无随机预言机的基于身份多签密方案

张 波 徐秋亮
(山东大学计算机科学与技术学院 济南 250101)

摘 要 签密是一种能够同时提供加密和签名功能的密码体制,是可以在公开信道上同时保证信息私密性和发送者身份可认证性的重要技术手段.为适应多参与者环境下通信安全的需求,提出了基于身份多签密方案的形式化安全模型,并基于判定双线性 Diffie-Hellman 假设和计算 Diffie-Hellman 假设构造了一个无随机预言机的具体方案.新方案在标准模型下是可证安全的,满足自适应选择密文攻击下的密文不可区分性和选择消息攻击下的签名不可伪造性.

关键词 签密;多签密;基于身份;随机预言模型;双线性对
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2010.00103

Identity-Based Multi-Signcryption Scheme without Random Oracles

ZHANG Bo XU Qiu-Liang
(*School of Computer Science and Technology, Shandong University, Jinan* 250101)

Abstract Signcryption is a very important technology in message security and the sender's identity authentication for communication in the open channel. To adapt multi-user settings, this paper defines the formal model of identity-based multi-signcryption scheme and proposes the first identity-based multi-signcryption scheme without random oracles based on Waters' identity-based encryption scheme. The scheme is proved secure against adaptive chosen ciphertext attacks and adaptive chosen message attacks under decisional bilinear Diffie-Hellman assumption and computational Diffie-Hellman assumption respectively.

Keywords signcryption; multi-signcryption; identity-based; random oracle; bilinear pairings

1 Introduction

Identity-based (ID-based) cryptosystems were introduced by Shamir[1] in 1984. Its main idea is that the public keys of a user can be easily derived from arbitrary strings corresponding to his identity information such as name, telephone number or email address. A private key generator (PKG) computes private keys from a master secret and distributes these to the users participating in the scheme. This eliminates the need for certificates as used in a traditional public key infrastructure. ID-based systems may be a good alternative for certificate-based systems from the viewpoint of efficiency and convenience. Since Boneh and Franklin gave a practical ID-based encryption scheme[2] from Weil pairing in 2001, a large number of papers have been published in this area such as [3-6].

In 1997, Zheng[7] proposed a new cryptographic primitive: signcryption, which can perform digital signature and public key encryption simultaneously at lower computational costs and communication overheads than sign-then-encrypt way to obtain private and authenticated communications in the open channel. Since then, there are many signcryption schemes proposed. By combining ID-

收稿日期:2009-07-24;最终修改稿收到日期:2009-10-09.本课题得到国家自然科学基金(60873232)、山东省自然基金(Y2007G37)资助.
张 波,男,1981 年生,博士研究生,主要研究方向为信息安全.**徐秋亮**,男,1960 年生,博士,教授,博士生导师,研究领域包括信息安全、网络安全、密码学. E-mail: xuqiuliang@sdu.edu.cn.

based cryptology and signcryption, Malone-Lee[8] proposed the first ID-based signcryption scheme. But Libert and Quisquater[9] pointed out that Malone-Lee's scheme is not semantically secure. Chow et al.[10] proposed an ID-based signcryption scheme that can provide both public verifiability and forward security. In 2003, Boyen[11] proposed a secure ID-based signcryption scheme with ciphertext anonymity and provable secure in the random oracle model. In [12], Chen and Malone-Lee improved Boyen's scheme in efficient. Barreto et al. proposed an efficient ID-based signcryption scheme[13]. Yu et al.[14] propose the first ID-based signcryption scheme without random oracles.

To adapt multi-user settings, Duan et al. proposed a multi-receiver ID-based signcryption scheme[15] and Bellare et al. gave an ID-based multi-signature scheme[16] based on RSA. In everyday life, many legal documents require signatures from more than one party. At the same time, the signers perhaps don't want someone else except the legal receiver to know the content of the signed message. Signing a secret contract by multi-parties is a good example to illustrate this case. Recently, Zhang et al.[17] proposed the first ID-based multi-signcryption scheme to complete efficient transmission and authentication in multi-party oriented environment. The security of the scheme was proven secure in the random oracle model[18]. Although the model is efficient and useful, it has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure[19]. Therefore, it is an important research problem to construct a secure ID-based multi-signcryption scheme without random oracles.

Our contribution

In this paper, motivated by Malone-Lee's ID-based signcryption scheme[8] and Waters' ID-based encryption scheme[5], we define formal model of ID-based multi-signcryption scheme and propose the first ID-based multi-signcryption scheme without random oracles. Our scheme is proved secure against adaptive chosen ciphertext attacks and adaptive chosen message attacks.

Rest of the paper is organized as follows: in section 2, the formal model of ID-based multi-signcryption scheme without random oracles is described. In section 3, related mathematical problems and complexity assumptions are described. The proposed ID-based multi-signcryption scheme is described in section 4 and the security and efficient analysis of the scheme are given in section 5. Finally, conclude the paper in section 6.

