A New Identity Based Signature in the Standard Model

Peng Wei[a], Bai Xia[b]

China Energy Engineering Group Gansu Electric Power Design Institute Co., Ltd Lanzhou 730050, China

[a]pwlut@163.com, [b]Xbai8725@ceec.net.cn

Keywords: id-based signature; key escrow; CDH problem; standard model

Abstract: Under the random oracle model, most identity based signature schemes without trusted PKG are secure. The identity based signature scheme is effective and provably secure under the standard model, does not need trusted PKG, and is suitable for applications. Because the user's private key can't be forged in the scheme, it can't be generated only in the part of PKG. In the case of computational difficulty, the scheme's attack on adaptive selection message is the existence of the unforgeable Herman hypothesis in the standard model. The scheme sloves the inherent key escrow problem, but also has traceability.

1. Introduction

In identity based cryptosystem (IBC), the user's public key is directly obtained from his identity information, while the private key is generated by the trusted private key generator (PKG). Scheme [1,2] proposes a provably secure identity based signature scheme using bilinear pairing technology. However, PKG uses the system master key to generate the private key for users, which leads to the problem of key escrow. Therefore, Al riyami et al. [3] proposed a certificateless public key cryptosystem (CL PKC), which avoids the inherent key escrow problem in ID based cryptosystem. Reference [4] proposed an identity based signature scheme without trusted center by binding two partial public keys to the same ID.

The above schemes can be proved safe under the random oracle model, which is an idealized computing model. As a random oracle, hash function will generate a random answer for each new query; However, in the specific digital signature scheme, because the hash value is not necessarily random, it is difficult to ensure the security of the scheme [5].

Therefore, it is of practical significance to design an efficient and provably secure signature scheme under the standard model. Standard model means that the security proof only depends on standard algebraic problems, and its security is also known as security in the real world. We believe that a provably secure cryptography scheme under the standard model can not be broken unless the algebraic problem on which it is based is solved. Waters first proposed a secure and efficient identity based encryption scheme under the standard model [6], and Paterson [7] proposed a secure identity based signature scheme under the standard model based on the waters scheme. Zhang et al. [8] constructed an effective identity based HIBS signature scheme and proved its security under the standard model. Li et al. [9] proposed a secure and efficient signature scheme under the standard model based on Paterson scheme.

Based on Paterson scheme and the signature scheme without trusted PKG, this paper proposes a new identity based signature scheme without trusted PKG. Under the standard model, the scheme can resist the existential forgery of adaptive selection message attack and provide traceability, that is, the arbitrator can determine whether the PKG is malicious through the tracking algorithm. The scheme eliminates the problems caused by key escrow and has higher efficiency than the typical identity based signature scheme.

2. Preparatory knowledge

2.1 bilinear pairing

Let G and G_T be two p-order cyclic groups, where p is a prime number and g is the generator of G. define the bilinear mapping on group G as e: $G\times G\rightarrow G_T$, and satisfy the following properties:

1) Bilinear: $e(g^a,g^b)=e(g,g)^{ab}$, for any a, $b\in Z_p^*$;

2) Non degradability: $e(g, g)\neq 1$;

3) Computability: for all u, $v\in G$, there is an effective algorithm to calculate $e(u, v)$.

2.2 Related mathematical problems

Definition 1. CDH problem: given the p order cyclic group G, where p is a prime number and g is the generator of G, arbitrarily select $a\in Z_p$, $b\in Z_p$, and assume that g^a, $g^b\in G$ are known to calculate g^{ab}.

Definition 2. (ε, t)-CDH hypothesis: if there is no probabilistic polynomial time algorithm that can solve the CDH problem on group G with a probability of at least in time t, then the (ε,t)-CDH hypothesis on group G is considered to be true.

3. Identity based signature without trusted PKG

3.1 Formal description of identity based untrusted PKG signature scheme

Definition 3. identity based untrusted PKG signature scheme consists of the following four parts: Setup, Extract, Sign and Verify.

Setup:

Input the security parameter k, and PKG outputs the master key x_{PKG} and the corresponding system parameter *parameters*; PKG confidential x_{PKG} public system parameters.

Extract:

1) GenX_1: enter the security parameter l, and the signer with id generates his own partial private key x_1; Calculate part of your public key y_1.

2) GenX_2: PKG calculates part of the signer's public key y_2 and part of the private key x_2 according to y_1, and sends x_2 to the signer through a secure channel. Thus, the signer with $id\in$ID gets his own private key pair (x_1, x_2).

