One Attribute-Based Proxy Signature

Sun Changxia
Computer department of Information and
Management Sciences college
Henan Agricultural University
zhengzhou,china
sunchang_xia@126.com

Guo Yufeng
Computer department of Information and
Management Sciences college
Henan Agricultural University
zhengzhou,china
gyfzhp@126.com

Yan Yu
School of electronic information and electrical
engineering
Shanghai Jiaotong University,
shanghai,china
hnndwyl@163.com

Corresponding Author: Si Haiping
Computer department of Information and
Management Sciences college
Henan Agricultural University
zhengzhou,china
pingsss@126.com

Abstract—For Identity-based proxy signature, when the original signer cannot sign for some reason，he delegate his signing capabilities to a person with an identity, in order to expand the scope of the proxy signer, an entity with a series of attribute properties can perform the right of signature. A new practical attribute-base proxy signature is devised and its security is proved equal to discrete logarithm problem and decisional bilinear Diffie-Hellman problem through using the methodology of reductionist security argument. The scheme possesses some security of strong unforgeability, strong identifiability, strong undeniability, verifiability, distinguishability, anti-collusion attack and avoids the misuse.

Keywords-Attribute-based; Proxy signature; Bilinear pairings; Access structure; Collusion attack

I. INTRODUCTION

The concept of attribute-based encryption (ABE) was introduced by Sahai and Waters[1],and In an ABE system, the identity of a user is not a single string but a set of descriptive attributes. Because of its flexible mechanism, the attribute-based encryption was paid much more attention by scholars both at home and abroad. Subsequently, many attribute-based encryption schemes [2-4] were put forward. Goyal et al[2] presented a scheme for fine grained access control of encrypted data that each private key represents a formula describing which sets of attributes must appear on the ciphertext in order for this user to decrypt. The advantage of Attribute-based encryption is that a variety of cryptographic operation and dialogue can be easily done with the partial attributes of a user instead of a precise identity of the user. Attribute-based signature (ABS) is developed from the concept of fuzzy identity-based signature[5] and a lot of ABS schemes[6-8] are proposed without detailed proven process.

The concept of proxy signature was introduced by Mambo, Usuda and Okamoto[9]. In a proxy signature scheme, an original signer delegates his signing right to a proxy signer in such a way that the proxy signer can sign messages on behalf of the original signer, while the verifier can verify and distinguish a proxy signature from an original signature. At present, there is little research on attribute-based proxy signature. In paper [10], the author simply extended his attribute-based signature to the proxy signature, thus he made a try about the attribute-based proxy signature. But there are a lot of problems existing, for example, the scheme couldn't meet the strong non-repudiation and strong recognition about proxy signature.

In this paper, we mainly studied attribute-based proxy signature, and present a new practical scheme in which the original signer delegates his signing right to a proxy signer with a set of properties, and prove it to be secure with distinguishablity, verifiability, strongly unforgeablity, strong identifiablity and strong non-repudiation, abuse resistance and resistance to the collusion attack.

II. ORGANIZATION

We organize the rest of the paper as follows. In the next Section, we describe some preliminaries such as bilinear pairings, computational Diffie-Hellman problem, and Lagrange interpolation. In Section 4, we formally give our security definition including syntax of attribute-based proxy signature. In Section 5, we give the construction of our attribute-based proxy signature scheme in the random oracle model .The following is the correctness and the security analysis in Section 6. We conclude in Section 7. Finally, give the acknowledgements.

III. PRELIMINARIES

A. Bilinear Pairings

Definition 1 Let q be a prime number and G_1, G_2, G_3 be cyclic groups with the order q. Let g_1 be a generator of G_1 and g_2 be a generator of G_2 .Let DL problem be difficult. A bilinear pairing is a map $e: G_1 \times G_2 \to G_3$ with the following properties :

1) Bilinearity: $\forall g_1 \in G_1, g_2 \in G_2, \forall a, b \in \mathbf{Z}_q$,we have

$$e(g_1{}^a, g_2{}^b) = e(g_1, g_2)^{ab} .$$

2) Non-degeneracy: there exists $g_1 \in G_1, g_2 \in G_2$ such that $e(g_1, g_2) \neq 1$,which 1 is a unit of G_3.

3) Computability: It is efficient to compute for $e(g_1, g_2)$,any $g_1 \in G_1, g_2 \in G_2$.