2 Formal Model of ID-Based Multi-Signcryption Schemes

2.1 Generic scheme

An ID-based multi-signcryption scheme consists of the following algorithms.

Setup. Given a security parameter k, PKG generates a master key S and common parameters P. P is made public while S is kept secret.

Extract. Given an identity ID_u, the PKG runs this algorithm to generate the private key d_u associated with ID_u and transmits it to the user via a secure channel.

Multi-Signcrypt. To send a message m to Bob whose identity is ID_B, Signcrypters with identity $ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n}$ obtain a ciphertext σ by running Multi-Signcrypt $(m, d_{A_1}, \cdots, d_{A_n}, ID_B)$.

Unsigncrypt. After Bob receives the ciphertext σ, he runs Unsigncrypt $(\sigma, d_B, ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n})$ and obtains the message m or the symbol $\perp$ indicating that the ciphertext is invalid.

2.2 Security Notions

Now we recall Malone-Lee's[8] security models for ID-based signcryption scheme. In the following, we modify his definitions to adapt for our ID-based multi-signcryption scheme. Besides the confidentiality defined in [17], the unforgeability has been also formally defined in our security model.

Definition 1. An ID-based multi-signcryption scheme is said to have the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDMSC-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game:

Setup. The challenger ϑ runs the Setup algorithm with a security parameter k and obtains common parameters P and a master key S. He sends P to the adversary and keeps S secret.

First stage. The adversary performs a polynomially bounded number of queries. These queries may be made adaptively, i.e. each query may depend on the answers to the previous queries.

① Key extraction queries: The adversary requests the private key of an identity ID_u and receives the extracted private key $d_u = Extract(ID_u)$.

② Multi-signcryption queries: The adversary produces a signcrypter list $ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n}$, the recipient identity ID_B and a plaintext m. ϑ computes $d_{A_i} = Extract(ID_{A_i})$ and $\sigma =$ Multi-Signcrypt $(m, d_{A_1}, \cdots, d_{A_n}, ID_B)$, then he sends σ to the ad-

versary.

③ Unsigncryption queries: The adversary produces a signcrypter list $ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n}$, the recipient identity ID_B and a ciphertext σ. ϑ computes $d_B = Extract(ID_B)$ and sends the result of Unsigncrypt $(\sigma, d_B, ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n})$ to the adversary. This result may be the symbol $\perp$ if σ is an invalid ciphertext.

Challenge. The adversary chooses two plaintexts, m_0 and m_1, a signcrypter list $ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n}$ and recipient identity ID_B on which he wishes to be challenged. He cannot have asked the private key corresponding ID_B in the first stage. ϑ chooses randomly a bit γ, computes $\sigma =$ Multi-Signcrypt $(m_\gamma, d_{A_1}, \cdots, d_{A_n}, ID_B)$ and sends it to the adversary.

Second stage. The adversary asks a polynomial number of queries adaptively again as in the first stage. It is not allowed to extract the private key corresponding to ID_B and it is not allowed to make an unsigncryption query for σ under ID_B.

Guess. Finally, the adversary produces a bit γ' and wins the game if $\gamma' = \gamma$.

Note that the security models described above deals with insider security since the adversary is assumed to have access to the private key of the signcrypter of a signcrypted message. This means that the scheme is security even if a signcrypter's private key is compromised.

Definition 2. An ID-based multi-signcryption scheme is said to be secure against an existential forgery for adaptive chosen message attacks (EUF-IDMSC-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game:

Setup. The challenger ϑ runs the Setup algorithm with a security parameter k and obtains common parameters P and a master key S. He sends P to the adversary and keeps S secret.

Queries. The adversary performs a polynomially bounded number of queries adaptively just like in the previous definition.

Forgery. Finally, the adversary produces a new tuple $(\sigma, ID_B, ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n})$ (i. e. a tuple that was not produced by the multi-signcryption oracle) where one of the private key of signcrypter was not asked in the second stage and wins the game if the result of Unsigncrypt $(\sigma, d_B, ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n})$ is not the symbol $\perp$.

Note that this definition allows the adversary to access to most secret key of the signcrypter and the receiver, which guarantees the insider security.

3 Preliminaries

In this section, we briefly review the basic concepts on bilinear pairings and some related complexity assumptions.

3.1 Bilinear Pairings

Let G and G_T be two cyclic multiplicative groups of prime order p and g be a generator of G. The map $e: G \times G \to G_T$ is said to be an admissible bilinear pairing if the following conditions hold true.

(1) e is bilinear, i. e. $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in Z_p$.

(2) e is non-degenerate, i. e. $e(g, g) \neq 1_{G_T}$.

(3) e is efficiently computable.

