Available online at www.sciencedirect.com
ScienceDirect
Progress in Natural Science 19 (2009) 1021–1025
Progress in Natural Science
www.elsevier.com/locate/pnsc

A new threshold signature scheme based on fuzzy biometric identity

Yongquan Cai *, Ke Zhang

College of Computer Science and Technology, Beijing University of Technology, No. 100 Pinleyuan chaoyang, Beijing 100124, China

Received 14 June 2008; received in revised form 15 January 2009; accepted 6 February 2009

Abstract

The focus of this paper is to present the first threshold signature scheme based on biometric identity, which is acquired from a recently proposed fuzzy identities-based encryption scheme. An important feature of this scheme, which is different from other previous ID-based threshold signature schemes, is that it can be applied to situations using not only average personal attributes in social contact but also people's noisy biometric inputs as identities. The security of our scheme in the selective-ID model reduces the limit in the hardness of the Decisional BDH Assumption.

Keywords: Biometric; Threshold signature; Identity; Fuzzy

1. Introduction

The concept of digital signature, first introduced by Diffie and Hellman [1] in 1976, allows a signer with a secret key to sign a message and anyone with a public key to verify the signature. In 1984, the notion of the ID-based cryptosystem was put forward in the pioneering paper of Shamir [2]. The main purpose of such systems is that any user may use the identity information, such as full name, e-mail address or telephone number, as his/her public key.

In a (t,n) threshold signature scheme, it is only when the number of participators is equal to or more than a threshold value t that a signature can be generated. Anyone can verify the authenticity of the message with a public key. Many such schemes [3,4] based on identities have been proposed.

However, all the previous schemes used people's attributes in social contact as identities, and viewed the identities as alphabetic or bit strings. The chief drawback of such schemes is that they did not allow human biometric characteristics to be used as identities; for example, speech-sounds and iris scans that are very special attributes but will easily cause aberration when sampled. What is more, in the (t,n) threshold signature schemes [1,5,6], the values of t are fixed and they cannot be applied to some situations.

Since the value of a biometric sample is often disturbed by many noises and has distortion when sampled, we will not be able to utilize previous common identity-based schemes.

In 2005, Sahai and Waters [7] proposed a new concept "Fuzzy ID-Based Encryption". The identities in his paper are viewed as the attributes set describing the characteristics of identities. If and only if there is some intersection between the encryption identity ω' and the decryption identity ω, a user holding the private key of ω would be able to decrypt the cipher text encrypted by ω'.

Based on the scheme presented by Sahai, a new ID-based signature scheme is constructed in our article. Combining of this signature scheme and Zhang's distribution key generation protocol [8], we propose the first threshold signature scheme based on fuzzy biometric identity without a trusted dealer.

Our threshold signature scheme has features of strong error-tolerance and flexibility. Its application is much more extensive.

* Corresponding author. Tel.: +86 1067392370.
E-mail address: cyq@bjut.edu.cn (Y. Cai).

1002-0071/$ - see front matter
doi:10.1016/j.pnsc.2009.02.001

In the selective-ID model, its security is reduced to the hardness of the decisional BDH assumption.

There are two main features of our scheme:

1. Using biometric attributes as identities. Some values of biometric attributes with noises can be used as private keys to partially sign a message and generate a valid signature, even if the values of biometric samples attained at several separate times are a little different from each other.
2. Viewing real people's names as identities, just like common ID-based schemes. In this situation, our scheme will show adaptability (flexibility). It can effectively resist intruders and forgers under the circumstances that $t-1$ participants conclude.

The identities in this article can be certain biometric attributes of human beings, or any of their accurate code names.

2. Preliminaries

2.1. Bilinear pairing

A bilinear pairing e is defined over two multiplicative groups of the same order p. The two groups are denoted as G_1 and G_2, respectively. Let g be a generator of G_1. The bilinear pairing is a map from G_1 to G_2, namely, $e{:}G_1 \times G_1 \to G_2$. It has the following properties:

Bilinear: $e(u^a, v^b) = e(u,v)^{ab}$, where $u, v \in G_1$ and $a, b \in G_2$.

