Li, Chun-Ta; Chen, Chin-Ling; Lee, Cheng-Chi; Weng, Chi-Yao; Chen, Chien-Ming

A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps. (English) Zbl 1398.94199


Summary: Three-party authenticated key exchange (3PAKE) protocol allows two communication users to authenticate each other and to establish a secure common session key with the help of a trusted remote server. In [Nonlinear Dyn. 77, No. 1–2, 399–411 (2014; Zbl 1314.94067)], M. S. Farash and M. A. Attari propose an efficient and secure 3PAKE protocol based on Chebyshev chaotic maps and their protocol is supported by the formal proof in the random oracle model. However, in this paper, we analyze the security of Farash-Attari’s protocol and show that it fails to resist password disclosure attack if the secret information stored in the server side is compromised. In addition, their protocol is insecure against user impersonation attack, and the server is not aware of having caused problem. Moreover, the password change phase is insecure to identify the validity of request where insecurity in password change phase can cause offline password guessing attacks and is not easily reparable. To remove these security weaknesses, based on Chebyshev chaotic maps and quadratic residues, we further design an improved protocol for 3PAKE with user anonymity. In comparison with the existing chaotic map-based 3PAKE protocols, our proposed 3PAKE protocol is more secure with acceptable computation complexity and communication overhead.

MSC:

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

Keywords:

Chebyshev chaotic maps; quadratic residues; password security; three-party authenticated key exchange; user anonymity

Software:

CMQV+

Full Text: DOI

References:


Islam, Sk H; Khan, MK; Li, X, Security analysis and improvement of a more secure anonymous user authentication scheme for the integrated EPR information system, Plos ONE, 10, e0131368, (2015) - doi:10.1371/journal.pone.0131368


Li, CT, A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card, IET Inf Secur, 7, 3-10, (2013) - doi:10.1049/iet-ifs.2012.0058

Li, CT; Lee, CC; Weng, CY; Fan, CI, An advanced multi-server-based user authentication scheme with user anonymity, KSHI Trans Internet Inf Syst 7, 119-131, (2013) - doi:10.3837/tiis.2013.01.008

Li, CT; Weng, CY; Lee, CC, An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks, Sensors, 13, 9589-9603, (2013) - doi:10.3390/s130809589


Li, X; Niu, J; Kumari, S; Khan, MK; Liao, J; Liang, W, Design and analysis of a chaotic maps-based three-party authenticated key agreement protocol, Nonlinear Dyn, 80, 1209v1220, (2015) - Zbl 1351.94075


Wen, F, A more secure anonymous user authentication scheme for the integrated EPR information system, J Med Syst, 38, 42, (2014) - doi:10.1007/s10916-014-0042-0


Yang, L; Ma, JF; Jiang, Q, Mutual authentication scheme with smart cards and password under trusted computing, Int J...

[42] Zhao, F; Gong, P; Li, S; Li, M; Li, P, Cryptanalysis and improvement of a three-party key agreement protocol using enhanced Chebyshev polynomials, Nonlinear Dyn, 74, 419-427, (2013) · Zbl 1281.94067 · doi:10.1007/s11071-013-0979-4

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.