Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 38-44
doi:10.4028/www.scientific.net/AEF.6-7.38

A Multi-Authority Attribute-Based Encryption System Against Malicious KGC

Guoyan Zhang[1, a]

[1] School of Computer Science and Technology，Shandong University，Shandong Provincial Key Laboratory of Software Engineering, Jinan, P.R China

[a]Guoyanzhang@sdu.edu.cn

Keywords: Attribute-Based Encryption Scheme; Malicious KGC, Key-Escrow; Multi-Authority; K-sibling Intractable Function

Abstract. 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. Similar with identity-based encryption scheme, attribute-based schemes are also confronted with key escrow problem. Furthermore, the attributes belonging to a user usually are monitored by different authorities. This paper resolves the two problems by using a general attribute-based encryption scheme and K-Sibling intractable function families. In our construction, different attributes sets of a user are still certified by different authorities, but the partial private keys corresponding to the attributes are generated by a central authority. Simultineously, different authorities jointly generate the users' secret value which cannot be obtained by the central authority. Compared with general multi-authourity attributed-based encryption scheme, our approach has more efficiency.

Introduction

With the development of the internet, expressive access-control is becoming more and more a key technology, where access decisions depend upon attributes of the protected data and access policies assigned to users. A natural solution for expressive access-control is attribute-based encryption (ABE) introduced by Sahai and Waters [1]. Following, two variants of ABE were subsequently proposed: key-policy variant (KP-ABE) of Goyal, Pandey, Sahai and Waters (GPSW) [2] and ciphertext-policy variant (CP-ABE) of Bethencourt, Sahai and Waters (BSW) [3]. 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.

With the increasing number of international cooperation among different organization and department, the attributes belonging to a user usually are monitored by different authorities. Furthermore, similar to identity-based encryption schemes, the attribute-based schemes encounters key escrow problem. One approach to mitigate the above two problems is to employ multi-authority attribute-based encryption scheme, which 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.

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. Müller, Katzenbeisser, and Eckert [14,15] give a system with a centralized authority that realizes any LSSS access structure. Their proof is limited to non-adaptive queries. The system achieves roughly the same functionality as the engineering approach above, except one can 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] give 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. Scheme [18] proposes a new multi-authority attribute-based encryption system.

Preliminaries

Definition 1 (Decisional Modified Bilinear Diffie-Hellman (MBDH) Assumption). Suppose a challenger chooses $a,b,c,z \in Z_p$ 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.

Definition 2 (K-Sibling Intractable Function Families) Let $k=k(n)$ be a polynomial with $k \geq 1$. Let $H=\{H_n \mid n \in N\}$, where $H_n=\{h \mid h:\Sigma^{l(n)} \to \Sigma^{m(n)}\}$, be a family of functions that is one-way, polynomial time computable and samplable, and that has the collision accessibility property. Also let $X=x_1,x_2,\ldots,x_i$ be any set of i initial strings, where $1 \leq i \leq k$. H is a k-sibling intractable function family, or simply $k-SIFF$, if for each $1 \leq i \leq k$, for each sibling finder F, for each polynomial Q, and for all sufficiently large n, $Pr[F(X,h) \neq ?] < 1/Q(n)$, where h is chosen randomly and uniformly from $H_n^X \in H_n$,the set of all functions in H_n that map $x_1,x_2,\ldots,x_i$ to the same strings in $\Sigma^{m(n)}$, and the probability $Pr[F(X,h) \neq ?]$ is computed over $H_n^X \in H_n$ and the sample space of all finite strings of coin flips that F could have tossed.

A General Construction for Multi-Authority Attribute-Based Encryption Scheme

We assume that there are n attribute authorities, and every attribute authority k monitors d_k attributes, and there are r users. Let (Setup'; SecretKeyExtract'; Encryption'; Decryption') be an IND-CPA secure attribute-based encryption scheme, $H=\{H_n : n \in N\}$ be a k-sibling intractable function family, where $H_n=\{h_n : \Sigma^{l(n)} \to \Sigma^{m(n)}\}$. $G=\{G_n : n \in N\}$ is a pseudo-random function families, where $G_n=\{g_n : \Sigma^{l'(n)} \to \Sigma^{l(n)}\}$ and $F=\{F_n : n \in N\}$ is a one-way trapdoor function family, where $F_n=\{f_n : \Sigma^{q(n)} \to \Sigma^{z(n)}\}$. Let (Setup; PartialPrivateKeyExtract; SetSecretValue; SetPrivateKey; SetPublicKey; Encrypt; Decrypt) be the attribute-based certificateless encryption scheme from the above attribute-based encryption scheme, k-sibling intractable function families and one-way trapdoor function, and the construction is as follows:

-SetUp: Central authority runs Setup' of attribute-based encryption scheme to get the master secret key msk and master public key mpk. The master public key mpk includes a description of the ciphertext space C.