Non-degenerate: $e(g,g) \neq 1$.

These properties imply that for any $a, b, c \in G_1$, we have $e(a, b \cdot c) = e(a,b) \cdot e(a,c)$.

2.2. Decisional bilinear Diffie–Hellman (DBDH) assumption

Suppose a challenger chooses $a, b, c \in_R \mathbb{Z}_p$ at random. The DBDH assumption is that no polynomial-time adversary is able to distinguish the tuple $(g^a, g^b, g^c, e(g,g)^{abc})$ from the tuple $(g^a, g^b, g^c, e(g,g)^z)$ with a negligible advantage.

3. Sahai's encryption scheme

We define the Lagrange coefficient $\Delta_{i,N}(x)$ for $i \in \mathbb{Z}_p$ and $N \subseteq \mathbb{Z}_p$

$$\Delta_{i,N}(x) = \prod_{\substack{j \in N \\ j \neq i}} \frac{x-j}{i-j}$$

Setup: Choose $g_1 = g^y, g_2, t_1, t_2, \ldots, t_{n+1} \in G_1$, and we define a function

$$T(x) = g_2^{x^n} \cdot \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$$

The public keys are $g_1, g_2, t_1, t_2, \ldots, t_{n+1}$, and the private key is y.

Key generation: Randomly select a $d-1$ degree polynomial q such that $q(0) = y$. The private key contains two sets $\{D_i\}_{i \in \omega}$ and $\{d_i\}_{i \in \omega}$, in which $D_i = g_2^{q(i)} \cdot T(i)^{r_i}$ and $d_i = g^{r_i}$.

Encryption: Given an identity ω' and a message m, the encryption is $E = (\omega', E' = m \cdot e(g_1, g_2)^s, E'' = g^s, \{E_i = T(i)^s\}_{i \in \omega'})$.

Decryption: $M = E' \cdot \prod_{i \in S} \left(\frac{e(d_i, E_i)}{e(D_i, E'')} \right)^{\Delta_{i,S}(0)}$, where S is a subset of $\omega \cap \omega'$, and $|S| = d$.

4. A new signature derived from Sahai's encryption scheme

Now, we consider designing a new signature scheme based on Sahai's encryption scheme. The new scheme consists of three algorithms: the parameters extraction algorithm (PE), the signature generation algorithm (SG) and the signature verification algorithm (SV).

PE: The definition of G_1 and G_2 is the same as that in Section 2.1. Choose $g_1 = g^s, g_2 \in G_1$ and define $T = g_2^n \cdot g^h$ for simplicity. Define a one-way collision-free hash function h as $\{0,1\}^* \to G_1^*$.

Given a message m, first select $x \in_R \mathbb{Z}_p$, and then compute $H = h(m), Y = e(H \cdot g_2, g^s)^x \in G_2$.

The public key is published as Y and the private key is x.

SG: Supposing that the private key is x and the given message is m, a signer randomly selects $\alpha \in_R \mathbb{Z}_p$, and calculates

$$Q = e(H^s, g)^x, U = g_2^x \cdot T^\alpha, V = g^{s\alpha}$$

The signature is $\sigma = (Q, U, V) \in (G_2 \times G_1^2)$.

SV: Anyone who has a signature σ can verify it with the public key $Y \in G_2$:

$$Q \cdot e(g_1, U) = e(V, T) \cdot Y. \tag{1}$$

Theorem 1. *Any signature σ satisfying Eq. (1) can be regarded as a valid signature, otherwise it cannot.*

Proof of Theorem 1.

$$Q \cdot e(g_1, U) = e(H^s, g)^x \cdot e\left(g_1, g_2^x \cdot T^\alpha\right) = e\left(g_1, H^x \cdot g_2^x \cdot T^\alpha\right)$$

$$e(V, T) \cdot Y = e(g^{s\alpha}, T) \cdot e(H \cdot g_2, g^s)^x = e\left(g_1, T^\alpha \cdot H^x \cdot g_2^x\right)$$

Therefore, we have $Q \cdot e(g_1, U) = e(V, T) \cdot Y$. □

5. Our threshold signature scheme

5.1. Distributed key generation (DKG) protocol

DKG is an important ingredient of a threshold signature system. Our threshold signature scheme is also based on a DKG protocol [8]. Participators can generate public

keys and private keys by cooperation without any trusted third parties.

