SCIENCE CHINA
Information Sciences

• LETTER •

September 2016, Vol. 59 099105:1–099105:3
doi: 10.1007/s11432-016-0012-9

Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption

Kai ZHANG[1], Jianfeng MA[2*], Jiajia LIU[3] & Hui LI[3]

[1]*School of Telecommunications Engineering, Xidian University, Xi'an* 710071*, China;*
[2]*School of Computer Science and Technology, Xidian University, Xi'an* 710071*, China;*
[3]*School of Cyber Engineering, Xidian University, Xi'an* 710071*, China*

Received January 4, 2016; accepted March 7, 2016; published online August 18, 2016

Citation Zhang K, Ma J F, Liu J J, et al. Adaptively secure multi-authority attribute-based encryption with verifiable outsourced decryption. Sci China Inf Sci, 2016, 59(9): 099105, doi: 10.1007/s11432-016-0012-9

Dear editor,

Attribute-based encryption (ABE) was first introduced by Sahai and Waters [1] where the decryption ability of a user is based on his attributes. Later, it was divided into ciphertext-policy ABE (CP-ABE) and key-policy ABE (KP-ABE) [2]. In CP-ABE, a secret key is associated with user attributes and a ciphertext is associated with a boolean formula; a user can decrypt the ciphertext if and only if his attributes satisfy the boolean formula. In KP-ABE, however, such relationship is inverted, i.e., a secret key is associated with a Boolean formula and a ciphertext is associated with attributes.

One common feature of these ABE schemes [1,2] is that a central authority is required to control all attributes and issue all private keys, even across different attribute domains. In many scenarios, however, it is impractical for a single party to act as the central authority over all attribute domains. Consider the e-healthcare cloud system shown in Figure 1, wherein a data owner wants to share some sensitive medical data with users having the attributes of "doctor" and "professor". Note that the attribute of "doctor" was issued by a hospital, while the attribute "professor" was issued by a university. Owing to the difficulties in verifying attributes and issuing private keys for users among different domains, the ABE scheme with a single central authority is obviously unsuitable.

To address this issue, a multi-authority ABE scheme [3] is presented, where different authorities issue secret keys for different attributes sets. As shown in Figure 1, for the user who is both a doctor and a professor, the university issues the secret key associated with the attribute "professor" and the hospital issues the secret key associated with the attribute "doctor" for him. To protect the patients' health information, the data owner encrypts his medical data using multi-authority ABE and stores the ABE ciphertext CT in a cloud server. Doctors often need to access patients' medical data from the cloud server by decrypting the ABE ciphertexts on mobile devices when making rounds. However, this presents a significant challenge for users who decrypt data on mobile devices because one common drawback of multi-authority ABE is the poor efficiency of its decryption algorithm, which imposes one pairing operation on every node satisfying the formula.

Green et al. [4] proposed ABE schemes with outsourced decryption to save the local computation time for the users. As shown in the right of Figure 1, the proxy uses a transformation key

* Corresponding author (email: jfma@mail.xidian.edu.cn)
The authors declare that they have no conflict of interest.

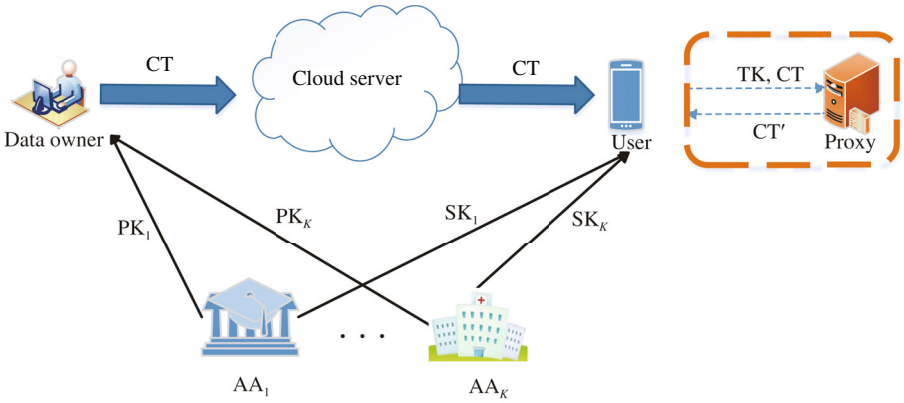

Figure 1 (Color online) Illustration of multi-authority ABE with outsourced decryption.

