**REFFERENCES**

[1] J. Carter and M. Wegman, “Universal classes of hash functions,” in Proceedings of the ninth annual ACM symposium on Theory of computing–STOC’77. ACM, 1977, pp. 106–112.

[2] M. Wegman and J. Carter, “New classes and applications of hash functions,” in 20th Annual Symposium on Foundations of Computer Science–FOCS’79. IEEE, 1979, pp. 175–182.

[3] L. Carter and M. Wegman, “Universal hash functions,” Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979.

[4] M. Wegman and L. Carter, “New hash functions and their use in authentication and set equality,” Journal of Computer and System Sciences, vol. 22, no. 3, pp. 265–279, 1981.

[5] J. Bierbrauer, “A2-codes from universal hash classes,” in Advances in Cryptology–EUROCRYPT’95, vol. 921, Lecture Notes in Computer Science. Springer, 1995, pp. 311–318.

[6] M. Atici and D. Stinson, “Universal Hashing and Multiple Authentication,” in Advances in Cryptology–CRYPTO’96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 16–30.

[7] T. Helleseth and T. Johansson, “Universal hash functions from exponential sums over finite fields and Galois rings,” in Advances in cryptology– CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 31–44.

[8] V. Shoup, “On fast and provably secure message authentication based on universal hashing,” in Advances in Cryptology–CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 313–328.

[9] J. Bierbrauer, “Universal hashing and geometric codes,” Designs, Codes and Cryptography, vol. 11, no. 3, pp. 207–221, 1997.

[10] B. Alomair, A. Clark, and R. Poovendran, “The Power of Primes: Security of Authentication Based on a Universal Hash-Function Family,” Journal of Mathematical Cryptology, vol. 4, no. 2, 2010.

[11] B. Alomair and R. Poovendran, “E-MACs: Towards More Secure and More Efficient Constructions of Secure Channels,” in the 13th International Conference on Information Security and Cryptology – ICISC’10. Springer, 2010.

[12] FIPS 113, “Computer Data Authentication,” Federal Information Processing Standards Publication, 113, 1985.

[13] ISO/IEC 9797-1, “Information technology – Security techniques –Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher,” 1999.

[14] M. Dworkin, “Recommendation for block cipher modes of operation: The CMAC mode for authentication,” 2005.

[15] T. Iwata and K. Kurosawa, “omac: One-key cbc mac,” in Fast Software Encryption–FSE’03, vol. 2887, Lecture notes in computer science. Springer, 2003, pp. 129–153.

[16] M. Bellare, R. Guerin, and P. Rogaway, “XOR MACs: New methods for message authentication using finite pseudorandom functions,” in Advances in Cryptology–CRYPTO’95, vol. 963, Lecture Notes in Computer Science. Springer, 1995, pp. 15–28.

[17] P. Rogaway and J. Black, “PMAC: Proposal to NIST for a parallelizable message authentication code,” 2001.

[18] M. Bellare, J. Kilian, and P. Rogaway, “The Security of the Cipher Block Chaining Message Authentication Code,” Journal of Computer and System Sciences, vol. 61, no. 3, pp. 362–399, 2000.

[19] B. Preneel and P. Van Oorschot, “On the security of iterated message authentication codes,” IEEE Transactions on Information theory, vol. 45, no. 1, pp. 188–199, 1999.

[20] P. Rogaway, “Comments on NISTs RMAC Proposal,” 2002.

[21] G. Tsudik, “Message authentication with one-way hash functions,” ACM SIGCOMM Computer Communication Review, vol. 22, no. 5, p. 38, 1992.

[22] M. Bellare, R. Canetti, and H. Krawczyk, “Keying Hash Functions for Message Authentication,” in Advances in Cryptology–CRYPTO’96, vol. 96, Lecture Notes in Computer Science. Springer, 1996, pp. 1–15.

[23] FIPS 198, “The Keyed-Hash Message Authentication Code (HMAC),” Federal Information Processing Standards Publication, vol. 198, 2002.

