References

1. 3GPP. ETSI (2014-10). Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi specification (3GPP TS 35.202 version 12.0.0 Release 12), 2014.
2. Mohamed Ahmed Abdelraheem. Estimating the probabilities of low-weight differential and linear approximations on PRESENT-like ciphers. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *ICISC 12: 15th International Conference on Information Security and Cryptology*, volume 7839 of *Lecture Notes in Computer Science*, pages 368–382, Seoul, Korea, November 28–30, 2013. Springer.
3. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, and Praveen Gauravaram. Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48. Cryptology ePrint Archive, Report 2015/988, 2015. http://eprint.iacr.org/2015/988.
4. Mohamed Ahmed Abdelraheem, Javad Alizadeh, Hoda A. Alkhzaimi, Mohammad Reza Aref, Nasour Bagheri, Praveen Gauravaram, and Martin M. Lauridsen. Improved linear cryptanalysis of reduced-round SIMON. Cryptology ePrint Archive, Report 2014/681, 2014. http://eprint.iacr.org/2014/681.
5. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Cryptanalysis of the speck family of block ciphers. Cryptology ePrint Archive, Report 2013/568, 2013. http://eprint.iacr.org/2013/568.
6. Farzaneh Abed, Eik List, Stefan Lucks, and Jakob Wenzel. Differential and linear cryptanalysis of reduced-round simon. Cryptology ePrint Archive, Report 2013/526, 2013. http://eprint.iacr.org/2013/526.
7. Osman Abul and Cansın Bayrak. From location to location pattern privacy in location-based services. *Knowledge and Information Systems*, Jan 2018.
8. Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle. Privacy in e-commerce: examining user scenarios and privacy preferences. In *EC*, pages 1–8, 1999.
9. Eytan Adar. User 4xxxxx9: Anonymizing query logs. In *Proc of Query Log Analysis Workshop, International Conference on World Wide Web*, 2007.
10. Mikhail Afanasyev, Tadayoshi Kohno, Justin Ma, Nick Murphy, Stefan Savage, Alex C. Snoeren, and Geoffrey M. Voelker. Privacy-preserving network forensics. *Commun. ACM*, 54(5):78–87, May 2011.
11. Dakshi Agrawal, Josyula R. Rao, Pankaj Rohatgi, and Kai Schramm. Templates as Master Keys. In *CHES*, volume 3659, pages 15–29. Springer, August 29 – September 1 2005. Edinburgh, UK.

G. Avoine, J. Hernandez-Castro (eds.), *Security of Ubiquitous Computing Systems*,
https://doi.org/10.1007/978-3-030-10591-4

12. Rakesh Agrawal and Ramakrishnan Srikant. Privacy-Preserving Data Mining. *ACM Sigmod Record*, 29(2):439–450, 2000.
13. Martin Ågren and Martin Hell. Cryptanalysis of the stream cipher bean. In *Security of Information and Networks, SIN 2011, Sydney, Australia, November 14–19, 2011*, pages 21–28, 2011.
14. Martin Ågren, Martin Hell, Thomas Johansson, and Willi Meier. Grain-128a: a new version of Grain-128 with optional authentication. *International Journal of Wireless and Mobile Computing*, 5(1):48–59, 2011.
15. Siavash Ahmadi, Zahra Ahmadian, Javad Mohajeri, and Mohammad Reza Aref. Low-data complexity biclique cryptanalysis of block ciphers with application to piccolo and HIGHT. *IEEE Trans. Information Forensics and Security*, 9(10):1641–1652, 2014.
16. Toru Akishita and Harunaga Hiwatari. Very compact hardware implementations of the blockcipher clefia. In *Selected Areas in Cryptography, SAC 2011, Ontario, Canada, August 11–12, 2011*, pages 278–292, 2011.
17. Martin R. Albrecht, Benedikt Driessen, Elif Bilge Kavun, Gregor Leander, Christof Paar, and Tolga Yalçin. Block ciphers - focus on the linear layer (feat. PRIDE). In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology – CRYPTO 2014, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 57–76, Santa Barbara, CA, USA, August 17–21, 2014. Springer.
18. Javad Alizadeh, Nasour Bagheri, Praveen Gauravaram, Abhishek Kumar, and Somitra Kumar Sanadhya. Linear cryptanalysis of round reduced SIMON. Cryptology ePrint Archive, Report 2013/663, 2013. http://eprint.iacr.org/2013/663.
19. Hoda A. Alkhzaimi and Martin M. Lauridsen. Cryptanalysis of the SIMON family of block ciphers. Cryptology ePrint Archive, Report 2013/543, 2013. http://eprint.iacr.org/2013/543.
20. Riham AlTawy, Raghvendra Rohit, Morgan He, Kalikinkar Mandal, Gangqiang Yang, and Guang Gong. sliscp: Simeck-based permutations for lightweight sponge cryptographic primitives. In *Selected Areas in Cryptography, SAC 2017, Ottawa, Canada, August 16–18, 2017*, pages 129–150, 2018.
21. Frederic Amiel, Benoit Feix, and Karine Villegas. Power analysis for secret recovering and reverse engineering of public key algorithms. In Carlisle Adams, Ali Miri, and Michael Wiener, editors, *Selected Areas in Cryptography*, volume 4876 of *Lecture Notes in Computer Science*, pages 110–125. Springer, 2007.
22. Elena Andreeva, Begül Bilgin, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. Ape: Authenticated permutation-based encryption for lightweight cryptography. In *Fast Software Encryption, FSE 2014, London, UK, March 3–5, 2014*, pages 168–186, 2015.
23. Ralph Ankele, Subhadeep Banik, Avik Chakraborti, Eik List, Florian Mendel, Siang Meng Sim, and Gaoli Wang. Related-key impossible-differential attack on reduced-round skinny. In Dieter Gollmann, Atsuko Miyaji, and Hiroaki Kikuchi, editors, *ACNS 17: 15th International Conference on Applied Cryptography and Network Security*, volume 10355 of *Lecture Notes in Computer Science*, pages 208–228, Kanazawa, Japan, July 10–12, 2017. Springer.
24. Ralph Ankele and Eik List. Differential cryptanalysis of round-reduced sparx-64/128. Cryptology ePrint Archive, Report 2018/332, 2018. https://eprint.iacr.org/2018/332.
25. Cédric Archambeau, Éric Peeters, François-Xavier Standaert, and Jean-Jacques Quisquater. Template Attacks in Principal Subspaces. In *CHES*, volume 4249 of *LNCS*, pages 1–14. Springer, October 10–13 2006. Yokohama, Japan.
26. Frederik Armknecht, Matthias Hamann, and Vasily Mikhalev. Lightweight authentication protocols on ultra-lightweight RFIDs – myths and facts. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
27. Frederik Armknecht and Vasily Mikhalev. On lightweight stream ciphers with shorter internal states. In Gregor Leander, editor, *Fast Software Encryption – FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 451–470, Istanbul, Turkey, March 8–11, 2015. Springer.

28. Tomer Ashur and Yunwen Liu. Rotational cryptanalysis in the presence of constants. *IACR Transactions on Symmetric Cryptology*, 2016(1):57–70, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/535.
29. Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P. Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges and countermeasures. *IEEE Internet of Things Journal*, pages 1–1, 2018.
30. Mehrnaz Ataei and Christian Kray. Ephemerality is the new black: A novel perspective on location data management and location privacy in lbs. In Georg Gartner and Haosheng Huang, editors, *Progress in Location-Based Services 2016*, pages 357–373, Cham, 2017. Springer International Publishing.
31. Giuseppe Ateniese, Bernardo Magri, and Daniele Venturi. Subversion-resilient signature schemes. In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12–16, 2015*, pages 364–375. ACM, 2015.
32. Jean-Philippe Aumasson and Daniel J. Bernstein. SipHash: A fast short-input PRF. In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology - INDOCRYPT 2012: 13th International Conference in Cryptology in India*, volume 7668 of *Lecture Notes in Computer Science*, pages 489–508, Kolkata, India, December 9–12, 2012. Springer.
33. Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A lightweight hash. *Journal of Cryptology*, 26(2):313–339, April 2013.
34. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. Norx8 and norx16: Authenticated encryption for low-end systems. IACR Cryptology ePrint Archive 2015/1154, 2015.
35. Jean-Philippe Aumasson, Philipp Jovanovic, and Samuel Neves. NORX v3.0. candidate for the CAESAR competition. https://norx.io, 2016.
36. Jean-Philippe Aumasson, Simon Knellwolf, and Willi Meier. Heavy quark for secure aead. In *Directions in Authenticated Ciphers, DIAC 2012, Stockholm, Sweden, July 05–06, 2012*, 2012.
37. Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O'Hearn, and Christian Winnerlein. BLAKE2: Simpler, smaller, fast as MD5. In Michael J. Jacobson Jr., Michael E. Locasto, Payman Mohassel, and Reihaneh Safavi-Naini, editors, *ACNS 13: 11th International Conference on Applied Cryptography and Network Security*, volume 7954 of *Lecture Notes in Computer Science*, pages 119–135, Banff, AB, Canada, June 25–28, 2013. Springer.
38. Autoelectric. XGecu TL866II. http://autoelectric.cn/EN/TL866_main.html.
39. Roberto Avanzi. The QARMA block cipher family – almost MDS matrices over rings with zero divisors, nearly symmetric Even-Mansour constructions with non-involutory central rounds, and search heuristics for low-latency S-boxes. Cryptology ePrint Archive, Report 2016/444, 2016. http://eprint.iacr.org/2016/444.
40. Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan čapkun, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. Security of distance-bounding: A survey. *ACM Comput. Surv.*, 51(5):94:1–94:33, September 2018.
41. Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux, and Benjamin Martin. A formal framework for analyzing RFID distance bounding protocols. In *Journal of Computer Security - Special Issue on RFID System Security, 2010*, volume 19, pages 289–317, 2011.
42. Gildas Avoine, Xavier Bultel, Sébastien Gambs, David Gérault, Pascal Lafourcade, Cristina Onete, and Jean-Marc Robert. A terrorist-fraud resistant and extractor-free anonymous distance-bounding protocol. In *ACM on Asia Conference on Computer and Communications Security*, ASIA CCS '17, pages 800–814, New York, NY, USA, 2017. ACM.
43. Gildas Avoine, Xavier Carpent, and Julio Hernandez-Castro. Pitfalls in ultralightweight authentication protocol designs. *IEEE Trans. Mob. Comput.*, 15(9):2317–2332, 2016.

44. Gildas Avoine, Xavier Carpent, and Benjamin Martin. Strong Authentication and Strong Integrity (SASI) is not that Strong. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 50–64, Istanbul, Turkey, June 2010. Springer.
45. Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: Balancing false-acceptance rate and memory requirement. In *International Conference on Information Security (ISC) 2009*, volume 5735 of *Lecture Notes in Computer Science*, pages 250–261. Springer, 2009.
46. Yossi Azar, Andrei Z. Broder, Anna R. Karlin, and Eli Upfal. Balanced allocations. *SIAM J. Comput.*, 29(1):180–200, 1999.
47. Steve Babbage. Improved "exhaustive search" attacks on stream ciphers. In *European Convention on Security and Detection*, pages 161–166. IET, May 1995.
48. Steve Babbage and Matthew Dodd. The MICKEY stream ciphers. In *New Stream Cipher Designs - The eSTREAM Finalists*, pages 191–209, 2008.
49. Stéphane Badel, Nilay Dagtekin, Jorge Nakahara, Khaled Ouafi, Nicolas Reffé, Pouyan Sepehrdad, Petr Susil, and Serge Vaudenay. ARMADILLO: A multi-purpose cryptographic primitive dedicated to hardware. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 398–412, Santa Barbara, CA, USA, August 17–20, 2010. Springer.
50. Subhadeep Banik. Some results on Sprout. In *INDOCRYPT 2015*, volume 9462 of *LNCS*, pages 124–139. Springer, 2015.
51. Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology – ASIACRYPT 2015, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436, Auckland, New Zealand, November 30 – December 3, 2015. Springer.
52. Subhadeep Banik, Takanori Isobe, Tingting Cui, and Jian Guo. Some cryptanalytic results on Lizard. *IACR Transactions on Symmetric Cryptology*, 2017(4):82–98, 2017.
53. Subhadeep Banik, Takanori Isobe, and Masakatu Morii. On design of robust lightweight stream cipher with short internal state. *IEICE Transactions*, 101-A(1):99–109, 2018.
54. Gaurav Bansod, Abhijit Patil, and Narayan Pisharoty. Granule: An ultra lightweight cipher design for embedded security. IACR Cryptology ePrint Archive 2018/600, 2018.
55. Achiya Bar-On, Itai Dinur, Orr Dunkelman, Virginie Lallemand, Nathan Keller, and Boaz Tsaban. Cryptanalysis of SP networks with partial non-linear layers. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 315–342, Sofia, Bulgaria, April 26–30, 2015. Springer.
56. Achiya Bar-On and Nathan Keller. A 2^{70} attack on the full MISTY1. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part I*, volume 9814 of *Lecture Notes in Computer Science*, pages 435–456, Santa Barbara, CA, USA, August 14–18, 2016. Springer.
57. Zachry Basnight, Jonathan Butts, Juan Lopez Jr., and Thomas Dube. Firmware modification attacks on programmable logic controllers. *International Journal of Critical Infrastructure Protection*, 2013.
58. Lejla Batina, Łukasz Chmielewski, Louiza Papachristodoulou, Peter Schwabe, and Michael Tunstall. Online template attacks. In Willi Meier and Debdeep Mukhopadhyay, editors, *Progress in Cryptology – INDOCRYPT 2014*, pages 21–36, Cham, 2014. Springer International Publishing.
59. Aurélie Bauer and Éliane Jaulmes. Correlation analysis against protected sfm implementations of rsa. In Goutam Paul and Serge Vaudenay, editors, *Progress in Cryptology - INDOCRYPT 2013*, volume 8250 of *Lecture Notes in Computer Science*, pages 98–115. Springer International Publishing, 2013.

60. Aurélie Bauer, Éliane Jaulmes, Emmanuel Prouff, and Justine Wild. Horizontal and vertical side-channel attacks against secure RSA implementations. In Ed Dawson, editor, *Topics in Cryptology – CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 1–17, San Francisco, CA, USA, February 25 – March 1, 2013. Springer.
61. Aurélie Bauer, Éliane Jaulmes, Emmanuel Prouff, and Justine Wild. Horizontal collision correlation attack on elliptic curves. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013: 20th Annual International Workshop on Selected Areas in Cryptography*, volume 8282 of *Lecture Notes in Computer Science*, pages 553–570, Burnaby, BC, Canada, August 14–16, 2014. Springer.
62. Aslı Bay, Ioana Boureanu, Aikaterini Mitrokotsa, Iosif Spulber, and Serge Vaudenay. The bussard-bagga and other distance-bounding protocols under attacks. In Mirosław Kutyłowski and Moti Yung, editors, *Information Security and Cryptology*, pages 371–391. Springer, 2013.
63. Adnan Baysal and Sühap Sahin. Roadrunner: A small and fast bitslice block cipher for low cost 8-bit processors. In *Lightweight Cryptography for Security and Privacy - 4th International Workshop, LightSec 2015, Bochum, Germany, September 10–11, 2015, Revised Selected Papers*, pages 58–76, 2015.
64. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK families of lightweight block ciphers. Cryptology ePrint Archive, Report 2013/404, 2013. http://eprint.iacr.org/2013/404.
65. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The simon and speck lightweight block ciphers. In *Proceedings of the 52Nd Annual Design Automation Conference*, DAC '15, pages 175:1–175:6, New York, NY, USA, 2015. ACM.
66. Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. Notes on the design and analysis of SIMON and SPECK. Cryptology ePrint Archive, Report 2017/560, 2017. http://eprint.iacr.org/2017/560.
67. G C Becker, Jennifer Cooper, E. DeMulder, Gilbert Goodwill, Jules Jaffe, G. Kenworthy, T. Kouzminov, Andrew Leiserson, Mark E. Marson, Pankaj Rohatgi, and Sami Saab. Test vector leakage assessment (tvla) methodology in practice. In *International Cryptographic Module Conference*, volume 1001, page 13, 2013.
68. Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153, Santa Barbara, CA, USA, August 14–18, 2016. Springer.
69. Fabrice Bellard. Qemu, a fast and portable dynamic translator. In *USENIX Annual Technical Conference, FREENIX Track*, volume 41, page 46, 2005.
70. Davide Bellizia, Milena Djukanovic, Giuseppe Scotti, and Alessandro Trifiletti. Template attacks exploiting static power and application to CMOS lightweight crypto-hardware. *I. J. Circuit Theory and Applications*, 45(2):229–241, 2017.
71. Richard Ernest Bellman. *Dynamic Programming*. Dover Publications, Incorporated, 2003.
72. Jens Bender, Marc Fischlin, and Dennis Kügler. Security analysis of the PACE key-agreement protocol. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *Information Security, 12th International Conference, ISC 2009, Pisa, Italy, September 7–9, 2009. Proceedings*, volume 5735 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 2009.
73. Jens Bender, Marc Fischlin, and Dennis Kügler. The PACE|CA Protocol for Machine Readable Travel Documents. In Roderick Bloem and Peter Lipp, editors, *Trusted Systems*, volume 8292 of *Lecture Notes in Computer Science*, pages 17–35. Springer International Publishing, 2013.
74. Samy Bengio, Gilles Brassard, Yvo G. Desmedt, Claude Goutier, and Jean-Jacques Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 4(3):175–183, January 1991.