1. Suppose that the players group is A_1, in which every player p_i randomly selects $a_{ik} \in_R \mathbb{Z}_p (k = 1, 2, \ldots, t)$, and $|A_1| = n_1$. Thus p_i can choose a t degree polynomial $f_i(x) = \sum_{k=0}^{t} a_{ik} \cdot x^k \in \mathbb{Z}_p[x]$ such that $a_{i0} = f_i(0)$.
2. For a message m, p_i computes $s_{ij} = f_i(j)$ and $H = h(m)$. Then it broadcasts $A_{ik} = e(H \cdot g_2, g^s)^{a_{ik}} (\mathrm{mod}\, p)$ and $y_{ij} = e(H \cdot g_2, g^s)^{s_{ij}} (\mathrm{mod}\, p)$. The secret key x is now defined as $x = \sum_{i \in A_1} a_{i0} (\mathrm{mod}\, q)$, even though it is not explicit.
3. Each player p_j verifies the value broadcast by other players in A_1. Namely, for $i \in A_1$, p_j checks whether $\prod_{k=0}^{t} A_{ik}^{j^k} = y_{ij} (\mathrm{mod}\, p)$.
4. At the end of this phase, every honest player p_i obtains $x_i = \sum_{i \in A_1} s_{ji}$ as his share of the secret key x. Thus the public key of p_i is $C_i = e(H \cdot g_2, g^s)^{x_i}$. Given $A_{ij} (1 \leqslant j \leqslant t + 1)$, A_{i0} can be calculated from the Lagrangian interpolation polynomial.

We are able to resist $l\,(l < n_1)$ dishonest players. As a matter of fact, they can be identified and then be excluded [8].

5.2. Partial signature generation

We assume that A_2 is the set of verifiers for partial signatures such that $|A_2| = n_2, A_1 \cap A_2 = S$ and $|S| \geqslant t$. Each participator p_i randomly chooses $t_1, t_2, \ldots, t_{n+1} \in_R G_1$ for himself, where n is independent of n_1 and n_2. Let N be the set $\{1, \ldots, n+1\}$ and he computes $T(i) = g_2^{t_i} \cdot \prod_{j=1}^{n+1} t_j^{\Delta_{i,N}(i)}$ as his secret value.

For player $p_i \in A_1$, an arbitrary value is selected $r_i \in_R \mathbb{Z}_p$ and calculated

$$\begin{cases} Q_i = e(g^s, H)^{x_i}, \\ R_i = T(i)^{r_i}, \\ U_i = g_2^{x_i} \cdot R_i. \end{cases}$$

The partial signature on message m given by player p_i is $\sigma_i = (Q_i, R_i, U_i)$ and is then broadcast to the set A_2.

Anyone in A_2 can be designated to verify the validity of each partial signature. We assume there is a designated player (DC) in S. After having received the partial signatures, DC verifies every partial signature.

