Meshram, Chandrashekhar; **Lee, Cheng-Chi**; **Meshram, Sarita Gajbhiye**; **Khan, Muhammad Khurram**

An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. (English) Zbl 1436.94083

Soft Comput. 23, No. 24, 13127-13138 (2019).

Summary: The advancement of the cloud storage technology opens up a wide range of possibilities for adaptable data sharing. When sharing data to an extensive number of users with fuzzy identities, the data proprietor must use an appropriate identity-based encryption technique that satisfies both efficiency and security prerequisites. Identity-based encryption is a promising possibility to ensure fuzzy user data sharing while meeting the security essentials; however, it may encounter efficiency trouble in multi-receiver settings. Recently, identity-based encryption has received much attention, and most of the research has aimed to apply the technique in real-world systems. A major concern about using identity-based encryption is the safety of the private keys, as disclosure of secret keys requires the reissuing of encryptions already doled out. The capability to minimize the risks associated with key disclosure is particularly important due to the increased use of mobile and unprotected devices. In this article, we shall propose a forward-secure identity-based encryption technique based on subtree for fuzzy user data sharing under cloud computing environment, and we shall demonstrate that the technique is semantically secure against a chosen subtree and chosen ciphertext attack (IND-CST-CCA). In addition, we will show the superiority of our new technique over the currently existing methods in terms of security and the length of public key. Then, we will also discuss the potential of our new technique to be deployed in pay TV systems and grid security.

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Keywords:

identity-based encryption; cloud storage; subtree; bilinear pairings; random oracle; pay TV system; grid security

Full Text: DOI

References:

[1] Abe M, Cui Y, Imai H, Kiltz E (2010) Efficient hybrid encryption from ID-based encryption. Des Codes Cryptogr 54:205-240 · Zbl 1197.94171

[2] Benasser A, Samsudin A (2010) A new identity based encryption (IBE) scheme using extended Chebyshev polynomial over finite fields Z. Phys Lett A 374(46):4670-4674 · Zbl 1238.94026

[3] Boneh D, Boyen X (2004) Efficient selective-id secure identity based encryption without random oracles. In: Advances in cryptology-EUROCRYPT 2004, Lecture Notes in Computer Science, vol 3027. Springer, Berlin, pp 223-238 · Zbl 1122.94355

[4] Boneh D, Franklin MK (2001) Identity-based encryption from the weil pairing. In: Advances in cryptology-CRYPTO 2001, Lecture Notes in Computer Science, vol 2193. Springer, Berlin, pp 213-229 · Zbl 1002.94023

[5] Boneh D, Franklin MK (2003) Identity based encryption from the Weil pairing. SIAM J Comput 32(3):586-615 · Zbl 1046.94008

[6] Boneh D, Canetti R, Halevi S, Katz J (2003) Chosen-ciphertext security from identity-based encryption. SIAM J Comput 36(5):1301-1328 · Zbl 1138.94010

[7] Boneh D, Gentry C, Hamburg M (2008) Space-efficient identity based encryption without pairings. In: Proceedings of the 49th annual IEEE symposium on foundations of computer science, pp 647-657

[8] Cao N, Wang C, Li M, Ren K, Lou W (2014) Privacy-preserving multi-keyword ranked search over encrypted cloud data. IEEE Trans Parallel Distrib Syst 25(1):222-233

[9] Chen HC (2016) A trusted user-to-role and role-to-key access control scheme. Soft Comput 20(5):1721-1733

[10] Chen R, Mu Y, Yang G, Guo F, Wang X (2015) A new general framework for secure public key encryption with keyword search. In: 20th Australasian conference on information security and privacy (ACISP 2015), Brisbane, QLD, Australia, LNCS, vol 9144. Springer, Berlin

[11] Deng H, Wu Q, Qin B, Domingo-Ferrer J, Zhang L, Liu J, Shi W (2014) Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts. Inf Sci 275:370-384 · Zbl 1341.68043

[12] ElGmal T (1995) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31:469-472 · Zbl 0571.94014