TK to transform the ABE ciphertext CT into a simple ciphertext CT′ that can be decrypted by the user without a pairing operation. However, all the available ABE schemes [4, 5] with outsourced decryption were constructed only for the single-authority setting; they cannot tackle the challenge for users who decrypt ABE ciphertexts on mobile devices in the multi-authority setting. How to construct ABE schemes with outsourced decryption for the multi-authority setting while simultaneously minimizing the computation overhead at the users' side remains a challenging task[1)]. Note also that the previous constructions of ABE with outsourced decryption were proved only to be selectively secure under non-interactive assumptions, which is actually a limited security model as the adversary needs to declare the target he will attack before seeing the global parameters.

In this letter, we provide a construction of multi-authority CP-ABE with verifiable outsourced decryption based on the Lewko-Waters (LW) scheme [7], in which neither any central authority nor any coordination between different authorities is required. Our construction allows the encryption algorithm to specify any access formula that can be expressed in terms of a linear secret-sharing scheme (LSSS). It reduces the required decryption operations for the user from $2|I|$ pairings and $|I|$ exponentiations in [7] to only $|I|$ exponentiations, where $|I|$ is related to the access formula and user attributes. In addition, we will prove that this construction is adaptively CPA-secure in the random oracle model and that the proof of its adaptive security is a black box reduction to the security of the LW scheme [7].

An adaptively secure construction. We now present our adaptively secure multi-authority CP-ABE scheme with outsourced decryption based on [7]. The scheme is constructed in the composite-order bilinear group G. We refer the reader to our supplementary file for the necessary background information and definition of multi-authority CP-ABE with outsourced decryption.

Global Setup(λ). The global setup algorithm takes as input a security parameter λ. It then chooses a bilinear group G of composite order $N = p_1p_2p_3$ (three distinct primes), a generator g_1 of G_{p1}, and a hash function $H : \{0,1\}^* \to G$. The global public parameters are published as $\mathrm{GP} = \{N, G, G_{p1}, g_1, H\}$. We view H as a random oracle.

Authority Setup(GP). For each attribute i belonging to the authority A_j, A_j chooses two random exponents $\alpha_i, y_i \in Z_N$. The public key is published as $\mathrm{PK}_j = \{e(g_1,g_1)^{\alpha_i}, g_1^{y_i} \forall i\}$. The authority A_j sets $\mathrm{SK}_j = \{\alpha_i, y_i \forall i\}$ as its secret key.

Encrypt$(\mathrm{GP}, \{\mathrm{PK}_j\}, M, (A,\rho))$. The encryption algorithm takes as input the global parameters GP, the public keys of the relevant authorities, a message M, and an LSSS access structure (A,ρ). A is an $n \times l$ matrix and ρ maps its rows to attributes. The algorithm first chooses a random $s \in Z_N$ and a random vector $v \in Z_N^l$ with s as its first entry. For $x = 1$ to l, it calculates $\lambda_x = A_x \cdot v$, where A_x is row x of A. The algorithm also chooses a random vector $\omega \in Z_N^l$ with 0 as its first entry. For $x = 1$ to l, it calculates $\omega_x = A_x \cdot \omega$. For each $x \in \{1, 2, \ldots, l\}$, it chooses a random $r_x \in Z_N$. The ciphertext CT is computed as

$$C_0 = Me(g_1,g_1)^s,$$

$$C_{1,x} = e(g_1,g_1)^{\lambda_x} e(g_1,g_1)^{\alpha_{\rho(x)} r_x},$$

$$C_{2,x} = g_1^{r_x}, \quad C_{3,x} = g_1^{y_{\rho(x)} r_x} g_1^{\omega_x}.$$

KeyGen$(\mathrm{GID}, S, \{\mathrm{SK}_j\}, \mathrm{GP})$. The key generation algorithm takes as input an identity GID, the

1) Although Li and Ma [6] made efforts to realize multi-authority ABE with outsourced decryption, there are flaws (shown in the supplementary file) in their work that prevented them from achieving the claimed security or multi-authority goals.

global parameters GP, the secret keys of the relevant authorities, and a set S of attributes. To create a key for GID for attribute i belonging to an authority, the authority computes $K_{i,\mathrm{GID}} = g_1^{\alpha_i} H(\mathrm{GID})^{y_i}$. The private key is $\mathrm{SK}_{S,\mathrm{GID}} = \{K_{i,\mathrm{GID}} = g_1^{\alpha_i} H(\mathrm{GID})^{y_i}\}_{i\in S}$.

TKGen($\mathrm{SK}_{S,\mathrm{GID}}$). For each $i \in S$, the transformation key generation algorithm chooses a random value $z_i \in Z_N^*$. It sets the transformation key $\mathrm{TK}_{S,\mathrm{GID}}$ as $\{K'_{i,\mathrm{GID}}\}_{i\in S} = \{K_{i,\mathrm{GID}}^{1/z_i}\}_{i\in S}$ and the retrieving key $\mathrm{RK}_{S,\mathrm{GID}}$ as $\{z_i\}_{i\in S}$.

