A New Construction of Fuzzy Identity Based Signature Scheme

Chang-Ji Wang, *Member, KIMICS*

Abstract—Sahai and Waters first introduced the concept of Fuzzy Identity Based Encryption (FIBE) to provide an error-tolerance property for Identity Based Encryption (IBE) in 2005. Yang et al. extended this idea and introduced the concept of Fuzzy Identity Based Signature (FIBS) in 2008, and constructed a FIBS scheme based on Sahai and Waters's FIBE scheme. In this paper, we further formalize the notion and security model of FIBS scheme and propose a new construction of FIBS scheme based on bilinear pairing. The proposed FIBS scheme not only provide shorter public parameters, private key and signature, but also have useful structures which result in more efficient key extraction, signing and verification than that of Yang et al.'s FIBS scheme.

Index Terms—Bilinear Pairings, Fuzzy Identity Based Encryption, Fuzzy Identity Based Signature, Secret Sharing Scheme.

I. INTRODUCTION

Shamir [1] first proposed the concept of Identity Based Cryptography (IBC), in which the public key of an entity can be easily computed from his identity information (e.g. an e-mail address, a telephone number, etc.), and the private key of an entity was generated from his identity information and a master key of a trusted third party called a Private Key Generator (PKG). This eliminates the need for certificates as used in a traditional public key infrastructure.

Shamir [1] also constructed the first Identity Based Signature (IBS) scheme based on the RSA algorithm and presented an open problem to provide an Identity Based Encryption (IBE) scheme. After seventeen years, Boneh and Franklin [2] proposed the first practical and secure IBE scheme using bilinear maps. Since then, many IBE and IBS schemes based on the bilinear pairing were presented.

However, a unique string identifier does not necessarily exist for each person, such as Email address or IP address can be easily modified, name can be duplicated. Instead, people are more often identified by their attributes. To fulfill this task, Sahai and Waters [3] first introduced the concept of Fuzzy Identity Based Encryption (FIBE). In a FIBE scheme, a descriptive set of attributes is used to encrypt a message, and decryption is performed using a secret key that corresponds to the set of attributes. In contrast to regular public key encryptions, we want to allow a certain tolerance in the key. That means that when the set of attributes used for encryption does not completely match the set of attributes that correspond to the secret key, decryption is still possible. However when the match is lower than a certain threshold, decryption should not be possible anymore.

FIBE gives rise to two interesting new applications. The first is that we can use user's biometrics as identities in IBE system. In existing IBE system, we can not use biometrics as identity directly since biometric measurements are noisy. However, this problem has been dealt with satisfactorily because of the error-tolerance property of Fuzzy-IBE. We can view a user's biometric, for example an iris scan, as that user's identity described by several attributes and then encrypt to the user using their biometric identity. The user with the private key (derived from a measurement of a biometric) can decrypt the ciphertext encrypted with a slightly different measurement of the same biometric. Some FIBE schemes are published since the work of Sahai and Waters, such as [4-8].

Secondly, FIBE can be used for an application that called "attribute based encryption". In this application, sender can encrypt a document to all users that have a certain set of attributes, without exact knowledge of the receiver set. For example, a teacher might wish to encrypt a document to all of students are enrolled in "network security" course in 2008. In this case it

Manuscript received November 8, 2008; revised February 15, 2009.Chang-Ji Wang is with the Department of Computer Science, Guangdong Province Information Security Key Laboratory, Sun Yat-sen University, Guangzhou, 510275, China (Tel: +86-20-84110087, Fax:+86-20-84113673,Email: isswchj@mail.sysu.edu.cn)

would encrypt to the identity {"student", "network security", "2008"}. Any user who has an identity that contains all of these attributes could decrypt the document. The advantage to using attribute based encryption is that the document can be stored on a simple untrusted storage server instead of relying on trusted server to perform authentication checks before delivering a document. Recently, the research of attribute based encryption has become a new hotpot in the field of public key cryptography. We refer the reader to literatures [9-11] for more details.

Yang et al. [12] first extended FIBE idea to introduce the concept of Fuzzy Identity Based Signature (FIBS). A FIBS 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 certain distance judged by some metric. Fuzzy IBS can be directly applied to identity based signature system that uses biometric identities. Yang et al. [12] also constructed a FIBS scheme based on Sahai and Waters's FIBE scheme. In this paper, we further formalize the notion and security model of FIBS scheme and construct a new FIBS scheme based on bilinear pairing, which is more efficient than Yang et al.'s FIBS scheme. The proposed FIBS scheme is proved to be existentially unforgeable under a chosen message attack and selective fuzzy identity attack under Computational Bilinear Diffie-Hellman assumption in the random oracle model.

