MLF

[91] S. Tiran, S. Ordas, Y. Teglia, M. Agoyan, and P. Maurine. A model of the leakage in the frequency domain and its application to CPA and DPA. *Journal of Cryptographic Engineering*, 4(3):197–212, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0074-x`.

Anonymous:2014:HCc

[92] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 4(3): ??, September 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Schindler:2014:PAP

[93] Werner Schindler and Andreas Wiemers. Power attacks in the presence of exponent blinding. *Journal of Cryptographic Engineering*, 4(4):213–236, November 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0081-y`.

Karati:2014:NAB

[94] Sabyasachi Karati, Abhijit Das, Dipanwita Roychowdhury, Bhargav Bellur, Debojyoti Bhattacharya, and Aravind Iyer. New algorithms for batch verification of standard ECDSA signatures. *Journal of Cryptographic Engineering*, 4(4):237–258, November 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0082-x`.

Clavier:2014:PIS

[95] Christophe Clavier, Jean-Luc Danger, Guillaume Duc, M. Abdelaziz Elaabid, Benoît Gérard, Sylvain Guilley, Annelie Heuser, Michael Kasper, Yang Li, Victor Lomné, Daisuke Nakatsu,

Kazuo Ohta, Kazuo Sakiyama, Laurent Sauvage, Werner Schindler, and et al. Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest. *Journal of Cryptographic Engineering*, 4(4):259–274, November 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0075-9.

Bos:2014:CTM

[96] Joppe W. Bos. Constant time modular inversion. *Journal of Cryptographic Engineering*, 4(4):275–281, November 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0084-8.

Anonymous:2014:HC

[97] Anonymous. Help & contacts. *Journal of Cryptographic Engineering*, 4(4): ??, November 2014. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Templin:2015:NPA

[98] Joshua R. Templin and Jason R. Hamlet. A new power-aware FPGA design metric. *Journal of Cryptographic Engineering*, 5(1):1–11, April 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-013-0060-8.

Banik:2015:IDF

[99] Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar. Improved differential fault attack on MICKEY 2.0. *Journal of Cryptographic Engineering*, 5(1):13–29, April 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0083-9.

Faz-Hernandez:2015:ESA

[100] Armando Faz-Hernández, Patrick Longa, and Ana H. Sánchez. Efficient and secure algorithms for GLV-based scalar multiplication and their implementation on GLV–GLS curves (extended version). *Journal of Cryptographic Engineering*, 5(1):31–52, April 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0085-7.

OFlynn:2015:SSC

[101] Colin O'Flynn and Zhizhang Chen. Synchronous sampling and clock recovery of internal oscillators for side channel analysis and fault injection. *Journal of Cryptographic Engineering*, 5(1):53–69, April 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0087-5.

Batina:2015:ICS

[102] Lejla Batina and M. J. B. Robshaw. Introduction to the CHES 2014 special issue. *Journal of Cryptographic Engineering*, 5(2):71–72, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0098-x; http://link.springer.com/content/pdf/10.1007/s13389-015-0098-x.pdf.

Coron:2015:FEP

[103] Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek. Fast evaluation of

polynomials over binary finite fields and application to side-channel countermeasures. *Journal of Cryptographic Engineering*, 5(2):73–83, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0099-9.

Sugawara:2015:RSD

[104] Takeshi Sugawara, Daisuke Suzuki, Ryoichi Fujii, Shigeaki Tawa, Ryohei Hori, Mitsuru Shiozaki, and Takeshi Fujino. Reversing stealthy dopant-level circuits. *Journal of Cryptographic Engineering*, 5(2):85–94, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0102-5.

Genkin:2015:GYH

[105] Daniel Genkin, Itamar Pipman, and Eran Tromer. Get your hands off my laptop: physical side-channel key-extraction attacks on PCs. *Journal of Cryptographic Engineering*, 5(2):95–112, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0100-7.

Vliegen:2015:PFE

[106] Jo Vliegen, Nele Mentens, Dirk Koch, Dries Schellekens, and Ingrid Verbauwhede. Practical feasibility evaluation and improvement of a pay-per-use licensing scheme for hardware IP cores in Xilinx FPGAs. *Journal of Cryptographic Engineering*, 5(2):113–122, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0088-4.

Lerman:2015:MLA

[107] Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. A machine learning approach against a masked AES. *Journal of Cryptographic Engineering*, 5(2):123–139, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0089-3.

Gueron:2015:FPF

[108] Shay Gueron and Vlad Krasnov. Fast prime field elliptic-curve cryptography with 256-bit primes. *Journal of Cryptographic Engineering*, 5(2):141–151, June 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0090-x.

Guo:2015:SAC

[109] Xiaofei Guo, Debdeep Mukhopadhyay, Chenglu Jin, and Ramesh Karri. Security analysis of concurrent error detection against differential fault analysis. *Journal of Cryptographic Engineering*, 5(3):153–169, September 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-014-0092-8.

Perin:2015:VHC

[110] Guilherme Perin, Laurent Imbert, Philippe Maurine, and Lionel Torres. Vertical and horizontal correlation attacks on RNS-based exponentiations. *Journal of Cryptographic Engineering*, 5(3):171–185, September

2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0095-0`.

Yamamoto:2015:NME

[111] Dai Yamamoto, Kazuo Sakiyama, Mitsugu Iwamoto, Kazuo Ohta, Masahiko Takenaka, Kouichi Itoh, and Naoya Torii. A new method for enhancing variety and maintaining reliability of PUF responses and its evaluation on ASICs. *Journal of Cryptographic Engineering*, 5(3):187–199, September 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-014-0091-9`.

Hutter:2015:MMA

[112] Michael Hutter and Peter Schwabe. Multiprecision multiplication on AVR revisited. *Journal of Cryptographic Engineering*, 5(3):201–214, September 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0093-2`.

Bluhm:2015:FSI

[113] Manuel Bluhm and Shay Gueron. Fast software implementation of binary elliptic curve cryptography. *Journal of Cryptographic Engineering*, 5(3):215–226, September 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0094-1`.

Fei:2015:SBS

[114] Yunsi Fei, A. Adam Ding, Jian Lao, and Liwei Zhang. A statistics-based success rate model for DPA and CPA. *Journal of Cryptographic Engineering*, 5(4):227–243, November 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0107-0`.

Hamlet:2015:TOI

[115] Jason R. Hamlet and Robert W. Brocato. Throughput-optimized implementations of QUAD. *Journal of Cryptographic Engineering*, 5(4):245–254, November 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0109-y`.

Lerman:2015:BVD

[116] Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. The bias-variance decomposition in profiled attacks. *Journal of Cryptographic Engineering*, 5(4):255–267, November 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0106-1`.

Bongiovanni:2015:DVT

[117] Simone Bongiovanni, Francesco Centurelli, Giuseppe Scotti, and Alessandro Trifiletti. Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks. *Journal of Cryptographic Engineering*, 5(4):269–288, November 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-015-0096-z`.

Cenk:2015:SNR

[118] Murat Cenk and M. Anwar Hasan. Some new results on binary polynomial multiplication. *Journal of Cryptographic Engineering*, 5(4):289–303, November 2015. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0101-6.

Konheim:2016:ATM

[119] Alan G. Konheim. Automated teller machines: their history and authentication protocols. *Journal of Cryptographic Engineering*, 6(1):1–29, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0104-3.

Aldaya:2016:ABT

[120] Alejandro Cabrera Aldaya, Alejandro J. Cabrera Sarmiento, and Santiago Sánchez-Solano. AES T-Box tampering attack. *Journal of Cryptographic Engineering*, 6(1):31–48, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0103-4.

Ferradi:2016:WOC

[121] Houda Ferradi, Rémi Géraud, David Naccache, and Assia Tria. When organized crime applies academic results: a forensic analysis of an in-card listening device. *Journal of Cryptographic Engineering*, 6(1):49–59, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0112-3.

Bayon:2016:FME

[122] Pierre Bayon, Lilian Bossuet, Alain Aubert, and Viktor Fischer. Fault model of electromagnetic attacks targeting ring oscillator-based true random number generators. *Journal of Cryptographic Engineering*, 6(1):61–74, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0113-2.

Saarinen:2016:BAC

[123] Markku-Juhani O. Saarinen. The BRUTUS automatic cryptanalytic framework. *Journal of Cryptographic Engineering*, 6(1):75–82, April 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-015-0114-1; http://link.springer.com/content/pdf/10.1007/s13389-015-0114-1.pdf.

Guneysu:2016:ICS

[124] Tim Güneysu and Helena Handschuh. Introduction to the CHES 2015 special issue. *Journal of Cryptographic Engineering*, 6(2):83–84, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0130-9; http://link.springer.com/content/pdf/10.1007/s13389-016-0130-9.pdf.

Schneider:2016:LAM

[125] Tobias Schneider and Amir Moradi. Leakage assessment methodology. *Journal of Cryptographic Engineering*, 6(2):85–99, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.

com/article/10.1007/s13389-016-0120-y.

Schindler:2016:EEB

[126] Werner Schindler. Exclusive exponent blinding is not enough to prevent any timing attack on RSA. *Journal of Cryptographic Engineering*, 6(2): 101–119, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0124-7.

Maes:2016:SKG

[127] Roel Maes, Vincent van der Leest, Erik van der Sluis, and Frans Willems. Secure key generation from biased PUFs: extended version. *Journal of Cryptographic Engineering*, 6(2):121–137, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0125-6.

