On the Security of Zhang–Wu–Wang’s Forward-Secure Group Signature Scheme in ICICS’03

Ping Wang, Xiaofeng Chen, and Kwangjo Kim

International Research center for Information Security (IRIS) and
Information and Communications University (ICU), Korea

Abstract

A group signature scheme allows a group member to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of the actual signer can be revealed by a designated entity. J. Zhang, Q. Wu, and Y. Wang proposed a novel efficient group signature scheme with forward secrecy at ICICS 2003. Later, Guilin Wang pointed out this scheme is linkable, untraceable, and forgeable at ICISC 2003. Furthermore, in this paper we show that this scheme is not coalition-resistant.

I. Introduction

The concept of group signature was introduced by Chaum and van Heyst [1] in 1991. It allows any member of a group to sign messages anonymously on behalf of the group. The signature can also be verified by using a single group key. However, in case of a dispute, a designated group manager can reveal the signer of a valid group signature. Furthermore, any two signatures produced by the same signer are unlinkable by anyone else with the sole exception of a designated group manager. The salient features of group signatures make them attractive for many specialized applications, such as e-voting, e-bidding and e-cash systems [2, 3, 4]. Many group signature schemes have been proposed after the initial work [5, 6, 7, 8, 9, 10].

The concept of forward secrecy was proposed by Ross Anderson [11] for traditional signatures. In 2001, Song [12] firstly presented a practical forward secrecy group signature scheme. J. Zhang, Q. Wu, and Y. Wang [13] proposed a novel efficient group signature scheme with forward security at ICICS 2003, and as they claimed their scheme is a little more efficient than Song’s scheme. Later, Guilin Wang [14] pointed out this scheme is linkable, untraceable, and forgeable at ICISC 2003. Furthermore, in this paper we show that this scheme is not coalition-resistant, i.e., a colluding subset of group members can generate a valid group signature that can not be traced by the group manager.

The rest of this paper is organized as follows. In Section II, we will introduce the definition of a forward-secure group signature scheme and the security properties. Section III reviews Zhang–Wu–Wang scheme. Then, our security analysis is presented in Section IV. Finally, we conclude this paper in Section V.

This work was supported by a grant No. R12-2003-004-01004-0 from the Ministry of Science and Technology, KOREA.
II. The Model

In this section we will introduce the definition and security properties of forward-secure group signature schemes.

Definition A forward-secure group signature scheme is comprised of the following procedures:

- **SETUP**: On input of a security parameter, this probabilistic algorithm outputs the initial group public key (including all system parameters) and the secret key for the group manager.

- **JOIN**: A protocol between the group manager and a user that results in the user becoming a new group member. The user's output is a membership certificate and a membership secret.

- **EVOLVE**: An algorithm that on input a group signing key for time period $j$, outputs the corresponding group signing key for time period $j+1$.

- **SIGN**: A probabilistic algorithm that on input a group public key, a membership certificate, a membership secret, and a message $m$ outputs a group signature of $m$.

- **VERIFY**: An algorithm for establishing the validity of an alleged group signature of a message with respect to a group public key.

- **OPEN**: An algorithm that, given a message, a valid group signature on it, a group public key and a group manager's secret key, determines the identity of the signer.

- **REVOKE**: An algorithm that on input a group member's certificate, a group public key and the corresponding group manager's secret key, outputs a revocation token that revokes the group member's signing ability.

A forward-secure group signature scheme must satisfy the following security properties:

- **Correctness**: Signatures produced by a group member using SIGN must be accepted by VERIFY.

- **Unforgeability**: Only group members are able to sign messages on behalf of the group.

- **Anonymity**: Given a valid group signature for some message, identifying the actual signer is computationally hard for everyone but the group manager.

- **Unlinkability**: Deciding whether two different valid signatures were generated by the same group member is computationally hard.

- **Exculpability**: Neither a group member nor the group manager can sign on behalf of other group members.

- **Traceability**: The group manager is always able to open a valid group signature and identify the actual signer.

- **Coalition-resistance**: A colluding subset of group members (even if comprised of the entire group) cannot generate a valid group signature that cannot be traced by the group manager.

- **Revocability**: The group manager can revoke a group member's signing ability so that this group member cannot produce a valid group signature any more after being deleted.

- **Forward secrecy**: When a group signing key is exposed, previously generated group signatures remain valid and do not need to be re-signed.

III. Zhang-Wu-Wang Scheme

In this section we will briefly review Zhang-Wu-Wang scheme.