B. Computational Diffie-Hellman Problem

Definition2 Discrete logarithm problem（DLP）: Let q be a prime number and G_1 be cyclic groups with order q .Given $m, y \in G_1$,the solution $x \in \mathbf{Z}_q$ which can satisfy the formula $y = m^x$ is hard.

Definition3 Decisive bilinear Diffie-Hellman problem （$DBDHP$）: $\forall a, b, c, r \in \mathbf{Z}_q$,given a prime q ,a generator $g \in \mathbf{Z}_q{}^*$ and quintuple (g, g^a, g^b, g^c, r) , determine whether r and $e(g,g)^{abc}$ are equal is considered hard to calculate.

C. Lagrange Interpolation

Let $f(x)$ be a n degree polynomial, given $n+1$ different points $(x_i, f(x_i)), \mathrm{i} = 1, 2, \ldots \mathrm{n}$, we can uniquely determine the n degree polynomial $f(x)$:

$$f(x) = \sum_{i=1}^{n} f(x_i)(\prod_{1 \le k \ne i \le n} (x - x_k) / (x_j - x_k)) .$$

We define the Lagrange coefficient $\Delta_{i,s}$:

$$\Delta_{i,s}(x) = \prod\nolimits_{i \in S, j \ne i} \frac{x-j}{i-j}$$

where S is a set composed of any $n+1$ different points $(x_i, f(x_i))$, $i \in Z_q$ and $S \subset Z_q$.

Finally $f(x) = \sum_{i=1}^{n+1} f(x_i) \Delta_{i,s}(x)$.

In a word, we couldn't get any information about the polynomial $f(x)$ in a threshold signature system if there are less than $n+1$ different points $(x_i, f(x_i))$ in S .

IV. SYNTAX OF ATTRIBUTE-BASED PROXY SIGNATURE

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph. Do not add any kind of pagination anywhere in the paper. Do not number text heads-the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar:

An attribute-based proxy signature scheme is similar to an ordinary proxy signature scheme, which includes several algorithms as follow: the setup algorithm, private key extraction algorithm ,the standard signing algorithm, the standard verification algorithm, proxy private key extraction algorithm, proxy signing algorithm, proxy signing verification algorithm, and also includes three parties: the original signer A and the proxy signer B and signing verification V .

Setup: The setup algorithm is a probabilistic algorithm. It takes as input 1^l where l is security parameter and publishes system parameters.

Extract: On inputs system parameters and security parameter, the private key extraction algorithm outputs the user's secret key and public key.

Standard Sign: The standard signing algorithm is a probabilistic algorithm. It takes a signing key of the original signer A and a warrant message m_W (including identity ID_A , ID_B and warrant restriction and so on) as input, and outputs a authorization certificate $W_{A \to B}$ which is also called standard signature)over the proxy signer B .

Verify: The verification algorithm of the standard signature above is a probabilistic algorithm. It is run by the proxy signer B. It takes ID_A, a warrant message m_W , and a $W_{A \to B}$ as input, and outputs 1 and accept if the delegated signature is valid, or 0 and reject otherwise.

PExtract: On inputting access structure Γ , the attributes set ω_B of the proxy singer B ,identity ID_B a warrant message m_W and $W_{A \to B}$, and then outputs a proxy signing key K_p.

PSigin: The proxy signing algorithm takes the access structure Γ, a proxy signing key K_p, a message m and a standard warrant signature $W_{A \to B}$ as input and outputs a proxy signature σ .

PVerify: The proxy verification algorithm is a probabilistic algorithm. It takes ID_A of the original signer, a message m_W , a standard warrant signature $W_{A \to B}$,a message m and a proxy signature σ as input, outputs 1 and accept if the proxy signature is valid, or 0 and reject otherwise.

V. ATTRIBUTE-BASED PROXY SIGNATURE

In this paper, the structure of the standard signing algorithm is inspired by the paper [11]and the identity-based proxy signature proposed in paper [12] .The original signer delegates his private key to a proxy signer B with some special attributes to sign some messages on behalf of the original signer. If the proxy signer B can meet published access structure Γ with the attributes set γ ,then $\Gamma(\gamma)=1$.

In following section, we give the description of our of proxy attribute-based signature. There are seven algorithms in this scheme .

Let G, G_1 be cyclic groups with prime order q of G , and let $e: G \times G \rightarrow G_1$ denote the bilinear map. Additionally, let g be a generator of G and an attribute domain $U=\{1,2,...n\}$.