Reparaz:2016:MRL

[128] Oscar Reparaz, Sujoy Sinha Roy, Ruan de Clercq, Frederik Vercauteren, and Ingrid Verbauwhede. Masking ring-LWE. *Journal of Cryptographic Engineering*, 6(2):139–153, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0126-5.

Coisel:2016:ICD

[129] Iwen Coisel and Ignacio Sanchez. Improved cryptanalysis of the DECT standard cipher. *Journal of Cryptographic Engineering*, 6(2):155–169, June 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0127-4; http://link.springer.com/content/pdf/10.1007/s13389-016-0127-4.pdf.

Lemire:2016:FBU

[130] Daniel Lemire and Owen Kaser. Faster 64-bit universal hashing using carry-less multiplications. *Journal of Cryptographic Engineering*, 6(3):171–185, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-015-0110-5; http://link.springer.com/article/10.1007/s13389-015-0110-5.

Goundar:2016:IFA

[131] Raveen R. Goundar and Marc Joye. Inversion-free arithmetic on elliptic curves through isomorphisms. *Journal of Cryptographic Engineering*, 6(3):187–199, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0131-8; http://link.springer.com/article/10.1007/s13389-016-0131-8.

Rauzy:2016:FPS

[132] Pablo Rauzy, Sylvain Guilley, and Zakaria Najm. Formally proved security of assembly code against power analysis. *Journal of Cryptographic Engineering*, 6(3):201–216, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-015-0105-2; http://link.springer.com/article/10.1007/s13389-015-0105-2.

Robisson:2016:PFC

[133] Bruno Robisson and Hélène Le Bouder. Physical functions: the common factor of side-channel and fault attacks? *Journal of Cryptographic Engineering*, 6(3): 217–227, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-015-0111-4; http://link.springer.com/article/10.1007/s13389-015-0111-4`.

Galindo:2016:ILR

[134] David Galindo, Johann Großschädl, Zhe Liu, Praveen Kumar Vadnala, and Srinivas Vivek. Implementation of a leakage-resilient ElGamal key encapsulation mechanism. *Journal of Cryptographic Engineering*, 6 (3):229–238, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0121-x; http://link.springer.com/content/pdf/10.1007/s13389-016-0121-x.pdf`.

Ngo:2016:MTA

[135] Xuan Thuy Ngo, Zakaria Najm, Shivam Bhasin, Sylvain Guilley, and Jean-Luc Danger. Method taking into account process dispersion to detect hardware Trojan Horse by side-channel analysis. *Journal of Cryptographic Engineering*, 6(3):239–247, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0129-2; http://link.springer.com/article/10.1007/s13389-016-0129-2`.

Ganji:2016:PLA

[136] Fatemeh Ganji, Shahin Tajik, and Jean-Pierre Seifert. PAC learning of arbiter PUFs. *Journal of Cryptographic Engineering*, 6(3):249–258, September 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0119-4; http://link.springer.com/article/10.1007/s13389-016-0119-4`.

Bos:2016:SEC

[137] Joppe W. Bos, Craig Costello, Patrick Longa, and Michael Naehrig. Selecting elliptic curves for cryptography: an efficiency and security analysis. *Journal of Cryptographic Engineering*, 6(4): 259–286, November 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-015-0097-y; http://link.springer.com/article/10.1007/s13389-015-0097-y`.

Wenger:2016:HBF

[138] Erich Wenger and Paul Wolfger. Harder, better, faster, stronger: elliptic curve discrete logarithm computations on FPGAs. *Journal of Cryptographic Engineering*, 6(4):287–297, November 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-015-0108-z; http://link.springer.com/article/10.1007/s13389-015-0108-z`.

Khalid:2016:RRP

[139] Ayesha Khalid, Muhammad Hassan,

Goutam Paul, and Anupam Chattopadhyay. RunFein: a rapid prototyping framework for Feistel and SPN-based block ciphers. *Journal of Cryptographic Engineering*, 6(4):299–323, November 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0116-7`; `http://link.springer.com/article/10.1007/s13389-016-0116-7`.

Moein:2016:HAA

[140] Samer Moein, Fayez Gebali, and T. Aaron Gulliver. Hardware attacks: an algebraic approach. *Journal of Cryptographic Engineering*, 6(4):325–337, November 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0117-6`; `http://link.springer.com/article/10.1007/s13389-016-0117-6`.

Ghafar:2016:SRV

[141] Amir Hamzah Abd Ghafar and Muhammad Rezal Kamel Ariffin. SPA on Rabin variant with public key $N = p^2q$. *Journal of Cryptographic Engineering*, 6(4):339–346, November 2016. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0118-5`; `http://link.springer.com/article/10.1007/s13389-016-0118-5`.

Carbone:2017:MIA

[142] Mathieu Carbone, Yannick Teglia, Gilles R. Ducharme, and Philippe Maurine. Mutual information analysis: higher-order statistical moments, efficiency and efficacy. *Journal of Cryptographic Engineering*, 7(1):1–17, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0123-8`; `http://link.springer.com/article/10.1007/s13389-016-0123-8`.

Guilley:2017:EAP

[143] Sylvain Guilley. Editorial about PROOFS 2015. *Journal of Cryptographic Engineering*, 7(1):19–20, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0140-7`; `http://link.springer.com/content/pdf/10.1007/s13389-016-0140-7.pdf`.

Idrissi:2017:TCM

[144] Noreddine El Janati El Idrissi, Guillaume Bouffard, Jean-Louis Lanet, and Said El Hajji. Trust can be misplaced. *Journal of Cryptographic Engineering*, 7(1):21–34, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/accesspage/article/10.1007/s13389-016-0142-5`; `http://link.springer.com/article/10.1007/s13389-016-0142-5`.

Nashimoto:2017:BOA

[145] Shoei Nashimoto, Naofumi Homma, Yu ichi Hayashi, Junko Takahashi, Hitoshi Fuji, and Takafumi Aoki. Buffer overflow attack with multiple fault injection and a proven countermeasure. *Journal of Cryptographic Engineering*, 7(1):35–46, April 2017. CODEN ????

ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0136-3; http://link.springer.com/article/10.1007/s13389-016-0136-3.

Robisson:2017:SSM

[146] Bruno Robisson, Michel Agoyan, Patrick Soquet, Sébastien Le-Henaff, Franck Wajsbürt, Pirouz Bazargan-Sabet, and Guillaume Phan. Smart security management in secure devices. *Journal of Cryptographic Engineering*, 7 (1):47–61, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0143-4; http://link.springer.com/article/10.1007/s13389-016-0143-4.

Lugou:2017:STU

[147] Florian Lugou, Ludovic Apvrille, and Aurélien Francillon. SMASHUP: a toolchain for unified verification of hardware/software co-designs. *Journal of Cryptographic Engineering*, 7 (1):63–74, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0145-2; http://link.springer.com/article/10.1007/s13389-016-0145-2.

Azzi:2017:ULC

[148] Sabine Azzi, Bruno Barras, Maria Christofi, and David Vigilant. Using linear codes as a fault countermeasure for nonlinear operations: application to AES and formal verification. *Journal of Cryptographic Engineering*, 7(1):75–85, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0138-1; http://link.springer.com/article/10.1007/s13389-016-0138-1.

Sauvage:2017:MLF

[149] Laurent Sauvage, Tarik Graba, and Thibault Porteboeuf. Multi-level formal verification. *Journal of Cryptographic Engineering*, 7(1):87–95, April 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/accesspage/article/10.1007/s13389-016-0144-3; http://link.springer.com/article/10.1007/s13389-016-0144-3.

Gierlichs:2017:ICS

[150] Benedikt Gierlichs and Axel Y. Poschmann. Introduction to the CHES 2016 special issue. *Journal of Cryptographic Engineering*, 7(2): 97–98, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/content/pdf/10.1007/s13389-017-0158-5.pdf.

Yarom:2017:CTA

[151] Yuval Yarom, Daniel Genkin, and Nadia Heninger. CacheBleed: a timing attack on OpenSSL constant-time RSA. *Journal of Cryptographic Engineering*, 7 (2):99–112, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Ganji:2017:HNM

[152] Fatemeh Ganji, Shahin Tajik, Fabian Fäßler, and Jean-Pierre Seifert. Hav-

ing no mathematical model may not secure PUFs. *Journal of Cryptographic Engineering*, 7(2):113–128, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Durvaux:2017:TEL

[153] François Durvaux, François-Xavier Standaert, and Santos Merino Del Pozo. Towards easy leakage certification: extended version. *Journal of Cryptographic Engineering*, 7(2):129–147, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Boss:2017:SBS

[154] Erik Boss, Vincent Grosso, Tim Güneysu, Gregor Leander, Amir Moradi, and Tobias Schneider. Strong 8-bit Sboxes with efficient masking in hardware extended version. *Journal of Cryptographic Engineering*, 7(2): 149–165, June 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

Bottinelli:2017:CAC

[155] Paul Bottinelli and Joppe W. Bos. Computational aspects of correlation power analysis. *Journal of Cryptographic Engineering*, 7(3):167–181, September 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0122-9`.

Ordas:2017:EFI

[156] S. Ordas, L. Guillaume-Sage, and P. Maurine. Electromagnetic fault injection: the curse of flip-flops. *Journal of Cryptographic Engineering*, 7(3):183–197, September 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0128-3`.

