2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

An Attribute-Based Encryption Scheme Secure Against Malicious KGC

Guoyan Zhang, Lei Liu, Yang Liu
School of Computer Science and Technology
Shandong University
Jinan, China
Email: guoyanzhang@sdu.edu.cn

***Abstract*—Different from identity-based encryption scheme, an attribute-based encryption scheme is a scheme in which each user is identified by a set of attributes, and some function of those attributes is used to determine decryption ability for each ciphertext. But key escrow problem is also the inherent problem in attribute-based encryption scheme.**

To avoid the problem of key escrow, this paper presents an attribute-based encryption scheme by use of another secret key that the KGC cannot obtain. Following, based on a concrete attribute-based encryption scheme insecure against malicious KGC, we give a scheme secure against malicious KGC. Furthermore, compared with the original scheme, our scheme doesn't increase the length of the public key and the ciphertext. The security of our scheme is obtained directly from the security of the original scheme.

***Keywords*-Attribute-Based Encryption Scheme; Malicious KGC, Key Escrow; Key-policy; Cipher-policy.**

I. Introduction

With the development of the internet of things and cloud computing, several distributed files and information systems require complex access-control mechanisms, where access decisions depend upon attributes of the protected data and access policies assigned to users. With the increasing number of worm attacks and other forms of intrusion, a trusted server cannot be unequal to this job and maintaining the security of any particular host is also becoming increasingly difficult. A natural solution to this problem is to encrypt stored data in order to reduce data vulnerability in the event that a storage server is compromised. However, traditional public key encryption or identity-based encryption methods require that data be encrypted to one particular user's public key or identity and are unsuitable for expressing more complex access control policies.

Sahai and Waters [1] addressed this issue by introducing the concept of attribute-based encryption (ABE). In attribute-based encryption schemes, a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. Two variants of ABE were subsequently proposed. In the key-policy variant (KP-ABE) of Goyal, Pandey, Sahai and Waters (GPSW) [2], every ciphertext is associated with a set of attributes, and every user secret key is associated with a threshold access structure on attributes. Decryption is enabled if and only if the ciphertext attributes set satisfies the access structure on the user secret key. In the ciphertext-policy variant (CP-ABE) of Bethencourt, Sahai and Waters (BSW) [3], the situation is reversed: attributes are associated with user secret keys and access structures with ciphertexts. Following, in order to make the access structure more expressive, many schemes have been presented ([2], [3], [4], [5], [6], [7], [8]). Simultaneously, schemes ([6], [9], [10], [11]) were devoted to get constant-size ciphertexts.

Similar to identity-based encryption schemes, the KGC is able to compute the private key corresponding to any attribute, and it has to be completely trusted. The KGC is free to engage in malicious activities without any risk of being confronted in a court of law. The malicious activities could include: decrypting and reading messages meant for any user, which is called the key escrow problem. One approach to mitigate the key escrow problem is to employ multi-authority attribute-based encryption, which allows the sender to specify for each authority k a set of attributes monitored by that authority and a number d_k so that the message can be decrypted only by a user who has at least d_k of the given attributes from every authority. Multi-authority attribute-based encryption also allow any number of attribute authorities to be corrupted, and guarantee the security of encryption as long as the required attributes cannot be obtained exclusively from those authorities and the trusted authority remains honest. This is an attractive solution and successfully avoids placing trust in a single entity by making the system distributed. However, this solution comes at the cost of introducing extra infrastructure and communication. It is burdensome for a user to go to several key authorities, prove his attributes to each of them and get the corresponding private key component (which has to be done over a secure channel).

A. Related Work

Building on the ideas from [12], Chase proposed a solution for multi-authority attribute-based encryption, provided that a trusted central authority is available [13], but a global identifier is a "linchpin" for tying users' keys together. Her system relied on a central authority and was limited

978-0-7695-4745-9/12 $26.00 © 2012 IEEE
DOI 10.1109/TrustCom.2012.74

to expressing a strict "AND" policy over a pre-determined set of authorities. Müller, Katzenbeisser, and Eckert([14], [15]) gave a system with a centralized authority that realized any LSSS access structure. Their proof was limited to non-adaptive queries. The system achieved roughly the same functionality as the engineering approach above, except one could still acquire attributes from additional authorities without revisiting the central authority. The scheme [16] removed the central authority using a distributed PRF; However, the same limitations of an AND policy of a determined set of authorities remained. Lin et. al. [17] gave a threshold based scheme that is also somewhat decentralized. The set of authorities is fixed ahead of time, and they must interact during the system setup. The system was only secure up to collusions of m users, where m is a system parameter chosen at setup such that the cost of operations and key storage scales with m. Scheme [18] proposed a new multi-authority attribute-based encryption system. In their system, any party can become an authority and there is no requirement for any global coordination other than the creation of an initial set of common reference parameters. (These will be created during a trusted setup.) A party can simply act as an authority by creating a public key and issuing private keys to different users that reflect their attributes. Different authorities need not even be aware of each other.

