

Bibliography on Security and Privacy in RFID Systems

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

Version March 3, 2010

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. Arjun Agarwal and Mala Mitra. RFID: Promises and Problems, April 2006.
2. Manfred Aigner and Martin Feldhofer. Secure Symmetric Authentication for RFID Tags. In *Telecommunication and Mobile Computing – TCMC 2005*, Graz, Austria, March 2005.
3. 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.
4. 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*, volume 4817 of *Lecture Notes in Computer Science*, pages 102–115, Seoul, Korea, November 2007. Springer-Verlag.
5. 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 *Cryptography and Information Security Series*, Singapore, Republic of Singapore, February 2010. IOS Press.
6. Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. Untraceable RFID Tags via Insubvertible Encryption. In *Conference on Computer and Communications Security – CCS'05*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
7. Ali Atici, Lejla Batina, Benedikt Gierlich, and Ingrid Verbauwhede. Power Analysis on NTRU Implementations for RFIDs: First Results. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
8. 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.
9. 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.
10. Gildas Avoine. *Cryptography in Radio Frequency Identification and Fair Exchange Protocols*. PhD thesis, EPFL, Lausanne, Switzerland, December 2005.
11. 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.
12. 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-Verlag.

13. Gildas Avoine, Christian Floerkemeier, and Benjamin Martin. RFID Distance Bounding Multistate Enhancement. In *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, New Delhi, India, December 2009.
14. 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-Verlag.
15. Gildas Avoine, Cédric Lauradoux, and Tania Martin. When Compromised Readers Meet RFID. In *Workshop on RFID Security – RFIDSec’09*, Leuven, Belgium, July 2009.
16. 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-Verlag.
17. 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 Press.
18. 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-Verlag.
19. Gildas Avoine and Aslan Tchamkerten. An asymptotically optimal RFID protocol against relay attacks. Cryptology ePrint Archive, Report 2008/406, 2008. <http://eprint.iacr.org/>.
20. Gildas Avoine and Aslan Tchamkerten. An efficient distance bounding RFID authentication protocol: balancing false-acceptance rate and memory requirement. In *Information Security Conference – ISC’09*, volume 5735 of *Lecture Notes in Computer Science*, Pisa, Italy, September 2009.
21. 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.
22. 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.iwst.org.uk/Files/2005/Proceedings2005.pdf>, London, UK, April 2005.
23. 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.
24. 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-Verlag.
25. Helen Balinsky, Edward McDonnell, Liqun Chen, and Keith Harrison. Anti-Counterfeiting using Memory Spots. In *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.
26. Mihaly Barasz, Balazs Boros, Peter Ligeti, Krisztina Loja, and Daniel Nagy. Breaking LMAP. In *Conference on RFID Security*, Malaga, Spain, July 2007.
27. 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.
28. 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.
29. 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.
30. 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 Press.
31. Côme Berbain, Olivier Billet, Jonathan Etrog, and Henri Gilbert. An Efficient Forward Private RFID Protocol. In *16th ACM Conference on Computer and Communications Security – CCS’09*, pages 43–53, Chicago, Illinois, USA, November 2009. ACM.
32. Olivier Billet and Kaoutar El-Khiyaoui. Two Attacks against the Ff RFID Protocol. In *Proceedings of the 10th International Conference on Cryptology in India – Indocrypt 2009*, New Delhi, India, December 2009.
33. Erik-Oliver Blass, Kaoutar El-Khiyaoui, and Refik Molva. AnSta: Anonymous Statistics using RFID tags. Cryptology ePrint Archive, Report 2009/481, 2009. <http://eprint.iacr.org/>.

34. 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.
35. Carlo Blundo, Angelo De Caro, and Giuseppe Persiano. Untraceable Tags based on Mild Assumptions. In *Second International Workshop on Autonomous and Spontaneous Security – SETOP’09*, Saint-Malo, France, September 2009.
36. Carlo Blundo, Guisepe 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.
37. Salvatore Bocchetti. Security and Privacy in RFID Protocols, July 2006.
38. Andrey Bogdanov. Attacks on the KeeLoq Block Cipher and Authentication Systems. In *Workshop on RFID Security – RFIDSec’07*, Malaga, Spain, July 2007.
39. Andrey Bogdanov, Lars Ramkilde Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J.B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *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-Verlag.
40. Andrey Bogdanov, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J.B. Robshaw, and Yannick Seurin. Hash Functions and RFID Tags : Mind The Gap. In Elisabeth Oswald and Pankaj Rohatgi, editors, *Proceedings of the 10th International Workshop Cryptographic Hardware and Embedded Systems, CHES 2008*, volume 5154 of *Lecture Notes in Computer Science*, Washington, DC, USA, August 2008. Springer.
41. 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 Press.
42. Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Avi Rubin, and Michael Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.
43. Julien Bringer and Hervé Chabanne. On the Wiretap Channel Induced by Noisy Tags. In *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-Verlag.
44. 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.
45. 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 Press.
46. Julien Bringer, Hervé Chabanne, and Thomas Icart. Cryptanalysis of EC-RAC, a RFID identification protocol. In M.K. Franklin, L.C.K. Hui, and D.S. Wong, editors, *Proceedings of the 7th International Conference on Cryptology And Network Security – CANS 2008*, volume 5339 of *Lecture Notes in Computer Science*, pages 149–161, Hong Kong, China, December 2008. Springer.
47. 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.
48. Julien Bringer, Hervé Chabanne, and Thomas Icart. Efficient Zero-Knowledge Identification Schemes which respect Privacy. In *ACM Symposium on Information, Computer and Communication Security – ASIACCS’09*, Sydney, Australia, March 2009.
49. Trevor Burbridge and Mark Harrison. Security Considerations in the Design and Peering of RFID Discovery Services. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
50. Mike Burmester and Breno De Medeiros. Persistent Security for RFID. In *Workshop on RFID Security – RFIDSec’07*, Malaga, Spain, July 2007.
51. Mike Burmester and Breno de Medeiros. The Security of EPC Gen2 Compliant RFID Protocols. In *Proceeding of the International Conference on Applied Cryptography and Network Security, ACNS 2008*, Lecture Notes in Computer Science, Columbia University, New York, USA, June 2008. Springer.
52. Mike Burmester, Breno de Medeiros, and Rossana Motta. Robust, Anonymous RFID Authentication with Constant Key-Lookup. *Cryptology ePrint Archive*, Report 2007/402, 2007.