Swierczynski:2017:IPH

[157] Pawel Swierczynski, Marc Fyrbiak, Philipp Koppe, Amir Moradi, and Christof Paar. Interdiction in practice — hardware Trojan against a high-security USB flash drive. *Journal of Cryptographic Engineering*, 7 (3):199–211, September 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0132-7`.

Mayhew:2017:OHL

[158] Matthew Mayhew and Radu Muresan. An overview of hardware-level statistical power analysis attack countermeasures. *Journal of Cryptographic Engineering*, 7(3):213–244, September 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0133-6`.

Negre:2017:ERM

[159] Christophe Negre and Thomas Plantard. Efficient regular modular exponentiation using multiplicative half-size splitting. *Journal of Cryptographic Engineering*, 7(3):245–253, September 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-016-0134-5`.

Schindler:2017:GPA

[160] Werner Schindler and Andreas Wiemers. Generic power attacks on RSA with CRT and exponent blinding: new re-

sults. *Journal of Cryptographic Engineering*, 7(4):255–272, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0146-1.

Aldaya:2017:SVB

[161] Alejandro Cabrera Aldaya, Alejandro J. Cabrera Sarmiento, and Santiago Sánchez-Solano. SPA vulnerabilities of the binary extended Euclidean algorithm. *Journal of Cryptographic Engineering*, 7(4):273–285, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0135-4.

Pasalic:2017:EIG

[162] Enes Pasalic, Anupam Chattopadhyay, and WeiGuo Zhang. Efficient implementation of generalized Maiorana–McFarland class of cryptographic functions. *Journal of Cryptographic Engineering*, 7(4):287–295, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0139-0.

Homma:2017:IPS

[163] Naofumi Homma. Introduction to the PROOFS 2016 special section. *Journal of Cryptographic Engineering*, 7(4):297–298, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0173-6; https://link.springer.com/content/pdf/10.1007/s13389-017-0173-6.pdf.

Bhattacharya:2017:FFA

[164] Sarani Bhattacharya and Debdeep Mukhopadhyay. Formal fault analysis of branch predictors: attacking countermeasures of asymmetric key ciphers. *Journal of Cryptographic Engineering*, 7(4):299–310, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0165-6.

Breier:2017:SAS

[165] Jakub Breier, Dirmanto Jap, and Shivam Bhasin. A study on analyzing side-channel resistant encoding schemes with respect to fault attacks. *Journal of Cryptographic Engineering*, 7(4):311–320, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0166-5.

Dugardin:2017:UME

[166] Margaux Dugardin, Sylvain Guilley, Martin Moreau, Zakaria Najm, and Pablo Rauzy. Using modular extension to provably protect Edwards curves against fault attacks. *Journal of Cryptographic Engineering*, 7(4):321–330, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0167-4.

Bruneau:2017:OSC

[167] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul. Optimal side-channel attacks for multivariate leakages and multiple models. *Journal of Cryptographic*

Engineering, 7(4):331–341, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0170-9.

Picek:2017:TAV

[168] Stjepan Picek, Annelie Heuser, and Sylvain Guilley. Template attack versus Bayes classifier. *Journal of Cryptographic Engineering*, 7(4):343–351, November 2017. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0172-7.

Ge:2018:SMT

[169] Qian Ge, Yuval Yarom, David Cock, and Gernot Heiser. A survey of microarchitectural timing attacks and countermeasures on contemporary hardware. *Journal of Cryptographic Engineering*, 8(1):1–27, April 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0141-6.

Chakraborti:2018:TUT

[170] Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan, and Mridul Nandi. TriviA and uTriviA: two fast and secure authenticated encryption schemes. *Journal of Cryptographic Engineering*, 8(1):29–48, April 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0137-2.

Chakraborty:2018:DED

[171] Debrup Chakraborty, Cuauhtemoc Mancillas López, and Palash Sarkar. Disk encryption: do we need to preserve length? *Journal of Cryptographic Engineering*, 8(1):49–69, April 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-016-0147-0.

Saarinen:2018:ACB

[172] Markku-Juhani O. Saarinen. Arithmetic coding and blinding countermeasures for lattice signatures. *Journal of Cryptographic Engineering*, 8(1):71–84, April 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0149-6.

Ferradi:2018:RPN

[173] Houda Ferradi, Rémi Géraud, Diana Maimut, David Naccache, and Amaury de Wargny. Regulating the pace of von Neumann correctors. *Journal of Cryptographic Engineering*, 8(1):85–91, April 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0153-x.

Fischer:2018:ICS

[174] Wieland Fischer and Naofumi Homma. Introduction to the CHES 2017 special issue. *Journal of Cryptographic Engineering*, 8(2):93–94, June 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0189-6; https://link.springer.com/content/pdf/10.1007/s13389-018-0189-6.pdf.

Chou:2018:MRT

[175] Tung Chou. McBits revisited: toward a fast constant-time code-based

KEM. *Journal of Cryptographic Engineering*, 8(2):95–107, June 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0186-9.

Gross:2018:UMA

[176] Hannes Gross and Stefan Mangard. A unified masking approach. *Journal of Cryptographic Engineering*, 8 (2):109–124, June 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0184-y; https://link.springer.com/content/pdf/10.1007/s13389-018-0184-y.pdf.

Immler:2018:YRC

[177] Vincent Immler, Robert Specht, and Florian Unterstein. Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs — extended version. *Journal of Cryptographic Engineering*, 8(2):125–139, June 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0185-x.

Hatzivasilis:2018:RLB

[178] George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers. *Journal of Cryptographic Engineering*, 8(2):141–184, June 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0160-y.

Rodriguez-Henriquez:2018:SIH

[179] Francisco Rodríguez-Henríquez and Erkay Savas. Special issue in honor of Peter Lawrence Montgomery. *Journal of Cryptographic Engineering*, 8 (3):185–187, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0168-3; https://link.springer.com/content/pdf/10.1007/s13389-017-0168-3.pdf.

Bajard:2018:MRW

[180] Jean-Claude Bajard, Julien Eynard, and Nabil Merkiche. Montgomery reduction within the context of residue number system arithmetic. *Journal of Cryptographic Engineering*, 8 (3):189–200, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0154-9.

Savas:2018:MI

[181] Erkay Savas and Çetin Kaya Koç. Montgomery inversion. *Journal of Cryptographic Engineering*, 8(3):201–210, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0161-x.

Dai:2018:SAM

[182] Wangchen Dai and Ray C. C. Cheung. Spectral arithmetic in Montgomery modular multiplication. *Journal of Cryptographic Engineering*, 8 (3):211–226, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL

http://link.springer.com/article/10.1007/s13389-017-0151-z.

Costello:2018:MCT

[183] Craig Costello and Benjamin Smith. Montgomery curves and their arithmetic. *Journal of Cryptographic Engineering*, 8(3):227–240, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0157-6.

Oliveira:2018:MLB

[184] Thomaz Oliveira, Julio López, and Francisco Rodríguez-Henríquez. The Montgomery ladder on binary elliptic curves. *Journal of Cryptographic Engineering*, 8(3):241–258, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0163-8.

Cenk:2018:KLF

[185] Murat Cenk. Karatsuba-like formulae and their associated techniques. *Journal of Cryptographic Engineering*, 8(3):259–269, September 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0155-8.

Farias:2018:CSE

[186] Luckas A. Farias, Bruno C. Albertini, and Paulo S. L. M. Barreto. A class of safe and efficient binary Edwards curves. *Journal of Cryptographic Engineering*, 8(4):271–283, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0174-5.

Jarvinen:2018:ATA

[187] Kimmo Järvinen, Sujoy Sinha Roy, and Ingrid Verbauwhede. Arithmetic of τ-adic expansions for lightweight Koblitz curve cryptography. *Journal of Cryptographic Engineering*, 8 (4):285–300, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0182-0.

Lerman:2018:TAV

[188] Liran Lerman, Romain Poussier, Olivier Markowitch, and François-Xavier Standaert. Template attacks versus machine learning revisited and the curse of dimensionality in side-channel analysis: extended version. *Journal of Cryptographic Engineering*, 8(4):301–313, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0162-9.

DeVale:2018:ADI

[189] John DeVale, Ryan Rakvic, and Kevin Rudd. Another dimension in integrated circuit trust. *Journal of Cryptographic Engineering*, 8(4):315–326, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0164-7.

Karmakar:2018:SBS

[190] Sandip Karmakar and Dipanwita Roy Chowdhury. Scan-based side channel attack on stream ciphers and its prevention. *Journal of Cryptographic Engineering*, 8(4):327–340, November 2018. CODEN ???? ISSN 2190-8508

(print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0178-1.

Skoric:2018:TDS

[191] Boris Škorić. A trivial debiasing scheme for Helper Data Systems. *Journal of Cryptographic Engineering*, 8 (4):341–349, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0183-z; https://link.springer.com/content/pdf/10.1007/s13389-018-0183-z.pdf.

Dosso:2018:EAC

[192] Yssouf Dosso, Fabien Herbaut, Nicolas Méloni, and Pascal Véron. Euclidean addition chains scalar multiplication on curves with efficient endomorphism. *Journal of Cryptographic Engineering*, 8(4):351–367, November 2018. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0190-0.

Hutchinson:2019:CMD

[193] Aaron Hutchinson and Koray Karabina. Constructing multidimensional differential addition chains and their applications. *Journal of Cryptographic Engineering*, 9(1):1–19, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0177-2.