3.2 Complexity Assumptions

3.2.1 Decisional Bilinear Diffie-Hellman (DBDH) Assumption

The challenger chooses $a, b, c, z \in Z_p$ at random and then flips a fair binary coin β. If $\beta = 1$ it output the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g, g)^{abc})$. Otherwise, if $\beta = 0$, the challenger outputs the tuple $(g, A = g^a, B = g^b, C = g^c, Z = e(g, g)^z)$. The adversary θ must then output a guess β' of β.

An adversary has at least an ε advantage in solving the decisional BDH problem if

$$|Pr[\theta(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - Pr[\theta(g, g^a, g^b, g^c, e(g, g)^z) = 1]| \geq \varepsilon,$$

where the probability is over the randomly chosen a, b, c, z and the random bits consumed by θ.

Definition 3. The decisional ε-DBDH assumption holds if no adversary has at least ε advantage in solving the above game.

3.2.2 Computational Diffie-Hellman (CDH) Assumption

The challenger chooses $a, b \in Z_p$ at random and outputs $(g, A = g^a, B = g^b)$. The adversary then attempts to output $g^{ab} \in G$. An adversar θ has at least an ε advantage if $Pr[\theta(g, g^a, g^b) = g^{ab}] \geq \varepsilon$ where the probability is over the randomly chosen a, b and the random bits consumed by θ.

Definition 4. The computational ε-CDH assumption holds if no adversary has at least ε advantage in solving the above game.

4 The Concrete Scheme

In the section, we describe our ID-based multi-signcryption scheme. In the following, all the identities will be assumed to be bit string of length n_u. A collision resistant Hash function should be employed to construct a more flexible scheme which allows identities of arbitrary length.

Our scheme is inspired by Waters' ID-based encryption scheme and consists of the following algorithms.

Setup. Choose groups G and G_T of prime order p such that an admissible pairing $e:G\times G\rightarrow G_T$ can be constructed and pick a generator g of G.

Now, pick a random secret $\alpha\in Z_p$, compute $g_1=g^\alpha$ and pick $g_2\leftarrow_R G$. Furthermore, pick elements $u',m'\leftarrow_R G$ and vectors $\Lambda_U=(u_i)$, $\Lambda_M=(m_i)$ of length n_u and n_m, respectively, whose entries are random elements from G. Let H, H_m are cryptography hash functions where $H:G_T\rightarrow\{0,1\}^{l_t}$, $H_m:\{0,1\}^{l_t}\times G_T\rightarrow\{0,1\}^{n_m}$ where l_t is the length of plaintext. The public parameters are $P=(G,G_T,e,g,g_1,g_2,u',\Lambda_U,m',\Lambda_M,H,H_m)$ and the master secret S is g_2^α.

Extract. Let u be a bit string of length n_u representing an identity and let $u[i]$ be the i-th bit of u. Define $U'\subset\{1,2,\cdots,n_u\}$ to be the set of indicies i such that $u[i]=1$.

To construct the private key d_u of the identity u, pick $r_u\leftarrow Z_p$ and compute:

$$d_u=\left(g_2^\alpha\left(u'\prod_{i\in U'}u_i\right)^{r_u},g^{r_u}\right).$$

Therefore, the signcrypters with identity $u_{A_i}(i=1,2,\cdots,n)$ and the receiver Bob's private keys are

$$d_{A_i}=(d_{A_i1},d_{A_i2})=\left(g_2^\alpha\left(u'\prod_{j\in U'_{A_i}}u_j\right)^{r_{A_i}},g^{r_{A_i}}\right)\text{ and}$$

$$d_B=(d_{B1},d_{B2})=\left(g_2^\alpha\left(u'\prod_{j\in U'_B}u_j\right)^{r_B},g^{r_B}\right).$$

Multi-Signcrypt. Let m be a bit string of length l_t representing a message. As in the Extract algorithm, let $M'\subset\{1,2,\cdots,n_m\}$ be the set of indicies j such that $m[j]=1$, where $m[j]$ is the j-th bit of bit string M of length n_m. Each signcrypter with identity $u_{A_i}(i=1,2,\cdots,n)$ picks $r_i\in Z_p$ randomly and follows the steps below:

① Compute $\omega_i=\left(e(g_1,g_2)e\left(d_{B2},u'\prod_{j\in U'_B}u_j\right)\right)^{r_i}$ and broadcast ω_i to other signcrypters securely.

② Compute $\sigma_{i1}=g^{r_i}$.

③ Compute $\sigma_{i2}=d_{A_i2}$.

④ Compute $\omega=\prod_{i=1}^n\omega_i$, $M=H_m(m\parallel\omega)$ and $\sigma_{i3}=d_{A_i1}\cdot\left(m'\prod_{j\in M'}m_j\right)^{r_i}$.

⑤ Send $(\sigma_{i1},\sigma_{i2},\sigma_{i3})$ to the appointed clerk Cindy, who is one of the signcrypters.

