2011 International Conference on Computer Science and Information Technology (ICCSIT 2011)
IPCSIT vol. 51 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V51.70

An Efficient Identity-based Ring Signcryption Scheme

Sun Hua[1, +], Guo Li[2] and Wang Aimin[1]

[1]School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China
[2]Party School of CPC Anyang Municipal Committee, Anyang 455000, China

Abstract. This paper presents an identity based ring signcryption scheme without random oracle by using bilinear pairings. The size of the ciphertext is a constant and independent of the size of the ring. By introducing the selective identity and selective chosen message attack model, we prove unforgeability of the scheme under the hardness of DHI problem and prove its indistinguishability against selective identity and chosen ciphertext attack under the hardness of DBDHE problem. This scheme is more efficient compared with other ring signcryption schemes.

Key words: Ring Signcryption; Bilinear Pairing; Decisional Bilinear Diffie-Hellman Exponent Problem; Diffie-Hellman Inversion Problem

1. Introduction

In 1984, Shamir[1] first proposed the identity-based cryptography which eliminates the operation of certificate in the conventional PKI system, and simplifies the key management. Boneh[2]put forward the first practical identity-based encryption scheme. Then some of the identity-based encryption schemes [3,4,5] and signature schemes[6,7] were proposed in the standard model successively.

Confidentiality and authentication are the two most basic services in public-key cryptography. The encryption scheme aims to provide confidentiality, while the digital signature provides certification and non-repudiation. At present, it requires to achieve the two attributes simultaneously in many practical cryptography applications.

In 1997, Zheng[8] first put forth the concept of signcryption. Namely it can achieve the functions of encryption and signature simultaneously in a reasonable step, while the computation cost are lower than the traditional signature and encryption respectively. The deficiencies of signcryption is enlarging the final ciphertext, and increasing the sender and receiver's computing time. Later on some efficient signcryption schemes was put forward. Baek[9] first proposed a proved secure signcryption scheme in the formal security model. The literature[10,11] combined identity-based signature with encryption to generate identity-based signcryption scheme which was merely proved secure in the random oracle model.

The user can signcrypt the message under a potential set of receivers without revealing who has actually produced it in the ring signcryption scheme. Therefore, the message of ring signcryption own anonymity in addition to authentication and confidentiality. To combine identity-based cryptography with ring signcryption can get the identity-based ring signcryption with the advantages of them. Huang[12] first put forward identity-based ring signcryption scheme with inefficient computation. Zhang[13] proposed identity-based ring signcryption scheme in which the real sender can verifies that the signcryption is generated by himself. Yu[14] posed another ring signcryption, however, the scheme was not adaptive chosen-ciphertext secrure.

[+] Sun Hua. Tel.:13703726634.
E-mail address: sh1227@163.com.

At present, most of the ring signcryption schemes were proved secure in the random oracle model, and the length of the ciphertext grows with the size of ring in linear. Therefore, it is more practical to design an identity-based ring signcryption scheme with constant size ciphertext proved secure in the standard model.

2. Preliminaries

2.1. Bilinear Pairing

Let G and G_T denote two cyclic groups of the same large prime q and g is the generator of group G. For us a bilinear pairing is a map $e: G\times G \to G_T$ with the following properties:

1)Bilinear: For all $P,Q\in G$ and $a,b\in Z$, we have $e\left(P^a,Q^b\right)=e\left(P,Q\right)^{ab}$;

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

3)Computable: There is an effecient algorithm to compute $e\left(P,Q\right)$, for all $P,Q\in G$.

2.2. Assumption Problem

Definition 1：(DBDHE assumption**)** Given $g,h,T,g^{\alpha^i}\in G$, $i=1,...,l-1,l+1,...,2l$, determine whether $T=e\left(g,h\right)^{\alpha^l}$ is true or not.

We say (ε, t, l)-DBDHE assumption is established, if there is no polynomial time algorithm t with non-negligible probability ε to solve the n-DHI problem .

Definition 2：(n-DHI assumption**)** Given $g,g^{\alpha},g^{\alpha^2},...,g^{\alpha^n}\in G$, where $\alpha\in\mathbb{Z}_p^*$ is unknown, compute $g^{\alpha^{n+1}}$.

We say (ε, t, n)-DHI assumption is established, if there is no polynomial time algorithm t with non-negligible probability ε to solve n-DHI problem.

