Alvarez, Gonzalo

Security problems with a chaos-based deniable authentication scheme. (English)

Chaos Solitons Fractals 26, No. 1, 7-11 (2005).

Summary: Recently, a new scheme was proposed for deniable authentication. Its main originality lied on applying a chaos-based encryption-hash parallel algorithm and the semi-group property of the Chebyshev chaotic map. Although original and practicable, its insecurity and inefficiency are shown in this paper, thus rendering it inadequate for adoption in e-commerce.

MSC:

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

Keywords:

encryption-hash parallel algorithm; Chebyshev chaotic map

Full Text: DOI arXiv

References:

[1] Álvarez G, Montoya F, Romera M, Pastor G. Chaotic cryptosystems. In: Sanson LD, editor. 33rd Annual 1999 International Carnahan Conference on Security Technology. IEEE, 1999; 332-8

[2] Kocarev, L., Chaos-based cryptography: a brief overview, IEEE circ syst mag, 1, 3, 6-21, (2001)

[3] Dachselt, F.; Schwarz, W., Chaos and cryptography, IEEE trans circ syst I, 48, 12, 1498-1509, (2001) - Zbl 0999.94030

[4] Li S. Analyse and new designs of digital chaotic ciphers. Ph.D. thesis, Xi'an Jiaotong University, Xi'an, China, available online at (2005)

[5] Yang, T., A survey of chaotic secure communication systems, Int J comp cognit, 2, 2, 81-130, (2004)

[6] Baptista, M., Cryptography with chaos, Phys lett A, 240, 1-2, 50-54, (1999) - Zbl 0936.94013

[7] Jakimoski, G.; Kocarev, L., Analysis of some recently proposed chaos-based encryption algorithms, Phys lett A, 291, 6, 381-384, (2001) - Zbl 0978.68061

[8] Wong, K., A fast chaotic cryptographic scheme with dynamic look-up table, Phys lett A, 298, 4, 238-242, (2002) - Zbl 0999.94029

[9] Palacios, A.; Juarez, H., Cryptography with cycling chaos, Phys lett A, 303, 5-6, 345-351, (2002) - Zbl 0999.94028

[10] Wong, K., A combined chaotic cryptographic and hashing scheme, Phys lett A, 307, 5-6, 292-298, (2003) - Zbl 1008.94018

[11] Li, S.; Mou, X.; Ji, Z.; Zhang, J.; Cai, Y., Performance analysis of jakimoski-kocarev attack on a class of chaotic cryptosystems, Phys lett A, 307, 1, 22-28, (2003), An erratum has been published in Phys. Lett. A 309(1-2) (2003) 165 - Zbl 1006.94018

[12] Álvarez, G.; Montoya, F.; Romera, M.; Pastor, G., Cryptanalysis of an ergodic chaotic cipher, Phys lett A, 311, 2-3, 172-179, (2003) - Zbl 1027.94009

[13] Li, S.; Chen, G.; Wong, K.-W.; Mou, X.; Cai, Y., Baptista-type chaotic cryptosystems: problems and countermeasures, Phys lett A, 332, 5-6, 368-375, (2004) - Zbl 1112.81430

[14] Huang, F.; Guan, Z.-H., Cryptosystem using chaotic keys, Chaos, solitons \& fractals, 23, 3, 851-855, (2005) - Zbl 1068.94013

[15] Xiao, D.; Liao, X.; Wong, K., An efficient entire chaos-based scheme for deniable authentication, Chaos, solitons \& fractals, 23, 4, 1327-1331, (2005) - Zbl 1070.94023

[16] Katz, J, Efficient and non-malleable proofs of plaintext knowledge and applications, (), 211-228 - Zbl 1038.94538

[17] Kocarev L, Tasev Z. Public-key encryption based on Chebyshev maps. In: Proceedings of the IEEE Symposium on Circuits and Systems (ISCAS’03), Vol. 3, 2003, pp. 28-31

[18] Álvarez, G.; Montoya, F.; Romera, M.; Pastor, G., Cryptanalysis of dynamic look-up table based chaotic cryptosystems, Phys lett A, 326, 3-4, 211-218, (2004) - Zbl 1138.9446

[19] Bergamo P, D’Arco P, Santis A, Kocarev L. Security of public key cryptosystems based on Chebyshev polynomials, IEEE Trans Circuits Syst I, preprint available online at arXiv:cs.CR/0411030, submitted for publication

[20] W. Dai, Speed comparison of popular crypto algorithms, available online at "

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically
matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.