Cindy compute $c=m\oplus H(\omega)$, $\sigma_1=\prod_{i=1}^n\sigma_{i1}$, $\sigma_2=\{\sigma_{i2}\mid i=1,2,\cdots,n\}$, $\sigma_3=\prod_{i=1}^n\sigma_{i3}$.

The resultant ciphertext is $\sigma=(c,\sigma_1,\sigma_2,\sigma_3)$.

Unsigncrypt. Received a ciphertext $\sigma=(c,\sigma_1,\sigma_2,\sigma_3)$, Bob decrypts the ciphertext as follows:

① Compute $\omega=e(\sigma_1,d_{B1})$.

② Compute $m=c\oplus H(\omega)$.

③ Compute $M=H_m(m\parallel\omega)$.

Accept the message if and only if the following equality holds:

$$e(\sigma_3,g)=e(g_1,g_2)^n\prod_{i=1}^n e\left(u'\prod_{j\in U'_{A_i}}u_j,d_{A_i2}\right)e\left(m'\prod_{j\in M'}m_j,\sigma_1\right).$$

Note that: $\prod_{i=1}^n e\left(u'\prod_{j\in U'_{A_i}}u_j,d_{A_i2}\right)$ could be computed beforehand and computed only once.

5 Analysis of the Scheme

5.1 Correctness

The correctness of the scheme can be directly verified by the following equations:

$$\begin{aligned}\omega&=e(\sigma_1,d_{B1})=e\left(\prod_{i=1}^n g^{r_i},g_2^\alpha\left(u'\prod_{i\in U'_B}u_i\right)^{r_B}\right)\\&=e\left(g^{\sum_{i=1}^n r_i},g_2^\alpha\right)e\left(g^{\sum_{i=1}^n r_i},\left(u'\prod_{i\in U'_B}u_i\right)^{r_B}\right)\\&=\left(e(g_1,g_2)e\left(g^{r_B},u'\prod_{i\in U'_B}u_i\right)\right)^{\sum_{i=1}^n r_i}\\&=\left(e(g_1,g_2)e\left(d_{B2},u'\prod_{i\in U'_B}u_i\right)\right)^{\sum_{i=1}^n r_i}=\prod_{i=1}^n\omega_i,\end{aligned}$$

$$\begin{aligned}e(\sigma_3,g)&=e\left(\prod_{i=1}^n\sigma_{i3},g\right)=e\left(\prod_{i=1}^n d_{A_i1}\cdot\left(m'\prod_{j\in M'}m_j\right)^{r_i},g\right)\\&=e\left(\prod_{i=1}^n d_{A_i1},g\right)e\left(\prod_{i=1}^n\left(m'\prod_{j\in M'}m_j\right)^{r_i},g\right)\\&=e\left(\prod_{i=1}^n g_2^\alpha\left(u'\prod_{j\in U'_{A_i}}u_j\right)^{r_{A_i}},g\right)e\left(\left(m'\prod_{j\in M'}m_j\right)^{\sum_{i=1}^n r_i},g\right)\\&=e(g_1,g_2)^n\prod_{i=1}^n e\left(u'\prod_{j\in U'_{A_i}}u_j,d_{A_i2}\right)e\left(m'\prod_{j\in M'}m_j,\sigma_1\right).\end{aligned}$$

5.2 Security

Theorem 1. Assume there is an IND-IDM-SC-CCA2 adversary that is able to distinguish two valid ciphertexts during the game defined in Definition1 with an advantage ε and asking at most q_E extraction queries, q_S multi-signcryption queries and q_U unsigncryption queries, then there exists a distinguisher ϑ that can solve an instance of the Decisional Bilinear Diffie-Hellman problem with an advantage $\dfrac{\varepsilon}{8(q_E+q_S+q_U)(n_u+1)q_S(n_m+1)}$.

Proof. Assume that the distinguisher ϑ re-

ceives a random DBDH problem instance $(g, A=g^a, B=g^b, C=g^c, Z\in G_T)$, his goal is to decide whether $Z=e(g,g)^{abc}$ or not. ϑ will run the adversary as a subroutine and act as the adversary's challenger in the IND-IDMSC-CCA2 game. Our proof is based on Waters' idea such as in [5-6].

Setup. Let $l_u=2(q_E+q_S+q_U)$ and $l_m=2q_S$, ϑ choose randomly

① Two integers k_u and k_m $(0\le k_u\le n_u,\ 0\le k_m\le n_m)$.

② An integer $x'\in Z_{l_u}$, an n_u-dimensional vector $X=(x_i)(x_i\in Z_{n_u})$.

③ An integer $z'\in Z_{l_m}$, an n_m-dimensional vector $Z=(z_j)(z_j\in Z_{n_m})$.

④ Two integers $y',\omega'\in Z_p$, an n_u-length vector $Y=y_i(y_i\in Z_p)$ and an n_m-length vector $W=\omega_j(\omega_j\in Z_p)$.

