Bibliography on Security and Privacy in RFID Systems

Information Security Group
Université catholique de Louvain
Louvain-la-Neuve, Belgium

Version October 13, 2015

Abstract. This document is the printable and citable version of the online bibliography on security and privacy in RFID systems, available at http://www.avoine.net/rfid/. The website is maintained by the UCL's Information Security Group (Belgium) headed by Gildas Avoine. This bibliography contains references toward refereed scientific papers published in journals and conference proceedings, as well as technical reports and thesis. It is updated on an irregular basis depending on the flow of papers published in the domain.

1. M. B. Abdelhalim, M. El-Mahallawy, M. Ayyad, and A. El-Mahallawy. Design and implementation of an encryption algorithm for use in RFID system. *International Journal of RFID Security and Cryptography*, 1:51–57, March 2012.
2. Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, and Mohammad Reza Aref. Cryptanalysis of two EPC-based RFID security schemes. In *International ISC Conference on Information Security and Cryptology – ISCISC2015*, pages 1–6. IEEE, September 2015.
3. Behzad Abdolmaleki, Karim Baghery, Bahareh Akhbari, and Mohammad Reza Aref. Attacks and improvements on two new-found RFID authentication protocols. In *International Symposium on Telecommunications – IST 2014*, pages 1–6, July 2014.
4. Shahab Abdolmaleky, Shahla Atapoor, Mohammad Hajighasemlou, and Hamid Sharini. A strengthened version of a hash-based RFID server-less security scheme. *Advances in Computer Science: an International Journal*, 4(3):18–23, May 2015.
5. Srujana Adepwar and P. Swetha. Security solution for real time location systems using distance bounding. *International Journal of Technology and Engineering Science*, 2(6):1933–1937, June 2014.
6. A. O. Afolabi, A. A. Atayero, P. Ajayi, and P. Wogu. Implementation of biometric RFID identification system: A case study of covenant university. Covenant University ePrint Repository, 2015.
7. Arjun Agarwal and Mala Mitra. RFID: Promises and Problems, April 2006.
8. Seyed Farhad Aghili, Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya. On the security of two RFID mutual authentication protocols. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
9. Tanvi Agrawal, P.K. Biswas, and A.D. Raoot. An optimized query tree algorithm in RFID inventory tracking – a case study evidence. *IJCSI International Journal of Computer Science Issues*, 9(1):85–93, July 2012.
10. Isaac Agudo, Ruben Rios, and Javier Lopez. A privacy-aware continuous authentication scheme for proximity-based access control. *Computers & Security*, (0), May 2013.
11. Hadi Ahmadi and Reihaneh Safavi-Naini. Secure distance bounding verification using physical-channel properties. arXiv.org, Computer Science, Cryptography and Security, 2013.
12. Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Desynchronization attack on RAPP ultralightweight authentication protocol. Cryptology ePrint Archive, Report 2012/490, 2012.
13. Zahra Ahmadian, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Recursive linear and differential cryptanalysis of ultralightweight authentication protocols. Cryptology ePrint Archive, Report 2012/489, 2012.
14. Manfred Aigner. Security in the Internet of Things. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
15. Manfred Aigner and Martin Feldhofer. Secure Symmetric Authentication for RFID Tags. In *Telecommunication and Mobile Computing – TCMC 2005*, Graz, Austria, March 2005.

16. Qurat Ul Ain, Yusra Mahmood, Umar Mujahid, and Muhammad Najam-ul islam. Cryptanalysis of mutual ultralightweight authentication protocols: SASI and RAPP. In *International Conference on Open Source Systems and Technologies – ICOSST 2014*, pages 136–145, Lahore, Pakistan, December 2014.
17. Mete Akgün, Ali Osman Bayrak, and Mehmet Ufuk Çağlayan. Attacks and improvements to chaotic map-based RFID authentication protocol. *Security and Communication Networks*, July 2015.
18. Mete Akgun and M. Ufuk Caglayan. Weaknesses of two RFID protocols regarding de-synchronization attacks. In *International Wireless Communications and Mobile Computing Conference IWCMC – 2015*, Dubrovnik, Croatia, August 2015.
19. Mete Akgün and M. Ufuk Çağlayan. On the security of recently proposed RFID protocols. Cryptology ePrint Archive, Report 2013/820, 2013.
20. Mete Akgün and M. Ufuk Çağlayan. Providing destructive privacy and scalability in RFID systems using PUFs. *Ad Hoc Networks*, February 2015.
21. Mete Akgün and Mehmet Çağlayan. Extending an rfid security and privacy model by considering forward untraceability. In *Security and Trust Management*, pages 239–254, Technical University of Denmark, Copenhagen, June 2011.
22. Mete Akgün and Mehmet Ufuk Çağlayan. Towards scalable identification in RFID systems. *Wireless Personal Communications*, August 2015.
23. Mahdi R. Alagheband and Mohammad R. Aref. Unified privacy analysis of new-found RFID authentication protocols. *Security and Communication Networks*, 5(12), December 2012.
24. Mahdi R. Alagheband and Mohammad R. Aref. Simulation-based traceability analysis of RFID authentication protocols. *Wireless Personal Communications*, December 2013.
25. Rima Hussin Embrak Alakrut, Azman Samsudin, and Alfin Syafalni. Provably lightweight RFID mutual authentication protocol. *International Journal of Security and Its Applications*, 7(4), July 2013.
26. Seyed Mohammad Alavi, Behzad Abdolmaleki, and Karim Baghery. Vulnerabilities and improvements on HRAP^{+}, a hash-based RFID authentication protocol. *Advances in Computer Science: an International Journal*, 3(6):51–56, November 2014.
27. Seyed Mohammad Alavi, Karim Baghery, and Behzad Abdolmaleki. Security and privacy flaws in a recent authentication protocol for EPC C1 G2 RFID tags. *Advances in Computer Science : an International Journal*, 3(5):44–52, September 2014.
28. Seyed Mohammad Alavi, Karim Baghery, Behzad Abdolmaleki, and Mohammad Reza Aref. Traceability analysis of recent RFID authentication protocols. *Wireless Personal Communications*, pages 1–20, March 2015.
29. Hisham Khalaf Allahem. Mutual authentication scheme for mobile rfid systems. Master thesis, Dalhousie University, Halifax, Nova Scotia, Canada, March 2013.
30. Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran. Scalable RFID Systems: a Privacy-Preserving Protocol with Constant-Time Identification. In *the 40th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – DSN'10*, Chicago, Illinois, USA, June 2010. IEEE, IEEE Computer Society.
31. Basel Alomair, Andrew Clark, Jorge Cuellar, and Radha Poovendran. Scalable RFID systems: A privacy-preserving protocol with constant-time identification. *IEEE Transactions on Parallel and Distributed Systems*, 2011.
32. Basel Alomair, Loukas Lazos, and Radha Poovendran. Passive Attacks on a Class of Authentication Protocols for RFID. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *International Conference on Information Security and Cryptology – ICISC 2007*, volume 4817 of *Lecture Notes in Computer Science*, pages 102–115, Seoul, Korea, November 2007. Springer.
33. Basel Alomair, Loukas Lazos, and Radha Poovendran. Securing Low-cost RFID Systems: an Unconditionally Secure Approach. *Journal of Computer Security – Special Issue on RFID System Security*, 2010.
34. Basel Alomair, Loukas Lazos, and Radha Poovendran. Securing Low-Cost RFID Systems: an Unconditionally Secure Approach. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
35. Basel Alomair and Radha Poovendran. On the Authentication of RFID Systems with Bitwise Operations. In *New Technologies, Mobility and Security – NTMS'08*, pages 1–6, Tangier, Morocco, November 2008. IEEE, IEEE Computer Society.
36. Basel Alomair and Radha Poovendran. Efficient Authentication for Mobile and Pervasive Computing. In Sihan Qing Miguel Soriano and Javier Lopez, editors, *International Conference on Information and Communications Security – ICICS'10*, volume 6476 of *Lecture Notes in Computer Science*, pages 186–202, Barcelona, Spain, December 2010. Springer.

37. Basel Alomair and Radha Poovendran. Privacy versus Scalability in Radio Frequency Identification Systems. *Computer Communication, Elsevier*, 2010.
38. Gergely Alpar, Lejla Batina, and Wouter Lueks. Designated attribute-based proofs for RFID applications. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
39. Abdulhadi Alqarni, Maali Alabdulhafith, and Srinivas Sampalli. A proposed RFID authentication protocol based on two stages of authentication. In *The 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks – EUSPN-2014*, Halifax, Nova Scotia, Canada, September 2014.
40. George T. Amariucai, Clifford Bergman, and Yong Guan. An Automatic, Time-Based, Secure Pairing Protocol for Passive RFID. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
41. Myrto Arapinis, Tom Chothia, Eike Ritter, and Mark Ryan. Analysing Unlinkability and Anonymity Using the Applied Pi Calculus. In *Computer Security Foundations Symposium – CSF 2010*, Edinburgh, United Kingdom, July 2010. IEEE.
42. Alex Arbit, Yoel Livne, Yossef Oren, and Avishai Wool. Implementing public-key cryptography on passive RFID tags is practical. *International Journal of Information Security*, April 2014.
43. Mohammad Arjmand, Mahmoud Gardeshi, Reza Taheri zohur, and Mohammad Kazemi. Providing a distance bounding protocol named pasargad in order to defend against relay attacks on RFID-based electronic voting system. *International Journal of UbiComp*, 2(3):69–82, 2011.
44. Frederik Armknecht, Liqun Chen, Ahmad-Reza Sadeghi, and Christian Wachsmann. Anonymous Authentication for RFID Systems. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 158–175, Istanbul, Turkey, June 2010. Springer.
45. 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.
46. Frederik Armknecht, Ahmad-Reza Sadeghi, Alessandra Scafuro, Ivan Visconti, and Christian Wachsmann. Impossibility Results for RFID Privacy Notions. *Transaction on Computational Science XI*, 6480:39–63, 2010.
47. Frederik Armknecht, Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. On RFID Privacy with Mutual Authentication and Tag Corruption. In Jianying Zhou and Moti Yung, editors, *Proceedings of the 8th International Conference on Applied Cryptography and Network Security – ACNS 2010*, volume 6123 of *Lecture Notes in Computer Science*, pages 493–510, Beijing, China, June 2010. Springer.
48. Mahdi Asadpour and Mohammad Torabi Dashti. A privacy-friendly RFID protocol using reusable anonymous tickets. In *10th International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2011*, pages 206–213, November 2011.
49. Aisha Aseeri and Omaima Bamasak. HB-MP*:towards a man-in-the-middle-resistant protocol of HB family. In *1st International Conference on Wireless Communications and Mobile Computing*, page 4, Istanbul, Turkey, June 2011.
50. Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable RFID Tags via Insubvertible Encryption. In Vijay Atluri, Catherine Meadows, and Ari Juels, editors, *Conference on Computer and Communications Security – ACM CCS'05*, pages 92–101, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
51. Ali Atici, Lejla Batina, Benedikt Gierlichs, and Ingrid Verbauwhede. Power Analysis on NTRU Implementations for RFIDs: First Results. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
52. Jean-Philippe Aumasson, Aikaterini Mitrokotsa, and Pedro Peris-Lopez. A note on a privacy-preserving distance-bounding protocol. In Sihan Qing, Willy Susilo, Guilin Wang, and Dongmei Liu, editors, *International Conference on Information and Communications Security – ICICS'11*, volume 2043 of *Lecture Notes in Computer Science*, pages 78–92. Springer Berlin / Heidelberg, November 2011.
53. Myo Min Aung, Yoon Seok Chang, and Jong-un Won. Emerging RFID/USN applications and challenges. *International Journal of RFID Security and Cryptography*, 1:3–8, March 2012.
54. Gildas Avoine. Privacy Issues in RFID Banknote Protection Schemes. In Jean-Jacques Quisquater, Pierre Paradinas, Yves Deswarte, and Anas Abou El Kadam, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS 2004*, pages 33–48, Toulouse, France, August 2004. IFIP, Kluwer Academic Publishers.
55. Gildas Avoine. Adversary Model for Radio Frequency Identification. Technical Report LASEC-REPORT-2005-001, Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, September 2005.
56. Gildas Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
57. Gildas Avoine, Muhammed Ali Bingol, Xavier Carpent, and Suleyman Kardas. Deploying OSK on low-resource mobile devices. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.

58. Gildas Avoine, Muhammed Ali Bingöl, Xavier Carpent, and Sıddıka Berna Örs Yalçın. Privacy-friendly authentication in RFID systems: On sub-linear protocols based on symmetric-key cryptography. *IEEE Transactions on Mobile Computing*, 12(10):2037–2049, October 2013.
59. Gildas Avoine, Muhammed Ali Bingol, Xavier Carpent, and Siddika Berna Ors Yalcin. Privacy-friendly authentication in RFID systems: On sub-linear protocols based on symmetric-key cryptography. *IEEE Transactions on Mobile Computing*, 99, September 2012.
60. Gildas Avoine, Muhammed Ali Bingöl, Süleyman Kardaş, Cédric Lauradoux, and Benjamin Martin. A Framework for Analyzing RFID Distance Bounding Protocols. *Journal of Computer Security – Special Issue on RFID System Security*, 19(2):289–317, March 2011.
61. Gildas Avoine, Levente Buttyán, Tamás Holczer, and István Vajda. Group-based private authentication. In *IEEE International Workshop on Trust, Security, and Privacy for Ubiquitous Computing – TSPUC*, pages 1–6, Helsinki, Finland, June 2007. IEEE, IEEE Computer Society.
62. Gildas Avoine, Luca Calderoni, Jonathan Delvaux, Dario Maio, and Paolo Palmieri. Passengers information in public transport and privacy: Can anonymous tickets prevent tracking? *International Journal of Information Management*, 34(5):682–688, October 2014.
63. Gildas Avoine and Xavier Carpent. Yet another ultralightweight authentication protocol that is broken. Cryptology ePrint Archive, Report 2011/691, 2011.
64. Gildas Avoine and Xavier Carpent. Yet another ultralightweight authentication protocol that is broken. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
65. 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.
66. Gildas Avoine, Xavier Carpent, and Benjamin Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Applications*, December 2011.
67. Gildas Avoine, Xavier Carpent, and Benjamin Martin. Privacy-friendly synchronized ultralightweight authentication protocols in the storm. *Journal of Network and Computer Applications*, 35(2):826–843, February 2012.
68. Gildas Avoine, Iwen Coisel, and Tania Martin. Time Measurement Threatens Privacy-Friendly RFID Authentication Protocols. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 138–157, Istanbul, Turkey, June 2010. Springer.
69. Gildas Avoine, Iwen Coisel, and Tania Martin. A privacy-restoring mechanism for offline RFID systems. In *Proceedings of the 5th ACM Conference on Wireless Network Security – WiSec'12*, pages 63–74, Tucson, Arizona, USA, April 2012. ACM, ACM Press.
70. Gildas Avoine, Iwen Coisel, and Tania Martin. Untraceability model for RFID. *IEEE Transactions on Mobile Computing*, PrePrint, November 2013.
71. Gildas Avoine, Iwen Coisel, and Tania Martin. Untraceability model for RFID. *IEEE Transactions on Mobile Computing*, 13(10):2397–2405, October 2014.
72. Gildas Avoine, Etienne Dysli, and Philippe Oechslin. Reducing Time Complexity in RFID Systems. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 291–306, Kingston, Canada, August 2005. Springer.
73. Gildas Avoine, Christian Floerkemeier, and Benjamin Martin. RFID Distance Bounding Multistate Enhancement. In Bimal K. Roy and Nicolas Sendrier, editors, *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, volume 5922 of *Lecture Notes in Computer Science*, pages 290–307, New Delhi, India, December 2009. Springer.
74. Gildas Avoine, Kassem Kalach, and Jean-Jacques Quisquater. ePassport: Securing International Contacts with Contactless Chips. In Gene Tsudik, editor, *Financial Cryptography and Data Security – FC'08*, volume 5143 of *Lecture Notes in Computer Science*, pages 141–155, Cozumel, Mexico, January 2008. IFCA, Springer.
75. Gildas Avoine, Cédric Lauradoux, and Benjamin Martin. How secret-sharing can defeat terrorist fraud. In *Proceedings of the 4th ACM Conference on Wireless Network Security – WiSec'11*, Hamburg, Germany, June 2011. ACM, ACM Press.
76. Gildas Avoine, Cédric Lauradoux, and Tania Martin. When Compromised Readers Meet RFID. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
77. Gildas Avoine, Cédric Lauradoux, and Tania Martin. When Compromised Readers Meet RFID. In H.Y. Youm and M. Yung, editors, *Workshop on Information Security Applications – WISA'09*, volume 5932 of *Lecture Notes in Computer Science*, pages 36–50, Busan, Korea, August 2009. Springer.

78. Gildas Avoine, Benjamin Martin, and Tania Martin. Tree-Based RFID Authentication Protocols Are Definitively Not Privacy-Friendly. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 103–122, Istanbul, Turkey, June 2010. Springer.
79. Gildas Avoine, Sjouke Mauw, and Rolando Trujillo-Rasua. Comparing distance bounding protocols: a critical mission supported by decision theory. arXiv.org, Computer Science, Cryptography and Security, March 2015.
80. Gildas Avoine and Philippe Oechslin. A Scalable and Provably Secure Hash Based RFID Protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society.
81. Gildas Avoine and Philippe Oechslin. RFID Traceability: A Multilayer Problem. In Andrew Patrick and Moti Yung, editors, *Financial Cryptography – FC'05*, volume 3570 of *Lecture Notes in Computer Science*, pages 125–140, Roseau, The Commonwealth Of Dominica, February–March 2005. IFCA, Springer.
82. Gildas Avoine and Aslan Tchamkerten. An asymptotically optimal RFID protocol against relay attacks. Cryptology ePrint Archive, Report 2008/406, 2008.
83. Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *Information Security Conference – ISC'09*, volume 5735 of *Lecture Notes in Computer Science*, pages 250–261, Pisa, Italy, September 2009. Springer.
84. John Ayoade. Privacy and RFID Systems: Roadmap to Solving Security and Privacy Concerns in RFID Systems. *Computer Law and Security Report*, 23(6):555–561, 2007.
85. John Ayoade, Osamu Takizawa, and Koji Nakao. A Prototype System of the RFID Authentication Processing Framework. In *International Workshop in Wireless Security Technologies, available at http://www.iwwst.org.uk/proceedings.html*, pages 34–38, London, United Kingdom, April 2005.
86. Aydin Aysu, Ege Gulcan, Daisuke Moriyama, Patrick Schaumont, and Moti Yung. End-to-end design of a PUF-based privacy preserving authentication protocol. Cryptology ePrint Archive, Report 2015/937, 2015.
87. Mahdi Azizi and Nasour Bagheri. Cryptanalysis of sulma, an ultralightweight mutual authentication protocol for low-cost RFID tags. *International Journal of UbiComp*, 2(4):15–25, 2011.
88. Mahdi Azizi, Nasour Bagheri, and Abdolrasol Mirgadri. Cryptanalysis of pasargad, a distance bounding protocol based on RFID system. *International Journal of UbiComp*, 3(3):31–42, July 2012.
89. Guillermo Azuara, Joan Josep Piles, José Luis Salazar, and José Luis Tornos. Reliable Food Traceability Using RFID Tagging. In *1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices – WLC'10*, Lecture Notes in Computer Science, Tenerife, Canary Islands, Spain, January 2010. Springer.
90. Guillermo Azuara and Jos Salazar. Comprehensive Protection of RFID Traceability Information Systems Using Aggregate Signatures. In lvaro Herrero and Emilio Corchado, editors, *Computational Intelligence in Security for Information Systems*, volume 6694 of *Lecture Notes in Computer Science*, pages 168–176. Springer, June 2011.
91. Shilpa S. Badhiye and Rupali S. Khule. Survey on enhancing security for RFID smart cards. *International Journal of Advance Research and Innovative Ideas in Education*, 1(3):323–330, September 2015.
92. Nasour Bagheri, Parvin Alenaby, and Masoumeh Safkhani. A new anti-collision protocol based on information of collided tags in RFID systems. *International Journal of Communication Systems*, May 2015.
93. Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya. Desynchronization and traceability attacks on RIPTA-DA protocol. In Michael Hutter and Jrn-Marc Schmidt, editors, *Workshop on RFID Security – RFIDSec'13*, pages 57–68, Graz, Austria, July 2013. Lecture Notes in Computer Science, Springer Berlin Heidelberg.
94. Nasour Bagheri, Praveen Gauravaram, Masoumeh Safkhani, and Somitra Kumar Sanadhya. The resistance to intermittent position trace attacks and desynchronization attacks (RIPTA-DA) protocol is not RIPTA-DA. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
95. Nasour Bagheri and Masoumeh Safkhani. Secret disclosure attack on kazahaya, a yoking-proof for low-cost RFID tags. Cryptology ePrint Archive, Report 2013/453, 2013.
96. Nasour Bagheri, Masoumeh Safkhani, and Hoda Jannati. Security analysis of Niu et al. authentication and ownership management protocol. Cryptology ePrint Archive, Report 2015/615, 2015.
97. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, Yiyuan Luo, and Qi Chai. Forgery attack is a piece of cake on a class of mutual authentication protocols. *International Journal of Information & Communication Technology Research*, 4(3):33–43, June 2012.
98. Nasour Bagheri, Masoumeh Safkhani, Majid Naderi, and Somitra Kumar Sanadhya. Security Analysis of $LMAP^{++}$, an RFID Authentication Protocol. Cryptology ePrint Archive, Report 2011/193, 2011.
99. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, and Juan E. Tapiador. Cryptanalysis of RAPP, an RFID authentication protocol. Cryptology ePrint Archive, Report 2012/702, 2012.

100. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, and Juan Estevez Tapiador. Weaknesses in a new ultralightweight rfid authentication protocol with permutationrapp. *Security and Communication Networks*, June 2013.
101. Nasour Bagheri, Masoumeh Safkhani, Pedro Peris-Lopez, and Juan M. E. Tapiador. Comments on "security improvement of an RFID security protocol of ISO/IEC WD 29167-6". *Communications Letters, IEEE*, PP(99):1–3, February 2013.
102. Nasour Bagheri, Masoumeh Safkhani, Somitra Kumar Sanadhya, Majid Naderi, and Hamid Behnam. On the security of mutual authentication protocols for RFID systems: The case of wei et al.ś protocol. In *Sixth International Workshop on Data Privacy Management – DPM'11*, Lecture Notes in Computer Science, Leuven, Belgium, September 2011. Springer.
103. Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Privacy analysis and improvements of two recent RFID authentication protocols. In *International ISC Conference on Information Security and Cryptology – ISCISC 2014*, pages 137–142, Tehran, Iran, September 2014. IEEE.
104. Karim Baghery, Behzad Abdolmaleki, Bahareh Akhbari, and Mohammad Reza Aref. Untraceable RFID authentication protocols for EPC compliant tags. In *Iranian Conference on Electrical Engineering – ICEE 2015*, pages 426–431, Tehran, Iran, May 2015. IEEE.
105. Daniel Bailey and Ari Juels. Shoehorning Security into the EPC Standard. In Roberto De Prisco and Moti Yung, editors, *International Conference on Security in Communication Networks – SCN 2006*, volume 4116 of *Lecture Notes in Computer Science*, pages 303–320, Maiori, Italy, September 2006. Springer.
106. Helen Balinsky, Edward McDonnell, Liqun Chen, and Keith Harrison. Anti-Counterfeiting using Memory Spots. In Olivier Markowitch, Angelos Bilas, Jaap-Henk Hoepman, Chris J. Mitchell, and Jean-Jacques Quisquater, editors, *Workshop on Information Security Theory and Practice – WISTP'09*, volume 5746 of *Lecture Notes in Computer Science*, pages 52–67, Brussels, Belgium, September 2009. Springer.
107. Valentina Banciu, Simon Hoerder, and Dan Page. Lightweight primitive, feather-weight security ? a cryptanalytic knock-out. (preliminary results). Cryptology ePrint Archive, Report 2013/421, 2013.
108. Mihály Bárász, Balázs Boros, Péter Ligeti, Krisztina Lója, and Dániel Nagy. Breaking EMAP. In *Conference on Security and Privacy for Communication Networks – SecureComm 2007*, pages 514–517, Nice, France, September 2007. IEEE, IEEE Computer Society.
109. Mihály Bárász, Balázs Boros, Péter Ligeti, Krisztina Lója, and Dániel Nagy. Breaking LMAP. In *Conference on RFID Security*, Malaga, Spain, July 2007.
110. Mihály Bárász, Balázs Boros, Péter Ligeti, Krisztina Lója, and Dániel Nagy. Passive Attack Against the M2AP Mutual Authentication Protocol for RFID Tags. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
111. Alessandro Barenghi, Cédric Hocquet, David Bol, François-Xavier Standaert, Francesco Regazzoni, and Israel Koren. Exploring the Feasibility of Low Cost Fault Injection Attacks on Sub-Threshold Devices through an example of a 65nm AES implementation. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
112. David F. Barrero, Julio Csar Hernndez-Castro, Pedro Peris-Lopez, David Camacho, and Mara D. R-Moreno. A genetic tango attack against the davidprasad RFID ultra-lightweight authentication protocol. *Expert Systems*, September 2012.
113. Ramzi Bassil, Wissam El-Beaino, Wassim Itani, Ayman Kayssi, and Ali Chehab. PUMAP: A PUF-based ultralightweight mutual-authentication RFID protocol. *International Journal of RFID Security and Cryptography*, 1(1):58–66, March 2012.
114. Lejla Batina, Amitabh Das, Baris Ege, Elif Bilge Kavun, Nele Mentens, Christof Paar, Ingrid Verbauwhede, and Tolga Yalcin. Dietary recommendations for lightweight block ciphers: Power, energy and area analysis of recently developed architectures. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
115. Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. An Elliptic Curve Processor Suitable For RFID-Tags. Cryptology ePrint Archive, Report 2006/227, 2006.
116. Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-Key Cryptography for RFID-Tags. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
117. Lejla Batina, Jorge Guajardo, Tim Kerins, Nele Mentens, Pim Tuyls, and Ingrid Verbauwhede. Public-Key Cryptography for RFID-Tags. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 217–222, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
118. Lejla Batina, Jens Hermans, Jaap-Henk Hoepman, and Anna Krasnova. High-speed dating – privacy-preserving attribute matching for RFID. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.

119. Lejla Batina, Yong Lee, Stefaan Seys, Dave Singele, and Ingrid Verbauwhede. Extending ECC-based RFID authentication protocols to privacy-preserving multi-party grouping proofs. *Personal and Ubiquitous Computing*, 15, 2011.
120. Lejla Batina, Stefaan Seys, Dave Singelee, and Ingrid Verbauwhede. Hierarchical ECC-Based RFID Authentication Protocol. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
121. Asli Bay, Ioana Cristina Boureanu, Aikaterini Mitrokotsa, Iosif-Daniel Spulber, and Serge Vaudenay. The bussard-bagga and other distance-bounding protocols under attacks. In *8th China International Conference on Information Security and Cryptology – Inscrypt'12*, Beijing, China, November 2012.
122. Rima Belguechi and Christophe Lacharme, Patrick Rosenberger. Enhancing the privacy of electronic passports. *International Journal of Information Technology and Management*, 11(1/2):122–137, December 2012.
123. Ahmed Benfarah, Benoit Miscopein, Jean-Marie Gorce, Cédric Lauradoux, and Bernard Roux. Distance Bounding Protocols on TH-UWB Link and their Analysis Over Noisy Channels. Technical Report RR-7385, INRIA, Grenoble, France, September 2010.
124. Mustapha Benssalah, Mustapha Djeddou, and Karim Drouiche. Security enhancement of the authenticated RFID security mechanism based on chaotic maps. *Security and Communication Networks*, 7(1), January 2014.
125. Côme Berbain, Olivier Billet, Jonathan Etrog, and Henri Gilbert. An Efficient Forward Private RFID Protocol. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *Conference on Computer and Communications Security – ACM CCS'09*, pages 43–53, Chicago, Illinois, USA, November 2009. ACM, ACM Press.
126. Daniel J. Bernstein and Tanja Lange. Never trust a bunny. Cryptology ePrint Archive, Report 2012/355, 2012.
127. Daniel J. Bernstein and Tanja Lange. Never trust a bunny. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
128. Michael Beye and Thijs Veugen. Improved anonymity for key-trees. Cryptology ePrint Archive, Report 2011/395, 2011.
129. Michael Beye and Thijs Veugen. Anonymity for key-trees with adaptive adversaries. In Muttukrishnan Rajarajan, Fred Piper, Haining Wang, and George Kesidis, editors, *Conference on Security and Privacy for Communication Networks – SecureComm 2012*, volume 96 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 409–425, London, UK, September 2012. Springer Berlin Heidelberg.
130. Zeeshan Bilal. *Addressing Security and Privacy Issues in Low-Cost RFID Systems*. PhD thesis, Royal Holloway, University of London, London, UK, June 2015.
131. Zeeshan Bilal and Keith Martin. Ultra-lightweight mutual authentication protocols: Weaknesses and countermeasures. In *Eighth International Conference on Availability, Reliability and Security – ARES 2013*, pages 304–309. IEEE, September 2013.
132. Zeeshan Bilal, Keith Martin, and Qasim Saeed. Multiple attacks on authentication protocols for low-cost RFID tags. *Applied Mathematics and Information Sciences*, 9(2):561–569, November 2014.
133. Olivier Billet and Kaoutar El-Khiyaoui. Two Attacks against the Ff RFID Protocol. In Bimal K. Roy and Nicolas Sendrier, editors, *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, volume 5922 of *Lecture Notes in Computer Science*, pages 308–320, New Delhi, India, December 2009. Springer.
134. Olivier Billet, Jonathan Etrog, and Henri Gilbert. Lightweight Privacy Preserving Authentication for RFID Using a Stream Cipher. In Seokhie Hong and Tetsu Iwata, editors, *Fast Software Encryption – FSE'10*, volume 6147 of *Lecture Notes in Computer Science*, pages 55–74, Seoul, Korea, February 2010. Springer.
135. Muhammed Ali Bingöl. *Security analysis of RFID authentication protocols based on symmetric cryptography and implementation of a forward private scheme*. PhD thesis, Istanbul Technical University, Istanbul, Turkey, January 2012.
136. Przemyslaw Blaskiewicz, Jacek Cichon, Miroslaw Kutylowski, and Krzysztof Majcher. RFID Electronic Visa with Personalized Verification. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 81–95, Wuxi, China, April 2011. IOS Press.
137. Erik-Oliver Blass, Kaoutar El-Khiyaoui, and Refik Molva. PPS: Privacy Preserving Statistics using RFID Tags. Cryptology ePrint Archive, Report 2009/481, 2009.
138. Erik-Oliver Blass, Anil Kurmus, Refik Molva, Guevara Noubir, and Abdullatif Shikfa. The Ff-Family of Protocols for RFID-Privacy and Authentication. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
139. Carlo Blundo, Angelo De Caro, and Giuseppe Persiano. Untraceable Tags based on Mild Assumptions. In Joaqun Garca-Alfaro, Guillermo Navarro-Arribas, Nora Cuppens-Boulahia, and Yves Roudier, editors, *Second International Workshop on Autonomous and Spontaneous Security – SETOP'09*, volume 5939 of *Lecture Notes in Computer Science*, pages 178–192, Saint-Malo, France, September 2009. Springer.