Setup Algorithm: First, choose $\{t_i\}_{i=1,2,...,n} \in Z_q$, $g_1, g_2 \in G$, $y, w \in Z_q$ at random and compute $T_i = g^{t_i}$, $Y = g^y$, $W = g_1{}^w$ .Next, two public Hash functions are also chosen such that $H_1: \{0,1\}^* \rightarrow G,$ and $H_2: \{0,1\}^* \rightarrow Z_q$ .Finally, we get the systematical master secret $MSK =< y, w, t_i >$ and the public key:

$$MPK =< g, g_1, g_2, T_i, G, G_1, H_1, H_2 > .$$

Extract Algorithm: Inputting the identity of the original signer ID_A and computing $h_A = H_1(ID_A)$, we got the signing private key $S_A = h_A{}^y$.

Standard Signing Algorithm: The original signer A chooses $r_A \in Z_q$ at random and compute $A_1 = g^{r_A}, A_2 = Y^{r_A} \cdot S_A{}^{H_2(m_w, A_1)}$, then sends the authorization certificate $W_{A \rightarrow B}$: (A_1, A_2, m_w) to the proxy signer B .

Standard Signing Verify Algorithm： The proxy signer B will verify the authorization certificate $W_{A \rightarrow B}$ (also is called the standard signature) from the original signer and check the equation $e(A_2, g) = e(A_1, Y) e(h_A, Y)$ .If the equation is equal, the proxy signer B will accept the signature and otherwise reject.

Proxy Private Key Algorithm: With the access structure Γ and the proxy signer attribute sets γ , the private key is acquired to perform the proxy signature. In the paper [2], the access structure is viewed as Attribute tree structure. According to the attributes tree structure, from the root node and a top-down we construct a polynomial q_x (q_x is confidential) at random, Let $q_l(0) = w$,for every node x in the tree, polynomial degree of the node x is smaller than threshold value 1.That is $d_x = k_x - 1$ and $q_x(0) = q_{parent(x)}(index(x))$ through recursively defining q_x .So, for every node x ,we can compute the private key about the attributes tree $S_B = g_1{}^{q_x(0)/t_i}, i \in att(x)$.

Proxy Signing Algorithm: Inputting the identity of the original signer ID_A and computing $h_A = H_1(ID_A)$, the proxy signer B chooses $r_B \in \mathbf{Z}_q$ at random and compute $B_1 = g^{r_B}, B_2 = Y^{r_B} \cdot A_2, B_3 = S_B \cdot (g_2{}^m \cdot h_B)^{r_B}$, $B_4 = T_i^{r_B}$, and outputs the proxy signature σ :

$$\sigma =< m, m_w, A_1, B_1, B_2, B_3, B_4, ID_B > .$$

Proxy Signing Verify Algorithm: The verifier takes ID_A , m and the proxy signature σ as input and verify whether the proxy signature σ is the original signer's valid signature. If the following equation is correct the verifier then accept the signature of the proxy signer and otherwise reject it.

$$\frac{e(B_2, g) e(B_3, T_i)}{e(g_2{}^m \cdot h_B, B_4)} = e(B_1, Y) e(A_1, Y) e(h_A{}^{H_2(m_w, A_1)}, Y) e(W, g)$$

VI. Analysis of the Scheme

A. Correctness

Theorem 1 If the original signer A and the proxy signer B execute the signature scheme in this paper, the user finally gained the legal proxy signature. Namely, the solution of the validation equation must be established.

Proof:

We need to explain that the node x of set S_B in the validation equation is divided into leaf nodes and non-leaf nodes. First, we define the recursive algorithm $VerNode(S_B, T_i, x)$ .Then we input the proxy signature σ and systematical parameter MPK .Finally, we output one element in G_1 or reject the signature.

First, considering the condition of $i = att(x),$ where is a leaf node, we will get the following equation:

$$VerNode(S_B, T_i, x) = \begin{cases} e(S_B, T_i) = e(g_1{}^{\frac{q_x(0)}{t_i}}, g^{t_i}) \\ = e(g_1, g)^{q_x(0)}, i \in \gamma \\ \\ \perp, i \notin \gamma \end{cases}$$

