An Efficient Identity-based Ring Signcryption Scheme

Sun Hua\textsuperscript{1,}\textsuperscript{+}, Guo Li\textsuperscript{2} and Wang Aimin\textsuperscript{1}

\textsuperscript{1}School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China
\textsuperscript{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\cite{1} first proposed the identity-based cryptography which eliminates the operation of certificate in the conventional PKI system, and simplifies the key management. Boneh\cite{2} put forward the first practical identity-based encryption scheme. Then some of the identity-based encryption schemes \cite{3,4,5} and signature schemes\cite{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\cite{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\cite{9} first proposed a proved secure signcryption scheme in the formal security model. The literature\cite{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\cite{12} first put forward identity-based ring signcryption scheme with inefficient computation. Zhang\cite{13} proposed identity-based ring signcryption scheme in which the real sender can verifies that the signcryption is generated by himself. Yu\cite{14} posed another ring signcryption, however, the scheme was not adaptive chosen-ciphertext secure.
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 \( e: G \times G \rightarrow G_T \) with the following properties:

1) Bilinear: For all \( P, Q \in G \) and \( a, b \in \mathbb{Z} \), we have \( e(P^a, Q^b) = e(P, Q)^{ab} \);
2) Non-degenerate: \( e(g, g) \neq 1 \);
3) Computable: There is an efficient algorithm to compute \( e(P, Q) \), for all \( P, Q \in G \).

2.2. Assumption Problem

Definition 1: (DBDHE assumption) Given \( g, h, T, g^a \in G \), \( i = 1, \ldots, l - 1, l + 1, \ldots, 2l \), determine whether \( T = e(g, h)^i \) is true or not.

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

Definition 2: (n-DHI assumption) Given \( g, g^a, g^x, \ldots, g^{x_n} \in G \), where \( \alpha \in \mathbb{Z}_p \) is unknown, compute \( g^{\alpha x_n} \).

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

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

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

Setup: Select \( e: G \times G \rightarrow G_T \) and \( g \) is \( G^* \) generator. Select \( \alpha \in \mathbb{Z}_p \), \( g_2 \in G \) and compute \( g_1 = g^\alpha \). Select \( u^1 \in gG \), vector \( \hat{U} = (\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_n) \in G^n \). Then the system public parameter is \( \text{params} = (G, G_T, e, g, g_1, g_2, u^1, \hat{U}) \), and the master-key is \( \text{msk} = g_2^\alpha \).

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

\[
d_{id} = \left( g_2^{u_i \hat{u}_i}, g^{\hat{u}_i}, \ldots, \hat{u}_1, \hat{u}_2, \ldots, \hat{u}_n \right) = (a_0, b_0, c_1, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n)
\]

Signcrypt: Let \( L = \{ID_1, \ldots, ID_n\} \) be a set of \( n \) members in ring \( L \) including the actual signer \( ID_k \), \( id = H_1(ID) \), \( 1 \leq i \leq n \), \( m \) is the message to encrypt, \( m = H_1(m, L) \). Let the identity of signcryption receiver be \( ID_{\alpha} \), \( id = H_1(ID_{\alpha}) \), the private key of signer is \( d_{ID_{\alpha}} \).

The signer select \( t \in \mathbb{Z}_p \) at random, compute \( C_1 = g^t \), \( C_2 = a_k \prod_{j=1, j \neq 2}^{i-1} c_{k+j}^{a_{id_j}} \left( u_1^{a_{id_1}} \cdots u_n^{a_{id_n}} \right)^{i-1} \), \( C_3 = b_k \theta g^t \), \( C_4 = \left( u_1^{a_{id_1}} \cdots u_n^{a_{id_n}} \right) \), \( C_5 = e(g_1, g_2) \oplus \{m, ID_k, C_2, C_3\} \), and generate the signcryption \( c = (C_1, C_2, C_3, C_4, C_5) \).

Unsigncrypt: The receiver \( ID_{\alpha} \) receive the signcryption \( c \), then compute as following:

1) Receiver \( ID_{\alpha} \) compute \( w = e(C_1, a_{id_\alpha}) \cdot e(C_4, b_{id_\alpha})^{-1} \) with his private key \( d_{ID_{\alpha}} = (a_{id_\alpha}, b_{id_\alpha}, c_{i+1}, \ldots, c_{i-1}, c_{i+1}, \ldots, c_n) \).
2) From \( \{m, ID_1, C_2, C_3\} = C_3 \oplus W \), ring members group \( L = \{ID_1, \ldots, ID_n\} \), compute \( m = H_2(m, L) \), when the equation \( e(g, C_2) = e(g, g) \cdot e\left(C_3, \prod_{i=1}^{n} u_i^{id_i} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right) \) 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 \( d_{bi} = (a_{r0}, b, c, \ldots, c_r, \ldots, c_{rn}) \) we can obtain:

\[
W = e(C_1, a_{r0}) \cdot e(C_1, b_{r0})^{-1} \\
= e\left(g', g_s^{-1} \left(\prod_{j=1}^{i} u_j^{id_j} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)^{-1}\right) \\
= e\left(g', \left(\prod_{j=1}^{i} u_j^{id_j} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)^{-1}\right) \\
= e\left(g', \left(\prod_{j=1}^{i} u_j^{id_j} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)^{-1}\right) \\
= e\left(g_{2r}, g_1\right)
\]

then we can verify the signcryption \( c \):

\[
e(g, C_2) = e\left(g, a_{s0} \left(\prod_{i=1}^{n} c_i^{-1} \cdots \prod_{j=1}^{i} u_j^{id_j} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)\right) \\
= e\left(g, g_s^{-1} \left(\prod_{j=1}^{i} u_j^{id_j} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)^{-1}\right) \\
= e(g, g) \cdot e\left(C_3, \prod_{i=1}^{n} u_i^{id_i} \cdots u_n^{id_n} \bar{u}_{n+1}^{id_{n+1}}\right)
\]

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