140. Carlo Blundo, Guiseppe Persiano, Ahmad-Reza Sadeghi, and Ivan Visconti. Resettable and Non-Transferable Chip Authentication for ePassports. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
141. Salvatore Bocchetti. Security and Privacy in RFID Protocols. Master's thesis, Università degli Studi di Napoli Federico II, Italy, July 2006.
142. Eyad Abdullah Bogari, Pavol Zavarsky, Dale Lindskog, and Ron Ruhl. An analysis of security weaknesses in the evolution of RFID enabled passport. In *Internet Security (WorldCIS), 2012 World Congress on*, pages 158–166, Ontario, Canada, June 2012.
143. Andrey Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
144. Andrey Bogdanov, Lars Ramkilde Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466, Vienna, Austria, September 2007. Springer.
145. Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matthew Robshaw, and Yannick Seurin. Hash Functions and RFID Tags : Mind The Gap. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Proceedings of the 10th International Workshop Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 283–299, Washington, DC, USA, August 2008. Springer.
146. Christopher Bolan. The lazarus effect: Resurrecting killed RFID tags. In *Australian Information Security Management Conference – AISMC 2006*, December 2006.
147. Leonid Bolotnyy and Gabriel Robins. Physically Unclonable Function-Based Security and Privacy in RFID Systems. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 211–220, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
148. Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *14th USENIX Security Symposium – USENIX'05*, pages 1–16, Baltimore, Maryland, USA, July–August 2005. USENIX.
149. Carl Bosley, Kristiyan Haralambiev, and Antonio Nicolosi. hb^n: An HB-like protocol secure against man-in-the-middle attacks. Cryptology ePrint Archive, Report 2011/350, 2011.
150. Selma Boumerdassi, Papa Kane Diop, Eric Renault, and Anne Wei. T2MAP: A two-message mutual authentication protocol for low-cost RFID sensor networks. In *64th Vehicular Technology Conference – VTC 2006*, pages 1–5, September 2006.
151. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. On the pseudorandom function assumption in (secure) distance-bounding protocols. In Alejandro Hevia and Gregory Neven, editors, *Second International Conference on Cryptology and Information Security in Latin America – LATINCRYPT 2012*, volume 7533, pages 100–200, Santiago, Chile, October 2012. Springer Berlin / Heidelberg.
152. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. On the need for provably secure distance bounding. In *Early Symmetric Crypto (ESC) seminar*, Mondorf-les-Bains, Luxembourg, January 2013.
153. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Practical & provably secure distance-bounding. Cryptology ePrint Archive, Report 2013/465, 2013.
154. Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Secure and lightweight distance-bounding. In Gildas Avoine and Orhun Kara, editors, *Second International Workshop on Lightweight Cryptography for Security and Privacy – LightSec 2013*, volume 8162 of *Lecture Notes in Computer Science*, pages 97–113, Gebze, Turkey, May 2013. Springer-Verlag.
155. Ioana Boureanu and Serge Vaudenay. Challenges in distance bounding. In *IEEE Symposium on Security and Privacy – S&P '15*, pages 41–48. IEEE, IEEE Computer Society, February 2015.
156. Ioana Cristina Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Practical & provably secure distance-bounding. In Yvo Desmedt, editor, *Information Security Conference – ISC'13*, Lecture Notes in Computer Science, Dallas, Texas, USA, November 2013. Springer-Verlag.
157. Ioana Cristina Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay. Towards secure distance bounding. In Shiho Moriai, editor, *Fast Software Encryption – 20th International Workshop, FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, Singapore, Republic of Singapore, February 2013. Springer-Verlag.
158. Kevin Bowers, Ari Juels, Ronald Rivest, and Emily Shen. Drifting keys: Impersonation detection for constrained devices. In *IEEE InfoCom 2013*, Turin, Italy, April 2013. IEEE.
159. Michael Braun, Ulrike Meyer, and Susanne Wetzel. Efficient Mutual Authentication for Multi-domain RFID Systems Using Distributed Signatures. In Pierangela Samarati, Michael Tunstall, Joachim Posegga, Konstantinos Markantonakis, and Damien Sauveron, editors, *Workshop on Information Security Theory and Practice –*

WISTP'10, volume 6033 of *Lecture Notes in Computer Science*, pages 122–137, Passau, Germany, April 2010. Springer.

160. Julien Bringer and Hervé Chabanne. On the Wiretap Channel Induced by Noisy Tags. In Levente Buttyán, Virgil D. Gligor, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'06*, volume 4357 of *Lecture Notes in Computer Science*, pages 113–120, Hamburg, Germany, September 2006. Springer.
161. Julien Bringer and Hervé Chabanne. Trusted-HB: A Low-Cost Version of HB^+ Secure Against Man-in-the-Middle Attacks. *IEEE Transactions on Information Theory*, 54(9):4339–4342, 2008.
162. Julien Bringer, Hervé Chabanne, and Dottax Emmanuelle. HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006*, Lyon, France, June 2006. IEEE, IEEE Computer Society.
163. Julien Bringer, Hervé Chabanne, and Thomas Icart. Cryptanalysis of EC-RAC, a RFID identification protocol. In Matthew K. Franklin, Lucas Chi Kwong Hui, and Duncan S. Wong, editors, *7th International Conference on Cryptology And Network Security – CANS'08*, volume 5339 of *Lecture Notes in Computer Science*, pages 149–161, Hong Kong, China, December 2008. Springer.
164. Julien Bringer, Hervé Chabanne, and Thomas Icart. Improved Privacy of the Tree-Based Hash Protocols Using Physically Unclonable Function. In Rafail Ostrovsky, Roberto De Prisco, and Ivan Visconti, editors, *Proceedings of the 6th International Conference on Security and Cryptography for Networks – SCN'08*, volume 5229 of *Lecture Notes in Computer Science*, pages 77–91, Amalfi, Italy, August 2008. Springer.
165. Julien Bringer, Hervé Chabanne, and Thomas Icart. Efficient Zero-Knowledge Identification Schemes which respect Privacy. In Wanqing Li, Willy Susilo, Udaya Kiran Tupakula, Reihaneh Safavi-Naini, and Vijay Varadharajan, editors, *ACM Symposium on Information, Computer and Communication Security – ASIACCS'09*, pages 195–205, Sydney, Australia, March 2009. ACM, ACM Press.
166. Mayla Bruso, Konstantinos Chatzikokolakis, and Jerry den Hartog. Formal Verification of Privacy for RFID Systems. In *Computer Security Foundations Symposium – CSF 2010*, Edinburgh, United Kingdom, July 2010. IEEE.
167. Kai Bu, Xuan Liu, and Bin Xiao. Approaching the time lower bound on cloned-tag identification for large RFID systems. *Ad Hoc Networks*, (0), August 2013.
168. Trevor Burbridge and Mark Harrison. Security Considerations in the Design and Peering of RFID Discovery Services. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
169. Trevor Burbridge and Andrea Soppera. Supply Chain Control Using a RFID Proxy Re-signature Scheme. In *IEEE International Conference on RFID – IEEE RFID 2010*, pages 29–36, Orlando, Florida, USA, April 2010. IEEE, IEEE Computer Society.
170. Mike Burmester and Breno De Medeiros. Persistent Security for RFID. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
171. Mike Burmester and Breno de Medeiros. The Security of EPC Gen2 Compliant RFID Protocols. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *Proceedings of the 6th International Conference on Applied Cryptography and Network Security – ACNS 2008*, volume 5037 of *Lecture Notes in Computer Science*, pages 490–506, New York City, New York, USA, June 2008. Springer.
172. Mike Burmester, Breno de Medeiros, and Rossana Motta. Robust, Anonymous RFID Authentication with Constant Key-Lookup. Cryptology ePrint Archive, Report 2007/402, 2007.
173. Mike Burmester, Breno de Medeiros, and Rossana Motta. Anonymous RFID authentication supporting constant-cost key-lookup against active adversaries. *International Journal of Applied Cryptography*, 1(2):79–90, 2008.
174. Mike Burmester, Breno de Medeiros, and Rossana Motta. Provably Secure Grouping-Proofs for RFID Tags. In Gilles Grimaud and Franois-Xavier Standaert, editors, *Proceedings of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, volume 5189 of *Lecture Notes in Computer Science*, pages 176–190, Royal Holloway University of London, United Kingdom, September 2008. Springer.
175. Mike Burmester, Breno de Medeiros, Jorge Munilla, and Alberto Peinado. Secure EPC Gen2 compliant Radio Frequency Identification. Cryptology ePrint Archive, Report 2009/149, 2009.
176. Mike Burmester, Tri van Le, and Breno de Medeiros. Provably Secure Ubiquitous Systems: Universally Composable RFID Authentication Protocols. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2006*, pages 1–10, Baltimore, Maryland, USA, August–September 2006. IEEE, IEEE Computer Society.

177. Mike Burmester, Tri van Le, and Breno de Medeiros. Towards Provable Security for Ubiquitous Applications. In Lynn Margaret Batten and Reihaneh Safavi-Naini, editors, *Australasian Conference on Information Security and Privacy – ACISP'06*, volume 4058 of *Lecture Notes in Computer Science*, pages 295–312, Melbourne, Australia, July 2006. Springer.
178. Mike Burmester, Tri van Le, and Breno de Medeiros. Universally Composable RFID Identification and Authentication Protocols. *ACM Transactions on Information and System Security – TISSEC'09*, 12(4):21:1–21:33, 2009.
179. Mike Burmester and Daniel Miller. Ad Hoc Subgroup Proofs for RFID. Technical Report TR-110415, Florida State University - Computer Science, Tallahassee, Florida, USA, 2010.
180. Mike Burmester and Jorge Munilla. A Flyweight RFID Authentication Protocol. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
181. Mike Burmester and Jorge Munilla. Distributed group authentication for RFID supply management. Cryptology ePrint Archive, Report 2013/779, 2013.
182. Laurent Bussard and Walid Bagga. Distance-bounding proof of knowledge to avoid real-time attacks. In Ryoichi Sasaki, Sihan Qing, and Eiji Okamoto, editors, *Security and Privacy in the Age of Ubiquitous Computing*, volume 181 of *IFIP International Federation for Information Processing*, pages 223–238, Chiba, Japan, June 2005. Springer-Verlag.
183. Levente Buttyán, Tamás Holczer, and István Vajda. Optimal Key-Trees for Tree-Based Private Authentication. In George Danezis and Philippe Golle, editors, *Workshop on Privacy Enhancing Technologies – PET 2006*, volume 4258 of *Lecture Notes in Computer Science*, pages 332–350, Cambridge, United Kingdom, June 2006. Springer.
184. Qing Ling Cai, Yi Ju Zhan, and Jian Yang. The improvement of RFID authentication protocols based on R-RAPSE. *Journal of Networks*, 9(1):28–35, January 2014.
185. QingLing Cai, YiJu Zhan, and Jian Yang. RFID authentication protocol design methodology. *International Journal of Embedded Systems*, 7(2), 2015.
186. Shaoying Cai, Robert Deng, Yingjiu Li, and Yunlei Zhao. A new framework for privacy of RFID path authentication. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Proceedings of the 10th International Conference on Applied Cryptography and Network Security – ACNS 2012*, Singapore, China, June 2012.
187. Shaoying Cai, Yingjiu Li, Tieyan Li, Robert H. Deng, and Haixia Yao. Achieving High Security and Efficiency in RFID-tagged Supply Chains. *International Journal of Applied Cryptography*, 2(1):3–12, 2010.
188. Shaoying Cai, Yingjiu Li, and Yunlei Zhao. Distributed path authentication for dynamic RFID-enabled supply chains. In *IFIP TC-11 27rd International Information Security Conference – SEC 2012*, Heraklion, Crete, Greece, June 2012.
189. Benoit Calmels, Sébastien Canard, Marc Girault, and Hervé Sibert. Low-Cost Cryptography for Privacy in RFID Systems. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 237–251, Tarragona, Spain, April 2006. IFIP, Springer.
190. Sébastien Canard and Iwen Coisel. Data Synchronization in Privacy-Preserving RFID Authentication Schemes. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
191. Sébastien Canard, Iwen Coisel, Jonathan Etrog, and Marc Girault. Privacy-Preserving RFID Systems: Model and Constructions. Cryptology ePrint Archive, Report 2010/405, 2010.
192. Sébastien Canard, Iwen Coisel, and Marc Girauld. Security of Privacy-Preserving RFID Systems. In *IEEE International Conference on RFID-Technology and Applications – RFID-TA'10*, pages 269–274, Guangzhou, China, June 2010. Sun Yat-sen University, IEEE.
193. Sébastien Canard, Jonathan Etrog, and Iwen Coisel. Lighten Encryption Schemes for Secure and Private RFID Systems. In Radu Sion, Reza Curtmola, Sven Dietrich, Aggelos Kiayias, Josep M. Miret, Kazue Sako, and Francesc Seb, editors, *1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices – WLC'10*, volume 6054 of *Lecture Notes in Computer Science*, pages 19–33, Tenerife, Canary Islands, Spain, January 2010. Springer.
194. Xiaolin Cao and Maire O'Neill. A private and scalable authentication for RFID systems using reasonable storage. In *10th International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2011*, pages 373–380, November 2011.
195. Srdjan Capkun, Karim El Defrawy, and Gene Tsudik. GDB: Group Distance Bounding Protocols. arXiv.org, Computer Science, Cryptography and Security, 2010.
196. Dario Carluccio, Timo Kasper, and Christof Paar. Implementation Details of a Multi Purpose ISO 14443 RFID-Tool. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.

197. Dario Carluccio, Kerstin Lemke, and Christof Paar. Electromagnetic Side Channel Analysis of a Contactless Smart Card: First Results. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
198. Dario Carluccio, Kerstin Lemke, Christof Paar, and Ahmad-Reza Sadeghi. E-passport: the Global Traceability or How to Feel Like an UPS Package. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
199. Dario Carluccio, Kerstin Lemke, Christof Paar, and Ahmad-Reza Sadeghi. E-passport: the global traceability or how to feel like an ups package. In Jae-Kwang Lee, Okyeon Yi, and Moti Yung, editors, *Workshop on Information Security Applications – WISA'06*, volume 4298 of *Lecture Notes in Computer Science*, pages 391–404, Jeju Island, Korea, August 2006. Springer.
200. Jose Carrijo, Rafael Tonicelli, and Anderson C. A. Nascimento. A Fault Analytic Method against HB+. Cryptology ePrint Archive, Report 2010/508, 2010.
201. Claude Castelluccia and Gildas Avoine. Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 289–299, Tarragona, Spain, April 2006. IFIP, Springer.
202. Claude Castelluccia and Mate Soos. Secret Shuffing: A Novel Approach to RFID Private Identification. In *Workshop on RFID Security – RFIDSec'07*, pages 169–180, Malaga, Spain, July 2007.
203. Shi-Cho Cha, Kuan-Ju Huang, and Hsiang-Meng Chang. An Efficient and Flexible Way to Protect Privacy in RFID Environment with Licenses. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 35–42, April 2008.
204. Rafik Chaabouni and Serge Vaudenay. The Extended Access Control for Machine Readable Travel Documents. In *Proceedings of the Special Interest Group on Biometrics and Electronic Signatures – BIOSIG 2009*, volume 155 of *Lecture Notes in Informatics*, pages 93–103, Darmstadt, Germany, September 2009. Gesellschaft für Informatik (GI).
205. Hervé Chabanne and Guillaume Fumaroli. Noisy Cryptographic Protocols for Low Cost RFID Tags. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
206. Herv Chabanne and Cline Chevalier. Vaudenays privacy model in the universal composability framework: A case study. In Changhoon Lee, Jean-Marc Seigneur, James J. Park, and Roland R. Wagner, editors, *Secure and Trust Computing, Data Management, and Applications*, volume 187 of *Communications in Computer and Information Science*, pages 16–24. Springer Berlin Heidelberg, June 2011.
207. Hee-Jin Chae, Daniel Yeager, Joshua Smith, and Kevin Fu. Maximalist Cryptography and Computation on the WISP UHF RFID Tag. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
208. Qi Chai. *Design and Analysis of Security Schemes for Low-cost RFID Systems*. PhD thesis, University of Waterloo, University of Waterloo, Waterloo, Ontario, Canada, January 2012.
209. Qi Chai and Guang Gong. BUPLE: Securing Passive RFID Communication Through Physical Layer Enhancements. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
210. Gwo-Ching Chang. A Feasible Security Mechanism for Low Cost RFID Tags. In *International Conference on Mobile Business – ICMB'05*, pages 675–677, Sydney, Australia, July 2005. IEEE, IEEE Computer Society.
211. Jen-Chun Chang and Hsin-Lung Wu. A Hybrid RFID Protocol against Tracking Attacks. Cryptology ePrint Archive, Report 2009/138, 2009.
212. Christy Chatmon, Tri van Le, and Mike Burmester. Secure Anonymous RFID Authentication Protocols. Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA, 2006.
213. Nidhi Chauhan. Vulnerability and countermeasures of RFID system. *International Journal of Engineering and Technical Research*, 2(9):235–237, September 2014.
214. Kirti Chawla, Gabriel Robins, and Westley Weimer. On the Presence of Covert Channels Embedded within RFID-Enabled Supply Chains. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
215. Wenyi Che, Huan Deng, Wang Tan, and Junyu Wang. *A Random Number Generator for Application in RFID Tags*, chapter 16, pages 279–287. Springer Berlin Heidelberg, 2008.
216. Chien-Ming Chen, Shuai-Min Chen, Xinying Zheng, Pei-Yu Chen, and Hung-Min Sun. A secure RFID authentication protocol adopting error correction code. *The Scientific World Journal*, March 2014.
217. Chin-Ling Chen and Chih-Feng Chien. An ownership transfer scheme using mobile RFIDs. *Wireless Personal Communications*, pages 1–27, January 2012.
218. Min Chen and Shigang Chen. An efficient anonymous authentication protocol for RFID systems using dynamic tokens. In *International Conference on Distributed Computing Systems – ICDCS 2015*, pages 756–757, Columbus, OH, USA, June 2015. IEEE.

219. Min Chen, Wen Luo, Zhen Mo, Shigang Chen, and Yuguang Fang. An efficient tag search protocol in large-scale RFID systems. In *IEEE InfoCom 2013*, Turin, Italy, April 2013. IEEE.
220. Xiuqing Chen, Tianjie Cao, and Yu Guo. A new scalable RFID delegation protocol. *Applied Mathematics and Information Sciences*, 8(4):1917–1924, February 2014.
221. Shu Cheng. Security and authentication schemes in RFID. Master thesis, University of Wollongong, Wollongong, New South Wales, Australia, December 2011.
222. Jung Hee Cheon, Jeongdae Hong, and Gene Tsudik. Reducing RFID Reader Load with the Meet-in-the-Middle Strategy. Cryptology ePrint Archive, Report 2009/092, 2009.
223. Jung Hee Cheon, Jeongdae Hong, and Gene Tsudik. Reducing RFID reader load with the meet-in-the-middle strategy. *Journal of Communications and Networks*, 14(1):10–14, February 2012.
224. 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.
225. Hung-Yu Chien. Combining rabin cryptosystem and error correction codes to facilitate anonymous authentication with un-traceability for low-end devices. *Computer Networks*, (0), June 2013.
226. Hung-Yu Chien. De-synchronization attack on quadratic residues-based RFID ownership transfer. In *Asia Joint Conference on Information Security – AsiaJCIS 2015*, pages 42–47, Kaohsiung, Taiwan, May 2015. IEEE.
227. Hung-Yu Chien and Che-Hao Chen. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 standards. *Computer Standars & Interfaces, Elsevier*, 29(2):254–259, February 2007.
228. Hung-Yu Chien and Chen-Wei Huang. A Lightweight RFID Protocol Using Substring. In Tei-Wei Kuo, Edwin Hsing-Mean Sha, Minyi Guo, Laurence Tianruo Yang, and Zili Shao, editors, *Embedded and Ubiquitous Computing – EUC'07*, volume 4808 of *Lecture Notes in Computer Science*, pages 422–431, Taipei, Taiwan, December 2007. Springer.
229. Hung-Yu Chien, Chu-Sing Yang, and Hung-Pin Hou. Non-linearity cannot help RFID resist full-disclosure attacks and terrorist fraud attacks. *Security and Communication Networks*, 2012.
230. Hung-yu Chien, Ming-kuei Yeh, Tzong-chen Wu, and Chin-i Lee. Comments on enhanced yoking proof protocols for radio frequency identification tags and tag groups. *Journal of Shanghai Jiaotong University (Science)*, 16(5):604–609, 2011.
231. Kevin Chiew, Yingjiu Li, Tieyan Li, and Robert H. Deng. On False Authentications for C1G2 Passive RFID Tags. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 50–65, Wuxi, China, April 2011. IOS Press.
232. Noureddine Chikouche, Foudil Cherif, and Mohamed Benmohammed. An authentication protocol based on combined RFID-biometric system. *International Journal of Advanced Computer Science and Applications*, 3(4):62–67, 2012.
233. Noureddine Chikouche, Foudil Cherif, and Mohamed Benmohammed. Vulnerabilities of two recently RFID authentication protocols. In *International Conference on Computer Science – ICCS 2012*, pages 1–6, November 2012.
234. Noureddine Chikouche, Foudil Cherif, and Mohamed Benmohammed. Algebraic replay attacks on authentication in RFID protocols. In Ali Ismail Awad, Aboul Ella Hassanien, and Kensuke Baba, editors, *Advances in Security of Information and Communication Networks – SecNet 2013*, volume 381 of *Communications in Computer and Information Science*, pages 153–163, Cairo, Egypt, September 2013. Springer Berlin Heidelberg.
235. Noureddine Chikouche, Foudil Cherif, Louis Cayrel, and Mohamed Benmohammed. A secure code-based authentication scheme for RFID systems. *International Journal on Computer Network and Information Security*, 9:1–9, August 2015.
236. Noureddine Chikouche, Foudil Cherif, Pierre-Louis Cayrel, and Mohamed Benmohammed. Improved RFID authentication protocol based on randomized McEliece cryptosystem. *International Journal of Network Security*, 17(4):413–422, July 2015.
237. Noureddine Chikouche, Foudil Cherif, Pierre-Louis Cayrel, and Mohamed Benmohammed. Weaknesses in two RFID authentication protocols. In *Codes, Cryptology, and Information Security – C2SI 2015*, volume 9084 of *Lecture Notes in Computer Science*, pages 162–172, Rabat, Morocco, May 2015. Springer.
238. Eun Young Choi, Su Mi Lee, and Dong Hoon Lee. Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. In Tomoya Enokido, Lu Yan, Bin Xiao, Daeyoung Kim, Yuanshun Dai, and Laurence Yang, editors, *International Workshop on Security in Ubiquitous Computing Systems – SecUbiq 2005*, volume 3823 of *Lecture Notes in Computer Science*, pages 945–954, Nagasaki, Japan, December 2005. Springer.
239. Soo-Hyun Choi and You-Hyeon Jeong. A Secure and Scalable Transaction Protocol for Ubiquitous Sensor Network using RFID Systems. In *International Conference on Advanced Communication Technology – ICACT 2008*, volume 3, pages 1781–1784, Phoenix Park, Korea, February 2008. IEEE, IEEE Computer Society.

240. Wonjoon Choi and Byeong-hee Roh. Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Lagan, Youngsong Mun, and Hyunseung Choo, editors, *International Conference on Computational Science and its Applications – ICCSA 2006, Proceedings, Part IV*, volume 3983 of *Lecture Notes in Computer Science*, pages 279–287, Glasgow, Scotland, May 2006. Springer.
241. Yongje Choi, Mooseop Kim, Taesung Kim, and Howon Kim. Low power implementation of SHA-1 algorithm for RFID system. In *IEEE Tenth International Symposium on Consumer Electronics – ISCE '06*, pages 1–5, St.Petersburg, Russia, September 2006. IEEE, IEEE Computer Society.
242. Tom Chothia and Vitaliy Smirnov. A traceability attack against e-passports. In Radu Sion, editor, *14th International Conference on Financial Cryptography and Data Security – FC'10*, volume 6052 of *Lecture Notes in Computer Science*, pages 20–34, Tenerife, Canary Islands, Spain, January 2010. IFCA, Springer.
243. Jue-Sam Chou. A constant-time identifying large-scale RFID tags using lines on a plane. *Transactions on Emerging Telecommunications Technologies*, April 2013.
244. Jue-Sam Chou. An efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, December 2013.
245. Jue-Sam Chou, Guey-Chuen Lee, and Chung-Ju Chan. A Novel Mutual Authentication Scheme Based on Quadratic Residues for RFID Systems. Cryptology ePrint Archive, Report 2007/224, 2007.
246. Hau Leung Harold Chung. Chaos based RFID authentication protocol. Master thesis, University of Ottawa, Ottawa, Canada, 2013.
247. Su Chunhua, Li Yingjiu, Zhao Yunlei, H. Deng Robert, Zhao Yiming, and Zhou Jianying. A survey on privacy frameworks for RFID authentication. *IEICE Transactions on Information and Systems*, E95.D(1):2–11, January 2012.
248. Jacek Cichon, Marek Klonowski, and Miroslaw Kutylowski. Privacy Protection in Dynamic Systems Based on RFID Tags. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 235–240, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
249. Iwen Coisel and Tania Martin. Untangling RFID privacy models. Cryptology ePrint Archive, Report 2011/636, 2011.
250. Iwen Coisel and Tania Martin. Untangling RFID privacy models. *Journal of Computer Networks and Communications*, July 2012.
251. Iwen Coisel and Tania Martin. Untangling RFID privacy models. *Journal of Computer Networks and Communications*, 2013.
252. Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Angelo Spognardi. FastRIPP: RFID Privacy Preserving protocol with Forward Secrecy and Fast Resynchronization. In *33th Annual Conference of the IEEE Industrial Electronics Society (IEEE IECON 07)*, pages 52–57, Taipei, Taiwan, November 2007. IEEE, IEEE Computer Society.
253. Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini, and Angelo Spognardi. RIPP-FS: an RFID Identification, Privacy Preserving Protocol with Forward Secrecy. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 229–234, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
254. Mauro Conti, Roberto Di Pietro, and Angelo Spognardi. "Who Counterfeited My Viagra?" Probabilistic Item Removal Detection via RFID Tag Cooperation. *EURASIP Journal on Wireless Communications and Networking*, 2011, 2011.
255. Pier Francesco Cortese, Francesco Gemmiti, Bernardo Palazzi, Maurizio Pizzonia, and Massimo Rimondini. Efficient and practical authentication of PUF-based RFID tags in supply chains. In *IEEE International Conference on RFID-Technology and Applications – RFID-TA'10*, pages 182–188, Guangzhou, China, June 2010. Sun Yat-sen University, IEEE.
256. Nicolas T. Courtois. The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
257. Nicolas T. Courtois, Karsten Nohl, and Sean O'Neil. Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166, 2008.
258. Nicolas T. Courtois, Sean O'Neil, and Jean-Jacques Quisquater. Practical Algebraic Attacks on the Hitag2 Stream Cipher. In Pierangela Samarati, Moti Yung, Fabio Martinelli, and Claudio Agostino Ardagna, editors, *Information Security Conference – ISC'09*, volume 5735 of *Lecture Notes in Computer Science*, pages 167–176, Pisa, Italy, September 2009. Springer.
259. Cas Cremers, Kasper Bonne Rasmussen, and Srdjan Capkun. Distance Hijacking Attacks on Distance Bounding Protocols. Cryptology ePrint Archive, Report 2011/129, 2011.