Let x be a leaf node, z be all child nodes of x , x be the parent node of z , and S_x be the attributes set of child nodes z with arbitrarily size k_x .The result is F_z after calling recursive algorithm $VerNode(S_B, T_i, z)$ and F_z meets the condition of $F_z \neq \perp$. If there is no such a collection, the node does not meet the condition, then the algorithm returns, or we can give the parent's formula derived from the child node:

$$\begin{aligned} F_x &= \prod_{z \in S_x} F_z{}^{\Delta_{i,s'}(0)} \\ &== \prod_{z \in S_x} (e(g_1, g)^{q_z(0)})^{\Delta_{i,S'_x}(0)} \\ &= \prod_{z \in S_x} e(g_1, g)^{q_{parent}(z)(index(z))})^{\Delta_{i,S'_x}(0)} \\ &= \prod_{z \in S_x} e(g_1, g)^{q_x(i) \cdot \Delta_{i,S'_x}(0)} \\ &= e(g_1, g)^{q_x(0)} \end{aligned}$$

Where $i = index(z), S'_x = \{index(z) : z \in S_x\}$.

For none of the value $\perp$,The value F_z derived from all leaf nodes to call the recursive algorithm $VerNode(S_B, T_i, x)$ can use Lagrange Interpolation and recursively calculate the value of root node l with the condition of $q_l(0) = w$.

Second, we will continue to prove the validity of the equation below:

$$\frac{e(B_2, g)e(B_3, T_i)}{e(g_1{}^m \cdot h_B, B_4)} \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$= \frac{e(Y^{r_B} \cdot A_2, g)e(g_1{}^{\frac{q_x(0)}{t_i}} (g_2{}^m \cdot h_B)^{r_B}, T_i)}{e(g_2{}^m \cdot h_B, T_i^{r_B})}$$

$$= \frac{e(Y^{r_B} \cdot A_2, g)e(g_1{}^{\frac{q_x(0)}{t_i}}, T_i)e((g_2{}^m \cdot h_B)^{r_B}, T_i)}{e(g_2{}^m \cdot h_B, T_i^{r_B})}$$

$$= e(Y^{r_B} \cdot A_2, g)e(g_1{}^{\frac{q_x(0)}{t_i}}, T_i)$$

$$= e(g^{yr_B} \cdot g^{yr_A} \cdot S_A{}^{H_2(m_w, A_1)}, g)e(g_1{}^{\frac{q_x(0)}{t_i}}, g_1{}^{t_i})$$

It is showed that the scheme is correct with the establishment of above equation, that is the attributes set γ of the proxy signer B can meet the declared access structure Γ of the original signer A , and the verifier V accepts the proxy signature of the proxy signers B .

B. Security

Theorem 2 The proposed attribute-based proxy signature scheme meets the six security requirement of proxy signature system: distinguishablity; verifiability; strong unforgeablity; strong non-repudition ; strong identifiablity; abuse resistance.

1)Distinguishablity: the original signer's public key h_A, the proxy signer's public key h_B will be in the verification equation of the proxy signature. Additionally, the warrant message m_W is also concluded in the verification equation of the standard signature and the proxy signature. So, anyone can determine the identity of the proxy signer from m_W .

2)Verifiability: Because of the fact that the necessary parameters of the verification equation are public, any verifier can be sure that the original signer A can agree with the information of the proxy signature. The warrant message m_W usually contains the original signer and the proxy signer's identity news, and the proxy signature limiting conditions of application, therefore it can ensure the verifiability. Moreover, with theorem 1, if B is the legal proxy signer, there is the equation below established:

$$\frac{e(B_2, g)e(B_3, T_i)}{e(g_2{}^m \cdot h_B, B_4)} = e(B_1, Y)e(A_1, Y)e(h_A{}^{H_2(m_w, A_1)}, Y)e(W, g)$$

From above equation, it is said that is the legal proxy signer’s signature can be verified to be valid.

3)Strong unforgeablity: The standard signing algorithm scheme above is deduced from the literature [11], the signature scheme in this paper has been proven to be secure against adaptive selective message attack in ROM, and it is impossible for the attacker to attempt to forge the original signer's warrant message m_W . The third-party attacker could not forge the proxy signature of relevant attributes set.It is shown in the paper[2]that, if the third party the attacker with the private key of the attribute set γ can succeed with non-ignorable probability, there is a simulator can figure out the problem with non-ignorable probability. Thus, this scheme is strong unforgeablity.

4)Strong non-repudiation: The standard signing algorithm contains a warrant message m_w and it need to be verified by the verification algorithm. In the meantime, the proxy signer B can't revise the warrant message m_w .In this way, the original signer A cannot repudiate its authorization of proxy signer B . In addition, the public key h_B of the proxy signer B must be appeared in the proxy signing verification, so, the proxy signer B can't deny his valid proxy signature.

