Password-based Selective Linkable Convertible Ring Blind Signature

Yulei Zhang¹, Tingting Song¹ and Yongjie Zhang²

¹ College of Computer Science and Engineering, Northwest Normal University, Lanzhou, 730070, China.
² Gansu Health Vocational College, Lanzhou, 730000, China.
Email: 1187208093@qq.com

Abstract. Ring signature has become an important way of privacy protection because of its anonymity and the spontaneity of ring members. It has been widely used in the field of information security. Password-based alternative linkable convertible ring blind signature scheme combines the advantages of strong anonymity of ring signature and blindness of blind signature to signature message, and adds the optional linkable and convertible characteristics, which makes it more secure than other schemes, and can also transform ring signature into ordinary signature in special occasions. At the same time, under the random oracle model, the scheme satisfies the unforgeability under the adaptive selection message attack. Performance analysis shows that the scheme has high operating efficiency.

1. Introduction

The ring signature was originally a digital signature proposed by Rivest et al. [1] at the 2001 Asia-Pacific Conference. It was named after the end of the ring according to certain rules. Essentially, the signer uses the public key of the other signer to generate a ring with a break, and then uses the private key to join the break into a complete ring. Any certifier can use the public key to verify, or understand that the ring signature is a simplified group signature, and the participating users have only ring members and no managers. The verifier can verify the identity of the signer without knowing the identity of the signer. This not only authenticates the signed message but also protects the user's identity. It is widely used in information security, privacy protection, Blockchain [2-3] and other fields due to the ambiguity of the signer's identity. Subsequently, various ring signature schemes and improvement schemes were continuously proposed, for example, in 2007, Shacham and Waters [4] proposed a bilinear pair-based ring signature scheme, which has small computational complexity, small storage space, and relatively fast processing speed, but most ring signature schemes cannot resist quantum attacks and are high computational complexity. In order to solve this problem, Zheng et al. [5] proposed a code-based ring signature scheme, the scheme is implemented on the basis of CFS [6] (Courtois Finiasz Sendrier), and its signature length is $144 + 126l$ (l represents the number of members in the ring), the CFS scheme has high security, and it becomes the basis of a large number of subsequent digital signature algorithm design based on coding. In addition to ring signature schemes based on bilinear pairings and RSA difficult problems, Liu et al. [7-8] have successively proposed the Linkable Spontaneous Anonymous Group (LSAG) and other frameworks for associated ring signatures [9-10], in order to avoid and solve the same person's repeated signature and voting issues. Other than this, some special cases may also need to convert the associated ring signature, that is, convert the ring signature into a common digital signature, and require the scheme to resist the convertible attack, Zhang Wenfang et al. [11] proposed a specific implementation in the alternative
transformable linkable ring signature scheme based on RSA public key cryptosystem. Different from the above signature scheme, Kristian et al. [12] added the password to the signature key in 2012, passwords are unpredictable random combination generated by the server, making the password an important part of the key.

The ring signature has strong anonymity of the signer identity, but the signed message is still insecure for the ring members. The blind signature has been widely recognized by academics and industry since it was proposed by Okamoto et al. [13] in 1992, immediately afterwards, some excellent programs [14-15] were proposed and applied to actual projects. This article combines the advantages of various schemes, the server password as part of the signature, any unilateral cannot produce the correct signature private key; the ring signature guarantees the strong anonymity of the scheme; the blind signature will blindly process the signed message; the optional association is determined by the signer; in special cases, the ring signature can also be converted into a normal signature. In addition, this solution has higher operational efficiency than other solutions.

2. The Detail Scheme

2.1. Initialization Algorithm

Two large prime numbers $p_i$ and $q_i$ are arbitrarily selected for each user $U_i$ ($i=1,2,...,n$) in the ring signature, where $\phi(N_i) = (p_i - 1)(q_i - 1)$. The message owner $U_o$ and the signer $U_t$ agree on a constant $c$, called $c$ partial blind factor, so that it can be used without the need to negotiate. The length of $c$ is $k-2$ bits, defining two single-item hash functions $H: \{0,1\}^* \rightarrow Z_{N_i}^*$ and $G: \{0,1\}^* \rightarrow Z_{N_i}^*$, and calculating $\tau(c) = 2^{k-1} + 2H(c) + 1$, the value $\tau(c)$ range is $2^{k-1} < \tau(c) < 2^k$.

Select the public key $e_i c \tau(c)(1 < e_i \tau(c) < \phi(N_i))$, where $e_i \tau(c)$ satisfies $\gcd(e_i \tau(c), \phi(N_i)) = 1$.