53. Mike Burmester, Breno de Medeiros, and Rossana Motta. Anonymous RFID authentication supporting constant-cost key-lookup against active adversaries. *Journal of Applied Cryptography*, 1(2):79–90, 2008.
54. Mike Burmester, Breno de Medeiros, and Rossana Motta. Provably Secure Grouping-Proofs for RFID Tags. In *Proceeding of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, Lecture Notes in Computer Science, Royal Holloway University of London, UK, September 2008. Springer.
55. Mike Burmester, Breno de Medeiros, Jorge Munilla, and Alberto Peinado. Secure EPC Gen2 compliant Radio Frequency Identification. Cryptology ePrint Archive, Report 2009/149, 2009.
56. 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*, Baltimore, Maryland, USA, August-September 2006. IEEE.
57. 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-Verlag.
58. Mike Burmester and Jorge Munilla. A Flyweight RFID Authentication Protocol. In *Workshop on RFID Security – RFIDSec’09*, Leuven, Belgium, July 2009.
59. Levente Buttyán, Tamás Holczer, and István Vajda. Optimal Key-Trees for Tree-Based Private Authentication. In *Workshop on Privacy Enhancing Technologies – PET 2006*, Cambridge, UK, June 2006.
60. Benoit Calmels, Sbastien 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*, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.
61. Sebastien Canard and Iwen Coisel. Data Synchronization in Privacy-Preserving RFID Authentication Schemes. In *Workshop on RFID Security – RFIDSec’08*, Budapest, Hungary, July 2008.
62. Sébastien Canard, Jonathan Etrog, and Iwen Coisel. Lighten Encryption Schemes for Secure and Private RFID Systems. 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.
63. 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.
64. 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.
65. 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.
66. Dario Carluccio, Kerstin Lemke, Christof Paar, and Ahmad-Reza Sadeghi. E-passport: the global traceability or how to feel like an UPS package. In Moti Yung Jae-Kwang Lee, Okyeon Yi, editor, *Workshop on Information Security Applications – WISA’06*, volume 4298 of *Lecture Notes in Computer Science*, pages 391–404, Jeju Island, Korea, August 2006. Springer-Verlag.
67. 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-Verlag.
68. Claude Castelluccia and Mate Soos. Secret Shuffling: A Novel Approach to RFID Private Identification. In *Workshop on RFID Security – RFIDSec’07*, pages 169–180, Malaga, Spain, July 2007.
69. 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*, pages 35–42, April 2008.
70. 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).
71. 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.
72. 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.
73. 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.

74. Jen-Chun Chang and Hsin-Lung Wu. A Hybrid RFID Protocol against Tracking Attacks. Cryptology ePrint Archive, Report 2009/138, 2009.
75. 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.
76. 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.
77. 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.
78. Hung-Yu Chien and Che-Hao Chen. Mutual Authentication Protocol for RFID Conforming to EPC Class 1 Generation 2 standards. *Computer Standards & Interfaces, Elsevier Science Publishers*, 29(2):254–259, February 2007.
79. Hung-Yu Chien and Chen-Wei Huang. A Lightweight RFID Protocol Using Substring. In *Embedded and Ubiquitous Computing – EUC’07*, volume 4808 of *Lecture Notes in Computer Science*, pages 422–431, Taipei, Taiwan, December 2007. Springer.
80. 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-Verlag.
81. Soo-Hyun Choi and You-Hyeon Jeong. A Secure and Scalable Transaction Protocol for Ubiquitous Sensor Network using RFID Systems. In *Proceedings of the 10th International Conference on Advanced Communication Technology – ICACT 2008*, volume 3, pages 1781–1784, Phoenix Park, Korea, February 2008. IEEE, IEEE Press.
82. 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-Verlag.
83. 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.
84. Tom Chothia and Vitaliy Smirnov. A Traceability Attack Against e-Passports. In *14th International Conference on Financial Cryptography and Data Security – FC’10*, Lecture Notes in Computer Science, Tenerife, Canary Islands, Spain, January 2010. Springer.
85. 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.
86. Jacek Cichon, Marek Klonowski, and Mirosław 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 Press.
87. 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.
88. 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 Press.
89. 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.
90. 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.
91. Nicolas T. Courtois, Sean O’Neil, and Jean-Jacques Quisquater. Practical Algebraic Attacks on the Hitag2 Stream Cipher. In *Information Security Conference – ISC’09*, Pisa, Italy, September 2009.
92. 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 Press.
93. Stefan Dahl. Anonymous Car Toll Payments using RFID Tags. Master thesis, Royal Institute of Technology, Stockholm, Sweden, 2006.

94. Ivan Damgård and Michael Østergaard. RFID Security: Tradeoffs between Security and Efficiency. Cryptology ePrint Archive, Report 2006/234, 2006.
95. Boris Danev, Thomas S. Heydt-Benjamin, and Srdjan Capkun. Physical-layer Identification of RFID Devices. In *Proceedings of the 18th USENIX Security Symposium – USENIX’09*, Montreal, Canada, August 2009.
96. 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.
97. Gerhard de Koning Gans. Analysis of the Mifare Classic used in the OV-Chipkaart Project, 2008.
98. Gerhard de Koning Gans, Jaap-Henk Hoepman, and Flavio D. Garcia. A Practical Attack on the MIFARE Classic. In *Proceeding of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, Lecture Notes in Computer Science, Royal Holloway University of London, UK, September 2008. Springer.
99. 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 Press.
100. Robert H. Deng, Yingjiu Li, Andrew C. Yao, Moti Yung, and Yunlei Zhao. A New Framework for RFID Privacy. Cryptology ePrint Archive, Report 2010/059, 2010.
101. 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*, pages 58–64, April 2008.
102. 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*, Athens, Greece, September 2005. IEEE.
103. Tassos Dimitriou. A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.
104. Tassos Dimitriou. Proxy Framework for Enhanced RFID Security and Privacy. In *Fifth Annual IEEE Consumer Communications & Networking Conference – CCNC 2007*, Las Vegas, Nevada, USA, January 2008. IEEE.
105. Tassos Dimitriou. RFID-DOT: RFID Delegation and Ownership Transfer made simple. In *4th International Conference on Security and Privacy for Communication Networks – SecureComm 2008*, Istanbul, Turkey, September 2008.
106. Tassos Dimitriou. RFID Security and Privacy. In *RFID Security: Techniques, Protocols and System-on-Chip Design*, pages 57–79, September 2008.
107. 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.
108. 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*, New Brunswick, Canada, October 2004.
109. Imran Erguler and Emin Anarim. Scalability and Security Conflict for RFID Authentication Protocols. Cryptology ePrint Archive, Report 2010/018, 2010.
110. 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 Press.
111. Junfeng Fan and Ingrid Verbauwhede. Hyperelliptic curve processor for RFID tags. In *Workshop on RFID Security – RFIDSec’09*, Leuven, Belgium, July 2009.
112. Martin Feldhofer. A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags, 2003.
113. 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.
114. 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.
115. 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 Press.
116. 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-Verlag.