B. Our Contributions.

We introduce a new approach to mitigate the key escrow problem in attribute-based encryption scheme. Different with the previous techniques, there are two third parties: one is the key generation center (KGC) who gives the partial private keys corresponding to the attributes of users, and another is the dealer who distributes to the user the secret keys that the KGC cannot obtain. In contrast to attribute-based encryption scheme under multiple authorities, our approach avoids extra infrastructure and communication.

C. Organization

The paper is organized as follows. In section 2 we give the preliminary including the definition of attribute-based encryption scheme and the security assumptions. We give the concrete scheme in section 3, and in section 4 we describe the security of our scheme. Finally, we conclude in section 5.

II. ATTRIBUTE-BASED ENCRYPTION SCHEME SECURE AGAINST MALICIOUS KGC

According to the vary types of attribute-based encryption, we give two definitions:

A. Definition

Definition 1. (Ciphertext-Policy Attribute-Based Encryption Scheme). A generic ciphertext-policy attribute-based encryption scheme consists of the following four algorithms:

-SetUp: a probabilistic polynomial time (PPT) algorithm run by a key generation center (KGC) given a security parameter k and an universe of attributes U as input which outputs a randomly chosen master secret key msk and master public key mpk. The master public key mpk includes a description of the message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.

-PrivateKeyExtract: given the master public key mpk, master secret key msk and an attributes set $S \in U$ for entity A, the KGC runs this PPT algorithm to generate the private key d_A for the attributes set. Then the private key d_A is transported to entity A over a confidential and authentic channel.

-Encrypt: given a plaintext $M \in \mathcal{M}$, master public key mpk, an access tree T over the universe of attributes U as inputs, a sender runs this PPT algorithm to create a ciphertext $C \in \mathcal{C}$ or the null symbol $\perp$ indicating an encryption failure.

-Decrypt: given master public key mpk, the entity's private key d_A, and the ciphertext $C \in \mathcal{C}$ that was encrypted under the access tree T as inputs, the entity as a recipient runs this deterministic algorithm to get a decryption σ, which is a plaintext message if the set S of attributes satisfies the access tree T.

Definition 2. (Key-Policy Attribute-Based Encryption Scheme). A generic key-policy attribute-based encryption scheme consists of the following four algorithms:

-SetUp: a probabilistic polynomial time (PPT) algorithm run by a key generation center (KGC) given a security parameter k and an universe of attributes U as input which outputs a randomly chosen master secret key msk and master public key mpk. The master public key mpk includes a description of the message space $\mathcal{M}$ and ciphertext space $\mathcal{C}$.

-PrivateKeyExtract: given the master public key mpk, master secret key msk, an access tree T over the universe of attributes U and an attributes set $S \in U$ for entity A, , the KGC runs this PPT algorithm to generate the partial private key d_A for the attributes set S. Then the partial private key d_A is transported to entity A over a confidential and authentic channel.

-Encrypt: given a plaintext $M \in \mathcal{M}$, master public key mpk as inputs, a sender runs this PPT algorithm to create a ciphertext $C \in \mathcal{C}$ or the null symbol $\perp$ indicating an encryption failure.

-Decrypt: given master public key mpk, the entity's private key d_A, and the ciphertext $C \in \mathcal{C}$ that was encrypted under the access tree T as inputs, the entity as a recipient runs this deterministic algorithm to get a decryption σ, which is a plaintext message if the set S of attributes satisfies the access tree T.

B. Security Model for Attribute-Based Encryption

We give the security model of the key-policy attribute-based encryption scheme as follows:

Selective-Set Model for ABE

Init The adversary declares the set of attributes, γ , that he wishes to be challenged upon.

Setup The challenger runs the Setup algorithm of ABE and gives the public parameters to the adversary.

