Liu, Weiran; **Liu, Jianwei**; **Wu, Qianhong**; **Qin, Bo**; **Naccache, David**; **Ferradi, Houda**
Efficient subtree-based encryption for fuzzy-entity data sharing. (English) Zbl 1402.68056
Soft Comput. 22, No. 23, 7961-7976 (2018).

Summary: Cloud storage brings strong conveniences for flexible data sharing. When sharing data with a large number of entities described with fuzzy identities, the data owners must leverage a suitable encryption scheme to meet the security and efficiency requirements. (hierarchical) Identity-based encryption is a promising candidate to ensure fuzzy-entity data sharing while meeting the security requirement, but encounters the efficiency difficulty in multireceiver settings. We introduce the notion of subtree-based encryption (SBE) to support multireceiver data sharing mechanism in large-scale enterprises. Users in SBE are organized in a tree structure. Superior users can generate the secret keys to their subordinates. Unlike HIBE merely allowing a single decryption path, SBE enables encryption for a subset of users. We define the security notion for SBE, namely ciphertext indistinguishability against adaptively chosen-sub-tree and chosen-ciphertext attack (IND-CST-CCA2). We propose two secure SBE schemes (SBEs). We first propose a basic SBEs against adaptively chosen-sub-tree and chosen-plaintext attack (IND-CST-CPA), in which we do not allow the attacker to get decryption results from other users in the security game. We then propose a CCA2-secure SBEs from the basic scheme without requiring any other cryptographic primitives. Our CCA2-secure scheme natively allows public ciphertext validity test, which is a useful property when a CCA2-secure SBEs is used to design advanced protocols and auditing mechanisms for fuzzy-entity data sharing.

MSC:

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

Keywords:

subtree-based broadcast encryption; fuzzy-entity data sharing; provable security

Full Text: DOI

References:

[1] Abdalla, Michel; Bellare, Mihir; Catalano, Dario; Kiltz, Eike; Kohno, Tadayoshi; Lange, Tanja; Malone-Lee, John; Neven, Gregory; Paillier, Pascal; Shi, Haixia, Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions, 205-222, (2005), Berlin, Heidelberg · Zbl 1145.94430

[2] Boneh, Dan; Boyen, Xavier, Efficient Selective-ID Secure Identity-Based Encryption Without Random Oracles, 223-238, (2004), Berlin, Heidelberg · Zbl 1122.94355

[3] Boneh, Dan; Boyen, Xavier, Secure Identity Based Encryption Without Random Oracles, 443-459, (2004), Berlin, Heidelberg · Zbl 1104.94019

[4] Boneh, Dan; Franklin, Matt, Identity-Based Encryption from the Weil Pairing, 213-229, (2001), Berlin, Heidelberg · Zbl 1002.94023

[5] Boneh, D.; Franklin, M., Identity-based encryption from the weil pairing, SIAM J Comput, 32, 586-615, (2003) · Zbl 1046.94008

[6] Boneh, Dan; Hamburg, Michael, Generalized Identity Based and Broadcast Encryption Schemes, 455-470, (2008), Berlin, Heidelberg · Zbl 1206.94054

[7] Boneh, Dan; Katz, Jonathan, Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption, 87-103, (2005), Berlin, Heidelberg · Zbl 1079.94535

[8] Boneh, Dan; Boyen, Xavier; Goh, Eu-Jin, Hierarchical Identity Based Encryption with Constant Size Ciphertext, 440-456, (2005), Berlin, Heidelberg · Zbl 1137.94340

[9] Boneh, Dan; Gentry, Craig; Waters, Brent, Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, 258-275, (2005), Berlin, Heidelberg · Zbl 1145.94434

[10] Boyen X, Mei Q, Waters B (2005) Direct chosen ciphertext security from identity-based techniques. In: CCS 2005. ACM, pp 320-329