75. Emma Benoit, Guillaume Heilles, and Philippe Teuwen. Quarkslab blog post: Flash dumping, September 2017. https://blog.quarkslab.com/flash-dumping-part-i.html.
76. Alastair R. Beresford and Frank Stajano. Mix zones: User privacy in location-aware services. In *2nd IEEE Conference on Pervasive Computing and Communications Workshops (PerCom 2004 Workshops), 14–17 March 2004, Orlando, FL, USA*, pages 127–131, 2004.
77. Thierry P. Berger, Joffrey D'Hayer, Kevin Marquet, Marine Minier, and Gaël Thomas. The GLUON family: A lightweight hash function family based on FCSRs. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT 12: 5th International Conference on Cryptology in Africa*, volume 7374 of *Lecture Notes in Computer Science*, pages 306–323, Ifrance, Morocco, July 10–12, 2012. Springer.
78. Thierry P. Berger, Julien Francq, Marine Minier, and Gaël Thomas. Extended generalized feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. *IEEE Trans. Computers*, 65(7):2074–2089, 2016.
79. Daniel J. Bernstein. Chacha, a variant of salsa20. In Workshop Record of SASC, volume 8, 2008.
80. Daniel J. Bernstein. The Salsa20 family of stream ciphers. In *New Stream Cipher Designs - The eSTREAM Finalists*, pages 84–97, 2008.
81. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. Keccak sponge function family main document. Submission to NIST (Round 2), 2009.
82. Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. Caesar submission: Ketje v2. candidate for the caesar competition. http://ketje.noekeon.org/, 2016.
83. Thomas Beth and Yvo Desmedt. Identification tokens – or: Solving the chess grandmaster problem. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology-CRYPT0' 90*, pages 169–176. Springer, 1991.
84. John Bethencourt, Amit Sahai, and Brent Waters. Ciphertext-policy attribute-based encryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE, 2007.
85. Claudio Bettini, X. Sean Wang, and Sushil Jajodia. Protecting privacy against location-based personal identification. In Willem Jonker and Milan Petković, editors, *Secure Data Management*, pages 185–199. Springer, 2005.
86. Karthikeyan Bhargavan and Gaëtan Leurent. On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *ACM CCS 16: 23rd Conference on Computer and Communications Security*, pages 456–467, Vienna, Austria, October 24–28, 2016. ACM Press.
87. Begül Bilgin, Andrey Bogdanov, Miroslav Knežević, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems – CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 142–158, Santa Barbara, CA, USA, August 20–23, 2013. Springer.
88. Alex Biryukov and Eyal Kushilevitz. Improved cryptanalysis of RC5. In Kaisa Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 85–99, Espoo, Finland, May 31 – June 4, 1998. Springer.
89. Alex Biryukov and Leo Perrin. State of the art in lightweight symmetric cryptography. Cryptology ePrint Archive, Report 2017/511, 2017. http://eprint.iacr.org/2017/511.
90. Alex Biryukov, Deike Priemuth-Schmid, and Bin Zhang. Multiset collision attacks on reduced-round SNOW 3G and SNOW 3G (+). In Jianying Zhou and Moti Yung, editors, *ACNS 10: 8th International Conference on Applied Cryptography and Network Security*, volume 6123 of *Lecture Notes in Computer Science*, pages 139–153, Beijing, China, June 22–25, 2010. Springer.
91. Alex Biryukov and Adi Shamir. Cryptanalytic time/memory/data tradeoffs for stream ciphers. In Tatsuaki Okamoto, editor, *Advances in Cryptology – ASIACRYPT 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 1–13, Kyoto, Japan, December 3–7, 2000. Springer.

92. Alex Biryukov, Adi Shamir, and David A. Wagner. Real time cryptanalysis of a5/1 on a pc. In *Fast Software Encryption, FSE 2000, New York, NY, USA, April 10–12, 2000*, pages 1–18, 2001.
93. Bruno Blanchet. An Efficient Cryptographic Protocol Verifier Based on Prolog Rules. In *IEEE Computer Security Foundations Workshop*, pages 82–96, Novia Scotia, Canada, 2001. IEEE.
94. Matt Blaze. Looking on the bright side of black-box cryptography (transcript of discussion). In *Security Protocols, 8th International Workshop, Cambridge, UK, April 3–5, 2000, Revised Papers*, pages 54–61, 2000.
95. Céline Blondeau and Benoît Gérard. Differential Cryptanalysis of PUFFIN and PUFFIN2, 11 2011.
96. Bluetooth^{TM}. Bluetooth specification, version 5.0, 2016.
97. Manuel Blum and Sampath Kannan. Designing programs that check their work. *J. ACM*, 42(1):269–291, 1995.
98. Martin Boesgaard, Mette Vesterager, Thomas Pedersen, Jesper Christiansen, and Ove Scavenius. Rabbit: A new high-performance stream cipher. In Thomas Johansson, editor, *Fast Software Encryption – FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 307–329, Lund, Sweden, February 24–26, 2003. Springer.
99. Andrey Bogdanov, Ilya Kizhvatov, and Andrey Pyshkin. Algebraic methods in side-channel collision attacks and practical collision detection. In DipanwitaRoy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT 2008*, volume 5365 of *Lecture Notes in Computer Science*, pages 251–265. Springer, 2008.
100. Andrey Bogdanov, Miroslav Knežević, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede. Spongent: A lightweight hash function. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 312–325, Nara, Japan, September 28 – October 1, 2011. Springer.
101. Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466, Vienna, Austria, September 10–13, 2007. Springer.
102. Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, and Yannick Seurin. Hash functions and RFID tags: Mind the gap. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 283–299, Washington, D.C., USA, August 10–13, 2008. Springer.
103. Andrey Bogdanov, Florian Mendel, Francesco Regazzoni, Vincent Rijmen, and Elmar Tischhauser. ALE: AES-based lightweight authenticated encryption. In Shiho Moriai, editor, *Fast Software Encryption – FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 447–466, Singapore, March 11–13, 2014. Springer.
104. Andrey Bogdanov and Christian Rechberger. A 3-subset meet-in-the-middle attack: Cryptanalysis of the lightweight block cipher KTANTAN. In Alex Biryukov, Guang Gong, and Douglas R. Stinson, editors, *SAC 2010: 17th Annual International Workshop on Selected Areas in Cryptography*, volume 6544 of *Lecture Notes in Computer Science*, pages 229–240, Waterloo, Ontario, Canada, August 12–13, 2011. Springer.
105. Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knežević, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 208–225, Beijing, China, December 2–6, 2012. Springer.
106. Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In

Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199, Kaoshiung, Taiwan, R.O.C., December 7–11, 2014. Springer.
107. Ioana Boureanu, David Gerault, and Pascal Lafourcade. Fine-grained and application-ready distance-bounding security. Cryptology ePrint Archive, Report 2018/384, 2018.
108. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. On the pseudorandom function assumption in (secure) distance-bounding protocols. In Alejandro Hevia and Gregory Neven, editors, *Progress in Cryptology – LATINCRYPT 2012*, pages 100–120. Springer, 2012.
109. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Towards secure distance bounding. In *Fast Software Encryption - 20th International Workshop, FSE 2013*, pages 55–67, Singapore, March 2013.
110. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Practical and provably secure distance-bounding. In Yvo Desmedt, editor, *Information Security*, pages 248–258, Cham, 2015. Springer.
111. Ioana Boureanu and Serge Vaudenay. Optimal proximity proofs. In *Information Security and Cryptology - 10th International Conference, Inscrypt 2014, Beijing, China, December 13–15, 2014, Revised Selected Papers*, pages 170–190, 2014.
112. Stefan Brands and David Chaum. Distance-bounding protocols. In Tor Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 344–359. Springer, 1994.
113. Stefan Brands and David Chaum. Distance-bounding protocols. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 344–359. Springer, 1994.
114. Agnès Brelurut, David Gerault, and Pascal Lafourcade. Survey of distance bounding protocols and threats. In Joaquin Garcia-Alfaro, Evangelos Kranakis, and Guillaume Bonfante, editors, *Foundations and Practice of Security*, pages 29–49, Cham, 2016. Springer.
115. Éric Brier, Christophe Clavier, and Francis Olivier. Correlation Power Analysis with a Leakage Model. In *CHES*, volume 3156 of *LNCS*, pages 16–29. Springer, August 11–13 2004. Cambridge, MA, USA.
116. Robert G Brown, Dirk Eddelbuettel, and David Bauer. Dieharder: A random number test suite. *Open Source software library, under development*, 2013.
117. Marco Bucci, Luca Giancane, Raimondo Luzzi, M. Marino, Giuseppe Scotti, and Alessandro Trifiletti. Enhancing power analysis attacks against cryptographic devices. *IET Circuits, Devices & Systems*, 2(3):298–305, 2008.
118. Xavier Bultel, Sébastien Gambs, David Gérault, Pascal Lafourcade, Cristina Onete, and Jean-Marc Robert. A prover-anonymous and terrorist-fraud resistant distance-bounding protocol. In *ACM Conference on Security & Privacy in Wireless and Mobile Networks*, WiSec '16, pages 121–133, New York, NY, USA, 2016. ACM.
119. Kang Byeong-Ho. Ubiquitous computing environment threats and defensive measures. *Int. J. Multimedia Ubiquit. Eng*, 2(1):47–60, 2007.
120. Cristian Cadar, Daniel Dunbar, and Dawson Engler. KLEE: Unassisted and Automatic Generation of High-coverage Tests for Complex Systems Programs. In *Proceedings of the 8th USENIX Conference on Operating Systems Design and Implementation*, OSDI '08, 2008.
121. Tom Caddy. Fips 140–2. In *Encyclopedia of Cryptography and Security*, pages 468–471. Springer, 2011.
122. Eleonora Cagli, Cécile Dumas, and Emmanuel Prouff. Convolutional neural networks with data augmentation against jitter-based countermeasures - profiling attacks without pre-processing. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25–28, 2017, Proceedings*, pages 45–68, 2017.
123. Ying Cai and Ge Xu. Cloaking with footprints to provide location privacy protection in location-based services, August 15 2017. US Patent 9,736,685.
124. Seyit Ahmet Çamtepe and Bülent Yener. Combinatorial design of key distribution mechanisms for wireless sensor networks. *IEEE/ACM Trans. Netw.*, 15(2):346–358, 2007.

125. Giovanni Camurati and Aurélien Francillon. Inception: system-wide security testing of real-world embedded systems software. In *USENIX Security Symposium*, 2018.
126. Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. In Christophe Clavier and Kris Gaj, editors, *Cryptographic Hardware and Embedded Systems – CHES 2009*, volume 5747 of *Lecture Notes in Computer Science*, pages 272–288, Lausanne, Switzerland, September 6–9, 2009. Springer.
127. Christophe De Cannière and Bart Preneel. Trivium. In *New Stream Cipher Designs - The eSTREAM Finalists*, pages 244–266, 2008.
128. Anne Canteaut, Thomas Fuhr, Henri Gilbert, María Naya-Plasencia, and Jean-René Reinhard. Multiple differential cryptanalysis of round-reduced PRINCE. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption – FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 591–610, London, UK, March 3–5, 2015. Springer.
129. Anne Canteaut, Virginie Lallemand, and María Naya-Plasencia. Related-key attack on full-round PICARO. In Orr Dunkelman and Liam Keliher, editors, *SAC 2015: 22nd Annual International Workshop on Selected Areas in Cryptography*, volume 9566 of *Lecture Notes in Computer Science*, pages 86–101, Sackville, NB, Canada, August 12–14, 2016. Springer.
130. Xavier Carpent. *RFID authentication and time-memory trade-offs*. PhD thesis, Catholic University of Louvain, Louvain-la-Neuve, Belgium, 2015.
131. Luca Caviglione, Steffen Wendzel, and Wojciech Mazurczyk. The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy*, 15(6):12–17, 2017.
132. Avik Chakraborti, Anupam Chattopadhyay, Muhammad Hassan, and Mridul Nandi. TriviA: A fast and secure authenticated encryption scheme. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems – CHES 2015*, volume 9293 of *Lecture Notes in Computer Science*, pages 330–353, Saint-Malo, France, September 13–16, 2015. Springer.
133. Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *International Cryptology Conference on Advances in Cryptology – CRYPTO'09*, Lecture Notes in Computer Science, pages 391–407. Springer, 2009.
134. Suresh Chari, Charanjit Jutla, Josyula Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In *Advances in Cryptology - CRYPTO'99*, pages 791–791. Springer, 1999.
135. Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi. Template Attacks. In *CHES*, volume 2523 of *LNCS*, pages 13–28. Springer, August 2002. San Francisco Bay (Redwood City), USA.
136. David Chaum and Torben P. Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 1992.
137. Daming D Chen, Manuel Egele, Maverick Woo, and David Brumley. Towards automated dynamic analysis for linux-based embedded firmware. In *ISOC NDSS 2016*, 2016.
138. Huaifeng Chen and Xiaoyun Wang. Improved linear hull attack on round-reduced Simon with dynamic key-guessing techniques. Cryptology ePrint Archive, Report 2015/666, 2015. http://eprint.iacr.org/2015/666.
139. Hung-Yu Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 4(4):337–340, December 2007.
140. Vitaly Chipounov, Volodymyr Kuznetsov, and George Candea. S2e: A platform for in-vivo multi-path analysis of software systems. *Acm Sigplan Notices*, 46(3):265–278, 2011.
141. Tom Chothia, Flavio D. Garcia, Joeri de Ruiter, Jordi van den Breekel, and Matthew Thompson. Relay cost bounding for contactless EMV payments. In Rainer Böhme and Tatsuaki Okamoto, editors, *Financial Cryptography and Data Security - 19th International Conference, FC 2015, San Juan, Puerto Rico, January 26–30, 2015, Revised Selected Papers*, volume 8975 of *Lecture Notes in Computer Science*, pages 189–206, Puerto Rico, January 2015. Springer.