-AuthorityCertify: In order to certify the attribute set i for user $A_i, i=1,2,\cdots,r$, attribute authority k generates signature $Sign_{s_k}(i,A_i)$ and sends this signature to the central authority with verifying secret key v_k. (s_k,v_k) *is signature and verification* sec*ret key pair of authority k*.

-PartialPrivateKeyExtract: Given the master public key mpk, master secret key msk, an attributes set $S_{A_i} \in U$ and its signature, the central authority verifies the validity of the signatures. If so, he runs PPT algorithm SecretKeyExtract' to generate the partial private key d_{A_i} for this attributes set. Then the partial private key d_{A_i} is transported to entity A_i over a confidential and authentic channel.

-SetSecretValue: Each authority chooses his secret key sk_k. Given master public key mpk and attributes set $d_k^i \in U$ as inputs, Authority k computes $y_k^i = g_{sk_k}(d_k^i), (k=1,2,\cdots,n, i=1,2,\cdots,r)$, then

chooses an entity to get a $nr+1$ -sibling intractable function h satisfying $h(y_k^i)=x,(k=1,2,\cdots,n,i=1,2,\cdots,r)$ and publish h, then each authority can compute x, and x is sent to entity A_i as his temporary secret key.

-SetPrivateKey: Given master public key mpk, the entity $A_i's$ temporary secret key x, and the entity $A_i's$ partial private key d_{A_i} as input, the entity runs this PPT algorithm to generate a private key SK_{A_i}.

-SetPublicKey: Given master public key mpk and the entity $A_i's$ temporary secret key x, one-way trapdoor function f with x as its trapdoor is returned.

-Encrypt: Given a plaintext $m \in M$, the ciphertext is $C = Encryption'(f(m))$

-Decrypt: Given master public key mpk, the entity's private key $SK_{A_i}=(d_{A_i},x)$ and the ciphertext $C \in C$. If entity's attributes set satisfying the access tree T related with C (ciphertext-policy attribute-based encryption scheme), or the attributes related with C satisfies the access tree T (key-policy attribute-based encryption scheme), and then he can get the message as follows:

$$m = f_x^{-1}(Decryption'_{d_{A_i}}(C)). \tag{1}$$

Otherwise outputs $\perp$.

Concrete Attribute-Based Encryption Scheme Secure against the Malicious KGC

Construction

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. $\Delta_{i,s}(x), i \in Z_p$ is the Lagrange coefficient, and S is a set of elements in Z_p. U is the universal set of attributes which is associated with a unique element in $Z^*{}_p$. Our construction is as follows:

-Setup (d)**:** First, Central authority take the integers $1,2,\ldots,|U|$ to be the universe.

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

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

The master key is:

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

Every attribute authority k generates his own signature secret key s_k and verifying secret key v_k.

-AuthorityCertify: in order to certify the attribute d_i^k for user A_i, attribute authority k generates signature $Sign_{s_k}(A_i,u)$ and sends this signature to the central authority with verifying secret key v_k.

-PartialPrivateKeyExtract: after verifying the signature for attributes set $d^i=(d_1{}^i,\cdots,d_n{}^i)$ for user A_i, the central authority picks $(d-1)$ degree polynomial q randomly so that $q(0)=y$. The partial private key for user A_i is

$$d_{A_i} = g^{\frac{q(i)}{t_i}}, i \in d^i. \tag{2}$$

-SecretValueExtract: Each authority chooses his secret key sk_k. Given master public key mpk and attributes set $d_k^i \in U$ as inputs, Authority k computes $y_k^i = g_{sk_k}(d_k^i), (k=1,2,\cdots,n,i=1,2,\cdots,r)$, then chooses an entity to get a $nr+1$ -sibling intractable function h satisfying $h(y_k^i)=x,(k=1,2,\cdots,n,i=1,2,\cdots,r)$ and publish h, then each authority can compute x, and x is sent to entity A_i as his temporary secret key.

-SetPrivateKey: Given master public key mpk, the entity $A_i's$ temporary secret key x, and the entity $A_i's$ partial private key d_{A_i} as input, the entity runs this PPT algorithm to generate a private key SK_{A_i}.
-SetPublicKey: Given master public key mpk and the entity $A_i's$ temporary secret key x, one-way trapdoor function f with x as its trapdoor is returned.
-Encrypt. In order to encrypt message $m \in G_T$ with attributes set ω', pick $s \in Z_P$ and compute the ciphertext as follows:

$$C = (C_0, C_1, C_2) = (\omega', f(m) \cdot Y^s, E_i = T_i^s, i \in \omega'). \tag{3}$$