The rest of the paper is organized as follows. In Section 2 we introduce some preliminary works. In Section 3 we formally define a FIBS scheme including the security model. We follow with a description of our new construction of FIBS scheme in Section 4, and analysis of efficiency and security of the proposed FIBS construction in Section 5. Finally, we conclude in Section 6.

II. PRELIMINARIES

In this section, we briefly review some concepts on bilinear pairings and some related mathematical problems.

A. Bilinear Pairing and Related Assumptions

Let G_1 and G_2 be two cyclic groups of the same prime order q. We use the notation $x \in_R E$ to mean that x is chosen randomly from the set E. The bilinear pairing is a map $e: G_1 \times G_1 \to G_2$, which satisfies the following properties:

- *Bilinear*: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.
- *Non-degenerate*: If P is a generator of G_1, then $e(P, P)$ is a generator of G_2. In other words, $e(P, P) \neq 1_{G_2}$.
- *Computable*: There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

Bilinear Diffie-Hellman (BDH) Assumption: For $a, b, c \in_R Z_q^*$, given P, aP, bP, cP and a bilinear pairing $e: G_1 \times G_1 \to G_2$, to compute $e(P, P)^{abc}$ is hard.

Computational Bilinear Diffie-Hellman (CBDH) Assumption: For $a, b, c, r \in_R Z_q^*$, given a bilinear pairing $e: G_1 \times G_1 \to G_2$, to distinguish between the distributions $\langle P, aP, bP, cP, e(P, P)^{abc} \rangle$ and $\langle P, aP, bP, cP, e(P, P)^{r} \rangle$ is hard.

B. Secret Sharing Schemes

Let t, n be positive integers, $t < n$. A (t, n)-threshold scheme is a method of sharing a secret $s \in Z_q$, which is chosen by the dealer (denoted by D), among a set of n participants (denoted by $\mathbf{P} = \{P_1, \ldots, P_n\}$, $D \notin \mathbf{P}$, in such a way that any t participants can compute the value of s, but no group of $t-1$ participants can do so.

Shamir [8] proposed a threshold secret sharing scheme by using polynomial interpolation, which is described as follows.

Let $s \in Z_q$ be the secret to be shared, D chooses a polynomial $f(x) \in Z_q[x]$ of degree $t-1$ with $f(0) = s$, i.e. $f(x) = s + \sum_{j=1}^{t-1} a_j x^j \mod q$.

If we assign every participant P_i with a unique element $\alpha_i \in_R Z_q^*$. Then D computes $s_i = f(\alpha_i)$ for $1 \le i \le n$ and gives the secret share s_i to P_i through a private channel.

Now a group $\mathbf{B} \subseteq \mathbf{P}$ of at least t participants, i.e. $|\mathbf{B}| \geq t$, can recover the secret s by using the following formula.

$$f(x) = \sum_{P_i \in B} f(\alpha_i)\Delta_{\alpha_i,B}(x) = \sum_{P_i \in B} s_i \Delta_{\alpha_i,B}(x).$$

where $\Delta_{\alpha_i,B}(x) = \prod_{\substack{P_i \in B \\ i \neq k}} \frac{x-\alpha_k}{\alpha_i - \alpha_k} \bmod q$.

On the other hand, it can be proved that if the subset $\mathbf{S} \subseteq \mathbf{P}$ such that $|\mathbf{S}| < t$ could not get any information about the polynomial $f(x)$.

III. SYNTAX AND SECURITY MODEL OF FIBS

A. Syntax of FIBS

A FIBS scheme can be described as a collection of the following four algorithms:

Setup: The Setup algorithm is a probabilistic algorithm that takes as input a security parameter k. It generates the master key mk and public parameters $params$ which contains an error tolerance parameter d. Note that $params$ is made public, while mk will be known only to PKG.

Extract: The Private Key Extraction algorithm is a probabilistic algorithm that takes as input the public parameters $params$, master key mk and an attribute set ω for an identity ID. It outputs a private key for the identity ID, denoted by S_{ID}.

Sign: The signing algorithm is a probabilistic algorithm that takes as input the public parameters $params$, private key S_{ID} for an identity ID associated with an attribute ω and a message m. It outputs the signature σ.

