Kiltz, Eike; **Pietrzak, Krzysztof**; **Venturi, Daniele**; **Cash, David**; **Jain, Abhishek**
Efficient authentication from hard learning problems. (English) Zbl 1386.94096
J. Cryptology 30, No. 4, 1238-1275 (2017).

Summary: We construct efficient authentication protocols and message authentication codes (MACs) whose security can be reduced to the learning parity with noise (LPN) problem. Despite a large body of work – starting with the HB protocol of *N. J. Hopper* and *M. Blum* in 2001 [Asiacrypt 2001, Lect. Notes Comput. Sci. 2248, 52–66 (2001; Zbl 1062.94549)] – until now, it was not even known how to construct an efficient authentication protocol from LPN which is secure against man-in-the-middle attacks. A MAC implies such a (two-round) protocol.

A preliminary version appeared in [Eurocrypt 2011, Lect. Notes Comput. Sci. 6632, 7–26 (2011; Zbl 1281.94083)].

MSC:

94A62 Authentication, digital signatures and secret sharing

Cited in **1** Review

Keywords:

authentication protocols; message authentication; hard learning problems

Software:

JDQR; JDQZ

Full Text: DOI

References:

[1] S. Agrawal, D. Boneh, X. Boyen, Efficient lattice (H)IBE in the standard model, in \textit{EUROCRYPT 2010}, volume 6110 of LNCS, ed. by H. Gilbert (Springer, May 2010), pp. 553-572 · Zbl 1227.94022

[2] Z. Bai, J. Demmel, J. Dongarra, A. Ruhe, H. van der Vorst, \textit{Templates for the Solution of Algebraic Eigenvalue Problems: A Practical Guide} (SIAM, Philadelphia, 2000) · Zbl 0965.65058

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

[4] O. Blazy, E. Kiltz, J. Pan, (Hierarchical) identity-based encryption from affine message authentication, in In \textit{CRYPTO 2014}, volume 8616 of LNCS, ed. by J.A. Garay, R. Gennaro (Springer, Aug 2014), pp. 408-425 · Zbl 1345.94044

[5] A. Blum, M.L. Furst, M.J. Kearns, R.J. Lipton, Cryptographic primitives based on hard learning problems, in \textit{CRYPTO'93}, volume 773 of LNCS, ed. by D.R. Stinson (Springer, Aug 1994), pp. 278-291 · Zbl 0870.94021

[6] Blum, Avrim; Kalai, Adam; Wasserman, Hal, Noise-tolerant learning, the parity problem, and the statistical query model, J. ACM, 50, 506-519, (2003) · Zbl 1325.68114

[7] S. Bogos, F. Tramèr, S. Vaudenay, On solving LPN using BKW and variants—implementation and analysis. \textit{Cryptogr. Commun.}\textbf{8}(3), 331-369 (2016) · Zbl 1338.94068

[8] S. Bogos, S. Vaudenay, Observations on the LPN solving algorithm from Eurocrypt'16. Cryptology ePrint Archive, Report 2016/437 (2016). http://eprint.iacr.org/2016/437 · Zbl 0596.65002

[9] S. Bogos, S. Vaudenay, Optimization of LPN solving algorithms. Cryptology ePrint Archive, Report 2016/288 (2016). http://eprint.iacr.org/2016/288 · Zbl 1404.94042

[10] X. Boyen, Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more, in \textit{PKC 2010}, volume 6056 of LNCS, ed. by P.Q. Nguyen, D. Pointcheval (Springer, May 2010), pp. 499-517 · Zbl 1281.94074

[11] J. Bringer, H. Chabanne, E. Dottax, ${\sf HB}^{++}$: a lightweight authentication protocol secure against some attacks, in \textit{SecPerU 2006} (IEEE Computer Society, June 2006), pp. 28-33

[12] D. Cash, E. Kiltz, S. Tessaro, Two-round man-in-the-middle security from LPN, in \textit{TCC 2016-A}, volume 9562 of LNCS, ed. by E. Kushilevitz, T. Malkin (Springer, Jan 2016), pp. 225-248 · Zbl 1378.94074

