Edith Cowan University
Research Online

Australian Information Security Management Conference

Conferences, Symposia and Campus Events

2011

Efficient and expressive fully secure attribute-based signature in the standard model

Piyi Yang
University of Shanghai for Science and Technology

Tanveer A. Zia
Charles Sturt University

Zhenfu Cao
Shanghai Jiaotong University

Xiaolei Dong
Shanghai Jiaotong University

DOI: 10.4225/75/57b54e95cd8cf
Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/134

EFFICIENT AND EXPRESSIVE FULLY SECURE ATTRIBUTE-BASED SIGNATURE IN THE STANDARD MODEL

[1]Piyi Yang, [2]Tanveer A Zia, [3]Zhenfu Cao and [4]Xiaolei Dong
[1]Department of Computer Science and Engineering, School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, Peoples Republic of China
[2]School of Computing & Mathematics, Charles Sturt University, NSW, Australia
[3, 4]Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai, People's Republic of China
yang.piyi@gmail.com, tzia@csu.edu.au, zfcao@cs.sjtu.edu.cn, dong-xl@cs.sjtu.edu.cn

Abstract

Designing a fully secure (adaptive-predicate unforgeable and perfectly private) attribute-based signature (ABS), which allows a signer to choose a set of attributes in stead of a single string representing the signer's identity, under standard cryptographic assumption in the standard model is a challenging problem. Existing schemes are either too complicated or only proved in the generic group model. In this paper, we present an efficient fully secure ABS scheme in the standard model based on q-parallel BDHE assumption which is more practical than the generic group model used in the previous scheme. To the best of our knowledge, our scheme is the most efficient one among all the previous ABS schemes in the standard model. Moreover, our proposed scheme is highly expressive since it allows any signer to specify claim-predicates in terms of any predicate consists of AND, OR, and Threshold gates over the attributes in the system. ABS has found many important applications in secure communications, such as anonymous authentication system and attribute based messaging system.

Keywords
Attribute-based signature, q-parallel BDHE assumption, standard model, unforgeability, privacy, collusion resistance

INTRODUCTION

Identity-based signature is a powerful mechanism for providing the authentication of the stored and transmitted information where the identity can be an arbitrary string such as an email address or a registration number, etc. While this is useful for applications where the data receiver knows specifically the identity of the data signer, in many applications the signer will want to have fine-grained control over how much of her personal information is revealed by the signature.

Maji, Prabhakaran, and Rosulek (2008) presented a new vision of identity-based signature that they called Attribute-Based Signature (ABS), in which a signer is defined by a set of attributes instead of a single string representing the signer's identity. In ABS, a user obtains a set of attributes from one or multiple attribute authorities. An attribute-based signature assures the verifier that a signer, whose set of attributes satisfies a (possibly) complex predicate, has endorsed the message. The following example illustrates the concept. Suppose we have the following predicate:

Professor **OR** (((Biology Department **OR** Female) **OR** above 50 years old) **AND** University A).

Alice's attributes are (University A, Female). Bob's attributes are (above 50 years old, Professor). Although their attributes are quite different, it is clear that Alice and Bob can generate a signature on this predicate, and such a signature releases no information regarding the attribute or identity of the signer, i.e. Alice or Bob, except that the attribute of the signer satisfies the predicate.

This kind of authentication required in attribute-based signatures differs from that offered by identity-based signatures. An ABS solution requires a richer semantics, including privacy requirements, similar to more recent signature variants like group signatures (Chaum; Heyst, 1991), ring signatures (Rivest; Shamir; Tauman, 2001), and mesh signatures (Boyen, 2007). All of these primitives share the following semantics:

- Unforgeability. By verifying the signature, one is assured that the message was indeed endorsed by a party who satisfies the condition described in the claim.

- Privacy. The signature reveals no information about the signer other than the fact that it satisfies the claim. In particular, different signatures cannot be identified as generated by the same party.

Besides these two semantics, ABS has another important property which is called collusion resistance. It assures different parties should not be able to pool together their attributes to sign a message with a claim which none of them satisfy alone. For instance, if Alice has an attribute Female, and her friend Bob has an attribute Professor, they should not be able to sign a message claiming to have both the attributes.

ABS has found many important applications. For instance, it helps to provide fine-grained access control in anonymous authentication systems (Li; Au; Susilo; Xie; Ren, 2010). Another application of ABS, given by (Maji; Prabhakaran; Rosulek, 2008; 2011), is to fulfil a critical security requirement in attribute-based messaging (ABM) systems using ABS.

Related Work

Attribute-Based Signatures were first introduced by Magi, Prabhakaran, and Rosales (2008) as a way to let a signature attest not to the identity of the individual who endorsed a message, but instead to a (possibly complex) claim regarding the attributes she possesses. They constructed an ABS scheme that supports a powerful set of predicates, namely, any predicate consists of AND, OR, and Threshold gates. However, the security of their scheme is weak as their construction is only proved in the generic group model. Since then, there have been lots of works on this subject (Escala; Herranz; Morillo, 2011; Khader, 2007a; 2007b; Li; Au; Susilo; Xie; Ren, 2010; Li; Kim, 2007; 2010; Maji; Prabhakaran; Rosulek, 2011; Okamoto; Takashima, 2011; Shahandashti; Safavi-Naini, 2009).

