ID-based Threshold Blind Signature scheme from Bilinear Pairing

Xiaohui Liang, Zhenfu Cao, ZhenChuan Chai, Rongxing Lu
Department of Computer Science and Engineering, Shanghai Jiao Tong University, liangxh127@sjtu.edu.cn; {cao-zf, zcchai, rxlu}@cs.sjtu.edu.cn

Abstract. Threshold and Blindness are two important properties in cryptography system. They can provide security and privacy. In this paper, We present an efficient construction from Bilinear pairing in an ID-based cryptography system. In an ID-based \((k, n)\) threshold blind signature scheme, Private Key Generation Center(PKGC) distributes the secret key to \(n\) group members. The user only communicates with the dealer who has collected no less than \(k\) valid sub-signatures and computes the group signature. During this process, the signer and the dealer have no information about the message(blindness). We analyze and prove the security of our scheme. To the best of the author’s knowledge, this is the first ID-based threshold blind signature scheme.

Keywords: Blind signature, Identity-based, Bilinear pairing, Threshold signature, Parallel one-more unforgeability.

1 Introduction

Two of the most important properties offered by cryptography are security and privacy. Plenty of research papers of such kind in cryptography have been done in recent years. Threshold signature and blind signature have many implementations and applications in reality.

The concept of ID-based cryptography is due to Shamir\[19\]. In an ID-based cryptography system, a user’s public key is an easily calculated function of his identity, while a user’s private key can be calculated for him by a trusted authority called Private Key Generation Center(PKGC). Since the ID-based system has significantly simplified key management and avoided the need of certificates to link users to their public keys, many research papers\[17\] are presented which are many suggestions for the implementation of identity based cryptography system.

Blind signatures are introduced by David Chaum\[14\] in 1982. Such a scheme allows a user to acquire a signature from the signer without revealing message content for personal privacy. The basic idea is as follows. The user chooses some random factors and embeds them into the message to be signed, while the signer cannot recover the message. Using the blind signature scheme, the user gets the blinded signature and removes the random factors. Then the user outputs a valid signature. This property is very important for implementing e-voting, e-commerce, and e-payment systems, etc.

Based on the ideas of secret sharing and threshold cryptography schemes introduced by Shamir\[16\], we construct the scheme with threshold which improves the security of our cryptography system. In a \((k, n)\) ID-based threshold blind signature scheme, the user communicates with the dealer for acquiring a group signature. The dealer collects no less than \(k\) members’ sub-signatures, then combines them together and sends to the user. If there are \(k - 1\) or less sub-signatures, the dealer cannot do the same thing. To implement threshold property in an ID-based cryptography system, PKGC has to distribute the secret to each group member firstly. During this process, the dealer can be seen as a trusted computing machinery. The user doesn’t directly know there is a threshold in the cryptography system.

In general, the voting system based on blind signature scheme is managed by a single administrator, who can be empowered to authorize votes. But, to prevent abusing power to cast fraudulent votes, we need more than one administrator using threshold signature scheme to sign a vote. In this paper,
we propose a new construction to combine these two different concepts in an ID-based cryptography system. Therefore, an ID-based threshold blind signature while giving user ability to get signature on a message without revealing its content, still maintains the secret key to be distributed among signers in an ID-based cryptography system.

The rest of this paper is organized as follows. Section 1.1 and 1.2 introduce the related works and our contributions. In section 2, we give the preliminaries which include the introductions and definitions of the concepts of bilinear pairing, threshold, and blindness. In section 3, we give our ID-based threshold blind signature (ITBS) scheme in details. We analyze and prove the security of our scheme in section 4 including three parts blindness, robustness and unforgeability. The performance is given in section 5. Finally, we give our conclusion and future work in section 6.

1.1 Related Work

Some research papers\[1, 3, 4, 5\] present the schemes which include blind signature and sign-cryption schemes under ID-based cryptography system. Our construction involves some basic ideas of them but applies in different environment for different purpose. Some threshold blind signature schemes\[2, 7, 8\] were introduced. Although they are implemented based on pairing or discrete logarithm, they can not be easily embedded into ID-based cryptography system. In the paper\[2\], each party acts as a dealer to choose the secret key and distributes it verifiably to other parties, whereas PKGC distributes the secret to group members in our proposed scheme. The paper\[6\] introduces some basic schemes including threshold signature, multi-signature and blind signature.