[13] J. Chen, H. Wee, Fully, (almost) tightly secure IBE and dual system groups, in \textit{CRYPTO 2013}, volume 8043 of LNCS, ed. by R. Canetti, J.A. Garay (Springer, Aug 2013), pp. 435-460 · Zbl 1311.94072

[14] R. Cramer, I. Damgård, On the amortized complexity of zero-knowledge protocols, in \textit{CRYPTO 2009}, volume 5677

of LNCS, ed. by S. Halevi (Springer, Aug 2009), pp. 177-191 · Zbl 1252.94056

[15] Y. Dodis, E. Kiltz, K. Pietrzak, D. Wichs, Message authentication, revisited, in \textit{EUROCRYPT 2012}, volume 7237 of LNCS, ed. by D. Pointcheval, T. Johansson (Springer, April 2012), pp. 355-374 · Zbl 1297.94117

[16] D.N. Duc, K. Kim, Securing ${\sf HB}^{+}$ against GRS man-in-the-middle attack, in \textit{2007 symposium on cryptography and information security}, Jan 2007

[17] J.-B. Fischer, J. Stern, An efficient pseudo-random generator provably as secure as syndrome decoding, in \textit{EUROCRYPT'96}, volume 1070 of LNCS, ed. by U.M. Maurer (Springer, May 1996), pp. 245-255 · Zbl 1304.94056

[18] M. Fürer, Faster integer multiplication. \textit{SIAM J. Comput.}\textbf{39}(3), 979-1005 (2009) · Zbl 1192.68926

[19] L. Gaspar, G. Leurent, F.-X. Standaert, Hardware implementation and side-channel analysis of Lapin, in \textit{CT-RSA 2014}, LNCS (Springer, 2014), pp. 206-226 · Zbl 1337.94096

[20] H. Gilbert, M. Robshaw, H. Sibert, An active attack against ${\sf HB}^{+}$—a provably secure lightweight authentication protocol. Cryptology ePrint Archive, Report 2005/237 (2005). http://eprint.iacr.org/

[21] H. Gilbert, M.J.B. Robshaw, Y. Seurin, Good variants of HB+ are hard to find, in \textit{FC 2008}, volume 5143 of LNCS, ed. by G. Tsudik (Springer, Jan 2008), pp. 156-170 · Zbl 1175.94079

[22] H. Gilbert, M.J.B. Robshaw, Y. Seurin, HB$^{\boxtimes}$: increasing the security and efficiency of HB^{+}, in \textit{EUROCRYPT 2008}, volume 4965 of LNCS, ed. by N.P. Smart (Springer, April 2008), pp. 361-378 · Zbl 1149.94334

[23] Goldreich, O; Goldwasser, S; Micali, S, How to construct random functions, J. ACM, 33, 792-807, (1986) · Zbl 0596.65002

[24] Q. Guo, T. Johansson, C. Löndahl, Solving LPN using covering codes, in \textit{ASIACRYPT 2014}, volume 8873 of LNCS, ed. by P. Sarkar, T. Iwata (Springer, Dec 2014), pp. 1-20 · Zbl 1306.94059

[25] S. Heyse, E. Kiltz, V. Lyubashevsky, C. Paar, K. Pietrzak, Lapin: an efficient authentication protocol based on Ring-LPN, in \textit{FSE 2012}, volume 7549 of LNCS, ed. by A. Canteaut (Springer, March 2012), pp. 346-365 · Zbl 1282.94078

[26] W. Hoeffding, Probability inequalities for sums of bounded random variables. \textit{J. Am. Stat. Assoc.}\textbf{58}(301), 13-30 (1963) · Zbl 0127.10602

[27] N.J. Hopper, M. Blum, Secure human identification protocols, in \textit{ASIACRYPT 2001}, volume 2248 of LNCS, ed. by C. Boyd (Springer, Dec 2001), pp. 52-66 · Zbl 1062.94549

[28] A. Juels, S.A. Weis, Authenticating pervasive devices with human protocols, in\textit{CRYPTO 2005}, volume 3621 of LNCS, ed. by V. Shoup (Springer, Aug 2005), pp. 293-308 · Zbl 1145.94470

