An Expressive Attribute-based Signature Scheme without Random Oracles

Dan Cao
School of Computer
National University of Defense Technology
Changsha, China
Email: d_cao@yahoo.cn

Xiaofeng Wang
School of Computer
National University of Defense Technology
Changsha, China

Tianzuo Wang
School of Computer
National University of Defense Technology
Changsha, China

Jinshu Su
School of Computer
National University of Defense Technology
Changsha, China

***Abstract*—Attribute-based signatures (ABS) is a new cryptographic primitive and can play a great role in attribute-based access control systems. In ABS, a signer can choose its attributes satisfying a policy of a verifier to generate a valid signature without reveal its identity or attributes, while the signature assures that the message is endorsed by an individual owning attributes the policy requiring. However, most existing works of ABS need random oracles, which is unpractical and results in the dependence of security on hash functions. In this paper, we refer to the mature techniques used in identity-based encryption (IBE) to propose an ABS scheme without random oracles. Our scheme support any expressive policy consisting of AND, OR, threshold gates, which offers great flexibility to the implementation of access control.**

Keywords-ABS;random oracles; policy; IBE

I. INTRODUCTION

Attribute-based signature (ABS) is a new and versatile cryptographic primitive proposed in [1, 2], in which a signature attests not to the identity of the individual who endorsed a message, but instead to a (possibly complex) claim regarding the attributes the signer obtained from an attribute authority. ABS offers an unforgeability guarantee for the verifier, that the signature was produced by a single party whose attributes satisfy the policy being made; i.e., not by a collusion of individuals who pooled their attributes together. Although the scheme in [2] reveals the set of attributes satisfying the policy, subsequent research of ABS offers an attribute-signer privacy guarantee for the signer, that is, a legitimate signer remains anonymous without the fear of revocation and is indistinguishable among all the users whose attributes satisfying the policy specified in the signature. ABS is useful in many important applications such as anonymous authentication and attribute-based messaging systems.

According to the policy the scheme supporting, existing works of ABS can be classified as threshold ABS [3-5] and expressive ABS [1]. The former only supports a threshold policy under computational Diffie-Hellman problem, while the latter supports an expressive policy consisting of AND, OR, threshold gates with a weak security in generic group model. There's no ABS scheme implementing an access policy consisting of AND, OR, threshold gates and constructing the security under standard Diffie-Hellman assumption at the same time until Cao et al. [6] present their ABS scheme. However, all of these works build their ABS schemes in random oracle model, except Li et al. [3] extend their original scheme without random oracles.

As in identity-based encryption (IBE) systems, it is an open problem to build secure attribute-based signatures in the standard computation model (rather than the random oracle model). In practice, it is difficult to build hash functions that hash arbitrary strings directly onto a group. We propose an ABS construction without random oracle model, adopting the technique used in [7], which's the best method in the history of IBE's evolution without random oracles, to improve previous work in [6]. Our ABS scheme supports any policy consisting of AND, OR, and threshold gates with the properties of unforgeability and attribute-signer privacy, and the security is based on computational Diffie-Hellman problem in standard model.

In the following parts of this paper, we introduce related works and preliminaries before showing our attribute-based signature without random oracles, and conclude in the end.

II. RELATED WORK

A. IBE without random oracles

Shamir [8] first presented the idea of identity-based encryption (IBE), and the first secure and efficient IBE scheme didn't appear until Boneh and Franklin [9] constructing it with computable bilinear maps in the random oracle model. Cocks [10] described another construction using quadratic residues modulo a composite, which however is less practical than the Boneh-Franklin system. IBE provides a public key encryption mechanism where an arbitrary string, such as recipient's identity, can be served as a public key, avoiding the need to distribute public key certificates. However, these systems are only proven secure in the random oracle model [11]. A natural question is to devise a secure IBE system without random oracles.

Published by Atlantis Press, Paris, France.

Canetti et al. [12, 13] presented an IBE system whose security could proven without random oracles, but in a weaker "selective-ID" model, in which the adversary must commit ahead of time (non-adaptively) to the identity it intends to attack. However, their construction is too inefficient to be of practical use.

Boneh and Boyen [14] provided more practical IBE systems in the selective-ID model without the random oracle model. But the proofs use an inefficient security reduction. Shortly thereafter, Boneh and Boyen [15] gave the first fully secure IBE scheme, in which the adversary may choose the target identity adaptively, with a polynomial time reduction in the absence of random oracles. Waters [7] simplified the scheme described in [15], substantially improving its efficiency. But Waters posed open problems regarding compact public parameters and a tight security reduction.