260. Cas Cremers, Kasper Bonne Rasmussen, Benedikt Schmidt, and Srdjan Capkun. Distance hijacking attacks on distance bounding protocols. In *IEEE Symposium on Security and Privacy – S&P '12*, San Francisco, California, USA, May 2012. IEEE, IEEE Computer Society.
261. Yang Cui, Kazukuni Kobara, Kanta Matsuura, and Hideki Imai. Lightweight Asymmetric Privacy-Preserving Authentication Protocols Secure against Active Attack. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 223–228, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
262. Stefan Dahl. Anonymous Car Toll Payments using RFID Tags. Master thesis, Royal Institute of Technology, Stockholm, Sweden, 2006.
263. Gökhan Dalkiliç, Mehmet Hilal Özcanhan, and Hafize Şen Çakir. Increasing key space at little extra cost in RFID authentications. *Turkish Journal of Electrical Engineering & Computer Sciences*, 22(1):155–165, October 2014.
264. Ivan Damgård and Michael Østergaard. RFID Security: Tradeoffs between Security and Efficiency. Cryptology ePrint Archive, Report 2006/234, 2006.
265. Boris Danev, Thomas S. Heydt-Benjamin, and Srdjan Čapkun. Physical-layer identification of RFID devices. In *18th USENIX Security Symposium – USENIX'09*, pages 199–214, Montreal, Canada, August 2009. USENIX, USENIX Association.
266. Paolo D'Arco and Alfredo De Santis. On Ultra-Lightweight RFID Authentication Protocols. *IEEE Transactions on Dependable and Secure Computing*, 99(PrePrints), 2010.
267. Paolo D'Arco, Alessandra Scafuro, and Ivan Visconti. Semi-Destructive Privacy in RFID Systems. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
268. Mathieu David. *Lightweight Cryptography for Passive RFID Tags*. PhD thesis, Aalborg University, Aalborg, Denmark, December 2011.
269. Mathieu David and Neeli R. Prasad. Providing strong security and high privacy in low-cost RFID networks. In Andreas U. Schmidt, Shiguo Lian, Ozgur Akan, Paolo Bellavista, Jiannong Cao, Falko Dressler, Domenico Ferrari, Mario Gerla, Hisashi Kobayashi, Sergio Palazzo, Sartaj Sahni, Xuemin (Sherman) Shen, Mircea Stan, Jia Xiaohua, Albert Zomaya, and Geoffrey Coulson, editors, *Security and Privacy in Mobile Information and Communication Systems*, volume 17 of *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pages 172–179, Turin, Italy, June 2009. Springer Berlin Heidelberg.
270. Mathieu David, Damith C. Ranasinghe, and Torben Larsen. A2U2: A stream cipher for printed electronics RFID tags. In *IEEE International Conference on RFID – IEEE RFID 2011*, pages 176–183, Orlando, Florida, USA, 2011. IEEE, IEEE Computer Society.
271. Gerhard de Koning Gans. Analysis of the Mifare Classic used in the OV-Chipkaart Project. Master's thesis, Radboud University Nijmegen, 2008.
272. Gerhard de Koning Gans. *Outsmarting Smart Cards*. PhD thesis, Radboud Universiteit Nijmegen, Nijmegen, Netherlands, March 2013.
273. Gerhard de Koning Gans and Flavio Garcia. Towards a Practical Solution to the RFID Desynchronization Problem. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 203–219, Istanbul, Turkey, June 2010. Springer.
274. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In Gilles Grimaud and Franois-Xavier Standaert, editors, *Proceedings of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, volume 5189 of *Lecture Notes in Computer Science*, pages 267–282, Royal Holloway University of London, United Kingdom, September 2008. Springer.
275. Benessa Defend, Kevin Fu, and Ari Juels. Cryptanalysis of Two Lightweight RFID Authentication Schemes. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2007*, pages 211–216, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
276. Masoud Hadian Dehkordi and Yousof Farzaneh. Improvement of the hash-based RFID mutual authentication protocol. *Wireless Personal Communications*, August 2013.
277. Guanyang Deng, Hui Li, Ying Zhang, and Jun Wang. Tree-LSHB+: An LPN-based lightweight mutual authentication RFID protocol. *Wireless Personal Communications*, pages 1–16, January 2013.
278. Miao Lei Deng, Hao Jun Zhang, and Wei Jun Zhu. Data desynchronization attacks on two lightweight security protocols for the rfid system. *Applied Mechanics and Materials*, 241:2331–2334, December 2012.
279. Miaolei Deng and Weijun Zhu. Desynchronization attacks on RFID security protocols. *Telkomnika Indonesian Journal of Electrical Engineering*, 11(2), February 2013.
280. Robert H. Deng, Yingjiu Li, Moti Yung, and Yunlei Zhao. A New Framework for RFID Privacy. In Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou, editors, *15th European Symposium on Research in*

Computer Security – ESORICS 2010, volume 6345 of *Lecture Notes in Computer Science*, pages 1–18, Athens, Greece, September 2010. Springer.

281. Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola, and Vivek Khandelwal. Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 58–64, April 2008.
282. Subhasish Dhal and Indranil Sengupta. Handling authentication and detection probability in multi-tag RFID environment. Cryptology ePrint Archive, Report 2013/486, 2013.
283. Roberto Di Pietro and Refik Molva. Information Confinement, Privacy, and Security in RFID Systems. In Joachim Biskup and Javier Lopez, editors, *12th European Symposium On Research In Computer Security – ESORICS 2007*, volume 4734 of *Lecture Notes in Computer Science*, pages 187–202, Dresden, Germany, September 2007. Springer.
284. Roberto Di Pietro and Refik Molva. An optimal probabilistic solution for information confinement, privacy, and security in RFID systems. *Journal of Network and Computer Applications*, May 2010.
285. Kurt Dietrich. Anonymous RFID Authentication using Trusted Computing Technologies. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 91–102, Istanbul, Turkey, June 2010. Springer.
286. Christos Dimitrakakis, Aikaterini Mitrokotsa, and Serge Vaudenay. Expected loss bounds for authentication in constrained channels. In *IEEE InfoCom 2012*, Orlando, FL, USA, March 2012. IEEE.
287. Antonis Dimitriou, Aggelos Bletsas, and Sahalos John Polycarpou, Anastasis. Theoretical Findings and Measurements on Planning a UHF RFID System inside a Room. *Radioengineering*, 20(2):387–397, 2011.
288. Tassos Dimitriou. A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 59–66, Athens, Greece, September 2005. IEEE, IEEE Computer Society.
289. Tassos Dimitriou. A Secure and Efcient RFID Protocol that could make Big Brother (partially) Obsolete. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, pages 269–275, Pisa, Italy, March 2006. IEEE, IEEE Computer Society.
290. Tassos Dimitriou. Proxy Framework for Enhanced RFID Security and Privacy. In *Fifth Annual IEEE Consumer Communications and Networking Conference – CCNC 2007*, Las Vegas, Nevada, USA, January 2008. IEEE, IEEE Computer Society.
291. Tassos Dimitriou. RFID-DOT: RFID Delegation and Ownership Transfer made simple. In *Conference on Security and Privacy for Communication Networks – SecureComm 2008*, pages 1–8, Istanbul, Turkey, September 2008. IEEE, IEEE Computer Society.
292. Tassos Dimitriou. RFID Security and Privacy. In Paris Kitsos and Yan Zhang, editors, *RFID Security: Techniques, Protocols and System-on-Chip Design*, pages 57–79. Springer, September 2008.
293. Tassos Dimitriou. Key evolving RFID systems: Forward/backward privacy and ownership transfer of RFID tags. *Ad Hoc Networks*, September 2015.
294. Vaibhaw Dixit, Harsh Kumar Verma, and Akhil Kumar Singh. Comparison of various security protocols in rfid. *International Journal of Computer Applications*, 24(7):17–21, June 2011.
295. Shlomi Dolev, Marina Kopeetsky, and Adi Shamir. RFID Authentication Efficient Proactive Information Security within Computational Security. *Theory of Computing Systems*, 48(1):132–149, 2009.
296. Sandra Dominikus, Hannes Gross, Manfred Aigner, and Stefan Kraxberger. Low-cost RFID Tags as IPv6 Nodes in the Internet of Things. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 114–128, Wuxi, China, April 2011. IOS Press.
297. Sandra Dominikus, Elisabeth Oswald, and Martin Feldhofer. Symmetric Authentication for RFID Systems in Practice. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
298. Robin Doss, Saravanan Sundaresan, and Wanlei Zhou. A practical quadratic residues based scheme for authentication and privacy in mobile RFID systems. *Ad How Networks*, July 2012.
299. Robin Doss, Zhou Wanlei, and Yu Shui. Secure RFID tag ownership transfer based on quadratic residues. *IEEE Transactions on Information Forensics and Security*, 8(2):390 – 401, February 2013.
300. Robin Doss, Wanlei Zhou, Saravanan Sundaresan, Shui Yu, and Longxiang Gao. A minimum disclosure approach to authentication and privacy in RFID systems. *Computer Networks*, July 2012.
301. Pierre Dusart and Sinaly Traoré. Lightweight authentication protocol for low-cost RFID tags. In Lorenzo Cavallaro and Dieter Gollmann, editors, *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems – WISTP 2013*, volume 7886 of *Lecture Notes in Computer Science*, pages 129–144, Heraklion, Greece, May 2013. Springer Berlin Heidelberg.

302. Paolo DArco. An Almost-Optimal Forward-Private RFID Mutual Authentication Protocol with Tag Control. In Claudio Ardagna and Jianying Zhou, editors, *Workshop on Information Security Theory and Practice – WISTP'11*, volume 6633 of *Lecture Notes in Computer Science*, pages 69–84, Heraklion, Crete, Greece, June 2011. Springer.
303. Aras Eghdamian and Azman Samsudin. A secure protocol for ultralightweight radio frequency identification (RFID) tags. In Azizah Abd Manaf, Akram Zeki, Mazdak Zamani, Suriayati Chuprat, and Eyas El-Qawasmeh, editors, *Informatics Engineering and Information Science – ICIEIS 2011*, volume 251 of *Communications in Computer and Information Science*, pages 200–213, Kuala Lumpur, Malaysia, November 2011. Springer Berlin Heidelberg.
304. Ethmane El Moustaine. *Authentication issues in low-cost RFID*. PhD thesis, Tlcom Sudparis and Universit Pierre et Marie Curie, Paris, France, December 2013.
305. Ethmane El Moustaine and Maryline Laurent. A lattice based authentication for low-cost RFID. In *2012 IEEE International Conference on RFID Technologies and Applications – RFID-TA 2012*, pages 68–73, Nice, France, November 2012.
306. Ethmane El Moustaine and Maryline Laurent. GPS+: a back-end coupons identification for low-cost RFID. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks – WiSec'13*, WiSec'13, pages 73–78, New York, USA, April 2013. ACM.
307. Kaoutar Elkhiyaoui, Erik-Oliver Blass, and Refik Molva. ROTIV: RFID Ownership Transfer with Issuer Verification. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
308. Kaoutar Elkhiyaoui, Erik-Oliver Blass, and Refik Molva. CHECKER: on-site checking in RFID-based supply chains. In *Proceedings of the 5th ACM Conference on Wireless Network Security – WiSec'12*, pages 173–184, Tucson, Arizona, USA, April 2012. ACM, ACM Press.
309. Kaoutar Elkhiyaoui, Erik-Oliver Blass, and Refik Molva. T-MATCH: Privacy-preserving item matching for storage-only RFID tags. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
310. Kosei Endo and Noboru Kunihiro. Security analysis on AUTH protocol and its variant against the man-in-the-middle attack. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E98-A(1):153–161, January 2015.
311. Stephan Engberg, Morten Harning, and Christian Damsgaard Jensen. Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In *Conference on Privacy, Security and Trust – PST'04*, pages 89–101, New Brunswick, Canada, October 2004.
312. Daniel Engels, Markku-Juhani O. Saarinen, and Eric M. Smith. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
313. Daniel W. Engels, You Sung Kang, and Junyu Wang. On security with the new Gen2 RFID security framework. In *IEEE International Conference on RFID – IEEE RFID 2013*, pages 144–151. IEEE, IEEE Computer Society, April 2013.
314. Rahim Entezari, Hossein Bahramgiri, and Mahnaz Tajamolian. A mafia and distance fraud high-resistance RFID distance bounding protocol. In *International ISC Conference on Information Security and Cryptology – ISCISC 2014*, pages 67–72, Tehran, Iran, September 2014. IEEE.
315. Rahim Entezari, Hossein Bahramgiri, and Mahnaz Tajamolian. An RFID unilateral distance bounding protocol and analysis over a noisy channel. *International Journal of Mechatronics, Electrical and Computer Technology*, 5(14):1–26, January 2015.
316. Imran Erguler. *Security and Privacy Analysis of Authentication Protocols in RFID Systems*. PhD thesis, Bogazici University, Bogazici University Electrical-Electronics Engineering, Istanbul, Turkey, June 2011.
317. Imran Erguler and Emin Anarim. Scalability and Security Conflict for RFID Authentication Protocols. Cryptology ePrint Archive, Report 2010/018, 2010.
318. Imran Erguler and Emin Anarim. Practical attacks and improvements to an efficient radio frequency identification authentication protocol. *Concurrency and Computation: Practice and Experience*, October 2011.
319. Imran Erguler and Emin Anarim. Security flaws in a recent RFID delegation protocol. *Personal and Ubiquitous Computing*, May 2011.
320. Imran Erguler, Emin Anarim, and Gokay Saldamli. A Salient Missing Link in RFID Security Protocols. *EURASIP Journal on Wireless Communications and Networking*, 2011, 2011.
321. Imran Erguler, Emin Anarim, and Gokay Saldamli. Unbalanced states violates RFID privacy. *Journal of Intelligent Manufacturing*, 23:1–9, 2012.
322. Benjamin Fabian, Oliver Günther, and Sarah Spiekermann. Security Analysis of the Object Name Service for RFID. In *International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU'05*, Santorini Island, Greece, July 2005. IEEE, IEEE Computer Society.

323. Abolfazl Falahati and Hoda Jannati. Application of distance bounding protocols with random challenges over RFID noisy communication systems. In *IET Conference on Wireless Sensor Systems – WSS 2012*, London, UK, June 2012.
324. Abolfazl Falahati and Hoda Jannati. All-or-nothing approach to protect a distance bounding protocol against terrorist fraud attack for low-cost devices. *Electronic Commerce Research*, November 2014.
325. Junfeng Fan, Jens Hermans, and Frederik Vercauteren. On the claimed privacy of EC-RAC III. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 66–74, Istanbul, Turkey, June 2010. Springer.
326. Junfeng Fan and Ingrid Verbauwhede. Hyperelliptic curve processor for RFID tags. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
327. Kai Fan, Yuanyuan Gong, Chen Liang, Hui Li, and Yintang Yang. Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. *Security and Communication Networks*, August 2015.
328. Xinxin Fan, Guang Gong, Daniel W. Engels, and Eric M. Smith. A lightweight privacy-preserving mutual authentication protocol for RFID systems. In *IEEE GLOBECOM Workshops*, pages 1083–1087. IEEE, December 2011.
329. Yousof Farzaneh, Mahdi Azizi, Masoud Dehkordi, and Abdolrasoul Mirghadri. Vulnerability analysis of two ultra lightweight RFID authentication protocols. *International Arab Journal of Information Technology*, 12(4):340–345, July 2015.
330. Martin Feldhofer. A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags, 2003.
331. Martin Feldhofer. An Authentication Protocol in a Security Layer for RFID Smart Tags. In *The 12th IEEE Mediterranean Electrotechnical Conference – MELECON 2004*, volume 2, pages 759–762, Dubrovnik, Croatia, May 2004. IEEE, IEEE Computer Society.
332. Martin Feldhofer. *Low-Power Hardware Design of Cryptographic Algorithms for RFID Tags*. PhD thesis, Graz University of Technology, Institute for Applied Information Processing and Communications (IAIK), Graz, Austria, November 2008.
333. Martin Feldhofer, Manfred Aigner, and Sandra Dominikus. An Application of RFID Tags using Secure Symmetric Authentication. In *International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU'05*, pages 43–49, Santorini Island, Greece, July 2005. IEEE, IEEE Computer Society.
334. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In Marc Joye and Jean-Jacques Quisquater, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA, August 2004. IACR, Springer.
335. Martin Feldhofer and Christian Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In Robert Meersman, Zahir Tari, and Pilar Herrero, editors, *On the Move to Meaningful Internet Systems 2006 – OTM 2006*, volume 4277 of *Lecture Notes in Computer Science*, pages 372–381, Montpellier, France, November 2006. Springer.
336. Martin Feldhofer and Johannes Wolkerstorfer. Strong Crypto for RFID Tags – a Comparison of Low-Power Hardware Implementations. In *IEEE International Symposium on Circuits and Systems – ISCAS 2007*, pages 1839–1842, New Orleans, Louisiana, USA, May 2007. IEEE, IEEE Computer Society.
337. Martin Feldhofer, Johannes Wolkerstorfer, and Vincent Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings – Information Security*, 152(1):13–20, October 2005.
338. Albert Fernandez-Mir, Jordi Castella-Roca, and Alexandre Viejo. Secure and Scalable RFID Authentication Protocol. In *Third International Workshop on Autonomous and Spontaneous Security – SETOP'10*, Lecture Notes in Computer Science, Athens, Greece, September 2010. Springer.
339. Albert Fernandez-Mir, Rolando Trujillo-Rasua, and Jordi Castella-Roca. Scalable RFID Authentication Protocol Supporting Ownership Transfer and Controlled Delegation. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
340. Harinda Fernando and Jemal Abawajy. Mutual authentication protocol for networked RFID systems. In *10th International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2011*, pages 417–424, November 2011.
341. Rui Figueiredo, Andr Zquete, and Toms Oliveira Silva. Massively parallel identification of privacy-preserving vehicle RFID tags. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
342. Marc Fischlin and Cristina Onete. Provably secure distance-bounding: an analysis of prominent protocols. Cryptology ePrint Archive, Report 2012/128, 2012.

343. Marc Fischlin and Cristina Onete. Subtle kinks in distance-bounding: an analysis of prominent protocols. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks – WiSec'13*, WiSec'13, pages 195–206, New York, USA, April 2013. ACM.
344. Kenneth Fishkin, Sumit Roy, and Bing Jiang. Some Methods for Privacy in RFID Communication. In Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff, editors, *European Workshop on Security in Ad-hoc and Sensor Networks – ESAS'04*, volume 3313 of *Lecture Notes in Computer Science*, pages 42–53, Heidelberg, Germany, August 2004. Springer.
345. Christian Floerkemeier, Roland Schneider, and Marc Langheinrich. Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. In Hitomi Murakami, Hideyuki Nakashima, Hideyuki Tokuda, and Michiaki Yasumura, editors, *International Symposium on Ubiquitous Computing Systems – UCS 2004*, volume 3598 of *Lecture Notes in Computer Science*, pages 214–231, Tokyo, Japan, November 2004. Springer.
346. Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Effectiveness of Distance-decreasing Attacks Against Impulse Radio Ranging. In Susanne Wetzel, Cristina Nita-Rotaru, and Frank Stajano, editors, *Proceedings of the 3rd ACM Conference on Wireless Network Security – WiSec'10*, pages 117–128, Hoboken, New Jersey, USA, March 2010. ACM, ACM Press.
347. Sepideh Fouladgar and Hossam Afifi. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
348. Aurelien Francillon, Boris Danev, and Srdjan Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. Cryptology ePrint Archive, Report 2010/332, 2010.
349. Aurélien Francillon, Boris Danev, and Srdjan Čapkun. Relay attacks on passive keyless entry and start systems in modern cars. In *Network and Distributed System Security Symposium*, San Diego, California, USA, February 2011.
350. Lishoy Francis, Gerhard Hancke, and Keith Mayes. A practical generic relay attack on contactless transactions by using NFC mobile phones. *International Journal of RFID Security and Cryptography*, 2(1):92–106, December 2013.
351. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Potential misuse of NFC enabled mobile phones with embedded security elements as contactless attack platforms. In *International Conference for Internet Technology and Secured Transactions – ICITST'09*, pages 1–8, London, UK, November 2009. IEEE, IEEE Computer Society.
352. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. On the security issues of NFC enabled mobile phones. *International Journal of Internet Technology and Secured Transactions*, 2(3/4):336–356, 2010.
353. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. A security framework model with communication protocol translator interface for enhancing NFC transactions. In *Advanced International Conference on Telecommunications – AICT 2010*, pages 452–461, Barcelona, Spain, May 2010. IEEE, IEEE Computer Society.
354. Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using NFC mobile phones. Cryptology ePrint Archive, Report 2011/618, 2011.
355. Lishoy Francis, Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical NFC Peer-to-Peer Relay Attack using Mobile Phones. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 35–49, Istanbul, Turkey, June 2010. Springer.
356. Dmitry Frumkin and Adi Shamir. Un-Trusted-HB: Security Vulnerabilities of Trusted-HB. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
357. Benjamin Fung, Khalil Al-Hussaeni, and Ming Cao. Preserving RFID Data Privacy. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
358. Sebastien Gambs, Cristina Onete, and Jean-Marc Robert. Prover anonymous and deniable distance-bounding authentication. Cryptology ePrint Archive, Report 2014/114, 2014.
359. Lijun Gao, Maode Ma, Yantai Shu, Feng Lin, Lei Zhang, and Yuhua Wei. A low-cost RFID authentication protocol against desynchronization with a random tuple. *Wireless Personal Communications*, October 2014.
360. Lijun Gao, Maode Ma, Yantai Shu, and Chunfeng Liu. Design and analysis of a low cost multiple-secret-key RFID security protocol. In *International Conference on Computer Science and Network Technology – ICCSNT 2011*, volume 2, pages 914–917, December 2011.
361. Lijun Gao, Maode Ma, Yantai Shu, and Chunfeng Liu. RFID security protocol trace attack and desynchronizing attack deep research. In *International Conference on Computer Science and Network Technology – ICCSNT 2011*, volume 2, pages 918–922, December 2011.

362. Lijun Gao, Maode Ma, Yantai Shu, and Yuhua Wei. A security protocol resistant to intermittent position trace attacks and desynchronization attacks in RFID systems. *Wireless Personal Communications*, pages 1–17, July 2012.
363. Lijun Gao, Maode Ma, Yantai Shu, and Yuhua Wei. An ultralightweight RFID authentication protocol with CRC and permutation. *Journal of Network and Computer Applications*, 36(6), November 2013.
364. Xingxin (Grace) Gao, Zhe (Alex) Xiang, Hao Wang, Jun Shen, Jian Huang, and Song Song. An Approach to Security and Privacy of RFID System for Supply Chain. In *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*, pages 164–168, Beijing, China, September 2005. IEEE, IEEE Computer Society.
365. Esteban Masobro Garcia. Security protocols for low cost RFID tags: Analysis and automated verification of proposed solutions. Technical report, Royal Holloway University of London, Egham, United Kingdom, March 2015.
366. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijrers, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling MIFARE Classic. In Sushil Jajodia and Javier Lpez, editors, *13th European Symposium on Research in Computer Security – ESORICS 2008*, volume 5283 of *Lecture Notes in Computer Science*, pages 97–114, Malaga, Spain, October 2008. Springer.
367. Flavio D. Garcia, Gerhard de Koning Gans, and Roel Verdult. Exposing iClass key diversification. In *20th USENIX Security Symposium – USENIX'11*, San Francisco, CA, August 2011. USENIX.
368. Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult, and Milosch Meriac. Dismantling iClass and iClass elite. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *17th European Symposium on Research in Computer Security – ESORICS 2012*, volume 7459, pages 697–715, Pisa, Italy, September 2012. Springer Berlin / Heidelberg.
369. Flavio D. Garcia and Peter van Rossum. Modeling Privacy for Off-line RFID Systems. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
370. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly Pickpocketing a Mifare Classic Card. In *IEEE Symposium on Security and Privacy – S&P '09*, Oakland, California, USA, May 2009. IEEE, IEEE Computer Society.
371. Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling SecureMemory, CryptoMemory and CryptoRF. Cryptology ePrint Archive, Report 2010/169, 2010.
372. Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis. Evaluation of Anonymized ONS Queries. In Cuppens et al., editor, *First International Workshop on Security of Autonomous and Spontaneous Networks – SETOP'08*, pages 47–60, Loctudy, France, October 2008.
373. Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis. Security Threat Mitigation Trends in Low-cost RFID Systems. In Joaqun Garca-Alfaro, Guillermo Navarro-Arribas, Nora Cuppens-Boulahia, and Yves Roudier, editors, *Second International Workshop on Autonomous and Spontaneous Security – SETOP'09*, volume 5939 of *Lecture Notes in Computer Science*, pages 193–207, Saint-Malo, France, September 2009. Springer.
374. Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis. Proactive Threshold Cryptosystem for EPC Tags. *Ad Hoc & Sensor Wireless Networks*, 12(3-4):187–208, 2011.
375. Simson Garfinkel, Ari Juels, and Ravi Pappu. RFID Privacy: An Overview of Problems and Proposed Solutions. *IEEE Security and Privacy*, 3(3):34–43, May–June 2005.
376. Seyed Salman Sajjadi GhaemMaghami, Afrooz Haghbin, and Mahtab Mirmohseni. Traceability improvements of a new RFID protocol based on EPC C1G2. Cryptology ePrint Archive, Report 2015/872, 2015.
377. Henri Gilbert, Matthew Robshaw, and Yannick Seurin. Good Variants of HB+ are Hard to Find. In Gene Tsudik, editor, *Financial Cryptography and Data Security – FC'08*, volume 5143 of *Lecture Notes in Computer Science*, pages 156–170, Cozumel, Mexico, January 2008. IFCA, Springer.
378. 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.
379. Henri Gilbert, Matthew Robshaw, and Hervé Sibert. An Active Attack Against HB^+ – A provably Secure Lightweight Authentication Protocol. Manuscript, July 2005.
380. Marc Girault, Loic Juniot, and Matthew Robshaw. The Feasibility of On-the-Tag Public Key Cryptography. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
381. Dara J. Glasser, Kenneth W. Goodman, and Norman G. Einspruch. Chips, Tags and Scanners: Ethical Challenges for Radio Frequency Identification. *Ethics and Information Technology*, 9(2):101–109, July 2007.
382. Jovan Dj. Goli. Cryptanalytic attacks on mifare classic protocol. In Ed Dawson, editor, *Topics in Cryptology – CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 239–258, San Francisco, USA, February 2013. Springer Berlin Heidelberg.

383. JovanDj. Goli. Cryptanalytic attacks on mifare classic protocol. In Ed Dawson, editor, *Topics in Cryptology CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 239–258, San Francisco, USA, February 2013. Springer Berlin Heidelberg.
384. Philippe Golle, Markus Jakobsson, Ari Juels, and Paul Syverson. Universal re-encryption for mixnets. In Tatsuaki Okamoto, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA 2004*, volume 2964 of *Lecture Notes in Computer Science*, pages 163–178, San Francisco, California, USA, February 2004. Springer.
385. Zheng Gong, Svetla Nikova, and Yee Wei Law. KLEIN: A New Family of Lightweight Block Ciphers. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
386. Nathan Good, John Han, Elizabeth Miles, David Molnar, Deirdre Mulligan, Laura Quilter, Jennifer Urban, and David Wagner. Radio Frequency Identification and Privacy with Information Goods. In Sabrina De Capitani di Vimercati and Paul Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES'04*, pages 41–42, Washington, DC, USA, October 2004. ACM, ACM Press.
387. Prosanta Gope and Tzonelih Hwang. A realistic lightweight authentication protocol preserving strong anonymity for securing RFID system. *Computers & Security*, May 2015.
388. Zbigniew Gobiewski, Krzysztof Majcher, Filip Zagrski, and Marcin Zawada. Practical Attacks on HB and HB+ Protocols. In Claudio Ardagna and Jianying Zhou, editors, *Workshop on Information Security Theory and Practice – WISTP'11*, volume 6633 of *Lecture Notes in Computer Science*, pages 244–253, Heraklion, Crete, Greece, June 2011. Springer.
389. Hannes Gross, Michael Hutter, Erich Wenger, and Honorio Martin Gonzalez. PIONEER – a prototype for the internet of things based on an extendable EPC gen2 RFID tag. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
390. Hannes Gro and Thomas Plos. On using instruction-set extensions for minimizing the hardware-implementation costs of symmetric-key algorithms on a low-resource microcontroller. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
391. Fuchun Guo, Yi Mu, Willy Susilo, and Vijay Varadharajan. A pre-computable signature scheme with efficient verification for RFID. In Mark Ryan, Ben Smyth, and Guilin Wang, editors, *Information Security Practice and Experience*, volume 7232 of *Lecture Notes in Computer Science*, pages 1–16. Springer Berlin / Heidelberg, 2012.
392. Ali Özhan Gürel, Atakan Arslan, and Mete Akgün. Non-Uniform Stepping Approach to RFID Distance Bounding Problem. In Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Ana Cavalli, and Jean Leneutre, editors, *Fifth International Workshop on Data Privacy Management – DPM'10*, volume 6514 of *Lecture Notes in Computer Science*, pages 64–78, Athens, Greece, September 2010. Springer.
393. Jitendra Gurubani, Harsh Thakkar, and Dhiren Patel. Improvements over extended LMAP+: RFID authentication protocol. In Theo Dimitrakos, Rajat Moona, Dhiren Patel, and D. McKnight, editors, *6th International Conference on Trust Management – IFIPTM 2012*, volume 374 of *IFIP Advances in Information and Communication Technology*, pages 225–231, Surat, India, May 2012. Springer Boston.
394. JungHoon Ha, SangJae Moon, Jianying Zhou, and JaeCheol Ha. A New Formal Proof Model for RFID Location Privacy. In Sushil Jajodia and Javier Lpez, editors, *13th European Symposium on Research in Computer Security – ESORICS 2008*, volume 5283 of *Lecture Notes in Computer Science*, pages 267–281, Malaga, Spain, October 2008. Springer.
395. Mohammad Habibi, Mahdi Alagheband, and Mohammad Aref. Attacks on a Lightweight Mutual Authentication Protocol under EPC C-1 G-2 Standard. In Claudio Ardagna and Jianying Zhou, editors, *Workshop on Information Security Theory and Practice – WISTP'11*, volume 6633 of *Lecture Notes in Computer Science*, pages 254–263, Heraklion, Crete, Greece, June 2011. Springer.
396. Mohammad Habibi and Mohammad Aref. Security and privacy analysis of SongMitchell RFID authentication protocol. *Wireless Personal Communications*, pages 1–14, May 2012.
397. Mohammad Habibi, Mohammad Aref, and Di Ma. Addressing flaws in RFID authentication protocols. In Daniel Bernstein and Sanjit Chatterjee, editors, *Proceedings of the 12th International Conference on Cryptology in India – Indocrypt 2011*, volume 7107, pages 216–235, Chennai, India, December 2011. Springer Berlin / Heidelberg.
398. Mohammad Hassan Habibi and Mohammad Reza Aref. Two RFID privacy models in front of a court. Cryptology ePrint Archive, Report 2011/625, 2011.
399. Mohammad Hassan Habibi and Mohammad Reza Aref. Attacks on recent RFID authentication protocols. *Journal of Signal Processing Systems*, September 2013.
400. Mohammad Hassan Habibi, Mahmoud Gardeshi, and Mahdi R. Alaghband. Cryptanalysis of two mutual authentication protocols for low-cost RFID. *International Journal of Distributed and Parallel systems*, 2(1):103–114, 2011.