117. Martin Feldhofer and Christian Rechberger. A Case Against Currently Used Hash Functions in RFID Protocols. In *Workshop on RFID Security – RFIDSec’06*, Graz, Austria, July 2006. Ecrypt.
118. 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.
119. Martin Feldhofer, Johannes Wolkerstorfer, and Vincent Rijmen. AES Implementation on a Grain of Sand. *IEE Proceedings - Information Security*, 152(1):13–20, October 2005.
120. 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 2004*, volume 3313 of *Lecture Notes in Computer Science*, pages 42–53, Heidelberg, Germany, August 2005. Springer-Verlag.
121. 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-Verlag.
122. Sepideh Fouladgar and Hossam Affi. An Efficient Delegation and Transfer of Ownership Protocol for RFID Tags. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
123. Dmitry Frumkin and Adi Shamir. Un-Trusted-HB: Security Vulnerabilities of Trusted-HB. In *Workshop on RFID Security – RFIDSec’09*, Leuven, Belgium, July 2009.
124. Benjamin Fung, Khalil Al-Hussaeni, and Ming Cao. Preserving RFID Data Privacy. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
125. 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.
126. Flavio D. Garcia, Gerhard de Koning Gans, Ruben Muijers, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Dismantling MIFARE Classic. In *Proceeding of the 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.
127. 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.
128. 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.
129. Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis. Evaluation of Anonymized ONS Queries. In Cuppens et al. (Eds.), editor, *First International Workshop on Security of Autonomous and Spontaneous Networks – SETOP’08*, pages 47–60, Loctudy, France, October 2008.
130. Joaquin Garcia-Alfaro, Michel Barbeau, and Evangelos Kranakis. Security Threat Mitigation Trends in Low-cost RFID Systems. In Garcia-Alfaro et al. (Eds), editor, *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.
131. 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.
132. Henri Gilbert, Matthew Robshaw, and Hervé Sibert. An Active Attack Against HB⁺ – A provably Secure Lightweight Authentication Protocol. Manuscript, July 2005.
133. Marc Girault, Loic Juniot, and Matt Robshaw. The Feasibility of On-the-Tag Public Key Cryptography. In *Workshop on RFID Security – RFIDSec’07*, Malaga, Spain, July 2007.
134. Dara J. Glasser, Kenneth W. Goodman, and Norman G. Einspruch. Chips, Tags and Scanners: Ethical Challenges for Radio Frequency Identification. In *Ethics and Information Technology*, volume 9 of 2, pages 101–109. Springer Netherlands, July 2007.
135. 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*, volume 2964 of *Lecture Notes in Computer Science*, pages 163–178, San Francisco, California, USA, February 2004. Springer-Verlag.
136. 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*, pages 41–42, Washington, DC, USA, October 2004. ACM, ACM Press.

137. JungHoon Ha, SangJae Moon, Jianying Zhou, and JaeCheol Ha. A New Formal Proof Model for RFID Location Privacy. In *Proceeding of the 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.
138. John Halamka, Ari Juels, Adam Stubblefield, and Jonathan Westhues. The Security Implications of VeriChip™ Cloning. Manuscript in submission, March 2006.
139. 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.
140. 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 *Proceedings of the 29th Annual IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2008.
141. Martin Halváč and Tomáš Rosa. A Note on the Relay Attacks on e-Passports: The Case of Czech e-Passports. Cryptology ePrint Archive, Report 2007/244, 2007.
142. Gerhard Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.
143. Gerhard Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In *IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2006. IEEE, IEEE Computer Society Press.
144. Gerhard Hancke. Noisy Carrier Modulation for HF RFID. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
145. Gerhard Hancke. Eavesdropping Attacks on High-Frequency RFID Tokens. In *Workshop on RFID Security – RFIDSec’08*, Budapest, Hungary, July 2008.
146. Gerhard 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.
147. Gerhard Hancke and Markus Kuhn. Attacks on Time-of-Flight Distance Bounding Channels. In *Proceedings of the first ACM Conference on Wireless Network Security, WiSec’08*, pages 194–202, Alexandria, Virginia, USA, March-April 2008. ACM.
148. Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Confidence in Smart Token Proximity: Relay Attacks Revisited. In *Elsevier Computers & Security*, June 2009.
149. Gerhard P. Hancke. *Security of Proximity Identification Systems*. PhD thesis, University of Cambridge, Cambridge, United Kingdom, February 2008.
150. Ernst Haselsteiner and Klemens Breitfuss. Security in Near Field Communication (NFC). In *Workshop on RFID Security – RFIDSec’06*, Graz, Austria, July 2006. Ecrypt.
151. 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.
152. 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.
153. 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.
154. Dirk Henrici and Paul Müller. Tackling Security and Privacy Issues in Radio Frequency Identification Devices. In Alois Ferscha and Friedemann Mattern, editors, *Pervasive Computing*, volume 3001 of *Lecture Notes in Computer Science*, pages 219–224, Vienna, Austria, April 2004. Springer-Verlag.
155. Julio C. Hernandez-Castro, Juan E. Tapiador, Pedro Peris-Lopez, John A. Clark, and El-Ghazali Talbi. Meta-heuristic 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.
156. Thomas Heydt-Benjamin, Hee-Jin Chae, Benessa Defend, and Kevin Fu. Privacy for Public Transportation. In *Workshop on Privacy Enhancing Technologies – PET 2006*, Cambridge, UK, June 2006.
157. Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and Tom O’Hare. Vulnerabilities in First-Generation RFID-Enabled Credit Cards. Manuscript, October 2006.
158. Thomas Hjorth. Supporting Privacy in RFID Systems. Master thesis, Technical University of Denmark, Lyngby, Denmark, December 2004.
159. 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