Verify: The verification algorithm is a deterministic algorithm that takes as input the public parameters $params$, an attribute set ω' such that $|\omega \cap \omega'| \geq d$, message m and corresponding signature σ. It outputs *accept* if σ is a valid signature on m for the attribute set ω' and outputs *reject* otherwise.

B. Security Models for FIBS

In this section we define our existential unforgeability under an adaptive chosen message attack and Selective Fuzzy ID attack for FIBS (EUF-sFID-CMA). It is very similar to the existential unforgeability under an adaptive chosen message attack and Selective ID attack for IBS (EUF-sID-CMA) with the exception that the adversary is only allowed to query for secret keys for attribute sets which have less than d overlap with the attribute set for the target identity. EUF-sFID-CMA is defined using the following game between a challenger C and an adversary A.

Init: A outputs an identity ID^* (associated with attribute set as ω) where it wishes to be challenged.

Setup. C takes a security parameter k, and runs the setup phase of FIBS scheme. A is given the resulting public parameters $params$ but the master key mk is kept by C.

Queries. A adaptively makes a number of different queries $q_1, q_2, \ldots, q_m$ to C, where query q_i is one of:

- *Extract Queries*: A issues private key queries for identity $ID_i \neq ID^*$ (associated with attribute set as γ_i). In response, C runs the Extract algorithm on input attribute set γ_i for identity ID_i to obtain the corresponding private key S_{ID_i} and gives it to A. The only restrictions is $|\omega \cap \gamma_i| < d$.
- *Signature Queries*: A can ask for the signature of any attribute set γ_i on any message $m_{i,j}$. In response, C first runs **Extract** to obtain the private key S_{ID_i} corresponding to the identity ID_i, and then runs **Sign** to obtain a signature σ_i corresponding to the identity ID_i, which is forwarded to A.

Output. Finally A outputs a pair $(\overline{\omega}, \overline{m}, \overline{\sigma})$. If $\overline{\sigma}$ is a valid signature of $(\overline{\omega}, \overline{m})$ according to **Verify**, and A has neither made an **Extract** Query on $\overline{\omega}$ nor a **Sign** Query on $(S_{\overline{ID}}, \overline{m})$, then A wins.

We define Adv_A to be the probability that A wins the above game, taken over the coin tosses made by A and C.

Definition 1. An adversary A is said to be a $(q_e, q_s, t, \varepsilon)$-forger of a FIBS scheme if A has advantage at least ε in the above game, runs in time

at most t, and makes at most q_e and q_s **Extract** and Sign queries, respectively. A FIBS scheme is said to be $(q_e, q_s, t, \varepsilon)$ -secure if no $(q_e, q_s, t, \varepsilon)$ -forger exists.

IV. NEW CONSTRUCTION OF FIBS SCHEME

Without loss of generality, we assume that an identity is a set of n different elements in Z_q^*. For example, each of n strings of arbitrary length with an index $i \in Z$ can be hashed using some collision-resistant hash function whose range is Z_q^*. The proposed FIBS scheme is described as follows:

Setup: PKG chooses groups G_1 and G_2 of prime order q such that a bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$ can be constructed, and P is a generator of G_1. Then PKG chooses $s \in_R Z_q^*$, computes $P_{pub} = sP$. PKG also choose two hash functions $H: \{0,1\}^* \rightarrow Z_q^*$ and $H_1: \{0,1\}^* \times G_1 \rightarrow Z_q^*$, which are assumed to be the random oracles. Next, PKG defines the error tolerance parameter d. Finally, PKG outputs public parameters $params = (G_1, G_2, q, e, P, P_{pub}, d, H, H_1)$ and keeps master key $mk = s$ secret.

Extract: For ID = $(\omega_1, \omega_2, \ldots, \omega_n)$, PKG picks a $d-1$ degree polynomial $p(x) \in_R Z_q[x]$ such that $p(0) = s$ and computes the corresponding private key components, $D_i = p(H(\omega_i))P$ for $i = 1,2,\ldots,n$ and sends $S_{ID} = (D_1, D_2, \ldots, D_n)$ to the user with identity ID.