401. Mohammad Hassan Habibi and Mahmud Gardeshi. Cryptanalysis and improvement on a new RFID mutual authentication protocol compatible with EPC standard. In *International Conference on Information Security and Cryptology – ICISC 2011*, pages 49–54, Mashhad, Iran, September 2011. Springer.
402. Mohammad Hassan Habibi, Mahmud Gardeshi, and Mahdi R. Alagheband. Attacks and Improvements to a New RFID Authentication Protocol. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 66–80, Wuxi, China, April 2011. IOS Press.
403. Mohammed J. Hakeem, Kaamran Raahemifar, and Gul N. Khan. A novel key management protocol for RFID systems. In *9th International Wireless Communications and Mobile Computing Conference – IWCMC 2013*, pages 1107–1113, Sardinia, July 2013. IEEE.
404. John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. The Security Implications of VeriChip^{TM}Cloning. Manuscript in submission, March 2006.
405. Tzipora Halevi, Haoyu Li, Di Ma, Nitesh Saxena, Jonathan Voris, and Tuo Xiang. Context-aware defenses to RFID unauthorized reading and relay attacks. *IEEE Transactions on Emerging Topics in Computing*, 1(2):307–318, December 2013.
406. Tzipora Halevi, Nitesh Saxena, and Shai Halevi. Using HB Family of Protocols for Privacy-Preserving Authentication of RFID Tags in a Population. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
407. Tzipora Halevi, Nitesh Saxena, and Shai Halevi. Tree-based HB Protocols for Privacy-Preserving Authentication of RFID Tags. *Journal of Computer Security - Special Issue on RFID System Security*, 2010.
408. Tzipora Halevi, Nitesh Saxena, and Shai Halevi. Tree-based HB protocols for privacy-preserving authentication of RFID tags. *Journal of Computer Security – Special Issue on RFID System Security*, 19(2):343–363, April 2011.
409. Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses. In *IEEE Symposium on Security and Privacy – S&P '08*, Oakland, California, USA, May 2008. IEEE, IEEE Computer Society.
410. Martin Halváč and Tomáč Rosa. A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports. Cryptology ePrint Archive, Report 2007/244, 2007.
411. Sana Tmar-Ben Hamida, Pierre-Henri Thevenon, Jean-Benoit Pierrot, Olivier Savry, and Claude Castelluccia. Detecting relay attacks in RFID systems using physical layer characteristics. In *Wireless and Mobile Networking Conference (WMNC), 2013 6th Joint IFIP – WMNC 2013*, pages 1–8, Dubai, United Arab Emirates, April 2013.
412. Kyusuk Han and Taeshik Shon. Sensor authentication in dynamic wireless sensor network environments. *International Journal of RFID Security and Cryptography*, 1:36–44, March 2012.
413. Yoshikazu Hanatani, Miyako Ohkubo, Shin'ichiro Matsuo, Kazuo Sakiyama, and Kazuo Ohta. A study on computational formal verification for practical cryptographic protocol: The case of synchronous RFID authentication. In George Danezis, Sven Dietrich, and Kazue Sako, editors, *16th International Conference on Financial Cryptography and Data Security – FC'12*, volume 7126 of *Lecture Notes in Computer Science*, pages 70–87, Bonaire, March 2012.
414. Gerhard P. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.
415. Gerhard P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy – S&P '06*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society.
416. Gerhard P. Hancke. Noisy Carrier Modulation for HF RFID. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
417. Gerhard P. Hancke. Eavesdropping Attacks on High-Frequency RFID Tokens. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
418. Gerhard P. Hancke. *Security of Proximity Identification Systems*. PhD thesis, University of Cambridge, Cambridge, United Kingdom, February 2008.
419. Gerhard P. Hancke. Design of a Secure Distance-Bounding Channel for RFID. *Journal of Network and Computer Applications*, May 2010.
420. Gerhard P. Hancke. Practical Eavesdropping and Skimming Attacks on High-Frequency RFID Tokens. *Journal of Computer Security – Special Issue on RFID System Security*, 2010.
421. Gerhard P. Hancke. Distance-bounding for RFID: Effectiveness of terrorist fraud in the presence of bit errors. In *2012 IEEE International Conference on RFID Technologies and Applications – RFID-TA 2012*, pages 91–96, Nice, France, November 2012. IEEE.

422. Gerhard P. Hancke and Markus Kuhn. An RFID Distance Bounding Protocol. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 67–73, Athens, Greece, September 2005. IEEE, IEEE Computer Society.
423. Gerhard P. Hancke and Markus Kuhn. Attacks on Time-of-Flight Distance Bounding Channels. In Virgil D. Gligor, Jean-Pierre Hubaux, and Radha Poovendran, editors, *Proceedings of the 1st ACM Conference on Wireless Network Security – WiSec'08*, pages 194–202, Alexandria, Virginia, USA, March–April 2008. ACM, ACM Press.
424. Gerhard P. Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in smart token proximity: Relay attacks revisited. In *Elsevier Computers & Security*, volume 28, pages 615–627, June 2009.
425. Ernst Haselsteiner and Klemens Breitfuss. Security in Near Field Communication (NFC). In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
426. Debiao He, Neeraj Kumar, Naveen Chilamkurti, and Jong-Hyouk Lee. Lightweight ECC based RFID authentication integrated with an ID verifier transfer protocol. *Journal of Medical Systems*, August 2014.
427. Debiao He and Sherali Zeadally. An analysis of RFID authentication schemes for internet of things in healthcare environment using elliptic curve cryptography. *IEEE Internet of Things Journal*, September 2014.
428. Daniel Hein, Johannes Wolkerstorfer, and Norbert Felber. ECC is Ready for RFID A Proof in Silicon. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
429. Jan Hennig, Peter Ladkin, and Bernd Sieker. Privacy Enhancing Technology Concepts for RFID Technology Scrutinised. Research Report RVS-RR-04-02, University of Bielefeld, Bielefeld, Germany, October 2004.
430. Dirk Henrici and Paul Müller. Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. In Ravi Sandhu and Roshan Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.
431. Dirk Henrici and Paul Müller. Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In Alois Ferscha and Friedemann Mattern, editors, *2nd International Conference on Pervasive Computing – Pervasive 2004*, volume 3001 of *Lecture Notes in Computer Science*, pages 219–224, Vienna, Austria, April 2004. Springer.
432. Jans Hermans. *Lightweight Public Key Cryptography.* PhD thesis, Katholieke Universiteit Leuven, Leuven, Belgium, August 2012.
433. Jens Hermans, Andreas Pashalidis, Frederik Vercauteren, and Bart Preneel. A new RFID privacy model. In *16th European Symposium on Research in Computer Security – ESORICS 2011*, Lecture Notes in Computer Science, Leuven, Belgium, September 2011. Springer.
434. Jens Hermans and Roel Peeters. Private yoking proofs: attacks, models and new provable constructions. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
435. Jens Hermans, Roel Peeters, and Cristina Onete. Efficient, secure, private distance bounding without key updates. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks – WiSec'13*, WiSec '13, pages 207–218, Budapest, Hungary, April 2013. ACM.
436. Jens Hermans, Roel Peeters, and Bart Preneel. Proper RFID privacy: Model and protocols. *IEEE Transactions on Mobile Computing*, March 2014.
437. Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, Pedro Peris-Lopez, and Jean-Jacques Quisquater. Cryptanalysis of the SASI Ultralightweight RFID Authentication Protocol with Modular Rotations. In *International Workshop on Coding and Cryptography – WCC'09*, Ullensvang, Norway, May 2009.
438. 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.
439. Julio C. Hernandez-Castro, Pedro Peris-Lopez, Juan M. E. Tapiador, Raphael C.-W. Phan, and Tieyan Li. Passive Black-Box Cryptanalysis of an Ultralightweight Protocol after Eavesdropping One Authentication Session. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 3–17, Wuxi, China, April 2011. IOS Press.
440. Julio C. Hernandez-Castro, Juan E. Tapiador, Pedro Peris-Lopez, John A. Clark, and El-Ghazali Talbi. Metaheuristic Traceability Attack against SLMAP, an RFID Lightweight Authentication Protocol. In *Proceedings of the 23rd IEEE International Parallel and Distributed Processing Symposium – IPDPS 2009*, Rome, Italy, May 2009. IEEE, IEEE Computer Society.
441. Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, and Jean-Philippe Aumasson. On the key schedule strength of PRESENT. In Joaquin Garcia-Alfaro, Guillermo Navarro-Arribas, Nora Cuppens-Boulahia, and Sabrina

Capitani di Vimercati, editors, *Data Privacy Management and Autonomous Spontaneus Security – SETOP 2012*, volume 7122 of *Lecture Notes in Computer Science*, pages 253–263, Pisa, Italy, September 2012. Springer Berlin Heidelberg.

442. Julio Cesar Hernandez-Castro, Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. Another fallen hash-based RFID authentication protocol. In Joachim Posegga Ioannis G. Askoxylakis, Henrich Christopher Pöhls, editor, *Workshop on Information Security Theory and Practice – WISTP'12*, volume 7322 of *LNCS*, pages 29–37, Egham, United Kingdom, June 2012. Springer.
443. Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security – FC'07*, volume 4886 of *Lecture Notes in Computer Science*, pages 2–14, Scarborough, Trinidad and Tobago, February 2007. IFCA, Springer.
444. Thomas S. Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. Privacy for Public Transportation. In George Danezis and Philippe Golle, editors, *Workshop on Privacy Enhancing Technologies – PET 2006*, volume 4258 of *Lecture Notes in Computer Science*, pages 1–19, Cambridge, United Kingdom, June 2006. Springer.
445. Gesine Hinterwalder, Christof Paar, and Wayne P. Burleson. Privacy preserving payments on ultra-low power devices with application in intelligent transportation systems. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
446. Thomas Hjorth. Supporting Privacy in RFID Systems. Master thesis, Technical University of Denmark, Lyngby, Denmark, December 2004.
447. Jaap-Henk Hoepman, Engelbert Hubbers, Bart Jacobs, Martijn Oostdijk, and Ronny Wichers Schreur. Crossing Borders: Security and Privacy Issues of the European e-Passport. In Hiroshi Yoshiura, Kouichi Sakurai, Kai Rannenberg, Yuko Murayama, and Shin-ichi Kawamura, editors, *Advances in Information and Computer Security, First International Workshop on Security – IWSEC'06*, volume 4266 of *Lecture Notes in Computer Science*, pages 152–167, Kyoto, Japan, October 2006. Springer.
448. Jaap-Henk Hoepman and Rieks Joosten. Practical Schemes for Privacy and Security Enhanced RFID. In Pierangela Samarati, Michael Tunstall, Joachim Posegga, Konstantinos Markantonakis, and Damien Sauveron, editors, *Workshop on Information Security Theory and Practice – WISTP'10*, volume 6033 of *Lecture Notes in Computer Science*, pages 138–153, Passau, Germany, April 2010. Springer.
449. Georg Hofferek and Johannes Wolkerstorfer. Coupon Recalculation for the GPS Authentication Scheme. In Gilles Grimaud and Franois-Xavier Standaert, editors, *Proceedings of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, volume 5189 of *Lecture Notes in Computer Science*, pages 162–175, Royal Holloway University of London, United Kingdom, September 2008. Springer.
450. Daniel Holcom, Wayne Burleson, and Kevin Fu. Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID Tags. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
451. Daniel Holcomb, Amir Rahmati, Mastooreh Salajegheh, Wayne Burleson, and Kevin Fu. DRV-Fingerprinting: Using data retention voltage of SRAM cells for chip identification. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
452. Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jaesang 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, November 2006. Springer.
453. Hilal Houssain and Turki F. Al-Somani. Elliptic curve cryptoprocessor implementation on a nano FPGA: Interesting for resource-constrained devices. *International Journal of RFID Security and Cryptography*, 1:45–50, March 2012.
454. Hilal Houssain, Mohamad Badra, and Turki F. Al-Somani. Comparative study of elliptic curve cryptography hardware implementations in wireless sensor networks. *International Journal of RFID Security and Cryptography*, 1:67–73, March 2012.
455. Cheng-Ter Hsi, Yuan-Hung Lien, Jung-Hui Chiu, and Henry Ker-Chang Chang. Solving scalability problems on secure RFID grouping-proof protocol. *Wireless Personal Communications*, May 2015.
456. Meng-Lin Hsia and O.T.-C. Chen. Low-complexity encryption using redundant bits and adaptive frequency rates in RFID. In *IEEE International Symposium on Circuits and Systems – ISCAS 2007*, pages 1601–1604, New Orleans, US, May 2007. IEEE.
457. Hui-Feng Huang, Po-Kai Yu, and Kuo-Ching Liu. A privacy and authentication protocol for mobile RFID system. In *International Symposium on Independent Computing – ISIC 2014*, pages 1–6, December 2014.

458. Yu-Chung Huang and Jehn-Ruey Jiang. Efficient ultralightweight RFID mutual authentication. In *IEEE International Conference on Internet of Things – iThings 2014*, Taipei, Taiwan, July 2014.
459. Yu-Chung Huang and Jehn-Ruey Jiang. Ultralightweight RFID reader-tag mutual authentication revisited. In *International Conference on Mobile Services, Special Track on Security and Privacy for Mobile Services – MS-SPMS 2015*, New York, USA, July 2015.
460. Yu-Jung Huang, Chi-Huan Jiang, Hsuan-Hsun Wu, Yi-Hao Hong, and Kai-Jen Liu. Mutual authentication protocol for RFID system. In *14th International Conference on Computational Science and Engineering – IEEE CSE 2011*, pages 73–80, Dalian, Liaoning, Augustus 2011. IEEE, IEEE Computer Society.
461. Michael Hutter, Martin Feldhofer, and Thomas Plos. An ECDSA Processor for RFID Authentication. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 189–202, Istanbul, Turkey, June 2010. Springer.
462. Michael Hutter, Stefan Mangard, and Martin Feldhofer. Power and EM Attacks on Passive 13.56 MHz RFID Devices. In Pascal Paillier and Ingrid Verbauwhede, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 320–333, Vienna, Austria, September 2007. Springer.
463. Michael Hutter, Marcel Medwed, Daniel Hein, and Johannes Wolkerstorfer. Attacking ECDSA-Enabled RFID Devices. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *Proceedings of the 7th International Conference on Applied Cryptography and Network Security – ACNS 2009*, volume 5536 of *Lecture Notes in Computer Science*, pages 519–534, Paris-Rocquencourt, France, June 2009. Springer.
464. Michael Hutter, Jörn-Marc Schmidt, and Thomas Plos. RFID and Its Vulnerability to Faults. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Proceedings of the 10th International Workshop Cryptographic Hardware and Embedded Systems – CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, pages 368–379, Washington, DC, USA, August 2008. Springer.
465. Sozo Inoue and Hiroto Yasuura. RFID Privacy Using User-controllable Uniqueness. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
466. Nazish Irfan, Mustapha Yagoub, and Khelifa Hettak. Redundant reader elimination approaches for RFID networks. In Mohamed Kamel, Fakhri Karray, Wail Gueaieb, and Alaa Khamis, editors, *Autonomous and Intelligent Systems*, volume 6752 of *Lecture Notes in Computer Science*, pages 396–405. Springer Berlin / Heidelberg, June 2011.
467. Nazish Irfan, Mustapha C. E. Yagoub, and Khelifa Hettak. Efficient approach for redundant reader elimination for directional antenna in RFID networks. *International Journal of RFID Security and Cryptography*, 1:74–81, March 2012.
468. Toshiharu Ishikawa, Yukiko Yumoto, Michio Kurata, Makoto Endo, Shingo Kinoshita, Fumitaka Hoshino, Satoshi Yagi, and Masatoshim Nomachi. Applying Auto-ID to the Japanese Publication Business. White Paper KEI-AUTOID-WH-004, Auto-ID Center, Keio University, Shonan-Fujisawa, Kanagawa, Japan, October 2003.
469. Salekul Islam. Security analysis of LMAP using AVISPA. *International Journal of Security and Networks*, 9(1):30–39, February 2014.
470. Pasin Israsena. Securing Ubiquitous and Low-Cost RFID Using Tiny Encryption Algorithm. In *International Symposium on Wireless Pervasive Computing*, Phuket, Thailand, January 2006. IEEE, IEEE Computer Society.
471. Wolfgang Issovits and Michael Hutter. Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks. In *2011 IEEE International Conference on RFID Technologies and Applications – RFID-TA 2011*, pages 335–342, September 2011.
472. Hoda Jannati. Analysis of relay, terrorist fraud and distance fraud attacks on RFID systems. *International Journal of Critical Infrastructure Protection*, August 2015.
473. Hoda Jannati and Abolfaz Falahati. Achieving an appropriate security level for distance bounding protocols over a noisy channel. *Telecommunication Systems*, October 2014.
474. Hoda Jannati and Abolfazl Falahati. Mutual implementation of predefined and random challenges over RFID distance bounding protocol. In *International Conference on Information Security and Cryptology – ICISC 2012*, pages 43–47, Tabriz, Iran, September 2012. IEEE.
475. Hoda Jannati and Abolfazl Falahati. Mutual distance bounding protocol with its implementability over a noisy channel and its utilization for key agreement in peer-to-peer wireless networks. *Wireless Personal Communications*, November 2013.
476. Hoda Jannati and Abolfazl Falahati. Analysis of false-reject probability in distance bounding protocols with mixed challenges over RFID noisy communication channel. *Information Processing Letters*, February 2015.
477. Hoda Jannati and Abolfazl Falahati. An RFID search protocol secured against relay attack based on distance bounding approach. *Wireless Personal Communications*, June 2015.

478. Pekka Jäppinen and Mikko Lampi. Hardware cost measurement of lightweight security protocols. *Wireless Personal Communications*, 71(2):1479–1486, July 2013.
479. Chitra Javali, Girish Revadigar, Lavy Libman, and Sanjay Jha. SeAK: Secure authentication and key generation protocol based on dual antennas for wireless body area networks. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
480. Z. Jeddi, E. Amini, and M. Bayoumi. RBS: Redundant bit security algorithm for RFID systems. In *21st International Conference on Computer Communications and Networks – ICCCN 2012*, pages 1–5, Munich, Germany, August 2012.
481. Il-Soo Jeon and Eun-Jun Yoon. Cryptanalysis and improvement of a new ultra-lightweight RFID authentication protocol with permutation. *Applied Mathematical Sciences*, 7(69):3433–3444, September 2013.
482. Il-Soo Jeon and Eun-Jun Yoon. A new ultra-lightweight RFID authentication protocol using merge and separation operations. *International Journal of Mathematical Analysis*, 7(52):2583–2593, October 2013.
483. Il-Soo Jeon and Eun-Jun Yoon. An ultralightweight RFID distance bounding protocol. *International Journal of Mathematical Analysis*, 8(46):2265–2275, November 2014.
484. Yang Jeongkyu. Security and Privacy on Authentication Protocol for Low-cost Radio Frequency Identification. Master thesis, Information and Communications University, Daejeon, Korea, December 2004.
485. Qing Xuan Jia, Xin Wang, Xin Gao, Pan Pan Gao, and Bing Zhao. An effective ultralightweight rfid secure protocol with mutual authentication. *Applied Mechanics and Materials*, 278 - 280:1966–1971, January 2013.
486. Ari Juels. Minimalist Cryptography for Low-Cost RFID Tags. In Carlo Blundo and Stelvio Cimato, editors, *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164, Amalfi, Italy, September 2004. Springer.
487. Ari Juels. "Yoking-Proofs" for RFID Tags. In Ravi Sandhu and Roshan Thomas, editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 138–143, Orlando, Florida, USA, March 2004. IEEE, IEEE Computer Society.
488. Ari Juels. *Privacy and Technologies of Identity, A Cross-Disciplinary Conversation (Eds K. Strandburg and D. Stan Raicu)*, chapter RFID Privacy: A Technical Primer for the Non-Technical Reader. Springer, 2005.
489. Ari Juels. Strengthening EPC Tags Against Cloning. Manuscript, March 2005.
490. Ari Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.
491. Ari Juels and John Brainard. Soft Blocking: Flexible Blocker Tags on the Cheap. In Sabrina De Capitani di Vimercati and Paul Syverson, editors, *Workshop on Privacy in the Electronic Society – WPES'04*, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.
492. Ari Juels, David Molnar, and David Wagner. Security and Privacy Issues in E-passports. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 74–88, Athens, Greece, September 2005. IEEE, IEEE Computer Society.
493. Ari Juels and Ravikanth Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Rebecca N. Wright, editor, *Financial Cryptography – FC'03*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121, Le Gosier, Guadeloupe, French West Indies, January 2003. IFCA, Springer.
494. Ari Juels, Ravikanth Pappu, and Bryan Parno. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. In Paul C. van Oorschot, editor, *17th USENIX Security Symposium – USENIX'08*, pages 75–90, San Jose, California, USA, July 2008. USENIX.
495. Ari Juels, Ronald Rivest, and Michael Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Sushil Jajodia, Vijayalakshmi Atluri, and Trent Jaeger, editors, *Conference on Computer and Communications Security – ACM CCS'03*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.
496. Ari Juels, Paul Syverson, and Dan Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. In George Danezis and David Martin, editors, *Workshop on Privacy Enhancing Technologies – PET 2005*, volume 3856 of *Lecture Notes in Computer Science*, pages 210–226, Cavtat, Croatia, May–June 2005. Springer.
497. Ari Juels and Stephen Weis. Authenticating Pervasive Devices with Human Protocols. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO'05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, California, USA, August 2005. IACR, Springer.
498. Ari Juels and Stephen Weis. Defining Strong Privacy for RFID. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 342–347, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
499. Khoureich Ahmad Ka. hHB: a harder HB+s protocol. Cryptology ePrint Archive, Report 2014/562, 2014.
500. Ulrich Kaiser. UICE: A High-Performance Cryptographic Module for SoC and RFID Applications. Cryptology ePrint Archive, Report 2007/258, 2007.

501. Jeonil Kang and Daehun Nyang. RFID Authentication Protocol with Strong Resistance against Traceability and Denial of Service Attacks. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 164–175, Visegrad, Hungary, July 2005. Springer.
502. You Sung Kang, Dong-Jo Park, Daniel W. Engels, and Dooho Choi. KeyQ: A dynamic key establishment method using an RFID anti-collision protocol. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E97-A(12):2662–2666, December 2014.
503. Gaurav Kapoor and Selwyn Piramuthu. Vulnerabilities in some recently proposed RFID ownership transfer protocols. *IEEE Communications Letters*, 14(3):260–262, March 2010.
504. Gaurav Kapoor and Selwyn Piramuthu. Single RFID Tag Ownership Transfer Protocols. *IEEE Transactions on Systems, Man, and Cybernetics*, pages 1–10, 2011.
505. Gaurav Kapoor, Wei Zhou, and Selwyn Piramuthu. Distance Bounding Protocol for Multiple RFID Tag Authentication. In Cheng-Zhong Xu and Minyi Guo, editors, *Embedded and Ubiquitous Computing - Volume 02 – EUC'08*, pages 115–120, Shanghai, China, December 2008. IEEE, IEEE Computer Society.
506. Gaurav Kapoor, Wei Zhou, and Selwyn Piramuthu. Multi-tag and multi-owner rfid ownership transfer in supply chains. *Decision Support Systems*, 2011.
507. Jens-Peter Kaps, Gunnar Gaubatz, and Berk Sunar. Cryptography on a Speck of Dust. *IEEE Computer*, 40(2):38–44, February 2007.
508. Orhun Kara, Süleyman Kardaş, Muhammed Ali Bingöl, and Gildas Avoine. Optimal Security Limits of RFID Distance Bounding Protocols. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 220–238, Istanbul, Turkey, June 2010. Springer.
509. Ferhat Karakoc, Huseyin Demirci, and A. Emre Harmanci. Biclique cryptanalysis of LBlock and TWINE. *Information Processing Letters*, 113(12):423–429, June 2013.
510. Süleyman Kardaş, Serkan Çelik, Muhammed Ali Bingöl, Mehmet Sabir Kiraz, Hüseyin Demirci, and Albert Levi. k-strong privacy for radio frequency identification authentication protocols based on physically unclonable functions. *Wireless Communications and Mobile Computing*, pages 1–17, June 2014.
511. Süleyman Kardaş, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci. A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions. Cryptology ePrint Archive, Report 2011/075, 2011.
512. Süleyman Kardaş, Mehmet Sabir Kiraz, Muhammed Ali Bingöl, and Hüseyin Demirci. A Novel RFID Distance Bounding Protocol Based on Physically Unclonable Functions. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
513. Süleyman Kardaş, Albert Levi, and Ertugrul Murat. Providing Resistance against Server Information Leakage in RFID Systems. In *New Technologies, Mobility and Security – NTMS'11*, pages 1–7, Paris, France, February 2011. IEEE, IEEE Computer Society.
514. Suleyman Kardas, Atakan Arslan, Serkan Celik, and Albert Levi. An efficient and private RFID authentication protocol supporting ownership transfer. Cryptology ePrint Archive, Report 2011/667, 2011.
515. Suleyman Kardas, Atakan Arslan, Serkan Celik, and Albert Levi. An efficient and private RFID authentication protocol supporting ownership transfer. In *Second International Workshop on Lightweight Cryptography for Security and Privacy – LightSec 2013*, Gebze, Turkey, May 2013.
516. Suleyman Kardas, Serkan Celik, Muhammed Ali Bingol, and Albert Levi. A new security and privacy framework for RFID in cloud computing. Cryptology ePrint Archive, Report 2013/165, 2013.
517. Sleyman Kardaa, Serkan elika, Muhammet Yldza, and Albert Levi. PUF-enhanced offline RFID security and privacy. *Journal of Network and Computer Applications*, September 2012.
518. Günter Karjoth and Paul Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. Research Report RC 23710, IBM Research Division, Zurich, Switzerland, August 2005.
519. Günter Karjoth and Paul Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *Workshop on Privacy in the Electronic Society – WPES'05*, pages 27–30, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
520. Sindhu Karthikeyan and Mikhail Nesterenko. RFID Security without Extensive Cryptography. In *Workshop on Security of Ad Hoc and Sensor Networks – SASN'05*, pages 63–67, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
521. Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips. Guidelines for Securing Radio Frequency Identification (RFID) Systems, April 2007.
522. Hamid Kashfi. Evaluation of practical attacks against RFID technology. Master thesis, Linnaeus University, Sweden, October 2014.

523. Timo Kasper. Embedded Security Analysis of RFID Devices. Master Thesis, July 2006.
524. Timo Kasper, Alexander Kühn, David Oswald, Christian Zenger, and Christof Paar. Rights management with nfc smartphones and electronic id cards: A proof of concept for modern car sharing. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
525. Timo Kasper, David Oswald, and Christof Paar. New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
526. Timo Kasper, David Oswald, and Christof Paar. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
527. Jonathan Katz, Ji Sun Shin, and Adam Smith. Parallel and Concurrent Security of the HB and HB+ Protocols. *Journal of Cryptology*, 23(3):402–421, July 2010.
528. Jonathan Katz and Adam Smith. Analyzing the HB and HB+ Protocols in the "Large Error" Case. Cryptology ePrint Archive, Report 2006/326, 2006.
529. Jonathan Katz and Ji Sun Shin. Parallel and Concurrent Security of the HB and HB^+ Protocols. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT'06*, volume 4004 of *Lecture Notes in Computer Science*, pages 73–87, Saint Petersburg, Russia, May–June 2006. IACR, Springer.
530. Sonam Devgan Kaul and Amit K. Awasthi. RFID authentication protocol to enhance patient medication safety. *Journal of Medical Systems*, 37(6), December 2013.
531. Firdous Kausar, Zeeshan Bilal, Senol Zafer Erdogan, and Jongsung Kim. AGVUS Ultra-Lightweight Mutual Authentication Protocol for Low-cost RFID Tags. In *International Symposium on Advances in Cryptography, Security and Application for Future Computing – ASCA'10*, Gwanglu, Korea, December 2010.
532. Elif Bilge Kavun and Tolga Yalcin. A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 258–269, Istanbul, Turkey, June 2010. Springer.
533. Gaurav S. Kc and Paul A. Karger. Security and Privacy Issues in Machine Readable Travel Documents. Technical Report RC 23575 (W0504-003), IBM Research Report, April 2005.
534. Florian Kerschbaum and Manfred Aigner. Securing RFID-supported Supply Chains. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
535. Florian Kerschbaum and Nina Oertel. Privacy-Preserving Pattern Matching for Anomaly Detection in RFID Anti-Counterfeiting. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 124–137, Istanbul, Turkey, June 2010. Springer.
536. Florian Kerschbaum and Alessandro Sorniotti. RFID-Based Supply Chain Partner Authentication and Key Agreement. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *Proceedings of the 2nd ACM Conference on Wireless Network Security – WiSec'09*, pages 41–50, Zurich, Switzerland, March 2009. ACM, ACM Press.
537. Ziv Kfir and Avishai Wool. Picking Virtual Pockets Using Relay Attacks on Contactless Smartcard Systems. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, pages 47–58, Athens, Greece, September 2005. IEEE, IEEE Computer Society.
538. Rushikesh Khasgiwale, Rohan Adyanthaya, and Daniel Engels. Extracting Information from Tag Collisions. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
539. Benjamin Khoo, Peter Harris, and Stephen Hartman. Security risk analysis of RFID technology: A RFID tag life cycle approach. In *Wireless Telecommunications Symposium – WTS 2009*, pages 1–7, Prague, April 2009.
540. Jing Huey Khor, Widad Ismail, and Mohammad Ghulam Rahman. Prevention and detection methods for enhancing security in an RFID system. *International Journal of Distributed Sensor Networks*, June 2012.
541. Ka Ahmad Khoureich. hHB: a harder HB+ protocol. Cryptology ePrint Archive, Report 2014/562, 2014.
542. Mehrdad Kianersi, Mahmoud Gardeshi, and Hamed Yousefi. Security analysis of ultra-lightweight protocol for low-cost RFID tags: SSL-MAP. In Abdulkadir zcan, Jan Zizka, and Dhinaharan Nagamalai, editors, *Recent Trends in Wireless and Mobile Networks*, volume 162 of *Communications in Computer and Information Science*, pages 236–245. Springer Berlin Heidelberg, June 2011.
543. Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *8th International Conference on Cryptology And Network Security – CANS'09*, volume 5888 of *Lecture Notes in Computer Science*, pages 119–133, Kanazawa, Ishikawa, Japan, December 2009. Springer.
544. Chong Hee Kim and Gildas Avoine. RFID distance bounding protocols with mixed challenges. *IEEE Transactions on Wireless Communications*, 10(5):1618–1626, May 2011.