Calculates $d_i = e_i \tau(c)^{-1} \mod \phi(N_i)$, $d_i = e_i \tau(c)^{-1} \mod \phi(N_i)$ is the private key, and $e_i \tau(c)$ is the public key containing the constant $c$.

$d_i$ satisfies $d_i = d_{ii} + d_{2i}$, sends $d_{ii}$ to the server, and $d_{2i}$ sends it to the user. The single ring user public key is $pk_i = (N_i, e_i \tau(c), H, G)$, and $L = \{pk_1, pk_2, ..., pk_n\}$ is the public key set of $n$ ring signed users.

2.2. Key Generation Algorithm

After the server $S$ receives $d_{ii}$, randomly selects a password $pw_i$ and processes by a hash function to obtain $G(pw_i)$, calculates $\eta = G(pw_i) - d_{ii}$, and $\eta$ is sent to the user. The user receives $d_{2i}$, and $\eta$ to calculate the signature private key $sk_i = d_{2i} \cdot \eta$.

2.3. Signature Algorithm

Public key set: $L = \{(N_1, e_1 \tau(c), H, G), ..., (N_n, e_n \tau(c), H, G)\}$, the signed user $U_t$ is recorded as $pk_i = (N_i, e_i \tau(c), H, G)$ and the private key is $sk_i$, and $1 \leq t \leq n$, $U_t$ generates a ring blind signature is as follows:
Step1: Blind message. The message $m \in \{0,1\}^*$ to be signed, $U_o$ agrees with $U_i$, a constant $c$; $U_o$ randomly select the blind factor $\alpha \in \mathbb{Z}_{N_i}^*$, blindly process the message $m$ to obtain $m = H(m)\alpha^{\epsilon(c)}$, sends $m$ to $U_i$, where $e_i\tau(c)$ is the public key containing the constant $c$.

Step2: Signature:
- The signature user $U_i$ randomly selects random initial value $r_i \in \mathbb{Z}_{N_i}^*$, $t_i \in \mathbb{Z}_{N_i}^*$, and calculates $t_i^{-1}$ so that $t_it_i^{-1} = 1 \mod N_i$, obtains linkable tags $\omega = t_i^{-1}r_i \mod N_i$.
- $U_i$ starts signing the blinded message $m = H(m)\alpha^{\epsilon(c)}$ and calculates $\beta' = m^d_i$.
- Forms a ring: $U_i$ randomly selects $v_i \in \mathbb{Z}_{N_i}^*$, $\gamma \in \mathbb{Z}_{N_i}^*$ and calculates:
  
  \[ j = H(y_1 \parallel y_2 \parallel \ldots \parallel y_{i-1} \parallel y_{i+1} \parallel \ldots \parallel y_n, \gamma) \]

  sets the subscript $i$ to $U_i$ and calculates:
  
  \[ v_{i+1} = H(m \parallel j, v_i) \]

  \[ v_{i+2} = H(m \parallel j, v_{i+1} \oplus m_i + 1) \]

  \[ \ldots \]

  \[ v_{i+1} = H(m \parallel j, v_{i+2} \oplus m_{i+2}) \]

  \[ v_i = H(m \parallel j, v_{i+1} \oplus m_{i+1}) \] .The subscripts of the above ring forming process belong to $\mathbb{Z}_{N_i}^*$, therefore, there is $v_{i+n} = v_i$ in order to construct a ring, let $v_i \oplus m_i = v_i$, then $m_i = v_i \oplus v_1$.

- Final output ring blind signature $\sigma' = (\omega \cdot v_0, v_1, \beta_1', \ldots, \beta_n')$.

Step3: Unblind. The signature $\sigma' = (\omega \cdot v_0, v_1, \beta_1', \ldots, \beta_n')$, starts to blind operation $\beta = \beta'\alpha^{-1}(\beta')^{G(p_w)}$.

2.4. Verification Algorithm

The verifier $V_i$ receives the message, the unblind verification equation $\beta = \beta'\alpha^{-1}(\beta')^{G(p_w)}$ of the message $m$ and the public key set $L = \{(N_i, e_i\tau(c), H.G), \ldots, (N_n, e_n\tau(c), H.G)\}$ start to verify the signature: $H(m) = \beta^{\epsilon(c)}$ is true, if it is established, the signature is valid, otherwise the signature is invalid.

3. Proof of Security

3.1. Correctness Analysis

Theorem 1 The scheme satisfies correctness.

Proof. Obtainable by public and private key generation and ring blindness signature process:

Key generation: $d_i = d_{i_1} + d_{i_2}$, $\eta = G(p_w) - d_{i_1}$, $sk_i = d_{i_2} - \eta$.