3. An Identity-Based Ring Signcryption Scheme with Constant Size Ciphertext

3.1. Scheme Description

Let two hash functions $H_1:\{0,1\}^*\to\mathbb{Z}_p^*$ and $H_2:\{0,1\}^*\to\mathbb{Z}_p^*$ map arbitrary length of identity ID and message m to two non-zero integer. The scheme is described as following :

Setup： Select $e:G\times G\to G_T$,and g is G' generator. Select $\alpha\in\mathbb{Z}_p$, $g_2\in G$ and compute $g_1=g^{\alpha}$. Select $u'\in_R G$, vector $\hat{U}=\left(\hat{u}_1,\hat{u}_2,\cdots,\hat{u}_n\right)\in G^n$. Then the system public parameter is $params=\left(G,G_T,e,g,g_1,g_2,u',\hat{U}\right)$, and the master-key is $msk=g_2^{\alpha}$.

Extract： For identity ID, let $id=H_1(ID)$, select $r_i\in\mathbb{Z}_p^*$ at random, $1\le i\le n+1$, the private key of identity ID is:

$$\begin{aligned}d_{ID}&=\left(g_2^{\alpha}\left(u'\hat{u}_i^{id}\right)^{r_i},g^{r_i},\hat{u}_1^{r_i},...,\hat{u}_{i-1}^{r_i},\hat{u}_{i+1}^{r_i},...,\hat{u}_n^{r_i}\right)\\&=\left(a_0,b_0,c_1,...,c_{i-1},c_{i+1},...,c_n\right)\end{aligned}$$

Signcrypt： Let $L=\left\{ID_1,...,ID_{n'}\right\}$ be a set of n' members in ring L including the actual signer ID_k, $id_i=H_1(ID_i)$, $1\le i\le n'$, m is the message to encrypt, $\mathrm{m}=H_2(m,L)$. Let the identity of signcryption receiver be ID_r, $id_r=H_1(ID_r)$, the private key of signer is d_{ID_k}.

The signer select $t\in\mathbb{Z}_p$ at random, compute $C_1=g^t$, $C_2=a_{k,0}\left(\prod_{j=1,j\neq k}^{n'}c_{k,j}^{id_j}\right)c_{k,n'+1}^{\mathrm{m}}\left(u'\hat{u}_1^{id_1}\cdots\hat{u}_{n'}^{id_{n'}}\hat{u}_{n'+1}^{\mathrm{m}}\right)^t$, $C_3=b_{k,0}g^t$, $C_4=\left(u'\hat{u}_r^{id_r}\right)^t$, $C_5=e\left(g_1,g_2\right)^t\oplus\left\langle m,ID_k,C_2,C_3\right\rangle$, and generate the signcryption $c=\left(C_1,C_2,C_3,C_4,C_5\right)$.

Unsigncrypt： The receiver ID_r receive the signcryption c, then compute as following:

1) Receiver ID_r compute $W=e\left(C_1,a_{r,0}\right)\cdot e\left(C_4,b_{r,0}\right)^{-1}$ with his private key $d_{ID_r}=\left(a_{r,0},b_{r,0},c_{r,1},...,c_{r,i-1},c_{r,i+1},...,c_{r,n}\right)$.

2) From $\langle m, ID_k, C_2, C_3 \rangle = C_5 \oplus W$, ring members group $L = \{ID_1, ..., ID_n\}$, compute $\mathrm{m} = H_2(m, L)$, when the equation $e(g, C_2) = e(g_1, g_2) \cdot e\left(C_3, u' \hat{u}_1^{id_1} \cdots \hat{u}_{n'}^{id_{n'}} \hat{u}_{n'+1}^{\mathrm{m}}\right)$ is true, then c is an efficient ring signcryption.

3.2. Correctness

The correctness of the scheme can be easily proved by the following equations:

From $d_{ID_r} = \left(a_{r,0}, b_{r,0}, c_{r,1}, ..., c_{r,i-1}, c_{r,i+1}, ..., c_{r,n}\right)$ we can obtain:

$$
\begin{aligned}
W &= e\left(C_1, a_{r,0}\right) \cdot e\left(C_4, b_{r,0}\right)^{-1} \\
&= e\left(g^t, g_2^{\alpha}\left(u' \hat{u}_r^{id_r}\right)^{r_r}\right) \cdot e\left(g^{r_r}, \left(u' \hat{u}_r^{id_r}\right)^t\right)^{-1} \\
&= \frac{e\left(g^t, g_2^{\alpha}\right) \cdot e\left(g^t, \left(u' \hat{u}_r^{id_r}\right)^{r_r}\right)}{e\left(g^{r_r}, \left(u' \hat{u}_r^{id_r}\right)^t\right)} \\
&= e\left(g_2, g_1\right)^t
\end{aligned}
$$