Theorem 2. *A partial signature is accepted if and only if the following equation holds.*

$$Q_i \cdot e(g_1, U_i) = e(g_1, R_i) \cdot C_i \tag{2}$$

Proof

$$\begin{aligned} Q_i \cdot e(g_1, U_i) &= e(g_1, H)^{x_i} \cdot e(g_1, g_2^{x_i} \cdot T(i)^{r_i}) \\ &= e(g_1, H^{x_i} \cdot g_2^{x_i} \cdot T(i)^{r_i}) \\ e(g_1, R_i) \cdot C_i &= e(g_1, T(i)^{r_i}) \cdot e(H \cdot g_2, g_1)^{x_i} \\ &= e(g_1, T(i)^{r_i} \cdot H^{x_i} \cdot g_2^{x_i}) \end{aligned}$$

So we have $Q_i \cdot e(g_1, U_i) = e(g_1, R_i) \cdot C_i$. □

5.3. Threshold signature generation

A DC computes

$$\begin{cases} Q = \prod_{i \in S} Q_i^{\Delta_{i,S}(0)} \\ R = \prod_{i \in S} R_i^{\Delta_{i,S}(0)} \\ U = \prod_{i \in S} U_i^{\Delta_{i,S}(0)} \\ Y = \prod_{i \in S} A_{i0} \end{cases}$$

Then $\sigma = (Q, R, U)$ is the signature on message m.

σ and Y are published so that any public personnel is able to verify the threshold signature σ.

Theorem 3. *A threshold signature is accepted if and only if*

$$Q \cdot e(g_1, U) = e(g_1, R) \cdot Y \tag{3}$$

Proof

$$\begin{aligned} Q &= \prod_{i \in S} Q_i^{\Delta_{i,S}(0)} = \prod_{i \in S} e(g_1, H)^{x_i \cdot \Delta_{i,S}(0)} = e(g_1, H)^{\sum_{i \in S} x_i \cdot \Delta_{i,S}(0)} \\ &= e(g_1, H)^{x} \end{aligned}$$

$$R = \prod_{i \in S} R_i^{\Delta_{i,S}(0)} = \prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)}$$

$$U = \prod_{i \in S} U_i^{\Delta_{i,S}(0)} = \prod_{i \in S} (g_2^{x_i} \cdot T(i)^{r_i})^{\Delta_{i,S}(0)} = g_2^{x} \cdot \left(\prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)} \right)$$

$$\begin{aligned} Y &= \prod_{i \in S} A_{i0} = \prod_{i \in S} e(H \cdot g_2, g_1)^{a_{i0}} = e(H \cdot g_2, g_1)^{\sum_{i \in S} a_{i0}} \\ &= e(H \cdot g_2, g_1)^{x} \end{aligned}$$

So, the left side of Eq. (3) equals

$$\begin{aligned} Q \cdot e(g_1, U) &= e(g_1, H)^{x} \cdot e\left(g_1, g_2^{x} \cdot \left(\prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)} \right) \right) \\ &= e\left(g_1, H^{x} \cdot g_2^{x} \cdot \prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)} \right) \end{aligned} \tag{4}$$

While the right side of Eq. (3) is

$$\begin{aligned} e(g_1, R) \cdot Y &= e\left(g_1, \prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)} \right) \cdot e(H \cdot g_2, g_1)^{x} \\ &= e\left(g_1, g_2^{x} \cdot H^{x} \cdot \prod_{i \in S} T(i)^{r_i \cdot \Delta_{i,S}(0)} \right) \end{aligned} \tag{5}$$

Obviously, expression (4) equals expression (5). Therefore, we have accomplished the proof. □

6. Security analysis

In the phase of DKG, the authentication on every participator is public and reliable. Any malicious participators would be excluded and $t+1$ honest players can reconstruct the secret key x.

Theorem 4. *In the selective-ID model, the security of our scheme reduces to the DBDH assumption.*

Proof. Sahai and Waters [7] have proved in his paper that in the selective-ID model the security of his encryption scheme is reduced to the hardness of the DBDH assumption.

Our proposed threshold signature scheme based on fuzzy biometric identity is a variant of Sahai's encryption scheme.