545. Chong Hee Kim, Gildas Avoine, François Koeune, François-Xavier Standaert, and Olivier Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In P.J. Lee and J.H. Cheon, editors, *International Conference on Information Security and Cryptology – ICISC 2008*, volume 5461 of *Lecture Notes in Computer Science*, pages 98–115, Seoul, Korea, December 2008. Springer.
546. Il Jung Kim, Eun Young Choi, and Dong Hoon Lee. Secure mobile RFID system against privacy and security problems. *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2007*, pages 67–72, July 2007.
547. Inseop Kim, Byunggil Lee, and Howon Kim. Privacy Protection based on User-defined Preferences in RFID System. In *International Conference on Advanced Communication Technology – ICACT'06*, Phoenix Park, Korea, February 2006. IEEE, IEEE Computer Society.
548. Jin Seok Kim, Kookrae Cho, Dae Hyun Yum, Sung Je Hong, and Pil Joong Lee. Lightweight distance bounding protocol against relay attacks. *IEICE Transactions on Information and Systems*, E95.D(4):1155–1158, April 2012.
549. Soo-Cheol Kim, Sang-Soo Yeo, and Sung Kwon Kim. MARP: Mobile Agent for RFID Privacy Protection. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 300–312, Tarragona, Spain, April 2006. IFIP, Springer.
550. Young-Sik Kim and Sang-Hyo Kim. RFID distance bounding protocol using m-ary challenges. In *Proceedings of the International Conference on ICT Convergence – ICTC 2011*, pages 782–783, Seoul, Korea, September 2011.
551. Shingo Kinoshita, Miyako Ohkubo, Fumitaka Hoshino, Gembu Morohashi, Osamu Shionoiri, and Atsushi Kanai. Privacy Enhanced Active RFID Tag. In *International Workshop on Exploiting Context Histories in Smart Environments – ECHISE'05*, Munich, Germany, May 2005.
552. Ilan Kirschenbaum and Avishai Wool. How to Build a Low-Cost, Extended-Range RFID Skimmer. Cryptology ePrint Archive, Report 2006/054, 2006.
553. Marek Klonowski, Krzysztof Majcher, Wojciech Macyna, and Filip Zagorski. Hidden bits approach for authentication in RFID systems. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
554. Heiko Knospe and Hartmut Pohl. RFID Security. *Information Security Technical Report, Elsevier*, 9(4):39–50, November–December 2004.
555. Eren Kocaağa, Bünyamin Tanil, Muhammed Ali Bingöl, and Süleyman Kardaş. Solution of a conjecture: On 2-PCD RFID distance bounding protocols. In *6th International Information Security and Cryptology Conference – ISC Turkey 2013*, pages 153–157, Ankara, Turkey, September 2013.
556. Divyan Konidala, Zeen Kim, and Kwangjo Kim. A Simple and Cost-Effective RFID Tag-Reader Mutual Authentication Scheme. In *Workshop on RFID Security – RFIDSec'07*, pages 141–152, Malaga, Spain, July 2007.
557. Krishan H.S.S. Koralalage and Jingde Cheng. A Comparative Study of RFID Solutions for Security and Privacy: POP vs. Previous Solutions. In *International Conference on Information Security and Assurance – ISA 2008*, pages 342–349, Busan, Korea, April 2008. IEEE, IEEE Computer Society.
558. Krishan H.S.S. Koralalage, Mohammed Reza Selim, Junichi Miura, Yuichi Goto, and Jingde Cheng. POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism. In Yookun Cho, Roger L. Wainwright, Hisham Haddad, Sung Y. Shin, and Yong Wan Koo, editors, *Proceedings of the 2007 ACM Symposium on Applied Computing – SAC'07*, pages 270–275, Seoul, Korea, March 2007. ACM, ACM Press.
559. Karl Koscher, Ari Juels, Tadayoshi Kohno, and Vjekoslav Brajkovic. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript, 2008.
560. Eleni Kosta, Martin Meints, Marit Hensen, and Mark Gasson. An Analysis of Security and Privacy Issues Relating to RFID Enabled ePassports. In Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, and Rossouw Von Solms, editors, *IFIP TC-11 22nd International Information Security Conference – SEC 2007*, volume 232 of *IFIP*, pages 467–472, Sandton, Gauteng, South Africa, May 2007. IFIP, Springer.
561. Matthias Krause and Dirk Stegemann. More on the Security of Linear RFID Authentication Protocols. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography – SAC'09*, volume 5867 of *Lecture Notes in Computer Science*, pages 182–196, Calgary, Alberta, Canada, August 2009. Springer.
562. Lito Kriara, Matthew Alsup, Giorgio Corbellini, Matthew Trotter, Joshua Griffin, and Stefan Mangold. RFID shakables: Pairing radio-frequency identification tags with the help of gesture recognition. In *Proceedings of the ninth ACM conference on Emerging networking experiments and technologies*, pages 327–332. ACM, 2013.

563. Dennis Kuegler, Heike Neumann, Sebastian Stappert, Markus Ullmann, and Matthias Voegeler. Password Authenticated Key Agreement for Contactless Smart Cards. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
564. Abhishek Kumar, Somitra Kumar Sanadhya, Praveen Gauravaram, Nasour Bagheri, Javad Alizadeh, Mohammad Reza Aref, Hoda A. Alkhzaimi, and Martin M. Lauridsen. Cryptanalysis of SIMON variants with connections. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
565. Adarsh Kumar, Krishna Gopal, and Alok Aggarwal. Modeling and analysis of RFID authentication protocols for supply chain management. In *International Conference on Parallel, Distributed and Grid Computing – PDGC 2014*, pages 256–261, Solan, India, December 2014.
566. Adarsh Kumar, Krishna Gopal, and Alok Aggarwal. A novel trusted hierarchy construction for RFID-sensor based MANETs using ECC. *Electronics and Telecommunications Research Institute Journal*, 2014.
567. Rakesh Kumar. Interaction of RFID Technology and Public Policy. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
568. Rakesh Kumar and Riti Chatterjee. Shaping Ubiquity for the Developing World. In *International Telecommunications Union (ITU), Workshop on Ubiquitous Network Societies*, Geneva, Switzerland, April 2005.
569. Sandeep Kumar and Christof Paar. Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID? In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
570. Jin Kwak, Keunwoo Rhee, Soohyun Oh, Seungjoo Kim, and Dongho Won. RFID System with Fairness within the framework of Security and Privacy. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 142–152, Visegrad, Hungary, July 2005. Springer.
571. Daesung Kwon, Daewan Han, Jooyoung Lee, and Yongjin Yeom. Vulnerability of an RFID Authentication Protocol Proposed at SecUbiq 2005. In Xiaobo Zhou, Oleg Sokolsky, Lu Yan, Eun-Sun Jung, Zili Shao, Yi Mu, Dong Chun Lee, Daeyoung Kim, Young-Sik Jeong, and Cheng-Zhong Xu, editors, *International Workshop on Security in Ubiquitous Computing Systems – Secubiq 2006*, volume 4097 of *Lecture Notes in Computer Science*, pages 262–270, Seoul, Korea, August 2006. Springer.
572. Junzuo Lai, Robert H. Deng, and Yingjiu Li. Revisiting Unpredictability-Based RFID Privacy Models. In Jianying Zhou and Moti Yung, editors, *Proceedings of the 8th International Conference on Applied Cryptography and Network Security – ACNS 2010*, volume 6123 of *Lecture Notes in Computer Science*, pages 475–492, Beijing, China, June 2010. Springer.
573. Marc Langheinrich. A Survey of RFID Privacy Approaches. *Personal and Ubiquitous Computing*, 13(6):413–421, August 2009.
574. Marc Langheinrich and Remo Marti. Practical Minimalist Cryptography for RFID Privacy. *IEEE Systems Journal, Special Issue on RFID Technology*, 1(2):115–128, December 2007.
575. Manju Lata and Adarsh Kumar. Survey on lightweight primitives and protocols for RFID in wireless sensor networks. *International Journal of Communication Networks and Information Security – IJCNIS*, 6(1):29–43, April 2014.
576. Tri van Le, Mike Burmester, and Breno de Medeiros. Forward-Secure RFID Authentication and Key Exchange. Cryptology ePrint Archive, Report 2007/051, 2007.
577. Cheng-Chi Lee, Chi-Tung Chen, Chun-Ta Li, and Ping-Hsien Wu. A practical RFID authentication mechanism for digital television. *Telecommunication Systems*, August 2013.
578. Chin-Feng Lee, Yu-Chang Chen, Hung-Yu Chien, and Chi-Sung Laih. Anonymous RFID Yoking Protocol Using Error Correction Codes. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
579. Hwaseong Lee, Eun Young Choi, Su-Mi Lee, and Dong Hoon Lee. Trapdoor-Based Mutual Authentication Scheme without Cryptographic Primitives in RFID Tags. *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2007*, pages 73–78, July 2007.
580. Jooyoung Lee and Yongjin Yeom. Efficient RFID Authentication Protocols Based on Pseudorandom Sequence Generators. Cryptology ePrint Archive, Report 2008/343, 2008.
581. Kaleb Lee. A two-step mutual authentication protocol based on randomized hash-lock for small RFID networks. In *4th International Conference on Network ans System Security – NSS 2010*, pages 527–533, Melbourne, Australia, September 2010.
582. Kaleb Lee, Juan Gonzalez Nieto, and Colin Boyd. A state-aware RFID privacy model with reader corruption. In Yang Xiang, Javier Lopez, C.-C. Jay Kuo, and Wanlei Zhou, editors, *Proceedings of the 4th international conference on Cyberspace Safety and Security – CSS 2012*, volume 7672 of *Lecture Notes in Computer Science*, pages 324–338, Melbourne, Australia, December 2012. Springer-Verlag.

583. Sangho Lee, Jin Seok Kim, Sung Je Hong, and Jong Kim. Distance bounding with delayed responses. *IEEE Commuication Letters*, PP(99), 2012.
584. Sangshin Lee. Mutual Authentication of RFID System using Synchronized Secret Information. Master thesis, School of Engineering Information and Communications University, Daejeon, Korea, December 2005.
585. Sangshin Lee, Tomoyuki Asano, and Kwangjo Kim. RFID Mutual Authentication Scheme based on Synchronized Secret Information. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan, January 2006.
586. Su-Mi Lee, Young Ju Hwang, Dong Hoon Lee, and Jong In Lim Lim. Efficient Authentication for Low-Cost RFID Systems. In Osvaldo Gervasi, Marina Gavrilova, Vipin Kumar, Antonio Laganaà, Heow Pueh Lee, Youngsong Mun, David Taniar, and Chih Jeng Kenneth Tan, editors, *International Conference on Computational Science and its Applications – ICCSA 2005, Proceedings, Part I*, volume 3480 of *Lecture Notes in Computer Science*, pages 619–627, Singapore, Republic of Singapore, May 2005. Springer.
587. Tian-Fu Lee, Hsin-Chang Chen, and Pei-Wen Sun. An efficient RFID authentication scheme with privacy protection for multi-services. In *2012 International Conference on Business and Information – BAI2012*, Sapporo, Japan, July 2012.
588. Y.-C. Lee, Y.-C. Hsieh, P.-S. You, and T.-C. Chen. A New Ultralightweight RFID Protocol with Mutual Authentication. In *WASE International Conference on Information Engineering – ICIE '09*, pages 58–61, Taiyuan, Shanxi, August 2009. IEEE, IEEE Computer Society.
589. Yong Ki Lee, Lejla Batina, Dave Singelee, Bart Preneel, and Ingrid Verbauwhede. Anti-counterfeiting, Untraceability and Other Security Challenges for RFID Systems: Public-Key-Based Protocols and Hardware. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security, Information Security and Cryptography – THIS 2010*, pages 237–257. Springer, November 2010.
590. Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID. In Susanne Wetzel, Cristina Nita-Rotaru, and Frank Stajano, editors, *Proceedings of the 3rd ACM Conference on Wireless Network Security – WiSec'10*, pages 55–64, Hoboken, New Jersey, USA, March 2010. ACM, ACM Press.
591. Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 97–104, April 2008.
592. Yong Ki Lee, Lejla Batina, and Ingrid Verbauwhede. Untraceable RFID Authentication Protocols: Revision of EC-RAC. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
593. Yong Ki Lee and Ingrid Verbauwhede. Secure and Low-Cost RFID Authentication Protocols. In *International Workshop on Adaptive Wireless Networks – AWiN*, Saint Louis, Missouri, USA, November–December 2005. IEEE, IEEE Computer Society.
594. Young Sil Lee, Tae Yong Kim, and Hoon Jae Lee. Mutual authentication protocol for enhanced RFID security and anti-counterfeiting. In *26nd International Conference on Advanced Information Networking and Applications - Workshops, 2012. AINAW 2012*, pages 558–563, March 2012.
595. Young Sil Lee, YoungMi Park, SangHan Lee, TaeYong Kim, and Hoon Jae Lee. RFID mutual authentication protocol with unclonable RFID-tags. In *International Conference on Mobile IT Convergence – ICMIC 2011*, pages 74–77, Gyeongsangbuk-do, South Korea, September 2011.
596. Yung-Cheng Lee. Two ultralightweight authentication protocols for low-cost RFID tags. *Applied Mathematics and Information Sciences*, 6(2S):425–431, May 2012.
597. Kaleb Lee Leemaqz. *Privacy of RFID Models and Protocols*. PhD thesis, Queensland University of Technology, Brisbane, Australia, June 2013.
598. Mikko Lehtonen, Florian Michahelles, and Elgar Fleisch. How to detect cloned tags in a reliable way from incomplete RFID traces. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
599. Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, and Florian Michahelles. Securing RFID Systems by Detecting Tag Cloning. In Hideyuki Tokuda, Michael Beigl, Adrian Friday, A. J. Bernheim Brush, and Yoshito Tobe, editors, *7th International Conference on Pervasive Computing – Pervasive 2009*, volume 5538 of *Lecture Notes in Computer Science*, pages 291–308, Nara, Japan, May 2009. Springer.
600. Mikko Lehtonen, Antti Ruhanen, Florian Michahelles, and Elgar Fleisch. Serialized TID numbers - A headache or a blessing for RFID crackers? In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.

601. Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch. From Identification to Authentication - A Review of RFID Product Authentication Techniques. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
602. Mikko Lehtonen, Thorsten Staake, Florian Michahelles, and Elgar Fleisch. Strengthening the Security of Machine Readable Documents by Combining RFID and Optical Memory Devices. In *Ambient Intelligence Developments Conference – AmI.d*, Sophia-Antipolis, France, September 2006.
603. Stéphane Lemieux and Adrian Tang. Clone Resistant Mutual Authentication for Low-Cost RFID Technology. Cryptology ePrint Archive, Report 2007/170, 2007.
604. Xuefei Leng, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Tag group authentication using bit-collisions. In *Information Security for South Africa – ISSA 2012*, pages 1–8, Sandton, Johannesburg, South Africa, August 2012. IEEE.
605. Xuefei Leng, Keith Mayes, and Konstantinos Markantonakis. HB-MP+ Protocol: An Improvement on the HB-MP Protocol. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 118–124, April 2008.
606. Nan Li, Yi Mu, Willy Susilo, Fuchun Guo, and Vijay Varadharajan. Privacy-preserving authorized RFID authentication protocols. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
607. Nan Li, Yi Mu, Willy Susilo, Fuchun Guo, and Vijay Varadharajan. Vulnerabilities of an ecc-based RDIF authentication scheme. *Security and Communication Networks*, March 2015.
608. Tieyan Li. Employing lightweight primitives on low-cost RFID tags for authentication. In *68th Vehicular Technology Conference – VTC 2008*, pages 1–5, September 2008.
609. Tieyan Li and Robert H. Deng. Vulnerability Analysis of EMAP - An Efficient RFID Mutual Authentication Protocol. In *Second International Conference on Availability, Reliability and Security – AReS 2007*, Vienna, Austria, April 2007.
610. Tieyan Li and Guilin Wan. SLMAP - a secure ultra-lightweight RFID mutual authentication protocol. In *Advances in Cryptology – CHINACRYPT'07*, Lecture Notes in Computer Science, pages 19–22, Cheng Du, China, October 2007. Springer.
611. Tieyan Li and Guilin Wang. Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In Hein Venter, Mariki Eloff, Les Labuschagne, Jan Eloff, and Rossouw Von Solms, editors, *IFIP TC-11 22nd International Information Security Conference – SEC 2007*, volume 232 of *IFIP*, pages 109–120, Sandton, Gauteng, South Africa, May 2007. IFIP, Springer.
612. Tieyan Li, Guilin Wang, and Robert H. Deng. Security Analysis on a Family of Ultra-lightweight RFID Authentication Protocols. *Journal of Software*, 3(3), March 2008.
613. Ye Li and Fumio Teraoka. Privacy protection for low-cost RFID tags in IoT systems. In *7th International Conference on Future Internet Technologies – CFI 2012*, pages 60–65, Seoul, Korea, 2012. ACM.
614. Yingjiu Li, Robert H. Deng, Junzuo Lai, and Changshe Ma. On two RFID privacy notions and their relations. *ACM Transactions on Information and System Security – TISSEC'11*, 14(4), December 2011.
615. Yingjiu Li and Xuhua Ding. Protecting RFID Communications in Supply Chains. In Feng Bao and Steven Miller, editors, *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security – ASIACCS '07*, pages 234–241, Singapore, Republic of Singapore, March 2007. ACM, ACM Press.
616. Zang Li, Chao-Hsien Chu, and Wen Yao. Semantic Access Control for RFID-enabled Supply Chains. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
617. Bing Liang. Security and Performance Analysis for RFID Protocols. Master thesis, Singapore Management University, Singapore, Republic of Singapore, 2010.
618. Yi-Pin Liao and Chih-Ming Hsiao. A secure ECC-based RFID authentication scheme integrated with id-verifier transfer protocol. *Ad Hoc Networks*, (0), March 2013.
619. Ingo Liersch. Electronic passports – from secure specifications to secure implementations. *Information Security Technical Report, Elsevier*, 14(2):96–100, May 2009.
620. 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, *Workshop on Information Security Applications – WISA'05*, volume 3786 of *Lecture Notes in Computer Science*, pages 243–258, Jeju Island, Korea, August 2005. Springer.
621. Chae Hoon Lim and Taekyoung Kwon. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *International Conference on Information and Communications Security – ICICS'06*, volume 4307 of *Lecture Notes in Computer Science*, pages 1–20, Raleigh, North Carolina, USA, December 2006. Springer.
622. Jiwhan Lim, Sangjin Kim, Heekuck Oh, and Donghyun Kim. A new designated query protocol for serverless mobile RFID systems with reader and tag privacy. *Tsinghua Science and Technology*, 17(5), October 2012.

623. Seongan Lim and Ikkwon Yie. Probabilistic privacy leakage from challenge-response RFID authentication protocols. In *Proceedings of the 7th Conference on 7th WSEAS International Conference on Applied Informatics and Communications – AIC'07*, volume 7, pages 285–288, Stevens Point, Wisconsin, USA, March 2007. World Scientific and Engineering Academy and Society (WSEAS).
624. Hardy Lin, Yu-Kai Chen, and Henry Ker-Chang Chang. A new EPC RFID protocol revised from yeh et al. protocol. In *International Conference on Electronic Engineering and Computer Science – EECS 2013*, volume 4, pages 110–117, Hong Kong, China, December 2013.
625. Ziyi Lin and Joo Seok Song. An improvement in HB-Family lightweight authentication protocols for practical use of RFID system. *Journal of Advances in Computer Networks – jacn*, 1(1):61–65, January 2013.
626. Jie Ling and Jinwei Shen. New defending ultra-lightweight RFID authentication protocol against DoS attacks. In *3rd International Conference on Consumer Electronics, Communications and Networks – CECNet 2013*, pages 423–426, Xianning, China, November 2013.
627. Bing Liu and Chao-Hsien Chu. A Fine-Grained Authentication Method for Inter-Domain EPCglobal Network. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 21–34, Wuxi, China, April 2011. IOS Press.
628. H. Liu and H. Ning. Zero-knowledge authentication protocol based on alternative mode in RFID systems. *IEEE Sensors Journal*, June 2011.
629. Ya Liu, Dawu Gu, Bailan Li, and Bo Qu. Legitimate-reader-only attack on MIFARE classic. *Mathematical and Computer Modelling*, July 2012.
630. Yan-Chen Liu, Hung-Yu Chien, Yu-Chang Chen, Chu-Sing Yang, and Nai-Wei Lo. Integrated EPC Information Service Authentication Using OpenID in Cross Domains. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 144–153, Wuxi, China, April 2011. IOS Press.
631. Yanfei Liu and Sha Feng. Scalable lightweight authentication protocol with privacy preservation. In *International Conference on Computational Intelligence and Security CIS – 2014*, pages 474–478, Kunming, China, November 2014.
632. Yifei Liu, Timo Kasper, Kerstin Lemke-Rust, and Christof Paar. E-Passport: Cracking basic access control keys with COPACOBANA. In *Special-purpose Hardware for Attacking Cryptographic Systems – SHARCS'07*, September 2007.
633. Z. Liu, D. Liu, L. Li, H. Lin, and Z. Yong. Implementation of a new RFID authentication protocol for EPC Gen2 standard. *IEEE Sensors Journal*, 2014.
634. Zhaoyu Liu and Dichao Peng. True Random Number Generator in RFID Systems Against Traceability. In *IEEE Consumer Communications and Networking Conference – CCNS 2006*, volume 1, pages 620–624, Las Vegas, Nevada, USA, January 2006. IEEE, IEEE Computer Society.
635. Nai-Wei Lo, Kuo-Hui Yeh, and Hsuan-Yu Chen. Cryptanalyses of two ultralightweight rfid authentication protocols. In *Radio Frequency Identification System Security – RFIDSec Asia'12*, Cryptology and Information Security, pages 85–94, Tapei, Taiwan, November 2012. IOS Press.
636. Tobias Lohmann, Mattias Schneider, and Christoph Ruland. Analysis of Power Constraints for Cryptographic Algorithms in Mid-Cost RFID Tags. In Josep Domingo-Ferrer, Joachim Posegga, and Daniel Schreckling, editors, *International Conference on Smart Card Research and Advanced Applications – CARDIS*, volume 3928 of *Lecture Notes in Computer Science*, pages 279–288, Tarragona, Spain, April 2006. IFIP, Springer.
637. Li Lu, Jinsong Han, Lei Hu, Yunhao Liu, and Lionel Ni. Dynamic Key-Updating: Privacy-Preserving Authentication for RFID Systems. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 13–22, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
638. Li Lu, Yunhao Liu, and Jinsong Han. ACTION: Breaking the Privacy Barrier for RFID Systems. In *IEEE InfoCom 2009*, Rio de Janeiro, Brazil, April 2009. IEEE, IEEE Computer Society.
639. Chao Lv, Hui Li, Jianfeng Ma, and Ben Niu. Vulnerability analysis of lightweight secure search protocols for low-cost RFID systems. *International Journal of Radio Frequency Identification Technology and Applications*, 4(1):3–12, January 2012.
640. Changshe Ma, Yingjiu Li, Robert H. Deng, and Tieyan Li. RFID Privacy: Relation Between Two Notions, Minimal Condition, and Efficient Construction. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *Conference on Computer and Communications Security – ACM CCS'09*, pages 54–65, Chicago, Illinois, USA, November 2009. ACM, ACM Press.
641. Di Ma, Anudath K. Prasad, Nitesh Saxena, and Tuo Xiang. Location-aware and safer cards: enhancing RFID security and privacy via location sensing. In *Proceedings of the 5th ACM Conference on Wireless Network Security – WiSec'12*, pages 51–62, Tucson, Arizona, USA, April 2012. ACM, ACM Press.
642. Di Ma and Nitesh Saxena. A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems. *Security and Communication Networks*, December 2011.

643. François Macé, François-Xavier Standaert, and Jean-Jacques Quisquater. ASIC Implementations of the Block Cipher SEA for Constrained Applications. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
644. Mukundan Madhavan, Andrew Thangaraj, Yogesh Sankarasubramaniam, and Kapali Viswanathan. NLHB: A Non-Linear Hopper Blum Protocol. arXiv.org, 2010.
645. Subhamoy Maitra, Santanu Sarkar, and Morshed Chowdhury. Faster CRT-RSA Decryption Towards RFID Applications. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
646. Behzad Malek. *Light-Weight Authentication Schemes With Applications To RFID Systems*. PhD thesis, University of Ottawa, Ontario, Canada, Ottawa, Ontario, Canada, May 2011.
647. Behzad Malek and Ali Miri. Chaotic masking for securing RFID systems against relay attacks. *Security and Communication Networks*, June 2012.
648. Behzad Malek and Ali Miri. Lightweight mutual RFID authentication. In *IEEE International Conference on Communications – ICC2012*, Ottawa, Canada, June 2012.
649. Mohammad S.I. Mamun and Atsuko Miyaji. A fully-secure RFID authentication protocol from exact LPN. In *International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2013*, pages 102–109, Melbourne, Australia, July 2013.
650. Mohammad S.I. Mamun and Atsuko Miyaji. A privacy-preserving efficient RFID authentication protocol from SLPN assumption. *International Journal of Computational Science and Engineering*, 9, September 2014.
651. Mohammad S.I. Mamun and Atsuko Miyaji. RFID path authentication, revisited. In *International Conference on Advanced Information Networking and Applications – AINA-2014*, Victoria, Canada, May 2014.
652. Mohammad S.I. Mamun and Atsuko Miyaji. A scalable secure RFID ownership transfer protocol for a large supply chain. In *International Conference on Advanced Information Networking and Applications – AINA-2014*, Victoria, Canada, May 2014.
653. Mohammad S.I. Mamun, Atsuko Miyaji, and Mohammad S. Rahman. A secure and private RFID authentication protocol under SLPN problem. In Li Xu, Elisa Bertino, and Yi Mu, editors, *Network and System Security – NSS 2012*, volume 7645 of *Lecture Notes in Computer Science*, pages 476–489, Wuyishan, Fujian, China, November 2012. Springer Berlin Heidelberg.
654. Kalikinkar Mandal, Xinxin Fan, and Guang Gong. Warbler: A lightweight pseudorandom number generator for EPC C1 Gen2 passive RFID tags. *International Journal of RFID Security and Cryptography*, 2(1):82–91, December 2013.
655. Deepak Mane and Patrick Schaumont. Energy-architecture tuning for ECC-based RFID tags. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
656. Manjulata and Adarsh Kumar. Performance and probability analysis of lightweight identification protocol. In *International Conference on Signal Processing and Communication – ICSC 2013*, pages 76–81, Carrara, Australia, December 2013.
657. Shohreh Sharif Mansouri and Elena Dubrova. An improved hardware implementation of the quark hash function. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
658. Honorio Martin, Enrique San Millan, Luis Entrena, Pedro Peris Lopez, and Julio Cesar Hernandez-Castro. AKARI-X: A pseudorandom number generator for secure lightweight systems. In *2011 IEEE 17th International On-Line Testing Symposium – IOLTS 2011*, pages 228–233, July 2011.
659. Honorio Martin, Enrique San Millan, Pedro Peris-Lopez, and Juan M. Estevez Tapiador. Efficient ASIC implementation and analysis of two EPC-C1G2 RFID authentication protocols. *IEEE Sensors Journal*, PP(99):1–1, June 2013.
660. Tania Martin. *Privacy in RFID Systems*. PhD thesis, Universit Catholique de Louvain, Louvain-la-Neuve, Belgium, June 2013.
661. Santi Martinez, Madga Valls, Concepcio Roig, Francesc Gine, and Josep Miret. An Elliptic Curve and Zero Knowledge Based Forward Secure RFID Protocol. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
662. Shin'ichiro Matsuo, Le Trieu Phong, Miyako Ohkubo, and Moti Yung. Leakage-Resilient RFID Authentication with Forward-Privacy. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 176–188, Istanbul, Turkey, June 2010. Springer.
663. Keith Mayes, Konstantinos Markantonakis, and Gerhard P. Hancke. Transport ticketing security and fraud controls. *Information Security Technical Report, Elsevier*, 14(2):87–95, May 2009.
664. Abdoulaye Mbaye, Abdoul Aziz Ciss, and Oumar Niang. A lightweight identification protocol for embedded devices. arXiv.org, Computer Science, Cryptography and Security, April 2014.

665. Maire McLoone and Matthew Robshaw. New Architectures for Low-Cost Public Key Cryptography on RFID Tags. In *IEEE International Symposium on Circuits and Systems*, pages 1827–1830, New Orleans, Louisiana, USA, May 2007. IEEE, IEEE Computer Society.
666. Maire McLoone and Matthew Robshaw. Public Key Cryptography and RFID Tags. In Masayuki Abe, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA 2007*, volume 4377 of *Lecture Notes in Computer Science*, pages 372–384, San Francisco, California, USA, February 2007. Springer.
667. Carlo Meijer and Roel Verdult. Ciphertext-only cryptanalysis on hardened mifare classic cards. In *Conference on Computer and Communications Security – ACM CCS'15*, pages 18–30, Denver, Colorado, USA, October 2015. ACM, ACM Press.
668. Joan Melia-Segui, Joaquin Garcia-Alfaro, and Jordi Herrera-Joancomarti. Analysis and Improvement of a Pseudorandom Number Generator for EPC Gen2 Tags. In *1st International Workshop on Lightweight Cryptography for Resource-Constrained Devices – WLC'10*, Lecture Notes in Computer Science, Tenerife, Canary Islands, Spain, January 2010. Springer.
669. Joan Melia-Segui, Joaquin Garcia-Alfaro, and Jordi Herrera-Joancomarti. A Practical Implementation Attack on Weak Pseudorandom Number Generator Designs for EPC Gen2 Tags. *Wireless Personal Communications*, 59(1):27–42, July 2011.
670. Joan Melia-Segui, Joaquin Garcia-Alfaro, and Jordi Herrera-Joancomarti. J3Gen: A PRNG for low-cost passive RFID. *Sensors*, 13(3):3816–3830, March 2013.
671. Mohamad Merhi, Julio Cesar Hernandez-Castro, and Pedro Peris-Lopez. Studying the pseudo random number generator of a low-cost RFID tag. In *2011 IEEE International Conference on RFID Technologies and Applications – RFID-TA 2011*, pages 381–385, September 2011.
672. Luke Mirowski. Exposing clone RFID tags at the reader. In *12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications – TrustCom 2013*, pages 1669–1674, Melbourne, Australia, July 2013. IEEE.
673. Luke Mirowski and Jacky Hartnett. Deckard: A System to Detect Change of RFID Tag Ownership. *International Journal of Computer Science and Network Security*, 7(7):89–98, July 2007.
674. Luke Mirowski, Jacqueline Hartnett, and Raymond Williams. How RFID Attacks Are Expressed in Output Data. In *10th International Symposium on Pervasive Systems, Algorithms, and Networks – ISPAN'09*, pages 794–799, Kaohsiung, Taiwan, December 2009. IEEE, IEEE Computer Society.
675. Luke Mirowski, Jacqueline Hartnett, and Raymond Williams. Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels. *IEEE Pervasive Computing*, 8(4):79–84, December 2009.
676. Luke Mirowski, Jacqueline Hartnett, and Raymond Williams. Tyrell: A RFID Simulation Platform. In *5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing – ISSNIP'09*, pages 325–330, Melbourne, Australia, December 2009. IEEE, IEEE Computer Society.
677. Mala Mitra. Privacy for RFID Systems to Prevent Tracking and Cloning. *International Journal of Computer Science and Network Security*, 8(1):1–5, January 2008.
678. Aikaterini Mitrokotsa, Christos Dimitrakakis, Pedro Peris-Lopez, and Julio C. Hernandez-Castro. Reid et al.'s Distance Bounding Protocol and Mafia Fraud Attacks over Noisy Channels. *IEEE Communications Letters*, 14(2):121–123, February 2010.
679. Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. Mafia fraud attack against the RČ distance-bounding protocol. In *IEEE International Conference on RFID-Technology and Applications – IEEE RFID TA 2012*, IEEE Press, Nice, France, November 2012. IEEE.
680. Aikaterini Mitrokotsa, Cristina Onete, and Serge Vaudenay. Location leakage in distance bounding: Why location privacy does not work. Cryptology ePrint Archive, Report 2013/776, 2013.
681. Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classification of RFID Attacks. In *Proceedings of the 2nd International Workshop on RFID Technology – IWRT 2008*, Barcelona, Spain, June 2008.
682. Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classifying RFID Attacks and Defenses. *Information Systems Frontiers*, July 2009.
683. Atsuko Miyaji and Mohammad Shahriar Rahman. KIMAP: Key-insulated mutual authentication protocol for RFID. arXiv.org, Computer Science, Cryptography and Security, 2012.
684. Amin Mohammadali, Zahra Ahmadian, and Mohammad Reza Aref. Analysis and improvement of the securing RFID systems conforming to EPC class 1 generation 2 standard. Cryptology ePrint Archive, Report 2013/066, 2013.
685. David Molnar. Security and Privacy in Two RFID Deployments, With New Methods For Private Authentication and RFID Pseudonyms. Master thesis, University of California Berkeley, Berkeley, California, USA, 2006.

