Conference on Information Security and Privacy, ACISP'05, LNCS 3574, pp. 184–194, 2005.

[78] C. Rolfes, A. Poschmann, G. Leander and C. 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*, LNCS 5189, pp. 89–103, 2008.

[79] A. Shamir, Memory efficient variants of public-key schemes for smart card applications, *Advances in Cryptology, EUROCRYPT'94*, LNCS 950, pp. 445–449, 1995.

[80] A. Shamir, SQUASH – a new MAC with provable security properties for highly constrained devices such as RFID tags, *Fast Software Encryption, FSE'08*, LNCS 5086, pp. 144–157, 2008.

[81] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita and T. Shirai, Piccolo: an ultra-lightweight blockcipher, *Cryptographic Hardware and Embedded Systems, CHES'11*, LNCS 6917, pp. 342–357, 2011.

[82] B. Song and C.J. Mitchell, RFID authentication protocol for low-cost tags, *In Proceedings of the first ACM conference on Wireless network Security, WiSec'08*, pp. 140–147, 2008.

[83] O. Savry, F. Pebay-Peyroula, F. Dehmas, G. Robert and J. Reverdy, RFID noisy reader: how to prevent from eavesdropping on the communication? *Cryptographic Hardware and Embedded Systems, CHES'07*, LNCS 4727, pp. 334–345, 2007.

[84] N. Saxena and J. Voris, We can remember it for you wholesale: implications of data remanence on the use of RAM for true random number generation on RFID tags, *Workshop on RFID Security, RFIDSec'09*, pp. 1–13, 2009.

[85] G. Tsudik, YA-TRAP: yet another trivial RFID authentication protocol, *International Conference on Pervasive Computing and Communications, Percom'06*, pp. 640–643, 2006.

[86] R. Trujillo-Rasua, B. Martin and G. Avoine, The Poulidor distance-bounding protocol, *Workshop on RFID Security, RFIDSec'10*, LNCS 6370, pp. 239–257, 2010.

[87] S.A. Weis, Security and privacy in radio-frequency identification devices, *Master Thesis, Massachusetts Institute of Technology*, pp. 49–51, 2003.

[88] A.D. Wyner, The wire-tap channel, *Bell Systems Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[89] J. Wu and D.R. Stinson, How to improve security and reduce hardware demands of the WIPR RFID protocol, *IEEE International Conference on RFID, RFID'09*, pp. 192–199, 2009.

[90] D.H. Yum, J.S. Kim, S.J. Hong and P.J. Lee, Distance bounding protocol for mutual authentication, *Wireless Communications, IEEE Transactions on*, vol. 10, no. 2, pp. 592–601, 2011.

[91] D. Zanetti, B. Danev and S. Capkun, Physical-layer identification of UHF RFID tags, *In Proceedings of the sixteenth annual International Conference on Mobile Computing and Networking, MobiCom'10*, pp. 353–364, 2010.

[92] B. Zhu and G. Gong, Guess-then-meet-in-the-middle attacks on the KTANTAN family of block ciphers, *Cryptology ePrint Archive, Report 2011/619*, pp. 1–14, 2011.

[93] D. Zanetti, P. Sachs and S. Capkun, On the practicality of UHF RFID fingerprinting: how real is the RFID tracking problem, *Privacy Enhancing Technologies, PET'11*, LNCS 6794, pp. 97–116, 2011.