For ease of analysis, we define the functions for an identity u and a message m respectively.

$F(u)=-l_uk_u+x'+\sum_{i\in U'}x_i$ and $J(u)=y'+\sum_{i\in U'}y_i$,

$K(m)=-l_mk_m+z'+\sum_{j\in M'}z_j$ and $L(m)=\omega'+\sum_{j\in M'}\omega_j$.

Then the challenger assigns a set of public parameters as follows:

$$g_1=g^a,\ g_2=g^b,$$
$$u'=g_2^{-l_uk_u+x'}g^{y'},\ u_i=g_2^{x_i}g^{y_i}(1\le i\le n_u),$$
$$m'=g_2^{-l_mk_m+z'}g^{\omega'},\ m_j=g_2^{z_j}g^{\omega_j}(1\le j\le n_m).$$

Note that these public parameters have the same distribution as in the game between the distinguisher ϑ and the adversary. For any identity u and any bit string M, we have

$$U=u'\prod_{i\in U'}u_i=g_2^{F(u)}g^{J(u)},$$
$$m'\prod_{j\in M'}m_j=g_2^{K(M)}g^{L(M)}.$$

First stage. ϑ answers the queries as follows:

① Extraction queries

When the adversary asks for the private key corresponding to an identity u, assuming $F(u)\neq 0 \bmod p$, the distinguisher ϑ chooses a random $r_u\in Z_p$ and gives the adversary the pair

$$d_u=(d_{u1},d_{u2})=\left(g_1^{\frac{-J(u)}{F(u)}}\left(u'\prod_{i\in U'}u_i\right)^{r_u},g_1^{\frac{-1}{F(u)}}g^{r_u}\right).$$

Let $\hat{r}_u=r_u-\frac{a}{F(u)}$, as in Waters' proof[5] and Paterson's proof[6] and we will show in the following, d_u is a valid private key for identity u. The distinguisher ϑ can generate such a d_u if and only if $F(u)\neq 0 \bmod p$. The simulation is perfect since

$$d_{u1}=g_1^{\frac{-J(u)}{F(u)}}(g_2^{F(u)}g^{J(u)})^{r_u}$$
$$=g_2^a(g_2^{F(u)}g^{J(u)})^{\frac{-a}{F(u)}}(g_2^{F(u)}g^{J(u)})^{r_u}$$
$$=g_2^a(g_2^{F(u)}g^{J(u)})^{r_u-\frac{a}{F(u)}}=g_2^a(g_2^{F(u)}g^{J(u)})^{\hat{r}_u}$$

and $d_{u2}=g_1^{\frac{-1}{F(u)}}g^{r_u}=g^{r_u-\frac{a}{F(u)}}=g^{\hat{r}_u}$.

If $F(u)=0 \bmod p$, since the above computation cannot be performed, ϑ simply aborts. To make it sample, assume $l_u(n_u+1)<p$ which implies $0\le l_un_u<p$, it is easy to see that $-p<F(u)=-l_uk_u+x'+\sum_{i\in U'}x_i<p$ and $F(u)=0 \bmod p\Rightarrow F(u)=0 \bmod l_u$. Hence, $F(u)\neq 0 \bmod l_u$ implies $F(u)\neq 0 \bmod p$. Thus the former condition will be sufficient to ensure that ϑ will not abort in extraction queries.

② Multi-signcryption queries

At any time, the adversary can perform a multi-signcryption query for a plaintext m, a signcrypter list $ID_{A_1},ID_{A_2},\cdots,ID_{A_n}$ and the recipient identity ID_B. If $F(u_{A_i})\neq 0 \bmod l_u$, ϑ first generates a private key for u_{A_i} just calling the extract query algorithm described above, and then runs Multi-Signcrypt $(m, d_{A_1},\cdots,d_{A_n}, ID_B)$ to answer the adversary's query. Otherwise, ϑ will simply abort.

③ Unsigncryption queries

At any time, the adversary can perform an unsigncryption query on a ciphertext σ for a signcrypter list $ID_{A_1},\cdots,ID_{A_n}$ and u_B. If $F(u_B)\neq 0 \bmod l_u$, ϑ first generates a private key for u_B just calling the extract query algorithm described above, and then runs Unsigncrypt $(\sigma,d_B,ID_{A_1},\cdots,ID_{A_n})$ to answer the adversary's query. Otherwise, ϑ will simply abort.