686. David Molnar, Andrea Soppera, and David Wagner. A Scalable, Delegatable, Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
687. David Molnar, Andrea Soppera, and David Wagner. A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In Bart Preneel and Stafford Tavares, editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 276–290, Kingston, Canada, August 2005. Springer.
688. David Molnar, Andrea Soppera, and David Wagner. Privacy for RFID Through Trusted Computing. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *Workshop on Privacy in the Electronic Society – WPES'05*, pages 31–34, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
689. David Molnar and David Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Vijayalakshmi Atluri, Birgit Pfitzmann, and Patrick Drew McDaniel, editors, *Conference on Computer and Communications Security – ACM CCS'04*, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.
690. Jean Monnerat, Serge Vaudenay, and Martin Vuagnoux. About Machine-Readable Travel Documents. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
691. Daisuke Moriyama. Cryptanalysis and improvement of a provably secure RFID ownership transfer protocol. In *Second International Workshop on Lightweight Cryptography for Security and Privacy – LightSec 2013*, Gebze, Turkey, May 2013.
692. Daisuke Moriyama. Provably secure two-round RFID grouping proof protocols. In *RFID Technology and Applications Conference – RFID-TA 2014*, pages 272–276, Tampere, Finland, September 2014.
693. Daisuke Moriyama. A provably secure offline RFID yoking-proof protocol with anonymity. In Thomas Eisenbarth and Erdinç Öztürk, editors, *Lightweight Cryptography for Security and Privacy – LightSec 2015*, volume 8898 of *Lecture Notes in Computer Science*, pages 155–167, Bochum, Germany, March 2015. Springer.
694. Daisuke Moriyama, Shin'ichiro Matsuo, and Miyako Ohkubo. Relations among notions of privacy for RFID authentication protocols. In Sara Foresti, Moti Yung, and Fabio Martinelli, editors, *17th European Symposium on Research in Computer Security – ESORICS 2012*, volume 7459, pages 661–678, Pisa, Italy, September 2012. Springer Berlin / Heidelberg.
695. Daisuke Moriyama, Shin'ichiro Matsuo, and Moti Yung. PUF-based RFID authentication secure and private under memory leakage. Cryptology ePrint Archive, Report 2013/712, 2013.
696. Daisuke Moriyama, Miyako Ohkubo, and Shinichiro Matsuo. A forward privacy model for RFID authentication protocols. In Lorenzo Cavallaro and Dieter Gollmann, editors, *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems – WISTP 2013*, volume 7886 of *Lecture Notes in Computer Science*, pages 98–111, Heraklion, Greece, May 2013. Springer Berlin Heidelberg.
697. M.M. Morshed. Efficient mutual authentication protocol for radiofrequency identification systems. *Communications, Institution of Engineering and Technology*, 6(16):2715–2724, November 2012.
698. Monzur Morshed, Anthony Atkins, and Hongnian Yu. Efficient mutual authentication protocol for radiofrequency identification systems. *Communications, Institution of Engineering and Technology*, 6(16):2715–2724, November 2012.
699. Umar Mujahid, M. Najam-ul islam, Jameel Ahmed, and Usman Mujahid. Cryptanalysis of ultralightweight RFID authentication protocol. Cryptology ePrint Archive, Report 2013/385, 2013.
700. 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.
701. Jorge Munilla, Mike Burmester, and Albert Peinado. Attacks on secure ownership transfer for multi-tag multi-owner passive RFID environments. Cryptology ePrint Archive, Report 2014/968, 2014.
702. Jorge Munilla, Andres Ortiz, and Alberto Peinado. Distance Bounding Protocols with Void-Challenges for RFID. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
703. Jorge Munilla and Alberto Peinado. Distance Bounding Protocols for RFID Enhanced by using Void-Challenges and Analysis in Noisy Channels. *Wireless Communications and Mobile Computing*, 8(9):1227–1232, January 2008.
704. Jorge Munilla and Alberto Peinado. Security Analysis of Tu and Piramuthu's Protocol. In *New Technologies, Mobility and Security – NTMS'08*, pages 1–5, Tangier, Morocco, November 2008. IEEE, IEEE Computer Society.
705. Jorge Munilla and Alberto Peinado. Enhanced Low-cost RFID Protocol to Detect Relay Attacks. *Wireless Communications and Mobile Computing*, 10(3):361–371, March 2009.

706. Jorge Munilla and Alberto Peinado. Attacks on a Distance Bounding Protocol. *Computer Communications, Elsevier*, 33(7):884–889, May 2010.
707. Christoph Nagl and Michael Hutter. Coupon Recalculation for the Schnorr and GPS Identification Scheme: A Performance Evaluation. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
708. Pablo Najera and Javier Lopez. *RFID: Technological Issues and Privacy Concerns*, pages 285–306. Auerbach Publications, 2007.
709. Pablo Najera, Francisc Moyano, and Javier Lopez. Security mechanisms and access control infrastructure for e-passports and general purpose e-documents. *Journal of Universal Computer Science*, 15(5):970–991, March 2009.
710. Jayagopal Narayanaswamy. Security framework for combining confidentiality and integrity. Master thesis, Dalhousie University, Halifax, Nova Scotia, Canada, April 2015.
711. Jayagopal Narayanaswamy, Raghav Sampangi, and Srinivas Sampalli. SCARS: Simplified cryptographic algorithm for RFID systems. In *RFID Technology and Applications Conference – RFID-TA 2014*, pages 32–37, Tampere, Finland, September 2014.
712. Mu' awya Naser, Mohammad Al Majaly, Muhammad Rafie, and Rahmat Budiarto. A Framework for RFID Systems Security for Human Identification Based on Three-Tier Categorization Model. In *International Conference on Signal Acquisition and Processing – ICSAP 2009*, pages 103–107, Kuala Lumpur, Malaysia, April 2009. IEEE, IEEE Computer Society.
713. Muaway Naser, Yazn Alshamaila, Rahmat Budiarto, and Pedro Peris-Lopez. SURV: Shelled ultralightweight randomized value authentication protocol for low-cost RFID tags. *International Journal of Computer and Electrical Engineering*, pages 206–214, April 2015.
714. Muawya Naser, Pedro Peris-Lopez, Rahmat Budiarto, and Benjamn Ramos lvarez. A note on the security of PAP. *Computer Communications*, 34(18):2248–2249, 2011.
715. Keyvan Kashkouli Nejad, Xiaohong Jiang, and Michitaka Kameyama. Non-blocking tag scanning for passive RFID localization. In *11th International Conference on Intelligent Systems Design and Applications – ISDA 2011*, pages 1140–1145, November 2011.
716. Long Hoang Nguyen. Rational distance-bounding protocols over noisy channels. In *The 4th International Conference on Security of Information and Networks – SIN 2011*, November 2011.
717. Dang Nguyen Duc and Kwangjo Kim. Grouping-Proof Protocol for RFID Tags: Security Definition and Scalable Construction. Cryptology ePrint Archive, Report 2009/609, 2009.
718. Dang Nguyen Duc, Kwangjo Kim, and Chan Yeob Yeun. Reconsidering Ryu-Takagi RFID Authentication Protocol. In *5th International Conference for Internet Technology and Secured Transactions – ICITST'10*, pages 1–6, London, UK, November 2010. IEEE, IEEE Computer Society.
719. Dang Nguyen Duc, Jaemin Park, Hyunrok Lee, and Kwangjo Kim. Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan, January 2006.
720. Ventzislav Nikov and Marc Vauclair. Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319, 2008.
721. Huansheng Ning, Hong Liu, and Chen Yang. Ultralightweight RFID authentication protocol based on random partitions of pseudorandom identifier and pre-shared secret value. *Chinese Journal of Electronics*, 20(4):701–707, October 2011.
722. Huansheng Ning, Hong Liu, Laurence T. Yang, and Yan Zhang. Dual cryptography authentication protocol and its security analysis for radio frequency identification systems. *Concurrency and Computation: Practice and Experience*, 2011.
723. Rishab Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. Cryptology ePrint Archive, Report 2009/200, 2009.
724. Rishab Nithyanand. Securing Personal RFID Tags and Infrastructures. Master thesis, University of California, Irvine, Irvine, California, USA, March 2010.
725. Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems. Cryptology ePrint Archive, Report 2009/465, 2009.
726. Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. Readers Behaving Badly - Reader Revocation in PKI-Based RFID Systems. In Dimitris Gritzalis, Bart Preneel, and Marianthi Theoharidou, editors, *15th European Symposium on Research in Computer Security – ESORICS 2010*, volume 6345 of *Lecture Notes in Computer Science*, pages 19–36, Athens, Greece, September 2010. Springer.
727. Ben Niu, Xiaoyan Zhu, Haotian Chi, and Hui Li. Privacy and authentication protocol for mobile RFID systems. *Wireless Personal Communications*, January 2014.

728. Haifeng Niu, Eyad Taqieddin, and Jagannathan Sarangapani. EPC Gen2v2 RFID standard authentication and ownership management protocol. *IEEE Transactions on Mobile Computing*, March 2015.
729. Yasunobu Nohara and Sozo Inoue. A Secure and Scalable Identification for Hash-based RFID Systems Using Updatable Pre-computation. In Susanne Wetzel, Cristina Nita-Rotaru, and Frank Stajano, editors, *Proceedings of the 3rd ACM Conference on Wireless Network Security – WiSec'10*, pages 65–74, Hoboken, New Jersey, USA, March 2010. ACM, ACM Press.
730. Yasunobu Nohara, Sozo Inoue, Kensuke Baba, and Hiroto Yasuura. Quantitative Evaluation of Unlinkable ID Matching Schemes. In Vijay Atluri, Sabrina De Capitani di Vimercati, and Roger Dingledine, editors, *Workshop on Privacy in the Electronic Society – WPES'05*, pages 55–60, Alexandria, Virginia, USA, November 2006. ACM, ACM Press.
731. Yasunobu Nohara, Sozo Inoue, and Hiroto Yasuura. A secure high-speed identification scheme for RFID using bloom filters. In *Third International Conference on Availability, Reliability and Security – AReS 2008*, pages 727–722, Barcelona, Spain, March 2008.
732. Karsten Nohl and David Evans. Quantifying Information Leakage in Tree-Based Hash Protocols. In Peng Ning, Sihan Qing, and Ninghui Li, editors, *International Conference on Information and Communications Security – ICICS'06*, volume 4307 of *Lecture Notes in Computer Science*, pages 228–237, Raleigh, North Carolina, USA, December 2006. Springer.
733. Karsten Nohl and David Evans. Quantifying Information Leakage in Tree-Based Hash Protocols. Technical Report UVA-CS-2006-20, University of Virginia, Department of Computer Science, Charlottesville, Virginia, USA, 2006.
734. Karsten Nohl and David Evans. Hiding in Groups: On the Expressiveness of Privacy Distributions. In Sushil Jajodia, Pierangela Samarati, and Stelvio Cimato, editors, *IFIP TC-11 23rd International Information Security Conference – SEC 2008*, volume 278 of *IFIP*, pages 1–15, Milan, Italy, September 2008. IFIP, Springer.
735. Karsten Nohl, David Evans, Starbug, and Henryk Plotz. Reverse-Engineering a Cryptographic RFID Tag. In Paul C. van Oorschot, editor, *17th USENIX Security Symposium – USENIX'08*, pages 185–194, San Jose, California, USA, July 2008. USENIX.
736. Dorice Diane Nyamy, Simon Elrharbi, Pascal Urien, Hervé Chabanne, Thomas Icart, Cyrille Pépin, Mathieu Bouet, Daniel De Oliveira Cunha, Vincent Guyot, Patrice Krzanik, and Jean-Ferdinand Susini. HIP tags, a new paradigm for the Internet of Things. In *Proceedings of the 1st IFIP Wireless Days Conference – IFIP 2008*, Dubai, United Arab Emirates, November 2008.
737. Miyako Ohkubo and Koutarou Suzuki. Forward Secure RFID Privacy Protection Scheme with Restricted Traceability. In Jianying Zhou, Moti Yung, and Feng Bao, editors, *International Conference on Applied Cryptography and Network Security – ACNS 2006*, volume 3989 of *Lecture Notes in Computer Science*, Singapore, Republic of Singapore, June 2006. Springer.
738. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to "Privacy-Friendly" Tags. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
739. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Efficient Hash-Chain Based RFID Privacy Protection Scheme. In *International Conference on Ubiquitous Computing – Ubicomp, Workshop Privacy: Current Status and Future Directions*, Nottingham, England, September 2004.
740. Maire O'Neill (McLoone). Low-Cost SHA-1 Hash Function Architecture for RFID Tags. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
741. Cristina Onete. Key updates for RFID distance-bounding protocols: Achieving narrow-destructive privacy. Cryptology ePrint Archive, Report 2012/165, 2012.
742. Maria Cristina Onete. *Security Aspects of Distance-Bounding Protocols.* PhD thesis, Technische Universitat Darmstadt, Darmstadt, Germany, December 2012.
743. Yossef Oren. Remote Power Analysis of RFID Tags. Cryptology ePrint Archive, Report 2007/330, 2007.
744. Yossef Oren and Martin Feldhofer. WIPR - a Public Key Identification on Two Grains of Sand. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
745. Yossef Oren and Martin Feldhofer. A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *Proceedings of the 2nd ACM Conference on Wireless Network Security – WiSec'09*, pages 59–68, Zurich, Switzerland, March 2009. ACM, ACM Press.
746. Yossef Oren and Avishai Wool. Relay Attacks on RFID-Based Electronic Voting Systems. Cryptology ePrint Archive, Report 2009/422, 2009.
747. Yossef Oren and Avishai Wool. RFID-based Electronic Voting: What Could Possibly Go Wrong? In *IEEE International Conference on RFID – IEEE RFID 2010*, pages 118–125, Orlando, Florida, USA, April 2010. IEEE, IEEE Computer Society.

748. David Oswald, Timo Kasper, and Christof Paar. Side-Channel Analysis of Cryptographic RFIDs with Analog Demodulation. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
749. Khaled Ouafi. *Security and Privacy in RFID Systems*. PhD thesis, EPFL, Lausanne, Switzerland, February 2012.
750. 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 2008. Springer.
751. Khaled Ouafi and Raphael C.-W. Phan. Privacy of Recent RFID Authentication Protocols. In Liqun Chen, Yi Mu, and Willy Susilo, editors, *4th International Conference on Information Security Practice and Experience – ISPEC 2008*, volume 4991 of *Lecture Notes in Computer Science*, pages 263–277, Sydney, Australia, April 2008. Springer.
752. Khaled Ouafi and Raphael C.-W. Phan. Traceable Privacy of Recent Provably-Secure RFID Protocols. In Steven M. Bellovin, Rosario Gennaro, Angelos D. Keromytis, and Moti Yung, editors, *Proceedings of the 6th International Conference on Applied Cryptography and Network Security – ACNS 2008*, volume 5037 of *Lecture Notes in Computer Science*, pages 479–489, New York City, New York, USA, June 2008. Springer.
753. Khaled Ouafi and Serge Vaudenay. Pathchecker: an RFID Application for Tracing Products in Suply-Chains. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
754. Khaled Ouafi and Serge Vaudenay. Strong privacy for rfid systems from plaintext-aware encryption. In *Proceedings of the 11th International Conference on Cryptology and Network Security – CANS 2012*, volume 7712 of *LNCS*, pages 247–262, Darmstadt, Germany, December 2012. Springer.
755. Mehmet Hilal Özcanhan, Gökhan Dalkiliç, and Semih Utku. Analysis of two protocols using EPC Gen-2 tags for safe inpatient medication. In *International Symposium on Innovations in Intelligent Systems and Applications – INISTA 2013*, pages 1–6, Albena, Bulgaria, June 2013.
756. Mehmet Hilal Özcanhan, Gökhan Dalkiliç, and Semih Utku. Is NFC a better option instead of EPC gen-2 in safe medication of inpatients. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
757. Mehmet Hilal Özcanhan, Gökhan Dalkiliç, and Semih Utku. Cryptographically supported NFC tags in medication for better inpatient safety. *Journal of Medical Systems*, 38(61):1–15, June 2014.
758. Krishna Pabbuleti, Deepak Mane, and Patrick Schaumont. Energy budget analysis for signature protocols on a self-powered wireless sensor node. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
759. Elena Pagnin, Gerhard Hancke, and Aikaterini Mitrokotsa. Using distance-bounding protocols to securely verify the proximity of two-hop neighbours. *Communications Letters, IEEE*, PP(99), May 2015.
760. Elena Pagnin, Anjia Yang, Gerhard Hancke, and Aikaterini Mitrokotsa. HB+DB, mitigating man-in-the-middle attacks against HB+ with distance bounding. In *Proceedings of the 8th ACM conference on Security and privacy in wireless and mobile networks – WiSec'15*, New York, USA, June 2015. ACM.
761. Radu-Ioan Paise and Serge Vaudenay. Mutual Authentication in RFID: Security and Privacy. In Masayuki Abe and Virgil D. Gligor, editors, *Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security – ASIACCS'08*, pages 292–299, Tokyo, Japan, March 2008. ACM, ACM Press.
762. Paolo Palmieri, Luca Calderoni, and Dario Maio. Spatial bloom filters: Enabling privacy in location-aware applications. Cryptology ePrint Archive, Report 2014/531, 2014.
763. Liaojun Pang, Huixian Li, Liwei He, Ali Alramadhan, and Yumin Wang. Secure and efficient lightweight RFID authentication protocol based on fast tag indexing. *International Journal of Communication Systems*, March 2013.
764. Konstantinos Papagiannopoulos and Aram Verstegen. Speed and size optimized implementations of the PRESENT cipher for tiny AVR devices. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
765. Kostas Papagiannopoulos. High throughput in slices: the case of PRESENT, PRINCE and KATAN64 ciphers. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
766. Ioannis Paparrizos, Stylianos Basagiannis, and Sophia Petridou. Quantitative analysis for authentication of low-cost RFID tags. In *IEEE 36th Conference on Local Computer Networks – LCN 2011*, pages 299–302. IEEE, October 2011.
767. T. Parameswaran, C. Palanisamy, and E. Lavanya. An optimized novel secure RFID authentication protocol against compromised tag attack. *International Journal of Advanced Research in Science, Engineering and Technology*, 1(5):295–302, December 2014.
768. Jeong Su Park, Su Mi Lee, Eun Young Choi, and Dong Hoon Lee. Self Re-encryption Protocol Providing Strong Privacy for Low Cost RFID System. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Lagan, Youngsong Mun, and Hyunseung Choo, editors, *International Conference*

on Computational Science and its Applications – ICCSA 2006, volume 3983 of *Lecture Notes in Computer Science*, pages 316–325, Glasgow, Scotland, May 2006. Springer.

769. Myung-Ho Park, Ki-Gon Nam, Jin Seok Kim, Dae Hyun Yum, and Pil Joong Lee. Unilateral distance bounding protocol with bidirectional challenges. *IEICE Transactions on Information and Systems*, E96-D(1):134–137, January 2013.
770. Vijayakrishnan Pasupathinathan, Josef Pieprzyk, and Huaxiong Wang. An On-Line Secure E-Passport Protocol. In Liqun Chen, Yi Mu, and Willy Susilo, editors, *4th International Conference on Information Security Practice and Experience – ISPEC 2008*, volume 4991 of *Lecture Notes in Computer Science*, pages 14–28, Sydney, Australia, April 2008. Springer.
771. Roel Peeters and Jens Hermans. Wide strong private RFID identification based on zero-knowledge. Cryptology ePrint Archive, Report 2012/389, 2012.
772. Roel Peeters and Jens Hermans. Attack on liao and hsiaos secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Cryptology ePrint Archive, Report 2013/399, 2013.
773. Christian Pendl, Markus Pelnar, and Michael Hutter. Elliptic Curve Cryptography on the WISP UHF RFID Tag. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
774. Senthilkumar Chinnappa Gounder Periaswamy, Dale R. Thompson, and Henry P. Romero. Fingerprinting Radio Frequency Identification Tags Using Timing Characteristics. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
775. Pedro Peris-Lopez. *Lightweight Cryptography in Radio Frequency Identification (RFID) Systems*. PhD thesis, Computer Science Department, Carlos III University of Madrid, November 2008.
776. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Christos Dimitrakakis, Aikaterini Mitrokotsa, and Juan M. Estevez-Tapiador. Shedding Light on RFID Distance Bounding Protocols and Terrorist Fraud Attacks. arXiv.org, Computer Science, Cryptography and Security, 2010.
777. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, Tieyan Li, and Yingjiu Li. Vulnerability analysis of RFID protocols for tag ownership transfer. *Computer Networks, Elsevier*, 54(9):1502–1508, June 2010.
778. 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.
779. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, Esther Palomar, and Jan C. A. van der Lubbe. Cryptographic Puzzles and Distance-bounding Protocols: Practical Tools for RFID Security. In *IEEE International Conference on RFID – IEEE RFID 2010*, pages 45–52, Orlando, Florida, USA, April 2010. IEEE, IEEE Computer Society.
780. 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.
781. 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.
782. 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.
783. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. RFID Systems: A Survey on Security Threats and Proposed Solutions. In Pedro Cuenca and Luis Orozco-Barbosa, editors, *11th IFIP International Conference on Personal Wireless Communications – PWC'06*, volume 4217 of *Lecture Notes in Computer Science*, pages 159–170, Albacete, Spain, September 2006. Springer.
784. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks. In Mieso K. Denko, Chi-Sheng Shih, Kuan-Ching Li, Shiao-Li Tsao, Qing-An Zeng, Soo-Hyun Park, Young-Bae Ko, Shih-Hao Hung, and Jong Hyuk Park, editors, *International Workshop on Security in Ubiquitous Computing Systems – Secubiq 2007*, volume 4809 of *Lecture Notes in Computer Science*, pages 781–794, Taipei, Taiwan, December 2007. Springer.

785. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Cryptanalysis of a Novel Authentication Protocol Conforming to EPC-C1G2 Standard. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
786. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. LAMED - A PRNG for EPC Class-1 Generation-2 RFID Specification. *Computer Standard & Interfaces, Elsevier*, In Press, Corrected Proof, February 2007.
787. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Solving the Simultaneous Scanning Problem Anonymously: Clumping Proofs for RFID Tags. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2007*, pages 55–60, Istanbul, Turkey, July 2007. IEEE, IEEE Computer Society.
788. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-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, *Workshop on Information Security Applications – WISA'08*, volume 5379 of *Lecture Notes in Computer Science*, pages 56–68, Jeju Island, Korea, September 2008. Springer.
789. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Jan C. A. van der Lubbe. Security Flaws in a Recent Ultralightweight RFID Protocol. arXiv.org, 2009.
790. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Jan C. A. van der Lubbe. Shedding Some Light on RFID Distance Bounding Protocols and Terrorist Attacks. arXiv.org, Computer Science, Cryptography and Security, 2009.
791. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, and Jan C. A. van der Lubbe. Security Flaws in a Recent Ultralightweight RFID Protocol. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, pages 83–93, Singapore, Republic of Singapore, February 2010. IOS Press.
792. 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.
793. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M.E. Tapiador, and Jan C.A. van der Lubbe. Cryptanalysis of an EPC class-1 generation-2 standard compliant authentication protocol. *Engineering Applications of Artificial Intelligence*, 24(6):1061–1069, 2011.
794. Pedro Peris-Lopez, Tieyan Li, Lim Tong Lee, Julio C. Hernandez-Castro, and Juan M. Estevez-Tapiador. Vulnerability Analysis of a Mutual Authentication Scheme under the EPC Class-1 Generation-2 Standard. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
795. Pedro Peris-Lopez, Agustin Orfila, Julio C. Hernandez-Castro, and Jan C.A. van der Lubbe. Flaws on RFID grouping-proofs. Guidelines for future sound protocols. *Journal of Network and Computer Applications*, May 2010.
796. Pedro Peris-Lopez, Agustin Orfila, Aikaterini Mitrokotsa, and Jan C.A. van der Lubbe. A Comprehensive RFID Solution to Enhance Inpatient Medication Safety. *International Journal of Medical Informatics*, October 2010.
797. Pedro Peris-Lopez, Agustin Orfila, Esther Palomar, and Julio Hernandez-Castro. A secure distance-based rfid identification protocol with an off-line back-end database. *Personal and Ubiquitous Computing*, 15, 2011.
798. Pedro Peris-Lopez, Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. RFID in ehealth: How combat medications errors and strengthen patient safety. *Journal of Medical and Biological Engineering*, January 2013.
799. Pedro Peris-Lopez, Enrique San Millan, Jan C.A. van der Lubbe, and Luis A. Entrena. Cryptographically Secure Pseudo-Random Bit Generator for RFID Tags. In *5th International Conference for Internet Technology and Secured Transactions – ICITST'10*, pages 490–495, London, UK, November 2010. IEEE, IEEE Computer Society.
800. Pedro Peris-Lopez, Juan Estevez Tapiador, and Enrique San Millan. An estimator for the ASIC footprint area of lightweight cryptographic algorithms. *IEEE Transactions on Industrial Informatics*, 2013.
801. Pedro Peris-Lopez, Li Tieyan, and Julio C. Hernandez-Castro. Lightweight Props on the Weak Security of EPC Class-1 Generation-2 Standard. *IEICE Transactions on Information and Systems*, E93.D(3):518–527, 2010.
802. Pedro Peris-Lopez, Lim Tong Lee, and Tieyan Li. Providing Stronger Authentication at a Low-Cost to RFID Tags Operating under the EPCglobal Framework. In Cheng-Zhong Xu and Minyi Guo, editors, *Embedded and Ubiquitous Computing - Volume 02 – EUC'08*, pages 159–166, Shanghai, China, December 2008. IEEE, IEEE Computer Society.
803. Peter Pessl and Michael Hutter. Curved tags – a low-resource ECDSA implementation tailored for RFID tags. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.

804. Tuan Anh Pham, Mohammad S. Hasan, and Hongnian Yu. A RFID mutual authentication protocol based on AES algorithm. In *UKACC International Conference on Control – CONTROL 2012*, pages 997–1002, Cardiff, UK, September 2012. IEEE.
805. Raphael C.-W. Phan. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol - SASI. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2008.
806. Pablo Picazo-Sanchez, Nasour Bagheri, Pedro Peris-Lopez, and Juan Estevez Tapiador. Two RFID standard-based security protocols for healthcare environments. *Journal of Medical Systems*, 37(5):1–12, August 2013.
807. Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, and Nasour Bagheri. Weaknesses of fingerprint-based mutual authentication protocol. *Security and Communication Networks*, November 2014.
808. Pablo Picazo-Sanchez, Lara Ortiz-Martin, Pedro Peris-Lopez, and Julio Cesar Hernandez-Castro. Cryptanalysis of the RNTS system. *The Journal of Supercomputing*, pages 1–12, January 2013.
809. Selwyn Piramuthu. HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication. In *Collaborative Electronic Commerce Technology and Research – CollECTeR 2006*, Basel, Switzerland, June 2006.
810. Selwyn Piramuthu. On Existence Proofs for Multiple RFID Tags. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006*, Lyon, France, June 2006. IEEE, IEEE Computer Society.
811. Selwyn Piramuthu. Lightweight Cryptographic Authentication in Passive RFID-Tagged Systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 38(3):360–376, 2008.
812. Selwyn Piramuthu. RFID Mutual Authentication Protocols. *Decision Support Systems, Elsevier*, In press, October 2010.
813. Thomas Plos, Manfred Aigner, Thomas Baier, Martin Feldhofer, Michael Hutter, Thomas Korak, and Erich Wenger. Semi-passive RFID development platform for implementing and attacking security tags. *International Journal of RFID Security and Cryptography*, 1:16–24, March 2012.
814. Thomas Plos, Michael Hutter, and Martin Feldhofer. Evaluation of Side-Channel Preprocessing Techniques on Cryptographic-Enabled HF and UHF RFID-Tag Prototypes. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
815. Ivo Pooters. Keep Out of My Passport: Access Control Mechanisms in E-passports, 2008.
816. Axel Poschmann, Gregor Leander, Kai Schramm, and Christof Paar. A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
817. Axel Poschmann, Matthew Robshaw, Frank Vater, and Christof Paar. Lightweight Cryptography and RFID: Tackling the Hidden Overheads. In *International Conference on Information Security and Cryptology – ICISC 2009*, Seoul, Korea, December 2009.
818. Marcin Poturalski, Manuel Flury, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures. *IEEE Transactions on Wireless Communications*, 10(4):1334–1344, 2011.
819. P. Prabhusundhar, V. K. Narendira Kumar, and B. Srinivasan. Border crossing security and privacy in biometric passport using cryptographic authentication protocol. In *International Conference on Computer Communication and Informatics (ICCCI) – 2013*, pages 1–7, January 2013.
820. Xiaofei Qian, Xinbao Liu, Shanlin Yang, and Chao Zuo. Security and privacy analysis of Tree-LSHB+ protocol. *Wireless Personal Communications*, March 2014.
821. 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.
822. Saša Radomirović and Mohammad Torabi Dashti. Derailing attacks. In *Security Protocols Workshop – SPW 2015*, LNCS, Cambridge, United Kingdom, March 2015. Springer-Verlag.
823. Tibor Radványi, Csaba Biró, Sándor Király, Péter Szigetváry, and Péter Takács. Survey of attacking and defending in the RFID system. *Annales Mathematicae et Informaticae*, 44:151–164, June 2015.
824. M. Raguramajayan, K. Sivasubramaniam, Y. Ananthi, and S. Nagarajan. Location-aware E-passport: Enhancing security and privacy. *International Journal of Applied Engineering Research*, 9(18):4693–4697, July 2014.
825. V. Ramachandra, M. Rahman, and S. Sampalli. Lightweight matrix-based authentication protocol for RFID. In *19th International Conference on Software Telecommunications and Computer Networks – SoftCOM'11*, pages 1–6, Split, Croatia, September 2011. IEEE, IEEE Computer Society.
826. Damith Ranasinghe, Daniel Engels, and Peter Cole. Low-Cost RFID Systems: Confronting Security and Privacy. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.

