An Efficient Identity-based Multi-signcryption Scheme

Z.H. Qi, H.C. Yang, H. Huang
School of Computer Science and Technology
Nanjing University of Posts and Telecommunications
Nanjing, China

***Abstract*—It is important to improve the efficiency of identity-based multi-signcryption schemes. There already have some schemes proposed. In this paper, we present an efficient identity-based multi-signcryption scheme which uses the bilinear pairing on elliptic curves and combines identity-based encryption algorithm with the multi-sender signature algorithm. We firstly present the framework of identity-based multi-signcryption schemes, then proved the correctness and analyzed the security and the computational efficiency of the new scheme in standard model. The results show that when the number of signcrypters is *n* (*n*>1), the new scheme reduced by *n*-1 exponentiations is a safe and more efficient multi-signcryption scheme.**

Keywords-index terms-identity-based; multi- signcryption; standard model; bilinear pairing

I. INTRODUCTION

The ID-based multi-signcryption scheme attracted people's attention when the same message needs to be signcrypted by more than one signcrypter then send to the receivers. In 2001, Mitomi[1] proposed an ID-based multi-signcryption scheme but didn't provide the security analysis. In 2010, ZHANG[2] presented the first ID-based multi-signcryption scheme without Random oracles. In 2012, Li[3] also proposed a multi-signcryption scheme, but like the analysis of the Gu's scheme[4] in Ref.[5], this scheme does not meet the unforgeability of signcryption. There also have some aggregate schemes[6,7], which is similar to the multi-signcryption. Aggregate signature allows aggregation of different signatures by n different users ID_i on different messages m_i. The aggregate signature also has a wide range of real world applications .

In this paper, motivated by ZHANG's scheme, we proposed an efficient ID-based multi-signcryption scheme. In ZHANG's scheme, all signcrypters should calculate *w*, but in our scheme, only need the specified signcrypter compute the *w*. Compared with ZHANG's program, the biggest improvement of our program is the computational efficiency, when the number of signcrypter is *n*(*n*>1),the exponentiation decreased from *n* to 1 during signcrypt. The scheme is proved secure against adaptive chosen ciphertext attacks and adaptive chosen message attacks under decidability bilinear Diffie-Hellman assumption and computational Diffie-Hellman assumption respectively.

II. IDENTITY-BASED MULTI-SIGNCRYPTION SCHEME

In the section, we describe our ID-based multi-signcryption scheme.

(i) Setup. Given a security parameter *k*, PKG chooses two groups, *G and* G_T, of the same prime order $q>2^k$,a bilinear map $e:G\times G\rightarrow G_T$,a generator *g* of *G* and two cryptographic hash functions described as follow: $Hu:\ \{0,1\}^* \rightarrow \{0,1\}^{n_u}$, $Hm:\ \{0,1\}^* \rightarrow \{0,1\}^{n_m}$. Then the PKG picks a random generator $g_2\in G$ and a random secret $\alpha\in Z_q$, compute $g_1=g^\alpha\in G$. Now, randomly selected $u'\in Z_q$,$m'\in G$ and vectors $U_u=(u_i)$, $M_m=(m_i)$ ($u_i\in_R Z_q$, $m_i\in_R G$) of length n_u and n_m ,respectively. The public parameters are $\pi=\{G, G_T, e, g, g_1, g_2, u', U_u, m', M_m, H_u, H_m\}$ and the master secret is g_2^{α} .

(ii) Extract. For a user *j* whose identity information is ID_j, PKG computes $U_j=H_u(ID_j)$,then U_j is a bit string of length n_u and let *U[i]* be the i-th bit of U_j. Define $U_j' \subset \{1,2,\cdots,n_u\}$ to be the set of subscripts *i* such that *U[i]=1*. Now, randomly picked $r_j\in Z_q$ and compute the private key d_j of the user *j*, $d_j=(d_{j1},d_{j2})=(g_2^{\alpha}(u'\prod_{i\in U_j'}u_i)^{r_j}, g^{r_j})$. Therefore, the private keys of signcrypters with identity $U_{Ai}(i=1,2,\cdots n)$ and the receiver are as $d_{Ai}=(g_2^{\alpha}(u'\prod_{j\in U_{Ai}'}u_j)^{r_{Ai}}, g^{r_{Ai}})$, $d_B=(g_2^{\alpha}(u'\prod_{j\in U_B'}u_j)^{r_B}, g^{r_B})$.