Challenge. After a polynomially bounded number of queries, the adversary chooses identities $u^*_{A_1},\cdots,u^*_{A_n}$, u^*_B on which he wishes to be challenged. Note that ϑ fails if the adversary has asked a key extraction query on u^*_B during the first stage. Then the adversary submits two messages m_0, $m_1\in G_T$ and $\{u^*_{A_i}\mid i=1,2,\cdots,n\}$, u^*_B to ϑ. ϑ will abort if $F(u^*_B)=0 \bmod p$. Then ϑ flips a fair binary coin γ and ϑ will abort if $K(M^*_\gamma)=0 \bmod p$ where $M^*_\gamma=H_m(m_\gamma \parallel Z\cdot e(d^*_{B2},C^{J(u^*_B)}))$, otherwise, ϑ constructs a multi-signcryption ciphertext of m_γ as: $\left(m_\gamma\oplus H(Z\cdot e(d^*_{B2},C^{J(u^*_B)})),C,\{d^*_{A_i2}\mid i=1,2,\cdots,n\},\prod_{i=1}^{n}d^*_{A_i1}\cdot C^{L(M_\gamma)}\right)$.

Let $c=\sum_{i=1}^{n}r_i$, $Z=e(g,g)^{abc}$, $C=g^c$, the simulation is perfect since

$$Z\cdot e(d^*_{B2},C^{J(u^*_B)})=e(g,g)^{abc}\cdot e(d^*_{B2},g^{c\cdot J(u^*_B)})$$
$$=\left(e(g_1,g_2)e\left(d^*_{B2},u'\prod_{j\in U^{*'}_B}u_j\right)\right)^{\sum_{i=1}^{n}r_i}=\prod_{i=1}^{n}\omega_i,$$

$$C=g^c=g^{\sum_{i=1}^{n}r_i}=\prod_{i=1}^{n}g^{r_i}=\prod_{i=1}^{n}\sigma_{i1},$$

$$\prod_{i=1}^{n}d_{A_i1}^{*}\cdot C^{L(M_\gamma)}=\prod_{i=1}^{n}d_{A_i1}^{*}\cdot\left(m'\prod_{j\in M'}m_j\right)^{\sum_{i=1}^{n}r_i}$$

$$=\prod_{i=1}^{n}\left(d_{A_i1}^{*}\cdot\left(m'\prod_{j\in M'}m_j\right)\right)^{r_i}=\prod_{i=1}^{n}\sigma_{i3}.$$

Second stage. The adversary then performs a second series of queries which are treated in the same way as the first stage. It is not allowed to extract the private key corresponding to u_B^* and it is not allowed to make an unsigncryption query for σ under u_B^*.

Guess. At the end of the simulation, the adversary outputs a guess γ' of γ. If $\gamma'=\gamma$, ϑ answers 1 indicating that $Z=e(g,g)^{abc}$; Otherwise, ϑ answers 0 to the DBDH problem.

Probability of success. Now we have to assess ϑ's probability of success. For the simulation to complete without aborting, we require the following conditions fulfilled:

① Extraction queries on an identity u have $F(u)\neq 0 \bmod l_u$.

② Multi-signcryption queries on a message m have $F(u_i)\neq 0 \bmod l_u$, for all $i\in[1,n]$.

③ Unsigncryption queries on a ciphertext σ have $F(u_B)\neq 0 \bmod l_u$.

④ $F(u_B^*)=0 \bmod p$ and $K(M_\gamma^*)=0 \bmod p$ in the challenge stage.

Let $u_1,\cdots,u_{q_I}$ be the identity appearing in queries not involving the challenge identity. Clearly, we will have $q_I\leq q_E+q_S+q_U$. Define the events

A_i: $F(u_i)\neq 0 \bmod l_u$ where $i=1,2,\cdots,q_I$,

A': $F(u_B^*)=0 \bmod p$,

B^*: $K(M_\gamma^*)=0 \bmod p$.

Then the probability of ϑ not aborting is $Pr[\overline{abort}]\geq Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A'\wedge B^*]$.

Since the function F and K are selected independently, therefore, the event $(\bigwedge_{i=1}^{q_I}A_i\wedge A')$ and B^* are independent. For the randomness of k_u, x' and X, we have

$$\begin{aligned}Pr[A']&=Pr[F(u^*)=0 \bmod p]\\&=Pr[F(u^*)=0 \bmod l_u]\cdot\\&\quad Pr[F(u^*)=0 \bmod p\mid F(u^*)=0 \bmod l_u]\\&=\frac{1}{l_u}\frac{1}{n_u+1}.\end{aligned}$$

On the other hand, for any i, the event A_i and A' are independent, so we have

$$Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A']=Pr[A']Pr[\bigwedge_{i=1}^{q_I}A_i\mid A']$$

$$=Pr[A'](1-Pr[\bigvee_{i=1}^{q_I}\overline{A_i}\mid A'])$$

$$\geq Pr[A'](1-\sum_{i=1}^{q_I}Pr[\overline{A_i}\mid A'])$$

$$=\left(\frac{1}{l_u}\frac{1}{n_u+1}\right)\left(1-\frac{q_I}{l_u}\right)$$

$$\geq\left(\frac{1}{2(q_E+q_S+q_U)(n_u+1)}\right)\left(1-\frac{q_E+q_S+q_U}{2(q_E+q_S+q_U)}\right)$$

$$=\frac{1}{4(q_E+q_S+q_U)(n_u+1)}.$$

Similarly, we have $Pr[B^*]=\frac{1}{l_m}\frac{1}{n_m+1}$.