One-more forgery is a kind of adversary’s behavior in blind signature introduced by Schnnor\[9\]. The papers\[10, 11\] analyze one-more forgery in a different view. Others \[12, 13\] analyzes the security in digital signature and blind signature in details. In 2005, TV\[1\] gives the definition of Generic Group Pairing Model(GGPM) extending Generic Group Model(GGM)\[9\] to help proving the unforgeability of his blind identity-based signcryption. We prove that our scheme is secure against parallel one-more forgery following this way. Moreover, we show that our scheme has blindness and robustness.

1.2 Contributions

This paper presents a provably secure ID-based threshold blind signature scheme(ITBS). We formulate an security model of ITBS. We analyze and prove the security of our ITBS which includes blindness, robustness and unforgeability. In addition, we show our scheme is flexible which is easily modified to an ID-based threshold blind signcryption scheme. To the best of our knowledge, our schemes are the first of their kind.

2 Preliminaries

2.1 Bilinear Pairing

Since our scheme uses bilinear pairing on elliptic curves, we give some brief definitions on the properties of bilinear pairing and hard problems. Let \(G_1, G_2\) be two cyclic multiplicative groups of the same order \(q\). We assume that the discrete logarithm problems in both \(G_1\) and \(G_2\) are hard. A bilinear pairing is a map \(e : G_1 \times G_1 \rightarrow G_2\) which satisfies the following properties:

- Bilinear: For any \(P, Q \in G_1\), and \(a, b \in \mathbb{Z}_q^*\), we have \(e(P^a, Q^b) = e(P, Q)^{ab}\).
- Non-degenerate: There exist \(P, Q \in G_1\) such that \(e(P, Q) \neq 1\).
- Computable: There is an efficient algorithm to compute \(e(P, Q)\) for all \(P, Q \in G_1\).

**Definition 1.** (CDH problem) The Computational Diffie-Hellman problem is, given \(P, P^\alpha, P^\beta \in G_1\), for unknown \(\alpha, \beta \in \mathbb{Z}_q^*\), to compute \(P^{\alpha \beta}\).
Definition 2. (DDH problem) The Decisional Diffie-Hellman problem is, given \(P, P^\alpha, P^\beta, P^\gamma \in G_1\), for unknown \(\alpha, \beta, \gamma \in \mathbb{Z}_q^\star\), to make a decision if \(P^{\alpha \beta} = P^\gamma\).

Definition 3. (co-CDH problem) The co-Computational Diffie-Hellman problem is, given \(P, P^\alpha \in G_1\) and \(Q \in G_2\) for unknown \(\alpha \in \mathbb{Z}_q\), to compute \(Q^\alpha\).

2.2 Secret Sharing and Threshold Cryptography Schemes

In 1979, Shamir\(^{16}\) firstly introduced the concept of threshold cryptography scheme which makes the scheme more secure and leads many applications in reality. So we review "Secret-Sharing over \(G\)" firstly.

Distribution phrase: Let \(q\) be a prime. The secret \(s \in \mathbb{Z}_q^\star\) generated by PKGC should be distributed. We assume there is a \((k, n)-\)threshold. That means, in a group of \(n\) members \(G_i(i = 1, 2, ..., n)\), no less than \(k\) members can reveal the secret \(s\). The basic idea is as follows. First, PKGC randomly chooses \(a_1, a_2, ..., a_{k-1} \in \mathbb{Z}_q^\star\) and forms a distribution function \(F(x) = s + a_1 x_1 + a_2 x_2 + \cdots + a_{k-1} x_{k-1}\). Then PKGC computes \(X_i = F(i) \in \mathbb{Z}_q^\star\) and sends \((i, X_i)\) to each member \(G_i\). Note that when \(i = 0\), we obtain the secret \(X_0 = F(0) = s\).

