Cryptography: General

[1] Alex Biryukov, Praveen Gauravaram, Jian Guo, Dmitry Khovratovich, San Ling, Krystian Matusiewicz, Ivica Nikolić, Josef Pieprzyk, and Huaxiong Wang, *Cryptanalysis of the LAKE hash family*, Fast Software Encryption, Lecture Notes in Computer Science, vol. 5665, Springer, Berlin, 2009, pp. 156–179.

[2] Carl Bracken, Eimear Byrne, Nadya Markin, and Gary McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials*, Finite Fields Appl. **14** (2008), no. 3, 703–714. MR MR2435056

[3] An Braeken, Christopher Wolf, and Bart Preneel, *Classification of highly nonlinear Boolean power functions with a randomised algorithm for checking normality*, 2004.

[4] Marcus Brinkmann and Gregor Leander, *On the classification of APN functions up to dimension five*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 273–288. MR MR2438456

[5] Johannes Buchmann, Carlos Coronado, Martin Dring, Daniela Engelbert, Christoph Ludwig, Raphael Overbeck, Arthur Schmidt, Ulrich Vollmer, and Ralf-Philipp Weinmann, *Post-quantum signatures*, 2004.

[6] Kelley Burgin, *The nonexistence of a bijective almost perfect nonlinear function of order 16*, Master's thesis, Auburn University, Alabama, 2002.

[7] Denis Charles, Kamal Jain, and Kristin Lauter, *Signatures for network coding*, International Journal of Information and Coding Theory **1** (2009), no. 1, 3–14.

[8] Mihai Cipu, *Dickson polynomials that are permutations*, Serdica Math. J. **30** (2004), no. 2-3, 177–194. MR MR2098331 (2005g:11244)

[9] Scott Contini and Igor E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.

[10] Scott Contini and Yiqun Lisa Yin, *Improved cryptanalysis of securID*, 2003.

[11] _____, *Fast software-based attacks on SecurID*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3017, Springer-Verlag, 2004, pp. 454–471.

[12] Deepak Dalai, *On some necessary conditions of boolean functions to resist algebraic attacks*, Ph D thesis, Indian Statistical Institute, Kolkata, India, 2006.

[13] Alexander W. Dent and Steven D. Galbraith, *Hidden pairings and trapdoor DDH groups*, Algorithmic Number Theory (Berlin, 2006), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2006, p. pp.15.

[14] Jintai Ding, Bo-Yin Yang, Chia-Hsin Owen Chen, Ming-Shing Chen, and Chen-Mou Cheng, *New differential-algebraic attacks and reparametrization of Rainbow*, Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol. 5037, Springer, 2008, pp. 242–257.

[15] D.G. Farmer and K.J. Horadam, *Presemifield bundles over GF(p^3)*, IEEE International Symposium on Information Theory, 2008. ISIT 2008 (2008), 2613–2616.

[16] Steven D. Galbraith, Colm Ó hÉigeartaigh, and Caroline Sheedy, *Simplified pairing computation and security implications*, J. Math. Cryptol. **1** (2007), no. 3, 267–281. MR MR2372156 (2009a:94027)

[17] Willi Geiselmann and Rainer Steinwandt, *Cryptanalysis of a hash function proposed at ICISC 2006*, Information Security and Cryptology - ICISC 2007, Lecture Notes in Computer Science, vol. 4817/2007, Springer Berlin / Heidelberg, 2007, pp. 1–10.

[18] Willi Geiselmann, Rainer Steinwandt, and Thomas Beth, *Attacking the affine parts of SFLASH*, Cryptography and Coding, Lecture Notes in Comput. Sci., vol. 2260, Springer, Berlin, 2001, pp. 355–359. MR MR2074529

[19] ———, *Revealing the affine parts of SFLASHv1, SFLASHv2, and FLASH*, Actas de la VII Reunisn Espaqola de Criptologma y Seguridad de la Informacisn, vol. 7, 2002, pp. 305–314.

[20] Markus Grassl and Rainer Steinwandt, *Cryptanalysis of an authentication scheme using truncated polynomials*, 2008.

[21] K. J. Horadam and D. G. Farmer, *Bundles, presemifields and nonlinear functions*, Des. Codes Cryptogr. **49** (2008), no. 1-3, 79–94. MR MR2438442

[22] Georg Illies and Marian Margraf, *Attacks on the ESA-PSS-04-151 MAC scheme*, Selected Areas in Cryptography, Lecture Notes in Computer Science, vol. 4876/2007, Springer Berlin / Heidelberg, 2007, pp. 296–310.

[23] Mariusz Jakubowski, Prasad Naldurg, Vijay Patankar, and Ramarathnam Venkatesan, *Software integrity checking expressions (ICEs) for robust tamper detection*, Information Hiding, Lecture Notes in Computer Science, vol. 4567, 2008, pp. 96–111.

[24] Gohar M. Kyureghyan and Alexander Pott, *On the linear complexity of the Sidelnikov-Lempel-Cohn-Eastman sequences*, Proceedings of the Conference on Finite Geometries (Oberwolfach, 2001), vol. 29, 2003, pp. 149–164. MR MR1993164 (2004g:94036)

[25] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.

[26] Bart Preneel (ed.), *Advances in Cryptology—Eurocrypt 2000*, Lecture Notes in Computer Science, vol. 1807, Berlin, Springer-Verlag, 2000. MR MR1772020 (2001b:94028)

[27] N. P. Smart, *Attacks on asymmetric cryptosystems: An analysis of Goubin's refined power analysis attack*, Cryptographic Hardware and Embedded Systems, Lecture Notes in Comput. Sci., vol. 2779, Springer, Berlin, 2003, pp. 281–290.

[28] Rainer Steinwandt, Markus Grassl, Willi Geiselmann, and Thomas Beth, *Weakness in the* $\mathrm{SL}_2(F_{2^n})$ *hashing scheme*, Advances in Cryptology—CRYPTO 2000 (Santa Barbara, CA), Lecture Notes in Comput. Sci., vol. 1880, Springer, Berlin, 2000, pp. 287–299. MR MR1850050 (2002i:94053)