[11] Canetti, Ran; Halevi, Shai; Katz, Jonathan, A Forward-Secure Public-Key Encryption Scheme, 255-271, (2003), Berlin, Heidelberg · Zbl 1037.68532

[12] Canetti, Ran; Halevi, Shai; Katz, Jonathan, Chosen-Ciphertext Security from Identity-Based Encryption, 207-222, (2004), Berlin, Heidelberg · Zbl 1122.94358

[13] Chen, HC, A trusted user-to-role and role-to-key access control scheme, Soft Comput, 20, 1721-1733, (2016)

[14] Chen, Jie; Wee, Hoeteck, Fully, (Almost) Tightly Secure IBE and Dual System Groups, 435-460, (2013), Berlin, Heidelberg · Zbl 1311.94072

[15] Chen, X.; Li, J.; Huang, X.; Ma, J.; Lou, W., New publicly verifiable databases with efficient updates, IEEE Trans Dependable Secure Comput, 12, 546-556, (2015)

[16] Cocks, Clifford, An Identity Based Encryption Scheme Based on Quadratic Residues, 360-363, (2001), Berlin, Heidelberg · Zbl 0999.94532

[17] Delerablée C (2007) Identity-based broadcast encryption with constant size ciphertexts and private keys. In: ASIACRYPT 2007, vol 4833. LNCS. Springer, Berlin, pp 200-215 · Zbl 1153.94366

[18] Delerablée C, Paillier P, Pointcheval D (2007) Fully collusion secure dynamic broadcast encryption with constant-size ciphertexts or decryption keys. In: Pairing 2007, vol 4575. LNCS. Springer, Berlin, pp 39-59 · Zbl 1151.94502

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

[20] Fiat A, Naor M (1994) Broadcast encryption. In: CRYPTO 1993, vol 773. LNCS. Springer, Berlin, pp 480-491 · Zbl 0870.94026

[21] Garg, Sanjam; Gentry, Craig; Halevi, Shai, Candidate Multilinear Maps from Ideal Lattices, 1-17, (2013), Berlin, Heidelberg · Zbl 1300.94055

[22] Gentry, Craig, Practical Identity-Based Encryption Without Random Oracles, 445-464, (2006), Berlin, Heidelberg · Zbl 1140.94340

[23] Gentry, Craig; Halevi, Shai, Hierarchical Identity Based Encryption with Polynomially Many Levels, 437-456, (2009), Berlin, Heidelberg · Zbl 1213.94102

[24] Gentry, Craig; Silverberg, Alice, Hierarchical ID-Based Cryptography, 548-566, (2002), Berlin, Heidelberg · Zbl 1065.94547

[25] Gentry, Craig; Waters, Brent, Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts), 171-188, (2009), Berlin, Heidelberg · Zbl 1239.94073

[26] Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: STOC 2008. ACM, pp 197-206 · Zbl 1231.68124

[27] Horwitz, Jeremy; Lynn, Ben, Toward Hierarchical Identity-Based Encryption, 466-481, (2002), Berlin, Heidelberg · Zbl 1056.94514

[28] Hu, Yupu; Jia, Huiwen, Cryptanalysis of GGH Map, 537-565, (2016), Berlin, Heidelberg · Zbl 1385.94044

[29] Huan, J.; Yang, Y.; Huang, X.; Yuen, TH; Li, J.; Cao, J., Accountable mobile e-commerce scheme via identity-based plaintext-checkable encryption, Inf Sci, 345, 143-155, (2016)

[30] Huang, X.; Xiang, Y.; Chonka, A.; Zhou, J.; Deng, RH, A generic framework for three-factor authentication: preserving security and privacy in distributed systems, IEEE Trans Parallel Distrib Syst, 22, 1390-1397, (2011)

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

[32] Kim, J.; Susilo, W.; Au, MH; Seberry, J., Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext, IEEE Trans Inf Forensics Secur, 10, 679-693, (2015)