- Rannenbergh, Yuko Murayama, and Shin-ichi Kawamura, editors, *Advances in Information and Computer Security, First International Workshop on Security – IWSEC*, volume 4266 of *Lecture Notes in Computer Science*, pages 152–167, Kyoto, Japan, October 2006. Springer-Verlag.
160. Georg Hofferek and Johannes Wolkerstorfer. Coupon Recalculation for the GPS Authentication Scheme. In *Proceeding of the 8th Smart Card Research and Advanced Applications – CARDIS 2008*, Lecture Notes in Computer Science, Royal Holloway University of London, UK, September 2008. Springer.
 161. 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.
 162. 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 *Cryptographic Hardware and Embedded Systems – CHES 2006*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59, Yokohama, Japan, November 2006. Springer.
 163. 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-Verlag.
 164. Michael Hutter, Marcel Medwed, Daniel Hein, and Johannes Wolkerstorfer. Attacking ECDSA-Enabled RFID Devices. In *Proceedings of the 7th International Conference on Applied Cryptography and Network Security – ACNS 2009*, pages 1–2, Paris, France, June 2009. Springer.
 165. 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.
 166. Sozo Inoue and Hiroto Yasuura. RFID Privacy Using User-controllable Uniqueness. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
 167. 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.
 168. 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 Press.
 169. Yang Jeongkyu. Security and Privacy on Authentication Protocol for Low-cost Radio Frequency Identification. Master thesis, Information and Communications University, Daejeon, Korea, December 2004.
 170. 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, Italia, September 2004. Springer-Verlag.
 171. 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.
 172. 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-Verlag, 2005.
 173. Ari Juels. Strengthening EPC Tags Against Cloning. Manuscript, March 2005.
 174. Ari Juels. RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394, February 2006.
 175. 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*, pages 1–7, Washington, DC, USA, October 2004. ACM, ACM Press.
 176. 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*, Athens, Greece, September 2005. IEEE.
 177. 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-Verlag.
 178. Ari Juels, Ravikanth Pappu, and Bryan Parno. Unidirectional Key Distribution Across Time and Space with Applications to RFID Security. In *17th USENIX Security Symposium*, pages 75–90, San Jose, California, USA, July 2008. USENIX.

179. Ari Juels, Ronald Rivest, and Michael Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Vijay Atluri, editor, *Conference on Computer and Communications Security – ACM CCS*, pages 103–111, Washington, DC, USA, October 2003. ACM, ACM Press.
180. Ari Juels, Paul Syverson, and Dan Bailey. High-Power Proxies for Enhancing RFID Privacy and Utility. In *Workshop on Privacy Enhancing Technologies – PET 2005*, Dubrovnik, Croatia, May-June 2005.
181. 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-Verlag.
182. 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 Press.
183. Ulrich Kaiser. UICE: A High-Performance Cryptographic Module for SoC and RFID Applications. Cryptology ePrint Archive, Report 2007/258, 2007.
184. 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-Verlag.
185. Gaurav Kapoor, Wei Zhou, and Selwyn Piramuthu. Distance Bounding Protocol for Multiple RFID Tag Authentication. In *Proceedings of the International Conference on Embedded and Ubiquitous Computing – Volume 02 – EUC’08*, pages 115–120, Shanghai, China, December 2008. IEEE.
186. Jens-Peter Kaps, Gunnar Gaubatz, and Berk Sunar. Cryptography on a Speck of Dust. *IEEE Computer*, 40(2):38–44, February 2007.
187. 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.
188. Günter Karjoth and Paul Moskowitz. Disabling RFID Tags with Visible Confirmation: Clipped Tags Are Silenced. In *Workshop on Privacy in the Electronic Society – WPES*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
189. 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.
190. Tom Karygiannis, Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips. Guidelines for Securing Radio Frequency Identification (RFID) Systems, April 2007.
191. Timo Kasper. *Embedded Security Analysis of RFID Devices*. PhD thesis, Ruhr-University Bochum, Bochum, Germany, July 2006.
192. 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.
193. Jonathan Katz and Adam Smith. Analyzing the HB and HB+ Protocols in the “Large Error” Case. Cryptology ePrint Archive, Report 2006/326, 2006.
194. Jonathan Katz and Ji Sun Shin. Parallel and Concurrent Security of the HB and HB+ Protocols. In Serge Vaude- nay, editor, *Advances in Cryptology – EUROCRYPT’06*, Lecture Notes in Computer Science, Saint Petersburg, Russia, May-June 2006. IACR, Springer-Verlag.
195. 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.
196. Florian Kerschbaum and Alessandro Sorniotti. RFID-Based Supply Chain Partner Authentication and Key Agreement. In *Proceedings of the second ACM Conference on Wireless Network Security – WiSec’09*, Zurich, Switzerland, March 2009. ACM.
197. 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*, Athens, Greece, September 2005. IEEE.
198. Rushikesh Khasgiwale, Rohan Adyanthaya, and Daniel Engels. Extracting Information from Tag Collisions. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
199. Chong Hee Kim and Gildas Avoine. RFID Distance Bounding Protocol with Mixed Challenges to Prevent Relay Attacks. In *8th International Conference on Cryptology And Network Security – CANS’09*, Kanazawa, Ishikawa, Japan, December 2009. Springer.
200. 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*, volume 5461 of *Lecture Notes in Computer Science*, pages 98–115, Seoul, Korea, December 2008. Springer-Verlag.
201. 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 Press.
 202. 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*, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.
 203. 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.
 204. Ilan Kirschenbaum and Avishai Wool. How to Build a Low-Cost, Extended-Range RFID Skimmer. Cryptology ePrint Archive, Report 2006/054, 2006.
 205. Heiko Knosp and Hartmut Pohl. RFID Security. *Information Security Technical Report*, 9(4):39–50, November–December 2004.
 206. 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.
 207. 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 Computer Society Press.
 208. 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 *Proceedings of the 2007 ACM symposium on Applied computing – SAC’07*, pages 270–275, Seoul, Korea, March 2007. ACM.
 209. Karl Koscher, Ari Juels, Tadayoshi Kohno, and Vjekoslav Brajkovic. EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript, 2008.
 210. 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 International Federation for Information Processing, New approaches for Security, Privacy and Trust in Complex Environments*, volume 232, pages 467–472, Sandton, Gauteng, South Africa, May 2007. IFIP, Springer.
 211. Matthias Krause and Dirk Stegemann. More on the Security of Linear RFID Authentication Protocols. In *Selected Areas in Cryptography – SAC’09*, Calgary, Alberta, Canada, August 2009.
 212. 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.
 213. Rakesh Kumar. Interaction of RFID Technology and Public Policy. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
 214. 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.
 215. 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.
 216. 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-Verlag.
 217. Daesung Kwon, Daewan Han, Jooyoung Lee, and Yongjin Yeom. Vulnerability of an RFID Authentication Protocol Proposed at SecUbiq 2005. In *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-Verlag.
 218. Marc Langheinrich. A Survey of RFID Privacy Approaches. *Personal and Ubiquitous Computing*, 13(6):413–421, August 2009.
 219. 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.
 220. Tri van Le, Mike Burmester, and Breno de Medeiros. Forward-Secure RFID Authentication and Key Exchange. Cryptology ePrint Archive, Report 2007/051, 2007.