Batina:2019:OTA

[194] Lejla Batina, Łukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall. Online template attacks. *Journal of Cryptographic Engineering*, 9(1):21–36, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0171-8; https://link.springer.com/content/pdf/10.1007/s13389-017-0171-8.pdf.

Diop:2019:TPH

[195] Ibrahima Diop, Yanis Linge, Thomas Ordas, Pierre-Yvan Liardet, and Philippe Maurine. From theory to practice: horizontal attacks on protected implementations of modular exponentiations. *Journal of Cryptographic Engineering*, 9(1):37–52, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0181-1.

Saha:2019:IDF

[196] Dhiman Saha and Dipanwita Roy Chowdhury. Internal differential fault analysis of parallelizable ciphers in the counter-mode. *Journal of Cryptographic Engineering*, 9(1):53–67, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0179-0.

Banik:2019:CCC

[197] Subhadeep Banik, Andrey Bogdanov, and Francesco Regazzoni. Compact circuits for combined AES encryption/decryption. *Journal of Cryptographic Engineering*, 9(1):69–83, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0176-3.

Konheim:2019:HFI

[198] Alan G. Konheim. Horst Feistel: the inventor of LUCIFER, the cryptographic algorithm that changed cryptology. *Journal of Cryptographic Engineering*, 9(1):85–100, April 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0198-5.

Ueno:2019:HEG

[199] Rei Ueno, Naofumi Homma, Yasuyuki Nogami, and Takafumi Aoki. Highly efficient $GF(2^8)$ inversion circuit based on hybrid GF representations. *Journal of Cryptographic Engineering*, 9(2):101–113, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0187-8.

Robert:2019:EFB

[200] Jean-Marc Robert, Christophe Negre, and Thomas Plantard. Efficient fixed-base exponentiation and scalar multiplication based on a multiplicative splitting exponent recoding. *Journal of Cryptographic Engineering*, 9(2):115–136, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0196-7.

Unterluggauer:2019:MME

[201] Thomas Unterluggauer, Mario Werner, and Stefan Mangard. MEAS: memory encryption and authentication secure against side-channel attacks. *Journal of Cryptographic Engineering*, 9 (2):137–158, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0180-2; https://link.springer.com/content/pdf/10.1007/s13389-018-0180-2.pdf.

Peccerillo:2019:PBA

[202] Biagio Peccerillo, Sandro Bartolini, and Çetin Kaya Koç. Parallel bitsliced AES through PHAST: a single-source high-performance library for multicores and GPUs. *Journal of Cryptographic Engineering*, 9(2):159–171, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-017-0175-4.

Hutter:2019:CTH

[203] Michael Hutter and Michael Tunstall. Constant-time higher-order Boolean-to-arithmetic masking. *Journal of Cryptographic Engineering*, 9(2):173–184, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0191-z.

Herbert:2019:DIL

[204] Vincent Herbert, Bhaskar Biswas, and Caroline Fontaine. Design and implementation of low-depth pairing-based homomorphic encryption scheme. *Journal of Cryptographic Engineering*, 9(2): 185–201, June 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0192-y.

Saha:2019:AFE

[205] Sayandeep Saha, Ujjawal Kumar, Debdeep Mukhopadhyay, and Pallab Dasgupta. An automated framework for

exploitable fault identification in block ciphers. *Journal of Cryptographic Engineering*, 9(3):203–219, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00203-9.

Wisiol:2019:WAL

[206] Nils Wisiol and Marian Margraf. Why attackers lose: design and security analysis of arbitrarily large XOR arbiter PUFs. *Journal of Cryptographic Engineering*, 9(3):221–230, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00204-8.

BenElOuahma:2019:SCR

[207] Inès Ben El Ouahma, Quentin L. Meunier, Karine Heydemann, and Emmanuelle Encrenaz. Side-channel robustness analysis of masked assembly codes using a symbolic approach. *Journal of Cryptographic Engineering*, 9(3):231–242, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00205-7.

Baumann:2019:VSL

[208] Christoph Baumann, Oliver Schwarz, and Mads Dam. On the verification of system-level information flow properties for virtualized execution platforms. *Journal of Cryptographic Engineering*, 9(3):243–261, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00216-4; https://link.springer.com/content/pdf/10.1007/s13389-019-00216-4.pdf.

Das:2019:AGH

[209] Poulami Das, Debapriya Basu Roy, and Debdeep Mukhopadhyay. Automatic generation of HCCA-resistant scalar multiplication algorithm by proper sequencing of field multiplier operands. *Journal of Cryptographic Engineering*, 9(3):263–275, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00219-1.

Geraud:2019:MRN

[210] Rémi Géraud and David Naccache. Mixed-radix Naccache–Stern encryption. *Journal of Cryptographic Engineering*, 9(3):277–282, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0188-7.

Dinu:2019:TLB

[211] Daniel Dinu, Yann Le Corre, Dmitry Khovratovich, Léo Perrin, Johann Großschädl, and Alex Biryukov. Triathlon of lightweight block ciphers for the Internet of Things. *Journal of Cryptographic Engineering*, 9(3):283–302, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-0193-x.

Carlet:2019:PDS

[212] Claude Carlet, Abderrahman Daif, Sylvain Guilley, and Cédric Tavernier. Polynomial direct sum masking to protect against both SCA and FIA.

Journal of Cryptographic Engineering, 9(3):303–312, September 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-018-0194-9`.

Kawamura:2019:RMR

[213] Shinichi Kawamura, Yuichi Komano, Hideo Shimizu, and Tomoko Yonemura. RNS Montgomery reduction algorithms using quadratic residuosity. *Journal of Cryptographic Engineering*, 9(4):313–331, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-018-0195-8`; `https://link.springer.com/content/pdf/10.1007/s13389-018-0195-8.pdf`.

Saldamli:2019:UMM

[214] Gokay Saldamli and Yoo-Jin Baek. Uniform Montgomery multiplier. *Journal of Cryptographic Engineering*, 9(4):333–339, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-019-00213-7`.

Drucker:2019:TSO

[215] Nir Drucker and Shay Gueron. A toolbox for software optimization of QC–MDPC code-based cryptosystems. *Journal of Cryptographic Engineering*, 9(4):341–357, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-018-00200-4`.

Banegas:2019:NCI

[216] Gustavo Banegas, Ricardo Custódio, and Daniel Panario. A new class of irreducible pentanomials for polynomial-based multipliers in binary fields. *Journal of Cryptographic Engineering*, 9(4):359–373, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-018-0197-6`; `https://link.springer.com/content/pdf/10.1007/s13389-018-0197-6.pdf`.

Cianfriglia:2019:KAR

[217] Marco Cianfriglia, Stefano Guarino, Massimo Bernaschi, Flavio Lombardi, and Marco Pedicini. Kite attack: reshaping the cube attack for a flexible GPU-based maxterm search. *Journal of Cryptographic Engineering*, 9(4):375–392, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-019-00217-3`.

Levina:2019:PMS

[218] Alla Levina, Roman Mostovoi, Daria Sleptsova, and Lavrentii Tcvetkov. Physical model of sensitive data leakage from PC-based cryptographic systems. *Journal of Cryptographic Engineering*, 9(4):393–400, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-019-00215-5`.

Wu:2019:FUE

[219] Tao Wu and Ruomei Wang. Fast unified elliptic curve point multiplication for NIST prime curves on FP-

GAs. *Journal of Cryptographic Engineering*, 9(4):401–410, November 2019. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00211-9.

Jauvart:2020:ISC

[220] Damien Jauvart, Nadia El Mrabet, Jacques J. A. Fournier, and Louis Goubin. Improving side-channel attacks against pairing-based cryptography. *Journal of Cryptographic Engineering*, 10(1):1–16, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-00201-3.

Barthe:2020:IPM

[221] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, François-Xavier Standaert, and Pierre-Yves Strub. Improved parallel mask refreshing algorithms: generic solutions with parametrized non-interference and automated optimizations. *Journal of Cryptographic Engineering*, 10(1):17–26, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-018-00202-2.

Abarzua:2020:SVA

[222] Rodrigo Abarzúa, Santi Martínez, Valeria Mendoza, and Nicolas Thériault. Same value analysis on Edwards curves. *Journal of Cryptographic Engineering*, 10(1):27–48, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00206-6.

Goubin:2020:HRS

[223] Louis Goubin, Pascal Paillier, Matthieu Rivain, and Junwei Wang. How to reveal the secrets of an obscure white-box implementation. *Journal of Cryptographic Engineering*, 10(1):49–66, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00207-5.

Willers:2020:FDC

[224] Oliver Willers, Christopher Huth, Jorge Guajardo, Helmut Seidel, and Peter Deutsch. On the feasibility of deriving cryptographic keys from MEMS sensors. *Journal of Cryptographic Engineering*, 10(1):67–83, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00208-4.

Zhou:2020:DLM

[225] Yuanyuan Zhou and François-Xavier Standaert. Deep learning mitigates but does not annihilate the need of aligned traces and a generalized ResNet model for side-channel attacks. *Journal of Cryptographic Engineering*, 10(1):85–95, April 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00209-3.

Bos:2020:FMA

[226] Joppe W. Bos and Simon J. Friedberger. Faster modular arithmetic for isogeny-based crypto on embedded devices. *Journal of Cryptographic Engineering*, 10(2):97–109, June 2020. CODEN ???? ISSN 2190-8508

(print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00214-6.

Didier:2020:EMO

[227] Laurent-Stéphane Didier, Fangan-Yssouf Dosso, and Pascal Véron. Efficient modular operations using the adapted modular number system. *Journal of Cryptographic Engineering*, 10(2):111–133, June 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00221-7.

