Block Ciphers

[1] Martin Albrecht, *Algebraic attacks on the Courtois Toy cipher*, Cryptologia **32** (2008), no. 3, 220–276.

[2] Martin Albrecht and Carlos Cid, *Algebraic techniques in differential cryptanalysis*, Fast Software Encryption (Orr Dunkelman, ed.), Lecture Notes in Computer Science, vol. 5665, Springer, 2009, pp. 193–208.

[3] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727/2007, Springer Berlin / Heidelberg, 2007, pp. 450–466.

[4] Andrey Bogdanov and Andrey Pyshkin, *Algebraic side-channel collision attacks on AES*, 2007.

[5] Johannes Buchmann, Andrei Pyshkin, and Ralf-Philipp Weinmann, *Block ciphers sensitive to Gröbner basis attacks*, Topics in Cryptology—CT-RSA 2006, Lecture Notes in Comput. Sci., vol. 3860, Springer, Berlin, 2006, pp. 313–331. MR MR2243996 (2007e:94052)

[6] Stanislav Bulygin and Michael Brickenstein, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, 2008.

[7] ———, *Obtaining and solving systems of equations in key variables only for the small variants of AES*, Math. Comput. Sci. **3** (2010), no. 2, 185–200.

[8] Chris Charnes, Martin Rötteler, and Thomas Beth, *On homogeneous bent functions*, Applied Algebra, Algebraic Algorithms and Error-correcting Codes (Melbourne, 2001), Lecture Notes in Comput. Sci., vol. 2227, Springer, Berlin, 2001, pp. 249–259. MR MR1913471 (2003e:94065)

[9] ———, *Homogeneous bent functions, invariants, and designs*, Des. Codes Cryptogr. **26** (2002), no. 1-3, 139–154. MR MR1919874 (2003h:05043)

[10] C. Cid, S. Murphy, and M. Robshaw, *Computational and algebraic aspects of the advanced encryption standard*, Seventh International Workshop on Computer Algebra in Scientific Computing, CASC 2004, St. Petersburg, Russia, 2004, pp. 93–103.

[11] ———, *Small scale variants of the AES*, LNCS 3557, Eds. Gilbert, H. and Handschuh, H., Springer, 2005, pp. 145–162.

[12] Carlos Cid, Sean Murphy, and Matthew Robshaw, *Algebraic Aspects of the Advanced Encryption Standard*, Springer, New York, 2006. MR MR2250327

[13] Nicolas T. Courtois and Gregory V. Bard, *Algebraic cryptanalysis of the data encryption standard*, Cryptography and Coding, Lecture Notes in Computer Science, vol. 4887/2007, Springer Berlin / Heidelberg, 2007, pp. 152–169.

[14] Nicolas T. Courtois, Gregory V. Bard, and David Wagner, *Algebraic and slide attacks on KeeLoq*, 2007.

[15] Jintai Ding, Bo-Yin Yang, Chen-Mou Cheng, Owen Chen, and Vivien Dubois, *Breaking the symmetry: A way to resist the new differential attack*, 2007.

[16] Tobias Eibach, Gunnar Völkel, and Enrico Pilz, *Optimising Gröbner bases on Bivium*, Math. Comput. Sci. **3** (2010), no. 2, 159–172.

[17] Jeremy Erickson, Jintai Ding, and Chris Christensen, *Algebraic cryptanalysis of SMS4: Gröbner basis attack and SAT attack compared*, Information, Security and Cryptology – ICISC 2009 (Donghoon Lee and Seokhie Hong, eds.), Lecture Notes in Computer Science, vol. 5984, Springer Berlin/Heidelberg, 2010, pp. 73–86.

[18] Jean-Charles Faugére and Ludovic Perret, *Algebraic cryptanalysis of Curry and Flurry using correlated messages*, 2008.

[19] Willi Geiselmann and Rainer Steinwandt, *A short comment on the affine parts of SFLASHv3*, 2003.

[20] Krystian Matusiewicz, Scott Contini, and Josef Pieprzyk, *Weaknesses of the fork-256 compression function*, 2006, pp. 1–21.

[21] Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede, *A systematic evaluation of compact hardware implementations for the Rijndael S-box*, Topics in Cryptology—CT-RSA 2005, Lecture Notes in Comput. Sci., vol. 3376, Springer, Berlin, 2005, pp. 323–333. MR MR2174386

[22] Sean Simmons, *Algebraic cryptanalysis of simplified AES**, Cryptologia **33** (2009), no. 4, 305–314.