221. Hwaseong Lee, Eun Young Choi, Su-Mi Lee, and Dong Hoon Lee. Trapdoor-Based Mutual Authentication Scheme without Cryptographic Primitives in RFID Tags. *Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, SecPerU*, pages 73–78, July 2007.
222. Jooyoung Lee and Yongjin Yeom. Efficient RFID Authentication Protocols Based on Pseudorandom Sequence Generators. Cryptology ePrint Archive, Report 2008/343, August 2008.
223. Sangshin Lee. Mutual Authentication of RFID System using Synchronized Secret Information. Master thesis, School of Engineering Information and Communications University, Daejeon, Korea, December 2005.
224. 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.
225. Su-Mi Lee, Young Ju Hwang, Dong Hoon Lee, and Jong In 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-Verlag.
226. Yong Ki Lee, Lejla Batina, Dave Singelée, and Ingrid Verbauwhede. Low-Cost Untraceable Authentication Protocols for RFID. In *3rd ACM Conference on Wireless Network Security - WiSec'10*, Hoboken, New Jersey, USA, March 2010.
227. 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*, pages 97–104, April 2008.
228. 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.
229. Yongki Lee, Lejla Batina, and Ingrid Verbauwhede. Untraceable RFID Authentication Protocols: Revision of EC-RAC. In *IEEE International Conference on RFID - RFID 2009*, Orlando, Florida, USA, April 2009.
230. 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 - RFID 2009*, Orlando, Florida, USA, April 2009.
231. Mikko Lehtonen, Daniel Ostojic, Alexander Ilic, and Florian Michahelles. Securing RFID Systems by Detecting Tag Cloning. In *7th International Conference on Pervasive Computing - Pervasive 2009*, volume 5538 of *Lecture Notes in Computer Science*, pages 291–308, Nara, Japan, May 2009. Springer.
232. 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 - RFID 2009*, Orlando, Florida, USA, April 2009.
233. 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.
234. 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.
235. Stéphane Lemieux and Adrian Tang. Clone Resistant Mutual Authentication for Low-Cost RFID Technology. Cryptology ePrint Archive, Report 2007/170, 2007.
236. Xuefei Leng, Keith Mayes, and Konstantinos Markantonakis. HB-MP+ Protocol: An Improvement on the HB-MP Protocol. *IEEE International Conference on RFID*, pages 118–124, April 2008.
237. Teyan 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.
238. Teyan Li and Guilin Wang. Security Analysis of Two Ultra-Lightweight RFID Authentication Protocols. In *IFIP SEC 2007*, Sandton, Gauteng, South Africa, May 2007. IFIP.
239. Teyan 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.
240. Yingjiu Li and Xuhua Ding. Protecting RFID Communications in Supply Chains. In *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security - ASIACCS '07*, pages 234–241, Singapore, Republic of Singapore, 2007. ACM.
241. Ingo Liersch. Electronic passports – from secure specifications to secure implementations. *Elsevier Information Security Technical Report*, 14(2):96–100, May 2009.

242. Chae Hoon Lim and Tymur Korkishko. mCrypton - A Lightweight Block Cipher For Security of Low-Cost RFID Tags and Sensors. In *Workshop on Information Security Applications – WISA '05*, Lecture Notes in Computer Science, Jeju Island, Korea, August 2005. Springer-Verlag.
243. Chae Hoon Lim and Taekyoung Kwon. Strong and Robust RFID Authentication Enabling Perfect Ownership Transfer. In *Conference on Information and Communications Security – ICICS'06*, Lecture Notes in Computer Science, Raleigh, North Carolina, USA, December 2006. Springer-Verlag.
244. 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*, pages 285–288, Stevens Point, Wisconsin, USA, March 2007. World Scientific and Engineering Academy and Society (WSEAS).
245. Zhaoyu Liu and Dichao Peng. True Random Number Generator in RFID Systems Against Traceability. In *IEEE Consumer Communications and Networking Conference – CCNS*, volume 1, pages 620–624, Las Vegas, Nevada, USA, January 2006. IEEE, IEEE.
246. 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*, Lecture Notes in Computer Science, Tarragona, Spain, April 2006. IFIP, Springer-Verlag.
247. 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.
248. Li Lu, Yunhao Liu, Lei Hu, Jinsong Han, and Lionel Ni. A Dynamic Key-Updating Private Authentication Protocol 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 Press.
249. Changshe Ma, Yingjiu Li, Robert Deng, and Tiejian Li. RFID Privacy: Relation Between Two Notions, Minimal Condition, and Efficient Construction. In *Proceedings of the 16th ACM Conference on Computer and Communications Security – CCS'09*, Chicago, Illinois, USA, November 2009.
250. 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*, pages 103–114, Malaga, Spain, July 2007.
251. Santi Martínez, Madga Valls, Concepció 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.
252. Keith Mayes, Konstantinos Markantonakis, and Gerhard Hancke. Transport ticketing security and fraud controls. *Elsevier Information Security Technical Report*, 14(2):87–95, May 2009.
253. Maire McLoone and Matt Robshaw. Public Key Cryptography and RFID Tags. In Masayuki Abe, editor, *The Cryptographers' Track at the RSA Conference – CT-RSA*, Lecture Notes in Computer Science, San Francisco, California, USA, February 2007. Springer-Verlag.
254. 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.
255. Joan Melia-Seguí, Joaquín García-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.
256. 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.
257. 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.
258. 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.
259. 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.
260. 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.