Re-construction phrase: Let \(\Psi \subseteq \{1, ..., n\}\) be a set such that \(|\Psi| \geq k\), where \(|.\)| denotes the cardinality of a given set. The function \(F(x)\) can be reconstructed by computing

\[
F(x) = \sum_{j \in \Psi} \lambda_{x_j} X_j \text{ where } \lambda_{x_j} = \prod_{t \in \Psi, t \neq j} \frac{x - t}{j - t}
\]

Note that \(\lambda_{x_j} \in \mathbb{Z}_q^\star\) is the Lagrange interpolation coefficient used in Shamir’s secret sharing scheme. In our scheme, we can reveal the secret:

\[
s = F(0) = \sum_{j \in \Psi} \lambda_{y_j} X_j \text{ where } \lambda_{y_j} = \prod_{t \in \Psi, t \neq j} \frac{0 - t}{j - t}
\]

2.3 ID-based Blind Signature

After Chaum\(^{14}\) suggested a construction method of a blind signature scheme based on RSA problem, there are many researches dealing with ID-based blind signature. We construct a general ID-based blind signature model which is defined as follows:

Let \(G_1\) be a cyclic multiplicative group of order \(q\). Let \(P\) be a generator of \(G_1\). The PKGC generates its master key \(s \in \mathbb{Z}_q^\star\) and publishes \(P_{pub} = P^s\). After receiving the public key \(Q_{ID} = H(ID)\) of the user, the PKGC sends the private key \(S_{ID} = Q_{ID}^t\) to the user, where \(H\) and \(H_1\) are hash functions \(H: \{0, 1\}^* \rightarrow G_1, H : G_1 \times \{0, 1\} \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^\star\). We record the signer \(A\), the receiver \(B\) and the message \(M\). Respectively, \(A, B\)'s identities, public keys and private keys are \((ID_A, Q_A, S_A), (ID_B, Q_B, S_B)\). Public information is \(I = (q, P, P_{pub}, ID_A, Q_A, ID_B, Q_B, H, H_1)\). A randomly chooses \(t \in \mathbb{Z}_q^\star\) and publishes \(U = P^t\). The new ID-based blind signature scheme \(IBSS = (IBP, IBS, IBV)\), where \(IBP, IBS\) and \(IBV\) are ID-based blind pre-process, ID-based blind signature and ID-based blind verification algorithms respectively, defined as:

- \(IBP(U, M, I)\): The user randomly picks \(\alpha, \beta \in \mathbb{Z}_q^\star\) and computes \(\hat{U} = P^{\alpha t + \beta}, \hat{h} = H_1(\hat{U}, M, ID_B)\), \(h = \alpha^{-1} \hat{h}\). Then sends \(h\) to \(A\).
IBS(h, S_A, I): A gives the signature σ = Sign(h, S_A, t, I) and sends σ to the user. Then the user computes \( \hat{\sigma} = F(\sigma, \alpha, \beta, I) \). F must satisfy that

\[
\hat{\sigma} = F(\sigma, \alpha, \beta, I) \\
= F(\text{Sign}(h, S_A, t, I), \alpha, \beta, I) \\
= \text{Sign}(\hat{h}, S_A, at + \beta, I)
\]

IBV(\( \hat{\sigma}, M, \hat{U}, S_B, I \)): After receiving \( \hat{\sigma} \), B computes \( \hat{h} = H_1(\hat{U}, M, ID_B) \). If \( V_{\text{DDH}}(\hat{\sigma}, \hat{h}, \hat{U}, S_B, I) = 1 \) then return 1 else return 0, where \( V_{\text{DDH}}() \) is an efficient algorithm which solves the DDH problem in \( G_1 \).

3 Our Proposed Scheme

Now we give our proposed scheme in details. Our scheme, similar to the TV[11]'s blind identity-based signcryption(BIBSC), consists of four steps Setup, Extract, Signing and Verification.

Setup

Let \( G_1, G_2 \) be two cyclic multiplicative groups of the same prime order \( q \). Let \( P \) be a generator of \( G_1 \). A bilinear pairing map \( e : G_1 \times G_1 \rightarrow G_2 \). We define three secure hash functions \( H : \{0,1\}^\ast \rightarrow G_1 \), \( H_1 : G_1 \times \{0,1\}^\ast \times \{0,1\}^\ast \rightarrow Z_q^\ast \) and \( H_2 : G_2 \times \{0,1\}^\ast \rightarrow G_1 \). PKGC first chooses a random number \( s \in Z_q^\ast \) and sets \( P_{\text{pub}} = P^s \), then keeps \( s \) as the master key. PKGC publishes the system parameters \( \{G_1, G_2, q, e, P, P_{\text{pub}}, H_1, H_2\} \).

