Bibliography

[1] Gregory V. Bard. *Algebraic Cryptanalysis*. Springer-Verlag, 2009.

[2] Gregory V. Bard, Nicolas T. Courtois, and Chris Jefferson. Efficient methods for conversion and solution of sparse systems of low-degree multivariate polynomials over gf(2) via sat-solvers. Cryptology ePrint Archive, Report 2007/024, 2007.

[3] Claude Carlet. Boolean functions for cryptography and error correcting codes. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 2:257, 2010.

[4] Claude Carlet. Comments on" constructions of cryptographically significant boolean functions using primitive polynomials. *Information Theory, IEEE Transactions on*, 57(7):4852–4853, 2011.

[5] Nicolas T. Courtois and Willi Meier. Algebraic attacks on stream ciphers with linear feedback. In *Proceedings of the 22Nd International Conference on Theory and Applications of Cryptographic Techniques*, EUROCRYPT'03, pages 345–359, Berlin, Heidelberg, 2003. Springer-Verlag.

[6] Nicolas T. Courtois and Karsten Nohl. Algebraic attacks on the crypto-1 stream cipher in mifare classic and oyster cards. *Cryptology ePrint Archive, Report 2008/166*, 2008.

[7] Nicolas T. Courtois, Sean O'neil, and Jean Jacques Quisquater. Practical algebraic attacks on the hitag2 stream cipher. In *Information Security Conference*. Springer-Verlag, September 2009.

[8] Niklas Eén and Niklas Sörensson. An extensible sat-solvers. In *Theory and applications of satisfiability testing*, volume 2919, pages 502 – 518. Springer Berlin Heidelberg, 2004.

[9] Simon Fischer. Analysis of lightweight stream ciphers. Master's thesis, Ecole Polytechnique Federale De Lausanne, April 2008.

[10] Flavio D. Garcia, Gerhard Koning Gans, Ruben Muijrers, Peter Rossum, Roel Verdult, Ronny Wichers Schreur, and Bart Jacobs. Dismantling mifare classic. In *Proceedings of the 13th European Symposium on Research in Computer Security: Computer Security*, ESORICS '08, pages 97–114, Berlin, Heidelberg, 2008. Springer-Verlag.

[11] Flavio D. Garcia, Peter van Rossum, Roel Verdult, and Ronny Wichers Schreur. Wirelessly pickpocketing a mifare classic card. In *Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*, SP '09, pages 3–15, Washington, DC, USA, 2009. IEEE Computer Society.

[12] Anup Hosangadi, Farzan Fallah, and Ryan Kastner. Optimizing polynomial expressions by algebraic factorization and common subexpression elimination. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 25(10):2012–2022, 2006.

[13] http://www.nxp.com. *MF1PLUS8001 - Mainstream contactless smart card IC for fast and easy solution development*, 1.0 edition, September 2008.

[14] http://www.nxp.com. *MF1S503x - MIFARE Classic 1K - Mainstream contactless smart card IC for fast and easy solution development*, rev. 3.1 edition, February 2011 2011.

[15] Meicheng Liu, Yin Zhang, and Dongdai Lin. Perfect algebraic immune functions. In *Advances in Cryptology–ASIACRYPT 2012*, pages 172–189. Springer, 2012.

[16] Karsten Nohl. Cryptanalysis of crypto-1. *Computer Science Department University of Virginia, White Paper*, 2008.

[17] Karsten Nohl. Disclosing secret algorithms from hardware, 2008.

[18] Mate Soos. Privacy-preserving security protocols for rfids. Master's thesis, Institut Polytechnique de Grenoble, 6 October 2009.

[19] Mate Soos. Grain of salt - an automated way to test stream ciphers through sat solvers. *Workshop on Tools for Cryptanalysis*, June, 2010.

[20] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending sat solvers to cryptographic problems. In *Theory and Applications of Satisfiability Testing-SAT*, pages 244–257. Springer Berlin Heidelberg, 2009.

[21] Whitney J Townsend and Mitchell A Thornton. Walsh spectrum computations using cayley graphs. *spectrum*, 15(11):5, 2001.

[22] Qichun Wang, Jie Peng, Haibin Kan, and Xiangyang Xue. Constructions of cryptographically significant boolean functions using primitive polynomials. *Information Theory, IEEE Transactions on*, 56(6):3048–3053, 2010.