By combining the above result, we have

$$Pr[\overline{abort}]\geq Pr[\bigwedge_{i=1}^{q_I}A_i\wedge A'\wedge B^*]$$

$$\geq\frac{1}{8(q_E+q_S+q_U)(n_u+1)q_S(n_m+1)}.$$

If the simulation does not abort, the adversary will win the game in definition 1 with probability at least ε. Thus ϑ can solve for the DBDH problem instance with probability

$$\frac{\varepsilon}{8(q_E+q_S+q_U)(n_u+1)q_S(n_m+1)}.$$

Theorem 2. Under the CDH assumption, the proposed ID-based multi-signcryption scheme is existentially unforgeable against adaptive chosen message attack.

Proof. Assume that a EUF-IDMSC-CMA forger for our scheme exists, we will construct a challenger ϑ, who runs the forger as a subroutine to solve an instance of CDH problem. ϑ is given a group G, a generator g and elements g^a and g^b. His goal is to compute g^{ab}. ϑ first sets the public parameters using the Setup algorithm described in the previous proof. Note that in Setup phase, ϑ assigns $g_1=g^a$ and $g_2=g^b$. After ϑ defines functions $F(u)$, $J(u)$, $K(m)$, $L(m)$ and public parameters u', m', u_i, m_j, we have $u'\prod_{i\in U'}u_i=g_2^{F(u)}g^{J(u)}$, $m'\prod_{j\in M'}m_j=g_2^{K(m)}g^{L(m)}$.

Then, the forger can perform a polynomially bounded number of queries including private key extraction queries, multi-signcryption queries, and unsigncryption queries. The challenger ϑ answers the forger in the same way as that of Theorem 1. Finally, if ϑ does not abort, the forger will return a new ciphertext $\sigma^*=(c^*,\sigma_1^*,\sigma_2^*,\sigma_3^*)$ on message m^*, where m^* has never been queried under identities $\{u_{A_i}^*\mid i=1,2,\cdots,n\}$ and u_B^*. Now, ϑ can unsigncrypt σ^* and obtain (m^*,ω^*). ϑ compute $M^*=H_m(m^*\parallel\omega^*)$. If $F(u_A^*)\neq 0 \bmod p$ and $K(M^*)\neq 0 \bmod p$ then ϑ will abort. Otherwise, $F(u_A^*)=0 \bmod p$ and $K(M^*)=0 \bmod p$, ϑ computes and outputs

$$\left(\frac{\sigma_3^*}{\prod_{i=1}^{n}(\sigma_{i2}^{*\,J(u_{A_i}^*)})(\sigma_1^*)^{L(M^*)}}\right)^{n^{-1}}=$$

$$\left(\frac{\prod_{i=1}^{n} g_2^a\left(u'\prod_{j\in U_{A_i}^*}u_j\right)^{r_{A_i}}\cdot\left(m'\prod_{j\in M'^*}m_j\right)^{r_m}}{\prod_{i=1}^{n}(g^{J(u_{A_i}^*)r_{A_i}})\cdot g^{L(M^*)r_m}}\right)^{n^{-1}}=g^{ab}$$

as the solution to the given CDH problem.

5.3 Efficiency analysis

We compare the new scheme to the first ID-based signcryption scheme[14] without random oracles, which is a 1-to-1 signcryption type. Our scheme is a multi-signcryption scheme, thus, it should belong to a n-to-1 signcryption type. To realize justice comparison, let $n=1$, then these two schemes are converted into 1-to-1 type. In the following table we denote by E an exponentiation, by M a scalar multiplication and by P a computation of the pairing. Other operations are omitted in the following analysis since their computation cost is trivial. We consider the pre-computation here and do not take hash evaluations into account.

Table 1　Comparing of our proposed scheme with Yu et al. scheme

Scheme	signcryption	unsigncryption
Yu et al. scheme	$4E+(n_m+2)M$	$4P+(n_m+6)M$
Our scheme	$3E+(n_m+2)M$	$3P+(n_m+3)M$

It can be seen from table 1 that our unsigncryption phase has one pairing computation, which is the operation takes the most running time, less than that in [14].

6　Conclusions

In this paper, we have modified Malone-Lee's[8] security models for ID-based signcryption scheme to adapt for our ID-based multi-signcryption scheme. The confidentiality and unforgeability have been formally defined in our security model. We have proposed a concrete ID-based multi-signcryption scheme based on Waters' identity based encryption scheme. To our best knowledge, this is the first ID-based multi-signcryption scheme that can be proven secure without random oracles. The scheme is proved secure against adaptive chosen ciphertext attacks and adaptive chosen message attacks under decisional bilinear Diffie-Hellman assumption and computational Diffie-Hellman assumption respectively.

