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

Parallel and concurrent security of the HB and HB^+ protocols. (English) Zbl 1201.94090

J. Cryptology 23, No. 3, 402-421 (2010).

N. Hopper and *M. Blum* [Secure human identification protocols. Advances in cryptology – ASIACRYPT 2001. 7th international conference on the theory and application of cryptology and information security, Gold Coast, Australia. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 2248, 52–66 (2001; Zbl 1062.94549)] and *A. Juels* and *S. A. Weis* [Authenticating pervasive devices with human protocols. Advances in cryptology – CRYPTO 2005. 25th annual international cryptology conference, Santa Barbara, CA, USA 2005. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 3621, 293–308 (2005; Zbl 1145.94470)] proposed the shared-key authentication protocols HB and HB^+, respectively. Their extremely low computational cost make them attractive for low-cost devices such as radio-frequency identification (RFID) tags. The security of these protocols is based on the conjectured hardness of the "learning parity with noise" (LPN) problem, which is equivalent to the problem of decoding random binary linear codes. In this paper, the HB protocol is proven secure against a passive (eavesdropping) adversary and the HB^+ protocol is proven secure against active attacks.

Reviewer: Jörg Desel (Hagen)

MSC:

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

Keywords:

authentiation protocols; RFID; learning parity with noise

Software:

HB-MP

Full Text: DOI

References:

[1] Bellare, M.; Impagliazzo, R., M. Naor. Does parallel repetition lower the error in computationally sound protocols?, 38th IEEE Symposium on Foundations of Computer Science, 374-383 (1997), New York: IEEE, New York

[2] Berlekamp, E. R.; McEliece, R. J.; van Tilborg, H. C.A., On the inherent intractability of certain coding problems, IEEE Trans. Inf. Theory, 24, 384-386 (1978) · Zbl 0377.94018

[3] Blum, A.; Furst, M.; Kearns, M.; Lipton, R., Cryptographic primitives based on hard learning problems, Adv. in Cryptology—Crypto'93, 278-291 (1994), Berlin: Springer, Berlin · Zbl 0870.94021

[4] 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

[5] Bringer, J.; Chabanne, H.; Dottax, E.; Georgiadis, P.; Lopez, J.; Gritzalis, S.; Marias, G., HB^++: A lightweight authentication protocol secure against some attacks, Proceedings of SecPerU 2006, 28-33 (2006), Los Alamitos: IEEE Computer Society Press, Los Alamitos

[6] Canetti, R.; Kilian, J.; Petrank, E.; Rosen, A., Black-box concurrent zero-knowledge requires (almost) logarithmically many rounds, SIAM J. Comput., 32, 1, 1-47 (2002) · Zbl 1037.94004

[7] Canetti, R.; Halevi, S., M. Steiner. Hardness amplification of weakly verifiable puzzles, 2nd Theory of Cryptography Conference (TCC 2005), 17-33 (2005), Berlin: Springer, Berlin · Zbl 1079.94538

[8] Chabaud, F., On the security of some cryptosystems based on error-correcting codes, Adv. in Cryptology—Eurocrypt '94, 131-139 (1995), Berlin: Springer, Berlin · Zbl 0881.94018

[9] D.N. Duc, K. Kim, HB^+ Securing against GRS man-in-the-middle attack, in Institute of Electronics, Information and Communication Engineers, Symposium on Cryptography and Information Security, Jan. 23-26, 2007

[10] Feige, U.; Shamir, A., Witness indistinguishability and witness hiding protocols, 22nd ACM Symposium on Theory of Computing, 416-426 (1990), New York: ACM, New York

[11] Fossorier, M.; Mihaljevic, M. J.; Imai, H.; Cui, Y.; Matsuura, K., An algorithm for solving the LPN problem and its application to security evaluation of the HB protocols for RFID authentication, Progress in Cryptology—INDOCRYPT 2006, 48-62 (2006), Berlin: Springer, Berlin · Zbl 1175.94078

[12] Gilbert, H.; Robshaw, M.; Silbert, H., An active attack against HB^+: A provably secure lightweight authentication protocol, IEE Electron. Lett., 41, 21, 1169-1170 (2005)

[13] Gilbert, H.; Robshaw, M. J.B.; Seurin, Y., Good variants of HB^+ are hard to find, Financial Cryptography and Data Security, 156-170 (2008), Berlin: Springer, Berlin · Zbl 1175.94079