[33] Lewko, Allison; Waters, Brent, New Techniques for Dual System Encryption and Fully Secure HIBE with Short Ciphertexts, 455-479, (2010), Berlin, Heidelberg · Zbl 1274.94092

[34] Lewko, Allison; Waters, Brent, New Proof Methods for Attribute-Based Encryption: Achieving Full Security through Selective Techniques, 180-198, (2012), Berlin, Heidelberg · Zbl 1296.94128

[35] Lewko, Allison; Okamoto, Tatsuaki; Sahai, Amit; Takashima, Katsuyuki; Waters, Brent, Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption, 62-91, (2010), Berlin, Heidelberg · Zbl 1279.94095

[36] Libert, Benoît; Paterson, Kenneth G.; Quaglia, Elizabeth A., Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model, 206-224, (2012), Berlin, Heidelberg · Zbl 1290.94107

[37] Liu, Weiran; Liu, Jianwei; Wu, Qianhong; Qin, Bo, Hierarchical Identity-Based Broadcast Encryption, 242-257, (2014), Cham · Zbl 1337.94050

[38] Liu W, Liu X, Liu J, Wu Q, Zhang J (2015a) Auditing and revocation enabled role-based access control over outsourced private ERHS. In: HPCC, pp 336-341

[39] Liu, Zheli; Weng, Jian; Li, Jin; Yang, Jun; Fu, Chuan; Jia, Chunfu, Cloud-based electronic health record system supporting fuzzy keyword search, Soft Computing, 20, 3243-3255, (2015)

[40] Liu, W.; Liu, J.; Wu, Q.; Qin, B.; Li, Y., Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption, Int J Inf Secur, 15, 35-50, (2016)

[41] Maurer UM, Yacobi Y (1991) Non-interactive public-key cryptography. In: EUROCRYPT 1991, vol 547. LNCS. Springer, Berlin, pp 498-507 · Zbl 0825.94189

[42] Qin, B.; Wu, Q.; Zhang, L.; Farràs, O.; Domingo-Ferrer, J., Provably secure threshold public-key encryption with adaptive security and short ciphertexts, Inf Sci, 210, 67-80, (2012) · Zbl 1250.94042

[43] Ren, Y.; Gu, D., Fully CCA2 secure identity based broadcast encryption without random oracles, Inf Process Lett, 109,

527-533, (2009) · Zbl 1211.68187

[44] Seo, Jae Hong; Kobayashi, Tetsutaro; Ohkubo, Miyako; Suzuki, Koutarou, Anonymous Hierarchical Identity-Based Encryption with Constant Size Ciphertexts, 215-234, (2009), Berlin, Heidelberg · Zbl 1227.94064

[45] Shamir A (1985) Identity-based cryptosystems and signature schemes. In: CRYPTO 1984, vol 196. LNCS. Springer, Berlin, pp 47-53 · Zbl 1359.94626

[46] Wang J, Chen X, Huang X, You I, Xiang Y (2015) Verifiable auditing for outsourced database in cloud computing. IEEE Trans Comput 64(11):3293-3303 · Zbl 1360.68187

[47] Waters, Brent, Efficient Identity-Based Encryption Without Random Oracles, 114-127, (2005), Berlin, Heidelberg · Zbl 1137.94360

[48] Waters, Brent, Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions, 619-636, (2009), Berlin, Heidelberg · Zbl 1252.94101

[49] Wu Q, Qin B, Zhang L, Domingo-Ferrer J, Farràs O, Manjón J (2016) Contributory broadcast encryption with efficient encryption and short ciphertexts. IEEE Trans Comput 65(2):466-479 · Zbl 1360.94337

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

[51] Zhang, M.; Yang, B.; Takagi, T., Anonymous spatial encryption under affine space delegation functionality with full security, Inf Sci, 277, 715-730, (2014) · Zbl 1354.94054

[52] Zhou X, Liu J, Liu W, Wu Q (2016) Anonymous role-based access control on e-health records. In: ASIACCS 2016. ACM, pp 559-570