142. Omar Choudary and Markus G. Kuhn. Efficient template attacks. In Aurélien Francillon and Pankaj Rohatgi, editors, *Smart Card Research and Advanced Applications - 12th International Conference, CARDIS 2013, Berlin, Germany, November 27–29, 2013. Revised Selected Papers*, volume 8419 of *LNCS*, pages 253–270. Springer, 2013.
143. Arka Rai Choudhuri and Subhamoy Maitra. Significantly improved multi-bit differentials for reduced round Salsa and ChaCha. *IACR Transactions on Symmetric Cryptology*, 2016(2):261–287, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/574.
144. Jiali Choy, Huihui Yap, Khoongming Khoo, Jian Guo, Thomas Peyrin, Axel Poschmann, and Chik How Tan. SPN-hash: Improving the provable resistance against differential collision attacks. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT 12: 5th International Conference on Cryptology in Africa*, volume 7374 of *Lecture Notes in Computer Science*, pages 270–286, Ifrance, Morocco, July 10–12, 2012. Springer.
145. Hyunji Chung, Jungheum Park, and Sangjin Lee. Digital forensic approaches for amazon alexa ecosystem. *Digital Investigation*, 22:S15–S25, 2017.
146. Jacek Cichoń, Zbigniew Golebiewski, and Mirosław Kutyłowski. From key predistribution to key redistribution. *Theor. Comput. Sci.*, 453:75–87, 2012.
147. Jacek Cichoń and Mirosław Kutyłowski. Anonymity and k-choice identities. In Dingyi Pei, Moti Yung, Dongdai Lin, and Chuankun Wu, editors, *Information Security and Cryptology, Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5, 2007, Revised Selected Papers*, volume 4990 of *Lecture Notes in Computer Science*, pages 283–297. Springer, 2007.
148. Carlos Cid, Shinsaku Kiyomoto, and Jun Kurihara. The rakaposhi stream cipher. In *Information and Communications Security, ICICS 2009, Beijing, China, December 14–17, 2009*, pages 32–46, 2009.
149. Jolyon Clulow, Gerhard P Hancke, Markus G Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *European Workshop on Security in Ad-hoc and Sensor Networks*, volume 4357 of *Lecture Notes in Computer Science*, pages 83–97. Springer, 2006.
150. Lucian Cojocar, Jonas Zaddach, Roel Verdult, Herbert Bos, Aurélien Francillon, and Davide Balzarotti. PIE: Parser Identification in Embedded Systems. *Annual Computer Security Applications Conference (ACSAC)*, December 2015.
151. SEC Consult. House of Keys: Industry-Wide HTTPS Certificate and SSH Key Reuse Endangers Millions of Devices Worldwide. *Blog, Nov*, 25, 2015.
152. Mauro Conti, Ali Dehghantanha, Katrin Franke, and Steve Watson. Internet of things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, 78:544–546, 2018.
153. Jean-Sbastien Coron, Aline Gouget, Thomas Icart, and Pascal Paillier. Supplemental access control (pace v2): Security analysis of pace integrated mapping. *IACR Cryptology ePrint Archive*, 2011:58, 2011.
154. Jean-Sébastien Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In *Proceedings of the First International Workshop on Cryptographic Hardware and Embedded Systems*, CHES '99, pages 292–302, London, UK, UK, 1999. Springer-Verlag.
155. Andrei Costin, Jonas Zaddach, Aurélien Francillon, and Davide Balzarotti. A Large Scale Analysis of the Security of Embedded Firmwares. In *Proceedings of the 23rd USENIX Security Symposium (USENIX Security)*, August 2014.
156. Andrei Costin, Apostolis Zarras, and Aurélien Francillon. Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces. In *11th ACM Asia Conference on Computer and Communications Security (ASIACCS*, ASIACCS 16, May 2016.
157. Andrei Costin, Apostolis Zarras, and Aurélien Francillon. Towards automated classification of firmware images and identification of embedded devices. In *IFIP International Conference on ICT Systems Security and Privacy Protection*, pages 233–247. Springer, 2017.

158. Franck Courbon, Sergei Skorobogatov, and Christopher Woods. Reverse engineering flash EEPROM memories using scanning electron microscopy. In *Smart Card Research and Advanced Applications - 15th International Conference, CARDIS 2016*, pages 57–72, 2016.
159. Nicolas T. Courtois. An improved differential attack on full GOST. In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pages 282–303, 2016.
160. Cas Cremers, Kasper B. Rasmussen, Benedikt Schmidt, and Srdjan Capkun. Distance hijacking attacks on distance bounding protocols. In *IEEE Symposium on Security and Privacy*, SP '12, pages 113–127, Washington, DC, USA, 2012. IEEE.
161. Ang Cui. Embedded Device Firmware Vulnerability Hunting with FRAK. *DefCon 20*, 2012.
162. Ang Cui, Michael Costello, and Salvatore J Stolfo. When Firmware Modifications Attack: A Case Study of Embedded Exploitation. In *Proceedings of the 20th Symposium on Network and Distributed System Security*, NDSS '13. The Internet Society, 2013.
163. Ang Cui and Salvatore J. Stolfo. Defending Embedded Systems with Software Symbiotes. In Robin Sommer, Davide Balzarotti, and Gregor Maier, editors, *Recent Advances in Intrusion Detection*, volume 6961 of *Lecture Notes in Computer Science*, pages 358–377. Springer, 2011.
164. Joan Daemen, René Govaerts, and Joos Vandewalle. A new approach to block cipher design. In Ross J. Anderson, editor, *Fast Software Encryption – FSE'93*, volume 809 of *Lecture Notes in Computer Science*, pages 18–32, Cambridge, UK, December 9–11, 1994. Springer.
165. Joan Daemen, Michaël Peeters, Gilles Van Assche, and Vincent Rijmen. Nessie proposal: NOEKEON, 2000. http://gro.noekeon.org/.
166. Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Springer-Verlag, 2002.
167. Yibin Dai and Shaozhen Chen. Cryptanalysis of full PRIDE block cipher. *Science China Information Sciences*, 60(5):052108, Sep 2016.
168. Boris Danev, Heinrich Luecken, Srdjan Capkun, and Karim El Defrawy. Attacks on physical-layer identification. In *ACM Conference on Wireless Network Security*, WiSec '10, pages 89–98, New York, NY, USA, 2010. ACM.
169. Paolo D'Arco and Alfredo De Santis. On Ultra-Lightweight RFID Authentication Protocols. *IEEE Transactions on Dependable and Secure Computing*, 99(PrePrints), 2010.
170. Paolo D'Arco and Roberto De Prisco. Design weaknesses in recent ultralightweight RFID authentication protocols. In *ICT Systems Security and Privacy Protection - 33rd IFIP TC 11 International Conference, SEC 2018, Held at the 24th IFIP World Computer Congress, WCC 2018, Poznan, Poland, September 18–20, 2018, Proceedings*, pages 3–17, 2018.
171. Lyla B Das. *Embedded Systems: An Integrated Approach*. Pearson Education India, 2012.
172. Sourav Das and Dipanwita Roy Chowdhury. Car30: a new scalable stream cipher with rule 30. *Cryptography and Communications*, 5(2):137–162, 2013.
173. Mathieu David, Damith Chinthana Ranasinghe, and Torben Bjerregaard Larsen. A2U2: A stream cipher for printed electronics RFID tags. *2011 IEEE International Conference on RFID*, pages 176–183, 2011.
174. Sherri Davidoff and Jonathan Ham. *Network forensics: tracking hackers through cyberspace*, volume 2014. Prentice hall Upper Saddle River, 2012.
175. Drew Davidson, Benjamin Moench, Thomas Ristenpart, and Somesh Jha. FIE on Firmware: Finding Vulnerabilities in Embedded Systems Using Symbolic Execution. In *Proceedings of the 22nd USENIX Security Symposium*, SEC '13, 2013.
176. Simon Davies. The Data Protection Regulation: A Triumph of Pragmatism over Principle? *European Data Protection Law Review*, 2:290, 2016.
177. Alexandre Debant, Stéphanie Delaune, and Cyrille Wiedling. Proving physical proximity using symbolic models. Technical report, Univ Rennes, CNRS, IRISA, France, February 2018.
178. Yvo Desmedt. Major security problems with the "unforgeable" (feige-)fiat-shamir proof of identity and how to overcome them. In *Securicom 88, 6th worldwide congress on computer and communications security and protection*, pages 147–159. SEDEP Paris France, 1988.

179. Lin Ding and Jie Guan. Cryptanalysis of mickey family of stream ciphers. *Security and Communication Networks*, 6(8):936–941, 2013.
180. Lin Ding, Chenhui Jin, Jie Guan, and Qiuyan Wang. Cryptanalysis of lightweight wg-8 stream cipher. *IEEE Transactions on Information Forensics and Security*, 9(4):645–652, 2014.
181. Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 484–513, Hanoi, Vietnam, December 4–8, 2016. Springer.
182. Dumitru-Daniel Dinu, Alex Biryukov, Johann Großschädl, Dmitry Khovra-Tovich, Yann Le Corre, and Léo Perrin. FELICS – fair evaluation of lightweight cryptographic systems. In NIST Workshop on Lightweight Cryptography 2015. National Institute of Standards and Technology (NIST), 2015.
183. Itai Dinur. Improved differential cryptanalysis of round-reduced Speck. Cryptology ePrint Archive, Report 2014/320, 2014. http://eprint.iacr.org/2014/320.
184. Itai Dinur and Jérémy Jean. Cryptanalysis of fides. In *Fast Software Encryption, FSE 2014, London, UK, March 3–5, 2014*, pages 224–240, 2015.
185. Christoph Dobraunig, Maria Eichlseder, Daniel Kales, and Florian Mendel. Practical key-recovery attack on mantis5. *IACR Trans. Symmetric Cryptol.*, 2016(2):248–260, 2017.
186. Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. candidate for the CAESAR competition. http://ascon.iaik.tugraz.at/, 2016.
187. Josep Domingo-Ferrer. A three-dimensional conceptual framework for database privacy. In *Workshop on Secure Data Management*, pages 193–202. Springer, 2007.
188. Christian D'Orazio, Kim-Kwang Raymond Choo, and Laurence T. Yang. Data exfiltration from internet of things devices: ios devices as case studies. *IEEE Internet of Things Journal*, 4(2):524–535, 2017.
189. Saar Drimer and Steven J. Murdoch. Keep your enemies close: Distance bounding against smartcard relay attacks. In *USENIX security symposium*, volume 312, 2007.
190. Yitao Duan and John Canny. Protecting user data in ubiquitous computing: Towards trustworthy environments. In *International Workshop on Privacy Enhancing Technologies*, pages 167–185. Springer, 2004.
191. Thomas Dullien and Rolf Rolles. Graph-based comparison of executable objects. In *Symposium sur la Securite des Technologies de lInformation et des Communications*, SSTIC '05, 2005.
192. Orr Dunkelman, Nathan Keller, and Adi Shamir. A practical-time related-key attack on the kasumi cryptosystem used in gsm and 3g telephony. In *Advances in Cryptology CRYPTO 2010, Santa Barbara, California, USA, August 15–19, 2010*, pages 393–410, 2010.
193. Ulrich Dürholz, Marc Fischlin, Michael Kasper, and Cristina Onete. A formal approach to distance bounding RFID protocols. In *Information Security Conference ISC 2011*, volume 7001 of *Lecture Notes in Computer Science*, pages 47–62. Springer, 2011.
194. François Durvaux, Mathieu Renauld, François-Xavier Standaert, Loic van Oldeneel tot Oldenzeel, and Nicolas Veyrat-Charvillon. Cryptanalysis of the ches 2009/2010 random delay countermeasure. *IACR Cryptology ePrint Archive*, 2012:38, 2012.
195. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*, pages 293–302. IEEE, 2008.
196. Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In *CRYPTO*, volume 5157 of *Lecture Notes in Computer Science*, pages 203–220. Springer, August 17–21 2008. Santa Barbara, CA, USA.
197. Thomas Eisenbarth, Sandeep S. Kumar, Christof Paar, Axel Poschmann, and Leif Uhsadel. A survey of lightweight-cryptography implementations. *IEEE Design & Test of Computers*, 24(6):522–533, 2007.

198. Elnec. Elnec beeprog2. https://www.elnec.com/en/products/universal-programmers/beeprog2/.
199. EMVCo. Book C-2 kernel 2 specification v2.5. EMV contactless specifications for payment system, March 2015.
200. Daniel W. Engels, Markku-Juhani O. Saarinen, Peter Schweitzer, and Eric M. Smith. The hummingbird-2 lightweight authenticated encryption algorithm. In *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26–28, 2011, Revised Selected Papers*, pages 19–31, 2011.
201. İmran Ergüler and Orhun Kara. A new approach to keystream based cryptosystems. In *SASC 2008, Workshop Record,*, pages 205–221. SASC, 2008.
202. Sebastian Eschweiler, Khaled Yakdan, and Elmar Gerhards-Padilla. discovRE: Efficient Cross-Architecture Identification of Bugs in Binary Code. In *ISOC NDSS 2016*, 2016.
203. Muhammed F. Esgin and Orhun Kara. Practical cryptanalysis of full Sprout with TMD tradeoff attacks. In *Selected Areas in Cryptography - SAC 2015*, pages 67–85, 2015.
204. ETSI/SAGE. Specification of the 3gpp confidentiality and integrity algorithms uea2 & uia2. document 2: Snow 3g specification. technical report, etsi/sage, 2006.
205. ETSI/SAGE. Specification of the 3gpp confidentiality and integrity algorithms 128-eea3 & 128-eia3. document 2: Zuc specification, version 1.6, 2011.
206. Limin Fan, Hua Chen, and Si Gao. A general method to evaluate the correlation of randomness tests. In *International Workshop on Information Security Applications*, pages 52–62. Springer, 2013.
207. Xinxin Fan, Kalikinkar Mandal, and Guang Gong. Wg-8: A lightweight stream cipher for resource-constrained smart devices. In *Quality, Reliability, Security and Robustness in Heterogeneous Networks, Qshine 2013, Greader Noida, India, January 11–12, 2013, Revised Selected Papers*, pages 617–632, 2013.
208. Dan Farmer and Wietse Venema. *Forensic Discovery*. Addison-Wesley Professional, 2005.
209. Horst Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.
210. Benoit Feix, Mylène Roussellet, and Alexandre Venelli. Side-channel analysis on blinded regular scalar multiplications. In Willi Meier and Debdeep Mukhopadhyay, editors, *Progress in Cryptology - INDOCRYPT 2014: 15th International Conference in Cryptology in India*, volume 8885 of *Lecture Notes in Computer Science*, pages 3–20, New Delhi, India, December 14–17, 2014. Springer.
211. Martin Feldhofer and Christian Rechberger. A case against currently used hash functions in rfid protocols. In *On the Move to Meaningful Internet Systems, OTM 2006, Montpellier, France, October 29 - November 3, 2006*, pages 372–381, 2006.
212. Qian Feng, Rundong Zhou, Chengcheng Xu, Yao Cheng, Brian Testa, and Heng Yin. Scalable Graph-based Bug Search for Firmware Images. In *ACM CCS 2016*, 2016.
213. Xiutao Feng and Fan Zhang. A practical state recovery attack on the stream cipher sablier v1. IACR Cryptology ePrint Archive 2014/245, 2014.
214. Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The skein hash function family (version 1.3). www.skein-hash.info/sites/default/files/skein1.3.pdf, 2010.
215. Niels Ferguson, Doug Whiting, Bruce Schneier, John Kelsey, Stefan Lucks, and Tadayoshi Kohno. Helix: Fast encryption and authentication in a single cryptographic primitive. In Thomas Johansson, editor, *Fast Software Encryption – FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 330–346, Lund, Sweden, February 24–26, 2003. Springer.
216. Marc Fischlin and Cristina Onete. Terrorism in distance bounding: Modeling terrorist-fraud resistance. In *Applied Cryptography and Network Security*, ACNS'13, pages 414–431. Springer, 2013.
217. International Organization for Standardization. Standardization and related activities – general vocabulary (iso/iec guide no. 2), 2004.
218. International Organization for Standardization. Information technology – security techniques – lightweight cryptography – part 2: Block ciphers (iso/iec standard no. 29192–2), 2012.