Sign:

The signer uses its identity information id, private key pair (x_1,x_2) and system parameter *parameters* to generate a valid signature σ on message m.

Verify:

Verify (id, m, y_1, y_2,σ)={True, False}, If the above verification is successful, true is output; otherwise, false is output.

4. Secure signature scheme without trusted PKG

In order to make the scheme adapt to different lengths of identity and message bit strings, hash functions can be used for preprocessing and mapping them to the required length, $H_u:\{0,1\}^*\rightarrow\{0,1\}^{n_u}$,$H_m:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$.

4.1 Setup

Let e: $G\times G\rightarrow G_T$ is a bilinear pair and satisfies various properties in Section 2. PKG first randomly selects $s\in Z_p$ as the system master key; Then calculate$g_1=g^s$, and randomly select $u'\in G$,$m'\in G$; PKG then selects the vector $U_v=(u_i)$ of n_u dimension and the vector $M_v=(m_i)$ of n_m dimension, where $u_i\in G$,$m_i\in G$. Finally, get the *parameters*= {e, G, G_T, g, g_1, u', m', U_v, M_v}.

4.2 Extract

Assuming that the user identity u is a bit string with a length of n_u and U is the set of positions with a bit value of 1 in u, then $U \subseteq \{1,\ldots, n_u\}$. The user randomly selects $s_1 \in Z_p$ as part of his private key; calculate $Q_1 = g^{s_1}$ and send Q_1 to PKG. PKG optional $r_u \in Z_p$, calculation $s_2 = Q_1^s (u' \prod_{i \in U} u_i)^{r_u}, Q_2 = g^{r_u}$; PKG sends s_2 to the user through a secure channel and discloses Q_2. So, the user with identity u gets his own private key (s_1, s_2).

4.3 Sign

Assuming that the message m is a bit string with a length of n_m, similar to the method of processing identity in step 2, let$M$ be the set of positions with a bit value of 1 in m, then $M \subseteq \{1,\ldots, n_u\}$. The signer randomly selects $r_m \in Z_p$ and calculates the signature $\sigma = (\sigma_1, \sigma_2)$ of message m, where $\sigma_1 = s_2 (m' \prod_{j \in M} m_j)^{r_m}, \sigma_2 = g^{r_m}$.

4.4 Verify

The verifier uses the system parameter *parameters* and the public information of the signer to verify the signature σ, if the equation

$$e(\sigma_1, g) = e(Q_1, g_1) e((u' \prod_{i \in U} u_i), Q_2) e((m' \prod_{j \in M} m_j), \sigma_2) \tag{1}$$

If established, the signature is valid; Otherwise, the signature is invalid.

5. Analysis of security and execution efficiency of the new scheme

5.1 Security

Theorem 1. Correctness of the new scheme.

$$\begin{aligned} & e(\sigma_1, g) \\ & = e(s_2 (m' \prod_{j \in M} m_j)^{r_m}, g) \\ & = e(Q_1^s (u' \prod_{i \in U} u_i)^{r_u} (m' \prod_{j \in M} m_j)^{r_m}, g) \\ & = e(Q_1^s, g) e((u' \prod_{i \in U} u_i)^{r_u}, g) e((m' \prod_{j \in M} m_j)^{r_m}, g) \\ & = e(Q_1, g_1) e((u' \prod_{i \in U} u_i), g^{r_u}) e((m' \prod_{j \in M} m_j), g^{r_m}) \\ & = e(Q_1, g_1) e((u' \prod_{i \in U} u_i), Q_2) e((m' \prod_{j \in M} m_j), \sigma_2) \end{aligned} \tag{2}$$

Theorem 2. if the (ε', t')-CDH hypothesis holds, the identity based signature scheme $(\varepsilon, t, q_e, q_s)$ without trusted PKG is secure, where

$$\begin{aligned} & \varepsilon' = \frac{\varepsilon}{16(q_e + q_s) q_s (n_u + 1)(n_m + 1)} \\ & t' = t + O((q_e n_u + q_s (n_u + n_m))\rho + (q_e + q_s)\tau) \end{aligned} \tag{3}$$

It should be noted that q_e is the number of key queries, q_s is the number of signature queries, ρ is the polynomial multiplication operation time in group G, τ is the exponential operation time in group G.