[24] B. Preneel and P. Van Oorschot, “MDx-MAC and building fast MACs from hash functions,” in Advances in Cryptology-CRYPTO’95, vol. 963, Lecture Notes in Computer Science. Springer, 1995, pp. 1–14.

[25] ISO/IEC 9797-2, “Information technology – Security techniques –Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function,” 2002.

[26] A. Bosselaers, R. Govaerts, and J. Vandewalle, “Fast hashing on the Pentium,” in Advances in Cryptology-CRYPTO’96, vol. 1109, Lecture Notes in Computer Science. Springer, 1996, pp. 298–312.

[27] J. Black, S. Halevi, H. Krawczyk, T. Krovetz, and P. Rogaway, “UMAC:Fast and Secure Message Authentication,” in Advances in Cryptology–CRYPTO’99, vol. 1666, Lecture Notes in Computer Science. Springer, 1999, pp. 216–233.

[28] D. Bernstein, “The Poly1305-AES message-authentication code,” in Proceedings of Fast Software Encryption–FSE’05, vol. 3557, Lecture Notes in Computer Science. Springer, 2005, pp. 32–49.

[29] D. McGrew and J. Viega, “The security and performance of the Galois/Counter Mode (GCM) of operation,” in Progress in Cryptology- INDOCRYPT’04, vol. 3348, Lecture notes in computer science. Springer, 2004, pp. 343–355.

[30] S. Halevi and H. Krawczyk, “MMH: Software message authentication in the Gbit/second rates,” in Proceedings of Fast Software Encryption– FSE’97, vol. 1267, Lecture notes in computer science. Springer, 1997,pp. 172–189.

[31] M. Etzel, S. Patel, and Z. Ramzan, “Square hash: Fast message authentication

via optimized universal hash functions,” in Advances in Cryptology–CRYPTO’99, vol. 1666, Lecture Notes in Computer Science. Springer, 1999, pp. 234–251.

[32] J. Kaps, K. Yuksel, and B. Sunar, “Energy scalable universal hashing,” IEEE Transactions on Computers, vol. 54, no. 12, pp. 1484–1495, 2005.

[33] D. Bernstein, “Floating-point arithmetic and message authentication,” Available at http:// cr.yp.to/hash127.html, 2004.

[34] H. van Tilborg, Encyclopedia of cryptography and security. Springer, 2005.

[35] T. Krovetz, “http://fastcrypto.org/umac/,” 2006.

[36] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey,” Computer networks, vol. 38, no. 4, pp. 393–422, 2002.

[37] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, “SPINS: Security protocols for sensor networks,” Wireless networks, vol. 8, no. 5, pp. 521–534, 2002.

[38] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless s Sensor networks,” Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.

[39] EPCglobal Inc., “Class-1 generation-2 uhf radio frequency identification protocol standard version 1.2.0,” 2008.

[40] S. Sarma, S. Weis, and D. Engels, “RFID systems and security and privacy implications,” Cryptographic Hardware and Embedded Systems-CHES 2002, pp. 1–19, 2003.

[41] A. Juels, “RFID security and privacy: A research survey,” IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 381–394, 2006.

[42] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda, “RFID systems: A survey on security threats and proposed solutions,” in Personal Wireless Communications. Springer, 2006, pp. 159–170.

[43] Y. Zhang, “A design proposal of security architecture for medical body sensor networks,” in Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on. IEEE, 2006, pp. 4–90.

[44] K. Venkatasubramanian, A. Banerjee, and S. Gupta, “Ekg-based key agreement in body sensor networks,” in INFOCOM Workshops 2008, IEEE. IEEE, 2008, pp. 1–6.

[45] C. Tan, H. Wang, S. Zhong, and Q. Li, “Body sensor network security: an identity-based cryptography approach,” in Proceedings of the first ACM conference on Wireless network security. ACM, 2008, pp. 148–153.

[46] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, “Strong Authentication for RFID Systems using the AES Algorithm,” in Cryptographic Hardware and Embedded Systems–CHES’04, vol. 3156, Lecture Notes in Computer Science. Springer, 2004, pp. 357–370.