261. 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, July 2010.
262. 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.
263. Aikaterini Mitrokotsa, Melanie R. Rieback, and Andrew S. Tanenbaum. Classifying RFID Attacks and Defenses. *Information Systems Frontiers*, July 2009.
264. 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.
265. 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.
266. 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-Verlag.
267. David Molnar, Andrea Soppera, and David Wagner. Privacy for RFID Through Trusted Computing. In *Workshop on Privacy in the Electronic Society – WPES*, Alexandria, Virginia, USA, November 2005. ACM, ACM Press.
268. David Molnar and David Wagner. Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Birgit Pfitzmann and Peng Liu, editors, *Conference on Computer and Communications Security – ACM CCS*, pages 210–219, Washington, DC, USA, October 2004. ACM, ACM Press.
269. Jean Monnerat, Serge Vaudenay, and Martin Vuagnoux. About Machine-Readable Travel Documents. In *Workshop on RFID Security – RFIDSec'07*, Malaga, Spain, July 2007.
270. 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.
271. 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.
272. 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.
273. Jorge Munilla and Alberto Peinado. Attacks on a Distance Dounding Protocol. *Elsevier Computer Communications*, 33(7):884–889, May 2010.
274. 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.
275. 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*, Kuala Lumpur, Malaysia, April 2009.
276. Dang Nguyen Duc and Kwangjo Kim. Grouping-Proof Protocol for RFID Tags: Security Definition and Scalable Construction. Cryptology ePrint Archive, Report 2009/609, 2009.
277. 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.
278. Ventzislav Nikov and Marc Vaclair. Yet Another Secure Distance-Bounding Protocol. Cryptology ePrint Archive, Report 2008/319, 2008. <http://eprint.iacr.org/>.
279. Rishab Nithyanand. The Evolution of Cryptographic Protocols in Electronic Passports. Cryptology ePrint Archive, Report 2009/200, 2009. <http://eprint.iacr.org/>.
280. Rishab Nithyanand, Gene Tsudik, and Ersin Uzun. Readers Behaving Badly: Reader Revocation in PKI-Based RFID Systems. Cryptology ePrint Archive, Report 2009/465, 2009. <http://eprint.iacr.org/>.
281. Yasunobu Nohara and Sozo Inoue. A Secure and Scalable Identification for Hash-based RFID Systems Using Updatable Pre-computation. In *3rd ACM Conference on Wireless Network Security – WiSec'10*, Hoboken, New Jersey, USA, March 2010.
282. Yasunobu Nohara, Sozo Inoue, Kensuke Baba, and Hiroto Yasuura. Quantitative Evaluation of Unlinkable ID Matching Schemes. In *Workshop on Privacy in the Electronic Society – WPES*, pages 55–60, Alexandria, Virginia, USA, November 2006. ACM, ACM Press.

283. Karsten Nohl and David Evans. Quantifying Information Leakage in Tree-Based Hash Protocols. In *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-Verlag.
284. 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.
285. Karsten Nohl and David Evans. Hiding in Groups: On the Expressiveness of Privacy Distributions. In *Proceedings of The Ifip Tc 11 23rd International Information Security Conference – SEC 2008*, volume 278 of *Lecture Notes in Computer Science*, pages 1–15, Milan, Italia, September 2008. Springer.
286. Karsten Nohl, David Evans, Starbug, and Henryk Plotz. Reverse-Engineering a Cryptographic RFID Tag. In *17th USENIX Security Symposium*, pages 185–194, San Jose, California, USA, July 2008. USENIX.
287. Dorice Diane Nyamy, Simon Elrhbari, 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.
288. Miyako Ohkubo and Koutarou Suzuki. Forward Secure RFID Privacy Protection Scheme with Restricted Traceability. In Jianying Zhou and Moti Yung, 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-Verlag.
289. Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita. Cryptographic Approach to “Privacy-Friendly” Tags. In *RFID Privacy Workshop*, MIT, Massachusetts, USA, November 2003.
290. 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.
291. 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.
292. Yossef Oren and Martin Feldhofer. WIPR - a Public Key Implementation on Two Grains of Sand. In *Workshop on RFID Security – RFIDSec’08*, Budapest, Hungary, July 2008. <http://iss.oy.ne.ro/WIPR>.
293. Yossef Oren and Martin Feldhofer. A Low-Resource Public-Key Identification Scheme for RFID Tags and Sensor Nodes. In *Proceedings of the second ACM Conference on Wireless Network Security – WiSec’09*, Zurich, Switzerland, March 2009. ACM.
294. Yossef Oren and Avishai Wool. Relay Attacks on RFID-Based Electronic Voting Systems. Cryptology ePrint Archive, Report 2009/442, 2009. <http://eprint.iacr.org/>.
295. Yossi Oren. Remote Power Analysis of RFID Tags. Cryptology ePrint Archive, Report 2007/330, 2007.
296. Khaled Ouafi, Raphael Overbeck, and Serge Vaudenay. On the Security of HB# against a Man-in-the-Middle Attack. In *Advances in Cryptology - Asiacrypt 2008*, volume 5350 of *Lecture Notes in Computer Science*, pages 108–124, Melbourne, Australia, December 2008. Springer.
297. Khaled Ouafi and Raphael C.-W. Phan. Privacy of Recent RFID Authentication Protocols. In *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.
298. Khaled Ouafi and Raphael C.-W. Phan. Traceable Privacy of Recent Provably-Secure RFID Protocols. In *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.
299. Khaled Ouafi and Serge Vaudenay. Pathchecker: an RFID Application for Tracing Products in Supply-Chains. In *Workshop on RFID Security – RFIDSec’09*, Leuven, Belgium, July 2009.
300. Radu-Ioan Païse and Serge Vaudenay. Mutual Authentication in RFID: Security and Privacy. In *Proceedings of the 3rd ACM Symposium on Information, Computer and Communications Security – ASIACCS’08*, pages 292–299, Tokyo, Japan, 2008. ACM Press.
301. 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-Verlag.
302. Pedro Peris-Lopez. *Lightweight Cryptography in Radio Frequency Identification (RFID) Systems*. PhD thesis, Computer Science Department, Carlos III University of Madrid, November 2008.

303. Pedro Peris-Lopez, Julio C. Hernandez-Castro, Juan M. Estevez-Tapiador, Tiejian 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.
304. 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 Press.
305. 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, Computer Science, Cryptography and Security, arXiv:0910.2115v1 [cs.CR], 2009.
306. 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.
307. 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 Series*, pages 83–93, Singapore, Republic of Singapore, February 2010. IOS Press.
308. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan 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.
309. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. M2AP: A Minimalist Mutual-Authentication Protocol for Low-cost RFID Tags. In *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-Verlag.
310. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan Estevez-Tapiador, and Arturo Ribagorda. RFID Systems: A Survey on Security Threats and Proposed Solutions. In *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-Verlag.
311. Pedro Peris-Lopez, Julio Cesar 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-Verlag.
312. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. An Efficient Authentication Protocol for RFID Systems Resistant to Active Attacks. In *EUC Workshops: SecUbig Workshop*, volume 4809 of *Lecture Notes in Computer Science*, pages 781–794. Springer-Verlag, December 2007.
313. Pedro Peris-Lopez, Julio Cesar 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.
314. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. LAMED - A PRNG for EPC Class-1 Generation-2 RFID Specification. In *Computer Standard and Interface*, volume In Press, Corrected Proof. Elsevier Science, 2007.
315. Pedro Peris-Lopez, Julio Cesar Hernandez-Castro, Juan M. Estevez-Tapiador, and Arturo Ribagorda. Advances in Ultralightweight Cryptography for Low-cost RFID Tags: Gossamer Protocol. In *Workshop on Information Security Applications*, Lecture Notes in Computer Science, Jeju Island, Korea, September 2008. Springer-Verlag.
316. Pedro Peris-Lopez, Tiejian Li, Lim Tong Lee, Julio Cesar 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.
317. Pedro Peris-Lopez, Lim Tong Lee, and Tiejian Li. Providing Stronger Authentication at a Low-Cost to RFID Tags Operating under the EPCglobal Framework. In *IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications – TSP’08*, pages 159–166, Shanghai, China, December 2008.
318. Raphael C.-W. Phan. Cryptanalysis of a New Ultralightweight RFID Authentication Protocol - SASI. *IEEE Transactions on Dependable and Secure Computing*, 99(1), 2008.
319. Roberto Di Pietro and Refik Molva. Information Confinement, Privacy, and Security in RFID Systems. In *Proceedings of the 12th European Symposium On Research In Computer Security – ESORICS 2007*, pages 187–202, Dresden, Germany, 2007.