-Decryption.: Suppose that a ciphertext, C is encrypted with a key for attributes set ω' and we have the partial private key d_{A_i} for attributes set ω, where $|\omega \cap \omega'| \geq d$. Choose an arbitrary d-element subset S of $\omega \cap \omega'$ and compute

$$\alpha = p(0) = \sum_{i \in S} p(i)\Delta_{i,s}(0), \tag{4}$$

$$f(m) = C_1 / \prod_{i \in S} (((e(d_{A_i}, E_i))^{\Delta_{i,s}(0)})^{\alpha}, \tag{5}$$

$$m = f_x^{-1}(f(m)). \tag{6}$$

Correctness:

$$C_1 / \prod_{i \in S} (((e(d_{A_i}, E_i))^{\Delta_{i,s}(0))^{\alpha}} \tag{7}$$

$$= f(m)e(g,g)^{xys} / \prod_{i \in S} (e(g^{\frac{q(i)}{t_i}}, g^{st_i})^{\Delta_{i,s}(0)\alpha}) \tag{8}$$

$$= f(m)e(g,g)^{xys} / \prod_{i \in S} (e(g,g)^{sq_i})^{\Delta_{i,s}(0)\alpha}) \tag{9}$$

$$= f(m), m = f_x^{-1}(f(m)). \tag{10}$$

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 A is a polynomial-time adversary, and he can success with advantage ε, then we can construct a scheme B to resolve the Modified Bilinear Diffie-Hellman problem with advantage ε by calling A. The following is the proceed:
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 $(A, B, C, Z) = (g^a, g^b, g^c, Z)$.
B runs A to obtain a challenge attributes set α.
Setup. 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 $i \in U - \alpha$, he sets $T_i = g^{\omega_i}$ for random ω_i.

phase1

SecretKey Extract. A makes requests for secret key for attributes set γ . If $|\gamma \cap \alpha| < d$. Set three sets Γ, Γ_1, S , where:

$$\Gamma = \gamma \cap \alpha, \Gamma \subseteq \Gamma_1 \subseteq \gamma \tag{11}$$

$$|\Gamma_1| = d - 1, \tag{12}$$

set

$$S = \Gamma_1 \cup \{0\}. \tag{13}$$

We can randomly define the secret key for Γ_1 as follows:

For $i \in \Gamma$, Set

$$D_i = g^{s_i}. \tag{14}$$

Where s_i is chosen randomly.

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

$$D_i = g^{\frac{\lambda_i}{\omega_i}}. \tag{15}$$

Where λ_i is chosen randomly.

Then from the definition, B have 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 $i \in \Gamma_1 - \Gamma, q(i) = \lambda_i$.

B can define the other secret key D_i :

$$D_i = (\prod_{j \in \Gamma} C^{\frac{t_j s_j \Delta_{j,S}(i)}{\omega_i}})(\prod_{j \in \Gamma_1 - \Gamma} g^{\frac{\lambda_j \Delta_{j,S}(i)}{\omega_i}}) Y^{\frac{\Delta_{0,S}(i)}{\omega_i}}. \tag{16}$$

Secret Value Extract. A asks a secret value for attributes set β , B divides $\beta = (\beta_1, \cdots, \beta_n)$, and acts as each authority, chooses computes $y_k = g_{sk_k}(\beta_k), (k = 1, 2, \cdots, n)$, then chooses an entity to get a $nr+1$ -sibling intractable function h satisfying $h(y_k) = x, (k = 1, 2, \cdots n)$ and x is sent to entity A .

Public Key Extract. Publish one-way trapdoor function f with x as its trapdoor.

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

$$C = (C_0, C_1, C_2) = (\alpha, f(m_b) \cdot Y, E_i = B_i^t \ i \in \alpha). \tag{17}$$

phase2 B acts exactly as it did in phase 1.

Guess If A correctly guess the bit b , 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 B is equal to the advantage of A .

Theorem 2. If f is one-way trapdoor function and h is a k -sibling intractable function, then our attribute-based encryption scheme is secure against malicious central authority.

Conclusion

In order to mitigate the key escrow, this paper gives a new approach which adds new secret value to the user by the attribute authorities, and the central authority doesn't know the secret value. Compared with the general multi-authority attribute-based encryption scheme, our approach is simple, and the length of the cipertext and the public key published to the sender is not increased.

Acknowledgement

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.ZR2012FQ028) and Independent Innovation Foundation of Shandong University (No. 2012TS070)

Reference

[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 (CCS'06), 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. 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. 2010. Vol 6056 of LNCS, Springer.

[12] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In R. Cramer, editor, Advances in Cryptology–EUROCRYPT 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 – TCC 2007, volume 4392 of Lecture Notes in Computer Science, pages 515–534. Springer-Verlag, 2007.

[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.