[47] C. H. Lim and T. Korkishko, “mCrypton - A Lightweight Block Cipher For Security of Low-Cost RFID Tags and Sensors,” in Workshop on Information Security Applications–WISA’05, ser. Lecture Notes in Computer Science, vol. 3786. Springer, 2005, pp. 243–258.

[48] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim, and S. Chee, “HIGHT: A New Block Cipher Suitable for Low-Resource Device,” in Cryptographic Hardware and Embedded Systems–CHES’06, ser. Lecture Notes in Computer Science, vol. 4249. Springer, 2006, pp. 46–59.

[49] A. Poschmann, G. Leander, K. Schramm, and C. Paar, “A Family of Light-Weight Block Ciphers Based on DES Suited for RFID Applications,” in Workshop on RFID Security–RFIDSec’06. Ecrypt, 2006.

[50] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw,

Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” in Cryptographic Hardware and Embedded Systems– CHES’07, vol. 4727, Lecture Notes in Computer Science. Springer, 2007, pp. 450–466.

[51] F. Mac´e, F.-X. Standaert, and J.-J. Quisquater, “ASIC Implementations

of the Block Cipher SEA for Constrained Applications,” in Workshop on RFID Security–RFIDSec’07, 2007.

[52] M. O’Neill (McLoone), “Low-Cost SHA-1 Hash Function Architecture for RFID Tags,” in Workshop on RFID Security–RFIDSec’08, 2008.

[53] A. Shamir, “SQUASH–A New MAC with Provable Security Properties for Highly Constrained Devices Such as RFID Tags,” in Fast Software Encryption–FSE’08, vol. 5086, Lecture Notes in Computer Science. Springer, 2008, pp. 144–157.

[54] A. Bogdanov, G. Leander, C. Paar, A. Poschmann, M. Robshaw, and Y. Seurin, “Hash Functions and RFID Tags : Mind The Gap,” in Proceedings of the 10th International Workshop Cryptographic Hardware and Embedded Systems–CHES’08, ser. Lecture Notes in Computer Science, vol. 5154. Springer, 2008, pp. 283–299.

[55] E. B. Kavun and T. Yalcin, “A Lightweight Implementation of Keccak Hash Function for Radio-Frequency Identification Applications,” in Workshop on RFID Security–RFIDSec’10, 2010.

[56] O. Goldreich, Foundations of Cryptography. Cambridge University Press, 2001.

[57] S. Goldwasser and S. Micali, “Probabilistic encryption,” Journal of Computer and System Sciences, vol. 28, no. 2, pp. 270–299, 1984.

[58] T. Kohno, J. Viega, and D. Whiting, “CWC: A high-performance conventional authenticated encryption mode,” in Fast Software Encryption– FSE’04, vol. 3017, Lecture Notes in Computer Science. Springer, 2004, pp. 408–426.

[59] M. Luby and C. Rackoff, “How to Construct Pseudorandom Permutations

from Pseudorandom Functions,” SIAM Journal on Computing, vol. 17, pp. 373–386, 1988.

[60] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, “A concrete security treatment of symmetric encryption,” in 38th Annual Symposium on Foundation of Computer Science–FOCS’97. IEEE Computer Society, 1997, pp. 394–403.

[61] J. Daemen and V. Rijmen, The design of Rijndael: AES–the Advanced

Encryption Standard. Springer Verlag, 2002.

[62] S. Schwarz, “The role of semigroups in the elementary theory of numbers,” Math. Slovaca, vol. 31, no. 4, pp. 369–395, 1981.

[63] Z. Liu and D. Peng, “True Random Number Generator in RFID Systems Against Traceability,” in IEEE Consumer Communications and Networking Conference–CCNS,06, vol. 1. IEEE, 2006, pp. 620–624.

[64] D. Holcom,W. Burleson, and K. Fu, “Initial SRAM state as a Fingerprint and Source of True Random Numbers for RFID Tags,” in Workshop on RFID Security–RFIDSec’07, 2007.

[65] D. Holcomb, W. Burleson, and K. Fu, “Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers,” IEEE Transactions on Computers, vol. 58, no. 9, 2009.