Phase 1 The adversary is allowed to issue queries for private keys for many access structures A_j, where γ cannot satisfy access structures A_j for all j.

Challenge The adversary submits two equal-length messages M_0 and M_1. The challenger flips a random coin $b \in \{0, 1\}$, and encrypts M_b with γ. The ciphertext is passed to the adversary.

Phase 2 Phase 1 is repeated.

Guess The adversary outputs a guess b' of b.

The advantage of an adversary A in this game is defined as $Pr[b' = b] - \frac{1}{2}$.

We note that the model can easily be extended to handle chosen-ciphertext attacks by allowing for decryption queries in Phase 1 and Phase 2.

Definition 5 An attribute-based encryption scheme is secure in the selective-set model of security if all polynomial time adversaries have at most a negligible advantage in the selective-set game.

C. Complexity Assumptions

The following are the complexity assumption related with our scheme:

Definition 4 (Decisional Bilinear Diffie-Hellman (BDH) Assumption). Suppose a challenger chooses $a, b, c, z \in \mathcal{Z}_p$ at random. The Decisional BDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$ from the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ with more than a negligible advantage.

Definition 5 (Decisional Modified Bilinear Diffie-Hellman (MBDH) Assumption). Suppose a challenger chooses $a, b, c, z \in \mathcal{Z}_p$ at random. The Decisional MBDH assumption is that no polynomial-time adversary is to be able to distinguish the tuple $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^{\frac{ab}{c}})$ from $(A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$ with more than a negligible advantage.

III. Concrete Attribute-Based Encryption Scheme Secure against the Malicious KGC

A. Construction

There are two third parties, one is the KGC who generates the partial private keys for the attributes of all the users, and another is the dealer who is responsible for the secret key that KGC don't know for all the users.

Let (G, G_T) be bilinear map groups of order $p > 2^k$ and let $e : G \times G \to G_T$ denote a bilinear map. Let g be a generator for G. k is the security parameter. $\Delta_{i,s}(x), i \in \mathcal{Z}_p$ is the lagrange coefficient, and S is a set of elements in $\mathcal{Z}_p$. $\mathcal{U}$ is the universal set of attributes which is associated with a unique element in ${\mathcal{Z}^*}_p$. Our construction is as follows:

Setup(d)**:** First, we take the integers $1, 2, \ldots, |\mathcal{U}|$ to be the universe.

Next, choose $t_1, \ldots, t_{|\mathcal{U}|}$ uniformly at random from $\mathcal{Z}_p$. Finally, choose y uniformly at random in $\mathcal{Z}_p$. The published public keys are:

$$T_1 = g^{t_1}, \ldots, T_{|\mathcal{U}|} = g^{t_{|\mathcal{U}|}}, Y = e(g, g)^y.$$

The master key is:

$$t_1, \ldots, t_{|\mathcal{U}|}, y.$$

PartialPrivateKeyExtract. In order to generate a partial private key for attributes set ω, the KGC picks $(d-1)$ degree polynomial q randomly so that $q(0) = y$. The partial private key is

$$D_i = g^{\frac{q(i)}{t_i}}, i \in \omega.$$

SetSecretKey. The dealer picks $(d-1)$ degree polynomial f randomly so that $f(0) = x$. Return secret value $f(i), i \in \omega$, and publishes the public key $Z = Y^x$.

Encrypt. In order to encrypt message $m \in G_T$ with attributes set ω', pick $s \in \mathcal{Z}_P$ and compute the ciphertext as follows:

$$C = (C_0, C_1, C_2) = (\omega', m \cdot Z^s, E_i = T_i^s, i \in \omega').$$

Decryption.: Suppose that a ciphertext, C, is encrypted with a key for attributes set ω' and we have the partial private key D_i and secret key $f(i)$ for $i \in \omega$, where $|\omega \bigcap \omega| \geq d$. Choose an arbitrary d-element subset, S, of $\omega \bigcap \omega$ and compute

$$x = f(0) = \sum_{i \in S} f(i)\Delta_{i,s}(0),$$

$$m = C_1 / \prod_{i \in S} (((e(D_i, E_i))^{\Delta_{i,s}(0)})^x.$$

Correctness:

$$C_1 / \prod_{i \in S} (((e(D_i, E_i))^{\Delta_{i,s}(0))^x}$$

$$= me(g, g)^{xys} / \prod_{i \in S} (e(g^{\frac{q(i)}{t_i}}, g^{st_i})^{\Delta_{i,s}(0)x})$$

$$= me(g, g)^{xys} / \prod_{i \in S} (e(g, g)^{sq_i})^{\Delta_{i,s}(0)x})$$

$$= m$$

IV. The Security Analysis

Theorem 1. If the Modified Bilinear Diffie-Hellman problem is hard, then our attribute-based encryption scheme is IND-CPA secure.