Hettwer:2020:AML

[228] Benjamin Hettwer, Stefan Gehrer, and Tim Güneysu. Applications of machine learning techniques in side-channel attacks: a survey. *Journal of Cryptographic Engineering*, 10(2):135–162, June 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00212-8.

Benadjila:2020:DLS

[229] Ryad Benadjila, Emmanuel Prouff, Rémi Strullu, Eleonora Cagli, and Cécile Dumas. Deep learning for side-channel analysis and introduction to ASCAD database. *Journal of Cryptographic Engineering*, 10(2):163–188, June 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00220-8.

Orumiehchiha:2020:DFA

[230] Mohammad Ali Orumiehchiha, Saeed Rostami, Elham Shakour, and Josef Pieprzyk. A differential fault attack on the WG family of stream ciphers. *Journal of Cryptographic Engineering*, 10(2):189–195, June 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00222-x.

Piccoli:2020:PMB

[231] Alessandro De Piccoli, Andrea Visconti, and Ottavio Giulio Rizzo. Polynomial multiplication over binary finite fields: new upper bounds. *Journal of Cryptographic Engineering*, 10(3):197–210, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00210-w.

Cruz:2020:ESS

[232] Rafael J. Cruz, Antonio Guimarães, and Diego F. Aranha. Efficient and secure software implementations of Fantomas. *Journal of Cryptographic Engineering*, 10(3):211–228, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-019-00218-2.

Hiller:2020:REC

[233] Matthias Hiller, Ludwig Kürzinger, and Georg Sigl. Review of error correction for PUFs and evaluation on state-of-the-art FPGAs. *Journal of Cryptographic Engineering*, 10(3):229–247, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00223-w; https:

//link.springer.com/content/pdf/10.1007/s13389-020-00223-w.pdf.

Schoinianakis:2020:RAS

[234] Dimitrios Schoinianakis. Residue arithmetic systems in cryptography: a survey on modern security applications. *Journal of Cryptographic Engineering*, 10(3):249–267, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00231-w.

Wiemers:2020:RSR

[235] Andreas Wiemers. A remark on a success rate model for side-channel attack analysis. *Journal of Cryptographic Engineering*, 10(3):269–274, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00235-6; https://link.springer.com/content/pdf/10.1007/s13389-020-00235-6.pdf.

Richter:2020:TAN

[236] Bastian Richter and Amir Moradi. Template attacks on nano-scale CMOS devices. *Journal of Cryptographic Engineering*, 10(3):275–285, September 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00225-8; https://link.springer.com/content/pdf/10.1007/s13389-020-00225-8.pdf.

Batina:2020:PE

[237] Lejla Batina and Nele Mentens. PROOFS 2018 editorial. *Journal of Cryptographic Engineering*, 10(4):287, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00248-1; https://link.springer.com/content/pdf/10.1007/s13389-020-00248-1.pdf.

Alam:2020:IAH

[238] Manaar Alam, Debdeep Mukhopadhyay, Sai Praveen Kadiyala, Siew-Kei Lam, and Thambipillai Srikanthan. Improving accuracy of HPC-based malware classification for embedded platforms using gradient descent optimization. *Journal of Cryptographic Engineering*, 10(4):289–303, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00232-9.

Sijacic:2020:TEA

[239] Danilo Sijačić, Josep Balasch, Bohan Yang, Santosh Ghosh, and Ingrid Verbauwhede. Towards efficient and automated side-channel evaluations at design time. *Journal of Cryptographic Engineering*, 10(4):305–319, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00233-8.

Gay:2020:ECS

[240] Mael Gay, Batya Karp, Osnat Keren, and Ilia Polian. Error control scheme for malicious and natural faults in cryptographic modules. *Journal of Cryptographic Engineering*, 10(4):321–336, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.

1007/s13389-020-00234-7; https://link.springer.com/content/pdf/10.1007/s13389-020-00234-7.pdf.

Ouladj:2020:PTA

[241] Maamar Ouladj, Nadia El Mrabet, Sylvain Guilley, Philippe Guillot, and Gilles Millérioux. On the power of template attacks in highly multivariate context. *Journal of Cryptographic Engineering*, 10(4):337–354, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00239-2.

Baksi:2020:IIC

[242] Anubhab Baksi, Dhiman Saha, and Sumanta Sarkar. To infect or not to infect: a critical analysis of infective countermeasures in fault attacks. *Journal of Cryptographic Engineering*, 10(4):355–374, November 2020. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00224-9.

Yeo:2021:IAA

[243] Sze Ling Yeo, Duc-Phong Le, and Khoongming Khoo. Improved algebraic attacks on lightweight block ciphers. *Journal of Cryptographic Engineering*, 11(1):1–19, April 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00237-4.

Resende:2021:FUP

[244] Amanda Cristina Davi Resende and Diego de Freitas Aranha. Faster unbalanced Private Set Intersection in the semi-honest setting. *Journal of Cryptographic Engineering*, 11(1):21–38, April 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00242-7.

Bronchain:2021:RRT

[245] Olivier Bronchain, Tobias Schneider, and François-Xavier Standaert. Reducing risks through simplicity: high side-channel security for lazy engineers. *Journal of Cryptographic Engineering*, 11(1):39–55, April 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00241-8.

Pereira:2021:OPA

[246] Geovandro Pereira, Javad Doliskani, and David Jao. x-only point addition formula and faster compressed SIKE. *Journal of Cryptographic Engineering*, 11(1):57–69, April 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00245-4.

Abarzua:2021:SPS

[247] Rodrigo Abarzúa, Claudio Valencia, and Julio López. Survey on performance and security problems of countermeasures for passive side-channel attacks on ECC. *Journal of Cryptographic Engineering*, 11(1):71–102, April 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00257-8.

Heydemann:2021:EAP

[248] Karine Heydemann and Letitia Li. Editorial about PROOFS 2019. *Journal of Cryptographic Engineering*, 11 (2):103–104, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00236-5; https://link.springer.com/content/pdf/10.1007/s13389-020-00236-5.pdf. See correction [256].

Ganji:2021:RPC

[249] Fatemeh Ganji, Shahin Tajik, Pascal Stauss, Jean-Pierre Seifert, Mark Tehranipoor, and Domenic Forte. Rock'n'roll PUFs: crafting provably secure PUFs from less secure ones (extended version). *Journal of Cryptographic Engineering*, 11(2):105–118, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00226-7.

Cheng:2021:DFI

[250] Wei Cheng, Claude Carlet, Kouassi Goli, Jean-Luc Danger, and Sylvain Guilley. Detecting faults in inner product masking scheme. *Journal of Cryptographic Engineering*, 11(2): 119–133, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00227-6.

Perianin:2021:EEA

[251] Thomas Perianin, Sebastien Carré, Victor Dyseryn, Adrien Facon, and Sylvain Guilley. End-to-end automated cache-timing attack driven by machine learning. *Journal of Cryptographic Engineering*, 11(2):135–146, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00228-5.

Keren:2021:IRC

[252] Osnat Keren and Ilia Polian. IPM-RED: combining higher-order masking with robust error detection. *Journal of Cryptographic Engineering*, 11 (2):147–160, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00229-4; https://link.springer.com/content/pdf/10.1007/s13389-020-00229-4.pdf.

Ueno:2021:MCS

[253] Rei Ueno, Junko Takahashi, Yu ichi Hayashi, and Naofumi Homma. A method for constructing sliding windows leak from noisy cache timing information. *Journal of Cryptographic Engineering*, 11(2):161–170, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00230-x; https://link.springer.com/content/pdf/10.1007/s13389-020-00230-x.pdf.

Kamel:2021:SCA

[254] Dina Kamel, Davide Bellizia, Olivier Bronchain, and François-Xavier Standaert. Side-channel analysis of a learning parity with physical noise processor. *Journal of Cryptographic Engineering*, 11(2):171–179, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL

http://link.springer.com/article/10.1007/s13389-020-00238-3.

Jacobson:2021:RWK

[255] Michael John Jacobson, Jr. and Prabhat Kushwaha. Removable weak keys for discrete logarithm-based cryptography. *Journal of Cryptographic Engineering*, 11(2):181–195, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00250-7.

Heydemann:2021:CEA

[256] Karine Heydemann and Letitia Li. Correction to: Editorial about PROOFS 2019. *Journal of Cryptographic Engineering*, 11(2):197, June 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00266-7; https://link.springer.com/content/pdf/10.1007/s13389-021-00266-7.pdf. See [248].

Chang:2021:ASI

[257] Chip-Hong Chang, Daniel E. Holcomb, Ulrich Rührmair, and Patrick Schaumont. The ASHES 2019 special issue at JCEN. *Journal of Cryptographic Engineering*, 11(3):199–200, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00270-x; https://link.springer.com/content/pdf/10.1007/s13389-021-00270-x.pdf.

Shiozaki:2021:SEA

[258] Mitsuru Shiozaki and Takeshi Fujino. Simple electromagnetic analysis attack based on geometric leak on ASIC implementation of ring-oscillator PUF. *Journal of Cryptographic Engineering*, 11(3):201–212, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00240-9.

Zhang:2021:NTG

[259] Yuqiao Zhang, Ayush Jain, Pinchen Cui, Ziqi Zhou, and Ujjwal Guin. A novel topology-guided attack and its countermeasure towards secure logic locking. *Journal of Cryptographic Engineering*, 11(3):213–226, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00243-6.