827. Damith Ranasinghe, Daniel Engels, and Peter Cole. Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.
828. Aanjhan Ranganathan, Boris Danev, and Srdjan Capkun. Low-power distance bounding. arXiv.org, Computer Science, Cryptography and Security, April 2014.
829. Kasper B. Rasmussen and Srdjan Capkun. Location Privacy of Distance Bounding Protocols. In Peng Ning, Paul F. Syverson, and Somesh Jha, editors, *Conference on Computer and Communications Security – ACM CCS'08*, pages 149–160, Alexandria, Virginia, USA, October 2008. ACM, ACM Press.
830. Kasper B. Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, and Srdjan Capkun. Proximity-based Access Control for Implantable Medical Devices. In Ehab Al-Shaer, Somesh Jha, and Angelos D. Keromytis, editors, *Conference on Computer and Communications Security – ACM CCS'09*, pages 43–53, Chicago, Illinois, USA, November 2009. ACM, ACM Press.
831. Kasper B. Rasmussen and Srdjan Čapkun. Realization of RF distance bounding. In *19th USENIX Security Symposium – USENIX'10*, Washington, DC, USA, August 2010. USENIX.
832. Biplob Ray, Morshed Howdhury, Jemal Abawajy, and Monika Jesmin. Secure object tracking protocol for networked RFID systems. In *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing – SNPD 2015*, pages 1–7, Takamatsu, Japan, June 2015. IEEE.
833. Jason Reid, Juan Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting Relay Attacks with Timing Based Protocols. QUT ePrint, Report 3264, 2006.
834. Jason Reid, Juan Gonzalez Nieto, Tee Tang, and Bouchra Senadji. Detecting Relay Attacks with Timing Based Protocols. In Feng Bao and Steven Miller, editors, *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security – ASIACCS '07*, pages 204–213, Singapore, Republic of Singapore, March 2007. ACM, ACM Press.
835. Keunwoo Rhee, Jin Kwak, Seungjoo Kim, and Dongho Won. Challenge-Response based RFID Authentication Protocol for Distributed Database Environment. In Dieter Hutter and Markus Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2005*, volume 3450 of *Lecture Notes in Computer Science*, pages 70–84, Boppard, Germany, April 2005. Springer.
836. Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting Passports. Epractice, 2008.
837. Melanie R. Rieback. *Security and Privacy of Radio Frequency Identification*. PhD thesis, Vrije Universiteit, Amsterdam, The Netherlands, 2008.
838. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags. In Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe, editors, *International Workshop on Security Protocols – IWSP'05*, volume 4631 of *Lecture Notes in Computer Science*, pages 51–59, Cambridge, England, April 2005. Springer.
839. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In Colin Boyd and Juan Manuel Gonzalez Nieto, editors, *Australasian Conference on Information Security and Privacy – ACISP'05*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194, Brisbane, Australia, July 2005. Springer.
840. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Uniting Legislation with RFID Privacy-Enhancing Technologies. In *Security and Protection of Information*, Brno, Czech Republic, May 2005.
841. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. Is Your Cat Infected with a Computer Virus? In *Pervasive Computing and Communications*, pages 169–179, Pisa, Italy, March 2006. IEEE, IEEE Computer Society.
842. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, 5(1):62–69, January–March 2006.
843. Melanie R. Rieback, Georgi Gaydadjiev, Bruno Crispo, Rutger Hofman, and Andrew S. Tanenbaum. A Platform for RFID Security and Privacy Administration. In *USENIX/SAGE Large Installation System Administration conference – LISA'06*, Washington, DC, USA, December 2006. USENIX.
844. Panagiotis Rizomiliotis and Stefanos Gritzalis. GHB#: A provably secure HB-like lightweight authentication protocol. In Feng Bao, Pierangela Samarati, and Jianying Zhou, editors, *Proceedings of the 10th International Conference on Applied Cryptography and Network Security – ACNS 2012*, Singapore, China, June 2012.
845. Panagiotis Rizomiliotis and Stefanos Gritzalis. Revisiting lightweight authentication protocols based on hard learning problems. In *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks – WiSec'13*, WiSec'13, pages 125–130, New York, USA, April 2013. ACM.
846. Panagiotis Rizomiliotis, Evangelos Rekleitis, and Stefanos Gritzalis. Designing secure RFID authentication protocols is (still) a non-trivial task. In *5th International Conference on Network ans System Security – NSS 2011*, pages 73–80, Milan, Italy, September 2011. IEEE, IEEE Computer Society.

847. Matthew Robshaw and Axel Poschmann. The Case for Dynamic RFID Tag Authentication. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
848. 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, Zurich, Switzerland, February 2013.
849. Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-Lightweight Implementations for Smart Devices — Security for 1000 Gate Equivalents. In Gilles Grimaud and Franois-Xavier Standaert, editors, *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications – CARDIS '08*, volume 5189 of *Lecture Notes in Computer Science*, pages 89–103, Royal Holloway University of London, United Kingdom, September 2008. Springer.
850. Samad Rostampour, Mojtaba Eslamnezhad Namin, and Mehdi Hosseinzadeh. A novel mutual RFID authentication protocol with low complexity and high security. *International Journal of Modern Education and Computer Science*, pages 17–24, January 2014.
851. Pawel Rotter. A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing*, 7(2):70–77, June 2008.
852. Pawel Rotter, Barbara Daskala, and Ramón Compano. RFID Implants: Opportunities and Challenges for Identifying People. *IEEE Technology and Society Magazine*, 27(2):24–32, Summer 2008.
853. Eun-Kyung Ryu, Dae-Soo Kim, and Kee-Young Yoo. On elliptic curve based untraceable RFID authentication protocols. In *Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security – IHMMSec'15*, pages 147–153, Portland, Oregon, USA, June 2015. ACM.
854. Markku-Juhani O. Saarinen. Related-key attacks against full hummingbird-2. In *Fast Software Encryption – FSE'13*, Singapore, Singapore, March 2013.
855. Markku-Juhani O. Saarinen and Daniel Engels. A do-it-all-cipher for RFID: Design requirements (extended abstract). Cryptology ePrint Archive, Report 2012/317, 2012.
856. Mohammad Sabzinejad Farash. Cryptanalysis and improvement of an efficient mutual authentication RFID scheme based on elliptic curve cryptography. *The Journal of Supercomputing*, July 2014.
857. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. User Privacy in Transport Systems Based on RFID E-Tickets. In *Workshop on Privacy in Location-Based Applications – PILBA'08*, Malaga, Spain, October 2008.
858. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. Anonymizer-Enabled Security and Privacy for RFID. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *8th International Conference on Cryptology And Network Security – CANS'09*, volume Lecture Notes in Computer Science of *5888*, pages 134–153, Kanazawa, Ishikawa, Japan, December 2009. Springer.
859. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. Efficient RFID Security and Privacy with Anonymizers. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
860. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. Enhancing RFID Security and Privacy by Physically Unclonable Functions. In Ahmad-Reza Sadeghi and David Naccache, editors, *Towards Hardware-Intrinsic Security, Information Security and Cryptography – THIS 2010*, pages 281–305. Springer, November 2010.
861. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. PUF-Enhanced RFID Security and Privacy. In *Secure Component and System Identification – SECSI'10*, Cologne, Germany, April 2010.
862. M.F. Sadikin and M. Kyas. Security and privacy protocol for emerging smart RFID applications. In *International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing – SNPD 2014*, pages 1–7, Las Vegas, NV, July 2014.
863. Masoumeh Safkhani, Nasour Bagheri, Somitra Sanadhya Kumar, and Majid Naderi. Cryptanalysis of improved yeh et al.'s authentication protocol: An EPC class-1 generation-2 standard compliant protocol. Cryptology ePrint Archive, Report 2011/426, 2011.
864. Masoumeh Safkhani, Nasour Bagheri, Somitra Sanadhya Kumar, and Majid Naderi. Security analysis of a PUF based RFID authentication protocol. Cryptology ePrint Archive, Report 2011/704, 2011.
865. Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. On the security of RFID anti cloning security protocol (ACSP). Cryptology ePrint Archive, Report 2011/563, 2011.
866. Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. On the designing of a tamper resistant prescription RFID access control system. *Journal Medical Systems*, 36(6):3995–4004, August 2012.
867. Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. On the traceability of tags in SUAP RFID authentication protocols. Cryptology ePrint Archive, Report 2012/334, 2012.
868. Masoumeh Safkhani, Nasour Bagheri, and Majid Naderi. Strengthening the security of EPC C-1 G-2 RFID standard. *Wireless Personal Communications*, pages 1–14, March 2013.

869. Masoumeh Safkhani, Nasour Bagheri, Majid Naderi, and Ali Mahani. On the security of Lo et al.'s ownership transfer protocol. Cryptology ePrint Archive, Report 2012/023, 2012.
870. Masoumeh Safkhani, Nasour Bagheri, Nasour Peris-Lopez, and Aikaterini Mitrokotsa. On the traceability of tags in SUAP RFID authentication protocols. In *IEEE International Conference on RFID-Technology and Applications – IEEE RFID TA 2012*, IEEE Press, Nice, France, November 2012. IEEE.
871. Masoumeh Safkhani, Nasour Bagheri, Nasour Peris-Lopez, Aikaterini Mitrokotsa, and Julio Cesar. Hernandez-Castro. Weaknesses in another Gen2-Based RFID authentication protocol. In *IEEE International Conference on RFID-Technology and Applications – IEEE RFID TA 2012*, IEEE Press, Nice, France, November 2012. IEEE.
872. Masoumeh Safkhani, Pedro Peris-Lopez, Nasour Badheri, Majid Naderi, and Julio Cesar Hernandez-Castro. On the security of tan et al. serverless RFID authentication and search protocols. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
873. Masoumeh Safkhani, Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, and Nasour Bagheri. Cryptanalysis of the cho et al. protocol: A hash-based RFID tag mutual authentication protocol. *Journal of Computational and Applied Mathematics*, October 2013.
874. Masoumeh Safkhani, Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Nasour Bagheri, and Majid Naderi. Cryptanalysis of cho *et al.*'s protocol, a hash-based mutual authentication protocol for RFID systems. Cryptology ePrint Archive, Report 2011/311, 2011.
875. Junichiro Saito and Sakurai Kouichi. Grouping Proof for RFID Tags. In *Conference on Advanced Information Networking and Applications – AINA*, volume 2, pages 621–624, Taiwan, March 2005. IEEE, IEEE Computer Society.
876. Junichiro Saito, Jae-Cheol Ryou, and Kouichi Sakurai. Enhancing Privacy of Universal Re-encryption Scheme for RFID Tags. In Laurence Jang, Minyi Guo, Guang Gao, and Niraj Jha, editors, *Embedded and Ubiquitous Computing – EUC'04*, volume 3207 of *Lecture Notes in Computer Science*, pages 879–890, Aizu-Wakamatsu City, Japan, August 2004. Springer.
877. Kazuya Saka, Min-Te Sun, Wei-Shinn Ku, Ten H. Lai, and Athanasios V. Vasilakos. Randomized skip lists-based private authentication for large-scale RFID systems. Technical Report TR12, The Ohio State University - Computer Science and Engineering, Columbus, Ohio, USA, May 2013.
878. Kazuo Sakiyama, Lejla Batina, Nele Mentens, Bart Preneel, and Ingrid Verbauwhede. Small-Footprint ALU for Public-Key Processors for Pervasive Security. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
879. Mastooreh Salajegheh, Shane Clark, Benjamin Ransford, Kevin Fu, and Ari Juels. CCCP: Secure Remote Storage for Computational RFIDs. In *Proceedings of the 18th USENIX Security Symposium – USENIX'09*, Montreal, Canada, August 2009. USENIX.
880. Raghav Sampangi and Srini Sampalli. RBS: Redundant bit security algorithm for RFID systems. In *IEEE Symposium on Computational Intelligence for Security and Defence Applications – CISDA 2012*, pages 1–8, Ottawa, Canada, July 2012.
881. Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka. Improving Efficiency of an 'On the Fly' Identification Scheme by Perfecting Zero-Knowledgeness. In Josef Pieprzyk, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA 2010*, volume 5985 of *Lecture Notes in Computer Science*, pages 284–301, San Francisco, California, USA, March 2010. Springer.
882. Sanjay Sarma, Stephen Weis, and Daniel Engels. RFID Systems and Security and Privacy Implications. In Burton Kaliski, Çetin Kaya ço, and Christof Paar, editors, *Cryptographic Hardware and Embedded Systems – CHES 2002*, volume 2523 of *Lecture Notes in Computer Science*, pages 454–469, Redwood Shores, California, USA, August 2002. Springer.
883. Sanjay Sarma, Stephen Weis, and Daniel Engels. Radio-Frequency Identification: Security Risks and Challenges. *Cryptobytes, RSA Laboratories*, 6(1):2–9, Spring 2003.
884. Olivier Savry, Florian Pebay-Peyroula, François Dehmas, Gérard Robert, and Jacques Reverdy. RFID Noisy Reader How to Prevent from Eavesdropping on the Communication? In Pascal Paillier and Ingrid Verbauwhede, editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 334–345, Vienna, Austria, September 2007. Springer.
885. Nitesh Saxena and Jonathan Voris. Still and Silent: Motion Detection for Enhanced RFID Security and Privacy without Changing the Usage Model. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 2–21, Istanbul, Turkey, June 2010. Springer.
886. Hwajeong Seo, Yeoncheol Lee, Hyunjin Kim, Taehwan Park, and Howon Kim. Binary and prime field multiplication for public key cryptography on embedded microprocessors. *Security and Communication Networks*, May 2013.

887. Youngjoon Seo. A Study on Scalable and Untraceable Authentication Protocol of RFID Tags. Master thesis, School of Engineering Information and Communications University, Daejeon, Korea, December 2007.
888. Youngjoon Seo and Kwangjo Kim. Scalable and Untraceable Authentication Protocol for RFID. In Xiaobo Zhou, Oleg Sokolsky, Lu Yan, Eun-Sun Jung, Zili Shao, Yi Mu, Dong Chun Lee, Daeyoung Kim, Young-Sik Jeong, and Cheng-Zhong Xu, editors, *International Workshop on Security in Ubiquitous Computing Systems – SecUbiq 2006*, volume 4097 of *Lecture Notes in Computer Science*, pages 252–261, Seoul, Korea, August 2006. Springer.
889. Muhammad Shahzad and Alex X. Liu. Every bit counts: fast and scalable RFID estimation. In Lili Qiu and Alex C. Snoeren, editors, *18th annual international conference on Mobile computing and networking – Mobicom '12*, pages 365–376, Istanbul, Turkey, August 2012. ACM New York, NY, USA.
890. Mohsen Shakiba, Mohammad Dakhilalian, and Hamid Mala. Cryptanalysis of mCrypton-64. *International Journal of Communication Systems*, 27(1), January 2014.
891. Shuai Shao, Guoai Xu, and Yanfei Liu. Efficient RFID authentication scheme with high security. In *Communication Software and Networks – ICCSN 2011*, pages 238–241, Xi'an, China, May 2011.
892. Wang Shao-Hui, Xiao Fu, Chen Dan-wei, and Wang Ru-chuan. Security analysis of lightweight authentication protocol from WISTP 2013. Cryptology ePrint Archive, Report 2013/411, 2013.
893. Wang Shaohui. Analysis and design of RFID tag ownership transfer protocol. In Liangzhong Jiang, editor, *International Conference on Informatics, Cybernetics, and Computer Engineering – ICCE 2011*, volume 110 of *Advances in Intelligent and Soft Computing*, pages 229–236, Melbourne, Australia, November 2011. Springer Berlin / Heidelberg.
894. Wang Shaohui. Analysis and design of RFID tag ownership transfer protocol. In Liangzhong Jiang, editor, *International Conference on Informatics, Cybernetics, and Computer Engineering – ICCE 2011*, volume 110 of *Advances in Intelligent and Soft Computing*, pages 229–236, Melbourne, Australia, November 2011. Springer Berlin / Heidelberg.
895. Wang Shaohui. Security flaws in two RFID lightweight authentication protocols. In Ming Ma, editor, *Communication Systems and Information Technology*, volume 100 of *Lecture Notes in Electrical Engineering*, pages 149–156. Springer Berlin Heidelberg, 2011.
896. Wang Shaohui and Wang Faxing. Security analysis of some RFID authentication protocols. In *2nd International Conference on e-Business and Information System Security – EBISS 2010*, pages 1–4, May 2010.
897. Wang Shaohui, Sujuan Liu, and Danwei Chen. Analysis and construction of efficient RFID authentication protocol with backward privacy. Cryptology ePrint Archive, Report 2012/391, 2012.
898. Wang Shaohui, Liu Sujuan, and Chen Danwei. Efficient passive full-disclosure attack on RFID light-weight authentication protocols LMAP++ and SUAP. *Telkomnika Indonesian Journal of Electrical Engineering*, 10(6), October 2012.
899. Wang Shaohui and Wei-wei Zhang. Passive attack on RFID LMAP++ authentication protocol. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *Proceedings of the 10th International Conference on Cryptology and Network Security – CANS 2011*, volume 7092, pages 185–193, Sanya, China, December 2011. Springer Berlin / Heidelberg.
900. Cai Shaoying, Yingjiu Li, Tieyan Li, and Robert H. Deng. Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions. In David A. Basin, Srdjan Capkun, and Wenke Lee, editors, *Proceedings of the 2nd ACM Conference on Wireless Network Security – WiSec'09*, pages 51–58, Zurich, Switzerland, March 2009. ACM, ACM Press.
901. Shah Sheetal. Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues, 2006.
902. Mouza Bani Shemaili, Chan Yeob Yeun, Khalid Mubarak, and Mohamed Jamal Zemerly. Security threats and challenges for RFID and WSN integration. *International Journal of RFID Security and Cryptography*, 1:9–15, March 2012.
903. Jian Shen, Wenying Zheng, Jin Wang, Zhihua Xia, and Zhangjie Fu. Study of the privacy models in RFID authentication protocols. *International Journal of Security and its Applications*, 7(6):345–354, December 2013.
904. Weiwei Shen, He Xu, Rui Sun, and Ruchuan Wang. Research on defense technology of relay attacks in RFID systems. In *International Conference on Computer Science and Intelligent Communication – CSIC 2015*, Zhengzhou, China, July 2015.
905. Bo Sheng, Chiu Chiang Tan, Qun Li, and Weizhen Mao. Finding popular categories for RFID tags. In *Proceedings of the 9th ACM international symposium on Mobile ad hoc networking and computing – MobiHoc '08*, pages 159–168, Hong Kong, China, May 2008. ACM, ACM Press.
906. Jie Shi, Yingjiu Li, Robert H. Deng, Wei He, and Eng Wah Lee. A secure platform for information sharing in EPCglobal network. *International Journal of RFID Security and Cryptography*, 2:107–118, December 2013.

907. Han Shuihua and Chao-Hsien Chu. Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 111–117, April 2008.
908. Pieter Siekerman and Maurits van der Schee. Security Evaluation of the disposable OV-chipkaart. Report, System and Network Engineering, University of Amsterdam, July 2007.
909. Dave Singelée and Bart Preneel. Distance bounding in noisy environments. In Frank Stajano, Catherine Meadows, Srdjan Čapkun, and Tyler Moore, editors, *Security and Privacy in Ad-hoc and Sensor Networks – ESAS 2007*, volume 4572 of *Lecture Notes in Computer Science*, pages 101–115, Cambridge, UK, July 2007. Springer-Verlag.
910. Mauw Sjouke and Selwyn Piramuthu. A PUF-based authentication protocol to address ticket-switching of RFID-tagged items. In *8th International Workshop on Security and Trust Management – STM 2012*, Pisa, Italy, September 2012.
911. Mohammad Reza Sohizadeh Abyaneh. On the Security of Non-Linear HB (NLHB) Protocol Against Passive Attack. Cryptology ePrint Archive, Report 2010/402, 2010.
912. Mohammad Reza Sohizadeh Abyaneh. Passive cryptanalysis of the UnConditionally secure authentication protocol for RFID systems. In Kyung-Hyune Rhee and DaeHun Nyang, editors, *International Conference on Information Security and Cryptology – ICISC 2010*, volume 6829 of *Lecture Notes in Computer Science*, pages 92–103, Seoul, Korea, December 2010. Springer.
913. Mohammad Reza Sohizadeh Abyaneh. Passive Cryptanalysis of Unconditionally Secure Authentication Protocol for RFID Systems. arXiv.org, Computer Science, Cryptography and Security, 2010.
914. Mohammad Reza Sohizadeh Abyaneh. Security Analysis of two Distance-Bounding Protocols. In *Workshop on RFID Security – RFIDSec'11*, Amherst, Massachusetts, USA, June 2011.
915. Agusti Solanas, Josep Domingo-Ferrer, Antoni Martínez-Ballesté, and Vanesa Daza. A Distributed Architecture for Scalable Private RFID Tag Identification. *Computer Networks, Elsevier*, 51(9), January 2007.
916. Boyeon Song. RFID Tag Ownership Transfer. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
917. Boyeon Song. Server Impersonation Attacks on RFID Protocols. In *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies – UBICOMM'08*, pages 50–55, Valencia, Spain, October 2008. IEEE, IEEE Computer Society.
918. Boyeon Song. *RFID Authentication Protocols using Symmetric Cryptography.* PhD thesis, Royal Holloway, Univeristy of London, Egham, Surrey, United Kingdom, December 2009.
919. Boyeon Song and Chris J. Mitchell. RFID Authentication Protocol for Low-cost Tags. In Virgil D. Gligor, Jean-Pierre Hubaux, and Radha Poovendran, editors, *Proceedings of the 1st ACM Conference on Wireless Network Security – WiSec'08*, pages 140–147, Alexandria, Virginia, USA, March–April 2008. ACM, ACM Press.
920. Boyeon Song and Chris J. Mitchell. Scalable RFID Authentication Protocol. In *3rd International Conference on Network ans System Security – NSS 2009*, pages 216–224, Gold Coast, Australia, October 2009. IEEE, IEEE Computer Society.
921. Boyeon Song and Chris J. Mitchell. Scalable RFID Security Protocols supporting Tag Ownership Transfer. *Computer Communication, Elsevier*, March 2010.
922. Raghuvir Songhela and Manik Lal Das. Wide-weak privacy preserving RFID mutual authentication protocol. Cryptology ePrint Archive, Report 2013/787, 2013.
923. Mate Soos. Analysing the Molva and Di Pietro Private RFID Authentication Scheme. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
924. Andrea Soppera and Trevor Burbridge. Wireless Identification – Privacy and Security. *BT Technology Journal*, 23(4):54–64, October 2005.
925. Andrea Soppera and Trevor Burbridge. Off by Default - RAT: RFID Acceptor Tag. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
926. Andrea Soppera, Trevor Burbridge, and Valentijn Broekhuizen. Trusted RFID Readers for Secure Multi-Party Services. EU RFID Forum, March 2007.
927. Sarah Spiekermann. Perceived Control: Scales for Privacy in Ubiquitous Computing Environments. In *Conference on User Modeling – UM'05*, Edinburgh, Scotland, July 2005.
928. Sarah Spiekermann and Oliver Berthold. Maintaining Privacy in RFID Enabled Environments – Proposal for a Disable-Model. In *Workshop on Security and Privacy, Conference on Pervasive Computing*, Vienna, Austria, April 2004.
929. Sarah Spiekermann and Sergei Evdokimov. Privacy Enhancing Technologies for RFID - A Critical Investigation of State of the Art Research. In *IEEE Privacy and Security.* IEEE, IEEE Computer Society, 2009.
930. Sarah Spiekermann and Holger Ziekow. RFID: A 7-point Plan to Ensure Privacy. In *European Conference on Information Systems – ECIS'05*, Regensburg, Germany, May 2005.

931. Luigi Sportiello. Weakening ePassports through bad implementations. In Jaap-Henk Hoepman and Ingrid Verbauwhede, editors, *Workshop on RFID Security – RFIDSec'12*, volume 7739 of *Lecture Notes in Computer Science*, pages 123–136, Nijmegen, Netherlands, July 2012. Springer.
932. Luigi Sportiello. ePassport: Side channel in the basic access control. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
933. Luigi Sportiello and Andrea Ciardulli. Long distance relay attack. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
934. Amandeep Singh Sran. RFID authentication scheme based on dynamic key generation. Master thesis, Dalhousie University, Halifax, Nova Scotia, Canada, December 2012.
935. Thorsten Staake, Frédéric Thiesse, and Elgar Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland, September 2004.
936. Thorsten Staake, Frédéric Thiesse, and Elgar Fleisch. Extending the EPC Network – The Potential of RFID in Anti-Counterfeiting. In Hisham Haddad, Lorie Liebrock, Andrea Omicini, and Roger Wainwright, editors, *Proceedings of the 2005 ACM Symposium on Applied Computing – SAC'05*, pages 1607–1612, Santa Fe, New Mexico, USA, March 2005. ACM, ACM Press.
937. Stefan Stadlober. An Evaluation of Security Threats and Countermeasures in Distributed RFID Infrastructures. Master thesis, Graz University of Technology, Graz, Austria, July 2005.
938. Chunhua Su, Yingjiu Li, and Robert H. Deng. RFID Mutual Authentication Protocols with Universally Composable Security. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 35–49, Wuxi, China, April 2011. IOS Press.
939. Bo Sun, Chung-Chih Li, and Yang Xiao. A lightweight secure solution for RFID. In *2006 IEEE Global Telecommunications Conference – GLOBECOM '06*, pages 1–5, December 2006.
940. Da-Zhi Sun, Zahra Ahmadian, Yue-Jiao Wang, Mahmoud Salmasizadeh, and Mohammad Reza Aref. Analysis and enhancement of desynchronization attack on an ultralightweight RFID authentication protoco. Cryptology ePrint Archive, Report 2015/037, 2015.
941. Da-Zhi Sun and Zhen-Fu Cao. On the privacy of khan et al.'s dynamic ID-based remote authentication scheme with user anonymity. *Cryptologia*, 37(4):345–355, October 2013.
942. Da-Zhi Sun and Ji-Dong Zhong. A hash-based rfid security protocol for strong privacy protection. *IEEE Transactions on Consumer Electronics*, 58(4):1246 – 1252, November 2012.
943. Hung-Min Sun, Shuai-Min Chen, and King-Hang Wang. Cryptanalysis on the RFID ACTION protocol. In *International Conference on Security and Management – SAM 2011*, Las Vegas, Nevada, USA, July 2011.
944. Hung-Min Sun and Wei-Chih Ting. A Gen2-based RFID Authentication Protocol for Security and Privacy. *IEEE Transactions on Mobile Computing*, 8(8):1052–1062, 2009.
945. Saravanan Sundaresan and Robin Doss. Secure yoking proof protocol for RFID systems. In *International Conference on Advances in Computing, Communications and Informatics – ICACCI 2014*, pages 1585–1591, New Delhi, India, September 2014. IEEE.
946. Saravanan Sundaresan, Robin Doss, Selwyn Piramuthu, and Wanlei Zhou. Secure tag search in RFID systems using mobile readers. *IEEE Transactions on Dependable and Secure Computing*, May 2014.
947. Saravanan Sundaresan, Robin Doss, and Wanlei Zhou. Offline grouping proof protocol for rfid systems. In *9th International Conference on Wireless and Mobile Computing, Networking and Communications – WiMob 2013*, Lyon, France, October 2013. IEEE.
948. Saravanan Sundaresan, Robin Doss, and Wanlei Zhou. RFID in healthcare – current trends and the future. *Mobile Health*, 5:839–870, February 2015.
949. Irfan Syamsuddin, Tharam Dillon, Elizabeth Chang, and Song Han. A survey of RFID authentication protocols based on hash-chain method. In *Convergence and Hybrid Information Technology – ICCIT'08*, volume 2, pages 559–564. IEEE, 2008.
950. Deepak Tagra, Musfiq Rahman, and Srinivas Sampalli. Technique for Preventing DoS Attacks on RFID Systems. In *18th International Conference on Software Telecommunications and Computer Networks – SoftCOM'10*, Bol, Island of Brac, Croatia, September 2010. IEEE, IEEE Computer Society.
951. Chiu C. Tan, Bo Sheng, and Qun Li. Serverless Search and Authentication Protocols for RFID. In *International Conference on Pervasive Computing and Communications – PerCom 2007*, pages 3–12, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society.
952. Chiu C. Tan and Jie Wu. *Security in RFID Networks and Communications*, chapter 10. Springer, 2010.
953. Wouter Teepe. Making the Best of Mifare Classic, October 2008. www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf.
954. Pierre-Henri Thevenon and Olivier Savry. *Implementation of a Countermeasure to Relay Attacks for Contactless HF Systems*. InTech, June 2013.