Recently, Magi, Prabhakaran, and Rosulek (2011) presented an ABS scheme which is proven secure in the standard model. But it is much less efficient and more complicated than the scheme in (Maji; Prabhakaran; Rosulek, 2008), since it employs the Groth-Sahai NIZK protocols (2008) as building blocks. Okamoto and Takashima (Okamoto; Takashima, 2011) presented a fully secure attribute-based signature (ABS) scheme in the standard model. The admissible predicates of the scheme support non-monotone predicates. Escala, Herranz, and Morillo (2011) proposed a fully secure attribute-based signature (ABS) scheme in the standard model. This scheme supports an additional property of revocability, so that an external judge can break the anonymity of a signature when necessary.

Another related notion to ABS is fuzzy identity-based signature which was proposed and formalized in (Shanqing; Yingpei, 2008; Yang; Cao; Dong, 2011). It allows a user with identity ω to issue a signature which could be verified with identity ω' if and only if ω and ω' are within a distance judged by some metric. However, this kind of signatures does not consider the anonymity for signer.

Table 1: Comparison Of ABS Systems In Terms Of Signature Size, Model, Assumptions, Predicates, Two Examples Of Signature Size

	MPR08 (Maji; Prabhakaran; Rosulek, 2008)	MPR11 (Maji; Prabhakaran; Rosulek, 2011) (Boneh-Boyen based)	MPR11 (Maji; Prabhakaran; Rosulek, 2011) (Waters based)	OT (Okamoto; Takashima, 2011)	EHM (Escala; Herranz; Morillo, 2011)	Proposed
Signature size (# of group elts)	$l + r + 2$	$51l + 2r + 18\lambda l$	$36l + 2r + 9\lambda + 12$	$7l + 11$	$9l + 7$	$4l + 1$
Model	generic group model	standard model	standard model	standard model	standard model	standard model
Security	full	full	full	full	full	full
Assmuptions	CR hash	q−SDH and DLIN	DLIN	DLIN and CR hash	CHD and Subgroup Decision	q−BDHE and CR hash
Predicates	monotone	monotone	monotone	non-monotone	monotone	monotone
Sig. size example 1 (l=10,r=5, λ = 128)	17	23560	1534	81	97	41
Sig. size example 2 (l=100,r=50, λ = 128)	152	282400	4864	711	907	401

Our Contribution

Maji, Prabhakaran, Rosulek (Maji; Prabhakaran; Rosulek, 2008; 2011) and Okamoto, Takashima (2011) pointed that the future work of ABS, on the theoretical front, is to base the security of ABS on a standard hardness assumption, while still preserve the efficiency for the most part. In this paper, we attempt to propose such an ABS scheme which is secure in the standard model based on decisional parallel bilinear Diffie-Hellman exponent assumption (Waters, 2011) which is more practical than the generic group model of (Maji; Prabhakaran; Rosulek, 2008).

The proposed ABS scheme is efficient and practical. We compare our scheme with the existing ABS schemes in the standard model: Maji, Prabhakaran, and Rosulek's (2011) (two typical instantiations), Okamoto and Takashima's (2011), and Escala, Herranz, and Morillo's (2011), as well as the ABS scheme in the generic group model (Maji; Prabhakaran; Rosulek, 2008) (as a benchmark). All of these schemes can be implemented over a pairing group and the size of a group element is about the size of Z_p (e.g., 256 bits). In Table 1 we summarize the comparison.

In Table 1, l and r represent the size of the underlying access structure matrix M for a predicate, i.e. $M \in Z^{l \times r}$. We also give comparison of two examples, the predicate with 4 AND and 5 OR gates as well as 10 variables which is expressed by a 10 × 5 matrix, and the predicate with 49 AND and 50 OR gates as well as 100 variables which is expressed by a 100 × 50 matrix (see the appendix of (Lewko; Waters, 2011)). λ is the security parameter (e.g. 128).

As the above comparison, our construction is the most efficient ABS scheme in the standard model of the literature.

NOTATIONS

We denote the finite field of order q by F_q. We also denote the group $\{0,1,\ldots,p-1\}$ under addition modulo p by $\mathbb{Z}_p$, and $\mathbb{Z}_p \setminus \{0\}$ by $\mathbb{Z}_p^*$, where p is a large prime number satisfying $p = 2p' + 1$ with p' itself prime. A vector symbol denotes a vector representation over $\mathbb{Z}_p$, e.g. $\vec{x}$ denotes $(x_1,\ldots,x_n) \in \mathbb{Z}_p^{1\times n}$. $y := z$ denotes that y is defined by z. We use $\mathbf{span}\langle \overrightarrow{x_1},\ldots,\overrightarrow{x_2}\rangle$ denotes the subspace generated by $\overrightarrow{x_1},\ldots,\overrightarrow{x_n}$. For two vectors $\vec{x} = (x_1,\ldots,x_n)$ and $\vec{y} = (y_1,\ldots,y_n)$, $\vec{x}\cdot\vec{y}$ denotes the inner-product $\sum_{i=1}^{n} x_i y_i$. X^{T} denotes the transpose of matrix X. $\mathbf{det}(\mathbf{M})$ denotes the rank of matrix $\mathbf{M}$. We denote a monotone span program (Beimel, 1996) over a field F_q as $\mathbf{M} := (\mathbf{M}, \rho)$ in which there exists a linear secret sharing scheme (Okamoto; Takashima, 2011). We define our attribute-based signature scheme, which consists of four algorithms, namely, setup algorithm $\mathbf{Setup}$, private key generation algorithm $\mathbf{KeyGen}$, signing algorithm $\mathbf{Sign}$, and verification algorithm $\mathbf{Verify}$, and its security definition as (Maji; Prabhakaran; Rosulek, 2008). We denote G and G_T as two multiplicative cyclic groups of prime order p, g as a generator of G, and e as a bilinear map, $e: \mathrm{G} \times \mathrm{G} \to \mathrm{G}_T$ (Boneh; Franklin, 2003).