Acknowledgements　The authors would like to thank anonymous reviewers for giving helpful suggestions.

References

[1] Shamir A. Identity-based cryptosystem and signature scheme//Proceedings of the CRYPTO 1984. California, USA, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairings//Proceedings of the CRYPTO 2001. California, USA, 2001: 213-229

[3] Hess F. Efficient identity based signature schemes based on pairings//Proceedings of the SAC 2002. Madrid, Spain, 2002: 310-324

[4] Cha J, Cheon J. An identity-based signature from gap Diffie-Hellman groups//Proceedings of the PKC 2003. Florida, USA, 2003: 18-30

[5] Waters R. Efficient identity based encryption without random oracles//Proceedings of the EUROCRYPT 2005. Aarhus, Denmark, 2005: 114-127

[6] Paterson K, Schuldt J. Efficient identity based signatures secure in the standard model//Proceedings of the ACISP 2006. Melbourne, Australia, 2006: 207-222

[7] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature)+cost(encryption)//Proceedings of the CRYPTO 1997. California, USA, 1997: 165-179

[8] Malone-Lee J. Identity based signcryption. Cryptology ePrint Archive, Report 2002/098, 2002

[9] Libert B, Quisquator J. A new identity based signcryption scheme from pairings//Proceedings of the 2003 IEEE Information Theory Workshop. Paris, France, 2003: 155-158

[10] Chow S, Yiu S, Hui L, Chow K. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity//Proceedings of the ICISC 2003. Seoul, Korea, 2004: 352-369

[11] Boyen X. Multipurpose identity based signcryption: A swiss army knife for identity based cryptography//Proceedings of the CRYPTO 2003. California, USA, 2003: 383-399

[12] Chen L, Malone-Lee J. Improved identity-based signcryption//Proceedings of the PKC 2005. Les Diablerets, Switzerland, 2005: 362-379

[13] Barreto P, Libert B, McCullagh N, Quisquater J. Efficient and provably-secure identity based signatures and signcryption from bilinear maps//Proceedings of the ASIACRYPT 2005. Chennai, India, 2005: 515-532

[14] Yu Y, Yang B, Sun Y, Zhou S. Identity based signcryption scheme without random oracles. Computer Standards & Interfaces, 2009, 31(1): 56-62

[15] Duan S, Cao Z. Efficient and provably secure multi-receiver identity-based signcryption//Proceedings of the ACISP 2006. Melbourne, Australia, 2006: 195-206

[16] Bellare M, Neven G. Identity-based multi-signatures from RSA//Proceedings of the CT-RSA 2007. CA, USA, 2007: 145-182

[17] Zhang J, Mao J. A novel identity-based multi-signcryption scheme. Computer Communications, 2009, 32(1): 14-18

[18] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols//Proceedings of the CCS 1993. Virginia, USA, 1993: 62-73

[19] Canetti R, Goldreich O, Halevi S. The random oracle methodology, revisited (preliminary version)//Proceedings of the STOC 1998. Texas, USA, 1998: 209-218

ZHANG Bo, born in 1981, Ph. D. candidate. His research interests focus on information security.

XU Qiu-Liang, born in 1960, Ph. D., professor, Ph. D. supervisor. His main research interests include theoretic research on cryptography, information security and network security.

Background

In traditional public key cryptosystems, the management of certificates is usually complex and costly. ID-based systems proposed by Shamir in 1984 may be a good alternative for certificate-based systems from the viewpoint of efficiency and convenience. Since Boneh and Franklin gave a practical ID-based encryption scheme from Weil pairing in 2001, a large number of papers have been published in this area.

Signcryption is another very important technology in message security and the sender's identity authentication for communication in the open channel. By combining ID-based cryptology and signcryption, Malone-Lee proposed the first ID-based signcryption scheme. To adapt multi-user settings, Zhang et al. proposed the first ID-based multi-signcryption scheme to complete efficient transmission and authentication in multi-party oriented environment. The security of the scheme was proven secure in the random oracle model. Although the model is efficient and useful, it has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure. Therefore, it is an important research problem to construct a secure ID-based multi-signcryption scheme without random oracles.

In this paper, motivated by Malone-Lee's ID-based signcryption scheme and Waters' ID-based encryption scheme, we define formal model of ID-based multi-signcryption scheme and propose the first ID-based multi-signcryption scheme without random oracles. Our scheme is proved secure against adaptive chosen ciphertext attacks and adaptive chosen message attacks. The research is supported by the National Natural Science Foundation of China under Grant No. 60873232 and the Natural Science Foundation of Shandong province under Grant No. Y2007G37. The projects focus on the study of foundational problem in multi-party oriented cryptography including the study of secure and efficient encryption scheme, signature scheme and key agreement protocols in multi-party setting.