219. A. P. Fournaris, L. Papachristodoulou, and N. Sklavos. Secure and efficient rns software implementation for elliptic curve cryptography. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, pages 86–93, April 2017.
220. Apostolos P. Fournaris. *Fault and Power Analysis Attack Protection Techniques for Standardized Public Key Cryptosystems*, pages 93–105. Springer International Publishing, Cham, 2017.
221. Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science, 2011.
222. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC peer-to-peer relay attack using mobile phones. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pages 35–49. Springer, 2010.
223. Kai Fu, Meiqin Wang, Yinghua Guo, Siwei Sun, and Lei Hu. MILP-based automatic search algorithms for differential and linear trails for speck. In Thomas Peyrin, editor, *Fast Software Encryption – FSE 2016*, volume 9783 of *Lecture Notes in Computer Science*, pages 268–288, Bochum, Germany, March 20–23, 2016. Springer.
224. Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier. A key-recovery attack on 855-round trivium. Cryptology ePrint Archive, Report 2018/198, 2018. https://eprint.iacr.org/2018/198.
225. Daniel Genkin, Adi Shamir, and Eran Tromer. Acoustic cryptanalysis. *Journal of Cryptology*, 30(2):392–443, Apr 2017.
226. Carmina Georgescu, Emil Simion, Alina-Petrescu Nita, and Antonela Toma. A view on nist randomness tests (in) dependence. In *Electronics, Computers and Artificial Intelligence (ECAI), 2017 9th International Conference on*, pages 1–4. IEEE, 2017.
227. Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems – CHES 2013*, volume 8086 of *Lecture Notes in Computer Science*, pages 383–399, Santa Barbara, CA, USA, August 20–23, 2013. Springer.
228. Vahid Amin Ghafari and Honggang Hu. Fruit-80: A secure ultra-lightweight stream cipher for constrained environments. *Entropy*, 20(3):180, 2018.
229. Benedikt Gierlichs, Lejla Batina, Pim Tuyls, and Bart Preneel. Mutual information analysis. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2008*, pages 426–442. Springer, 2008.
230. Benedikt Gierlichs, Kerstin Lemke-Rust, and Christof Paar. Templates vs. Stochastic Methods. In *CHES*, volume 4249 of *LNCS*, pages 15–29. Springer, October 10–13 2006. Yokohama, Japan.
231. Henri Gilbert, Matthew Robshaw, and Hervé Sibert. An active attack against HB^+ – a provably secure lightweight authentication protocol. *IET Electronics Letters*, 41(21):1169–1170, October 2005.
232. Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. Good variants of HB+ are hard to find. In Gene Tsudik, editor, *FC 2008: 12th International Conference on Financial Cryptography and Data Security*, volume 5143 of *Lecture Notes in Computer Science*, pages 156–170, Cozumel, Mexico, January 28–31, 2008. Springer.
233. Henri Gilbert, Matthew J. B. Robshaw, and Yannick Seurin. $HB^\sharp$: Increasing the security and efficiency of HB^+. In Nigel P. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 361–378, Istanbul, Turkey, April 13–17, 2008. Springer.
234. Henri Gilbert, Matthew JB Robshaw, and Yannick Seurin. How to encrypt with the LPN problem. In *International Colloquium on Automata, Languages, and Programming*, pages 679–690. Springer, 2008.

235. R. Gilmore, N. Hanley, and M. O'Neill. Neural network based attack on a masked implementation of aes. In *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 106–111, May 2015.
236. Jovan Dj. Golic. Cryptanalysis of alleged A5 stream cipher. In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT'97*, volume 1233 of *Lecture Notes in Computer Science*, pages 239–255, Konstanz, Germany, May 11–15, 1997. Springer.
237. Jovan Dj. Golíc. Cryptanalysis of alleged A5 stream cipher. In Walter Fumy, editor, *Advances in Cryptology – EUROCRYPT 97*, volume 1233 of *Lecture Notes in Computer Science*, pages 239–255. Springer, 1997.
238. Zheng Gong, Pieter H. Hartel, Svetla Nikova, Shaohua Tang, and Bo Zhu. Tulp: A family of lightweight message authentication codes for body sensor networks. *J. Comput. Sci. Technol.*, 29(1):53–68, 2014.
239. Zheng Gong, Svetla Nikova, and Yee Wei Law. KLEIN: A new family of lightweight block ciphers. In *RFID. Security and Privacy - 7th International Workshop, RFIDSec 2011, Amherst, USA, June 26–28, 2011, Revised Selected Papers*, pages 1–18, 2011.
240. T. Good and M. Benaissa. Hardware performance of estream phase-iii stream cipher candidates. In *In SASC 2008*, pages 163–174, 2008.
241. Dan Goodin. Record-breaking ddos reportedly delivered by >145k hacked cameras. Ars Technica, 09 2016.
242. Xavier Torrent Gorjón. Protecting against relay attacks forging increased distance reports. Research Project, Universiteit van Amsterdam, 2015.
243. Louis Goubin and Jacques Patarin. Des and differential power analysis the "duplication" method. In *Cryptographic Hardware and Embedded Systems*, pages 728–728. Springer, 1999.
244. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 89–98. Acm, 2006.
245. Hannes Gross, Erich Wenger, Christoph Dobraunig, and Christoph Ehrenhfer. Ascon hardware implementations and side-channel evaluation. *Microprocessors and Microsystems*, 22(1):1–10, 2016.
246. Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici, Françcois Durvaux, Lubos Gaspar, and Stéphanie Kerckhof. SCREAM & iSCREAM, side-channel resistant authenticated encryption with masking. submission to the caesar competition, 2014.
247. Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. LS-designs: Bitslice encryption for efficient masked software implementations. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption – FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 18–37, London, UK, March 3–5, 2015. Springer.
248. Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services*, pages 31–42, 2003.
249. Christoph G Günther. A universal algorithm for homophonic coding. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 405–414. Springer, 1988.
250. Jian Guo, Jérémy Jean, Ivica Nikolic, Kexin Qiao, Yu Sasaki, and Siang Meng Sim. Invariant subspace attack against Midori64 and the resistance criteria for S-box designs. *IACR Transactions on Symmetric Cryptology*, 2016(1):33–56, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/534.
251. Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239, Santa Barbara, CA, USA, August 14–18, 2011. Springer.
252. Jian Guo, Thomas Peyrin, Axel Poschmann, and Matthew J. B. Robshaw. The LED block cipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 326–341, Nara, Japan, September 28 – October 1, 2011. Springer.

253. Matthias Hamann, Matthias Krause, and Willi Meier. LIZARD – A lightweight stream cipher for power-constrained devices. *IACR Transactions on Symmetric Cryptology*, 2017(1):45–79, 2017.
254. Gerhard P. Hancke and Markus G. Kuhn. An RFID distance bounding protocol. In *Conference on Security and Privacy for Emergency Areas in Communication Networks (SecureComm) 2005*, pages 67–73. IEEE, 2005.
255. Gerhard P Hancke and Markus G Kuhn. Attacks on time-of-flight distance bounding channels. In *ACM conference on Wireless network security*, pages 194–202. ACM, 2008.
256. Gerhard P Hancke, KE Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.
257. Lucjan Hanzlik, Łukasz Krzywiecki, and Mirosław Kutyłowski. Simplified PACE|AA protocol. In Robert H. Deng and Tao Feng, editors, *Information Security Practice and Experience - 9th International Conference, ISPEC 2013, Lanzhou, China, May 12–14, 2013. Proceedings*, volume 7863 of *Lecture Notes in Computer Science*, pages 218–232. Springer, 2013.
258. Malek Harbawi and Asaf Varol. An improved digital evidence acquisition model for the internet of things forensic i: A theoretical framework. In *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, pages 1–6, April 2017.
259. Mária Hatalová. *Security of small office home routers*. PhD thesis, Masarykova univerzita, Fakulta informatiky, 2015.
260. George Hatzivasilis, Konstantinos Fysarakis, Ioannis Papaefstathiou, and Charalampos Manifavas. A review of lightweight block ciphers. *J. Cryptographic Engineering*, 8(2):141–184, 2018.
261. Steve Heath. *Embedded systems design*. Newnes, 2002.
262. C Heffner and J Collake. Firmware mod kit-modify firmware images without recompiling, 2015.
263. Craig Heffner. binwalk – firmware analysis tool designed to assist in the analysis, extraction, and reverse engineering of firmware images. https://github.com/ReFirmLabs/binwalk.
264. Robert Hegarty, David J Lamb, and Andrew Attwood. Digital evidence challenges in the internet of things. In *Tenth International Network Conference (INC 2014)*, 2014.
265. Martin Hell, Thomas Johansson, Alexander Maximov, and Willi Meier. The grain family of stream ciphers. In *New Stream Cipher Designs*, pages 179–190. Springer, 2008.
266. Martin Hell, Thomas Johansson, Er Maximov, and Willi Meier. A stream cipher proposal: Grain-128. In *2006 IEEE International Symposium on Information Theory*, pages 1614–1618, July 2006.
267. Martin Hell, Thomas Johansson, and Willi Meier. Grain: a stream cipher for constrained environments. *IJWMC*, 2(1):86–93, 2007.
268. Martin E. Hellman. A cryptanalytic time-memory trade-off. *IEEE Trans. Information Theory*, 26(4):401–406, 1980.
269. Armijn Hemel, Karl Trygve Kalleberg, Rob Vermaas, and Eelco Dolstra. Finding Software License Violations Through Binary Code Clone Detection. In *Proceedings of the 8th Working Conference on Mining Software Repositories*, MSR '11. ACM, 2011.
270. Luca Henzen, Flavio Carbognani, Norbert Felber, and Wolfgang Fichtner. Vlsi hardware evaluation of the stream ciphers salsa20 and chacha, and the compression function rumba. In *2nd International Conference on Signals, Circuits and Systems, SCS 2008, Monastir, Tunisia, November 7–9, 2008*, pages 1–5, 2008.
271. Alex Hern. Revolv devices bricked as Google's Nest shuts down smart home company. The Guardian, April 2016. https://www.theguardian.com/technology/2016/apr/05/revolv-devices-bricked-google-nest-smart-home.
272. Julio Hernandez-Castro and David F Barrero. Evolutionary generation and degeneration of randomness to assess the indepedence of the ent test battery. In *Evolutionary Computation (CEC), 2017 IEEE Congress on*, pages 1420–1427. IEEE, 2017.
273. Julio C. Hernandez-Castro, Pedro Peris-Lopez, Raphael C.W. Phan, and Juan M. Estevez-Tapiador. Cryptanalysis of the David-Prasad RFID Ultralightweight Authentication Protocol.

In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 22–34, Istanbul, Turkey, June 2010. Springer.
274. A. Heuser, S. Picek, S. Guilley, and N. Mentens. Lightweight ciphers and their side-channel resilience. *IEEE Transactions on Computers*, PP(99):1–1, 2017.
275. Annelie Heuser, Michael Kasper, Werner Schindler, and Marc Stöttinger. A New Difference Method for Side-Channel Analysis with High-Dimensional Leakage Models. In Orr Dunkelman, editor, *CT-RSA*, volume 7178 of *Lecture Notes in Computer Science*, pages 365–382. Springer, 2012.
276. Annelie Heuser, Stjepan Picek, Sylvain Guilley, and Nele Mentens. Side-channel analysis of lightweight ciphers: Does lightweight equal easy? In *Radio Frequency Identification and IoT Security - 12th International Workshop, RFIDSec 2016, Hong Kong, China, November 30 - December 2, 2016, Revised Selected Papers*, pages 91–104, 2016.
277. Annelie Heuser, Olivier Rioul, and Sylvain Guilley. Good is Not Good Enough — Deriving Optimal Distinguishers from Communication Theory. In Lejla Batina and Matthew Robshaw, editors, *CHES*, volume 8731 of *Lecture Notes in Computer Science*. Springer, 2014.
278. Annelie Heuser, Werner Schindler, and Marc Stöttinger. Revealing side-channel issues of complex circuits by enhanced leakage models. In Wolfgang Rosenstiel and Lothar Thiele, editors, *DATE*, pages 1179–1184. IEEE, 2012.
279. Annelie Heuser and Michael Zohner. Intelligent Machine Homicide - Breaking Cryptographic Devices Using Support Vector Machines. In Werner Schindler and Sorin A. Huss, editors, *COSADE*, volume 7275 of *LNCS*, pages 249–264. Springer, 2012.
280. Hewlett Packard Enterprise (HPE). Internet of things research study – 2015 report, 2015.
281. Shoichi Hirose, Kota Ideguchi, Hidenori Kuwakado, Toru Owada, Bart Preneel, and Hirotaka Yoshida. A lightweight 256-bit hash function for hardware and low-end devices: Lesamnta-LW. In Kyung Hyune Rhee and DaeHun Nyang, editors, *ICISC 10: 13th International Conference on Information Security and Cryptology*, volume 6829 of *Lecture Notes in Computer Science*, pages 151–168, Seoul, Korea, December 1–3, 2011. Springer.
282. Deukjo Hong, Jung-Keun Lee, Dong-Chan Kim, Daesung Kwon, Kwon Ho Ryu, and Dong-Geon Lee. LEA: A 128-bit block cipher for fast encryption on common processors. In Yongdae Kim, Heejo Lee, and Adrian Perrig, editors, *WISA 13: 14th International Workshop on Information Security Applications*, volume 8267 of *Lecture Notes in Computer Science*, pages 3–27, Jeju Island, Korea, August 19–21, 2014. Springer.
283. Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bon-Seok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. HIGHT: A new block cipher suitable for low-resource device. In Louis Goubin and Mitsuru Matsui, editors, *Cryptographic Hardware and Embedded Systems – CHES 2006*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59, Yokohama, Japan, October 10–13, 2006. Springer.
284. Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 52–66, Gold Coast, Australia, December 9–13, 2001. Springer.
285. 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*, 1:293–302, 2011. 10.1007/s13389-011-0023-x.
286. Max Houck and Jay Siegel. *Fundamentals of Forensic Science*. Academic Press. Elsevier Science & Technology Books, 2015.
287. Anco Hundepool, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Eric Schulte Nordholt, Keith Spicer, and Peter-Paul De Wolf. *Statistical disclosure control*. John Wiley & Sons, 2012.
288. Darren Hurley-Smith and Julio Hernandez-Castro. Bias in the mifare desfire ev1 trng. In *Radio Frequency Identification: 12th International Workshop, RFIDsec 2016, Hong Kong, China, November 30-December 2, 2016*. Springer International Publishing, 2016.

289. Darren Hurley-Smith and Julio Hernandez-Castro. Certifiably biased: An in-depth analysis of a common criteria eal4+ certified trng. *IEEE Transactions on Information Forensics and Security*, 13(4):1031–1041, 2018.
290. IBM Marketing Cloud. 10 Key Marketing Trends for 2017 and Ideas for Exceeding Customer Expectations, 2017.
291. ICAO. Machine Readable Travel Documents - Part 11: Security Mechanism for MRTDs. Doc 9303, 2015.
292. Independen Security Evaluators. Exploiting SOHO Routers, April 2013.
293. insideBIGDATA. Guide to the Intelligent Use of Big Data on an Industrial Scale, 2017. Special Research Report.
294. Internet World Stats. Internet usage statistics, the internet big picture, 2017.
295. ISO. Iso/iec directives, part 1 – consolidated jtc 1 supplement 2017 – procedures specific to jtc 1.
296. ISO. Iso/iec directives, part 2 – principles and rules for the structure and drafting of iso and iec documents (2018).
297. Takanori Isobe, Toshihiro Ohigashi, and Masakatu Morii. Slide cryptanalysis of lightweight stream cipher rakaposhi. In *Advances in Information and Computer Security, IWSEC 2012, Fukuoka, Japan, November 7–9, 2012*, pages 138–155, 2012.
298. ISO/IEC. ISO/IEC JTC1 SC17 WG3/TF5 for ICAO: Supplemental Access Control for Machine Readable Travel Documents v1.1. Technical Report, April 15 2014.
299. Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki. MIBS: A new lightweight block cipher. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *CANS 09: 8th International Conference on Cryptology and Network Security*, volume 5888 of *Lecture Notes in Computer Science*, pages 334–348, Kanazawa, Japan, December 12–14, 2009. Springer.
300. Goce Jakimoski and Samant Khajuria. ASC-1: An authenticated encryption stream cipher. In Ali Miri and Serge Vaudenay, editors, *SAC 2011: 18th Annual International Workshop on Selected Areas in Cryptography*, volume 7118 of *Lecture Notes in Computer Science*, pages 356–372, Toronto, Ontario, Canada, August 11–12, 2012. Springer.
301. Gareth James, Daniela Witten, Trevor Hastie, and Robert Tibsihrani. *An Introduction to Statistical Learning*. Springer Texts in Statistics. Springer, 2001.
302. Joshua James and Eoghan Casey. dfrws2017-challenge. https://github.com/dfrws/dfrws2017-challenge, 2018.
303. Pieter Janssens. Proximity check for communication devices, April 2015.
304. Jérémy Jean, Ivica Nikolić, and Thomas Peyrin. Joltik v1. submission to the caesar competition, 2014.
305. Keith J. Jones, Richard Bejtlich, and Curtis W. Rose. *Real Digital Forensics: Computer Security and Incident Response*. Addison-Wesley Professional, 2005.
306. Anthony Journault, François-Xavier Standaert, and Kerem Varici. Improving the security and efficiency of block ciphers based on ls-designs. *Des. Codes Cryptography*, 82(1–2):495–509, 2017.
307. Lyndon Judge, Michael Cantrell, Cagil Kendir, and Patrick Schaumont. A modular testing environment for implementation attacks. In *2012 ASE/IEEE International Conference on BioMedical Computing (BioMedCom)*, pages 86–95, Dec 2012.
308. Ari Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.
309. Ari Juels and Stephen A Weis. Authenticating pervasive devices with human protocols. In *Advances in Cryptology–CRYPTO 2005*, pages 293–308. Springer, 2005.
310. Ari Juels and Stephen A. Weis. Authenticating pervasive devices with human protocols. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, CA, USA, August 14–18, 2005. Springer.
311. Pascal Junod. On the complexity of matsuis attack. In *Selected Areas in Cryptography, SAC 2001 Toronto, Ontario, Canada, August 1617, 2001*, pages 199–211, 2001.