Proof. Suppose $\mathcal{A}$ is a polynomial-time adversary, and he can success with advantage ϵ, then we can construct a scheme $\mathcal{B}$ to resolve the Modified Bilinear Diffie-Hellman problem with advantage ϵ by calling $\mathcal{A}$. The following is the proceed:

$\mathcal{B}$ sets the groups (G, G_T) be bilinear map groups of order $p > 2^k$ and let $e : G \times G \to G_T$ denote a bilinear map. Let g be a generator for G, and he is given the tuple$(A, B, C, Z) = (g^a, g^b, g^c, Z)$.

$\mathcal{B}$ runs $\mathcal{A}$ to obtain a challenge attributes set α.

Setup. $\mathcal{B}$ sets the public key as follows. He sets $Y = e(g, A) = e(g, g)^a$. For all attributes $i \in \alpha$, he sets $T_i = C^{t_i} = g^{ct_i}$ for random t_i, and for all $i \in \mathcal{U} - \alpha$, he sets $T_i = g^{\omega i}$ for random ω_i.

phase1

Partial Private Key Extract. $\mathcal{A}$ makes request for partial private key for attributes set γ . If $|\gamma \cap \alpha| < d$. Set three sects Γ, Γ_1, S, where:

$$\Gamma = \gamma \cap \alpha, \Gamma \subseteq \Gamma_1 \subseteq \gamma$$

$$|\Gamma_1| = d - 1,$$

and set

$$S = \Gamma_1 \cup \{0\}.$$

We can randomly define the partial private key for Γ_1 as follows:

For $i \in \Gamma$, Set

$$D_i = g^{s_i}.$$

Where s_i is chosen randomly.

For $i \in \Gamma_1 - \Gamma$, Set

$$D_i = g^{\frac{\lambda_i}{\omega_i}}.$$

Where λ_i is chosen randomly.

Then from the above definition, $\mathcal{B}$ has chosen a $(d-1)$ degree polynomial $q(x)$ by choose $(d-1)$ random value and set $q(0) = a$. Especially, $i \in \Gamma, q(i) = ct_i s_i$, and for $i \in \Gamma_1 - \Gamma, q(i) = \lambda_i$.

$\mathcal{B}$ can define the other partial private key D_i:

$$D_i = (\prod_{j \in \Gamma} C^{\frac{t_j s_j \Delta_{j,S(i)}}{\omega_i}})(\prod_{j \in \Gamma_1 - \Gamma} g^{\frac{\lambda_j \Delta_{j,S(i)}}{\omega_i}}) Y^{\frac{\Delta_{0,S(i)}}{\omega_i}}.$$

Secret Key Extract. $\mathcal{A}$ asks a secret key for attributes set β, if $|\beta| > d$, choose a polynomial $f(x)$ and compute $f(i)$ for $i \in \beta$, set $f(0) = x$. Compute $Y_1 = Y^x$. If $|\beta| < d$, choose $|\beta|$ random values to $\mathcal{A}$.

Public Key Extract Publish $Y_1 = Y^x$.

Challenge. $\mathcal{A}$ submits two challenge message M_1, M_0 to $\mathcal{B}$, and $\mathcal{B}$ chooses a bit $b \in \{0, 1\}$. The ciphertext is output as:

$$C = (C_0, C_1, C_2) = (\alpha, m_b \cdot Y_1, E_i = B^{t_i}, i \in \alpha).$$

phase2 $\mathcal{B}$ acts exactly as it do in phase 1.

Guess If $\mathcal{A}$ correctly guesses the bit b, $\mathcal{B}$ will decide that the tuple(A, B, C, Z) is the Modified Bilinear Diffie-Hellman tuple, else it is not.

From the above analysis, we find that the advantage of $\mathcal{B}$ is equal to the advantage of $\mathcal{A}$.

Theorem 2. If the discrete logarithm problem is hard, then our attribute-based encryption scheme is secure against malicious KGC.