(iii) Multi-signcrypt. Let *m* be the message to be transmitted, compute $M=H_m(m)$,then M is a bit string of length n_m and let *M[j]* be the j-th bit of *M*. Define $M'\subset\{1,2,\cdots,n_m\}$ to be the set of subscripts *j* such that *M[j]=1*. Each signcrypter picks $r_i\in Z_p$ randomly and computes $\sigma_{i1}=g^{r_i}$, $\sigma_{i2}=d_{A_{i2}}$, $\sigma_{i3}=d_{A_{i1}}(m'\prod_{j\in M'}m_j)^{r_i}$. Then sent $(\sigma_{i1},\sigma_{i2},\sigma_{i3})$ to the specified signcrypter A_j, who is one of the signcrypters. Assume that A_j randomly selected number is r_j. To avoid confusion, let $r_c=r_j$. A_j computes as $\omega=(e(g_1,g_2)e(d_{B2},u'\prod_{j\in U_B'}u_j))^{r_c}$, $M=H_m(m\,||\,\omega)$, $c=m\oplus H(\omega)$, $\sigma_1=\prod_{i=1}^{n}\sigma_{i1}$, $\sigma_2=\{\sigma_{i2}\mid i=1,2,\cdots n\}$, $\sigma_3=\prod_{i=1}^{n}\sigma_{i3}$, $\sigma_4=g^{r_c}$. Then the resultant ciphertext is $\sigma=(c,\sigma_1,\sigma_2,\sigma_3,\sigma_4)$.

(iv) Unsigncrypt. When Bob receives a ciphertext, decrypts the ciphertext as follows: computes $\omega = e(\sigma_4, d_{B1})$, $m = c \oplus H(\omega)$, $M = H(m \| \omega)$.Accept the message if and only if the following equality holds: $e(\sigma_3, g) = e(g_1, g_2)^n \prod_{i=1}^{n} e(u' \prod_{j \in U'_{A_i}} u_j, d_{A_{i2}}) e(m' \prod_{j \in M'} m_j, \sigma_1)$.

III. ANALYSIS OF OUR SCHEME

A. Correctness

The correctness of the scheme can be verified as follows:

$$e(\sigma_3, g) = e(\prod_{i=1}^{n} \sigma_{i3}, g) = e(\prod_{i=1}^{n} d_{A_{i1}} (m' \prod_{j \in M'} m_j)^{r_i}, g) = e(\prod_{i=1}^{n} d_{A_{i1}}, g) e(\prod_{i=1}^{n} (m' \prod_{j \in M'} m_j)^{r_i}, g)$$

$$= e(\prod_{i=1}^{n} g_2^{a} (u' \prod_{j \in U'_{A_i}} u_j)^{r_{ui}}, g) e((m' \prod_{j \in M'} m_j)^{r_i}, g) = e(g_1, g_2)^{a} \prod_{i=1}^{n} e(u' \prod_{j \in U'_{A_i}} u_j, d_{A_{i2}}) e(m' \prod_{j \in M'} m_j, \sigma_1)$$

$$\omega = e(\sigma_4, d_{B1}) = e(g^{r_c}, g_2^{a} (u' \prod_{j \in U'_B} u_j)^{r_B}) = e(g^{r_c}, g_2^{a}) e(g^{r_c}, (u' \prod_{j \in U'_B} u_j)^{r_B})$$

$$= (e(g_1, g_2) e(d_{B2}, u' \prod_{j \in U'_B} u_j))^{r_c}$$

B. Security Analysis

Theorem 1. Assuming that there has an adversary Λ who is able to distinguish two valid ciphertexts with an advantage ε, and asks at most q_E extraction queries, q_S multi-signcryption queries and q_U unsigncryption queries. Then there exists a distinguisher C that can solve an instance of the Decisional Bilinear Diffie-Hellman problem with an advantage $\dfrac{\varepsilon}{8(q_E + q_S + q_U)(n_u + 1)(n_m + 1)}$.

Proof. Assuming that the distinguisher C receives a random DBDH problem instance $(g, g^a, g^b, g^c, \alpha \in G_T)$, his goal is to judge whether $\alpha = e(P, P)^{abc}$ or not. C will run the adversary Λ as a subroutine. Our proof is based on Water's idea such as in Ref. [8, 9].

Step 1: Two integers, k_u and $k_m, (0 \le k_u \le n_u, 0 \le k_m \le n_m)$;

Step2: An integer $x' \in Z_{l_u}$, an n_u -dimensional vector $X = (x_i), x_i \in Z_{l_u}$;

Step 3: An integer $z' \in Z_{l_m}$, an n_m -dimensional vector $Z = (z_i), z_i \in Z_{l_m}$;

Step 4: Two integers $y', w' \in Z_q$, an n_u -dimensional vector $Y = (y_i), y_i \in Z_q$ and an n_m -dimensional vector $W = (w_i), w_i \in Z_q$.

For ease of analysis, we define the functions as follows for an identity u and a message m respectively: $F(u) = -l_u k_u + x' + \sum_{i \in U_u} x_i, J(u) = y' + \sum_{i \in U_u} y_i$, $K(m) = -l_m k_m + z' + \sum_{i \in M} z_i, L(m) = w' + \sum_{i \in M} w_i$.