312. Markus Kammerstetter, Christian Platzer, and Wolfgang Kastner. Prospect: peripheral proxying supported embedded code testing. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*, pages 329–340. ACM, 2014.
313. Orhun Kara, İmran Ergüler, and Emin Anarim. A new security relation between information rate and state size of a keystream generator. *Turkish Journal of Electrical Engineering & Computer Sciences*, 24(3):1916–1929, 2016.
314. Orhun Kara and Muhammed F. Esgin. On analysis of lightweight stream ciphers with keyed update. *IEEE Trans. Computers*, 68(1):99–110, 2019.
315. Ferhat Karakoç, Hüseyin Demirci, and A. Emre Harmanci. Itubee: A software oriented lightweight block cipher. In *Lightweight Cryptography for Security and Privacy - Second International Workshop, LightSec 2013, Gebze, Turkey, May 6–7, 2013, Revised Selected Papers*, pages 16–27, 2013.
316. Chris Karlof, Naveen Sastry, and David Wagner. Tinysec: A link layer security architecture for wireless sensor networks. In *Embedded networked sensor systems, SenSys04, Baltimore, USA, November 03–05, 2004*, pages 162–175, 2004.
317. Pierre Karpman and Benjamin Grégoire. The Littlun S-box and the fly block cipher. Lightweight Cryptography Workshop, October 17–18 2016, NIST, 2016.
318. Victor R. Kebande and Indrakshi Ray. A generic digital forensic investigation framework for internet of things (IoT). In *4th IEEE International Conference on Future Internet of Things and Cloud, FiCloud 2016, Vienna, Austria, August 22–24, 2016*, pages 356–362, 2016.
319. John Kelsey, Bruce Schneier, and David Wagner. Mod *n* cryptanalysis, with applications against RC5P and M6. In Lars R. Knudsen, editor, *Fast Software Encryption – FSE'99*, volume 1636 of *Lecture Notes in Computer Science*, pages 139–155, Rome, Italy, March 24–26, 1999. Springer.
320. John Kelsey, Bruce Schneier, and David A. Wagner. Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea. In *Information and Communication Security, First International Conference, ICICS'97, Beijing, China, November 11–14, 1997*, pages 233–246, 1997.
321. Yahya S Khiabani and Shuangqing Wei. A joint shannon cipher and privacy amplification approach to attaining exponentially decaying information leakage. *Information Sciences*, 357:6–22, 2016.
322. Yahya S Khiabani, Shuangqing Wei, Jian Yuan, and Jian Wang. Enhancement of secrecy of block ciphered systems by deliberate noise. *IEEE Transactions on Information Forensics and Security*, 7(5):1604–1613, 2012.
323. Umar Mujahid Khokhar, Muhammad Najam-ul-Islam, and Shahzad Sarwar. A new ultra-lightweight RFID authentication protocol for passive low cost tags: KMAP. *Wireless Personal Communications*, 94(3):725–744, 2017.
324. Dmitry Khovratovich and Christian Rechberger. The local attack: Cryptanalysis of the authenticated encryption scheme ale. In *Selected Areas in Cryptography, SAC 2013, Burnaby, Canada, August 14–16, 2013*, pages 174–184, 2013.
325. Handan Kilinç and Serge Vaudenay. Optimal proximity proofs revisited. In Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, and Michalis Polychronakis, editors, *ACNS 15: 13th International Conference on Applied Cryptography and Network Security*, volume 9092 of *Lecture Notes in Computer Science*, pages 478–494, New York, NY, USA, June 2–5, 2015. Springer.
326. Handan Kılınç and Serge Vaudenay. Formal analysis of distance bounding with secure hardware. Cryptology ePrint Archive, Report 2018/440, 2018.
327. Wolfgang Killmann and Werner Schindler. Ais 31: Functionality classes and evaluation methodology for true (physical) random number generators, version 3.1. *Bundesamt fur Sicherheit in der Informationstechnik (BSI), Bonn*, 2001.
328. Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID distance bounding protocol. In *Information Security and Cryptology (ICISC) 2008*, volume 5461 of *Lecture Notes in Computer Science*, pages 98–115. Springer, 2008.

329. Jaehun Kim, Stjepan Picek, Annelie Heuser, Shivam Bhasin, and Alan Hanjalic. Make some noise: Unleashing the power of convolutional neural networks for profiled side-channel analysis. Cryptology ePrint Archive, Report 2018/1023, 2018. https://eprint.iacr.org/2018/1023.
330. Aleksandar Kircanski and Amr M. Youssef. Differential fault analysis of rabbit. In *Selected Areas in Cryptography, SAC 2009, Calgary, Alberta, Canada, August 13–14, 2009*, pages 197–214, 2009.
331. Marek Klonowski, Mirosław Kutyłowski, Michał Ren, and Katarzyna Rybarczyk. Mixing in random digraphs with application to the forward-secure key evolution in wireless sensor networks. *TOSN*, 11(2):29:1–29:27, 2015.
332. Marek Klonowski and Piotr Syga. Enhancing privacy for ad hoc systems with predeployment key distribution. *Ad Hoc Networks*, 59:35–47, 2017.
333. Lars R. Knudsen, Gregor Leander, Axel Poschmann, and Matthew J. B. Robshaw. PRINTcipher: A block cipher for IC-printing. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 16–32, Santa Barbara, CA, USA, August 17–20, 2010. Springer.
334. Lars R. Knudsen and Havard Raddum. On Noekeon, 2001.
335. Çetin Kaya Koç. *Cryptographic Engineering*. Springer Publishing Company, Incorporated, 1st edition, 2008.
336. Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Advances in Cryptology Proceedings of Crypto 99*, pages 388–397. Springer-Verlag, 1999.
337. Paul Kocher, Ruby Lee, Gary McGraw, and Anand Raghunathan. Security as a new dimension in embedded system design. In *Proceedings of the 41st Annual Design Automation Conference*, DAC '04, pages 753–760, New York, NY, USA, 2004. ACM. Moderator-Ravi, Srivaths.
338. Paul C. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Proceedings of CRYPTO'96*, volume 1109 of *LNCS*, pages 104–113. Springer-Verlag, 1996.
339. Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In *Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '99, pages 388–397, London, UK, UK, 1999. Springer-Verlag.
340. Jesse D. Kornblum. Identifying Almost Identical Files Using Context Triggered Piecewise Hashing. In *Proceedings of the Digital Forensic Workshop*, 2006.
341. Karl Koscher, Tadayoshi Kohno, and David Molnar. Surrogates: enabling near-real-time dynamic analyses of embedded systems. In *Proceedings of the 9th USENIX Conference on Offensive Technologies*. USENIX Association, 2015.
342. Panayiotis Kotzanikolaou, Constantinos Patsakis, Emmanouil Magkos, and Michalis Korakakis. Lightweight private proximity testing for geospatial social networks. *Computer Communications*, 73:263–270, 2016.
343. Takuma Koyama, Yu Sasaki, and Noboru Kunihiro. Multi-differential cryptanalysis on reduced DM-PRESENT-80: Collisions and other differential properties. In Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, editors, *ICISC 12: 15th International Conference on Information Security and Cryptology*, volume 7839 of *Lecture Notes in Computer Science*, pages 352–367, Seoul, Korea, November 28–30, 2013. Springer.
344. Brian Krebs. KrebsOnSecurity Hit With Record DDoS. Krebs On Security, September 2016.
345. Brian Krebs. Who Makes the IoT Things Under Attack? Krebs On Security, October 2016.
346. Jukka M Krisp. *Progress in location-based services*. Springer, 2013.
347. J. Krumm and E. Horvitz. Locadio: inferring motion and location from wi-fi signal strengths. In *The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004.*, pages 4–13, August 2004.
348. John Krumm. *Ubiquitous Computing Fundamentals*. CRC Press, 2016.
349. Przemysław Kubiak and Mirosław Kutyłowski. Supervised usage of signature creation devices. In Dongdai Lin, Shouhuai Xu, and Moti Yung, editors, *Information Security and*

Cryptology - 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27–30, 2013, Revised Selected Papers, volume 8567 of *Lecture Notes in Computer Science*, pages 132–149. Springer, 2013.
350. Naveen Kumar, Shrikant Ojha, Kritika Jain, and Sangeeta Lal. Bean: a lightweight stream cipher. In *Security of Information and Networks, SIN 09, Famagusta, North Cyprus, October 06–10, 2009*, pages 168–171, 2009.
351. Ponnurangam Kumaraguru and Lorrie Faith Cranor. Privacy indexes: A survey of Westin's studies. Technical Report CMU-ISRI-5-138, Carnegei Mellon University, 2005.
352. Ema Kušen and Mark Strembeck. Security-related Research in Ubiquitous Computing–Results of a Systematic Literature Review. *arXiv preprint arXiv:1701.00773*, 2017.
353. Satoh Labs and Morita Tech. Sasebo/sakura project. http://satoh.cs.uec.ac.jp/SAKURA/index.html.
354. Satoh Labs and Morita Tech. Sasebo/sakura quick start source codes. http://satoh.cs.uec.ac.jp/SAKURA/hardware.html.
355. Virginie Lallemand and María Naya-Plasencia. Cryptanalysis of full Sprout. In *Advances in Cryptology – CRYPTO 2015*, volume 9215 of *LNCS*, pages 663–682. Springer, 2015.
356. Jingjing Lan, Jun Zhou, and Xin Liu. An area-efficient implementation of a message authentication code (mac) algorithm for cryptographic systems. In *TENCON 1016, Singapore, Singapore, November 22–25, 2016*, pages 601–617, 2016.
357. Marc Langheinrich. Privacy by design – principles of privacy-aware ubiquitous systems. In Gregory D. Abowd, Barry Brumitt, and Steven Shafer, editors, *Ubicomp 2001: Ubiquitous Computing*, pages 273–291. Springer, 2001.
358. Marc Langheinrich. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing*, pages 237–245. Springer, 2002.
359. Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of PRINTcipher: The invariant subspace attack. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 206–221, Santa Barbara, CA, USA, August 14–18, 2011. Springer.
360. Gregor Leander, Brice Minaud, and Sondre Rønjom. A generic approach to invariant subspace attacks: Cryptanalysis of robin, iSCREAM and Zorro. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 254–283, Sofia, Bulgaria, April 26–30, 2015. Springer.
361. Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm. New lightweight DES variants. In Alex Biryukov, editor, *Fast Software Encryption – FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 196–210, Luxembourg, Luxembourg, March 26–28, 2007. Springer.
362. Pierre L'Ecuyer and Richard Simard. Testu01: Ac library for empirical testing of random number generators. *ACM Transactions on Mathematical Software (TOMS)*, 33(4):22, 2007.
363. Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. Power analysis attack: An approach based on machine learning. *Int. J. Appl. Cryptol.*, 3(2):97–115, June 2014.
364. Liran Lerman, Gianluca Bontempi, and Olivier Markowitch. A machine learning approach against a masked AES - Reaching the limit of side-channel attacks with a learning model. *J. Cryptographic Engineering*, 5(2):123–139, 2015.
365. Liran Lerman, Stephane Fernandes Medeiros, Gianluca Bontempi, and Olivier Markowitch. A Machine Learning Approach Against a Masked AES. In *CARDIS*, Lecture Notes in Computer Science. Springer, November 2013. Berlin, Germany.
366. Liran Lerman, Stephane Fernandes Medeiros, Nikita Veshchikov, Cédric Meuter, Gianluca Bontempi, and Olivier Markowitch. Semi-supervised template attack. In Emmanuel Prouff, editor, *COSADE 2013, Paris, France, 2013, Revised Selected Papers*, pages 184–199. Springer, 2013.
367. Liran Lerman, Romain Poussier, Gianluca Bontempi, Olivier Markowitch, and François-Xavier Standaert. Template attacks vs. machine learning revisited (and the curse of dimensionality in side-channel analysis). In Stefan Mangard and Axel Y. Poschmann, editors, *Constructive Side-Channel Analysis and Secure Design - 6th International Workshop,*

COSADE 2015, Berlin, Germany, April 13–14, 2015. Revised Selected Papers, volume 9064 of *Lecture Notes in Computer Science*, pages 20–33. Springer, 2015.
368. Gaëtan Leurent. Differential forgery attack against lac. In *Selected Areas in Cryptography, SAC 2015, Sackville, Canada, August 12–14, 2015*, pages 217–224, 2016.
369. Gaëtan Leurent. Improved differential-linear cryptanalysis of 7-round chaskey with partitioning. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 344–371, Vienna, Austria, May 8–12, 2016. Springer.
370. T. Li, H. Wu, X. Wang, and F. Bao. Sensec design. i^2r sensor network flagship project (snfp: security part): Technical report-tr v1.0, 2005.
371. Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. Conditional cube attack on round-reduced ascon. *IACR Trans. Symmetric Cryptol.*, 2017(1):175–202, 2017.
372. Chae Hoon Lim and Tymur Korkishko. mCrypton - a lightweight block cipher for security of low-cost RFID tags and sensors. In Jooseok Song, Taekyoung Kwon, and Moti Yung, editors, *WISA 05: 6th International Workshop on Information Security Applications*, volume 3786 of *Lecture Notes in Computer Science*, pages 243–258, Jeju Island, Korea, August 22–24, 2006. Springer.
373. Li Lin, Wenling Wu, and Yafei Zheng. Automatic search for key-bridging technique: Applications to LBlock and TWINE. In Thomas Peyrin, editor, *Fast Software Encryption – FSE 2016*, volume 9783 of *Lecture Notes in Computer Science*, pages 247–267, Bochum, Germany, March 20–23, 2016. Springer.
374. Jigang Liu. Iot forensics issues, strategies, and challenges. In *A presentation at 12th IDF Annual Conference*, 2015.
375. Yifei Liu, Timo Kasper, Kerstin Lemke-Rust, and Christof Paar. E-passport: Cracking basic access control keys. In Robert Meersman and Zahir Tari, editors, *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS, OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS 2007, Vilamoura, Portugal, November 25–30, 2007, Proceedings, Part II*, volume 4804 of *Lecture Notes in Computer Science*, pages 1531–1547. Springer, 2007.
376. Yunwen Liu, Glenn De Witte, Adrin Ranea, and Tomer Ashur. Rotational-xor cryptanalysis of reduced-round speck. *IACR Transactions on Symmetric Cryptology*, 2017(3):24–36, Sep. 2017.
377. Yunwen Liu, Qingju Wang, and Vincent Rijmen. Automatic search of linear trails in ARX with applications to SPECK and chaskey. In Mark Manulis, Ahmad-Reza Sadeghi, and Steve Schneider, editors, *ACNS 16: 14th International Conference on Applied Cryptography and Network Security*, volume 9696 of *Lecture Notes in Computer Science*, pages 485–499, Guildford, UK, June 19–22, 2016. Springer.
378. Zongbin Liu, Qinglong Zhang, Cunqing Ma, Changting Li, and Jiwu Jing. Hpaz: a high-throughput pipeline architecture of zuc in hardware. In *Design, Automation & Test in Europe, DATE 2016, Dresden, Germany, March 14–18, 2016*, pages 269–272, 2016.
379. NXP Semiconductors Ltd. *MF1PLUSx0y1 Public Datasheet*. NXP Semiconductors.
380. Jiqiang Lu. Related-key rectangle attack on 36 rounds of the XTEA block cipher. *Int. J. Inf. Sec.*, 8(1):1–11, 2009.
381. Yi Lu, Willi Meier, and Serge Vaudenay. The conditional correlation attack: a practical attack on bluetooth encryption. In *Advances in Cryptology CRYPTO 2005, Santa Barbara, California, USA, August 14–18, 2005*, pages 97–117, 2005.
382. Mark Luk, Ghita Mezzour, Adrian Perrig, and Virgil Gligor. Minisec: A secure sensor network communication architecture. In *6th International Symposium on Information Processing in Sensor Networks, IPSN 2007, Cambridge, MA, USA, April 25–27, 2007*, pages 479–488, 2007.
383. Hanguang Luo, Guangjun Wen, Jian Su, and Zhong Huang. SLAP: succinct and lightweight authentication protocol for low-cost RFID system. *Wireless Networks*, 24(1):69–78, 2018.