Gu:2021:LSC

[260] Chongyan Gu, Chip-Hong Chang, Weiqiang Liu, Neil Hanley, Jack Miskelly, and Máire O'Neill. A large-scale comprehensive evaluation of single-slice ring oscillator and PicoPUF bit cells on 28-nm Xilinx FPGAs. *Journal of Cryptographic Engineering*, 11 (3):227–238, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00244-5; https://link.springer.com/content/pdf/10.1007/s13389-020-00244-5.pdf.

Bandara:2021:ACD

[261] Sahan Bandara and Michel A. Kinsy. Adaptive caches as a defense mechanism against cache side-channel attacks. *Journal of Cryptographic Engineering*, 11(3):239–255, September 2021. CODEN ???? ISSN 2190-8508

(print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-020-00246-3`.

Unterstein:2021:SSU

[262] Florian Unterstein, Nisha Jacob, Neil Hanley, Chongyan Gu, and Johann Heyszl. SCA secure and updatable crypto engines for FPGA SoC bitstream decryption: extended version. *Journal of Cryptographic Engineering*, 11 (3):257–272, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-020-00247-2`; `https://link.springer.com/content/pdf/10.1007/s13389-020-00247-2.pdf`.

Ramezanpour:2021:FIM

[263] Keyvan Ramezanpour, Paul Ampadu, and William Diehl. Fault intensity map analysis with neural network key distinguisher. *Journal of Cryptographic Engineering*, 11(3):273–288, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-020-00249-0`.

Nashimoto:2021:LCD

[264] Shoei Nashimoto, Daisuke Suzuki, Noriyuki Miura, Tatsuya Machida, Kohei Matsuda, and Makoto Nagata. Low-cost distance-spoofing attack on FMCW radar and its feasibility study on countermeasure. *Journal of Cryptographic Engineering*, 11(3):289–298, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-020-00252-5`.

Azriel:2021:SAM

[265] Leonid Azriel, Julian Speith, Nils Albartus, Ran Ginosar, Avi Mendelson, and Christof Paar. A survey of algorithmic methods in IC reverse engineering. *Journal of Cryptographic Engineering*, 11(3):299–315, September 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-021-00268-5`.

Howe:2021:EPI

[266] James Howe, Marco Martinoli, Elisabeth Oswald, and Francesco Regazzoni. Exploring parallelism to improve the performance of FrodoKEM in hardware. *Journal of Cryptographic Engineering*, 11(4):317–327, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-021-00258-7`; `https://link.springer.com/content/pdf/10.1007/s13389-021-00258-7.pdf`.

Perin:2021:ICS

[267] Lucas Pandolfo Perin, Gustavo Zambonin, Ricardo Custódio, Lucia Moura, and Daniel Panario. Improved constant-sum encodings for hash-based signatures. *Journal of Cryptographic Engineering*, 11(4):329–351, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `http://link.springer.com/article/10.1007/s13389-021-00264-9`.

Trouchkine:2021:EFI

[268] Thomas Trouchkine, Sébanjila Kevin Bukasa, Mathieu Escouteloup, Ronan Lashermes, and Guillaume Bouffard. Electromagnetic fault injec-

tion against a complex CPU, toward new micro-architectural fault models. *Journal of Cryptographic Engineering*, 11(4):353–367, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00259-6.

Mittmann:2021:TAL

[269] Johannes Mittmann and Werner Schindler. Timing attacks and local timing attacks against Barrett's modular multiplication algorithm. *Journal of Cryptographic Engineering*, 11(4):369–397, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-020-00254-3; https://link.springer.com/content/pdf/10.1007/s13389-020-00254-3.pdf.

Bajard:2021:MFP

[270] Jean Claude Bajard and Sylvain Duquesne. Montgomery-friendly primes and applications to cryptography. *Journal of Cryptographic Engineering*, 11(4):399–415, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00260-z.

Lombardia:2021:SSL

[271] Sergio Roldán Lombardía, Fatih Balli, and Subhadeep Banik. Six shades lighter: a bit-serial implementation of the AES family. *Journal of Cryptographic Engineering*, 11(4):417–439, November 2021. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL http://link.springer.com/article/10.1007/s13389-021-00265-8; https://link.springer.com/content/pdf/10.1007/s13389-021-00265-8.pdf.

Molteni:2022:RCR

[272] Maria Chiara Molteni and Vittorio Zaccaria. A relation calculus for reasoning about t-probing security. *Journal of Cryptographic Engineering*, 12(1):1–14, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00286-x.

Bozilov:2022:OTI

[273] Dusan Bozilov, Miroslav Knezević, and Ventzislav Nikov. Optimized threshold implementations: securing cryptographic accelerators for low-energy and low-latency applications. *Journal of Cryptographic Engineering*, 12(1):15–51, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00276-5.

Caforio:2022:MSV

[274] Andrea Caforio, Fatih Balli, and Subhadeep Banik. Melting SNOW-V: improved lightweight architectures. *Journal of Cryptographic Engineering*, 12(1):53–73, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-020-00251-6.

Ouladj:2022:SAP

[275] Maamar Ouladj, Sylvain Guilley, and Farid Mokrane. Spectral approach

to process the (multivariate) high-order template attack against any masking scheme. *Journal of Cryptographic Engineering*, 12(1):75–93, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-020-00253-4.

Buhrow:2022:PMM

[276] Benjamin Buhrow, Barry Gilbert, and Clifton Haider. Parallel modular multiplication using 512-bit advanced vector instructions. *Journal of Cryptographic Engineering*, 12(1):95–105, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00256-9.

Nath:2022:SET

[277] Kaushik Nath and Palash Sarkar. Security and efficiency trade-offs for elliptic curve Diffie–Hellman at the 128-bit and 224-bit security levels. *Journal of Cryptographic Engineering*, 12(1):107–121, April 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00261-y.

Brunetta:2022:MCD

[278] Carlo Brunetta and Pablo Picazo-Sanchez. Modelling cryptographic distinguishers using machine learning. *Journal of Cryptographic Engineering*, 12(2):123–135, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00262-x.

Winderickx:2022:DEA

[279] Jori Winderickx, An Braeken, and Nele Mentens. In-depth energy analysis of security algorithms and protocols for the Internet of Things. *Journal of Cryptographic Engineering*, 12(2):137–149, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00274-7.

David:2022:REB

[280] Liron David and Avishai Wool. Rank estimation with bounded error via exponential sampling. *Journal of Cryptographic Engineering*, 12(2):151–168, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00269-4.

Le:2022:IFA

[281] Duc-Phong Le, Rongxing Lu, and Ali A. Ghorbani. Improved fault analysis on SIMECK ciphers. *Journal of Cryptographic Engineering*, 12(2):169–180, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00263-w.

Gross:2022:BTM

[282] Mathieu Gross, Nisha Jacob, and Georg Sigl. Breaking TrustZone memory isolation and secure boot through malicious hardware on a modern FPGA-SoC. *Journal of Cryptographic Engineering*, 12(2):181–196, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic).

URL https://link.springer.com/article/10.1007/s13389-021-00273-8.

Liu:2022:CTA

[283] Fanghui Liu, Waldemar Cruz, and Laurent Michel. A comprehensive tolerant algebraic side-channel attack over modern ciphers using constraint programming. *Journal of Cryptographic Engineering*, 12(2):197–228, June 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00280-9.

Engels:2022:CVR

[284] Susanne Engels, Max Hoffmann, and Christof Paar. A critical view on the real-world security of logic locking. *Journal of Cryptographic Engineering*, 12(3):229–244, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00294-x.

Dutertre:2022:PPF

[285] Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, and Assia Tria. Photonic power firewalls. *Journal of Cryptographic Engineering*, 12(3):245–254, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00291-0.

DiMauro:2022:DIN

[286] Juan Di Mauro, Eduardo Salazar, and Hugo D. Scolnik. Design and implementation of a novel cryptographically secure pseudorandom number generator. *Journal of Cryptographic Engineering*, 12(3):255–265, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00297-8.

Chowdhury:2022:PSP

[287] Sreeja Chowdhury, Ana Covic, Rabin Yu Acharya, Spencer Dupee, Fatemeh Ganji, and Domenic Forte. Physical security in the post-quantum era. *Journal of Cryptographic Engineering*, 12(3):267–303, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00255-w.

Mandal:2022:SNM

[288] Kalikinkar Mandal, Dhiman Saha, Sumanta Sarkar, and Yosuke Todo. Sycon: a new milestone in designing ASCON-like permutations. *Journal of Cryptographic Engineering*, 12(3):305–327, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00272-9.

Yeniaras:2022:FCT

[289] Esra Yeniaras and Murat Cenk. Faster characteristic three polynomial multiplication and its application to NTRU prime decapsulation. *Journal of Cryptographic Engineering*, 12(3):329–348, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.

com/article/10.1007/s13389-021-00282-7.

Chavez-Saab:2022:SCS

[290] Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12(3):349–368, September 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00271-w.

Chang:2022:ASI

[291] Chip-Hong Chang, Stefan Katzenbeisser, Ulrich Rührmair, and Patrick Schaumont. The ASHES 2020 special issue at JCEN. *Journal of Cryptographic Engineering*, 12(4):369–370, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00300-2.

Saarinen:2022:DRV

[292] Markku-Juhani O. Saarinen, G. Richard Newell, and Ben Marshall. Development of the RISC-V entropy source interface. *Journal of Cryptographic Engineering*, 12(4):371–386, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00275-6.