then we can verify the signcryption c :

$$
\begin{aligned}
e(g, C_2) &= e\left(g, a_{k,0}\left(\prod_{j=1, j \neq k}^{n'} c_{k,j}^{id_j}\right) c_{k,n'+1}^{\mathrm{m}}\left(u' \hat{u}_1^{id_1} \cdots \hat{u}_{n'}^{id_{n'}} \hat{u}_{n'+1}^{\mathrm{m}}\right)^t\right) \\
&= e\left(g, g_2^{\alpha}\left(u' \hat{u}_1^{id_1} \cdots \hat{u}_{n'}^{id_{n'}} \hat{u}_{n'+1}^{\mathrm{m}}\right)^{r_k+t}\right) = e(g_1, g_2)\, e\left(C_3, u' \hat{u}_1^{id_1} \cdots \hat{u}_{n'}^{id_{n'}} \hat{u}_{n'+1}^{\mathrm{m}}\right)
\end{aligned}
$$

4. Conclusion

The paper proposes an identity-based ring signcryption scheme with constant size ciphertext. This scheme need not the random oracle and is proved secure in the standard model. Compared with the existing ring signcryption schemes, the length of the ciphertext is a constant and independent of the size of the ring . We can prove the unforgeability of the scheme and the indistinguishability of the scheme under the hardness of DHI problem and DBDHE problem. This scheme is more efficient compared with other ring signcryption schemes.

5. References

[1] Shamir A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Crypto 1984, volume 196 of LNCS, Springer-Verlag, 1985: 47-53.

[2] Boneh D,Franklin M. Identity-based encryption from the Weil pairing[C]//Proceedings of Crypto 2001, volume 2139 of LNCS, 213-229.

[3] Boneh D,Boyen X. Efficient selective-id secure identity based encryption without random oracles [C]//Proceedings of EUROCRYPT 2004, volume 3027 of LNCS, Springer-Verlag, 2004: 223-238.

[4] Boneh D,Boyen X. Secure identity based encryption without random oracles[C]//Proceedings of CRYPTO 2004, volume 3152 of LNCS, Springer-Verlag, 2004: 443-459.

[5] Gentry C. Practical identity-based encryption without random oracles[C]//Proceedings of EUROCRYPT 2006, volume 4004 of LNCS, Springer-Verlag, 2006: 445-464.

[6] Paterson K G,Schuldt J C N. Efficient identity-based signatures secure in the standard model[C]//Proceedings of ACISP 2006, volume 4058 of LNCS, 207-222.

[7] Ren Yanli ,Gu Dawu . Efficient hierarchical identity based signature scheme in the standard model[J]. Wuhan University Journal of Natural Sciences, volume 13, 2008: 665-669.

[8] Zheng Yuliang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [C]//Advances in Cryptology-Crypto 1997, volume 1294 of LNCS, Springer-Verlag, 1997: 165-179.

[9] Baek J,Steinfeld R, Zheng Yuliang . Formal proofs for the security of signcryption[C]//Proceedings of PKC 2002, volume 2274 of LNCS, Springer-Verlag, 2002: 363-366.

[10] Malone-Lee J. Identity-based signcryption[J]. Cryptology ePrint Archive, Report 2002/098, 2002. http://eprint.iacr.org/.

[11] Libert B,Quisquater J J. New identity based signcryption schemes from pairings[J]. Cryptology ePrint Archive, Report 2003/023, 2003. http://eprint.iacr.org/.

[12] Huang Xinyi , Susilo W, Mu Yi et al. Identity-based ring signcryption schemes: cryptographic primitives for preserving privacy and authenticity in the ubiquitous world[C]// Advanced Information Networking and Application 2005, volume 2, 649-654.

[13] Zhang Mingwu , Yang Bo , Zhu Shenlin et al. Efficient secret authenticatable anonymous signcryption scheme with identity privacy[C]//Proceedings of the PAISI 2008, volume 5075 of LNCS, Springer-Verlag, 2008: 126-137.

[14] Yu Yong, Li Fagen, Xu Chunxiang et al. An efficient identity-based anonymous signcryption scheme[J]. Wuhan University Journal of Natural Sciences, volume 13, 2008: 670-674.