[13] Fang L, Susilo W, Ge C, Wang J (2013) Public key encryption with keyword search secure against keyword guessing attack without random oracle. Inf Sci 238:221-241 · Zbl 1321.94057

[14] Fujisaki E, Okamoto T (1999) Secure integration of asymmetric and symmetric encryption schemes. In: Advances in Cryptology-Crypto'99, Lecture Notes in Computer Science, vol 1666. Springer, Berlin, pp 537-554 · Zbl 0942.94019

[15] Galindo D (2004) The exact security of pairing based encryption and signature schemes. Working Draft, November 1, 2004. http://www.cs.ru.nl/dgalindo/galindoEcrypt.pdf. Accessed 3-5 Nov 2004

[16] Galindo D (2015) Compact hierarchical identity-based encryption based on a harder decisional problem. Int J Comput Math 92(3):463-472 · Zbl 1375.94126

[17] Gentry C, Silverberg A (2002) Hierarchical id-based cryptography. In: ASIACRYPT 2002, LNCS, vol 2501. Springer, Berlin, pp 548-566 · Zbl 1065.94547

[18] Heng S, Kurosawa K (2004) k-Resilient identity-based encryption in the standard model. In: Topics in Cryptology- CT-RSA 2004, Lecture Notes in Computer Science, vol 2964. Springer, Berlin, pp 67-80 · Zbl 1196.94056

[19] Heng S, Kurosawa K (2006) k-Resilient identity-based encryption in the standard model. IEICE Trans Fundam E89CA(1):39-46

[20] Huang X, Liu JK, Hua S, Xiang Y, Liang K, Zhou J (2015) Cost-effective authentic and anonymous data sharing with forward security. IEEE Trans Comput 64(4):971-983 · Zbl 1360.68432

[21] Katz J, MacKenzie P, Taban G, Gligor V (2012) Two-server password-only authenticated key exchange. J Comput Syst Sci 78(2):651-669 · Zbl 1277.94059

[22] Liu C, Zhu L, Wang M, Tan Y (2014) Search pattern leakage in searchable encryption: attacks and new construction. Inf Sci 265:176-188

[23] Liu W, Liu J, Wu Q, Qin B, Naccache D, Ferradi H (2017) Efficient subtree-based encryption for fuzzy-entity data sharing. Soft Comput. https://doi.org/10.1007/s00500-017-2743-z · Zbl 1402.68056

[24] Luo S, Shen Q, Jin Y, Chen Y (2011) A variant of Boyen-Waters anonymous IBE scheme. In: Lecture Notes in Computer Sciences, vol 7043, pp 42-56

[25] Ma S (2016) Identity-based encryption with outsourced equality test in cloud computing. Inf Sci 328:389-402 · Zbl 1390.68278

[26] Mao Y, Li J, Chen MR, Liu J, Xie C, Zhan Y (2016) Fully secure fuzzy identity-based encryption for secure IoT communications. Comput Stand Interfaces 44:117-121

[27] Meshram C (2015) An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem. Inf Process Lett 115(2):351-358 · Zbl 1320.94075

[28] Meshram C, Meshram S (2011) An identity based beta cryptosystem. In: IEEE proceedings of 7th international conference on information assurance and security (IAS 2011) Dec 5-8, pp 298-303 · Zbl 1358.94071

[29] Meshram C, Meshram S (2013) An identity-based cryptographic model for discrete logarithm and integer factoring based cryptosystem. Inf Process Lett 113(10-11):375-380 · Zbl 1358.94071

[30] Meshram C, Meshram SA (2017) Constructing new an ID-based cryptosystem for IFP and GDLP based cryptosystem. J Discrete Math Sci Cryptogr 20(5):1121-1134

[31] Meshram C, Obaidat MS (2015) An ID-based quadratic-exponentiation randomized cryptographic scheme. In: IEEE proceeding of international conference on computer, information and telecommunication systems, (2015), pp 1-5

[32] Meshram C, Powar PL (2016) An efficient identity-based QER cryptographic scheme. Complex Intell Syst 2(4):285-291

[33] Meshram C, Meshram S, Zhang M (2012a) An ID-based cryptographic mechanisms based on GDLP and IFP. Inf Process Lett 112(19):753-758 · Zbl 1250.94059