955. Yuan Tian, Biao Song, and Eui-nam Huh. A novel threat evaluation method for privacy-aware system in RFID. In *International Journal of Ad Hoc and Ubiquitous Computing*, volume 8, pages 230–240, 2011.
956. Yun Tian, Gongliang Chen, and Jianhua Li. A new ultralightweight RFID authentication protocol with permutation. *IEEE Communications Letters*, 16(5):702–705, May 2012.
957. Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn, and Srdjan Capkun. UWB rapid-bit-exchange system for distance bounding. In *Proceedings of the 8th ACM conference on Security and privacy in wireless and mobile networks – WiSec'15*, New York, USA, June 2015. ACM.
958. Batbold Toiruul, KyungOh Lee, and JinMook Kim. SLAP - A Secure but Light Authentication Protocol for RFID Based on Modular Exponentiation. In *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies – UBICOMM '07*, pages 29–34, Papeete, French Polynesia (Tahiti), November 2007. IEEE, IEEE Computer Society.
959. Wiem Tounsi, Nora Cuppens-Boulahia, Joaquin Garcia-Alfaro, Yannick Chevalier, and Frédéric Cuppens. KEDGEN2: A key establishment and derivation protocol for EPC gen2 RFID systems. *Journal of Network and Computer Applications*, (0), June 2013.
960. K. Toyoda and I. Sasase. Secret sharing based unidirectional key distribution with dummy tags in Gen2v2 RFID-enabled supply chains. In *IEEE International Conference on RFID – IEEE RFID 2015*, pages 63–69, San Diego, California, USA, April 2015. IEEE, IEEE Computer Society.
961. Duy-Thinh Tran and Sung Je Hong. RFID anti-counterfeiting for retailing systems. *Journal of Applied Mathematics and Physics*, 3:1–9, January 2015.
962. Denis Trcek and Andrej Brodnik. Hard and soft security provisioning for computationally weak pervasive computing systems in e-Health. *Wireless Communications for e-Health Applications*, pages 2–9, August 2013.
963. Somanath Tripathy and Sukumar Nandi. Cellular Automata-based Authentication for Low-cost RFID Systems. *International Journal of Communication Networks and Distributed Systems*, 3(3):199–216, 2009.
964. Rolando Trujillo-Rasua. *Privacy in RFID and mobile objects.* PhD thesis, Universitat Rovira i Virgili, Tarragona, Spain, June 2012.
965. Rolando Trujillo Rasua, Benjamin Martin, and Gildas Avoine. The Poulidor Distance-Bounding Protocol. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 239–257, Istanbul, Turkey, June 2010. Springer.
966. Rolando Trujillo Rasua, Benjamin Martin, and Gildas Avoine. Distance-bounding facing both mafia and distance frauds. *IEEE Transactions on Wireless Communications*, 13(10):5690–5698, October 2014.
967. Rolando Trujillo-Rasua, Agusti Solanas, Pablo A. Prez-Martnez, and Josep Domingo-Ferrer. Predictive protocol for the scalable identification of RFID tags through collaborative readers. *Computers in Industry*, 2012.
968. Denis Trček and Pekka Jäppinen. *Non-deterministic Lightweight Protocols for Security and Privacy in RFID Environments.* Auerbach Publication, 2009.
969. Denis Trček and Pekka Jäppinen. *Non-deterministic Lightweight Protocols for Security and Privacy in RFID Environments.* Auerbach Publication, 2009.
970. Denis Trček and Damjan Kovač. Formal Appartus for Measurement of Lightweight Protocols. *Computer Standard & Interface, Elsevier*, In Press, Corrected Proof, 2008.
971. Gene Tsudik. YA-TRAP: Yet Another Trivial RFID Authentication Protocol. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, pages 640–643, Pisa, Italy, March 2006. IEEE, IEEE Computer Society.
972. Gene Tsudik. A Family of Dunces: Trivial RFID Identification and Authentication Protocols. Cryptology ePrint Archive, Report 2006/015, 2007.
973. Gene Tsudik. A Family of Dunces: Trivial RFID Identification and Authentication Protocols. In Nikita Borisov and Philippe Golle, editors, *Workshop on Privacy Enhancing Technologies – PET 2007*, volume 4776 of *Lecture Notes in Computer Science*, pages 45–61, Ottawa, Canada,, June 2007. Springer.
974. Yu-Ju Tu and Selwyn Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
975. Cornel Turcu, editor. *Current Trends and Challenges in RFID.*
976. Pim Tuyls and Lejla Batina. RFID-Tags for Anti-Counterfeiting. In David Pointcheval, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA 2006*, volume 3860 of *Lecture Notes in Computer Science*, pages 115–131, San Jose, California, USA, February 2006. Springer.
977. Duerholz Ulrich, Fischlin Marc, Kasper Michael, and Onete Cristina. A formal approach to distance-bounding rfid protocols. Cryptology ePrint Archive, Report 2011/321, 2011.
978. Pascal Urien, Hervé Chabanne, Cyrille Pépin, Mathieu Bouet, Daniel De Oliveira Cunha, Vincent Guyot, Guy Pujolle, Pierre Paradinas, Eric Gressier-Soudan, and Jean-Ferdinand Susini. HIP-based RFID Networking Architecture. In *IFIP International Conference on Wireless and Optical Communications Networks – WOCN'07*, pages 1–5, Singapore, Republic of Singapore, July 2007. IEEE, IEEE Computer Society.

979. Pascal Urien, Simon Elrharbi, Hervé Chabanne, Thomas Icart, Cyrille Pépin, Mathieu Bouet, Daniel De Oliveira Cunha, Vincent Guyot, Guy Pujolle, Eric Gressier-Soudan, and Jean-Ferdinand Susini. HIP tags, a privacy architecture for networking in the Internet of Things. In *Networking and Electronic Commerce Research Conference – NAEC 2008*, Lake Garda, Italy, September 2008.
980. Pascal Urien, Dorice Nyami, Simon Elrharbi, Hervé Chabanne, Thomas Icart, Cyrille Pépin, Mathieu Bouet, Daniel De Oliveira Cunha, Vincent Guyot, Guy Pujolle, Eric Gressier-Soudan, and Jean-Ferdinand Susini. HIP Tags Privacy Architecture. In *Proceedings of the 3rd International Conference on Systems and Networks Communications – ICSNC'08*, pages 179–184, Sliema, Malta, October 2008. IEEE, IEEE Computer Society.
981. Pascal Uriena and Selwyn Piramuthu. Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. *Decision Support Systems*, October 2013.
982. Pascal Uriena and Selwyn Piramuthu. Elliptic curve-based RFID/NFC authentication with temperature sensor input for relay attacks. *Decision Support Systems*, 59(0):28–36, March 2014.
983. Jaanus Uudmae, Harshitha Sunkara, Dale R. Thompson, Sean Bruce, and Jayamadhuri Penumarthi. MIXNET for Radio Frequency Identification. In *2007 IEEE Region 5 Technical Conference*, pages 382–385, Fayetteville, Arkansas, USA, April 2007. IEEE, IEEE Computer Society.
984. Ehsan Vahedi. *Security, Privacy and Efficiency in RFID Systems.* PhD thesis, The University of British Columbia, Vancouver, Canada, September 2013.
985. Ehsan Vahedi, Vahid Shah-Mansouri, Vincent W.S. Wong, Ian F. Blake, and Rabab K. Ward. Probabilistic Analysis of Blocking Attack in RFID Systems. *IEEE Transactions on Information Forensics and Security*, 2011.
986. Ehsan Vahedi, Rabab Ward, and Ian Blake. Security Analysis and Complexity Comparison of Some Recent Lightweight RFID Protocols. *Computational Intelligence in Security for Information Systems*, 6694:92–99, 2011.
987. István Vajda and Levente Buttyán. Lightweight Authentication Protocols for Low-Cost RFID Tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, Seattle, Washington, USA, October 2003.
988. Gauthier Van Damme, Karel Wouters, and Bart Preneel. Practical Experiences with NFC Security on mobile Phones. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
989. Ton van Deursen, Sjouke Mauw, and Saša Radomirović. Untraceability of RFID Protocols. In Jose Antonio Onieva, Damien Sauveron, Serge Chaumette, Dieter Gollmann, and Constantinos Markantonakis, editors, *Workshop on Information Security Theory and Practice – WISTP'08*, volume 5019 of *Lecture Notes in Computer Science*, pages 1–15, Sevilla, Spain, May 2008. Springer.
990. Ton van Deursen, Sjouke Mauw, Saša Radomirović, and Pim Vullers. Secure Ownership and Ownership Transfer in RFID Systems. In Michael Backes and Peng Ning, editors, *14th European Symposium on Research in Computer Security – ESORICS 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 637–654, Saint-Malo, France, September 2009. Springer.
991. Ton van Deursen and Saša Radomirović. Attacks on RFID Protocols. Cryptology ePrint Archive, Report 2008/310, 2008.
992. Ton van Deursen and Saša Radomirović. Algebraic Attacks on RFID Protocols. In Olivier Markowitch, Angelos Bilas, Jaap-Henk Hoepman, Chris J. Mitchell, and Jean-Jacques Quisquater, editors, *Workshop on Information Security Theory and Practice – WISTP'09*, volume 5746 of *Lecture Notes in Computer Science*, pages 38–51, Brussels, Belgium, September 2009. Springer.
993. Ton van Deursen and Saša Radomirović. EC-RAC: Enriching a Capacious RFID Attack Collection. In S.B. Ors Yalcin, editor, *Workshop on RFID Security – RFIDSec'10*, volume 6370 of *Lecture Notes in Computer Science*, pages 75–90, Istanbul, Turkey, June 2010. Springer.
994. Ton Frederik Petrus Van Deursen. *Security of RFID protocols.* PhD thesis, Universit du Luxembourg, Luxembourg, September 2011.
995. Tri Van Le, Mike Burmester, and Breno de Medeiros. Universally Composable and Forward-secure RFID Authentication and Authenticated Key Exchange. In Feng Bao and Steven Miller, editors, *ACM Symposium on Information, Computer and Communications Security – ASIACCS 2007*, pages 242–252, Singapore, Republic of Singapore, March 2007. ACM, ACM Press.
996. Tristan Crispijn van Stijn. Analyzing RFID Authentication Protocols. Master's thesis, Technische Universiteit Eindhoven, 2007.
997. Nimish Vartak. Protecting the Privacy of RFID tags. Master thesis, University of Maryland, College Park, Maryland, USA, May 2006.
998. Serge Vaudenay. RFID Privacy Based on Public-Key Cryptography (Abstract). In Min Surp Rhee and Byoungcheon Lee, editors, *International Conference on Information Security and Cryptology – ICISC 2006*,

volume 4296 of *Lecture Notes in Computer Science*, pages 1–6, Busan, Korea, November–December 2006. Springer.

999. Serge Vaudenay. On Privacy Models for RFID. In Kaoru Kurosawa, editor, *Advances in Cryptology – Asiacrypt 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 68–87, Kuching, Malaysia, December 2007. Springer.
1000. Serge Vaudenay. Private and secure public-key distance bounding – application to NFC payment. In *Financial Cryptography and Data Security 2015*, Puerto Rico, January 2015.
1001. Serge Vaudenay and Martin Vuagnoux. About Machine-Readable Travel Documents. In *ICS'07*, Lecture Notes in Computer Science. Springer, 2007.
1002. Roel Verdult. Security analysis of RFID tags. Master's thesis, Radboud University Nijmegen, 2008.
1003. Roel Verdult, Flavio Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with Hitag2. In *21th USENIX Security Symposium – USENIX'12*, pages 237–252, Bellevue, WA, USA, August 2012. USENIX, USENIX Association.
1004. Thijs Veugen and Michael Beye. Improved anonymity for key-trees. In *Workshop on RFID Security – RFIDSec'12*, Nijmegen, Netherlands, June 2012.
1005. Markus Vogt, Axel Poschmann, and Christof Paar. Cryptography is Feasible on 4-Bit Microcontrollers - A Proof of Concept. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
1006. Jonathan Voris and Nitesh Saxena. We Can Remember It for You Wholesale: Implications of Data Remanence on the Use of RAM for True Random Number Generation on RFID Tags. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium, July 2009.
1007. Andreas Wallstabe and Hartmut Pohl. Implementing high-level Counterfeit Security using RFID and PKI. In *3rd European Workshop on RFID Systems and Technologies – RFID SysTech 2007*, Duisburg, Germany, June 2007. VDE Verlag.
1008. Bin Wang and Maode Ma. An untraceable and server-independent RFID authentication scheme. In *International Conference on Information, Communications and Signal Processing – ICICS 2011*, pages 1–5, December 2011.
1009. Junyu Wang, Christian Floerkemeier, and Sanjay E. Sarma. Session-based security enhancement of RFID systems for emerging open-loop applications. *Personal and Ubiquitous Computing*, August 2014.
1010. Shao-hui Wang and Wei-wei Zhang. Passive attack on RFID LMAP++ authentication protocol. In Dongdai Lin, Gene Tsudik, and Xiaoyun Wang, editors, *Proceedings of the 10th International Conference on Cryptology and Network Security – CANS 2011*, volume 7092, pages 185–193, Sanya, China, December 2011. Springer Berlin / Heidelberg.
1011. Shaohui Wang, Sujuan Liu, and Danwei Chen. Analysis and construction of efficient RFID authentication protocol with backward privacy. Cryptology ePrint Archive, Report 2012/391, 2012.
1012. Shaohui Wang, Sujuan Liu, and Danwei Chen. Security analysis and improvement on two RFID authentication protocols. *Wireless Personal Communications*, November 2014.
1013. Weijia Wang, Yong Li, Lei Hu, and Li Lu. Storage-awareness: RFID private authentication based on sparse tree. *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2007*, pages 61–66, July 2007.
1014. Zhao Wang, Xu Zhigang, Wei Xin, and Zhong Chen. Implementation and analysis of a practical NFC relay attack example. In *Proceedings of the 2nd International Conference on Instrumentation, Measurement, Computer, Communication and Control – IMCCC 2012*, pages 143–146, Harbin, China, December 2012.
1015. Nisha R. Wartha and Vaishali Londhe. Context-aware approach for enhancing security and privacy of RFID. *International Journal Of Engineering And Computer Science*, 4(1):10078–10088, January 2015.
1016. Michael Weiner, Salvador Manich, and Georg Sigl. A low area probing detector for power efficient RFID security ICs. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
1017. Michael Weiner, Maurice Massar, Erik Tews, Dennis Giese, and Wolfgang Wieser. Security analysis of a widely deployed locking system. In *Conference on Computer and Communications Security – ACM CCS'13*, pages 929–940, Berlin, November 2013. Lecture Notes in Computer Science, Springer Berlin Heidelberg.
1018. Stephen Weis. Security and Privacy in Radio-Frequency Identification Devices. Master thesis, Massachusetts Institute of Technology (MIT), MIT, Massachusetts, USA, May 2003.
1019. Stephen Weis. Security Parallels Between People and Pervasive Devices. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 105–109, Kauai Island, Hawaii, USA, March 2005. IEEE, IEEE Computer Society.
1020. Stephen Weis. *New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness Testing*. PhD thesis, MIT, Cambridge, Massachusetts, USA, May 2006.

1021. Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Dieter Hutter, Günter Müller, Werner Stephan, and Markus Ullmann, editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469, Boppard, Germany, March 2003. Springer.
1022. Michael Weiss. Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment. Master thesis, Technischen Universitat Munchen, Munich, Germany, May 2010.
1023. Erich Wenger, Thomas Korak, and Mario Kirschbaum. Analyzing side-channel leakage of RFID-suitable lightweight ECC hardware. In *Workshop on RFID Security – RFIDSec'13*, Graz, Austria, July 2013.
1024. Pieter Westein and Wouter van Dullink. Relay attacks for RFID access controls. Technical report, The National Cyber Security Centre (NCSC), The Hague, Netherlands, 2013.
1025. Jos Wetzels. Broken keys to the kingdom security and privacy aspects of RFID-based car keys. arXiv.org, Computer Science, Cryptography and Security, 2014.
1026. Johannes Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
1027. Kirk Wong, Patrick Hui, and Allan Chan. Cryptography and Authentication on RFID Passive Tags for Apparel Products. *Computers in Industry, Elsevier*, May 2006.
1028. Jiang Wu and Douglas R. Stinson. A Highly Scalable RFID Authentication Protocol. In Colin Boyd and Juan Manuel Gonzalez Nieto, editors, *Proceedings of the 14th Austrialasian Conference on Information Security and Privacy – ACISP'09*, volume 5594 of *Lecture Notes in Computer Science*, pages 360–376, Brisbane, Australia, July 2009. Springer.
1029. Jiang Wu and Douglas R. Stinson. How to Improve Security and Reduce Hardware Demands of the WIPR RFID Protocol. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
1030. Wei Xie, Lei Xie, Chen Zhang, Qiang Wang, Jian Xu, Quan Zhang, and Chaojing Tang. RFID seeking: Finding a lost tag rather than only detecting its missing. *Journal of Network and Computer Applications*, January 2014.
1031. Wei Xie, Chen Zhang, Quan Zhang, and Chaojing Tang. RFID authentication against an unsecure backend server. arXiv.org, Computer Science, Cryptography and Security, 2013.
1032. Wei Xin, Cong Tang, Hu Xiong, Yonggang Wang, Huiping Sun, Zhi Guan, and Zhong Chen. MEED: A Memory-efficient Distance Bounding Protocol with Error Detection. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 129–143, Wuxi, China, April 2011. IOS Press.
1033. Wei Xin, Tao Yang, Cong Tang, Jianbin Hu, and Zhong Chen. A distance bounding protocol using error state and punishment. In *Proceedings of the 1st International Conference on Instrumentation, Measurement, Computer, Communication and Control – IMCCC 2011*, volume 0, pages 436–440, Beijing, China, October 2011.
1034. Yang Xing-Chun, Xu Chun-Xiang, Mou Jian-Ping, and Li Jian-Ping. An improved RFID tag ownership transfer scheme. In *10th International Computer Conference on Wavelet Active Media Technology and Information Processing – ICCWAMTIP 2013*, pages 356–361, Chengdu, China, December 2013.
1035. Youjun Xu, Jialiang He, Jian Wang, and Dongxing Wang. Enhance patient medication safety with a RFID-based authentication scheme. *International Journal of u- and e-Service, Science and Technology*, 7(4):85–94, 2014.
1036. Akira Yamamoto, Shigeya Suzuki, Hisakazu Hada, Jin Mitsugi, Fumio Teraoka, and Osamu Nakamura. A Tamper Detection Method for RFID Tag Data. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 51–57, April 2008.
1037. Qiang Yan, Yingjiu Li, and Robert H. Deng. Anti-tracking in rfid discovery service for dynamic supply chain systems. *International Journal of RFID Security and Cryptography*, 1:25–35, March 2012.
1038. Anjia Yang, Kaitai Liang, Yunhui Zhuang, Duncan S. Wong, and Xiaohua Jia. A new unpredictability-based RFID forward privacy model and a provably secure construction. *Security and Communication Networks*, February 2015.
1039. Anjia Yang, Yunhui Zhuang, and Duncan S. Wong. An efficient single-slow-phase mutually authenticated RFID distance bounding protocol with tag privacy. In TatWing Chim and TszHon Yuen, editors, *International Conference on Information and Communications Security – ICICS'12*, volume 7618 of *Lecture Notes in Computer Science*, pages 285–292, Hong Kong, China, October 2012. Springer Berlin Heidelberg.
1040. Fan Yang, Fengli Zhang, Jiahao Wang, Zhiguang Qin, and Xiaolu Yuan. Distance-bounding trust protocol in anonymous radio-frequency identification systems. *Concurrency and Computation: Practice and Experience*, June 2015.

1041. Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim. Mutual Authentication Protocol for Low-Cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
1042. Ming-Hour Yang and Jia-Ning Luo. Fast anti-noise RFID-aided medical care system. *International Journal of Distributed Sensor Networks*, October 2015.
1043. Qingsong Yao, Jinsong Han, Yong Qi, Lei Yang, and Yunhao Liu. Privacy leakage in access mode: Revisiting private RFID authentication protocols. In *International Conference on Parallel Processing – ICPP 2011*, pages 713–721, Taipei City, China, September 2011.
1044. Qingsong Yao, Yong Qi, Jinsong Han, Jizhong Zhao, Xiang-Yang Li, and Yunhao Liu. Randomizing RFID Private Authentication. In *International Conference on Pervasive Computing and Communications – PerCom 2009*, pages 1–10, Galveston, Texas, USA, March 2009. IEEE, IEEE Computer Society.
1045. Yu Yao, Jiawei Huang, Sudhanshu Khanna, Abhi Shelat, Benton Highsmith Calhoun, John Lach, and David Evans. A Sub-0.5V Lattice-Based Public-Key Encryption Scheme for RFID Platforms in 130nm CMOS. In *Workshop on RFID Security – RFIDSec Asia'11*, volume 6 of *Cryptology and Information Security*, pages 96–113, Wuxi, China, April 2011. IOS Press.
1046. Xin Ye, Cong Chen, and Thomas Eisenbarth. Non-linear collision analysis. In *Workshop on RFID Security – RFIDSec'14*, Oxford, UK, July 2014.
1047. Kuo-Hui Yeh, Naiwei Lo, and Enrico Winata. An Efficient Ultralightweight Authentication Protocol for RFID Systems. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
1048. Kuo-Hui Yeh and N.W. Lo. Improvement of Two Lightweight RFID Authentication Protocols. *Information Assurance and Security Letters – IASL 2010*, 1:6–11, 2010.
1049. Chih-Ta Yen, Ming-Huang Guo, Nai-Wei Lo, and Der-Jiunn Deng. Authentication with low-cost rfid tags in mobile networks. *Security and Communication Networks*, 6(2), January 2013.
1050. Sang-Soo Yeo and Sung-Kwon Kim. Scalable and Flexible Privacy Protection Scheme for RFID Systems. In Refik Molva, Gene Tsudik, and Dirk Westhoff, editors, *European Workshop on Security and Privacy in Ad hoc and Sensor Networks – ESAS'05*, volume 3813 of *Lecture Notes in Computer Science*, pages 153–163, Visegrad, Hungary, July 2005. Springer.
1051. Chi-En Yin, Gang Qu, and Qiang Zhou. Design and implementation of a group-based ro puf. In *Design, Automation Test in Europe Conference Exhibition – DATE*, pages 416 – 421, Grenoble, France, March 2013.
1052. Xinchun Yin and Wang Li. LP0: A RFID authentication protocol for low-cost tags without back-end database. In *International Conference on Computer Distributed Control and Intelligent Environmental Monitoring – CDCIEM 2012*, volume 0, pages 393–396, Los Alamitos, CA, USA, 2012. IEEE Computer Society.
1053. Bongno Yoon. HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System. In *IEEE International Conference on RFID – IEEE RFID 2009*, Orlando, Florida, USA, April 2009. IEEE, IEEE Computer Society.
1054. Oren Yossef. *Secure Hardware Physical Attacks and Countermeasures*. PhD thesis, Tel Aviv University, Tel Aviv, Israel, May 2013.
1055. Taek-Young Youn and Dowon Hong. Authenticated distance bounding protocol with improved FAR: Beyond the minimal bound of FAR. *IEICE Transactions on Communications*, 97B(5):930–935, May 2014.
1056. Yawer Yousuf and Vidyasagar Potdar. A Survey of RFID Authentication Protocols. *22nd International Conference on Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008*, pages 1346–1350, March 2008.
1057. Pengyuan Yu, Patrick Schaumont, and Dong Ha. Securing RFID with Ultra-Wideband Modulation. In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria, July 2006. Ecrypt.
1058. Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini. New Privacy Results on Synchronized RFID Authentication Protocols against Tag Tracing. In Michael Backes and Peng Ning, editors, *14th European Symposium on Research in Computer Security – ESORICS 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 321–336, Saint-Malo, France, September 2009. Springer.
1059. Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini. Practical RFID Ownership Transfer Scheme. *Journal of Computer Security - Special Issue on RFID System Security*, 2010.
1060. Ching Yu Ng, Willy Susilo, Yi Mu, and Rei Safavi-Naini. Practical RFID Ownership Transfer Scheme. In *Workshop on RFID Security – RFIDSec Asia'10*, volume 4 of *Cryptology and Information Security*, Singapore, Republic of Singapore, February 2010. IOS Press.
1061. Zheng Yuanqing and Li Mo. Fast tag searching protocol for large-scale RFID systems. In *Proceedings of the 19th IEEE International Conference on Network Protocols – ICNP 2011*, pages 363–372, Vancouver, Canada, October 2011.

1062. Dae Hyun Yum, Jin Seok Kim, Sung Je Hong, and Pil Joong Lee. Distance Bounding Protocol for Mutual Authentication. *IEEE Transactions on Wireless Communications*, pages 592–601, 2011.
1063. Dae Hyun Yum, Jin Seok Kim, Sung Je Hong, and Pil Joong Lee. Distance bounding protocol with adjustable false acceptance rate. *IEEE Commuication Letters*, 15(4):434–436, April 2011.
1064. Dae Hyun Yum, Jin Seok Kim, Je Hong Sung, and Pil Joong Lee. Probabilistic Analysis of Blocking Attack in RFID Systems. *IEEE Communications Letters*, 15(4):434–436, 2011.
1065. Jeddi Zahra, Amini Esmaeil, and Bayoumi Magdy. A novel authenticated encryption algorithm for RFID systems. In Jos Silva Matos and Francesco Leporati, editors, *16th Euromicro Conference on Digital System Design – DSD 2013*, pages 658–661, Santander, Cantabria, Spain, September 2013.
1066. Davide Zanetti, Boris Danev, and Srdjan Čapkun. Physical-layer Identification of UHF RFID Tags. In *Proceedings of the 16th ACM Conference on Mobile Computing and Networking – MobiCom'10*, pages 353–364, Chicago, Illinois, USA, September 2010. ACM, ACM Press.
1067. Davide Zanetti, Leo Fellmann, and Srdjan Čapkun. Privacy-preserving Clone Detection for RFID-enabled Supply Chains. In *IEEE International Conference on RFID – IEEE RFID 2010*, pages 37–44, Orlando, Florida, USA, April 2010. IEEE, IEEE Computer Society.
1068. Azam Zavvari, Masoud Shakiba, Mohammad Tariqul Islam, Elankovan Sundararajan, and Mandeep Jit Singh. Computational cost analysis on securing RFID protocols conforming to EPC class-1 generation-2 standard. In *International Conference on Electrical Engineering and Informatics – ICEEI 2013*, Malaysia, June 2013.
1069. Ashraf Masood Zeeshan Bilal and Firdous Kausar. Security Analysis of Ultra-lightweight Cryptographic Protocol for Low-cost RFID Tags: Gossamer Protocol. In *International Conference on Network-Based Information Systems – NBIS'09*, pages 260–267, Indianapolis, Indiana, USA, August 2009. IEEE, IEEE Computer Society.
1070. Jia Zhai, Chang Mok-Park, and Gi-Nam Wang. Hash-Based RFID Security Protocol Using Randomly Key-Changed Identification Procedure. In Marina L. Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Kenneth Tan, David Taniar, Antonio Lagan, Youngsong Mun, and Hyunseung Choo, editors, *International Conference on Computational Science and its Applications – ICCSA 2006*, volume 3983 of *Lecture Notes in Computer Science*, pages 296–305, Glasgow, Scotland, May 2006. Springer.
1071. Li Zhai and ChuanKun Wu. An efficient RFID distance bounding protocol. *Advances in Intelligent Systems and Computing*, 369:367–376, May 2015.
1072. Shiyong Zhang, Gongliang Chen, Yongkai Zhou, and Jianhua Li. Enhanced-bivium algorithm for RFID system. *Mathematical Problems in Engineering*, July 2015.
1073. Xiaolan Zhang and Brian King. Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting. In Jianying Zhou, Javier Lopez, Robert Deng, and Feng Bao, editors, *Information Security Conference – ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 474–481, Singapore, Republic of Singapore, September 2005. Springer.
1074. Xiaolan Zhang and Brian King. Modeling RFID Security. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Conference on Information Security and Cryptology – ISC 2005*, volume 3822 of *Lecture Notes in Computer Science*, pages 75–90, Beijing, China, December 2005. Springer.
1075. Zezhong Zhang and Qingqing Qi. An efficient RFID authentication protocol to enhance patient medication safety using elliptic curve cryptography. *Journal of Medical Systems*, April 2014.
1076. Zhihua Zhang, Huanwen Wang, and Yanghua Gao. C2MP: Chebyshev chaotic map-based authentication protocol for RFID applications. *Personal and Ubiquitous Computing*, September 2015.
1077. Zhenguo Zhao. A secure RFID authentication protocol for healthcare environments using elliptic curve cryptosystem. *Journal of Medical Systems*, April 2014.
1078. Jingxian Zhou, Yajian Zhou, Feng Xiao, and Xinxin Niu. Mutual authentication protocol for mobile RFID systems. *Journal of Computational Information Systems*, 8(8):3261–3268, April 2012.
1079. Wei Zhou, Eun Jung Yoon, and Selwyn Piramuthu. Hierarchical RFID tag ownership and transfer in supply chains. In Michael J. Shaw, Dongsong Zhang, Wei T. Yue, Wil Aalst, John Mylopoulos, Michael Rosemann, and Clemens Szyperski, editors, *10th Workshop on E-Business – WEB 2011*, volume 108 of *Lecture Notes in Business Information Processing*, pages 390–398, Shanghai, China, December 2011. Springer Berlin Heidelberg.
1080. Wei Zhou, Eun Jung Yoon, and Selwyn Piramuthu. Varying levels of RFID tag ownership in supply chains. In Robert Meersman, Tharam Dillon, and Pilar Herrero, editors, *On the Move to Meaningful Internet Systems – OTM 2011*, pages 228–235, Crete, Greece, October 2011. Springer Berlin / Heidelberg.
1081. Wei Zhou, Eun Jung Yoon, and Selwyn Piramuthu. Simultaneous multi-level RFID tag ownership & transfer in health care environments. *Decision Support Systems*, May 2012.
1082. Huafei Zhu and Feng Bao. Aggregating Symmetric/Asymmetric Attestations. *IEEE International Conference on RFID – IEEE RFID 2008*, pages 105–110, April 2008.

1083. Xu Zhuang, Zhi-Hui Wang, Chin-Chen Chang, and Yan Zhu. Security analysis of a new ultra-lightweight RFID protocol and its improvement. *Journal of Information Hiding and Multimedia Signal Processing*, 4(3), July 2013.
1084. Xu Zhuang, Yan Zhun, and Chin-Chen Chang. A new ultralightweight RFID protocol for low-cost tags: R^2AP. *Wireless Personal Communications*, July 2014.
1085. Yanjun Zuo. RFID Survivability Quantification and Attack Modeling (short paper). In Susanne Wetzel, Cristina Nita-Rotaru, and Frank Stajano, editors, *Proceedings of the 3rd ACM Conference on Wireless Network Security – WiSec'10*, pages 13–18, Hoboken, New Jersey, USA, March 2010. ACM, ACM Press.