OUR CONSTRUCTION

Our construction is inspired by the attribute based encryption scheme (ABE) of Waters (Waters, 2011). Roughly speaking, a secret signing key SK_S with attribute set S corresponds to a secret decryption key SK_S with S in ABE (Waters, 2011). No counterpart of a signature σ in our construction exists in the ABE (Waters, 2011). In order to meet the privacy condition for σ, a novel technique is applied to randomly generate a signature from the private key SK_S and the claim-predicate Y. And there are many subtleties in the proof of unforgeability, e.g., we need to cancel all the unknown terms in order to answer the queries and solve the $q-$BDHE problem. We develop a novel technique to resolve the difficulty. See the proof for more details.

Let U be the universe of possible attributes. A *claim-predicate* over U is a monotone boolean function, whose inputs are associated with attributes of U. We say an attribute set $S \subset \mathrm{U}$ satisfies a claim-predicate Y if $\mathrm{Y}(S) = 1$.

Setup (U): The input parameter U is the number of attributes in the system. Choose suitable cyclic groups G and G_{T} of prime order p, equipped with a bilinear pairing $e : \mathrm{G} \times \mathrm{G} \to \mathrm{G}_T$. Choose a generator g and U random group elements $h_1, \ldots, h_U \in \mathrm{G}$ that are associated with the U attributes in the system. Pick random number $\alpha, a \in \mathbb{Z}_p$. Choose a collision resistant hash function $H : \{0,1\}^* \to \mathbb{Z}_p$. The master key is $\mathrm{MSK} = g^{\alpha}$. The public key PK is a description of the groups G, G_T and their pairing function, as well as, $g, e(g,g)^{\alpha}, g^a, h_1, \ldots, h_U$.

KeyGen (MSK, *S*): On input the master secret key MSK and a set S of attributes, the algorithm fist picks a random $t \in \mathbb{Z}_p$. Create the private key SK as

$$K = g^{\alpha} g^{at} \quad L = g^t \quad \forall x \in S \; K_x = h_x^t.$$

Sign (PK, SK_s, M, Y): On input the private key SK_s for an attribute set S, a message M ,and a claim-predicate Y such that $\mathrm{Y}(S) = 1$. First convert Y to its corresponding monotone span program $\mathbf{M} \in (\mathbb{Z}_p)^{l \times n}$, with row labeling function ρ associates rows of $\mathbf{M}$ to attributes. Computes $\vec{\alpha} = (\alpha_1, \ldots, \alpha_l)$ such that $\sum_{i \in I} \alpha_i \mathbf{M}_i = \vec{1}$ and $\alpha_i = 0, i \notin I$, where $\mathbf{M}_i$ is the vector corresponding to the ith row of $\mathbf{M}$, and $I := \{i \mid \rho(i) \in S\}$. If there is no such $\alpha_j^{'}$ and J that $\sum_{j \in J} \alpha_j^{'} \cdot M_j = \vec{0}$, let $\vec{\beta} = (\beta_1, \ldots, \beta_l) = (0, \ldots, 0)$. In this case, any attribute set from $\{\rho(i) \mid 1 \le i \le l\}$ satisfies the claim-predicate Y and the rank of matrix $\mathbf{M}$ is less than l. Otherwise, chooses $\vec{\beta} = (\beta_1, \ldots, \beta_l)$ randomly from $\mathbb{Z}_p^{*1 \times l}$ and solves the equation $\mathbf{M}^{\mathbf{T}} \cdot \vec{\gamma}^{\mathbf{T}} = \vec{\beta} \cdot \mathbf{M}$ to obtain $\vec{\gamma} = \gamma_1, \ldots, \gamma_l$. In addition, the algorithm chooses random $r, r_1, \ldots, r_l \in \mathbb{Z}_p$.

The signature σ is computed as follows,

$$A = (K \cdot g^{ar})^{H(\mathrm{M} \| \mathrm{Y})}$$

$$(B_i = g^{r_i \gamma_i}, C_i = h_{\rho(i)}^{-r_i \gamma_i}, E_i = K_{\rho(i)}^{\alpha_i H(\mathrm{M} \| \mathrm{Y})} \cdot h_{\rho(i)}^{r_i \beta_i} \cdot h_{\rho(i)}^{r \alpha_i H(\mathrm{M} \| \mathrm{Y})}, F_i = L^{\alpha_i H(\mathrm{M} \| \mathrm{Y})} \cdot g^{r_i \beta_i} \cdot g^{r \alpha_i H(\mathrm{M} \| \mathrm{Y})}) \text{ for } 1 \le i \le l$$

, along with description of Y.