The user can validate the correctness of the private key components by choosing an arbitrary d-element subset $\mathbf{S}$ of ID and checking the following equation.

$$\prod_{\omega_i \in S} e(D_i, P)^{\Delta_{H(\omega_i),S}(0)} = e(P, P_{pub}).$$

Sign: Given an identity ID = $(\omega_1, \omega_2, \ldots, \omega_n)$ and a message m, the signing procedure is performed as follows.

- The signer chooses $r \in_R Z_q^*$, computes $U = rP$ and $h = H_1(m, U)$.
- Chooses a $d-1$ degree polynomial $f(x) \in_R Z_q[x]$ such that $f(0) = r$.
- Computes $V_i = f(H(\omega_i))P_{pub} + hD_i$ for $i = 1,2,\ldots,n$.

The resulting signature is $\sigma = (\mathrm{ID}, U, V_i)$.

Verify: To verify a signature $\sigma = (\mathrm{ID}, U, V_i)$ against an identity ID', where $|\mathrm{ID} \cap \mathrm{ID}'| \geq d$, and a message m, verifier chooses an arbitrary d-element subset $\mathbf{S}$ of ID $\cap$ ID', computes $h = H_1(m, U)$ and verifies that

$$\begin{aligned}
&\prod_{\omega_i \in S} e(V_i, P)^{\Delta_{H(\omega_i),S}(0)} \\
&= \prod_{\omega_i \in S} e(f(H(\omega_i))P_{pub} + hD_i, P)^{\Delta_{H(\omega_i),S}(0)} \\
&= \prod_{\omega_i \in S} e(P_{pub}, P)^{f(H(\omega_i))\Delta_{H(\omega_i),S}(0)} \prod_{\omega_i \in S} e(hP, P)^{p(H(\omega_i))\Delta_{H(\omega_i),S}(0)} \\
&= e(P_{pub}, P)^{\sum_{\omega_i \in S} f(H(\omega_i))\Delta_{H(\omega_i),S}(0)} \; e(hP, P)^{\sum_{\omega_i \in S} p(H(\omega_i))\Delta_{H(\omega_i),S}(0)} \\
&= e(P_{pub}, U)e(P, hP_{pub}) \\
&= e(P_{pub}, U + hP).
\end{aligned}$$

V. EFFICIENCY AND SECURITY ANALYSIS

A. Efficiency Analysis

The number of group elements in the public parameters $params$ does not grow linearly with the number of attributes in the system, while it does in Yang et al.'s FIBS scheme. The number of group elements that compose a signer's private key and resulting signature σ grows linearly with the number of attributes associated with the signer.

The number of scalar multiplications in the group G_1 for a signer to sign a message will be linear in the number of elements in the attribute set ω for the signer. The procedure of signing does not need any bilinear pairing computations. The cost of verification will be dominated by $d+1$ bilinear pairing computations.

In table 1 below, we compare the proposed FIBS scheme with Yang et al.'s FIBS scheme [12] in terms of the length of the public parameters, private key and

signature, and the number of the dominant operations required in Extract, Sign and Verify. In table we use pms, and pcs as abbreviations for scalar multiplications in G_1 and computations of bilinear pairing respectively. We also use n to denote the number of attributes for ID and m to denote the length of message to be signed.

Table 1 Comparison of FIBS schemes

	Yang et al. scheme [12]	The proposed scheme
Length of public parameters	$(n+m+4)\|G_1\|+\|G_2\|$	$2\|G_1\|$
Length of private key	$2n\|G_1\|$	$n\|G_1\|$
Length of Signature	$3n\|G_1\|$	$(n+1)\|G_1\|$
Extract	$3n$ (pms)	n (pms)
Sign	$(m+n)$ (pms)	$(n+1)$ (pms)
Verify	$3d$ (pms)+$3d$ (pcs)	d (pms)+ d (pcs)

B. Security Analysis

In the proposed FIBS scheme, a user's private key is constructed as a set of private key components, one for each attribute in the user's identity. We use Shamir's method of secret sharing to distribute shares of a master secret in the coefficients of the user's private key components [13]. Shamir's secret sharing within coefficients gives the proposed FIBS scheme the crucial property of being error-tolerant since only a subset of the private key components are needed to verify a pair of message and signature.

Additionally, the proposed FIBS scheme is resistant to collusion attacks. Different users have their private key components generated with different random polynomials. If multiple users collude they will be unable to combine their private key components in any useful way.