384. Atul Luykx, Bart Preneel, Elmar Tischhauser, and Kan Yasuda. A MAC mode for lightweight block ciphers. In Thomas Peyrin, editor, *Fast Software Encryption – FSE 2016*, volume 9783 of *Lecture Notes in Computer Science*, pages 43–59, Bochum, Germany, March 20–23, 2016. Springer.
385. Zhen Ma, Tian Tian, and Wen-Feng Qi. Internal state recovery of Grain v1 employing guess-and-determine attack. *IET Information Security*, 11(6):363–368, 2017.
386. Houssem Maghrebi, Thibault Portigliatti, and Emmanuel Prouff. Breaking cryptographic implementations using deep learning techniques. In *Security, Privacy, and Applied Cryptography Engineering - 6th International Conference, SPACE 2016, Hyderabad, India, December 14–18, 2016, Proceedings*, pages 3–26, 2016.
387. Subhamoy Maitra, Santanu Sarkar, Anubhab Baksi, and Pramit Dey. Key recovery from state information of Sprout: Application to cryptanalysis and fault attack. Cryptology ePrint Archive, Report 2015/236.
388. Hamid Mala, Mohammad Dakhilalian, and Mohsen Shakiba. Cryptanalysis of mcrypton - A lightweight block cipher for security of RFID tags and sensors. *Int. J. Communication Systems*, 25(4):415–426, 2012.
389. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. Springer, December 2006. ISBN 0-387-30857-1, http://www.dpabook.org/.
390. Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security)*. Springer, feb 2007.
391. Charalampos Manifavas, George Hatzivasilis, Konstantinos Fysarakis, and Yannis Papaefstathiou. A survey of lightweight stream ciphers for embedded systems. *Security and Communication Networks*, 9(10):1226–1246, 2016.
392. Konstantinos Markantonakis, Lishoy Francis, Gerhard Hancke, and Keith Mayes. Practical relay attack on contactless transactions by using nfc mobile phones. *Radio Frequency Identification System Security: RFIDsec*, 12:21, 2012.
393. George Marsaglia. Diehard, a battery of tests for random number generators. *CD-ROM, Department of Statistics and Supercomputer Computations Research Institute, Florida State University, USA*, 1995.
394. George Marsaglia. The marsaglia random number cdrom including the diehard battery of tests of randomness, 1995.
395. Antoni Martínez-Ballesté, Pablo A. Pérez-Martínez, and Agusti Solanas. The pursuit of citizens' privacy: A privacy-aware smart city is possible. *IEEE Communications Magazine*, 51(6):136–141, 2013.
396. Kinga Marton and Alin Suciu. On the interpretation of results from the nist statistical test suite. *Science and Technology*, 18(1):18–32, 2015.
397. James L Massey. Some applications of source coding in cryptography. *Transactions on Emerging Telecommunications Technologies*, 5(4):421–430, 1994.
398. Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *Fast Software Encryption – FSE'97*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68, Haifa, Israel, January 20–22, 1997. Springer.
399. Tsutomu Matsumoto, Shinichi Kawamura, Kouichi Fujisaki, Naoya Torii, Shuichi Ishida, Yukiyasu Tsunoo, Minoru Saeki, and Atsuhiro Yamagishi. Tamper-resistance standarization research committee report. The 2006 Symposium on Cryptography and Information Security, 2006.
400. Tobias Matzner. Why privacy is not enough privacy in the context of "ubiquitous computing" and "big data". *Journal of Information, Communication and Ethics in Society*, 12(2):93–106, 2014.
401. S. Mauw, Z. Smith, J. Toro-Pozo, and R. Trujillo-Rasua. Distance-bounding protocols: Verification without time and location. In *IEEE Symposium on Security and Privacy*, volume 00, pages 152–169, 2018.

402. Rita Mayer-Sommer. Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards. In *CHES*, volume 1965 of *LNCS*, pages 78–92. Springer, May 14–16 2001. http://citeseer.nj.nec.com/mayer-sommer01smartly.html.
403. BD McCullough. A review of testu01. *Journal of Applied Econometrics*, 21(5):677–682, 2006.
404. Kerry A. McKay, Larry Bassham, Meltem Sönmez Turan, and Nicky Mouha. Nistir 8114 - report on lightweight cryptography, 2016.
405. Christopher Meffert, Devon Clark, Ibrahim Baggili, and Frank Breitinger. Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition. In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, pages 56:1–56:11, New York, NY, USA, 2017. ACM.
406. Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. The tamarin prover for the symbolic analysis of security protocols. In *International Conference on Computer Aided Verification*, CAV'13, pages 696–701. Springer, 2013.
407. Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini. A common criteria based security requirements engineering process for the development of secure information systems. *Computer standards & interfaces*, 29(2):244–253, 2007.
408. Imran Memon, Qasim Ali Arain, Muhammad Hammad Memon, Farman Ali Mangi, and Rizwan Akhtar. Search me if you can: Multiple mix zones with location privacy protection for mapping services. *International Journal of Communication Systems*, 30(16), 2017.
409. Nele Mentens, Jan Genoe, Bart Preneel, and Ingrid Verbauwhede. A low-cost implementation of Trivium. In *SASC 2008*, pages 197–204, 2008.
410. Thomas S. Messerges. Using Second-Order Power Analysis to Attack DPA Resistant Software. In *CHES*, volume 1965 of *LNCS*, pages 238–251. Springer-Verlag, August 17–18 2000. Worcester, MA, USA.
411. Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Investigations of power analysis attacks on smartcards. In *Proceedings of the USENIX Workshop on Smartcard Technology on USENIX Workshop on Smartcard Technology*, WOST'99, pages 17–17, Berkeley, CA, USA, 1999. USENIX Association.
412. Thomas S. Messerges, Ezzy A. Dabbish, and Robert H. Sloan. Power Analysis Attacks of Modular Exponentiation in Smartcards. In Çetin Kaya Koç and Christof Paar, editors, *CHES*, volume 1717 of *LNCS*, pages 144–157. Springer, 1999.
413. Miodrag J Mihaljevic. A framework for stream ciphers based on pseudorandomness, randomness and coding. In *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, pages 117–139. IOS Press, Amsterdam, The Netherlands, 2009.
414. Miodrag J Mihaljević. An approach for light-weight encryption employing dedicated coding. In *Global Communications Conference, 2012 IEEE*, pages 874–880. IEEE, 2012.
415. Miodrag J. Mihaljevic, Sugata Gangopadhyay, Goutam Paul, and Hideki Imai. Generic cryptographic weakness of k-normal boolean functions in certain stream ciphers and cryptanalysis of grain-128. *Periodica Mathematica Hungarica*, 65(2):205–227, 2012.
416. Miodrag J. Mihaljevic, Sugata Gangopadhyay, Goutam Paul, and Hideki Imai. Internal state recovery of grain-v1 employing normality order of the filter function. *IET Information Security*, 6(2):55–64, 2012.
417. Miodrag J. Mihaljevic, Sugata Gangopadhyay, Goutam Paul, and Hideki Imai. Internal state recovery of keystream generator LILI-128 based on a novel weakness of the employed boolean function. *Inf. Process. Lett.*, 112(21):805–810, 2012.
418. Miodrag J Mihaljević and Hideki Imai. An approach for stream ciphers design based on joint computing over random and secret data. *Computing*, 85(1–2):153–168, 2009.
419. Miodrag J Mihaljević and Hideki Imai. Employment of homophonic coding for improvement of certain encryption approaches based on the lpn problem. In *Symmetric Key Encryption Workshop, SKEW*, pages 16–17, 2011.
420. Miodrag J Mihaljević and Frédérique Oggier. Security evaluation and design elements for a class of randomised encryptions. *IET Information Security*, 13(1):36–47, 2019.

421. Vasily Mikhalev, Frederik Armknecht, and Christian Müller. On ciphers that continuously access the non-volatile key. *IACR Transactions on Symmetric Cryptology*, 2016(2):52–79, 2016. http://tosc.iacr.org/index.php/ToSC/article/view/565.
422. Vasily Mikhalev, Frederik Armknecht, and Christian Müller. On ciphers that continuously access the non-volatile key. *IACR Transactions on Symmetric Cryptology*, 2016(2):52–79, 2017.
423. Thomas M. Mitchell. *Machine Learning*. McGraw-Hill, Inc., New York, NY, USA, 1 edition, 1997.
424. Seyyed Mohamamd Reza Moosavi and Abolghasem Sadeghi-Niaraki. A survey of smart electrical boards in ubiquitous sensor networks for geomatics applications. *The International Archives of Photogrammetry, Remote Sensing and Spatial Information Sciences*, 40(1):503, 2015.
425. Amir Moradi. Statistical tools flavor side-channel collision attacks. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 428–445. Springer, 2012.
426. Amir Moradi, Axel Poschmann, San Ling, Christof Paar, and Huaxiong Wang. Pushing the limits: A very compact and a threshold implementation of AES. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 69–88, Tallinn, Estonia, May 15–19, 2011. Springer.
427. Athanassios Moschos, Apostolos P. Fournaris, and Odysseas Koufopavlou. A flexible leakage trace collection setup for arbitrary cryptographic ip cores. In *2018 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 138–142, April 2018.
428. Nicky Mouha, Bart Mennink, Anthony Van Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede. Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In Antoine Joux and Amr M. Youssef, editors, *SAC 2014: 21st Annual International Workshop on Selected Areas in Cryptography*, volume 8781 of *Lecture Notes in Computer Science*, pages 306–323, Montreal, QC, Canada, August 14–15, 2014. Springer.
429. Marius Muench, Dario Nisi, Aurélien Francillon, and Davide Balzarotti. Avatar2: A Multi-target Orchestration Platform. In *Workshop on Binary Analysis Research (colocated with NDSS Symposium)*, BAR 18, February 2018.
430. Marius Muench, Jan Stijohann, Frank Kargl, Aurélien Francillon, and Davide Balzarotti. What you corrupt is not what you crash: Challenges in fuzzing embedded devices. In *ISOC NDSS 2018*, 2018.
431. Umar Mujahid, Muhammad Najam-ul Islam, and Ali Shami. RCIA: A new ultralightweight RFID authentication protocol using recursive hashing. *International Journal of Distributed Sensor Networks*, December 2014.
432. Frédéric Muller. Differential attacks against the helix stream cipher. In *Fast Software Encryption,FSE 2004, Delhi, India, February 5–7 , 2004*, pages 94–108, 2004.
433. Kiran-Kumar Muniswamy-Reddy, David A. Holland, Uri Braun, and Margo Seltzer. Provenance-aware storage systems. In *Proceedings of the Annual Conference on USENIX '06 Annual Technical Conference*, ATEC '06, pages 4–4, Berkeley, CA, USA, 2006. USENIX Association.
434. Radu Muresan and Stefano Gregori. Protection Circuit against Differential Power Analysis Attacks for Smart Cards. *IEEE Trans. Computers*, 57(11):1540–1549, 2008.
435. Mara Naya-Plasencia and Thomas Peyrin. Practical cryptanalysis of armadillo2. In *Fast Software Encryption,FSE 2012, Washington, DC, USA, March 19–21, 2012*, pages 146–162, 2012.
436. Roger M. Needham and David J. Wheeler. Tea extensions. Technical report, Computer Laboratory, University of Cambridge, 1997.
437. Irene C. L. Ng and Susan Y. L. Wakenshaw. The internet-of-things: Review and research directions. *International Journal of Research in Marketing*, 34(1):3–21, 2017.
438. David H. Nguyen and Gillian R. Hayes. Information privacy in institutional and end-user tracking and recording technologies. *Personal and Ubiquitous Computing*, 14(1):53–72, 2010.

439. Marcus Niemietz and Jörg Schwenk. Owning your home network: Router security revisited. In *9th Workshop on Web 2.0 Security and Privacy (W2SP) 2015*, 2015.
440. Ana Nieto, Ruben Rios, and Javier Lopez. A methodology for privacy-aware iot-forensics. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pages 626–633, Aug 2017.
441. Ana Nieto, Ruben Rios, and Javier Lopez. Iot-forensics meets privacy: Towards cooperative digital investigations. *Sensors*, 18(2), 2018.
442. Ana Nieto, Rodrigo Roman, and Javier López. Digital witness: Safeguarding digital evidence by using secure architectures in personal devices. *IEEE Network*, 30(6):34–41, 2016.
443. Ivica Nikolic, Lei Wang, and Shuang Wu. Cryptanalysis of round-reduced \mathttled. In *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11–13, 2013. Revised Selected Papers*, pages 112–129, 2013.
444. NIST. Cryptographic standards and guidelines: Aes development. https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines/Archived-Crypto-Projects/AES-Development.
445. NXP. Nxp mifare plus ev1 – latest features on highest security level scalable – flexible – future proof, April 2016.
446. NXP. Nxp mifare desfire ev2 – contactless IC for next-generation, multi-application solutions in smart cities, May 2018.
447. Johannes Obermaier and Stefan Tatschner. Shedding too much light on a microcontroller's firmware protection. In *11th USENIX Workshop on Offensive Technologies (WOOT 17)*, Vancouver, BC, 2017. USENIX Association.
448. National Institute of Standards and Technology. *NIST SP800-22 Revision 1a – A Statistical Test Suite for Random And Pseudorandom Number Generators for Cryptographic Applications*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf 16:53 21/05/2018.
449. National Institute of Standards and Technology. *NIST SP800-90 B – Reccommendation for the Entropy Sources used for Random Bit Generation*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf 17:33 21/05/2018.
450. Colin O'Flynn. Chipwhisperer. https://wiki.newae.com/Main_Page.
451. Colin O'Flynn and Zhizhang (David) Chen. *ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research*, pages 243–260. Springer International Publishing, Cham, 2014.
452. Frédérique Oggier and Miodrag J Mihaljević. An information-theoretic security evaluation of a class of randomized encryption schemes. *IEEE Transactions on Information Forensics and Security*, 9(2):158–168, 2014.
453. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
454. Femi Olumofin, Piotr K. Tysowski, Ian Goldberg, and Urs Hengartner. Achieving efficient query privacy for location based services. In Mikhail J. Atallah and Nicholas J. Hopper, editors, *Privacy Enhancing Technologies*, pages 93–110. Springer, 2010.
455. Edewede Oriwoh, David Jazani, Gregory Epiphaniou, and Paul Sant. Internet of things forensics: Challenges and approaches. In *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Austin, TX, USA, October 20–23, 2013*, pages 608–615, 2013.
456. Edewede Oriwoh and Paul Sant. The forensics edge management system: A concept and design. In *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, UIC/ATC 2013, Vietri sul Mare, Sorrento Peninsula, Italy, December 18–21, 2013*, pages 544–550, 2013.
457. Khaled Ouafi, Raphael Overbeck, and Serge Vaudenay. On the security of HB# against a man-in-the-middle attack. In Josef Pieprzyk, editor, *Advances in Cryptology – ASIACRYPT 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 108–124, Melbourne, Australia, December 7–11, 2008. Springer.