Here, three points should be noted.

1. The signer may not have $K_{\rho(i)}$ for every attribute $1 \le i \le l$. But when this is the case, $\alpha_i = 0$, and so the value is not needed.

2. $t\alpha_i H(\mathrm{M} \| \mathrm{Y}) + r\beta_i + r\alpha_i H(\mathrm{M} \| \mathrm{Y}) = 0$ will not leak any information about the signer's attribute. Because this only occurs when $\vec{\beta} = \vec{0}$, which means any attribute set from $\{\rho(i) \mid 1 \le i \le l\}$ satisfies the claim-predicate Y. Therefore, α_i could be zero whether $i \in I$ or not, so α_i being zero has no relationship with the signer holding the attribute $\rho(i)$. Because if α_i is chosen zero, the remaining $\alpha_j (j \in I \setminus \{i\})$ still guarantees $\sum_{j \in I \setminus \{i\}} \alpha_j \mathbf{M}_j = \vec{1}$. In this case, when $t\alpha_i H(\mathrm{M} \| \mathrm{Y}) + r\beta_i + r\alpha_i H(\mathrm{M} \| \mathrm{Y}) = 0$, the

signer may either hold the attribute $\rho(i)$ or not hold the attribute $\rho(i)$. As a result, people gain no knowledge about whether the signer has the attribute $\rho(i)$ giving the knowledge of $t\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y}) + r\beta_i + r\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y}) = 0$.

3. $\vec{\gamma}$ is a random vector from $\mathbb{Z}_p^{1\times n}$ and has no relationship with $\vec{\beta}$ ($\vec{\beta} \neq \vec{0}$). Since $\vec{\beta} \neq \vec{0}$, we have $\mathbf{det}(\mathbf{M}) < l$. Given $\vec{\gamma}$, there are $p^{l-\mathbf{det}(\mathbf{M})}$ possible $\vec{\beta}$ for $\mathbf{M}^{\mathbf{T}} \cdot \vec{\gamma}^{\mathbf{T}} = \vec{\beta} \cdot \mathbf{M}$. Here, $\mathbf{det}(\mathbf{M})$ is the rank of matrix $\mathbf{M}$. Therefore, the probability to deduce $g^{r_i\beta_i}$ successfully from $\{g^{r_i\gamma_i}\}_{i=1,\ldots,n}$ is negligible, since p is a large prime number.

Verify ($\mathrm{PK}, \sigma, \mathrm{M}$): On input public parameters PK, the message M, and the signature σ which is generated under the claim-predicate Y such that $\mathrm{Y}(S) = 1$. First convert Y to its corresponding monotone span program $\mathbf{M} \in (\mathbb{Z}_p)^{l\times n}$ with row labeling function ρ. Choose a random vector $\vec{v} \in \mathbb{Z}_p^{1\times n}$. Computes $\vec{s}^{\mathbf{T}} = (s_1, \ldots, s_l)^{\mathbf{T}} = \mathbf{M} \cdot \vec{v}^{\mathbf{T}}, s_0 = \vec{1} \cdot \vec{v}^{\mathbf{T}}$. Check the following constraints,

$$e(B_i, g) \stackrel{?}{=} e(C_i, 1/h_{\rho(i)}),\ e(E_i, g) \stackrel{?}{=} e(F_i, h_{\rho(i)}), \quad \text{for } 1 \le i \le l$$

$$\frac{e(A, g^{s_0}) \cdot \prod_{i=1}^{l} e(B_i, g^a)^{s_i}}{\prod_{i=1}^{l} (e(C_i, F_i) \cdot e(g^a, F_i) \cdot e(B_i, E_i))^{s_i}} \stackrel{?}{=} e(g, g)^{\alpha \cdot H(\mathrm{M} \,\|\, \mathrm{Y}) \cdot s_0},$$

returns **accept** if the above check succeed, and **reject** otherwise.

[Correctness]

$$\frac{e(A, g^{s_0}) \cdot \prod_{i=1}^{l} e(B_i, g^a)^{s_i}}{\prod_{i=1}^{l} (e(C_i, F_i) \cdot e(g^a, F_i) \cdot e(B_i, E_i))^{s_i}}$$

$$= \frac{e(g^{\alpha H(\mathrm{M} \,\|\, \mathrm{Y})} g^{atH(\mathrm{M} \,\|\, \mathrm{Y})} g^{arH(\mathrm{M} \,\|\, \mathrm{Y})}, g^{s_0}) \cdot \prod_{i=1}^{n} e(g^{r_i\gamma_i}, g^a)^{s_i}}{\prod_{i=1}^{l} (e(h_{\rho(i)}^{-r_i\gamma_i}, g^{t\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})} g^{r_i\beta_i} g^{r\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})}) \cdot e(g^a, g^{t\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})} g^{r_i\beta_i} g^{r\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})}) \cdot e(g^{r_i\gamma_i}, h_{\rho(i)}^{t\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})} h_{\rho(i)}^{r_i\beta_i} h_{\rho(i)}^{r\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})}))^{s_i}}$$