Pointcheval and Stern [14] presented a notion of generic signature scheme which, given the input message m, produces a triple (σ_1, h, σ_2), where σ_1 randomly takes its values in a large set, h is the hash value of (m, σ_1) and σ_2 only depends on σ_1, the message m and h. They introduce the Forking Lemma, which is based on a reduction technique that they call *oracle replay attack*.

Gu et al. [15] successfully extends the Forking Lemma for ID-based signature schemes. Using the result of [15], a large class of ID-based signature schemes, which called ID-based generic digital signature schemes, can be proved to be secure easily in the random oracle model. We can use the same techniques in [15] to extend the Forking Lemma for FIBS schemes, and prove that the proposed FIBS scheme is existentially unforgeable under a chosen message attack and selective fuzzy identity attack under CBDH assumption in the random oracle model. We omit the detailed proof here due to space limitation.

VI. CONCLUSIONS

In this paper, we introduced the concept of FIDS scheme, where user's identity is viewed as a set of descriptive attributes. FIBS allows for error-tolerance between the attribute set used to sign a message and the attribute set used to verify the signature. We first gave the definition and security model of FIBS scheme, and then we presented a new efficient and provable secure FIBS scheme. We will carry on our research on efficient and secure FIBS scheme with special properties, such as Fuzzy Identity Based proxy signature and FIBS scheme in the standard model.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China under Grant (No.60503005).

REFERENCES

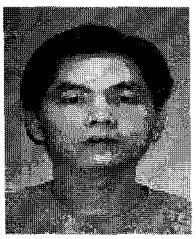
[1] A. Shamir, et al. Identity-based Cryptosystems and Signature Schemes, In Advances in Cryptology-CRYPTO'84, LNCS 196, Springer-Verlag, 1985, pp.47–53.

[2] D. Boneh and M.K. Franklin. Identity-based encryption from the Weil pairing, In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Springer-Verlag, 2001, pp. 213–229.

[3] A. Sahai and B. Waters. Fuzzy identity-based encryption, In EUROCRYPT 2005, LNCS 3494, Springer-Verlag, 2005, pp.457–473.

[4] J. Baek et al. New constructions of fuzzy identity based encryption, In Proc. of the 2nd ACM Symposium on Information, Computer and Communications Security, 2007, pp. 368–370.

[5] G. Ateniese, M. Blanton and J. Kirsch. Secret Handshakes with Dynamic and Fuzzy Matching, Network and Distributed System Security Symposium 2007, pp. 159-177.
[6] L.M. Fang. Full Security: Fuzzy Identity Based Encryption, Cryptology ePrint Archive, Report /2008/307, 2008, http://eprint.iacr.org/.
[7] L.M. Fang, et al. Chosen-Ciphertext Secure Multi-authority Fuzzy Identity-Based Key Encapsulation without ROM, 2008 International Conference on Computational Intelligence and Security, 2008, pp. 326-330.
[8] Jun F. et al. `A Fuzzy ID-Based Encryption Efficient When Error Rate Is Low', INDOCRYPT 2008, LNCS 5365, Springer, 2008, pp. 116-129.
[9] V. Goyal, et al. Attribute-based encryption for fine-grained access control of encrypted data, In Proc. Of CCS, 2006, pp. 221-238.
[10] R. Ostrovsky, A. Sahai and B. Waters. Attribute-based encryption with non-monotonic access structures, In Proc. ACM Conference on Computer and Communications Security (CCS), 2007, pp. 195-203.
[11] J. Bethencourt, A. Sahai and B. Waters. Ciphertext-policy attribute-based encryption, In: Proc. IEEE Symposium on Security and Privacy, 2007, pp. 321-334.
[12] P.Y. Yang, et al. Fuzzy Identity Based Signature, Available: http://eprint.iacr.org/2008/002.pdf 2008.
[13] A. Shamir, et al. How to share a secret, Communications of the ACM, 1979, pp.612-613.
[14] D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures, Journal of Cryptology, 2000, 13(3), pp.361-396.
[15] C.X. Gu, et al. Forking Lemma and the Security Proofs for a Class of ID-Based Signatures, Journal of Software, vol.18, No.4, 2007, pp.1007-1014.



Chang-Ji Wang
received the M.S. degree in Applied Mathematics from Sun Yat-sen University in 1997, and received the Ph.d. degree in Applied Mathematics from the Graduate School of Chinese Academy of Sciences. During 2002-2004, he stayed in network research center of Tsinghua University for postdoctoral research. He now is a teacher at the department of computer science in Sun Yat-sen University.