Extract

Since there are two types of member in our scheme, PKGC has to give two kinds of public/private key for them. One type is for the verifier, such as the public key is \( Q_{ID} = H(ID) \) and the private key is \( S_{ID} = Q_{ID}^t \). The other type is for group members. To implement ID-based threshold blind signature, PKGC should distribute the secret key’s shadows to group members.

We assume there is a group with its identity \( ID_B \), and the public key of this group is \( Q_B = H(ID_B) \). The group \( B \) has \( n \) members, \( B_1, B_2, ..., B_n \). Without loss of generality, we assume \( B_1, B_2, ..., B_k \) participate in the signature scheme. The PKGC carries out the following steps:

1. Randomly chooses \( r, a_1, a_2, ..., a_{k-1} \in Z_q^\ast \)
2. Forms a function \( F(x) = sr + a_1x + a_2x^2 + ... + a_{k-1}x^{k-1} \), and computes \( F(1), ..., F(n) \), where \( s \) is the master key.
3. Sends \( X_i = F(i) \) to \( B_i \) as its secret key. \( i \in \{1, 2, ..., n\} \)
4. Computes \( Y_i = Q_B^{X_i} \) as \( B_i \)’s public key and \( Z_i = P^{X_i} \), \( i \in \{1, 2, ..., n\} \)
5. Publishes \( K = P^{sr}, L = P^r \) and \( Y_i, Z_i, i \in \{1, 2, ..., n\} \).

For each member \( B_i, i \in \{1, 2, ..., n\} \), after receiving \((X_i, Y_i, Z_i)\), he can verify its secret key by checking \( Y_i = Q_B^{X_i} \) and \( Z_i = P^{X_i} \). The verifier can check \( K \)’s correctness by \( e(K, P) = e(L, P_{\text{pub}}) \).

Signing

During this step, the user will communicate with the dealer. In the user’s view, he doesn’t know any information about threshold cryptography scheme. In the dealer and signer’s view, they don’t know any information about the message \( M \). The group signature is not supplied to the user until the dealer receives \( k \) valid sub-signatures. We describe the scheme as following:

1. The signer randomly chooses \( t_i \in Z_q^\ast \) and computes \( T_i = Q_{B_i}^{t_i}, U_{B_i} = P^{t_i}, H_i = P_{\text{pub}}^{t_i} \). Then sends \( T_i, U_{B_i}, H_i \) to the dealer.
2. The dealer authenticates \( U_{B_i}, H_i \) by using \( e(U_{B_i}, Y_i) = e(Z_i, T_i) \) and \( e(P, H_i) = e(U_{B_i}, P_{\text{pub}}) \).

Then he computes \( U = \prod_{i=1}^{k} U_{B_i} = P^{\sum_{i=1}^{k} t_i} = P^t \) and sends it to the user, where \( t = \sum_{i=1}^{k} t_i \).
3. For blindness property, the user randomly chooses \( \alpha, \beta \) as blind factors. He computes \( \hat{U} = U_p^{\alpha} P^\beta \) and \( \hat{h} = H_1(\hat{U}, M, ID_C) \). Then sends \( \hat{h} = \alpha^{-1} \hat{h} \) to the dealer.
4. The dealer records \( h \) and passes them to group member \( B_i, i \in \{1, 2, ..., n\} \).
5. The signer computes and sends \( V_i = (Q_B Q_C)^{t_i + \lambda_i X_i h} \) to the dealer, where \( \lambda_i = \prod_{j=1, j \neq i}^{n} (0_{-j}) / \prod_{j=1, j \neq i}^{n} (1_{-j}) \).
6. The dealer can use the following equation to verify each sub-signature \( V_i \)

\[
e(Q_B, V_i) = e(T_i, Q_B Q_C) e(Y_i, (Q_B Q_C)^{h \lambda_i})
\]

If the equation does hold, the sub-signature can be accepted, otherwise, rejected. Since,

\[
e(Q_B, V_i) = e(Q_B, (Q_B Q_C)^{t_i + \lambda_i X_i h})
\]

\[
= e(Q_B, (Q_B Q_C)^{X_i} (Q_B Q_C)^{\lambda_i h})
\]

\[
= e(T_i, Q_B Q_C) e(Y_i, (Q_B Q_C)^{\lambda_i h})
\]