[14] Gilbert, H.; Robshaw, M. J.B.; Seurin, Y., HB^#: Increasing the security and efficiency of HB^+, Adv. in Cryptology—EUROCRYPT 2008, 361-378 (2008), Berlin: Springer, Berlin · Zbl 1149.94334

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

[16] Goldreich, O.; Krawczyk, H., On the composition of zero-knowledge proof systems, SIAM J. Comput., 25, 1, 169-192 (1996) · Zbl 0841.68112

[17] Goldreich, O.; Oren, Y., Definitions and properties of zero-knowledge proof systems, J. Cryptol., 7, 1, 1-32 (1994) · Zbl 0791.94010

[18] O. Goldreich, N. Nisan, A. Wigderson, On Yao's XOR-lemma. Available at http://eccc.uni-trier.de/eccc-reports/1995/TR95-050/ · Zbl 1304.68074

[19] Guruswami, V., List Decoding of Error-Correcting Codes (2004), Berlin: Springer, Berlin · Zbl 1075.94001

[20] Håstad, J., Some optimal inapproximability results, J. ACM, 48, 4, 798-859 (2001) · Zbl 1127.68405

[21] N. Hopper, M. Blum, A secure human-computer authentication scheme. Technical Report CMU-CS-00-139, Carnegie Mellon University, 2000

[22] Hopper, N.; Blum, M., Secure human identification protocols, Adv. in Cryptology—Asiacrypt 2001, 52-66 (2001), Berlin: Springer, Berlin · Zbl 1062.94549

[23] Johnson, S. M., A new upper bound for error-correcting codes, IRE Trans. Inf. Theory, 8, 3, 203-207 (1962) · Zbl 0102.34602

[24] Johnson, S. M., Improved asymptotic bounds for error-correcting codes, IEEE Trans. Inf. Theory, 9, 3, 198-205 (1963) · Zbl 0282.94010

[25] Juels, A.; Weis, S., Authenticating pervasive devices with human protocols, Adv. in Cryptology—Crypto 2005, 293-308 (2005), Berlin: Springer, Berlin · Zbl 1145.94470

[26] Katz, J.; Shin, J.-S., Parallel and concurrent security of the HB and HB^+ protocols, Adv. in Cryptology—Eurocrypt 2006, 73-87 (2006), Berlin: Springer, Berlin · Zbl 1140.94352

[27] J. Katz, A. Smith, Analyzing the HB and HB+ protocols in the "large error" case. Available at http://eprint.iacr.org/2006/326 · Zbl 1201.94090

[28] Kearns, M., Efficient noise-tolerant learning from statistical queries, J. ACM, 45, 6, 983-1006 (1998) · Zbl 1065.68605

[29] Z. Kfir, A. Wool, Picking virtual pockets using relay attacks on contactless smartcard systems. Available at http://eprint.iacr.org/2005/052

[30] I. Kirschenbaum, A. Wool, How to build a low-cost, extended-range RFID skimmer. Available at http://eprint.iacr.org/2006/054

[31] Levieil, E.; Fouque, P.-A., An improved LPN algorithm, Security and Cryptography for Networks (SCN 2006), 348-359 (2006), Berlin: Springer, Berlin · Zbl 1152.94434

[32] Lyubashevsky, V., The parity problem in the presence of noise, decoding random linear codes, and the subset sum problem, 9th Intl. Workshop on Randomization and Computation (RANDOM 2005), 378-389 (2005), Berlin: Springer, Berlin · Zbl 1142.68399

[33] Munilla, J.; Peinado, A., HB-MP: A further step in the hb-family of lightweight authentication protocols, Comput. Netw., 51, 2262-2267 (2007) · Zbl 1118.68015

[34] Pass, R.; Venkitasubramaniam, M., An efficient parallel repetition theorem for Arthur-Merlin games, 39th ACM Symposium on Theory of Computing, 420-429 (2007), New York: ACM, New York · Zbl 1232.68057

[35] Peikert, C., Public-key cryptosystems from the worst-case shortest vector problem, 41st ACM Symposium on Theory of Computing, 333-342 (2009), New York: ACM, New York · Zbl 1304.94079

[36] Raz, R., A parallel repetition theorem, SIAM J. Comput., 27, 3, 763-803 (1998) · Zbl 0911.68082

[37] Regev, O., On lattices, learning with errors, random linear codes, and cryptography, 37th ACM Symposium on Theory of Computing, 84-93 (2005), New York: ACM, New York · Zbl 1192.94106

[38] Yao, A. C.-C., Theory and applications of trapdoor functions, 23rd IEEE Symposium on Foundations of Computer Science, 80-91 (1982), New York: IEEE, New York