Gentry [16] presented an IBE system, which is fully secure without random oracles and has several advantages over previous systems, including computational efficiency, shorter public parameters, a tight security reduction, and recipient-anonymity, albeit to a stronger assumption that depends on the number of private key generation queries made by the adversary.

B. Attribute-based signatures

Recently, there have been several attempts to construct attribute-based signatures. As a similar notion to ABS, fuzzy identity-based signature was proposed and formalized in [17, 18], which enables users to generate signatures with part of their attributes. To achieve the same goal as the fuzzy identity-based signature, the notion of attribute-based signature was given in [2], but Tan et al. [19] pointed out that this scheme is vulnerable to the partial key replacement attack. Moreover, in these works, authors do not consider any notion of privacy, resulting in leaking attributes used in producing signatures to the verifier.

To achieve weak attribute-privacy, Shahandashti and Safavi-Naini [5] presented a (d, n)-threshold ABS scheme, allowing users to sign messages with subset of attributes satisfying the fixed threshold d, and only the d attributes of the signer chosen by the signature holder were revealed to the verifier. To support flexible, not fixed, threshold value k, Li and Kim [4] used a default set of attributes during signing, and constructed a (k, d)-threshold ABS scheme, realizing attribute-signer privacy. However, in both schemes, the size of signature components is three times of attributes used for signing. In order to enhance the efficiency, Li et al. [3] integrated all the secret attributes components into one, at the same time maintaining attribute-privacy and realizing flexible (k, d)-threshold policy. Moreover, Li et al extended their construction without random oracles. Whereas, these schemes cannot provide expressive policies, that is, any policies formed by AND, OR and threshold gates.

Maji et al. [1] constructed an ABS scheme using monotone span programs [20] that supports a powerful set of policies, namely, any policy consisting of AND, OR and threshold gates. It holds signer privacy against everyone, including all authorities. However, the security is weak as the construction is only proved in the generic group model.

Cao et al. [6] presented the first ABS scheme supporting policies consisting of AND, OR, threshold gates and achieving security in random oracle model under computational Diffie-Hellman problem at the same time, while holding attribute-signer privacy and unforgeability.

III. PRELIMINARIES

In this Section we briefly review the basic concepts on bilinear pairing, Lagrange interpolation, complexity assumptions, and attribute tree, while introducing notations used in this paper.

A. Notation

Let q be a prime. From here on we use $\mathbb{Z}_q$ to denote the group $\{0,\ldots,q\text{-}1\}$ under addition modulo q. Let G_1 and G_2 be multiplicative groups of order q. Let g denote a generator of G_1.

B. Bilinear pairing

A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ with the following properties:

- Bilinear: Given $a, b \in \mathbb{Z}_q$, $f, h \in G_1$, we have $e(f^a, h^b) = e(f, h)^{ab}$.
- Non-degenerate: $e(g, g) \neq 1$ and therefore it is a generator of G_2.
- Computable: There is an efficient algorithm to compute $e(f, h)$ for all $f, h \in G_1$.

C. Lagrange interpolation

Lagrange interpolation for a polynomial $p(\cdot)$ over $\mathbb{Z}_q$ of order d-1 and a set $S \subset \mathbb{Z}_q$ with size $|S| = d$ is calculate as

$$p(x) = \sum_{i \in S} p(i)\Delta_{i,S}(x) \text{ , where } \Delta_{i,S}(x) = \prod_{j \in S, j \neq i} (x - j)/(i - j) \text{ .}$$

D. Complexity assumptions

Here we describe some mathematical problems.

- Discrete Logarithm (DL) Assumption: Given two group elements f and h in G_1, find an integer n, such that $h = f^n$.
- Computational Diffie-Hellman (CDH) Assumption: Given (g, g^a, g^b) for some $a, b \in \mathbb{Z}_q^*$, compute g^{ab}.

E. Attribute tree

An attribute tree Γ can describe a policy. Each interior node is a threshold gate, described by its children and a threshold value. If num_x is the number of children of a node x and k_x is its threshold value, then $0 < k_x \leq num_x$. This setting is expressive to represent AND (k_x=num_x), OR (k_x=1), and threshold gates over attributes. The children of every node are numbered from 1 to num. The function index(x) returns such a number associated with the node x, where the index values are uniquely assigned to nodes in the attribute tree in an arbitrary manner. Let function parent(x) denote the parent

of the node x. Each leaf node x of the tree is described by an attribute and a threshold value $k_x = 1$. The function att(x) denotes the attribute associated with the leaf node x.

