Katz, Jonathan; **Shin, Ji Sun**

Parallel and concurrent security of the HB and HB$^+$ protocols. (English) Zbl 1140.94352

Vaudenay, Serge (ed.), Advances in cryptology – EUROCRYPT 2006. 25th annual international conference on the theory and applications of cryptographic techniques, St. Petersburg, Russia, May 28 – June 1, 2006. Proceedings. Berlin: Springer (ISBN 3-540-34546-9/pbk). Lecture Notes in Computer Science 4004, 73-87 (2006).

Summary: Juels and Weis (building on prior work of Hopper and Blum) propose and analyze two shared-key authentication protocols – HB and HB$^+$ – whose extremely low computational cost makes them attractive for low-cost devices such as radio-frequency identification (RFID) tags. Security of these protocols is based on the conjectured hardness of the "learning parity with noise" (LPN) problem: the HB protocol is proven secure against a passive (eavesdropping) adversary, while the HB$^+$ protocol is proven secure against active attacks.

Juels and Weis prove security of these protocols only for the case of *sequential* executions, and explicitly leave open the question of whether security holds also in the case of *parallel* or *concurrent* executions. In addition to guaranteeing security against a stronger class of adversaries, a positive answer to this question would allow the HB$^+$ protocol to be parallelized, thereby substantially reducing its round complexity.

Adapting a recent result by Regev, we answer the aforementioned question in the affirmative and prove security of the HB and HB$^+$ protocols under parallel/concurrent executions. We also give what we believe to be substantially simpler security proofs for these protocols which are more complete in that they explicitly address the dependence of the soundness error on the number of iterations.

For the entire collection see [Zbl 1108.94002].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Full Text: DOI

References:

[1] Associated Press. Geeks Flex Hacker Muscles at Defcon. Article appeared on CNN.com, August 2 (2005)

[2] Bellare, M., Fischlin, M., Goldwasser, S., Micali, S.: Identification Protocols Secure against Reset Attacks. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol.˜2045, pp. 495–511. Springer, Heidelberg (2001) · Zbl 1012.94554 · doi:10.1007/3-540-44987-6_30

[3] Bellare, M., Impagliazzo, R., Naor, M.: Does Parallel Repetition Lower the Error in Computationally-Sound Protocols? In: 38th IEEE Symposium on Foundations of Computer Science, pp. 374–383. IEEE, Los Alamitos (1997)

[4] Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the Inherent Intractability of Certain Coding Problems. IEEE Trans. Info. Theory˜24, 384–386 (1978) · Zbl 0377.94018 · doi:10.1109/TIT.1978.1055873

[5] Blum, A., Furst, M., Kearns, M., Lipton, R.: Cryptographic Primitives Based on Hard Learning Problems. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol.˜773, pp. 278–291. Springer, Heidelberg (1994) · Zbl 0870.94021 · doi:10.1007/3-540-48329-2_24

[6] Blum, A., Kalai, A., Wasserman, H.: Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. J. ACM˜50(4), 506–519 (2003) · Zbl 1325.68114 · doi:10.1145/792538.792543

[7] Canetti, R., Halevi, S., Steiner, M.: Hardness Amplification of Weakly Verifiable Puzzles. In: Kilian, J. (ed.) TCC 2005. LNCS, vol.˜3378, pp. 17–33. Springer, Heidelberg (2005) · Zbl 1079.94538 · doi:10.1007/978-3-540-30576-7_2

[8] Canetti, R., Kilian, J., Petrank, E., Rosen, A.: Black-Box Concurrent Zero-Knowledge Requires (Almost) Logarithmically Many Rounds. SIAM J. Computing˜32(1), 1–47 (2002) · Zbl 1037.94004 · doi:10.1137/S0097539701392949

[9] Chabaud, F.: On the Security of Some Cryptosystems Based on Error-Correcting Codes. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol.˜950, pp. 131–139. Springer, Heidelberg (1995) · Zbl 0881.94018 · doi:10.1007/BFb0053430

[10] Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Trans. Info. Theory˜22(6), 644–654 (1976) · Zbl 0435.94018 · doi:10.1109/TIT.1976.1055638

[11] Feige, U., Shamir, A.: Witness Indistinguishability and Witness Hiding Protocols. In: 22nd ACM Symposium on Theory of

Computing, pp. 416–426. ACM, New York (1990)

[12] Gilbert, H., Robshaw, M., Silbert, H.: An Active Attack against HB\ +\ – a Provably Secure Lightweight Authentication Protocol (2005), available at: http://eprint.iacr.org/2005/237

[13] Goldreich, O.: Modern Cryptography, Probabilistic Proofs, and Pseudorandomness. Springer, Heidelberg (1998)

[14] Goldreich, O., Krawczyk, H.: On the Composition of Zero-Knowledge Proof Systems. SIAM J. Computing˜25(1), 169–192 (1996) · Zbl 0841.68112 · doi:10.1137/S0097539791220688

[15] Goldreich, O., Nisan, N., Wigderson, A.: On Yao's XOR-Lemma (1995), available at: http://eccc.uni-trier.de/eccc-reports/1995/TR95-050/ · Zbl 1304.68074

[16] Goldreich, O., Oren, Y.: Definitions and Properties of Zero-Knowledge Proof Systems. J. Cryptology˜7(1), 1–32 (1994) · Zbl 0791.94010 · doi:10.1007/BF00195207

[17] Håstad, J.: Some Optimal Inapproximability Results. J. ACM˜48(4), 798–859 (2001) · Zbl 1127.68405 · doi:10.1145/502090.502098

[18] Hopper, N., Blum, M.: A Secure Human-Computer Authentication Scheme. Technical Report CMU-CS-00-139, Carnegie Mellon University (2000)

[19] Hopper, N., 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

[20] Juels, A., Weis, S.: Authenticating Pervasive Devices with Human Protocols. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol.˜3621, pp. 293–308. Springer, Heidelberg (2005), Updated version available at: http://www.rsasecurity.com/rsalabs/staff/ · Zbl 1145.94470 · doi:10.1007/11535218_18

[21] Kearns, M.: Efficient Noise-Tolerant Learning from Statistical Queries. J. ACM˜45(6), 983–1006 (1998) · Zbl 1065.68605 · doi:10.1145/293347.293351

[22] Kfir, Z., Wool, A.: Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems (2005), available at: http://eprint.iacr.org/2005/052

[23] Kirschenbaum, I., Wool, A.: How to Build a Low-Cost, Extended-Range RFID Skimmer (2006), available at: http://eprint.iacr.org/2006/054

[24] Raz, R.: A Parallel Repetition Theorem. SIAM J. Computing˜27(3), 763–803 (1998) · Zbl 0911.68082 · doi:10.1137/S0097539795280895

[25] Regev, O.: On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In: 37th ACM Symposium on Theory of Computing, pp. 84–93. ACM, New York (2005) · Zbl 1192.94106

[26] Yao, A.C.-C.: Theory and Applications of Trapdoor Functions. In: 23rd IEEE Symposium on Foundations of Computer Science, pp. 80–91. IEEE, Los Alamitos (1982)