3.1 SETUP Procedure

The group manager (GM) randomly chooses two large primes $p_1$, $p_2$ of the same size such that $p_1 = 2p_1' + 1$ and $p_2 = 2p_2' + 1$, where both $p_1'$ and $p_2'$ are also primes. Let $n = p_1p_2$, and $G = \langle g \rangle$ be a cyclic subgroup of $\mathbb{Z}_n^*$. GM randomly chooses an integer $x$ as his secret key, and then sets his public key as $y = g^x \mod n$. GM selects a random integer $e$ (e.g., $e = 3$) which satisfies $\gcd(e, \phi(n)) = 1$, and computes $d$ such that $de = 1 \mod \phi(n)$, where $\phi(n)$ is the Euler Totient function. Let $h(\cdot)$ be a publicly known coalition-resistant hash function (e.g., SHA-1, MD5). The expected system life-time is divided into $T$ intervals and the
found to be publicly known. $(c, s) = SPK(\gamma : \gamma = g^{c})$ denotes the signature of the key log on the empty message. Finally, the group manager publishes the public key $(\gamma, n, g, c, k_0, ID_{GM}, T)$, where $ID_{GM}$ is the identity of the group manager.

### 3.2 JOIN Procedure

If a user, say Bob, wants to join the group, he executes an interactive protocol with GM. Firstly, Bob chooses a random number $k \in \mathbb{Z}_n^*$ as his secret key, and computes his identity $ID_B = g^k \mod n$. Then, Bob generates the signature of knowledge $(c, s) = SPK(\gamma : \gamma = g^{c})$ to show that he knows a secret value $k$ to meet $ID_B = g^k \mod n$. Finally, Bob keeps $k$ privately and sends $(ID_B, (c, s))$ to the group manager.

While receiving $(ID_B, (c, s))$, GM first verifies the signature of knowledge $(c, s)$. If the verification holds, GM chooses a random number $a \in \mathbb{Z}_n^*$ and computes as follows:

$$
\begin{align*}
  r_B &= g^a \mod n, \\
  s_B &= a + r_Bk \\
  w_B &= (r_BID_{GM}ID_B)^{-a} \mod n
\end{align*}
$$

Then, GM sends Bob $(s_B, r_B, w_B)$ via a private channel, and stores $(s_B, r_B, w_B)$ together with $(ID_B, (c, s))$ in his local database.

Bob accepts $(s_B, r_B, w_B)$ as his initial membership certificate if the following two equalities hold:

$$
\begin{align*}
  g^{s_B} &= r_B \cdot y^{r_B} \mod n \\
  r_BID_{GM}ID_B &= w_B \cdot g^{-c} \mod n
\end{align*}
$$

### 3.3 EVOLVE Procedure

Assume that Bob has the group membership certificate $(s_B, r_B, w_B)$ at time period $j$. Then at time period $j+1$, he updates his group membership certificate as $(s_{B+1}, r_{B+1}, w_{B+1})$ by computing

$$
\begin{align*}
  w_{B+1} &= (w_B)^{r_{B+1}} \mod n
\end{align*}
$$

### 3.4 SIGN Procedure

Suppose that $(s_B, r_B, w_B)$ be Bob's group membership certificate at time period $j$. To sign a message $m$, Bob randomly chooses two numbers $q_1, q_2 \in \mathbb{Z}_n^*$, and computes $z_1, u, r_1, r_2, r_3$ as follows:

$$
\begin{align*}
  z_1 &= g^{q_1}y^{q_2} \mod n \\
  u &= h(z_1, m) \\
  r_2 &= w_B^{q_1} \mod n \\
  r_1 &= q_1 + (s_B + R \cdot u \cdot h(r_2)) \text{ (in } \mathbb{Z}) \\
  r_3 &= q_2 \cdot r_2 + u \cdot h(r_2) \text{ (in } \mathbb{Z})
\end{align*}
$$

The resulting group signature on $m$ is $\sigma = (u, r_1, r_2, r_3, m, \beta)$.

### 3.5 VERIFY Procedure

Given $\sigma = (u, r_1, r_2, r_3, m, \beta)$, a verifier accepts it as a valid group signature on $m$ if and only if $u = h(z_1', m)$, where $z_1'$ is computed by

$$
\begin{align*}
  z_1' &= ID_{GM}^{uh(r_1)} \cdot g^{r_2h(r_1)c^{-r_2}y^{r_2}} \mod n
\end{align*}
$$

### 3.6 OPEN Procedure

Given a group signature $\sigma = (u, r_1, r_2, r_3, m, \beta)$, if necessary, GM can open it to reveal the actual identity of the signer who produced the signature. GM first checks $\sigma$'s validity via VERIFY procedure. If $\sigma$ is a valid signature, GM operates as follows to find the signer's identity:

1. Compute $\eta_1 = 1/(u \cdot h(r_2)) \mod \phi(n)$.
2. Compute $z_1' = ID_{GM}^{uh(r_1)} \cdot g^{r_2h(r_1)c^{-r_2}y^{r_2}} \mod n$.
3. Search his database to find a pair $(ID_B, r_B)$ that satisfies the following equality:

$$
  r_BID_B = (g^{r_2}y^{r_1}/z_1')^\beta \mod n.
$$
4. If there is a tuple $(r_B, ID_B)$ satisfying the above equation, GM concludes that $ID_B$ is the identity of the actual signer.