$$= \frac{e(g, g)^{\alpha \cdot s_0 H(\mathrm{M} \,\|\, \mathrm{Y})} \cdot e(g, g)^{as_0 tH(\mathrm{M} \,\|\, \mathrm{Y})} \cdot e(g, g)^{ars_0 H(\mathrm{M} \,\|\, \mathrm{Y})} \cdot \prod_{i=1}^{l} \prod_{j=1}^{n} e(g^{r_i\gamma_i \cdot \mathbf{M}_{*j}}, g^a)^{v_j}}{\prod_{i=1}^{l} e(g^a, g^{t\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})} g^{r_i\beta_i} g^{r\alpha_i H(\mathrm{M} \,\|\, \mathrm{Y})})^{s_i}}$$

$$= \frac{e(g, g)^{\alpha \cdot s_0 H(\mathrm{M} \,\|\, \mathrm{Y})} \cdot e(g, g)^{as_0 tH(\mathrm{M} \,\|\, \mathrm{Y})} \cdot e(g, g)^{ars_0 H(\mathrm{M} \,\|\, \mathrm{Y})} \cdot \prod_{i=1}^{l} \prod_{j=1}^{n} e(g^{r_i\gamma_i \cdot \mathbf{M}_{*j}}, g^a)^{v_i}}{e(g^a, g^t)^{H(\mathrm{M} \,\|\, \mathrm{Y}) \sum_{i=1}^{l} s_i\alpha_i} \cdot e(g^{r_i\beta_i \cdot \mathbf{M}_{*j}}, g^a)^{v_i} \cdot e(g^a, g^{rH(\mathrm{M} \,\|\, \mathrm{Y})})^{\sum_{i=1}^{l} \alpha_i s_i}}$$

$$= e(g, g)^{\alpha \cdot s_0 H(\mathrm{M} \,\|\, \mathrm{Y})}$$

Note that $\mathbf{M}_{*j}$ is the jth column of the monotone span program $\mathbf{M}$.

Theorem 1. *Our construction is correct and perfectly private.*
The proof of theorem 1 is given in the full version of this paper.

Theorem 2. *Our construction is (adaptive-predicate) unforgeable under the decisional q-parallel BDHE*

assumption (Waters, 2011) and the existence of collision resistant hash functions.

Proof: In this proof, we embed a random k attribute $\mathbf{M}^*$ into the public parameters h_x using $q-$parallel BDHE assumption. For each row i of $\mathbf{M}^*$ the simulator programs n pieces of information $(\mathbf{M}^*_{i,1},\ldots,\mathbf{M}^*_{i,n})$ into the h_x related to the attribute assigned to that row. With this method, the simulator is able to cancel the unknown terms during private key queries and signature queries, as well as combine the forged signature to solve the $q-$parallel BDHE problem.

Suppose an adversary A has a non-negligible advantage $\grave{o}=\mathbf{Adv}_{\mathrm{A}}$ advantage in attacking our scheme. We show how to build a simulator B that solves the decisional $q-$parallel BDHE problem.

Initial Phase: The simulator takes in a decisional $q-$parallel BDHE challenge $\vec{y},T$. The simulator randomly chooses a $k=\lfloor U-\log_2 3t \rfloor$ attribute predicate Y^* and converts Y^* to its corresponding monotone span program $(\mathbf{M}^*,\rho^*)$, where $\mathbf{M}^*$ has l^* rows and n^* columns. Here, $\lfloor\ \rfloor$ is the round down operation, t is the maximum number of private key queries and signature generation queries, and $l^*,n^*<q$.

Setup Phase: The simulator chooses random $\alpha'\in\square_p$ and implicitly sets $\alpha=\alpha'+a^{q+1}$ by letting $e(g,g)^{\alpha}=e(g^a,g^{a^q})e(g,g)^{\alpha'}$. We describe how the simulator programs $h_1,\ldots,h_U$.

For each x where $1\le x\le U$, it begins by choosing a random value z_x. Let X denotes the set of indices of i such that $\rho^*(i)=x$. The simulator programs h_x as:

$$h_x=g^{z_x}\prod_{i\in X}g^{aM^*_{i,1}/b_i}\cdot g^{a^2M^*_{i,2}/b_i}\cdots g^{a^{n^*}M^*_{i,n^*}/b_i}$$

If $X=\varnothing$ then we have $h_x=g^{z_x}$. *Note that h_x are distributed randomly due to the g^{z_x} value.*

The simulator gives to A the public key: $g,e(g,g)^{\alpha},g^a,h_1,\ldots,h_U$.

The corresponding master key, $\mathrm{MSK}=g^{\alpha}$, is unknown to the simulator.

Query Phase: In this phase the simulator answers private key queries and signature queries. Suppose the simulator is given a private key query for a set S.

If S satisfies Y^*, then the simulator aborts and randomly chooses its guess β of the $q-$parallel BDHE problem. Otherwise, the simulator first picks a random $r\in\square_p$. Next it finds a vector $\vec{w}=(w_1,\ldots,w_{n^*})\in\square_p^{1\times n^*}$ such that $w_1=-1$ and for all i where $\rho^*(i)\in S$ we have that $\vec{w}\cdot\mathbf{M}^*_i=0$. By the definition of monotone span program such a vector must exist.

