Krause, Matthias; **Hamann, Matthias**

The cryptographic power of random selection. (English) Zbl 1292.94096

Miri, Ali (ed.) et al., Selected areas in cryptography. 18th international workshop, SAC 2011, Toronto, ON, Canada, August 11–12, 2011. Revised selected papers. Berlin: Springer (ISBN 978-3-642-28495-3/pbk). Lecture Notes in Computer Science 7118, 134-150 (2012).

Summary: The principle of random selection and the principle of adding biased noise are new paradigms used in several recent papers for constructing lightweight RFID authentication protocols. The cryptographic power of adding biased noise can be characterized by the hardness of the intensively studied Learning Parity with Noise (LPN) Problem. In analogy to this, we identify a corresponding learning problem for random selection and study its complexity. Given L secret linear functions $f_1, \ldots, f_L : \{0,1\}^n \longrightarrow \{0,1\}^a$, $RandomSelect\,(L, n, a)$ denotes the problem of learning $f_1, \cdots, f_L$ from values $(u, f_l\,(u))$, where the secret indices $l \in \{1, \cdots, L\}$ and the inputs $u \in \{0,1\}^n$ are randomly chosen by an oracle. We take an algebraic attack approach to design a nontrivial learning algorithm for this problem, where the running time is dominated by the time needed to solve full-rank systems of linear equations over $O\left(n^L\right)$ unknowns. In addition to the mathematical findings relating correctness and average running time of the suggested algorithm, we also provide an experimental assessment of our results.

For the entire collection see [Zbl 1234.94005].

MSC:

94A60 Cryptography

Keywords:

Lightweight Cryptography; Algebraic Attacks; Algorithmic Learning; Foundations and Complexity Theory

Software:

KATAN; KTANTAN; Magma; PRESENT

Full Text: DOI

References:

[1] Armknecht, F., Krause, M.: Algebraic Attacks on Combiners with Memory. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol.˜2729, pp. 162–175. Springer, Heidelberg (2003) · Zbl 1122.94346 · doi:10.1007/978-3-540-45146-4_10

[2] Arora, S., Ge, R.: New algorithms for learning in presence of errors (submitted, 2010), http://www.cs.princeton.edu/˜rongge/LPSN.pdf · Zbl 1332.68099

[3] Blass, E.-O., Kurmus, A., Molva, R., Noubir, G., Shikfa, A.: The F f -family of protocols for RFID-privacy and authentication. In: 5th Workshop on RFID Security, RFIDSec 2009 (2009)

[4] Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol.˜4727, pp. 450–466. Springer, Heidelberg (2007) · Zbl 1142.94334 · doi:10.1007/978-3-540-74735-2_31

[5] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput.˜24(3-4), 235–265 (1997) · Zbl 0898.68039 · doi:10.1006/jsco.1996.0125

[6] Bringer, J., Chabanne, H.: Trusted-HB: A low cost version of HB\ +\ secure against a man-in-the-middle attack. IEEE Trans. Inform. Theor.˜54, 4339–4342 (2008) · Zbl 1322.94096 · doi:10.1109/TIT.2008.928290

[7] Cichoń, J., Klonowski, M., Kutyłowski, M.: Privacy Protection for RFID with Hidden Subset Identifiers. In: Indulska, J., Patterson, D.J., Rodden, T., Ott, M. (eds.) PERVASIVE 2008. LNCS, vol.˜5013, pp. 298–314. Springer, Heidelberg (2008) · Zbl 05280589 · doi:10.1007/978-3-540-79576-6_18

[8] Courtois, N.: Fast Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol.˜2729, pp. 176–194. Springer, Heidelberg (2003) · Zbl 1122.94365 · doi:10.1007/978-3-540-45146-4_11

[9] Courtois, N., Meier, W.: Algebraic Attacks on Stream Ciphers with Linear Feedback. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol.˜2656, pp. 345–359. Springer, Heidelberg (2003) · Zbl 1038.94525 · doi:10.1007/3-540-39200-9_21

[10] De Cannière, C., Dunkelman, O., Knežević, M.: KATAN and KTANTAN – A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol.˜5747, pp. 272–288. Springer, Heidelberg (2009) · Zbl 1290.94060 · doi:10.1007/978-3-642-04138-9_20

[11] Gołębiewski, Z., Majcher, K., Zagórski, F.: Attacks on CKK Family of RFID Authentication Protocols. In: Coudert, D., Simplot-Ryl, D., Stojmenovic, I. (eds.) ADHOC-NOW 2008. LNCS, vol.˜5198, pp. 241–250. Springer, Heidelberg (2008) · Zbl 05487155 · doi:10.1007/978-3-540-85209-4_19

[12] Frumkin, D., Shamir, A.: Untrusted-HB: Security vulnerabilities of Trusted-HB. Cryptology ePrint Archive, Report 2009/044 (2009), http://eprint.iacr.org

[13] Gilbert, H., Robshaw, M.J.B., Seurin, Y.: HB#: Increasing the security and efficiency of HB\ +\ . In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol.˜4965, pp. 361–378. Springer, Heidelberg (2008) · Zbl 1149.94334 · doi:10.1007/978-3-540-78967-3_21

[14] Gilbert, H., Robshaw, M.J.B., Sibert, H.: Active attack against HB\ +\ : A provable secure lightweight authentication protocol. Electronic Letters˜41, 1169–1170 (2005) · doi:10.1049/el:20052622

[15] Goldreich, O., Levin, L.A.: A hard-core predicate for all one-way functions. In: Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing (STOC), pp. 25–32. ACM Press (1989) · doi:10.1145/73007.73010

[16] Hopper, N.J., Blum, M.: Secure Human Identification Protocols. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol.˜2248, pp. 52–66. Springer, Heidelberg (2001) · Zbl 1062.94549 · doi:10.1007/3-540-45682-1_4

[17] Juels, A., Weis, S.A.: Authenticating Pervasive Devices with Human Protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 293–308. Springer, Heidelberg (2005) · Zbl 1145.94470 · doi:10.1007/11535218_18

[18] Krause, M., Stegemann, D.: More on the Security of Linear RFID Authentication Protocols. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol.˜5867, pp. 182–196. Springer, Heidelberg (2009) · Zbl 1267.94077 · doi:10.1007/978-3-642-05445-7_12

[19] Krause, M., Hamann, M.: The cryptographic power of random selection. Cryptology ePrint Archive, Report 2011/511 (2011), http://eprint.iacr.org/

[20] Meier, W., Pasalic, E., Carlet, C.: Algebraic Attacks and Decomposition of Boolean Functions. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol.˜3027, pp. 474–491. Springer, Heidelberg (2004) · Zbl 1122.94041 · doi:10.1007/978-3-540-24676-3_28

[21] Ouafi, K., Overbeck, R., Vaudenay, S.: On the Security of HB# against a Man-in-the-Middle Attack. In: Pieprzyk, J. (ed.) ASIACRYPT 2008. LNCS, vol.˜5350, pp. 108–124. Springer, Heidelberg (2008) · Zbl 1206.94084 · doi:10.1007/978-3-540-89255-7_8

[22] Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing (STOC), pp. 84–93. ACM Press (2005) · Zbl 1192.94106 · doi:10.1145/1060590.1060603

[23] Courtois, N.T., Klimov, A.B., Patarin, J., Shamir, A.: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol.˜1807, pp. 392–407. Springer, Heidelberg (2000) · Zbl 1082.94514 · doi:10.1007/3-540-45539-6_27