Then the challenger assigns a set of public parameters as $g_1 = g^a, g_2 = g^b, u' = g_2^{-l_u k_u + x'} g^{y'}, u_i = g_2^{x_i} g^{y_i} \ (1 \le i \le n_u)$, $m' = g_2^{-l_m k_m + z'} g^{w'}, m_j = g_2^{z_j} g^{w_j} (1 \le j \le n_m)$

Under this designed, these public parameters have the same probability distribution as in the real situation. At this time, for any identity u and any message 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. C answers the adversary Λ's queries as follows:

(i) Extraction queries

When the adversary Λ asks for the private key corresponding to an identity u, checking whether the equation $F(u) = 0 \bmod q$ is satisfied. If established, the simulation process is terminated; otherwise, the distinguisher C picks $t_u \in Z_q$ randomly and gives adversary Λ the simulation of the private key $d_u = (d_{u1}, d_{u2}) = (g_1^{\frac{-J(u)}{F(u)}} (u' \prod_{i \in U'} u_i)^{r_u}, g_1^{\frac{-1}{F(u)}} g^{r_u})$. Let $\hat{r}_u = r_u - \dfrac{a}{F(u)}$, so $d_{u1} = g_1^{\frac{-J(u)}{F(u)}} \left(g_2^{F(u)} g^{J(u)}\right)^{r_u} = g_2^{a} (g_2^{F(u)} g^{J(u)})^{\hat{r}_u}$, $d_{u2} = g_1^{\frac{-1}{F(u)}} g^{r_u} = g^{r_u - \frac{a}{F(u)}} = g^{\hat{r}_u}$. Therefore, d_u is a valid private key for identity u.

To make it sample, assume that $0 \le l_u (n_u + 1) \le q, 0 \le k_u \le n_u, F(u) = -l_u k_u + x' + \sum_{i \in U_u} x_i$ which implies $0 \le l_u k_u \le q, 0 \le x' + \sum_{i \in U_u} x_i$. Hence, $F(u) = 0 \bmod q$ implies $F(u) = 0 \bmod l_u$, $F(u) \ne 0 \bmod l_u$ implies $F(u) \ne 0 \bmod q$. Thus, $F(u) \ne 0 \bmod l_u$ will be the prerequisite to the success of faking secret key.

(ii) Multi-signcryption queries

At any time, the adversary Λ can perform a 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 $F(u_{A_i}) \ne 0 \bmod l_u$, C first generates a private key for u_{A_i} ,then runs Multi-signcrypt $(m, d_{A_1}, d_{A_2} \cdots d_{A_n}, ID_B)$ to answer the adversary's query. Otherwise, C will direct abort.

(iii) Unsigncryption queries

At any time, the adversary Λ can perform an unsigncryption query for a ciphertext σ. If $F(u_B) \ne 0 \bmod l_u$, C first generates a private key for u_B by running the extract algorithm, then runs Unsigncrypt $(\sigma, d_B, ID_{A_1}, ID_{A_2}, \cdots, ID_{A_n})$ to answer the adversary's query. Otherwise, C will direct abort.

Challenge. After a ploynomially bounded number of queries, the adversary chooses signcrypters and receiver's identities $u^*_{A_1},\cdots,u^*_{A_n},u^*_B$. C will abort the game if the adversary has asked the private key corresponding to identity u^*_B during the first stage. Otherwise, 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 C. C will abort game if $F(ID^*_j)=0 \bmod l_u$. Else, C randomly picks r and C will abort game if $K(M^*_r)=0 \bmod p$ where $M^*_r = H_m(m_r \,||\, Ze(d^*_{B2}, C_2^{J(u^*_B)}))$. Otherwise, C sets a multi-signcryption ciphertext of m_c as: $(m_r \oplus H(Ze(d^*_{B2}, C_2^{J(u^*_B)}), C_1, \{d^*_{A_{i2}} \mid i=1,2,\cdots,n\}, \prod_{i=1}^{n} d^*_{A_{i1}} C_1^{L(M_r)}, C_2)$.

Let $c = r_C$ $c_1 = \sum_{i=1}^{n} r_i$ $Z = e(g,g)^{abc}$, $C_1 = g^{c_1}$, $C_2 = g^c$, the simulation is perfect since $Ze(d^*_{B2}, C_2^{J(U^*_B)}) = e(g,g)^{abc} e(d^*_{B2}, g^{cJ(U^*_B)}) = (e(g_1,g_2)e(d^*_{B2}, U'\prod_{j\in U^*_B} U_j))^{r_C} = \omega$.