The simulator begins by implicitly defining t as $r+w_1a^q+w_2a^{q-1}+\cdots+w_{n^*}a^{a^{-n^*+1}}$. It performs this by setting $L=g^r\prod_{i=1,..,n^*}(g^{a^{q+1-i}})^{w_i}=g^t$.

We observe that by our definition of t, g^{at} contains a term $g^{-a^{q+1}}$ which will cancel out the unknown term in g^{α} when generating K. The simulator can compute K as:

$$K = g^{\alpha'} g^{ar} \prod_{i=2,..,n^*} (g^{a^{q+2-i}})^{w_i} .$$

Now we calculate the key components K_x for $\forall x \in S$. First, we consider $x \in S$ for which there is no i such that $\rho^*(i) = x$. For those we can simply let $K_x = L^{z_x}$.

The more difficult task is to create keys for attribute $x \in S$, where there exists an i such that $\rho^*(i) = x$ and $i \le n^*$. To compute these keys we must make sure that there are no terms of the form g^{a^{q+1}/b_i} that we can't simulate. Notice that in calculating $K_x = h_x^t$ all terms of this form come from $g^{a^{q+1}/b_i M_{i,j} w_j}$, where $\rho^*(i) = x$. However we have that $\vec{w} \cdot \mathbf{M}_i^* = 0$, all of these terms cancel.

Again, let X be the set of all i such that $\rho(i)^* = x$. The simulator creates K_x in this case as follows.

$$K_x = L^{z_x} \prod_{i \in X} \prod_{j=1,...n^*} (g^{(a^j/b_i)r} \prod_{\substack{k=1,..,n^* \\ k \ne j}} (g^{a^{a+1+j-k}/b_i})^{w_k})^{M^*_{i,j}} .$$

The simulator B returns $(K, L, (K_x)_{x \in S})$ to the adversary A.

To answer a signature query on (M, Y). If $\forall S$ that satisfies Y also satisfies Y^*, the simulator aborts and outputs a random guess for β. Otherwise, the simulator randomly chooses a set S that satisfies Y but does not satisfy Y^*, and asks the private key generation oracle to get the private key for S. Next, it uses the private key to generate the signature on (M, Y), and returns it to the adversary A.

Forgery: After a polynomially bounded number of private key queries and signature queries, the adversary outputs a forged signature $\sigma' = (A', (B_i')_{i=1,..,n}, (C_i', D_i', E_i', F_i')_{i=1,..,l})$ on message M' for the claim-predicate Y', such that $(\mathrm{M}', \mathrm{Y}')$ was never queried to the signature generation oracle and Y' does not accept any S queried to the key generation oracle. If $\exists S$ that is accepted by Y' but not accepted by Y^*, the simulator aborts and outputs a random guess for β. Otherwise, the simulator can solve the decisional $q-$ parallel BDHE problem as follows.

First, convert Y' to its corresponding monotone span program $\mathbf{M}' \in \mathbb{Z}_p^{l^* \times n^*}$ with row labeling function ρ'. The tricky part is to compute the g^{as_i} since it contains terms ($g^{a^i s}$) that we must cancel out. However, the simulator can use secret splitting to make these terms cancel out. Intuitively, the simulator chooses random $y_{2'}, \ldots, y_{n^*}$. Then the simulator shares the secret using the vector $\vec{v} = (s, sa + y_{2'}, sa^2 + y_{3'}, \ldots, sa^{n-1} + y_{n^*}) \in \mathbb{Z}_p^{1 \times n}$. Next, we define

$$R_i = \{k \mid \rho^*(k) = \rho'(i) \wedge k \ne i, i = 1, \ldots, n\}.$$

Suppose $r_1', \ldots, r_l'$ are random values, we have the following equations,

$$B_i' = g^{r_i \gamma_i} = g^{-r_i'} g^{sb_i}, C_{i'} = h^{-r_i \gamma_i} = h_{\rho'(i)}^{r_i' - sb_i}$$

$$g^{as_i} C_i' = h_{\rho'(i)}^{r_i'} (\prod_{j=2,..,n^*} (g^a)^{M^*_{i,j} y_j'}) (g^{b_i \cdot s})^{-z_{\rho'(i)}} (\prod_{k \in R_i} \prod_{j=1,..,n^*} (g^{a^j \cdot s \cdot (b_i/b_k)})^{M^*_{k,j}})$$

Thus, the simulator could compute g^{as_i} and $g^{r_i'}$ as follows,

$$g^{as_i} = h_{\rho'(i)}^{r_i'}(\prod_{j=2,\ldots,n}(g^a)^{M^*_{i,j}y_j'})(g^{b_i\cdot s})^{-z_{\rho'(i)}}(\prod_{k\in R_i}\prod_{j=1,\ldots,n}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}})/C_i'$$

$$g^{r_i'} = g^{sb_i}/B_i'$$

Thus, the simulator compute $e(F_i', g^{as_i})$ and $e(B_i', g^{as_i})$ as follows.