IV. ATTRIBUTE-BASED SIGNATURE WITHOUT RANDOM ORACLES

In this section, we construct an ABS without random oracles, which consists of five algorithms: **Setup**, **Extract**$_{private}$, **Extract**$_{public}$, **Sign**, and **Verify**.

A. Construction

It is assumed that there are l attributes in universe denoted by the set U in the system. Associate each element in U with a unique integer in $\mathbb{Z}_q$. The bit length of a message is n, a separate parameter unrelated to q. The messages could be bit strings of arbitrary length and n be the output of a collision-resistant hash function $H:\{0,1\}^* \to \{0,1\}^n$.

We now describe our ABS construction, which supports any policy Γ consisting of AND, OR, and thresholds gates, that is, all policies $\Gamma(\cdot) \to 0/1$. Our construction works as follows:

Setup(l): To generate system parameters and the master key of the attribute authority, proceed as follows:

- Define the attributes in universe U as elements in $\mathbb{Z}_q$. For simplicity, let $l = |U|$ and take the first l elements of $\mathbb{Z}_q$ to be the universe. Namely, the integers 1,…,l (mod q).
- Select a random generator $g \in G_1$, a random $\alpha \in \mathbb{Z}_q^*$, and set $g_1 = g^\alpha$.
- Pick random elements $g_2, v' \in G_1$, a random l-length vector $\mathbf{F} = (f_i)$ and a random n-length vector $\mathbf{V} = (v_i)$, whose elements are chosen from G_1.
- Define $Z=e(g_1,g_2)$.
- The public parameters are $params=(q,G_1,G_2,e,g,g_1,g_2,Z,\mathbf{F},\mathbf{V})$, the master key MK is α.

Extract$_{private}$($params,MK,\omega$): To generate a private key for the attribute set ω, the following steps are taking:

- Choose a random $r \in \mathbb{Z}_q$ and compute $d = g_2^{r+\alpha}$.
- For each $i \in \omega$, choose $r_i \in \mathbb{Z}_q$ and compute $d_{i0} = g_2^{r/\alpha}(g_1 f_i)^{r_i}$, $d_{i1} = g^{r_i}$.
- Finally, output $sk_\omega = (d, \{d_{i0}, d_{i1}\}_{i\in\omega})$ as the private key for the user.

Extract$_{public}$($params,MK,\Gamma$): This algorithm generates a public key for a specific attribute tree Γ. Choose a polynomial p_x of degree $d_x = k_x - 1$ for each node in the tree, where k_x is the threshold gate. That is done in a top-down manner. Starting from the $p_{root}(0) = \alpha$ and d_{root} other points in the polynomial will be random. The other nodes we set $p_x(0) = p_{\text{parent}(x)}(\text{index}(x))$ and choose d_x other points randomly.

Once the polynomials have been decided, the public key gpk for Γ is $\{D_x = g^{p_x(0)}, h_i = (g_1 f_i)^{p_x(0)}\}$, where i=att(x), x is a leaf node.

Sign($params,M,\Gamma,sk_\omega$): Suppose one has a private key for the attribute set ω. To generate a signature on message $M = (m_1,...,m_n) \in \{0,1\}^n$ with policy Γ, namely, to prove ω satisfies the policy, i.e. $\Gamma(\omega) = 1$, he proceeds as follows:

- Choose a random $s \in \mathbb{Z}_q$ and compute $\sigma_0 = (v'\prod_{j=1}^{n} v_j^{m_j})^s d$, $\sigma_0' = g^s$.
- Let ω^* denote attributes set associated with leaves in Γ. For each $i \in \omega^*$, choose $r_i' \in \mathbb{Z}_q$ randomly and compute $\{\sigma_{i0} = d_{i0}(g_1 f_i)^{r_i'}, \sigma_{i1} = d_{i1} g^{r_i'}\}_{i\in\omega\cap\omega^*}$, $\{\sigma_{i0} = (g_1 f_i)^{r_i'}, \sigma_{i1} = g^{r_i'}\}_{i\in\omega^*/\omega\cap\omega^*}$.
- Finally, he outputs the signature $\sigma = (\sigma_0, \{\sigma_{i0}, \sigma_{i1}\}_{i\in\omega^*}, \sigma_0')$.