Ruhrmair:2022:SFS

[293] Ulrich Rührmair. Secret-free security: a survey and tutorial. *Journal of Cryptographic Engineering*, 12(4):387–412, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00283-6.

Jin:2022:PAC

[294] Chenglu Jin, Wayne Burleson, Marten van Dijk, and Ulrich Rührmair. Programmable access-controlled and generic erasable PUF design and its applications. *Journal of Cryptographic Engineering*, 12(4):413–432, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00284-z.

Jana:2022:DFA

[295] Amit Jana, Anirban Nath, Goutam Paul, and Dhiman Saha. Differential fault analysis of NORX using variants of coupon collector problem. *Journal of Cryptographic Engineering*, 12(4):433–459, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00285-y.

Fustos:2022:FLS

[296] Jacob Fustos, Michael Bechtel, and Heechul Yun. A framework for leaking secrets to past instructions. *Journal of Cryptographic Engineering*, 12(4): 461–473, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00289-8.

Kundu:2022:FAP

[297] Anup Kumar Kundu, Aikata, Banashri Karmakar, and Dhiman Saha. Fault analysis of the PRINCE family of lightweight ciphers. *Journal of Cryptographic Engineering*, 12(4):475–494, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00290-1.

Mukherjee:2022:CSP

[298] Rijoy Mukherjee, Sree Ranjani Rajendran, and Rajat Subhra Chakraborty. A comprehensive survey of physical and logic testing techniques for Hardware Trojan detection and prevention. *Journal of Cryptographic Engineering*, 12(4):495–522, November 2022. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00295-w.

Wiemers:2023:IRS

[299] Andreas Wiemers and Johannes Mittmann. Improving recent side-channel attacks against the DES key schedule. *Journal of Cryptographic Engineering*, 13 (1):1–17, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00279-2.

Cicek:2023:NRW

[300] Ihsan Cicek and Ahmad Al Khas. A new read-write collision-based SRAM PUF implemented on Xilinx FPGAs. *Journal of Cryptographic Engineering*, 13(1):19–36, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00281-8.

Robert:2023:FMM

[301] Jean-Marc Robert and Pascal Véron. Faster multiplication over $F_2[X]$ using AVX512 instruction set and VPCLMULQDQ instruction. *Journal of Cryptographic Engineering*, 13(1):37–55, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-021-00278-3.

Attias:2023:RMM

[302] Vidal Attias, Luigi Vigneri, and Vassil Dimitrov. Rethinking modular multi-exponentiation in real-world applications. *Journal of Cryptographic Engineering*, 13(1):57–70, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00287-w.

Giron:2023:PQH

[303] Alexandre Augusto Giron, Ricardo Custódio, and Francisco Rodríguez-Henríquez. Post-quantum hybrid key exchange: a systematic mapping study. *Journal of Cryptographic Engineering*, 13(1):71–88, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00288-9.

Adj:2023:KBS

[304] Gora Adj, Jesús-Javier Chi-Domínguez, and Francisco Rodríguez-Henríquez. Karatsuba-based square-root Vélu's formulas applied to two isogeny-based protocols. *Journal of Cryptographic Engineering*, 13(1):89–106, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00293-y.

Nadikuda:2023:LAT

[305] Pradeep Kumar Goud Nadikuda and Lakshmi Boppana. Low area-time complexity point multiplication architecture for ECC over GF(2^m) using polynomial basis. *Journal of Cryptographic Engineering*, 13(1):107–123, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00302-0.

Koshelev:2023:SMT

[306] Dmitrii Koshelev. Subgroup membership testing on elliptic curves via the Tate pairing. *Journal of Cryptographic Engineering*, 13(1):125–128, April 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00296-9. See correction [338].

Masure:2023:SCA

[307] Loïc Masure and Rémi Strullu. Side-channel analysis against ANSSI's protected AES implementation on ARM: end-to-end attacks with multi-task learning. *Journal of Cryptographic Engineering*, 13(2):129–147, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00311-7.

Werner:2023:EEA

[308] Vincent Werner, Laurent Maingault, and Marie-Laure Potet. An end-to-end approach to identify and exploit multi-fault injection vulnerabilities on microcontrollers. *Journal of Cryptographic Engineering*, 13(2):149–165, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00292-z.

Peng:2023:SNP

[309] Bo-Yuan Peng, Adrian Marotzke, Ming-Han Tsai, Bo-Yin Yang, and Ho-Lin Chen. Streamlined NTRU prime on FPGA. *Journal of Cryptographic Engineering*, 13(2):167–186, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00303-z.

Debnath:2023:MIM

[310] Sumit Kumar Debnath, Sihem Mesnager, Vikas Srivastava, Saibal Kumar Pal, and Nibedita Kundu. Mul-IBS: a multivariate identity-based signature scheme compatible with IoT-based NDN architecture. *Journal of Cryptographic Engineering*, 13(2):187–199, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/

article/10.1007/s13389-022-00308-8.

Joshi:2023:SSP

[311] Priyanka Joshi and Bodhisatwa Mazumdar. SPSA: Semi-permanent stuck-at fault analysis of AES Rijndael SBox. *Journal of Cryptographic Engineering*, 13(2):201–222, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00301-1.

Cui:2023:CEL

[312] Yaxin Cui, Hong Xu, Lin Tan, Huajin Chen, and Wenfeng Qi. Construction of equivalent linear trails and multiple linear attack on reduced-round GIFT-64. *Journal of Cryptographic Engineering*, 13(2):223–234, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00298-7.

Luengo:2023:STS

[313] Elena Almaraz Luengo, Bittor Alaña Olivares, Luis Javier García Villalba, Julio Hernandez-Castro, and Darren Hurley-Smith. StringENT test suite: ENT battery revisited for efficient P value computation. *Journal of Cryptographic Engineering*, 13(2):235–249, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00313-5.

Koseki:2023:HES

[314] Ryusuke Koseki, Akira Ito, Rei Ueno, Mehdi Tibouchi, and Naofumi Homma. Homomorphic encryption for stochastic computing. *Journal of Cryptographic Engineering*, 13(2):251–263, June 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00299-6.

Salam:2023:DFA

[315] Iftekhar Salam, Wei-Chuen Yau, Raphaël C.-W. Phan, and Josef Pieprzyk. Differential fault attacks on the lightweight authenticated encryption algorithm CLX-128. *Journal of Cryptographic Engineering*, 13(3):265–281, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00326-0.

LeGrow:2023:FMF

[316] Jason T. LeGrow. A faster method for fault attack resistance in static/ephemeral CSIDH. *Journal of Cryptographic Engineering*, 13(3):283–294, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00318-0.

Alves:2023:PHT

[317] Pedro Geraldo M. R. Alves, Jheyne N. Ortiz, and Diego F. Aranha. Performance of hierarchical transforms in homomorphic encryption: a case study on logistic regression inference. *Journal of Cryptographic Engineering*, 13(3):295–310, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/

article/10.1007/s13389-023-00325-1.

Kerkhof:2023:NGL

[318] Maikel Kerkhof, Lichao Wu, Guilherme Perin, and Stjepan Picek. No (good) loss no gain: systematic evaluation of loss functions in deep learning-based side-channel analysis. *Journal of Cryptographic Engineering*, 13(3):311–324, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00320-6.

Salomon:2023:MLP

[319] Dor Salomon and Itamar Levi. MaskSIMD-lib: on the performance gap of a generic C optimized assembly and wide vector extensions for masked software with an Ascon-*p* test case. *Journal of Cryptographic Engineering*, 13(3):325–342, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00322-4.

Arshad:2023:ABE

[320] Hamed Arshad, Pablo Picazo-Sanchez, Christian Johansen, and Gerardo Schneider. Attribute-based encryption with enforceable obligations. *Journal of Cryptographic Engineering*, 13(3):343–371, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00317-1.

Bajard:2023:FVP

[321] Jean-Claude Bajard, Kazuhide Fukushima, Thomas Plantard, and Arnaud Sipasseuth. Fast verification and public key storage optimization for unstructured lattice-based signatures. *Journal of Cryptographic Engineering*, 13(3):373–388, September 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00309-1.

Chang:2023:ASI

[322] Chip-Hong Chang, Stefan Katzenbeisser, Debdeep Mukhopadhyay, and Ulrich Rührmair. The ASHES 2021 special issue at JCEN. *Journal of Cryptographic Engineering*, 13(4):389–390, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00338-w.

Deutschbein:2023:IAI

[323] Calvin Deutschbein, Andres Meza, Francesco Restuccia, Ryan Kastner, and Cynthia Sturton. Isadora: automated information-flow property generation for hardware security verification. *Journal of Cryptographic Engineering*, 13(4):391–407, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00306-w.

Vasselle:2023:SDA

[324] Aurélien Vasselle, Hugues Thiebeauld, and Philippe Maurine. Spatial dependency analysis to extract information

from side-channel mixtures: extended version. *Journal of Cryptographic Engineering*, 13(4):409–425, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-022-00307-9.

Kuroda:2023:PAN

[325] Kunihiro Kuroda, Yuta Fukuda, Kota Yoshida, and Takeshi Fujino. Practical aspects on non-profiled deep-learning side-channel attacks against AES software implementation with two types of masking countermeasures including RSM. *Journal of Cryptographic Engineering*, 13(4):427–442, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00312-6.