### 3.7 REVOKE Procedure

When GM wants to revoke Bob's membership certificate at time period $j$, he publishes tuple $(R, j)$ in the CRL (the Certificate Revocation List), where the value $R$ is computed by
\[ R_j = (r_j ID_B)^{d_{ij}} \mod n \]

Given a valid group signature \( \sigma = (u, r_1, r_2, r_3, m, \beta) \), a verifier can identify whether \( \sigma \) is produced by a revoked group member. For this sake, he performs as follows:

1. Compute \( z'_1 = ID_{C \mu} u h_{(z_2)} g^{r_1 h_{(r_1)} y_1} \mod n \)
2. Search all \((R_i, \beta) (i \leq j)\) in CRL to check whether there is a \( R_i (i \leq j) \) such that the following equality holds:
   \[ g^{z'_1} = z'_1 (R_i^{e_{1i}})^{h_{(r_1)}} \mod n. \]
3. If one such \( R_i (i \leq j) \) is found, the verifier concludes that the signature \( \sigma \) is revoked, i.e., it is generated by a group member after it is deleted.

### IV. Security analysis

In [14], Guilin Wang presented a security analysis of Zhang-Wu-Wang group signature scheme proposed in [13]. By successfully identifying several attacks, he demonstrated that this scheme is insecure. More specifically, his results show that this scheme is linkable, untraceable and forgeable.

In this section we show that this scheme is not coalition-resistant, which means that a colluding of group members, such as, Alice and Bob, can generate a valid group signature that cannot be traced by the group manager. For simplicity, let \( sk_{A,j} = (s_A, r_A, w_{A,j}, ID_A, k_A) \), and \( sk_{B,j} = (s_B, r_B, w_{B,j}, ID_B, k_B) \), where \( w_{A,j} = w_{A,j}^e \mod n = w_{A,j}^e \mod n \), and \( w_{B,j} = w_{B,j}^e \mod n = w_{B,j}^e \mod n \). \( sk_{A,j} \) and \( sk_{B,j} \) denote Alice’s and Bob’s signing key respectively at time period \( j \).

Firstly, they can forged a valid certificate, and then they can generate valid group signature on any message using this forged certificate which also can not be traced.

They forge \( w_{C,j}, ID_{C,j}, k_C \) as follows:
\[ w_{C,j} = ID_A w_{B,j} \mod n \]
\[ ID_{C,j} = ID_B g^{k_C e_j} \mod n \]

\[ k_C = k_B - k_A e_j \text{ (in }\mathbb{Z}\)\]

Now, we will show \((s_B, r_B, w_{C,j}, ID_{C,j}, k_c)\) is a valid group membership certificate. Notice that
\[ ID_C = ID_B g^{k_C e_j} \mod n = g^{k_C} \mod n. \]
Then we have the following equalities.

\[ r_B ID_{C,j} ID_C = (r_B ID_{C,j} ID_B) g^{k_C e_j} \mod n \]
\[ = w_{B,j}^{-e_j} g^{k_B e_j} \mod n \]
\[ = (w_{C,j} ID_A)^{-e_j} \mod n \]
\[ = w_{C,j}^{-e_j} \mod n \]

Now, Alice and Bob get another new valid certificate \((s_B, r_B, w_{C,j}, ID_{C,j}, k_c)\) according to JOIN procedure. They can generate valid signature on any message with this certificate. When such signatures are forged, neither Alice nor Bob will be traced, because \( r_B ID_{C,j} \neq r_A ID_A \mod n \) and \( r_B ID_{C,j} \neq r_B ID_B \mod n \).

The above discussion shows that a colluding of two group members can generate a valid group signature that cannot be traced by the group manager. So this scheme is not coalition-resistant.

### V. Concluding remarks

In this paper, we presented a further security analysis of Zhang-Wu-Wang group signature scheme proposed in [13]. More precisely, our results show that their scheme is not coalition-resistant. In fact, how to design a secure and more efficient group signature scheme is still a hot issue. The most recent investigations are given in [15, 16, 17].

### References