Assuming that there is an attacker $A(\varepsilon, t, q_e, q_s)$, A constructs an algorithm B, which solves the CDH difficult problem with a probability ε' of at least □ in the time of t'. Assuming g is the generator of group G, then g^a and g^b are the elements in G. in order to calculate g^{ab}, algorithm B simulates the interaction process between a challenger and A, as follows

System parameter setup:

Let's $l_u = 2(q_e + q_s), l_m = 2q_s$, randomly select two integers k_u and k_m, where $0 \le k_u \le n_u, 0 \le k_m \le n_m$. For a given ($q_e$, q_s, n_u, n_m), assume $l_u(n_u + 1) < p, l_m(n_m + 1) < p$. Random selection $x' \in Z_{l_u}$, n_u dimension vector $X=(x_i)$, and $x_i \in Z_{l_u}$; Random selection $z' \in Z_{l_m}$, n_m dimension vector $Z=(z_i)$ and $z_i \in Z_{l_m}$; Finally, B selects two integers $y' \in Z_p, w' \in Z_p$ and n_u dimension vector $Y=(y_i)$, n_m dimension vector $W=(w_i)$, and $y_i \in Z_p$, $w_i \in Z_p$.

For ease of analysis, *B* defines the following functions about user identity *u* and message *m*:

$$\begin{aligned} F(u) &= x' + \sum_{i \in U} x_i - l_u k_u, \quad \text{where } J(u) = y' + \sum_{i \in U} y_i \\ K(m) &= z' + \sum_{j \in M} z_j - l_m k_m, \quad \text{where } L(m) = w' + \sum_{j \in M} w_j \end{aligned} \tag{4}$$

Queries：

Algorithm *B* uses *a* to simulate the system master key, *b* to simulate the user's partial private key s_1, and g_2 to simulate the user's partial public key Q_1; The following system parameters can be obtained

$$\begin{aligned} & g_1 = g^a, \qquad Q_1 = g_2 = g^b, \\ & u' = g_2^{-l_u k_u + x'} g^{y'}, \quad u_i = g_2^{x_i} g^{y_i} \quad \text{where } 1 \le i \le n_u \\ & m' = g_2^{-l_m k_m + z'} g^{w'}, \quad m_j = g_2^{z_i} g^{w_j} \quad \text{where } 1 \le j \le n_m \end{aligned} \tag{5}$$

So we get the following equation:

$$\begin{aligned} u' \prod_{i \in U} u_i &= g_2^{F(u)} g^{J(u)} \\ m' \prod_{j \in M} m_j &= g_2^{K(m)} g^{L(m)} \end{aligned} \tag{6}$$

B sends system parameters to attacker *A*

$$\begin{aligned} u' \prod_{i \in U} u_i &= g_2^{F(u)} g^{J(u)} \\ m' \prod_{j \in M} m_j &= g_2^{K(m)} g^{L(m)} \end{aligned} \tag{7}$$

Extract Queries:

Considering the key query of identity *u*, when $F(u) \neq 0 \bmod p$, *B* can generate part of the key s_2 corresponding to the identity. For the randomly selected $r_u \in Z_p$, calculate

$$\begin{aligned} s_2 &= g_1^{-J(u)/F(u)} (u' \prod_{i \in U} u_i)^{r_u} \\ &= g_1^{-J(u)/F(u)} (g_2^{F(u)} g^{J(u)})^{r_u} \\ &= g_2^a (g_2^{F(u)} g^{J(u)})^{-a/F(u)} (g_2^{F(u)} g^{J(u)})^{r_u} \\ &= g_2^a (g_2^{F(u)} g^{J(u)})^{r_u - a/F(u)} \\ &= g_2^a (u' \prod_{i \in U} u_j)^{r_u - a/F(u)} \end{aligned} \tag{8}$$

When $F(u) = 0 \bmod p$, the above algorithm stops and the simulation process ends.

Signature queries: consider signing queries about message *m* for identity *u*. When $K(m) \neq 0 \bmod p$, randomly select $r_u \in Z_p$, $r_m \in Z_p$ and calculate

$$\begin{aligned}\sigma_1 &= (u'\prod_{i\in U} u_i)^{r_u} g_1^{-L(m)/K(m)} (m'\prod_{j\in M} m_j)^{r_m} \\ &= g_2^a (u'\prod_{i\in U} u_i)^{r_u} (m'\prod_{j\in M} m_j)^{r_m - a/K(m)} \\ \sigma_2 &= g^{r_m}\end{aligned} \tag{9}$$

When $K(m)=0 \bmod p$, the above algorithm stops and the simulation process ends.