Verify($params$, σ ,M,gpk):To verify the signature we first define a recursive algorithm VerNode(σ ,gpk,x) , where x is a node in the tree Γ. It outputs a group element of G_2 or $\perp$.

Let i=att(x). If the node x is a leaf node then:

$$\text{VerNode}(\sigma, gpk, x) = \begin{cases} \dfrac{e(\sigma_{i0}, D_x)}{e(\sigma_{i1}, h_i)}, \text{if } \dfrac{e(\sigma_{i0}, D_x)}{e(\sigma_{i1}, h_i)} \neq 1 \\ \perp, \text{otherwise} \end{cases}$$

Notice that if $i \in \omega \cap \omega^*$

$$\begin{aligned} \frac{e(\sigma_{i0}, D_x)}{e(\sigma_{i1}, h_i)} &= \frac{e(d_{i0}(g_1 f_i)^{r_i'}, g^{p_x(0)})}{e(d_{i1} g^{r_i'}, (g_1 f_i)^{p_x(0)})} \\ &= \frac{e(g_2^{r/\alpha}(g_1 f_i)^{r_i + r_i'}, g^{p_x(0)})}{e(g^{r_i + r_i'}, (g_1 f_i)^{p_x(0)})} \\ &= \frac{e(g_2^{r/\alpha}, g^{p_x(0)}) e((g_1 f_i)^{r_i + r_i'}, g^{p_x(0)})}{e((g_1 f_i)^{r_i + r_i'}, g^{p_x(0)})} \\ &= e(g, g_2)^{r/\alpha p_x(0)} \end{aligned}$$

And if $i \in \omega^*/\omega \cap \omega^*$

$$\frac{e(\sigma_{i0}, D_x)}{e(\sigma_{i1}, h_i)} = \frac{e((g_1 f_i)^{r_i'}, g^{p_x(0)})}{e(g^{r_i'}, (g_1 f_i)^{p_x(0)})} = 1.$$

For a non-leaf node x. The algorithm VerNode(σ ,gpk,x) then proceeds as follows: For all nodes z that are children of x, it calls VerNode(σ ,gpk,z) and stores the output as F_z. Let S_x be an arbitrary k_x -sized set of child nodes z such that $F_z \neq \perp$. If no such set exists then the node was not satisfied and the function returns $\perp$. Otherwise let i=index(z), $S_x' = \{\text{index}(z) : z \in S_x\}$ and compute:

$$
\begin{aligned}
F_x &= \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (e(g,g_2)^{r/\alpha p_z(0)})^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} (e(g,g_2)^{r/\alpha p_{\mathrm{parent}(z)}(\mathrm{index}(z))})^{\Delta_{i,S_x'}(0)} \\
&= \prod_{z \in S_x} e(g,g_2)^{r/\alpha p_x(i)\Delta_{i,S_x'}(0)} \\
&= e(g,g_2)^{r/\alpha p_x(0)}
\end{aligned}
$$

To verify the signature calculate F_{root}. Then check if

$$\frac{e(g,\sigma_0)}{F_{root} \cdot e(v' \prod_{j=1}^{n} v_j^{m_j}, \sigma_0')} \stackrel{?}{=} Z$$

If the equation holds then output ***accept***, which indicates the signature is indeed from some user with attributes satisfying Γ. Otherwise ***reject***.

B. Correctness

If and only if the policy is satisfied, i.e. $\Gamma(\omega) = 1$, then according to Lagrange interpolation,

$F_{root} = e(g,g_2)^{r/\alpha \cdot p_{root}(0)} = e(g,g_2)^{r/\alpha \cdot \alpha} = e(g,g_2)^r$. So

$$
\begin{aligned}
\frac{e(g,\sigma_0)}{F_{root} \cdot e(v' \prod_{j=1}^{n} v_j^{m_j}, \sigma_0')} &= \frac{e(g,(v' \prod_{j=1}^{n} v_j^{m_j})^s d)}{e(g,g_2)^r e(v' \prod_{j=1}^{n} v_j^{m_j}, g^s)} \\
&= \frac{e(g,(v' \prod_{j=1}^{n} v_j^{m_j})^s g_2^{r+\alpha})}{e(g,g_2)^r e(v' \prod_{j=1}^{n} v_j^{m_j}, g)^s} \\
&= \frac{e(g,(v' \prod_{j=1}^{n} v_j^{m_j})^s) e(g,g_2^{r+\alpha})}{e(g,g_2)^r e(g,(v' \prod_{j=1}^{n} v_j^{m_j})^s)} \\
&= \frac{e(g,g_2)^{r+\alpha}}{e(g,g_2)^r} = Z
\end{aligned}
$$

V. CONCLUSION

In this paper, we propose an attribute-based signature scheme without random oracles, which improve the previous work in [6], supporting any policy consisting of AND, OR, threshold gates under computational Diffie-Hellman problem. The way to build our scheme without random oracle model is similar to that in Waters [7], which represents a high level of IBE without random oracles. In future, we will enhance the efficiency of our work, and attempt to use it in real applications.