320. 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.
321. 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 Press.
322. 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.
323. Ivo Pooters. Keep Out of My Passport: Access Control Mechanisms in E-passports, 2008.
324. 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.
325. 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.
326. 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.
327. 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.
328. Jason Reid, Juan Gonzalez Neito, Tee Tang, and Bouchra Senadji. Detecting Relay Attacks with Timing Based Protocols. QUT ePrint, Report 3264, 2006.
329. Jason Reid, Juan Gonzalez Neito, 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.
330. 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-Verlag.
331. Henning Richter, Wojciech Mostowski, and Erik Poll. Fingerprinting Passports. Epractice, 2008.
332. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Keep on Blockin’ in the Free World: Personal Access Control for Low-Cost RFID Tags. In *International Workshop on Security Protocols – IWSP’05*, Lecture Notes in Computer Science, Cambridge, England, April 2005. Springer-Verlag.
333. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In Colin Boyd and Juan Manuel González 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-Verlag.
334. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Uniting Legislation with RFID Privacy-Enhancing Technologies. In *Security and Protection of Information*, Brno, Czech Republic, May 2005.
335. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. Is Your Cat Infected with a Computer Virus? In *Pervasive Computing and Communications*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.
336. Melanie Rieback, Bruno Crispo, and Andrew Tanenbaum. The Evolution of RFID Security. *IEEE Pervasive Computing*, 5(1):62–69, January–March 2006.
337. Melanie Rieback, Georgi Gaydadjiev, Bruno Crispo, Rutger Hofman, and Andrew Tanenbaum. A Platform for RFID Security and Privacy Administration. In *USENIX/SAGE Large Installation System Administration conference – LISA’06*, Washington, DC, USA, December 2006.
338. Melanie R. Rieback. *Security and Privacy of Radio Frequency Identification*. PhD thesis, Vrije Universiteit, Amsterdam, The Netherlands, 2008.
339. Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-Lightweight Implementations for Smart Devices — Security for 1000 Gate Equivalents. In *Proceedings of the 8th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications – CARDIS ’08*, Lecture Notes in Computer Science, pages 89–103, Royal Holloway University of London, UK, September 2008. Springer-Verlag.
340. Pawel Rotter. A Framework for Assessing RFID System Security and Privacy Risks. *IEEE Pervasive Computing*, 7(2):70–77, June 2008.
341. 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.

342. 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.
343. Ahmad-Reza Sadeghi, Ivan Visconti, and Christian Wachsmann. Anonymizer-Enabled Security and Privacy for RFID. In *8th International Conference on Cryptology And Network Security – CANS'09*, Kanazawa, Ishikawa, Japan, December 2009. Springer.
344. 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.
345. 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.
346. 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 2004*, volume 3207 of *Lecture Notes in Computer Science*, pages 879–890, Aizu-Wakamatsu City, Japan, August 2004. Springer-Verlag.
347. 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.
348. 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.
349. 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-Verlag.
350. Sanjay Sarma, Stephen Weis, and Daniel Engels. Radio-Frequency Identification: Security Risks and Challenges. *Cryptobytes, RSA Laboratories*, 6(1):2–9, Spring 2003.
351. 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-Verlag.
352. 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.
353. Youngjoon Seo and Kwangjo Kim. Scalable and Untraceable Authentication Protocol for RFID. In *International Workshop on Security in Ubiquitous Computing Systems – SecUbiq 2006*, Lecture Notes in Computer Science, Seoul, Korea, August 2006. Springer-Verlag.
354. Cai Shaoying, Yingjiu Li, Tiejian Li, and Robert Deng. Attacks and Improvements to an RFID Mutual Authentication Protocol and its Extensions. In *Proceedings of the second ACM Conference on Wireless Network Security – WiSec'09*, Zurich, Switzerland, March 2009. ACM.
355. Shah Sheetal. Technical analysis of security mechanisms used in RFID E-passport, related threats, security and privacy issues, 2006.
356. 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.
357. Han Shuihua and Chao-Hsien Chu. Tamper Detection in RFID-Enabled Supply Chains Using Fragile Watermarking. *IEEE International Conference on RFID*, pages 111–117, April 2008.
358. Pieter Siekerman and Maurits van der Schee. Security Evaluation of the disposable OV-chipkaart. Report, System and Network Engineering, University of Amsterdam, July 2007.
359. 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.
360. Boyeon Song. RFID Tag Ownership Transfer. In *Workshop on RFID Security – RFIDSec'08*, Budapest, Hungary, July 2008.
361. Boyeon Song. Server Impersonation Attacks on RFID Protocols. In *The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies – UBICOMM'08*, pages 50–55, Valencia, Spain, October 2008. IEEE Computer Society.
362. Boyeon Song and Chris J. Mitchell. RFID Authentication Protocol for Low-cost Tags. In V. D. Gligor, J. Hubaux, and R. Poovendran, editors, *ACM Conference on Wireless Network Security, WiSec'08*, pages 140–147, Alexandria, Virginia, USA, April 2008. ACM Press.