Once the dealer has received \( k \) valid sub-signatures, he computes the whole signature as

\[
V = \prod_{i=1}^{k} V_i
\]

\[
= \prod_{i=1}^{k} (Q_B Q_C)^{t_i + \lambda_i F(i) X_i h}
\]

\[
= (Q_B Q_C)^{\sum_{i=1}^{k} (Q_B Q_C)^{t_i + \lambda_i X_i h}}
\]

And the dealer computes

\[
W = e \left( \prod_{i=1}^{k} H_i, Q_C \right) = e(P_{pub}', Q_C)
\]

Then the dealer sends \((V, W)\) to the user.
7. The user modifies the signature with \( \alpha, \beta \). So he computes

\[
\hat{V} = V^\alpha (Q_B Q_C)^\beta
\]

\[
\hat{W} = W^\alpha e(P_{pub}', Q_B)^\beta
\]

\[
\hat{Y} = H_2(\hat{W}, ID_B) \oplus \hat{V}
\]

Finally, the user gives the ID-based threshold blind signature \( \sigma = (\hat{U}, \hat{Y}) \). Figure 1 describes the whole process intuitively.

<table>
<thead>
<tr>
<th>Signer</th>
<th>Dealer</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>randomly chooses ( t_i )</td>
<td>( B_i \rightarrow )</td>
<td>( U_i \rightarrow )</td>
</tr>
<tr>
<td>sends ( U_i = P_B^{t_i} )</td>
<td>( B_i \rightarrow )</td>
<td>computes ( U = \prod_{i=1}^{k} U_i )</td>
</tr>
<tr>
<td>sends ( H_i = P_{pub}^{t_i} )</td>
<td>( B_i \rightarrow )</td>
<td>computes ( \hat{U} = U^\alpha P^\beta )</td>
</tr>
<tr>
<td>checks ( e(Q_B, V_i) )</td>
<td>( U_i \rightarrow )</td>
<td>computes ( h = H_1(\hat{U}, M, ID_C) )</td>
</tr>
<tr>
<td>( = e(T_i, Q_B Q_C) e(Y_i, (Q_B Q_C)^{\lambda_i h}) )</td>
<td>( )</td>
<td>( \rightarrow )</td>
</tr>
<tr>
<td>yes(k times): does follows</td>
<td></td>
<td>sends ( h = \alpha^{-1} )</td>
</tr>
</tbody>
</table>
| sends \( V_i = (Q_B Q_C)^{t_i + \lambda_i X_i h} \) | \( \rightarrow \) | logic and sends \( h \)
| | | computes \( \hat{V} = V^\alpha (Q_B Q_C)^\beta \) |
| | | computes \( W = W^\alpha e(P_{pub}', Q_C)^\beta \) |
| | | computes \( \hat{Y} = H_2(W, ID_B) \oplus \hat{V} \) |
| | | outputs \( \sigma = (\hat{U}, \hat{Y}) \) |

Fig. 1. ID-based Threshold Blind Signature
Verification
To verify the signature $\sigma = (\hat{U}, \hat{Y})$, $C$ carries out the following steps:

1. $C$ computes
   \[
   W' = e(\hat{U}, S_C) = e(U^\alpha P^\beta, S_C) = W'^\alpha e(P^{\alpha t}, S_C) e(P^\beta, S_C) = \hat{W}
   \]

2. $C$ computes $\hat{h} = H_1(\hat{U}, M, ID_C)$ and $\hat{V} = \hat{Y} \oplus H_2(W', ID_B)$

3. $C$ checks $e(P, \hat{V}) = e(\hat{U} K^h, Q_B Q_C)$. Since
   \[
   e(P, \hat{V}) = e(P, V'^\alpha (Q_B Q_C)^\beta) = e(P, (Q_B Q_C)^{(r h)^\alpha} (Q_B Q_C)^{\beta}) = e(P, (Q_B Q_C)^{srh} (Q_B Q_C)^{\beta}) = e(P^{\alpha t + \beta + srh}, Q_B Q_C) = e(\hat{U} K^h, Q_B Q_C)
   \]

Our scheme is similar to the TV’s scheme\[1\] and is based on the most efficient ID-based blind signature scheme compared with others. In another view, the threshold increases the total computation in our system, since that one signature is divided into $k$ sub-signatures. Therefore, the dealer needs to have strong computation power.