[34] Meshram C, Huang X, Meshram S (2012b) New Identity-based cryptographic scheme for IFP and DLP based cryptosystem. Int J Pure Appl Math 81(1):65-79 · Zbl 1305.94065

[35] Meshram C, Powar PL, Obaidat MS, Lee CC (2016) An IBE technique using partial discrete logarithm. Procedia Comput Sci 93:735-741

[36] Meshram C, Tseng YM, Lee CC, Meshram SG (2017a) An IND-ID-CPA secure ID-based cryptographic protocol using GDLP and IFP. Informatica 28(3):471-484 · Zbl 1398.94141

[37] Meshram C, Lee CC, Li CT, Chen CL (2017b) A secure key authentication scheme for cryptosystems based on GDLP and IFP. Soft Comput 21(24):7285-7291

[38] Meshram C, Lee CC, Meshram SG, Li CT (2018a) An efficient ID-based cryptographic transformation model for extended chaotic-map-based cryptosystem. Soft Comput. https://doi.org/10.1007/s00500-018-3332-5 · Zbl 1418.94057

[39] Meshram C, Li CT, Meshram SG (2018b) An efficient online/offline ID-based short signature procedure using extended chaotic maps. Soft Comput. https://doi.org/10.1007/s00500-018-3112-2 · Zbl 1415.94469

[40] Meshram C, Obaidat MS, Meshram SG (2018c) Chebyshev chaotic maps based ID-based cryptographic model using subtree and fuzzy-entity data sharing for public key cryptography. Secur Priv 1(1):e12

[41] Meshram C, Powar PL, Obaidat MS, Lee CC, Meshram SG (2018d) Efficient online/offline IBSS protocol using partial discrete logarithm for WSNs. IET Netw 7(6):363-367

[42] Orencik C, Selcuk A, Savas E, Kantarcioglu M (2016) Multi-keyword search over encrypted data with scoring and search pattern obfuscation. Int J Inf Secur 15(3):251-269

[43] Shamir A (1984) Identity-based cryptosystems and signature schemes. In: Proceedings of CRYPTO'84, Lecture Notes in Computer Science, vol 196, pp 47-53 · Zbl 1359.94626

[44] Sun W, Lou W, Hou Y, Li H (2014) Privacy-preserving keyword search over encrypted data in cloud computing. Secur Cloud Comput (Springer, Berlin) 2014:189-212

[45] Tsujii S, Itoh T (1989) An ID-based cryptosystem based on the discrete logarithm problem. IEEE J Sel Areas Commun 7:467-473

[46] Waters B (2005) Efficient identity-based encryption without random oracles. In: Advances in cryptology-CRYPTO 2005, Lecture Notes in Computer Science. Springer, Berlin, pp 114-127 · Zbl 1137.94360

[47] Xu P, Cui G, Lei F (2008) An efficient and provably secure IBE scheme without bilinear map. J Comput Res Dev 45(10):1687-1695

[48] Xu P, Cui G, Fu C, Tang X (2010) A more efficient accountable authority IBE scheme under the DL assumption. Sci China 53(3):581-592

[49] Xu P, Jin H, Wu Q, Wang W (2013) Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack. IEEE Trans Comput 62:2266-2277 · Zbl 1365.94466

[50] Yang X, Wu L, Zhang M, Wei P, Wei L (2011) An ideal lattice based IBE scheme in the standard model. Wuhan Univ J Nat Sci 16(5):439-446

[51] Yu Y, Ni J, Yang H, Mu Y, Susilo W (2014) Efficient public key encryption with revocable keyword search. Secur Commun Netw 7(2):466-472

[52] Zhang L, Wu Q, Domingo-Ferrer J, Qin B, Zeng P (2014) Signatures in hierarchical certificateless cryptography: efficient constructions and provable security. Inf Sci 272:223-237 · Zbl 1341.94024

[53] Zheng M, Xiang Y, Zhou H (2015) A strong provably secure IBE scheme without bilinear map. J Comput Syst Sci 81:125-131 · Zbl 1339.94071