458. Khaled Ouafi and Serge Vaudenay. Smashing SQUASH-0. In Antoine Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, volume 5479 of *Lecture Notes in Computer Science*, pages 300–312, Cologne, Germany, April 26–30, 2009. Springer.
459. Achilleas Papageorgiou, Michael Strigkos, Eugenia A. Politou, Efthimios Alepis, Agusti Solanas, and Constantinos Patsakis. Security and privacy analysis of mobile health applications: The alarming state of practice. *IEEE Access*, 6:9390–9403, 2018.
460. Constantinos Patsakis, Panayiotis Kotzanikolaou, and Mélanie Bouroche. Private proximity testing on steroids: An ntru-based protocol. In *Security and Trust Management - 11th International Workshop, STM 2015, Vienna, Austria, September 21–22, 2015, Proceedings*, pages 172–184, 2015.
461. Pablo A. Pérez-Martínez and Agusti Solanas. W3-privacy: the three dimensions of user privacy in lbs. In *12th ACM Intl. Symp. Mobile Ad Hoc Networking and Computing*, 2011.
462. Pablo A. Pérez-Martínez, Agusti Solanas, and Antoni Martínez-Ballesté. Location Privacy Through Users' Collaboration: A Distributed Pseudonymizer. In *Proceedings of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, pages 338–341, 2009.
463. Pedro Peris-Lopez, Julio Hernandez-Castro, Juan M. Estévez-Tapiador, and Arturo Ribagorda. Advances in ultralightweight cryptography for low-cost RFID tags: Gossamer protocol. In Kyo-Il Chung, Kiwook Sohn, and Moti Yung, editors, *WISA 08: 9th International Workshop on Information Security Applications*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68, Jeju Island, Korea, September 23–25, 2009. Springer.
464. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, Tieyan Li, and Jan C.A. van der Lubbe. Weaknesses in Two Recent Lightweight RFID Authentication Protocols. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
465. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. EMAP: An Efficient Mutual Authentication Protocol for Low-Cost RFID Tags. In *OTM Federated Conferences and Workshop: IS Workshop – IS'06*, volume 4277 of *Lecture Notes in Computer Science*, pages 352–361, Montpellier, France, November 2006. Springer.
466. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
467. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags. In Jianhua Ma, Hai Jin, Laurence Tianruo Yang, and Jeffrey J. P. Tsai, editors, *International Conference on Ubiquitous Intelligence and Computing – UIC'06*, volume 4159 of *Lecture Notes in Computer Science*, pages 912–923, Wuhan and Three Gorges, China, September 2006. Springer.
468. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Raphael C.-W. Phan, Juan M. E. Tapiador, and Tieyan Li. Quasi-Linear Cryptanalysis of a Secure RFID Ultralightweight Authentication Protocol. In *6th China International Conference on Information Security and Cryptology – Inscrypt'10*, Shanghai, China, October 2010. Springer.
469. Léo Perrin and Dmitry Khovratovich. Collision spectrum, entropy loss, T-sponges, and cryptanalysis of GLUON-64. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption – FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 82–103, London, UK, March 3–5, 2015. Springer.
470. Sundresan Perumal, Norita M. Norwawi, and Valliappan Raman. Internet of things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, pages 19–23, Oct 2015.
471. Petter Pessl and Michael Hutter. Pushing the limits of sha-3 hardware implementations to fit on rfid. In *Cryptographic Hardware and Embedded Systems, CHES 2013, Santa Barbara, CA, USA, August 20–23, 2013*, pages 126–141, 2013.

472. Christophe Petit and Jean-Jacques Quisquater. Cryptographic hash functions and expander graphs: The end of the story? In *The New Codebreakers - Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*, pages 304–311, 2016.
473. Raphael C.-W. Phan. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol - SASI. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2008.
474. Raphael C.-W. Phan and Adi Shamir. Improved related-key attacks on desx and desx+. *Cryptologia*, 32(1):13–22, 2008.
475. Stjepan Picek, Annelie Heuser, Cesare Alippi, and Francesco Regazzoni. When theory meets practice: A framework for robust profiled side-channel analysis. Cryptology ePrint Archive, Report 2018/1123, 2018. https://eprint.iacr.org/2018/1123.
476. Stjepan Picek, Annelie Heuser, and Sylvain Guilley. Template attack versus bayes classifier. *Journal of Cryptographic Engineering*, 7(4):343–351, Nov 2017.
477. Stjepan Picek, Annelie Heuser, Alan Jovic, Lejla Batina, and Axel Legay. The secrets of profiling for side-channel analysis: feature selection matters. *IACR Cryptology ePrint Archive*, 2017:1110, 2017.
478. Stjepan Picek, Annelie Heuser, Alan Jovic, Shivam Bhasin, and Francesco Regazzoni. The curse of class imbalance and conflicting metrics with machine learning for side-channel evaluations. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(1):209–237, Nov. 2018.
479. Stjepan Picek, Annelie Heuser, Alan Jovic, and Axel Legay. Climbing down the hierarchy: Hierarchical classification for machine learning side-channel attacks. In Marc Joye and Abderrahmane Nitaj, editors, *Progress in Cryptology - AFRICACRYPT 2017: 9th International Conference on Cryptology in Africa, Dakar, Senegal, May 24–26, 2017, Proceedings*, pages 61–78, Cham, 2017. Springer International Publishing.
480. Stjepan Picek, Annelie Heuser, Alan Jovic, Axel Legay, and Karlo Knezevic. Profiled sca with a new twist: Semi-supervised learning. Cryptology ePrint Archive, Report 2017/1085, 2017. https://eprint.iacr.org/2017/1085.
481. Stjepan Picek, Annelie Heuser, Alan Jovic, Simone A. Ludwig, Sylvain Guilley, Domagoj Jakobovic, and Nele Mentens. Side-channel analysis and machine learning: A practical perspective. In *2017 International Joint Conference on Neural Networks, IJCNN 2017, Anchorage, AK, USA, May 14–19, 2017*, pages 4095–4102, 2017.
482. Stjepan Picek, Ioannis Petros Samiotis, Jaehun Kim, Annelie Heuser, Shivam Bhasin, and Axel Legay. On the performance of convolutional neural networks for side-channel analysis. In Anupam Chattopadhyay, Chester Rebeiro, and Yuval Yarom, editors, *Security, Privacy, and Applied Cryptography Engineering*, pages 157–176, Cham, 2018. Springer International Publishing.
483. Ameer Pichan, Mihai Lazarescu, and Sie Teng Soh. Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, 13:38–57, 2015.
484. Aniket Pingley, Nan Zhang, Xinwen Fu, Hyeong-Ah Choi, Suresh Subramaniam, and Wei Zhao. Protection of query privacy for continuous location based services. In *INFOCOM 2011. 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies, 10–15 April 2011, Shanghai, China*, pages 1710–1718, 2011.
485. Gilles Piret, Thomas Roche, and Claude Carlet. PICARO - a block cipher allowing efficient higher-order side-channel resistance. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *ACNS 12: 10th International Conference on Applied Cryptography and Network Security*, volume 7341 of *Lecture Notes in Computer Science*, pages 311–328, Singapore, June 26–29, 2012. Springer.
486. Eugenia Politou, Efthimios Alepis, and Constantinos Patsakis. Forgetting personal data and revoking consent under the gdpr: Challenges and proposed solutions. *Journal of Cybersecurity*, page tyy001, 2018.

487. Axel Poschmann, San Ling, and Huaxiong Wang. 256 bit standardized crypto for 650 GE - GOST revisited. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 219–233, Santa Barbara, CA, USA, August 17–20, 2010. Springer.
488. David Martin Ward Powers. Evaluation: from precision, recall and f-factor to roc, informedness, markedness and correlation, 2007.
489. Sihang Pu, Yu Yu, Weijia Wang, Zheng Guo, Junrong Liu, Dawu Gu, Lingyun Wang, and Jie Gan. Trace augmentation: What can be done even before preprocessing in a profiled sca? In Thomas Eisenbarth and Yannick Teglia, editors, *Smart Card Research and Advanced Applications*, pages 232–247, Cham, 2018. Springer International Publishing.
490. Kexin Qiao, Lei Hu, and Siwei Sun. Differential security evaluation of simeck with dynamic key-guessing techniques. Cryptology ePrint Archive, Report 2015/902, 2015. http://eprint.iacr.org/2015/902.
491. Lingyue Qin, Huaifeng Chen, and Xiaoyun Wang. Linear hull attack on round-reduced simeck with dynamic key-guessing techniques. In Joseph K. Liu and Ron Steinfeld, editors, *ACISP 16: 21st Australasian Conference on Information Security and Privacy, Part II*, volume 9723 of *Lecture Notes in Computer Science*, pages 409–424, Melbourne, VIC, Australia, July 4–6, 2016. Springer.
492. Cai Qingling, Zhan Yiju, and Wang Yonghua. A Minimalist Mutual Authentication Protocol for RFID System & BAN Logic Analysis. In *ISECS International Colloquium on Computing, Communication, Control, and Management – CCCM'08.*, volume 2, pages 449–453, August 2008.
493. Jean-Jacques Quisquater and David Samyde. Electromagnetic analysis (ema): Measures and counter-measures for smart cards. In Isabelle Attali and Thomas Jensen, editors, *Smart Card Programming and Security*, pages 200–210. Springer, 2001.
494. KM Sabidur Rahman, Matt Bishop, and Albert Holt. Internet of things mobility forensics. *Researchgate. net*, 2017.
495. Rambus. Dpa workstation testing platform. http://info.rambus.com/hubfs/rambus.com/Gated-Content/Cryptography/DPA-Workstation-Product-Brief.pdf.
496. Kasper Bonne Rasmussen and Srdjan Čapkun. Location privacy of distance bounding protocols. In *Conference on Computer and Communications Security (CCS)*, pages 149–160. ACM, 2008.
497. Shahram Rasoolzadeh, Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. An improved truncated differential cryptanalysis of KLEIN. *Tatra Mountains Mathematical Publications*, 67:135–147, 2017.
498. Christian Rechberger and Elisabeth Oswald. Practical Template Attacks. In *WISA*, volume 3325 of *LNCS*, pages 443–457. Springer, August 23-25 2004. Jeju Island, Korea.
499. Michał Ren, Tanmoy Kanti Das, and Jianying Zhou. Diverging keys in wireless sensor networks. In Sokratis K. Katsikas, Javier López, Michael Backes, Stefanos Gritzalis, and Bart Preneel, editors, *Information Security, 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2, 2006, Proceedings*, volume 4176 of *Lecture Notes in Computer Science*, pages 257–269. Springer, 2006.
500. Mathieu Renauld, François-Xavier Standaert, Nicolas Veyrat-Charvillon, Dina Kamel, and Denis Flandre. A formal study of power variability issues and side-channel attacks for nanoscale devices. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 109–128. Springer, 2011.
501. Riscure. Inspector: The side channel test tool. https://www.riscure.com/security-tools/inspector-sca/.
502. Ronald L. Rivest. The RC5 encryption algorithm. In Bart Preneel, editor, *Fast Software Encryption – FSE'94*, volume 1008 of *Lecture Notes in Computer Science*, pages 86–96, Leuven, Belgium, December 14–16, 1995. Springer.
503. Ronald L Rivest and Alan T Sherman. Randomized encryption techniques. In *Advances in Cryptology*, pages 145–163. Springer, 1983.

504. Phillip Rogaway, Mihir Bellare, and John Black. Ocb: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security*, 6(3):365–403, 2003.
505. Michael Roland, Josef Langer, and Josef Scharinger. Applying relay attacks to google wallet. In *Near Field Communication (NFC), 2013 5th International Workshop on*, pages 1–6. IEEE, 2013.
506. John D. Roth, Murali Tummala, John C. McEachen, and James W. Scrofani. On location privacy in LTE networks. *IEEE Trans. Information Forensics and Security*, 12(6):1358–1368, 2017.
507. Vassil Roussev. Data Fingerprinting with Similarity Digests. In *IFIP International Conference on Digital Forensics*, pages 207–226, 2010.
508. Andrew Rukhin, Juan Soto, and James Nechvatal. A statistical test suite for random and pseudorandom number generators for cryptographic applications. nist dtic document. *NIST SP800-22*, 2010.
509. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, and Elaine Barker. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, DTIC Document, 2001.
510. Alexander Russell, Qiang Tang, Moti Yung, and Hong-Sheng Zhou. Cliptography: Clipping the power of kleptographic attacks. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 34–64, 2016.
511. Karmakar Sandip, Mukhopadhyay Debdeep, and Roy Chowdhury Dipanwita. Cavium strengthening trivium stream cipher using cellular automata. *Journal of Cellular Automata*, 7(2):179–197, 2012.
512. Yu Sasaki and Yosuke Todo. New differential bounds and division property of Lilliput: Block cipher with extended generalized Feistel network. In Roberto Avanzi and Howard M. Heys, editors, *SAC 2016: 23rd Annual International Workshop on Selected Areas in Cryptography*, volume 10532 of *Lecture Notes in Computer Science*, pages 264–283, St. John's, NL, Canada, August 10–12, 2016. Springer.
513. Florian Schaub, Bastian Könings, and Michael Weber. Context-adaptive privacy: Leveraging context awareness to support privacy decision making. *IEEE Pervasive Computing*, 14(1):34–43, 2015.
514. Werner Schindler and Wolfgang Killmann. Evaluation criteria for true (physical) random number generators used in cryptographic applications. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 431–449. Springer, 2002.
515. Werner Schindler, Kerstin Lemke, and Christof Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In LNCS, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005. Edinburgh, Scotland, UK.
516. Tobias Schneider and Amir Moradi. Leakage assessment methodology. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 495–513. Springer, 2015.
517. Friedhelm Schwenker and Edmondo Trentin. Pattern classification and clustering: A review of partially supervised learning approaches. *Pattern Recognition Letters*, 37:4–14, 2014.
518. Jaydip Sen. Ubiquitous computing: Potentials and challenges. *arXiv preprint arXiv:1011.1960*, 2010.
519. Mohammad Hossein Faghihi Sereshgi, Mohammad Dakhilalian, and Mohsen Shakiba. Biclique cryptanalysis of MIBS-80 and PRESENT-80 block ciphers. *Security and Communication Networks*, 9(1):27–33, 2016.
520. Adi Shamir. SQUASH - a new MAC with provable security properties for highly constrained devices such as RFID tags. In Kaisa Nyberg, editor, *Fast Software Encryption – FSE 2008*, volume 5086 of *Lecture Notes in Computer Science*, pages 144–157, Lausanne, Switzerland, February 10–13, 2008. Springer.