$$e(F_i', g^{as_i})$$

$$= e(F_{i'}, h_{\rho'(i)}^{r_{i'}}) \cdot e(F_i', (\prod_{j=2,\ldots,n}(g^a)^{M^*_{i,j}y_{j'}})(g^{b_i\cdot s})^{-z_{\rho'(i)}}(\prod_{k\in R_i}\prod_{j=1,\ldots,n}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}})/C_i')$$

$$= e(E_i', g^{r_i'}) \cdot e(F_i', (\prod_{j=2,\ldots,n}(g^a)^{M^*_{i,j}y_j'})(g^{b_i\cdot s})^{-z_{\rho'(i)}} \cdot (\prod_{k\in R_i}\prod_{j=1,\ldots,n}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}})/C_i')$$

$$e(B_i', g^{as_i})$$

$$= e(B_{i'}, h^{r_i'}) \cdot e(B_i', (\prod_{j=2,\ldots,n}(g^a)^{M^*_{i,j}y_j'})(g^{b_i\cdot s})^{-z_{\rho'(i)}} \cdot (\prod_{k\in R_i}\prod_{j=1,\ldots,n}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}})/C_i')$$

$$= e(C_i', g^{r_i'}) \cdot e(B_i', (\prod_{j=2,\ldots,n}(g^a)^{M^*_{i,j}y_{j'}})(g^{b_i\cdot s})^{-z_{\rho'(i)}} \cdot (\prod_{k\in R_i}\prod_{j=1,\ldots,n}(g^{a^j\cdot s\cdot(b_i/b_k)})^{M^*_{k,j}})/C_i')$$

If $(e(A', g^s)\cdot\prod_{j=1}^{n} e(B_i', g^{as_i}))/\prod_{i=1}^{l} e(F_i', g^{as_i}) = T^{H(\mathrm{M}'\|\mathrm{Y}')}\cdot e(g^s, g^{\alpha'})^{H(\mathrm{M}'\|\mathrm{Y}')}$, the simulator then outputs $\beta = 1$ to guess that $T = e(g,g)^{a^{q+1}s}$; otherwise, it outputs $\beta = 0$ to indicate that it believes T is a random group element in G_T.

Next, we calculate the lower bound of the probability that the simulator completes without aborting. Without loss of generality we can assume the adversary always makes t queries which are the maximum number of the private key query and signature generation query. For any set of t private key queries on set $S_1,\ldots,S_t$ and t signature queries on set $(\mathrm{Y}_1, M_1),\ldots,(\mathrm{Y}_t, M_t)$ and the forged matrix $\mathbf{M}'$, we have

$$\Pr[\overline{\mathbf{abort}}] = \Pr[(\wedge_{i=1}^{t}\mathrm{Y}^*(S_i) = 0)\wedge(\wedge_{i=1}^{t}K(\mathrm{Y}_i)\not\subseteq K(\mathrm{Y}^*))\wedge(K(\mathrm{Y}')\subseteq K(\mathrm{Y}^*))]$$

Here, $K(\mathrm{Y})$ is defined as the set of all attribute sets that satisfy Y. We can then lower bound the probability of not aborting as follows.

$$\Pr[(\wedge_{i=1}^{t}\mathrm{Y}^*(S_i) = 0)\wedge(\wedge_{i=1}^{t}K(\mathrm{Y}_i)\not\subseteq K(\mathrm{Y}^*))\wedge(K(\mathrm{Y}')\subseteq K(\mathrm{Y}^*))]$$

$$= (1-\Pr[\vee_{i=1}^{t}\mathrm{Y}^*(S_i) = 1])\cdot(1-\Pr[\vee_{i=1}^{t}K(\mathrm{Y}_i)\subseteq \mathrm{Y}^*])\cdot\Pr[K(\mathrm{Y}')\subseteq K(\mathrm{Y}^*)]$$

$$\geq (1-\sum_{i=1}^{t}\Pr[\mathrm{Y}^*(S_i) = 1])\cdot(1-\sum_{i=1}^{t}\Pr[K(\mathrm{Y}_i)\subseteq \mathrm{Y}^*])\cdot\Pr[K(\mathrm{Y}')\subseteq K(\mathrm{Y}^*)]$$

$$= (1-\frac{t}{2^{U-k}})\cdot(1-\frac{t}{2^{U-k}})\cdot\frac{1}{2^{U-k}} \qquad (1.4)$$

Equations 1.4 comes from the fact that,

$$\Pr[\mathrm{Y}^*(S_i) = 1] = \Pr[K(\mathrm{Y}_i)\subseteq K(\mathrm{Y}^*)] = \Pr[K(\mathrm{Y}')\subseteq K(\mathrm{Y}^*)] = \frac{1}{2^{U-k}}.$$

We can optimize the last equation by setting $k = \lfloor U - \log_2 3t \rfloor$ (as we did in the simulation), where t is the maximum number of private key queries and signature generation queries. Solving for this gives us a lower bound $\lambda = (1-\frac{t}{2^{U-\lfloor U-\log_2 3t\rfloor}})^2 \cdot \frac{1}{2^{U-\lfloor U-\log_2 3t\rfloor}}$. Suppose the adversary succeeds with probability ò after q

private key queries and signature generation queries, and this probability is independent of the random choices made by the simulator, we conclude that the simulator succeeds with probability,

$$\tilde{\delta} = \Pr[\beta = 1 \mid \overline{\mathbf{abort}}]\Pr[\overline{\mathbf{abort}}] = \delta \Pr[\overline{\mathbf{abort}}] \geq (1 - \frac{t}{2^{U - \lfloor U - \log_2 3t \rfloor}})^2 \frac{1}{2^{U - \lfloor U - \log_2 3t \rfloor}} \delta.$$

CONCLUSION

We have presented an efficient and fully secure attribute-based signature system that is expressive and provably secure under decisional q-parallel BDHE assumption (Waters, 2011) in the standard model. We have proved that our scheme is (adaptive-predicate) unforgeable against adaptively chosen message attack and perfectly private in the standard model. Our method of embedding a monotone span program into the public parameters allowed us to create clean, modular proof of security. The new construction is most efficient ABS scheme in the standard model comparing with the state-of-the-art (Escala; Herranz; Morillo, 2011; Maji; Prabhakaran; Rosulek, 2011; Okamoto; Takashima, 2011) construction.