Second stage. The adversary Λ performs a series of queries, and C answers these queries in the same way as in the first stage. But Λ didn't allowed to extract the private key corresponding to u^*_B and make an unsigncryption query for σ under u^*_B. Guess. At the end, the adversary Λ outputs a guess r' of r. If $r'=r$, C answers 1 indicating that $Z = e(g,g)^{abc}$; Otherwise, C answers 0 to the DBDH problem. Probability of analog success. To complete the simulation, we need to satisfy the following conditions: (a) Extraction queries on an identity u satisfy $F(u)\neq 0 \bmod l_u$; (b) Multi-signcryption queries on a message m satisfy $F(u_i)\neq 0 \bmod l_u, i\in[1,n]$; (c) Unsigncryption queries on a ciphertext σ satisfy $F(u_B)\neq 0 \bmod l_u$; (d) In the challenge stage, have $F(u^*_B)=0 \bmod p$ and $K(M^*_r)=0 \bmod p$.

Let $u_1,\cdots,u_{q_I}$ be the identity appearing in queries not involving the challenge identity. To express clearly, assuming that $q_I \le q_E+q_S+q_U$. Define the events $A_i: F(u_i)\neq 0 \bmod l_u, i=1,2,\cdots,q_I$, $A': F(u^*_B)$ =0 mod p; $B^*: K(M^*_r)=0 \bmod p$. Then the probability of the adversary Λ not aborting the game is $Pr[\overline{abort}] \ge Pr[\bigwedge_{i=1}^{q_I} A_i \wedge A' \wedge B^*]$. For the function F and K are selected independently, so $\bigwedge_{i=1}^{q_I} A_i \wedge A'$ and B^* are mutually independent events. Firstly, $Pr[A'] = Pr[F(u^*)=0 \bmod p] = Pr[F(u^*)= = \frac{1}{l_u}\frac{1}{n_u+1}$.

Similarly, we have $Pr[B^*] = \frac{1}{l_m}\frac{1}{n_m+1}$. By combining the above result, we have $Pr[\overline{abort}] \ge \frac{1}{8(q_E+q_S+q_U)(n_u+1)q_S(n_m+1)}$. . If the simulation does not abort, the C can solve the DBDH problem with probability $\frac{\varepsilon}{8(q_E+q_S+q_U)(n_u+1)q_S(n_m+1)}$.

IV. Conclusion

In this paper, we have modified the proposed ID-based multi-signcryption scheme to adapt for our ID-based multi-signcryption scheme. The computational efficiency of our scheme is improved compared with proposed schemes and the confidentiality and unforgeability have been formally defined in our security model. In the scheme,only need the specified signcrypter calculated *w*, so when the number of signcrypter is n(n>1), the exponentiation reduced (n-1). In the future work, how to continue to improve the computational efficiency and shorten the length of ciphertext remains need further research.

Acknowledgements

This work is supported by National Natural Science Foundation of China (61073188), China Postdoctoral Science Foundation (20100471355) and Natural Science Foundation of Jiangsu Province (BK2009426).

References

[1] Mitomi S. & Miyaji A., A general model of multi-signature schemes with message flexibility, order flexibility and order verifiability. *IEICE Transactions on Fundamentals*, **84(10)**, pp. 2488-2499, 2001.

[2] Zhang Bo & Xu Qiuliang, Identity-Based Multi-Signcryption Scheme without Random Oracles. *CHINESE JOURNAL OF COMPUTERS*, **33(1)**, pp. 103-109, 2010.

[3] Li Cong, Yan Deqin, Zheng Hongliang, Efficient and secure identity-based multi-signcryption scheme in standard model. *Journal of computer Applications*, **34(4)**, pp. 957-959, 2012.

[4] Gu Ke, Jia WeiJia, Jiang ChunLing,Efficient and Secure Identity-Based Signature Scheme. *Journal of Software*, **22(6)**, pp. 1350−1360. 2011.

[5] Huang Bin & Deng Xiaohong, Cryptanalysis of efficient identity-based signature scheme. *Journal of computer Applications*, **33(1)**, pp. 168-170, 2013.

[6] XunYi Ren, ZhengHua Qi & Geng, Provably Secure Aggregate Signcryption Scheme. *ETRI journal*, **34(3)**, pp. 421-428, 2012.

[7] S.S.D. Selvi et al., Identity Based Aggregate Signcryption Schemes.*INDOCRYPT, LNCS*, **5922**, pp. 378-397, 2009.

[8] Water R., Efficient identity based encryption without random oracles. *Proc. of the EUROCRYPT*, Aarhus, Denmark, pp. 114-127, 2005.

[9] Paterson K & Schuldt J, Efficient identity based signatures secure in the standard model. *Proc. of the ACISP* , Melbourne, Australia, pp. 207-222, 2006.