4 Security Analysis

In this section we discuss about the security issues of our proposed scheme. The security consideration includes blindness, robustness and unforgeability of our scheme.

On blindness, the user can obtain a valid signature on a message without revealing the content of the message to signers. Robustness of the scheme ensures that the scheme can tolerate even $k - 1$ of $n \geq 2k - 1$ signers are corrupted. Moreover, unforgeability not only is secure against one-more-forgery attack but also is secure even when $k - 1$ signers were corrupted by an adversary.

Definition 4. Let ITBS is a ID-based threshold blind signature scheme. ITBS is secure if:

1. Blindness. The signer can not obtain the message from interaction. That means, the signer who knows the transcript has the same probability of obtaining the message with the one who has not.
2. Robustness. Even there exists an adversary who can corrupt up to $k - 1$ signers, our scheme completes successfully.
3. Unforgeability. No adversary who corrupts at most $k - 1$ signers, with non-negligible probability, can do on-more forgery attack.

4.1 Blindness

The blindness of our proposed scheme is shown by the following theorem:

Theorem 1. Our ITBS is a blind scheme if given a ciphertext $\hat{\sigma}$ by the user, $Prob\{\hat{\sigma} by User\} = Prob\{\hat{\sigma} by User|Transcript\}$

Proof. We show that given a valid ciphertext $\hat{\sigma} = (\hat{U}, \hat{Y})$ and any transcript of threshold blind signature $(U, h, V, W)$, there always exist a unique pair of blinding factors $\alpha, \beta \in Z_q^*$. Since the blinding factors are randomly chosen, the blindness of ITBS is achieved.
Given a valid ciphertext \((\hat{U}, \hat{Y})\), then there exists a unique \(M\) for this ciphertext. Then with the transcript, the following equations must be hold.

\[
\begin{align*}
\hat{U} &= U^\alpha P^\beta \\
h &= \alpha^{-1} H_1(\hat{U}, M, ID_C) \\
\hat{V} &= V^\alpha (QBQC)^\beta \\
\hat{W} &= W^\alpha e(P_{pub}, QC)^\beta
\end{align*}
\]

By the first two equations, we see that there exist blind factors \(\alpha = H_1(\hat{U}, M, ID_C)/h\), \(\beta = \log_P(UU^{-\alpha})\). And also \(\alpha, \beta\) satisfy the last two equations.

\[
e(P, \hat{V}) = e(UK^h, QBQC) \\
= e(P^\alpha t^\beta P^{srh}, QBQC) \\
= e(P, (QBQC)^{(\alpha t + srh)}(QBQC)^\beta) \\
= e(P, V^\alpha (QBQC)^\beta)
\]

and

\[
\hat{W} = e(\hat{U}, SC) \\
= e(U^\alpha P^\beta , SC) \\
= e(P^\alpha t^\beta , SC) \\
= e(P_{pub}^\alpha , QC)^\beta e(P_{pub}, QC)^\beta \\
= W^\alpha e(P_{pub}, QC)^\beta
\]

Hence, there always exists a unique pair of blind factors \(\alpha, \beta \in Z_q^*\). Therefore, \(\text{Prob}\{\hat{\sigma} \text{ by User}\} = \text{Prob}\{\hat{\sigma} \text{ by User} | \text{Transcript}\}\). The blindness of our ITBS is proved.

4.2 Robustness

The robustness of our proposed scheme is shown by the following theorem:

**Theorem 2.** Our ITBS is robust for an adversary who can corrupt \(k - 1\) signers among \(n\) signers such that \(n \geq 2k - 1\) signers.

**Proof.** From the robustness property of the scheme to generate a random shared signature, it follows that every honest signer computes correct value \(V_i\). Because there are at least \(k\) honest players, and the dealer can verify the correctness of \(V_i\) by \(e(QB, V_i) = e(T, QBQC)e(Y_i, (QBQC)^{\lambda_i h})\). It follows directly by the correctness property that the honest players will always compute a valid sub-signature. Finally, the dealer can compute a valid signature with \(k\) sub-signatures. These showed that our ITBS is robust.

