Tomović, Siniša; **Mihaljević, Miodrag J.**; **Perović, Aleksandar**; **Ognjanović, Zoran**

A protocol for provably secure authentication of a tiny entity to a high performance computing one. (English) Zbl 1400.94187

Math. Probl. Eng. 2016, Article ID 9289050, 9 p. (2016).

Summary: The problem of developing authentication protocols dedicated to a specific scenario where an entity with limited computational capabilities should prove the identity to a computationally powerful Verifier is addressed. An authentication protocol suitable for the considered scenario which jointly employs the learning parity with noise (LPN) problem and a paradigm of random selection is proposed. It is shown that the proposed protocol is secure against active attacking scenarios and so called GRS man-in-the-middle (MIM) attacking scenarios. In comparison with the related previously reported authentication protocols the proposed one provides reduction of the implementation complexity and at least the same level of the cryptographic security.

MSC:

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

Software:

HB-MP

Full Text: DOI

References:

[1] Juels, A., RFID security and privacy: a research survey, IEEE Journal on Selected Areas in Communications, 24, 2, 381-394, (2006)

[2] Piramuthu, S., Lightweight cryptographic authentication in passive RFID-Tagged systems, IEEE Transactions on Systems, Man and Cybernetics—Part C: Applications and Reviews, 38, 3, 360-376, (2008)

[3] Hernandez-Ramos, J. L.; Pawlowski, M. P.; Jara, A. J.; Skarmeta, A. F.; Ladid, L., Toward a lightweight authentication and authorization framework for smart objects, IEEE Journal on Selected Areas in Communications, 33, 4, 690-702, (2015)

[4] Ratković, I.; Bežanić, N.; Ünsal, O. S.; Cristal, A.; Milutinović, V., An overview of architecture-level power- and energy-efficient design techniques, Advances in Computers, 98, 1-57, (2015)

[5] Hopper, N. J.; Blum, M.; Boyd, C., Secure human identification protocols, Advances in Cryptology—ASIACRYPT 2001. Advances in Cryptology—ASIACRYPT 2001, Lecture Notes in Computer Science, 2248, 52-66, (2001), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1062.94549

[6] Berlekamp, E. R.; McEliece, R. J.; van Tilborg, H. C., On the inherent intractability of certain coding problems, Institute of Electrical and Electronics Engineers. Transactions on Information Theory, IT-24, 3, 384-386, (1978) · Zbl 0377.94018

[7] Juels, A.; Weis, S. A.; Shoup, V., Authenticating pervasive devices with human protocols, Advances in Cryptology—CRYPTO 2005. Advances in Cryptology—CRYPTO 2005, Lecture Notes in Computer Science, 3621, 293-308, (2005), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1145.94470

[8] Katz, J.; Shin, J. S.; Vaudenay, S., Parallel and concurrent security of the HB and HB protocols, Advances in Cryptology—EUROCRYPT 2006. Advances in Cryptology—EUROCRYPT 2006, Lecture Notes in Computer Science, 4004, 73-87, (2006), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1140.94352

[9] Katz, J.; Shin, J. S.; Smith, A., Parallel and concurrent security of the HB and HB protocols, Journal of Cryptology, 23, 3, 402-421, (2010) · Zbl 1201.94090

[10] Gilbert, H.; Robshaw, M.; Sibert, H., Active attack against HB+: a provably secure lightweight authentication protocol, Electronics Letters, 41, 21, 1169-1170, (2005)

[11] Munilla, J.; Peinado, A., HB-MP: a further step in the HB-family of lightweight authentication protocols, Computer Networks, 51, 9, 2262-2267, (2007) · Zbl 1118.68015

[12] Bringer, J.; Chabanne, H., Trusted-HB: a low-cost version of HB+ secure against man-in-the-middle attacks, IEEE Transactions on Information Theory, 54, 9, 4339-4342, (2008) · Zbl 1322.94096

[13] Gilbert, H.; Robshaw, M. J. B.; Seurin, Y.; Smart, N., HB: increasing the security and efficiency of HB, Advances in Cryptology—EUROCRYPT 2008. Advances in Cryptology—EUROCRYPT 2008, Lecture Notes in Computer Science, 4965, 361-378, (2008), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1149.94334

[14] Ouafi, K.; Overbeck, R.; Vaudenay, S.; Pieprzyk, J., On the security of HB against a man-in-the-middle attack, Advances in Cryptology—ASIACRYPT 2008. Advances in Cryptology—ASIACRYPT 2008, Lecture Notes in Computer Science, 5350, 108-124, (2008), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1206.94084

[15] Kiltz, E.; Pietrzak, K.; Cash, D.; Jain, A.; Venturi, D.; Paterson, K. G., Efficient authentication from hard learning problems, Advances in Cryptology—EUROCRYPT 2011. Advances in Cryptology—EUROCRYPT 2011, Lecture Notes in Computer Science, 6632, 7-26, (2011), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1281.94083

[16] Kosei, E.; Kunihiro, N.; Yoshida, M.; Mouri, K., On the security proof of an authentication protocol from Eurocrypt 2011, Advances in Information and Computer Security. Advances in Information and Computer Security, Lecture Notes in Computer Science, 8639, 187-203, (2014), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1417.94094

[17] Cichoń, J.; Klonowski, M.; Kutyłowski, M.; Indulska, J.; Patterson, D. J.; Rodden, T.; Ott, M., Privacy protection for RFID with hidden subset identifiers, Pervasive Computing. Pervasive Computing, Lecture Notes in Computer Science, 5013, 298-314, (2008)

[18] Gołębiewski, Z.; Majcher, K.; Zagórski, F.; Coudert, D.; Simplot-Ryl, D.; Stojmenovic, I., Attacks on CKK family of RFID authentication protocols, Ad-Hoc, Mobile and Wireless Networks. Ad-Hoc, Mobile and Wireless Networks, Lecture Notes in Computer Science, 5198, 241-250, (2008)

[19] Krause, M.; Hamann, M., The cryptographic power of random selection, Selected Areas in Cryptography, SAC 2011. Selected Areas in Cryptography, SAC 2011, Lecture Notes in Computer Science, 7118, 134-150, (2012), New York, NY, USA: Springer, New York, NY, USA · Zbl 1292.94096

[20] Lyubashevsky, V.; Masny, D.; Canetti, R.; Garay, J. A., Man-in-the-middle secure authentication schemes from LPN and weak PRFs, Advances in Cryptology—CRYPTO 2013. Advances in Cryptology—CRYPTO 2013, Lecture Notes in Computer Science, 8043, 308-325, (2013), Heidelberg, Germany: Springer, Heidelberg, Germany · Zbl 1316.94102