[29] T. Kailath, A.H. Sayed, \textit{Fast Reliable Algorithms for Matrices with Structure} (SIAM, Philadelphia, 1999) · Zbl 0931.65018

[30] J. Katz, J.S. Shin, Parallel and concurrent security of the HB and HB+ protocols, in \textit{EUROCRYPT 2006}, volume 4004 of LNCS, ed. by S. Vaudenay (Springer, May/June 2006), pp. 73-87 · Zbl 1140.94352

[31] J. Katz, J.S. Shin, A. Smith, Parallel and concurrent security of the HB and HB+ protocols. \textit{J. Cryptol.}\textbf{23}(3), 402-421 (2010) · Zbl 1201.94090

[32] M.J. Kearns, Efficient noise-tolerant learning from statistical queries. \textit{J. ACM}\textbf{45}(6), 983-1006 (1998) · Zbl 1065.68605

[33] E. Kiltz, K. Pietrzak, D. Cash, A. Jain, D. Venturi, Efficient authentication from hard learning problems, in \textit{EUROCRYPT 2011}, volume 6632 of LNCS, ed. by K.G. Paterson (Springer, May 2011), pp. 7-26. · Zbl 1281.94083

[34] É. Levieil, P.-A. Fouque, An improved LPN algorithm, in \textit{SCN 06}, volume 4116 of LNCS, ed. by R. De Prisco, M. Yung (Springer, Sept 2006), pp. 348-359 · Zbl 1152.94434

[35] V. Lyubashevsky, D. Masny, Man-in-the-middle secure authentication schemes from LPN and weak PRFs, in \textit{CRYPTO 2013}, volume 8043 of LNCS, ed. by R. Canetti, J.A. Garay (Springer, Aug 2013), pp. 308-325 · Zbl 1316.94102

[36] V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors over rings, in \textit{EUROCRYPT 2010}, volume 6110 of LNCS, ed. by H. Gilbert (Springer, June 2010), pp. 1-23 · Zbl 1279.94099

[37] J. Munilla, A. Peinado, ${\sf HB\sf -\sf MP}$: a further step in the HB-family of lightweight authentication protocols. \textit{Comput. Netw.}\textbf{51}(9), 2262-2267 (2007) · Zbl 1118.68015

[38] K. Ouafi, R. Overbeck, S. Vaudenay, On the security of HB# against a man-in-the-middle attack, in \textit{ASIACRYPT 2008}, volume 5350 of LNCS, ed. by J. Pieprzyk (Springer, Dec 2008), pp. 108-124 · Zbl 1206.94084

[39] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem: extended abstract, in \textit{41st ACM STOC}, ed. by M. Mitzenmacher (ACM Press, May/June 2009), pp. 333-342 · Zbl 1304.94079

[40] K. Pietrzak, Subspace LWE, in \textit{TCC 2012}, volume 7194 of LNCS, ed. by R. Cramer (Springer, March 2012), pp. 548-563

[41] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in \textit{37th ACM STOC}, ed. by H.N. Gabow, R. Fagin (ACM Press, May 2005), pp. 84-93 · Zbl 1192.94106

[42] Schönhage, V. Strassen, Schnelle multiplikation grosser zahlen. \textit{Computing}\textbf{7}, 281-292 (1971) · Zbl 0223.68007

[43] J. Van De Graaf, \textit{Towards a formal definition of security for quantum protocols}. PhD thesis, Universite de Montreal, Monreal, P.Q., Canada, Canada, AAINQ35648, 1998 · Zbl 1325.68114

[44] B.R. Waters, Efficient identity-based encryption without random oracles, in \textit{EUROCRYPT 2005}, volume 3494 of LNCS, ed. by R. Cramer (Springer, May 2005), pp. 114-127 · Zbl 1137.94360

[45] J. Watrous, Zero-knowledge against quantum attacks. \textit{SIAM J. Comput.}\textbf{39}(1), 25-58 (2009) · Zbl 1186.81048

[46] B. Zhang, L. Jiao, M. Wang, Faster algorithms for solving LPN, in \textit{EUROCRYPT 2016}, volume 9665 of LNCS, ed. by M. Fischlin, J.-S. Coron (Springer, May 2016), pp. 168-195 · Zbl 1347.94064