Transform($\mathrm{TK}_{S,\mathrm{GID}}, \mathrm{CT}$). The transformation algorithm takes as input a transformation key $\mathrm{TK}_{S,\mathrm{GID}} = \{K'_{i,\mathrm{GID}}\}_{i\in S}$ for a set S and a ciphertext $(C_0, \{C_{1,x}, C_{2,x}, C_{3,x}\}_{x\in\{1,2,\ldots,l\}})$ for an access structure (A, ρ). If S does not satisfy the access structure (A, ρ), it outputs $\perp$. Suppose that S satisfies the access structure (A, ρ) and let $I \subset \{1, 2, \ldots, l\}$ be defined as $I = \{x : \rho(x) \in S\}$. The transformation algorithm chooses the constants $\{c_x \in Z_N\}_{x\in I}$ such that $\sum_{x\in I} c_x A_x = (1, 0, \ldots, 0)$ and computes

$$T_1 = \prod_{x\in I} (C_{1,x} \cdot e(H(\mathrm{GID}), C_{3,x}))^{c_x},$$

$$\{T_{2,x} = e(K'_{\rho(x),\mathrm{GID}}, C_{2,x})^{c_x}\}_{x\in I}.$$

It outputs the partially decrypted ciphertext CT' as $(T_0 = C_0, T_1, \{T_{2,x}\}_{x\in I})$.

Decrypt$_{\mathrm{out}}$($\mathrm{RK}_{S,\mathrm{GID}}, \mathrm{CT}'$). The decryption algorithm takes as input a retrieving key $\mathrm{RK}_{S,\mathrm{GID}} = \{z_i\}_{i\in S}$ and a partially decrypted ciphertext $\mathrm{CT}' = (T_0, T_1, \{T_{2,x}\}_{x\in I})$. It computes $M = T_0 \prod_{x\in I} T_{2,x}^{z_{\rho(x)}} / T_1$.

We prove that our scheme is adaptively secure by a direct black box reduction to the underlying LW scheme [7]. The LW scheme that we reduce security to is adaptively CPA-secure based on three static assumptions in the random oracle model.

Theorem 1. The above multi-authority CP-ABE scheme with outsourced decryption is adaptively CPA-secure, assuming that the LW scheme [7] is an adaptively CPA-secure CP-ABE scheme.

Owing to space constraints, we defer the proof of Theorem 1 to the supplementary file.

Efficient and verifiable. As the pairing and exponentiation operations in prime order groups are 1–2 orders of magnitude faster than those in composite order groups [8], we provide another much more efficient multi-authority CP-ABE scheme with verifiable outsourced decryption in prime order bilinear groups. It supports a large universe without the restriction that "each attribute is used only once in each access policy" and is proved to be statically secure in the random oracle model. Furthermore, we can extend our constructions to achieve verifiability by the method from [5]. Owing to space constraints, we present these constructions, their security proofs, and the efficiency analysis in the supplementary file.

Conclusion. In this letter, we have investigated the multi-authority ABE for user decryption on mobile phones. An adaptively secure multi-authority ABE scheme with outsourced decryption has been proposed, which requires no pairing operations for user decryption. In the supplementary file, we improve our scheme to achieve verifiability and provide another much more efficient statically secure construction. Note that the latter scheme can be an alternative to the former one since it achieves a relatively lower security level but with much higher performance.

Acknowledgements This work was supported by National High Technology Research and Development Program of China (863 Program) (Grant No. 2015AA016007), and National Natural Science Foundation of China (Grant Nos. U1405255, 61472310).

Supporting information The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Sahai A, Waters B. Fuzzy identity-based encryption. In: Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, 2005. 457–473
2 Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, 2006. 89–98
3 Chase M. Multi-authority attribute based encryption. In: Proceedings of the 4th Theory of Cryptography Conference, Amsterdam, 2007. 515–534
4 Green M, Hohenberger S, Waters B. Outsourcing the decryption of ABE ciphertexts. In: Proceedings of the 20th USENIX Security Symposium, San Francisco, 2011. 523–538
5 Qin B, Deng R, Liu S, et al. Attribute-based encryption with efficient verifiable outsourced decryption. IEEE Trans Inf Foren Secur, 2015, 10: 1384–1393
6 Li K, Ma H. Outsourcing decryption of multi-authority ABE ciphertexts. Int J Netw Secur, 2014, 16: 286–294
7 Lewko A, Waters B. Decentralizing attribute-based encryption. In: Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, 2011. 568–588
8 Rouselakis Y, Waters B. Efficient statically-secure large-universe multi-authority attribute-based encryption. In: Financial Cryptography and Data Security. Berlin: Springer, 2015. 315–332