Meshram, Chandrashekhar; **Meshram, Suchitra A.**; **Zhang, Mingwu**

An ID-based cryptographic mechanisms based on GDLP and IFP. (English) Zbl 1250.94059

Inf. Process. Lett. 112, No. 19, 753-758 (2012).

Summary: In 1984, Shamir introduced the concept of an identity-based cryptosystem. In this system, each user needs to visit a key authentication center (KAC) and identify himself before joining a communication network. Once a user is accepted, the KAC will provide him with a secret key. In this way, if a user wants to communicate with others, he only needs to know the identity of his communication partner and the public key of the KAC. There is no public file required in this system. However, Shamir did not succeed in constructing an identity-based cryptosystem, but only in constructing an identity-based signature scheme. In this paper, we propose an ID-based cryptosystem under the security assumptions of the generalized discrete logarithm problem and integer factorization problem. We consider the security against a conspiracy of some entities in the proposed system and show the possibility of establishing a more secure system.

MSC:

94A62 Authentication, digital signatures and secret sharing
68P30 Coding and information theory (compaction, compression, models of communication, encoding schemes, etc.) (aspects in computer science)
94A60 Cryptography

Cited in **6** Documents

Keywords:

cryptography; public key cryptosystem; identity-based cryptosystem; discrete logarithm problem; generalized discrete logarithm problem; integer factorization problem (IFP)

Full Text: DOI

References:

[1] Shamir, A., Identity-based cryptosystem and signature scheme, (), 47-53 · Zbl 1359.94626

[2] Tsujii, S.; Itoh, T., An ID-based cryptosystem based on the discrete logarithm problem, IEEE J. selected areas commun., 7, 467-473, (1989)

[3] ElGamal, T., A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE trans. inform. theory, 31, 469-472, (1995) · Zbl 0571.94014

[4] Diffie, W.; Hellman, M.E., New direction in cryptography, IEEE trans. inform. theory, 22, 644-654, (1976) · Zbl 0435.94018

[5] Kohnfelder, L.M., A method for certification, (May 1978), Lab. Comput. Sci. Mass. Inst. Technol. Cambridge, MA

[6] Okarnoto, E.; Tanaka, K., Key distribution system based on identification information, IEEE J. selected areas commun., 7, 481-485, (May 1989)

[7] R. Blorn, An optimal class of symmetric key generation systems, in: Proc. Eurocryp '84, Pans, France, Apr. 9-11, 1984, pp. 335-338.

[8] Lee, W.B.; Liao, K.C., Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, J. network computer appl., 27, 191-199, (2004)

[9] Hwang, M.S.; Lo, J.W.; Lin, S.C., An efficient user identification scheme based on ID-based cryptosystem, Computer standards \& interfaces, 26, 565-569, (2004)

[10] Ohta, K., Efficient identification and signature schemes, Electron. lett., 24, 2, 115-116, (1988) · Zbl 0681.94011

[11] Harn, L., Public key cryptosystem design based on factoring and discrete logarithm, IEE proc. comput. digit. tech., 141, 3, 193-195, (1994) · Zbl 0812.94010

[12] Kiltz, E.; Vahlis, Y., CCA2 secure IBE: standard model efficiency through authenticated symmetric encryption, (), 221-239 · Zbl 1153.94400

[13] Meshram, C., A cryptosystem based on double generalized discrete logarithm problem, Int. J. contemp. math. sci., 6, 6, 285-297, (2011) · Zbl 1233.94021

[14] Meshram, C., Modified ID-based public key cryptosystem using double discrete logarithm problem, Int. J. adv. comput. sci. appl., 1, 6, 30-34, (2010)

[15] Gangishetti, R.; Choudary Gorantla, M.; Lal Das, Manik; Saxena, Ashutosh, Threshold key issuing in identity-based cryptosystems, Computer standards \& interfaces, 29, 260-264, (2007)

[16] Sun, J.; Zhang, C.; Zhang, Y.; Fang, Y., An identity-based security system for user privacy in vehicular ad hoc networks, IEEE tran. parall. distributed syst., 27, 9, 1227-1239, (2010)

[17] Boneh, D.; Franklin, M.K., Identity based encryption from the Weil pairing, SIAM J. comput., 32, 3, 586-615, (2003) · Zbl 1046.94008

[18] Boneh, D.; Canetti, R.; Halevi, S.; Katz, J., Chosen-ciphertext security from identity-based encryption, SIAM J. comput., 5, 36, 1301-1328, (2006) · Zbl 1138.94010

[19] Maurer, U.M.; Yacobi, Y., Non-interactive public key cryptography, (), 498-507 · Zbl 0825.94189

[20] Maurer, U.M.; Yacobi, Y., A non-interactive public-key distribution system, Des. codes cryptogr., 9, 3, 305-316, (1996) · Zbl 0871.94039

[21] Y.M. Tseng, J.K. Jan, ID-based cryptographic schemes using a non-interactive public-key distribution system, in: The 14th Annual Computer Security Applications Conference, 1998, pp. 237-243.

[22] Cocks, C., An identity based encryption scheme based on quadratic residues, (), 360-363 · Zbl 0999.94532

[23] D. Coppersmith, private communication, Nov. 1987.

[24] A. Shamir, private communication, June 1988.