**Definition 5.** The PKGC is robust, that is, the master key \(s\) can not be obtained by the adversary.

**Theorem 3.** Our ITBS’s PKGC is robust for a strong adversary who can corrupt more than \(k - 1\).

**Proof.** We assume the strong adversary knows \(k\) secret key of signers \(X_1, X_2, ..., X_k\). So he can easily compute:

\[sr = F(0) = \sum_{j \in \Psi} \lambda_j X_j \text{ where } \lambda_j = \prod_{t=1, t \neq j}^{t=k} 0 - t \]

However, \(r \in Z_q^*\) is randomly chosen by the PKGC. The adversary can not get the PKGC’s master key \(s\) from \(sr, K = P^s, L = Pr, P_{pub} = P^a\) based on discrete logarithm problem from bilinear pairing. So we said that PKGC is robust.
In another view, the adversary can not compute the group B’s private key $S_B = Q_B$ from $sr, K = P^{sr}, L = P^r, P_{pub} = P^s, Q_B$ based on CDH problem. In this way, the group private key could be used to avoid such strong adversaries.

### 4.3 Unforgeability

To show unforgeability, we first introduce the ROS problem, then prove our scheme is against one-more forgery adversary. In Schnorr’s paper, it gives the definitions of non-interactive and interactive adversary existing in blind signature scheme. In 2005, TV introduces the generic group and pairing model(GGPM) by extending the generic group model(GGM), to include support for the pairing oracle. We use some of their definitions to complete our proof.

**Definition 6.** Parallel one-more forgery against blind signature is that an adversary interacts for $l$ times with a signer and produces $l + 1$ signatures from these interactions.

**Definition 7.** ROS problem: Find an overdetermined, solvable system of linear equations modulo $q$ with random inhomogenities. Specifically, given an oracle random function $F: \mathbb{Z}_q^t \rightarrow \mathbb{Z}_q$, find coefficients $a_{k,1}, ..., a_{k,t} \in \mathbb{Z}_q$ and a solvable system of $l + 1$ distinct equations in the unknowns $c_1, ..., c_l$ over $\mathbb{Z}_q$:

$$a_{k,1}c_1 + ... + a_{k,t}c_t = F(a_{k,1}, ..., a_{k,t}) \text{ for } k = 1, ..., t$$

We evaluate the expected number of solvable subsystems consisting of $l + 1$ out of $t$ equations.

We briefly introduce the generic group pairing model(GGPM). We divide all the data into two types which are group elements in $G_1, G_2$ and non-group data.

We mainly discuss the interactive adversary here. A generic adversary $A$ is an interactive algorithm that interacts with blind signature oracle and hash oracle. We count the following generic steps:

- group operations
- queries to hash oracle $H$
- interactions with a blind signature oracle

This algorithm performs some $t$ generic steps resulting in $t' \leq t$ group elements $f_1, ..., f_{t'}$. The input consists of group elements in $G_1, G_2$ including public keys $P, Q_B, Q_C, P_{pub}, K, L$ and non-group data including $q$, messages, ciphertexts, pairing $e$.

$A$’s transmission to key extraction oracle depends arbitrarily on given group elements and non-group data. Requesting for the sender’s private key is not allowed.

$A$’s output and transmission to blind signature oracle consists of non-group data $NG$ and previously computed group elements $f_i$, where $NG$ and $i, 1 \leq i \leq t'$, depend arbitrarily on given non-group data.

The restriction of GGPM is that $A$ can use group elements only for generic group operations, equality tests and for queries to hash oracle, whereas non group data can be randomly selected.

The following lemma shows the collision probability for group elements are negligible except when involving oracle queries. The proof is similar to Schnorr’s lemma 1 and omitted.

**Lemma 1.** In an arbitrary instantiation of the generic groups and the generic pairing, the probability of a PPT generic algorithm being able to compute a collision is negligible, except those collisions obtain via oracle queries. The probability is taken over randomized instantiations of all randomly generated base elements.