5)Strong identifiablity: The warrant message m_w is in the proxy signature and the identity h_B of the proxy signer B is in the warrant message m_w , Therefore, anyone can know the identity of the proxy signer from the proxy signature.

6)Abuse resistance: In order that the warrant message m_w limits the proxy signature’s right, and additionally the warrant message m_w also is present in the proxy signing verification equation, therefore the proxy signer B can't sign the unauthorized message, and also can't illegally transferred his signing right to other third players.

Theorem 3 This scheme in this paper also has the security with resistance to the collusion attack required in the attribute-based signature system.

Resistance to the collusion attack refers to the different signers together colludes and cannot fake a valid signature that can’t previously satisfy the attributes set alone. As in the literature [8], because the randomly selected polynomial q_x in this scheme is different for each user, the polynomial q_x is confidentiality, and the private key $S_B = g_1{}^{\frac{q_x(0)}{t_i}}$ must be different. Moreover, because the random number r_B of the different proxy signer B is randomly selected, so it is impossible for the different users to collude together and generate an effective signature without declared attributes set. If the different users can succeed in colluding with non-ignorable probability, there is a simulator can figure out the DL problem and the $DBDH$ problem with non-ignorable probability.A contradiction! So, the presented scheme has the security with resistance to the collusion attack.

VII. CONCLUSIONS

In this paper we propose a new attribute-based proxy signature scheme, and analysis to prove that the scheme meet the six security requirement of proxy signature scheme and resistance to the collusion attack .At the same time, the efficiency of the proxy signature algorithm is higher, signature, because that the signing process only involves exponentiation, addition and multiplication of the group. At present, most of the proxy signatures are lack of strict security formalization, and the research about attribute-based proxy signature scheme is very few, so in the next work we will focus on the security proof and the efficiency of verification by improving validation algorithm, and try the attribute-based proxy signature scheme in electronic commerce.

ACKNOWLEDGMENT

This work was supported partially by National Science-technology Supported Plan Project under Grant No. 2013BAC09B01-03,Henan Province Major Science-technology Project under Grant No.131100110400, Henan Province Major Science-technology Project under Grant No. 121100110900, Henan Province Key Science-technology Research Project under Grant No.132102110043, Science-technology Research Key Project of Henan Province Education Department under Grant No.14B413009, Science-technology Research Project of Zhengzhou city under Grant No.141PPTGG431,and Henan Province Major Science-technology Project under Grant No.121100111300-04.

REFERENCES

[1] A.Sahai, B.Waters. Fuzzy identity-based encryption. Advances in Cryptology-EUROCRYPT 2005,Aarhus,Denmark,Springer-Verlag, 2005, pp.457-473.

[2] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Proceeding of CCS , New York ,ACM Press,2006, pp.89–98.

[3] J.Bethencourt, A Sahai, B.Waters. “Ciphertext-Policy Attribute-Based Encryption”.IEEE Symposium on Security and Privacy,2007, pp.321-334.

[4] Q.Tang, D.Ji. Verifiable Attribute-Based Encryption. Cryptology ePrint Archive, Report 2007,46l , http://eprint.iaer.org/2007 /461, 2007.

[5] M.Pirretti, P.Traynor, P.McDaniel, B.Waters. Secure Attribute-Based Systems[C].on 13th ACM conference Computer and communications security, Alexanandria Virginia USA, 2006, 99-112.

[6] Guo,Y.Zeng.Attribute-Based Signature Scheme. 2008 International Conference Information Security and Assurance(ISA 2008),2008,509-511.

[7] Shahandashti, S.F., Safavi-Naini, R. Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems[C]. Cryptology ePrint Archive, Report 2009, Berlin, Springer-Verlag, 2009, 198-216.

[8] C. X. Sun, W. P. Ma and H. F. Chen. Multi-authority Attribute-based Signature. Journal of Sichuan University (Engineering Science Edition) [J], volume 43, pp: 83-86, January, 2011.

[9] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation [C].Proc. 3rd ACM Conference on Computer and Communications Security. ACM Press, 1996:48- 57.

[10] Y. L. Zhang. The study on the attribute-based signature [D],Guangzhou, Computer college of sun yat-sen university,2009.

[11] C. G. Liu, Y. X. Zhou, W. Qing. The study on ID-based proxy signature [J]. Journal of Harbin institute of technology university, 1052-1054,2008.

[12] Xun Yi. An Identity-based Signature Scheme From the Weil Pairing[J]. IEEE Communications Letters, 2003,7 (2) : 76 - 78 .