521. Jinyong Shan, Lei Hu, Ling Song, Siwei Sun, and Xiaoshuang Ma. Related-key differential attack on round reduced RECTANGLE-80. Cryptology ePrint Archive, Report 2014/986, 2014. http://eprint.iacr.org/2014/986.
522. Claude Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.
523. Danping Shi, Lei Hu, Siwei Sun, Ling Song, Kexin Qiao, and Xiaoshuang Ma. Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. Cryptology ePrint Archive, Report 2014/973, 2014. http://eprint.iacr.org/2014/973.
524. Zhenqing Shi, Xiutao Feng, Dengguo Feng, and Chuankun Wu. A real-time key recovery attack on the lightweight stream cipher a2u2. In *Cryptology and Network Security, CANS 2012, Darmstadt, Germany, December 12-14, 2012*, pages 12–22, 2012.
525. Zhenqing Shi, Bin Zhang, and Dengguo Feng. Practical-time related-key attack on hummingbird-2. *IET Information Security*, 9(6):321–327, 2015.
526. Kyoji Shibutani, Takanori Isobe, Harunaga Hiwatari, Atsushi Mitsuda, Toru Akishita, and Taizo Shirai. Piccolo: An ultra-lightweight blockcipher. In Bart Preneel and Tsuyoshi Takagi, editors, *Cryptographic Hardware and Embedded Systems – CHES 2011*, volume 6917 of *Lecture Notes in Computer Science*, pages 342–357, Nara, Japan, September 28 – October 1, 2011. Springer.
527. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, and Tetsu Iwata. The 128-bit blockcipher CLEFIA (extended abstract). In Alex Biryukov, editor, *Fast Software Encryption – FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195, Luxembourg, Luxembourg, March 26–28, 2007. Springer.
528. Yan Shoshitaishvili, Ruoyu Wang, Christophe Hauser, Christopher Kruegel, and Giovanni Vigna. Firmalice-automatic detection of authentication bypass vulnerabilities in binary firmware. In *NDSS*, 2015.
529. O. Shwartz, Y. Mathov, M. Bohadana, Y. Oren, and Y. Elovici. Reverse engineering iot devices: Effective techniques and methods. *IEEE Internet of Things Journal*, pages 1–1, 2018.
530. Siang Meng Sim and Lei Wang. Practical forgery attacks on scream and iscream. http://www1.spms.ntu.edu.sg/~syllab/m/images/b/b3/ForgeryAttackonSCREAM.pdf.
531. Mridula Singh, Patrick Leu, and Srdjan Capkun. UWB with pulse reordering: Securing ranging against relay and physical layer attacks. IACR ePrint Report 2017/1240, December 2017.
532. Sergei Skorobogatov and Christopher Woods. In the blink of an eye: There goes your AES key, 2012.
533. Agusti Solanas and Josep Domingo-Ferrer. Location privacy in location-based services: Beyond ttp-based schemes. In *In Proceedings of the 1st international workshop on privacy in location-based applications (PILBA)*, pages 12–23, 2008.
534. Agusti Solanas and Antoni Martínez-Ballesté. V-MDAV: a multivariate microaggregation with variable group size. In *17th COMPSTAT Symposium of the IASC*, pages 917–925, 2006.
535. Agusti Solanas, Constantinos Patsakis, Mauro Conti, Ioannis S. Vlachos, Victoria Ramos, Francisco Falcone, Octavian Postolache, Pablo A. Pérez-Martínez, Roberto Di Pietro, Despina N. Perrea, and Antoni Martínez-Ballesté. Smart health: A context-aware health paradigm within smart cities. *IEEE Communications Magazine*, 52(8):74–81, 2014.
536. Agusti Solanas, Jens H. Weber, Ayse Basar Bener, Frank van der Linden, and Rafael Capilla. Recent advances in healthcare software: Toward context-aware and smart solutions. *IEEE Software*, 34(6):36–40, 2017.
537. Ling Song, Zhangjie Huang, and Qianqian Yang. Automatic differential analysis of ARX block ciphers with application to SPECK and LEA. In Joseph K. Liu and Ron Steinfeld, editors, *ACISP 16: 21st Australasian Conference on Information Security and Privacy, Part II*, volume 9723 of *Lecture Notes in Computer Science*, pages 379–394, Melbourne, VIC, Australia, July 4–6, 2016. Springer.
538. Juan Soto. Statistical testing of random number generators. In *Proceedings of the 22nd National Information Systems Security Conference*, volume 10, page 12. NIST, 1999.

539. Luigi Sportiello and Andrea Ciardulli. Long distance relay attack. In *International Workshop on Radio Frequency Identification: Security and Privacy Issues*, pages 69–85. Springer, 2013.
540. Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, February 2002.
541. François-Xavier Standaert, Gilles Piret, Gaël Rouvroy, Jean-Jacques Quisquater, and Jean-Didier Legat. ICEBERG: An involutional cipher efficient for block encryption in reconfigurable hardware. In Bimal K. Roy and Willi Meier, editors, *Fast Software Encryption – FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 279–299, New Delhi, India, February 5–7, 2004. Springer.
542. François-Xavier Standaert, Gilles Piret, Neil Gershenfeld, and Jean-Jacques Quisquater. SEA: A scalable encryption algorithm for small embedded applications. In *Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference, CARDIS 2006, Tarragona, Spain, April 19-21, 2006, Proceedings*, pages 222–236, 2006.
543. Yue Sun, Meiqin Wang, Shujia Jiang, and Qiumei Sun. Differential cryptanalysis of reduced-round ICEBERG. In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT 12: 5th International Conference on Cryptology in Africa*, volume 7374 of *Lecture Notes in Computer Science*, pages 155–171, Ifrance, Morocco, July 10–12, 2012. Springer.
544. Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight, versatile block cipher. In *ECRYPT Workshop on Lightweight Cryptography*, pages 146–169, 2011.
545. Biaoshuai Tao and Hongjun Wu. Improving the biclique cryptanalysis of aes. In *Information Security and Privacy, ACISP 2015, Brisbane, Australia, June 29 - July 1, 2015*, pages 39–56, 2015.
546. The European Parliament and the Council of the European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/ec. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG, 2014.
547. The European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ec (General Data Protection Regulation). *Official Journal of the European Union*, 119(1), 2016.
548. Pierre-Henri Thevenon and Olivier Savry. Implementation of a countermeasure to relay attacks for contactless hf systems. In *Radio Frequency Identification from System to Applications*. InTech, 2013.
549. Olivier Thomas and Dmitry Nedospasov. On the impact of automating the ic analysis process. BlackHat 2015, August 2015.
550. Sam L. Thomas, Tom Chothia, and Flavio D. Garcia. Stringer: Measuring the Importance of Static Data Comparisons to Detect Backdoors and Undocumented Functionality. In *Proceedings of the 22nd European Symposium on Research in Computer Security*, ESORICS '17, 2017.
551. Sam L. Thomas and Aurélien Francillon. Backdoors: Definition, Deniability and Detection. In *Symposium on Research in Attacks, Intrusion, and Defenses (RAID)*. Springer, September 2018.
552. Sam L. Thomas, Flavio D. Garcia, and Tom Chothia. HumIDIFy: A Tool for Hidden Functionality Detection in Firmware. In *Proceedings of the 14th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, DIMVA '17, 2017.
553. Peter Thueringer, Hans De Jong, Bruce Murray, Heike Neumann, Paul Hubmer, and Susanne Stern. Decoupling of measuring the response time of a transponder and its authentication, November 2008.
554. Yun Tian, Gongliang Chen, and Jianhua Li. A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702–705, May 2012.
555. Yun Tian, Gongliang Chen, and Jianhua Li. Quavium - a new stream cipher inspired by trivium. *Journal of Computers*, 7(5):1278–1283, 2012.

556. Andrew Tierney (@cybergibbons). Bypassing code readout protections on microcontrollers, January 2018.
557. K. Tiri and I. Verbauwhede. A logic level design methodology for a secure dpa resistant asic or fpga implementation. In *Proceedings Design, Automation and Test in Europe Conference and Exhibition*, volume 1, pages 246–251 Vol.1, Feb 2004.
558. Tjaldur Software Governance Solutions. Binary Analysis Tool (BAT).
559. Jevgenijus Toldinas, Algimantas Venčkauskas, Šarūnas Grigaliūnas, Robertas Damaševičius, and Vacius Jusas. Suitability of the digital forensic tools for investigation of cyber crime in the internet of things and services. In *The 3rd International Virtual Research Conference In Technical Disciplines*, pages 86–97, October 2015.
560. Meltem Sönmez Turan, Ali DoĞanaksoy, and Serdar Boztaş. On independence and sensitivity of statistical randomness tests. In *International Conference on Sequences and Their Applications*, pages 18–29. Springer, 2008.
561. Pascal Urien and Selwyn Piramuthu. Elliptic curve-based rfid/nfc authentication with temperature sensor input for relay attacks. *Decis. Support Syst.*, 59:28–36, March 2014.
562. Lachlan Urquhart, Neelima Sailaja, and Derek McAuley. Realising the right to data portability for the domestic internet of things. *Personal and Ubiquitous Computing*, pages 1–16, 2017.
563. Jordi van den Breekel, Diego A. Ortiz-Yepes, Erik Poll, and Joeri de Ruiter. EMV in a nutshell. June, KPMG, IBM Research Zurich, Radboud University Nijmegen, 2016.
564. S. Vasile, D. Oswald, and T. Chothia. Breaking all the things - a systematic survey of firmware extraction techniques for iot devices. In *CARDIS*, 2018.
565. Rajesh Velegalati and Jens-Peter Kaps. Introducing FOBOS: Flexible Open-source BOard for Side-channel analysis. Work in Progress (WiP), Third International Workshop on Constructive Side-Channel Analysis and Secure Design, COSADE 2012, May 2012.
566. Rajesh Velegalati and Jens-Peter Kaps. Towards a Flexible, Opensource BOard for Side-channel analysis (FOBOS). Cryptographic architectures embedded in reconfigurable devices, CRYPTARCHI 2013, June 2013.
567. José Vila and Ricardo J. Rodríguez. Practical experiences on NFC relay attacks with android: Virtual pickpocketing revisited. In Stefan Mangard and Patrick Schaumont, editors, *Radio Frequency Identification. Security and Privacy Issues - 11th International Workshop, RFIDsec 2015, New York, NY, USA, June 23-24, 2015, Revised Selected Papers*, volume 9440 of *Lecture Notes in Computer Science*, pages 87–103, New York City, USA, June 2015. Springer.
568. John Walker. Ent, a pseudorandom number sequence test program. Fourmilab, 2008.
569. Cheng Wang and Howard M. Heys. An ultra compact block cipher for serialized architecture implementations. In *Proceedings of the 22nd Canadian Conference on Electrical and Computer Engineering, CCECE 2009, 3-6 May 2009, Delta St. John's Hotel and Conference Centre, St. John's, Newfoundland, Canada*, pages 1085–1090, 2009.
570. Jian Wang, Jiaqi Mu, Shuangqing Wei, Chunxiao Jiang, and Norman C Beaulieu. Statistical characterization of decryption errors in block-ciphered systems. *IEEE Transactions on Communications*, 63(11):4363–4376, 2015.
571. Jinbao Wang, Zhipeng Cai, Yingshu Li, Donghua Yang, Ji Li, and Hong Gao. Protecting query privacy with differentially private k-anonymity in location-based services. *Personal and Ubiquitous Computing*, Mar 2018.
572. Qi Wang, Wajih Ul Hassan, Adam Bates, and Carl Gunter. Fear and logging in the internet of things. *Network and Distributed Systems Symposium*, Feb 2018.
573. Shengling Wang, Qin Hu, Yunchuan Sun, and Jianhui Huang. Privacy preservation in location-based services. *IEEE Communications Magazine*, 56(3):134–140, MARCH 2018.
574. Dai Watanabe, Kota Ideguchi, Jun Kitahara, Kenichiro Muto, Hiroki Furuichi, and Toshinobu Kaneko. Enocoro-80: A hardware oriented stream cipher. In *Proceedings of the The Third International Conference on Availability, Reliability and Security, ARES 2008, March 4-7, 2008, Technical University of Catalonia, Barcelona , Spain*, pages 1294–1300, 2008.

575. Dai Watanabe, Kazuto Okamoto, and Toshinobu Kaneko. A hardware-oriented light weight pseudo-random number generator enocoro-128v2. In *SCIS 2010, 3D1-3, (2010). In Japanese*, 2010.
576. Steve Watson and Ali Dehghantanha. Digital forensics: the missing piece of the internet of things promise. *Computer Fraud & Security*, 2016(6):5–8, 2016.
577. Shuangqing Wei, Jian Wang, Ruming Yin, and Jian Yuan. Trade-off between security and performance in block ciphered systems with erroneous ciphertexts. *IEEE Transactions on Information Forensics and Security*, 8(4):636–645, 2013.
578. Mark Weiser. The computer for the 21st century. *Mobile Computing and Communications Review*, 3(3):3–11, 1999.
579. Oscar Williams-Grut. Hackers once stole a casino's high-roller database through a thermometer in the lobby fish tank. Business Insider, 2018.
580. Ian H. Witten and Eibe Frank. *Data Mining: Practical Machine Learning Tools and Techniques, Second Edition (Morgan Kaufmann Series in Data Management Systems)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2005.
581. Hongjun Wu. Acorn: A lighweight authenticated cipher (v3). Candidate for the CAESAR Competition, 2016.
582. Wenling Wu, Shuang Wu, Lei Zhang, Jian Zou, and Le Dong. Lhash: A lightweight hash function. In *Information Security and Cryptology - 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013, Revised Selected Papers*, pages 291–308, 2013.
583. Wenling Wu and Lei Zhang. LBlock: A lightweight block cipher. In Javier Lopez and Gene Tsudik, editors, *ACNS 11: 9th International Conference on Applied Cryptography and Network Security*, volume 6715 of *Lecture Notes in Computer Science*, pages 327–344, Nerja, Spain, June 7–10, 2011. Springer.
584. Minm Xie, Jingjing Li, and Yuechuan Zang. Related-key impossible differential cryptanalysis of lblock. *Chinese Journal of Electronics*, 26(1):35–41, 2017.
585. Xiaojun Xu, Chang Liu, Qian Feng, Heng Yin, Le Song, and Dawn Song. Neural network-based graph embedding for cross-platform binary code similarity detection. In *ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, 2017.
586. Dai Yamamoto, Kouichi Itoh, and Jun Yajima. A very compact hardware implementation of the kasumi block cipher. In *4th IFIP WG 11.2 International Workshop WISTP 2010, Passau, Germany, April 12-14, 2010*, pages 293–307, 2010.
587. Gangqiang Yang, Xinxin Fan, Mark Aagaard, and Guang Gong. Design space exploration of the lightweight stream cipher wg-8 for fpgas and asics. In *Workshop on Embedded Systems Security, WESS'13, Article No. 8, Montreal, Quebec, Canada, September 29 - October 04, 2013*, 2013.
588. Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems – CHES 2015*, volume 9293 of *Lecture Notes in Computer Science*, pages 307–329, Saint-Malo, France, September 13–16, 2015. Springer.
589. Sergey Yekhanin. Private Information Retrieval. *Communications of the ACM*, 53(4):68–73, 2010.
590. Adam L. Young and Moti Yung. *Malicious cryptography - exposing cryptovirology*. Wiley, 2004.
591. Jonas Zaddach, Luca Bruno, Aurélien Francillon, and Davide Balzarotti. Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares. In *NDSS 2014*, February 2014.
592. Shams Zawoad and Ragib Hasan. FAIoT: Towards building a forensics aware eco system for the internet of things. In *2015 IEEE International Conference on Services Computing, SCC 2015, New York City, NY, USA, June 27 - July 2, 2015*, pages 279–284, 2015.
593. Bin Zhang and Xinxin Gong. Another tradeoff attack on Sprout-like stream ciphers. In *ASIACRYPT 2015*, volume 9453 of *LNCS*, pages 561–585. Springer, 2015.

594. Bin Zhang, Zhenqing Shi, Chao Xu, Yuan Yao, and Zhenqi Li. Sablier v1. Candidate for the CAESAR Competition, 2014.
595. Bin Zhang, Chao Xu, and Willi Meier. Fast near collision attack on the Grain v1 stream cipher. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 771–802, Tel Aviv, Israel, April 29 – May 3, 2018. Springer.
596. Lei Zhang, Wenling Wu, Yanfeng Wang, Shengbao Wu, and Jian Zhang. LAC: A lightweight authenticated encryption cipher. Candidate for the CAESAR Competition, 2014.
597. Liwei Zhang, A. Adam Ding, Francois Durvaux, Francois-Xavier Standaert, and Yunsi Fei. Towards sound and optimal leakage detection procedure. Cryptology ePrint Archive, Report 2017/287, 2017. http://eprint.iacr.org/2017/287.
598. WenTao Zhang, ZhenZhen Bao, DongDai Lin, Vincent Rijmen, BoHan Yang, and Ingrid Verbauwhede. Rectangle: a bit-slice lightweight block cipher suitable for multiple platforms. *Science China Information Sciences*, 58(12):1–15, 2015.
599. Huang Zhangwei and Xin Mingjun. A distributed spatial cloaking protocol for location privacy. In *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, volume 2, pages 468–471, April 2010.
600. Yingxian Zheng, Yongbin Zhou, Zhenmei Yu, Chengyu Hu, and Hailong Zhang. How to Compare Selections of Points of Interest for Side-Channel Distinguishers in Practice? In Lucas C. K. Hui, S. H. Qing, Elaine Shi, and S. M. Yiu, editors, *ICICS 2014, Revised Selected Papers*, pages 200–214, Cham, 2015. Springer International Publishing.
601. Shuangyi Zhu, Yuan Ma, Jingqiang Lin, Jia Zhuang, and Jiwu Jing. More powerful and reliable second-level statistical randomness tests for nist sp 800-22. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 307–329. Springer, 2016.
602. Tanveer Zia, Peng Liu, and Weili Han. Application-specific digital forensics investigative model in internet of things (iot). In *Proceedings of the 12th International Conference on Availability, Reliability and Security*, ARES '17, pages 55:1–55:7, New York, NY, USA, 2017. ACM.