The decryption in [7] and the verification of Eq. (3) in our scheme almost use the same symbols.

$$e(g_1,H)^x \cdot e\left(g_1, g_2^x \cdot \prod_{i\in S} T(i)^{r_i\cdot\Delta_{i,S}(0)}\right) = e\left(g^s, \prod_{i\in S} T(i)^{r_i\cdot\Delta_{i,S}(0)}\right)\cdot e(g_2H, g^s)^x \quad (6)$$

And the equation in [6] is equivalent to

$$e(g_1,g_2)^s \cdot \prod_{i\in S} e(g^{r_i}, T(i)^s)^{\Delta_{i,S}(0)} = \prod_{i\in S} e\left(g_2^{q(i)}\cdot T(i)^{r_i}, g^s\right)^{\Delta_{i,S}(0)} \quad (7)$$

The accession of H and some variations in Eq. (7) do not compromise the security of Sahai's encryption. Therefore, no adversary can break our scheme in the selective-ID model if the decisional BDH assumption is hard.

No adversaries are able to obtain a player's secret share x_i, nor can they gain the secret key x by the value of Y, because they would encounter discrete Logarithm problems. □

Theorem 5. *No adversaries could possibly deduce a private value r_i or s.*

Given g, g_1, g_2 and m, it is obvious that adversaries will encounter DLP if they try to solve equations $g_1 = g^s$ and $R_i = T(i)^{r_i}$.

On the other hand, neither can they deduce r_i or s by means of an arbitrary number of partial signatures.

One partial signature is represented as $\sigma_i = (Q_i, R_i, U_i)$, and

$$\begin{cases} Q_i = e(g^s, H)^{x_i} \\ R_i = T(i)^{r_i} \\ U_i = g_2^{x_i}\cdot R_i \end{cases}$$

Take Q_i, for example. The value of x_i is not available to the public (see Section 6.3). In addition to s, there are two unknown quantities in Q_i. The adversaries may face not only discrete Logarithm problems but also bilinear pairing inversion problems.

Even though they have the ability to solve the above two problems, owing to the fact that $T(i)$ is set as a private value, it will be almost impossible for them to succeed. The reason is that no matter how many partial signatures are intercepted, the number of unknown quantities in the equations set constituted by $\{Q_{k_1}, Q_{k_2}, \ldots, Q_{k_l}\}$ will be twice as many as that of equations in the equations set.

Therefore, it is unfeasible to deduce r_i or s.

No forgers would be able to fabricate a partial signature σ_i of player p_i.

We assume that a forger randomly selects $T(i)' \in G_1$, and $r_i', s' \in \mathbb{Z}_p$ to forge a $\sigma_i' = (Q_i', R_i', U_i')$. Then the right side expression of Eq. (2) is $e(g^{s'}, T'(i)^{r_i'})\cdot e(H\cdot g_2, g^{s'})^{x_i}$. However, without the knowledge of x_i, his/her fake partial signature will not be accepted according to Eq. (2).

Theorem 6. *Any forger, however, cannot fabricate a threshold signature σ.*

Definition. We say a threshold signature cannot be forged on the condition that at most $t-1$ players in collusion with each other do not have the ability to output a valid signature on a message m which has never been signed before.

Proof of Theorem 6. It is evident that group members in our proposed threshold signature scheme share the group secret key x with a (t,n_1) threshold scheme; therefore, group members less than t cannot conspire to generate a valid signature through the operation of our scheme.

But what if a forger attempts to fabricate a valid signature through analysis of Eq (3)? Now we show that it will not work.

Assume a forger chooses a value for Q. In order to make Eq. (3) hold, the forger has to work out $U = g_2^x \cdot R$.

The problem is now reduced, as shown below:

$$e(g^s, U) = e(g^s, R)\cdot Y\cdot Q^{-1} \Rightarrow e(g^s, g_2^x) = Y\cdot Q^{-1}$$

Given the public key Y and an assumed value of Q, however, it is a DL problem to calculate s and x.

On the other hand, if the forger chooses U first, Q needs to be computed similarly.

$$Q\cdot e(g_1,U) = e(g_1,R)\cdot Y \Rightarrow Q = e(g_1,H^x)$$

Now, the question is the computation of $Q = e(g_1,H^x)$. Again, without the knowledge of x (see Section 6.3), the forger cannot forge a signature in this way either. □

7. Discussion

If all the participators in group A_1 have effective contribution to threshold signature, it would be natural for certain adversaries to breach the players one by one.