[66] C. Petrie and J. Connelly, “A noise-based IC random number generator for applications in cryptography,” IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 47, no. 5, pp. 615–621, 2000.

[67] S. Callegari, R. Rovatti, and G. Setti, “Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos,” IEEE Transactions on Signal Processing, vol. 53, no. 2 Part 2, pp. 793–805, 2005.

[68] A. Francillon, C. Castelluccia, and P. Inria, “TinyRNG: A cryptographic random number generator for wireless sensors network nodes,” in Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks– WiOpt’07. Citeseer, 2007, pp. 1–7.

[69] J. Nakajima and M. Matsui, “Performance analysis and parallel implementation of dedicated hash functions,” in Advances in Cryptology– EUROCRYPT 2002. Springer, 2002, pp. 165–180.

[70] B. Preneel, “Using Cryptography Well,” Printed handout available at http://secappdev.org/handouts/2010/Bart%20Preneel/using crypto well

pdf, 2010.

[71] J. Großsch¨adl, R. Avanzi, E. Savas¸, and S. Tillich, “Energy-efficient software implementation of long integer modular arithmetic,” in Proceedings of the 7th international conference on Cryptographic hardware and embedded systems – CHES’05, vol. 3659. Springer-Verlag, 2005, pp. 75–90.

[72] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, and T. Kohno, “Helix: Fast encryption and authentication in a single cryptographic primitive,” in Proceedings of Fast Software Encryption–FSE’03, vol. 2887, Lecture notes in computer science. Springer, 2003, pp. 330–346.

[73] D. Whiting, B. Schneier, S. Lucks, and F. Muller, “Phelix-fast encryption and authentication in a single cryptographic primitive, eSTREAM,” ECRYPT Stream Cipher Project, Report 2005/020, [www.ecrypt.eu.org/](http://www.ecrypt.eu.org/) stream, 2005.

[74] F. Muller, “Differential attacks against the Helix stream cipher,” in Fast Software Encryption–FSE’04, vol. 3017, Lecture Notes in Computer Science. Springer, 2004, pp. 94–108.

[75] S. Paul and B. Preneel, “Solving systems of differential equations of addition,” in Australasian Conference on Information Security and Privacy–ICISP’05, vol. 3574, Lecture Notes in Computer Science. Springer, 2005, pp. 75–88.

[76] ——, “Near Optimal Algorithms for Solving Differential Equations of Addition with Batch Queries,” in Progress in Cryptology– INDOCRYPT’05, vol. 3797, Lecture Notes in Computer Science. Springer, 2005, pp. 90–103.

[77] H. Wu and B. Preneel, “Differential-linear attacks against the stream cipher Phelix,” in Fast Software Encryption–FSE’07, vol. 4593, Lecture Notes in Computer Science. Springer, 2007, pp. 87–100.

[78] D. Stinson, Cryptography: Theory and Practice. CRC Press, 2006.

[79] M. Bellare and C. Namprempre, “Authenticated Encryption: Relations Among Notions and Analysis of the Generic Composition Paradigm,” Journal of Cryptology, vol. 21, no. 4, pp. 469–491, 2008.

[80] J. Katz and Y. Lindell, Introduction to modern cryptography. Chapman

& Hall/CRC, 2008.

[81] M. F¨urer, “Faster integer multiplication,” in ACM symposium on Theory of computing–STOC’07. ACM, 2007, p. 66.

[82] C. Jutla, “Encryption modes with almost free message integrity,” Journal

of Cryptology, vol. 21, no. 4, pp. 547–578, 2008.

[83] P. Rogaway, M. Bellare, and J. Black, “OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption,” ACM Transactions on Information and System Security, vol. 6, no. 3, pp. 365–403, 2003.

[84] A. Menezes, P. Van Oorschot, and S. Vanstone, Handbook of applied cryptography. CRC, 1997.

[85] B. Alomair and R. Poovendran, “Efficient Authentication for Mobile and Pervasive Computing,” in The 12th International Conference on Information and Communications Security–ICICS’10. Springer, 2010.