363. Boyeon Song and Chris J. Mitchell. Scalable RFID Authentication Protocol. In *3rd International Conference on Network & System Security — NSS 2009*, pages 216–224, Gold Coast, Australia, October 2009. IEEE Computer Society.
364. Mate Soos. Analysing the Molva and Di Pietro Private RFID Authentication Scheme. In *Workshop on RFID Security – RFIDSec’08*, Budapest, Hungary, July 2008.
365. Andrea Soppera and Trevor Burbridge. Wireless Identification – Privacy and Security. *BT Technology Journal*, 23(4):54–64, October 2005.
366. Andrea Soppera and Trevor Burbridge. Off by Default - RAT: RFID Acceptor Tag. In *Workshop on RFID Security – RFIDSec’06*, Graz, Austria, July 2006. Ecrypt.
367. Andrea Soppera, Trevor Burbridge, and Valentijn Broekhuizen. Trusted RFID Readers for Secure Multi-Party Services. EU RFID Forum, March 2007.
368. Sarah Spiekermann. Perceived Control: Scales for Privacy in Ubiquitous Computing Environments. In *Conference on User Modeling – UM’05*, Edinburgh, Scotland, July 2005.
369. 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.
370. Sarah Spiekermann and Sergei Evdokimov. Privacy Enhancing Technologies for RFID - A Critical Investigation of State of the Art Research. In *IEEE Privacy and Security*, 2009.
371. 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.
372. 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.
373. 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, *Symposium on Applied Computing – SAC*, pages 1607–1612, Santa Fe, New Mexico, USA, March 2005. ACM, ACM Press.
374. Stefan Stadlober. An Evaluation of Security Threats and Countermeasures in Distributed RFID Infrastructures. Master thesis, Graz University of Technology, Graz, Austria, July 2005.
375. 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*, New York City, New York, USA, March 2007. IEEE, IEEE Computer Society Press.
376. Wouter Teepe. Making the Best of Mifare Classic, October 2008. www.sos.cs.ru.nl/applications/rfid/2008-thebest.pdf.
377. 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.
378. Denis Trček and Pekka Jäppinen. *Non-deterministic Lightweight Protocols for Security and Privacy in RFID Environments*. Auerbach Publication, 2009.
379. Denis Trček and Damjan Kovač. Formal Appartus for Measurement of Lightweight Protocols. In *Computer Standard and Interface*, volume In Press, Corrected Proof. Elsevier Science, 2008.
380. Gene Tsudik. YA-TRAP: Yet Another Trivial RFID Authentication Protocol. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy, March 2006. IEEE, IEEE Computer Society Press.
381. Gene Tsudik. A Family of Dunces: Trivial RFID Identification and Authentication Protocols. Cryptology ePrint Archive, Report 2006/015, 2007.
382. Yu-Ju Tu and Selwyn Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007.
383. Pim Tuyls and Lejla Batina. RFID-Tags for Anti-Counterfeiting. In David Pointcheval, editor, *Topics in Cryptology - CT-RSA 2006, The Cryptographers’ Track at the RSA Conference 2006*, Lecture Notes in Computer Science, San Jose, California, USA, February 2006. Springer-Verlag.
384. 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.

385. 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.
386. 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 Computer Society.
387. 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.
388. 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.
389. 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.
390. Ton van Deursen, Sjouke Mauw, and Saša Radomirović. Untraceability of RFID Protocols. In *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, volume 5019 of *Lecture Notes in Computer Science*, pages 1–15, Sevilla, Spain, May 2008. Springer.
391. Ton van Deursen and Saša Radomirović. Attacks on RFID Protocols. Cryptology ePrint Archive, Report 2008/310, July 2008.
392. Ton van Deursen and Saša Radomirović. Algebraic Attacks on RFID Protocols. In *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.
393. Tristan Crispijn van Stijn. Analyzing RFID Authentication Protocols, 2007.
394. Nimish Vartak. Protecting the Privacy of RFID tags. Master thesis, University of Maryland, College Park, Maryland, USA, May 2006.
395. Serge Vaudenay. RFID Privacy Based on Public-Key Cryptography (Abstract). In Min Surp Rhee and Byoungcheon Lee, editors, *Information Security and Cryptology – ICISC 2006*, volume 4296 of *Lecture Notes in Computer Science*, pages 1–6, Busan, Korea, November-December 2006. Springer-Verlag.
396. Serge Vaudenay. On Privacy Models for RFID. In *Advances in Cryptology - Asiacrypt 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 68–87, Kuching, Malaysia, December 2007. Springer-Verlag.
397. Serge Vaudenay and Martin Vuagnoux. About Machine-Readable Travel Documents. In *ICS’07*, Lecture Notes in Computer Science. Springer, 2007.
398. Roel Verdult. Security analysis of RFID tags, 2008.
399. Markus Vogt, Axel Poschmann, and Christof Paar. Cryptography is Feasible on 4-Bit Microcontrollers - A Proof of Concept. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
400. 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.
401. 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.
402. Stephen Weis. Security and Privacy in Radio-Frequency Identification Devices. Master thesis, Massachusetts Institute of Technology (MIT), MIT, Massachusetts, USA, May 2003.
403. 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 Press.
404. Stephen Weis. *New Foundations for Efficient Authentication, Commutative Cryptography, and Private Disjointness Testing*. PhD thesis, MIT, Cambridge, Massachusetts, USA, May 2006.
405. 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-Verlag.
406. Johannes Wolkerstorfer. Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto, July 2005.
407. Kirk Wong, Patrick Hui, and Allan Chan. Cryptography and Authentication on RFID Passive Tags for Apparel Products. *Computers in Industry*, May 2006.

408. Jiang Wu and Doug Stinson. How to Improve Security and Reduce Hardware Demands of the WIPR RFID Protocol. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
409. Jiang Wu and Douglas R. Stinson. A Highly Scalable RFID Authentication Protocol. In *Proceedings of the 14th Australasian Conference on Information Security and Privacy – ACISP’09*, Brisbane, Australia, July 2009.
410. 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*, pages 51–57, April 2008.
411. 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.
412. 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-Verlag.
413. Bongno Yoon. HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA, April 2009.
414. 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.
415. 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.
416. 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-Verlag.
417. 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-Verlag.
418. Xiaolan Zhang and Brian King. Modeling RFID Security. In Dengguo Feng, Dongdai Lin, and Moti Yung, editors, *Conference on Information Security and Cryptology – CISC 2005*, volume 3822 of *Lecture Notes in Computer Science*, pages 75–90, Beijing, China, December 2005. Springer-Verlag.
419. Huafei Zhu and Feng Bao. Aggregating Symmetric/Asymmetric Attestations. *IEEE International Conference on RFID*, pages 105–110, April 2008.
420. Yanjun Zuo. RFID Survivability Quantification and Attack Modeling (short paper). In *3rd ACM Conference on Wireless Network Security – WiSec’10*, Hoboken, New Jersey, USA, March 2010.