ACKNOWLEDGMENT

The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No.2009CB320503; the National 863 Development Plan of China under Grant No. 2009AA01A334, 2009AA01A346, 2009AA01Z423; and the project of National Science Foundation of China under Grant No. 61070199, 61003301, 60903223, 60903224; and is supported by Program for Changjiang Scholars and Innovative Research Team in University of the Ministry of Education, the Innovation Research Team in Universities of Hunan Province.

REFERENCES

[1] H. Maji, M. Prabhakaran and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," http://eprint.iacr.org/2008/328, 2008.

[2] G. Shanqing and Z. Yingpei, "Attribute-based Signature Scheme," Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), Washington, DC, USA, 2008, pp. 509--511.

[3] J. Li, M. H. Au, W. Susilo, D. Xie, and K. Ren, "Attribute-based signature and its applications," Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security-ASIACCS'10, Beijing, China, 2010, pp. 60-69.

[4] J. Li and K. Kim, "Hidden attribute-based signatures without anonymity revocation," Information Sciences: an International Journal, vol. 180, pp. 1681-1689, 2010-05-01 2010.

[5] S. Shahandashti and R. Safavi-Naini, "Threshold Attribute-Based Signatures and Their Application to Anonymous Credential Systems," Progress in Cryptology – AFRICACRYPT 2009, 2009, pp. 198-216.

[6] D. Cao, B. Zhao, X. Wang, J. Su, and Y. Chen, "Authenticating with Attributes in Online Social Networks," 2th International Symposium on Frontiers in Ubiquitous Computing, Networking and Applications (NeoFUSION-2011), to appear, 2011.

[7] B. Waters, "Efficient Identity-Based Encryption Without Random Oracles," Advances in Cryptology-EUROCRYPT'05, 2005, pp. 114-127.

[8] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Advances in Cryptology-CRYPTO'84, 1984, pp. 47-53.

[9] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Advances in Cryptology-CRYPTO'01, 2001, pp. 213-229.

[10] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001, pp. 26-28.

[11] M. Bellare and P. Rogaway, "Random oracles are practical : a paradigm for designing efficient protocols," Computer and communications security, Fairfax, Virginia, United States, 1993, pp. 62-73.

[12] R. Canetti, S. Halevi and J. Katz, "Chosen-Ciphertext Security from Identity-Based Encryption," Advances in Cryptology-EUROCRYPT'04, 2004, pp. 207-222.

[13] R. Canetti, S. Halevi and J. Katz, "A Forward-Secure Public-Key Encryption Scheme," Advances in Cryptology-EUROCRYPT'03, 2003, pp. 255-271.

[14] D. Boneh and X. Boyen, " Efficient selective-ID secure identity based encryption without random oracles," Advances in Cryptology-EUROCRYPT'04, 2004, pp. 223 – 238.

[15] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," Advances in Cryptology-CRYPTO'04, 2004, pp. 443-459.

[16] C. Gentry, "Practical Identity-based encryption without random oracles," Advances in Cryptology-Eurocrypt'06, 2006, pp. 445 – 464.

[17] C. Wang, W. Chen and Y. Liu, "A Fuzzy Identity Based Signature Scheme," International Conference on E-Business and Information System Security(EBISS'09), 2009, pp. 1 -5.

[18] P. Yang, Z. Cao and X. Dong, "Fuzzy Identity Based Signature," http://eprint.iacr.org/2008/002.pdf, 2008.

[19] S. Tan, S. Heng and B. Goi, "On the Security of an Attribute-Based Signature Scheme," Communications in Computer and Information Science, 2009, pp. 161-168.

[20] M. Karchmer and A. Wigderson, "On Span Programs," the 8th Annual Structure in Complexity Theory, 1993, pp. 102-111.

Published by Atlantis Press, Paris, France.