Forgery: if attacker A successfully forges the valid signature $\sigma^* = (\sigma_1^*, \sigma_2^*)$ of the message m^* by the user with identity u^* with a probability of at least ε. If $F(u^*)=0 \bmod p$, $K(m^*)= 0 \bmod p$, then B calculates the following formula

$$\begin{aligned}&\frac{\sigma_1}{g^{J(u^*)r_u} g^{L(m^*)r_m}} \\ &= \frac{Q_1^a (u'\prod_{i\in U} u_i)^{r_u} (m'\prod_{j\in M} m_j)^{r_m}}{g^{J(u^*)r_u} g^{L(m^*)r_m}} \\ &= Q_1^a \frac{(g_2^{F(u^*)} g^{J(u^*)})^{r_u} (g_2^{K(m^*)} g^{L(m^*)})^{r_m}}{g^{J(u^*)r_u} g^{L(m^*)r_m}} \\ &= Q_1^a g_2^{F(u^*)r_u + K(m^*)r_m} \\ &= Q_1^a \\ &= g^{ab}\end{aligned} \tag{10}$$

According to reference [7], the probability of successful simulation of algorithm B is $\varepsilon' = \frac{\varepsilon}{16(q_e+q_s)q_s(n_u+1)(n_m+1)}$, and the time complexity of algorithm B is $t'=t+O((q_e n_u + q_s(n_u+n_m))\rho + (q_e+q_s)\tau)$.

It can be seen from the above process that B successfully solved a CDH problem with probability ε' in the time of t' which is contrary to the CDH assumption, so this scheme is safe.

6. Conclusion

There is a key escrow problem in identity based cryptosystems. In order to solve this problem, people have constructed a signature scheme without trusted PKG. However, almost all the existing schemes prove their security under the random oracle model. Random oracle model is an idealized computing model. In a specific digital signature scheme, because the value of hash function is not necessarily random, it is difficult to ensure the security of the scheme. Based on the provably secure signature scheme under the existing standard model, combined with the signature scheme without trusted PKG, we propose a new identity based signature scheme without trusted PKG. The new scheme can resist the existential forgery of adaptive selection message attack under the standard model. The scheme not only eliminates the problems caused by key escrow, but also provides traceability.

References

[1] HESS F. Efficient identity based signature schemes based on pairings[A]. Selected Areas in Cryptography the 9th Annual International Workshop, SAC2002[C]. Heidelberg: Springer-Verlag, 2002. 310-324.

[2] CHA J, CHEON J. An identity-based signature from gap Diffie Hellman groups[A]. Public Key Cryptography-PKC 2003[C]. Heidelberg: Springer-Verlag, 2003. 18-30.

[3] AL-RIYAMI S, PATERSON K. CBE from CL-PKE: a generic construction and efficient schemes[A]. Public Key Cryptography-PKC 2005: the 8th International Workshop on Theory and Practice in Public Key Cryptography[C]. LNCS 3386, Heidelberg: Springer-Verlag, 2005. 398-415.

[4] LIU J, SUN R, KOU W, WANG X. Efficient ID-based Signature Without Trusted PKG[EB/OL]. http://eprint.iacr.org/2007/135. 2007.

[5] FENG Deng-Guo. Research on t heory and approach of provable security[J]. Journal of Software, 2005, 16(10): 1743-1756(In Chinese)

[6] Waters B. Efficient identity-based encryption without random oracles[C]. Advances in Cryptology EUROCRYPT 2005. LNCS 3494. Heidelberg: Springer-Verlag, 2005. 114-127.

[7] Paterson K, Schuldt J. Efficient identity based signatures secure in the standard model[C]. Proceedings of the ACISP'2006. LNCS 4058. Heidelberg: Springer Verlag, 2006. 207-222.

[8] Leyou Zhang, Yupu Hu, Qing Wu. New Construction of Short Hierarchical ID-Based Signature in the standard model[C]. Fundamenta Infomaticae. IOS Press, 2009,90(1-2), 191-201.

[9] LI Ji-Guo, JIANG Ping-Jin. An Eff icient and Provably Secure Identity Based Signature Scheme in the Standard Model[J]. Chinese Journal of Computers. 2009, 32(11):2130-2136(In Chinese).