**Theorem 4.** Our ITBS scheme is parallel one-more unforgeability secure provided Schnorr’s ROS problem is hard in the ROM+GGPM.
Proof. We consider a generic interactive adversary $A$ performing $t$ steps, including some $q_B$ interactions $(U_1, h_1, V_1, W_1), \ldots, (U_{q_B}, h_{q_B}, V_{q_B}, W_{q_B})$ with blind signature oracle, producing some $t'$ group elements in $G_1$. We let $t = (t_1, \ldots, t_{q_B})$ denote the dealer random coins. Let $f_1 = P, f_2 = P_{pub}, f_3, \ldots, f_t \in G_1$ denote the group elements of $A$’s computation. The generic adversary $A$ computes $f_j = P_{pub} \cdot f_{pub,j}^q \prod_{m=1}^{q_B} f_{b,m}^{3\gamma}$, where $a_j^{-1} \ldots a_{j,q_B}$ is randomly generated by $A$. Since that $r$ is only visible to PKGC and $K, L$ contain the unknown parameter $r$, the adversary won’t take $K$ and $L$ account in his attack.

Let $A$ outputs $(\hat{U}_i, \hat{V}_i)$ be valid for message $M_i$, sender ID and recipient ID in $ID_{C,1}$, for $1 \leq i \leq q_B + 1$. We have $\hat{h}_i = H_1(\hat{U}_i, M_i, ID_{C,1})$ for some hash query satisfying $e(P, \hat{V}_i) = e(\hat{U}_i, K^{-h_i} Q B Q C)$. Then we have the following two equations: $e(P, \hat{V}_i) e(K, (Q_B Q C)^{-h_i}) = e(\hat{U}_i, Q_B Q C) = e(f_{a_i}, Q_B Q C) = e(P_{pub} \cdot \prod_{m=1}^{q_B} \hat{U}_{m}^{a_{i,m}}, Q B Q C)$ and $e(U_m, Q_B Q C) = e(P, V_m) e(K, (Q_B Q C)^{-h_m})$ imply:

$$\hat{V}_i = (Q_B Q C)^{a_{i,0}} \prod_{m=1}^{q_B} \left( Q_B Q C \right)^{a_{i,m}} (Q_B Q C)^{\sum_{m=1}^{q_B} - a r h_m a_{i,m}}$$

$$\hat{V}_i = (Q_B Q C)^{a_{i,0}} \prod_{m=1}^{q_B} \left( Q_B Q C \right)^{a_{i,m}} (Q_B Q C)^{\sum_{m=1}^{q_B} - a r h_m a_{i,m}}$$

If $A$ makes $r \hat{h}_i + a_{i,0} - \sum_{m=1}^{q_B} r h_m a_{i,m} = 0$, $A$ could easily get the valid signature, since that $Q_B, a_{i,0}, \ldots, a_{i,q_B}, V_m$ for $m = (1, 2, \ldots, q_B)$ are known to him. Conversely, $A$ must select $h_1, \ldots, h_m$ as to zero the coefficient involving the master key $s$. Otherwise, we can recover $(Q_B Q C)^{s r}$ from $V_1, \ldots, V_{q_B}, a_{i,0}, \ldots, a_{i,q_B}, \hat{h}_i, \hat{V}_i$ which are known to $A$. Thus we can use it to solve CDH problem. We assume that the probability of solving CDH in GGPM is negligible. Hence $A$ must solve the ROS problem which is an NP-complete problem[18]. In the whole process, due to the invisibility of $r$, the security of our scheme is enhanced.

Thus, we prove that our scheme is secure under one-more forgery attack.

5 Conclusion

In this paper, we give the first ITBS scheme and define its security model. To implement a threshold signature in an ID-based cryptography system, PKGC distributes the master key to each group member. The signature contains the recipient’s ID and it can be verified by everyone. We have proved our scheme is blind, robust and is secure against parallel one-more forgery. The parallel one-more unforgeability was proven under GGPM and ROM.

As for flexibility, our scheme is easily modified to an ID-based threshold blind signcryption scheme. In section 3, after the user get a valid group $B$ signature, he executes group operations. He outputs $\hat{Z} = H_2(\hat{W}) \oplus (ID_B, M)$, where $H_2$ is a hash function $G_2 \rightarrow \{0, 1\}^*$. Following this way, our scheme is extended to signcryption scheme.

In the future work, we should consider the efficiency and other security issues to make our scheme better.

References