ACKNOWEDGEMENTS

The authors thank anonymous reviewers for their valuable comments. This work was supported in part by the National Natural Science Foundation of China under Grant Nos. 60972034, 60970110, 61033014, and 61161140320.

REFERENCES

Beimel, A.. (1996). “Secure schemes for secret sharing and key distribution.” PhD thesis, Israel Institute of Technology, Technion, Haiifa, Israel, 1996.

Boneh, D and Franklin, M.. (2003). “Identity-based encryption from the weil pairing.” SIAM J. Comput., 32:586–615, March 2003.

Boyen, X. (2007). “Mesh signatures.” In Advances in Cryptology—EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, pages 210–227. Berlin: Springer-Verlag, 2007.

Chaum, D. and Van Heyst, E. (1991). “Group signatures.” In Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques, EUROCRYPT’91, pages 257–265, Berlin, Heidelberg, 1991. Springer-Verlag.

Escala, A., Herranz, J. and Morillo, P. (2011). “Revocable attribute-based signatures with adaptive security in the standard model.” In Advances in Cryptology—Africacrypt 2011, volume 6737 of Lecture Notes in Computer Science, pages 224–241. Berlin: Springer-Verlag, 2011.

Groth, J. and Sahai, A. (2008). “Efficient non-interactive proof systems for bilinear groups.” In Advances in Cryptology - EUROCRYPT 2008, volume 4965 of Lecture Notes in Computer Science, pages 415–432. Berlin: Springer-Verlag, 2008.

Khader, D. (2007a). “Attribute based group signature with revocation.” Cryptology ePrint Archive, Report 2007/241, 2007.

Khader, D. (2007b). “Attribute based group signatures.” Cryptology ePrint Archive, Report 2007/159, 2007.

Lewko, A. and Waters, B. (2011). “Decentralizing attribute-based encryption.” In Advances in Cryptology-EUROCRYPT 2011, volume 6632 of Lecture Notes in Computer Science, pages 568–588. Berlin: Springer-Verlag, 2011.

Li, J., Au, M.H., Susilo, W., Xie,D. and Ren, K. (2010). “Attribute-based signature and its applications.” In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ASIACCS ’10, pages 60–69, New York, NY, USA, 2010. ACM.

Li, J. and Kim, K. (2007). “Attribute-based ring signatures.” In Cryptology ePrint Archive, Report 2008/394 2007. To appear in Journal of Information Sciences.

Li, J. and Kim, K. (2010). “Hidden attribute-based signatures without anonymity revocation.” Information Sciences, 180(9):1681 – 1689, 2010.

Maji, H., Prabhakaran, M., and Rosulek, M. (2008). “Attribute-based signatures: Achieving attribute-privacy and collusion-resistance.” Cryptology ePrint Archive, Report 2008/328, 2008.

Maji,H., Prabhakaran, M. and Rosulek, M. (2011). “Attribute-based signatures.” In A. Kiayias, editor, Topics in Cryptology - CT-RSA 2011, volume 6558 of Lecture Notes in Computer Science, pages 376–392. Springer Berlin / Heidelberg, 2011.

Okamoto, T. and Takashima, K. (2011). “Efficient attribute-based signatures for non-monotone predicates in the standard model.” In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, Public Key Cryptography - PKC 2011, volume 6571 of Lecture Notes in Computer Science, pages 35–52. Springer Berlin / Heidelberg, 2011.

Rivest, R., Shamir, A. and Tauman, Y. (2001). “How to leak a secret.” In C. Boyd, editor, Advances in Cryptology - ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 552–565. Springer Berlin / Heidelberg, 2001.

Shahandashti, S. and Safavi-Naini, R. (2009). Threshold attribute-based signatures and their application to anonymous credential systems. In B. Preneel, editor, Progress in Cryptology - AFRICACRYPT 2009, volume 5580 of Lecture Notes in Computer Science, pages 198–216. Springer Berlin / Heidelberg, 2009.

Shanqing, G and Yingpei, Z. (2008). Attribute-based signature scheme. In Proceedings of the 2008 International Conference on Information Security and Assurance (ISA 2008), pages 509–511, Washington, DC, USA, 2008. IEEE Computer Society.

Waters, B. (2011). “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization.” In D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, editors, Public Key Cryptography - PKC 2011, volume 6571 of Lecture Notes in Computer Science, pages 53–70. Springer Berlin / Heidelberg, 2011.

Yang,P., Cao, Z. and Dong,X. (2011). “Fuzzy identity based signature with applications to biometric authentication.” Computers & Electrical Engineering, 37(4):532 – 540, 2011.