Proof. From the public key Y, Y_1, we can see if the KGC wants to get the secret key x, he must compute the discrete logarithm $\log_y^{Y_1}$, but the discrete logarithm problem is hard, and the KGC cannot obtain the secret key and he cannot obtain any information about the plaintext.

V. Conclusion

In order to mitigate the key escrow problem, this paper gives a new approach which adds new secret key to the user by the dealer, and the KGC don't know the secret key. Compared with the multi-authority, our approach is simple, and the length of the ciphertext and the public key published to the sender is not increased. Simultaneously, we present an attribute-based encryption scheme secure against the malicious KGC by modifying the scheme [1] using this new technique. Furthermore, compared with the original scheme, our scheme has the same length of the public key and the ciphertext. The security of our scheme is obtained directly from the security of the original scheme. But, our scheme only admits the "threshold" access control, and an efficient scheme admitting expressive access structure secure against malicious KGC is our further research.

Acknowledgment

This work is Supported by the National Natural Science Foundation of China(No.60873232), Open Research Fund from Key Laboratory of Computer Network and Information Integration In Southeast University, Ministry of Education, China, Shandong Natural Science Foundation(No.Y2008A22) and Independent Innovation Foundation of Shandong University(No. 2012TS070).

References

[1] A. Sahai and B. Waters. Fuzzy identity based encryption. In Advances in Cryptology-Eurocrypt, volume 3494 of LNCS, pages 457-473, 2005.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and Communications Security (CCS06), pages 89-98, 2006.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland), pages 321-334, 2007.

[4] Rafail Ostrovsky, Amit Sahai, and Brent Waters. Attribute-based encryption with non-monotonic access structures. In ACM Conference on Computer and Communications Security, pages 195-203, 2007.

[5] Lewko, A., Sahai, A., Waters, B. Revocation Systems with Very Small Private Keys. In: IEEE Symposium on Security and Privacy, 2010.

[6] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu. Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts. In PKC 2011, Vol 6571 of LNCS. pages 90-108, 2011, Springer Verlag.

[7] Ling Cheung and Calvin C. Newport. Provably secure ciphertext policy abe. In ACM Conference on Computer and Communications Security, pages 456-465, 2011.

[8] Vipul Goyal, Abishek Jain, Omkant Pandey and Amit Sahai. Bounded ciphertext policy attribute-based encryption. In ICALP, 2008.

[9] Daza, V., Herranz, J., Morillo, P., R'afols, C. Extended access structures and their cryptographic applications. To appear in Applicable Algebra in Engineering, Communication and Computing (2008), http://eprint.iacr.org/2008/502

[10] Emura, K., Miyaji, A., Nomura, A., Omote, K., Soshi, M. A ciphertextpolicy attribute-based encryption scheme with constant ciphertext length. In: Bao, F., Li, H., Wang, G. (eds.) ISPEC 2009. Vol 5451 of LNCS, pages 13-23, 2009, Springer, Heidelberg .

[11] J. Herranz, F. Laguillaumie, C. Rafols. Constant-Size Ciphertexts in Threshold Attribute-Based Encryption. In PKC'2010. Vol 6056 of LNCS, 2010, Springer.

[12] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In R. Cramer, editor, Advances in CryptologyCEUROCRYPT 2005, volume 3494 of Lecture Notes in Computer Science, pages 457-473, 2005.

[13] M. Chase. Multi-authority Attribute Based Encryption. In S.P. Vadhan, editor, Theory of Cryptography C TCC 2007, volume 4392 of Lecture Notes in Computer Science, pages 515-534, 2007, Springer-Verlag.

[14] S. Müller, S. Katzenbeisser, and C. Eckert. Distributed attribute-based encryption. In ICISC, pages 20-36, 2008.

[15] S. Müuller, S. Katzenbeisser, and C. Eckert. On multi-authority ciphertext-policy attributebased encryption. In Bulletin of the Korean Mathematical Society 46, 4, pages 803-819, 2009.

[16] M. Chase and S. Chow. Improving privacy and security in multi-authority attribute-based encryption. In ACM Conference on Computer and Communications Security, pages 121-130, 2009.

[17] H. Lin, Z. Cao, X. Liang, and J. Shao. Secure threshold multi authority attribute based encryption without a central authority. In INDOCRYPT, pages 426-436, 2008.

[18] Allison B. Lewko, Brent Waters: Decentralizing Attribute-Based Encryption. EUROCRYPT 2011, pages 568-588, 2011.