Ngo:2023:SCA

[326] Kalle Ngo, Elena Dubrova, and Thomas Johansson. A side-channel attack on a masked and shuffled software implementation of Saber. *Journal of Cryptographic Engineering*, 13(4):443–460, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00315-3.

Imran:2023:HSS

[327] Malik Imran, Felipe Almeida, Andrea Basso, Sujoy Sinha Roy, and Samuel Pagliarini. High-speed SABER key encapsulation mechanism in 65nm CMOS. *Journal of Cryptographic Engineering*, 13(4):461–471, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00316-2.

Komissarov:2023:SAA

[328] Rony Komissarov, Sharon Vaisman, and Avishai Wool. Spoofing attacks against vehicular FMCW radar. *Journal of Cryptographic Engineering*, 13(4):473–484, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00321-5.

Krachenfels:2023:TAD

[329] Thilo Krachenfels, Jean-Pierre Seifert, and Shahin Tajik. Trojan awakener: detecting dormant malicious hardware using laser logic state imaging (extended version). *Journal of Cryptographic Engineering*, 13(4):485–499, November 2023. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00323-3.

Oberhansl:2024:UIS

[330] Felix Oberhansl, Tim Fritzmann, Thomas Pöppelmann, Debapriya Basu Roy, and Georg Sigl. Uniform instruction set extensions for multiplications in contemporary and post-quantum cryptography. *Journal of Cryptographic Engineering*, 14(1):1–18, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL https://link.springer.com/article/10.1007/s13389-023-00332-2.

Kumar:2024:RNC

[331] Satyam Kumar, Sandip Kumar Mondal, Santanu Sarkar, Takanori Isobe, Anubhab Baksi, and Avishek Adhikari. Restricted near collision attack on Plantlet. *Journal of Cryptographic Engineering*, 14(1):19–34, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00336-y`.

Ribeiro:2024:SPQ

[332] Leonardo A. D. S. Ribeiro, José Paulo da Silva Lima, Ruy J. G. B. de Queiroz, Amirton B. Chagas, José R. R. Junior, Jonysberg P. Quintino, Fabio Q. B. da Silva, and André L. M. Santos. SABER post-quantum key encapsulation mechanism (KEM): evaluating performance in ARM and x64 architectures. *Journal of Cryptographic Engineering*, 14(1):35–41, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00337-x`.

Cai:2024:ENA

[333] Shiping Cai, Zhi Hu, Zheng-An Yao, and Chang-An Zhao. The elliptic net algorithm revisited. *Journal of Cryptographic Engineering*, 14(1):43–55, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-022-00304-y`.

Shao:2024:DSV

[334] Cuiping Shao, Dongyan Zhao, Huiyun Li, Song Cheng, Shunxian Gao, and Liuqing Yang. Detection of security vulnerabilities in cryptographic ICs against fault injection attacks based on compressed sensing and basis pursuit. *Journal of Cryptographic Engineering*, 14(1):57–70, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00324-2`.

Marchiori:2024:PRF

[335] Dúnia Marchiori, Ricardo Custódio, Daniel Panario, and Lucia Moura. Probabilistic root finding in code-based cryptography. *Journal of Cryptographic Engineering*, 14(1):71–85, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00329-x`.

Gurler:2024:CGL

[336] Elif Ozbay Gurler and Huseyin Hisil. Complete group law for genus 2 Jacobians on Jacobian coordinates. *Journal of Cryptographic Engineering*, 14(1):87–101, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00351-7`.

Joshi:2024:DRK

[337] Priyanka Joshi and Bodhisatwa Mazumdar. Deep round key recovery attacks and countermeasure in persistent fault model: a case study on GIFT and KLEIN. *Journal of Cryptographic Engineering*, 14(1):103–125, April 2024. CODEN ???? ISSN 2190-

8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00349-1`.

Koshelev:2024:CSM

[338] Dmitrii Koshelev. Correction to: Subgroup membership testing on elliptic curves via the Tate pairing. *Journal of Cryptographic Engineering*, 14 (1):127–128, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00331-3`. See [306].

Zhang:2024:EAP

[339] Fan Zhang. Editorial about PROOFS 2021. *Journal of Cryptographic Engineering*, 14(1):129, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00345-x`.

Cheng:2024:TFB

[340] Wei Cheng, Yi Liu, Sylvain Guilley, and Olivier Rioul. Toward finding best linear codes for side-channel protections (extended version). *Journal of Cryptographic Engineering*, 14(1):131–145, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-022-00305-x`.

Lacombe:2024:CSA

[341] Guilhem Lacombe, David Feliot, Etienne Boespflug, and Marie-Laure Potet. Combining static analysis and dynamic symbolic execution in a toolchain to detect fault injection vulnerabilities. *Journal of Cryptographic Engineering*, 14 (1):147–164, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00310-8`.

Asano:2024:SBE

[342] Tamon Asano and Takeshi Sugawara. Simulation-based evaluation of bit-interaction side-channel leakage on RISC-V: extended version. *Journal of Cryptographic Engineering*, 14(1): 165–180, April 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00319-z`.

Guillen:2024:AFC

[343] Luis Guillen. The asymmetric five-card trick: working with variable encoding in card-based protocols. *Journal of Cryptographic Engineering*, 14(2):181–192, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00333-1`.

Sideris:2024:HAD

[344] Argyrios Sideris, Theodora Sanida, and Minas Dasygenis. Hardware acceleration design of the SHA-3 for high throughput and low area on FPGA. *Journal of Cryptographic Engineering*, 14(2):193–205, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00334-0`.

Viera:2024:TFM

[345] Raphael Viera, Jean-Max Dutertre, Rodrigo Silva Lima, Matthieu Pom-

mies, and Anthony Bertrand. Tampering with the flash memory of microcontrollers: permanent fault injection via laser illumination during read operations. *Journal of Cryptographic Engineering*, 14(2):207–221, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00335-z`.

Carlet:2024:MMB

[346] Claude Carlet, Abderrahman Daif, Sylvain Guilley, and Cédric Tavernier. A masking method based on orthonormal spaces, protecting several bytes against both SCA and FIA with a reduced cost. *Journal of Cryptographic Engineering*, 14(2):223–240, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00339-9`.

Aydin:2024:LSH

[347] Furkan Aydin and Aydin Aysu. Leaking secrets in homomorphic encryption with side-channel attacks. *Journal of Cryptographic Engineering*, 14(2):241–251, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00340-2`.

kumar:2024:QRN

[348] Vaishnavi kumar and Padmapriya Pravinkumar. Quantum random number generator on IBM QX. *Journal of Cryptographic Engineering*, 14(2):253–259, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00341-1`.

Al-Muhammed:2024:BSC

[349] Muhammed Jassem Al-Muhammed. Bit-sensitive chaos-based encryption technique with nonparametric memory loss-based key hiding code generation. *Journal of Cryptographic Engineering*, 14(2):261–279, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00343-z`.

Seddigh:2024:BKM

[350] Milad Seddigh, Mahdi Esfahani, Sarani Bhattacharya, Mohammad Reza Aref, and Hadi Soleimany. Breaking KASLR on mobile devices without any use of cache memory (extended version). *Journal of Cryptographic Engineering*, 14 (2):281–294, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-023-00344-y`.

Vollala:2024:EET

[351] Satyanarayana Vollala. Energy efficient triple-modular exponential techniques for batch verification schemes. *Journal of Cryptographic Engineering*, 14 (2):295–309, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00348-2`.

Aljafar:2024:ULE

[352] Muayad J. Aljafar, Florence Azais, Marie-Lise Flottes, and Samuel Pagliarini. Utilizing layout effects for analog

logic locking. *Journal of Cryptographic Engineering*, 14(2):311–324, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00350-8`.

Alshaer:2024:CLA

[353] Ihab Alshaer, Gijs Burghoorn, Brice Colombier, Christophe Deleuze, Vincent Beroulle, and Paolo Maistri. Cross-layer analysis of clock glitch fault injection while fetching variable-length instructions. *Journal of Cryptographic Engineering*, 14(2):325–342, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00352-6`.

Kim:2024:MCA

[354] Kwang Ho Kim, Sihem Mesnager, and Kyong Il Pak. Montgomery curve arithmetic revisited. *Journal of Cryptographic Engineering*, 14(2):343–362, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00353-5`.

Jana:2024:DFA

[355] Amit Jana and Goutam Paul. Differential fault attack on SPN-based sponge and SIV-like AE schemes. *Journal of Cryptographic Engineering*, 14(2):363–381, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00354-4`.

Hu:2024:UGE

[356] Jingwei Hu, Wen Wang, Kris Gaj, Donglong Chen, and Huaxiong Wang. Universal Gaussian elimination hardware for cryptographic purposes. *Journal of Cryptographic Engineering*, 14(2):383–397, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00355-3`.

Lashermes:2024:GSR

[357] Ronan Lashermes and Hélène Le Bouder. Generic SCARE: reverse engineering without knowing the algorithm nor the machine. *Journal of Cryptographic Engineering*, 14(2):399–414, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00356-2`.

Salarifard:2024:EHA

[358] Raziyeh Salarifard and Hadi Soleimany. An efficient hardware accelerator for NTT-based polynomial multiplication using FPGA. *Journal of Cryptographic Engineering*, 14(2):415–426, June 2024. CODEN ???? ISSN 2190-8508 (print), 2190-8516 (electronic). URL `https://link.springer.com/article/10.1007/s13389-024-00357-1`.