In our scheme, though every player can generate his/her partial signature, some (perhaps a large number) players in A_1 have nothing to do with the generation of a threshold signature. The corresponding secret shares are meaningless.

This feature makes the adversaries hesitate when trying to breach a specific participator. Due to the redundancy in the signers group, even though adversaries have attained a few secret shares from A_1, they cannot decide whether the shares are valuable. The size of the number of redundant players in A_1 will surely increase an adversary's computation by a certain degree.

Here, we suppose $|A_1| = n_1$. The "valuable players", whose partial signatures constitute a threshold signature, form the set S, which is determined by both A_1 and A_2 such that $|S| = t$.

An adversary may possibly randomly select t players from A_1. The players selected are defined as a subset K such that $|K| = t$. Therefore, the possibility

$$P\{S = K\} = \frac{t!}{n_1!/(n_1 - t)!} = \left(C_t^{n_1}\right)^{-1}$$

From the property of combinatorics, we know that $P\{S = K\}$ gets its minimum $P_{\min}\{S = K\}$ when $t = \left\lfloor \frac{n_1}{2} \right\rfloor$.

Depending on the practical situation, we can determine the values of t and n_1. For example, ordinary messages need 30% ($t = 0.30n_1$) of all the players to sign, while important ones need at least 75% ($t = 0.75n_1$) players. In addition, each player's prestige, authority and credibility should also be considered.

The design of redundancy affords the scheme better flexibility and better adaptability.

When the identities in our scheme are viewed as biometric attributes, the situation is similar.

8. Conclusion

We have constructed a new signature scheme derived from Sahai's fuzzy ID-based encryption, and have proved its correctness. We have also extended the proposed signature scheme to the first fuzzy biometric ID-based threshold signature scheme, in which the key generation phase does not require a trusted authority and is equipped with cheater detection, which is essential in a distributed system. We have also shown some good properties of our threshold signature scheme as:

Tolerance: A slight difference within a certain error range between several samplings of the same biometric identity is allowed. And some players' noncooperation has no influence on our scheme, if their social names are viewed as identities.

Unforgeability: Compared with other previous schemes, the main contribution of this proposed scheme is that it can be applied to many more fields, which means that we can also use biological specificities whose property values cannot be sampled accurately as identities. This will make the signature generation more believable and more convenient.

Acknowledgment

This work was supported by the National Key Basic Research Program of China (Grant No. 2007CB311106).

References

[1] Diffie W, Hellman M. New directions in cryptography. IEEE IT 1976;22:644–54.
[2] Shamir A. Identity-based cryptosystems and signature schemes. In: Advances in cryptology-crypto'84, LNCS 196; 1985. p. 47–53.
[3] Beak J, Zheng Y. Identity-based threshold signature scheme from the bilinear pairings. In: Proceedings of the of ITCC, vol. 1; 2004. p. 124–8.
[4] Chen X, Zhang F, Konidala DM, et al. New ID-based threshold signature scheme from bilinear pairings. In: Proceedings of the INDOCRYPT; 2004. p. 371–83.
[5] Li M, Hwang T, Lee NY, et al. (t,n) Threshold-multisignature scheme and generalized multisignature scheme where suspected forgery implies traceability of adversarial shareholders. Cryptologia 2000;24(3): 250–68.
[6] Ham L. Group-oriented (t,n) threshold digital signature scheme and digital multisignature. IEE Proc Comput Digital Tech 1994;141(5): 307–13.
[7] Sahai A, Waters B. Fuzzy identity-based encryption. In: Advances in cryptology-eurocrypt 2005, LNCS 3494; 2005. p. 457–73.
[8] Zhang R, Imai H. Round optimal distributed key generation of threshold cryptosystem based on discrete logarithm problem. In: Proceedings of the ACNS 2003, LNCS 2846; 2003. p. 96–110.