Message blindness: $m = H(m)\alpha^{\epsilon(c)}$

Ring signature: $\beta' = (H(m)\alpha^{\epsilon(c)})^{d_i} = (H(m)\alpha^{\epsilon(c)})^{d_i - G(p_w)}$

Unblind: $\beta = \beta'\alpha^{-1}(\beta')^{G(p_w)}$

Public key: $e_i\tau(c) \leftarrow d_i^{-1} \mod (N_i)$

Verify: $H(m) = \beta^{\epsilon(c)}$ is true, if it is established, the scheme satisfies the correctness.

3.2. Non-forgeability Analysis

Theorem 2 If the RSA inversion problem is difficult, then the scheme satisfies the unforgeability in the random oracle mode.
Lemma 1 Suppose there is an advantage of the EUF-CMA adversary \( A \), \( A \) performs a maximum of one signature inquiry, then there must be an adversary to solve the RSA problem with at least the \( \text{Adv}^A_{\text{P}}(k) \geq \epsilon(k)/q_h \) advantage of \( \epsilon \) is the bottom of the natural logarithm). If for any polynomial time adversary \( A \), \( \text{Adv}^A_{\text{P}}(k) \) is negligible, then the scheme is said to have the existence of unforgeability under the adaptive selection message attack.

Proof. Initialization. Challenger \( C \) running algorithm \( \text{Setup}(\lambda) \), adversary \( A \) gets the public key set \( L = \{ (N_i, e, \tau(c), H, G), \ldots, (N_n, e, \tau(c), H, G) \} \), sending \( L \) to adversary \( A \) and randomly select \( j \leftarrow \{ 1, 2, \ldots, q_h \} \). \( j \) is a guess value of challenger \( C \), and the \( j \)th inquiry of \( A \) corresponds to the final counterfeiting result of \( A \). The adversary \( A \) knows \( (N_i, e, \tau(c), H, G, \epsilon) \), \( c^*_i \in \mathbb{Z}_{N_i} \) and the goal is to calculate \( \beta_j = (c^*_j)^{t_{\text{let}(c)}} \). 

- Phase 1. \( A \) initiates the following inquiry to \( C \), \( C \) responds accordingly.

\( H \) query (max \( q_h \) times): Challenger \( C \) creates a list \( (M_i, L, c_i, \beta_i, \sigma_i) \) with an initial value of null, at the beginning, \( c_i = (m^{\alpha(c)})^{t_{\text{let}(c)}} \) has been set. When \( i = 1, 2, \ldots, n \), calculates \( c_i = (m^{\alpha(c)})^{t_{\text{let}(c)}} \).

If \( i = j \), return \( c^*_i \); Then selects a random value \( c_i \in \mathbb{Z}_{N_i} \), and calculates \( \beta_j = (m^{\alpha(c)})^{t_{\text{let}(c)}} \), store \( \beta_i \) as the query response in the table \( (M_i, L, c_i, \beta_i, \sigma_i) \).

- Phase 2. \( A \) performs the following polynomial \( q = q(k) \) bounded sub-adaptive queries.

- Forgery. Adversary \( A \) begins to forge signature. If \( M \neq M_j \), interrupt the operation;

Otherwise \( M = M_j \) and \( \beta_j^{t_{\text{let}(c)}} = c_j \). Here \( c_j = (m^{\alpha(c)})^{t_{\text{let}(c)}} \), \( C \) outputs the signature \( \sigma_j \).

Therefore, in the above process, as long as the inquiry and forgery process is not interrupted, the challenger’s simulation is complete. If \( C \) guesses is correct, and \( \sigma_j \) outputs a forgery, the challenger successfully solved the difficult problem given by the scheme. Challenger \( C \) is determined by three events: \( C \) not interrupted in \( A \) signature query; \( A \) generate a valid message signature pair \( (M_j, \sigma_j) \); \( M \) corresponds to the subscript in the quintuple \( i = j \), the return value of the verification result of the message \( \text{status} \leftarrow \text{Verify}(L, M, \sigma) \) is 1.

\[
Pr[a_i] = (1 - 1/q_h)^{q_h}, \ Pr[a_j | a_i] = \epsilon(k), \ Pr[a_i | a_j] = Pr[i = j | a_i] = 1/q_h.
\]

So the advantage of adversary \( A \) is \( Pr[a_i, a_j] = Pr[a_i]Pr[a_j | a_i]Pr[a_j | a_i] = Pr(a_i, a_j) = (1 - 1/q_h)^{q_h} \cdot \epsilon(k). \)

\( 1/q_h \approx 1/eqH(\epsilon(k)) \). The solution obtained by the above proof process is unforgeable.

3.3. Strong Anonymity Analisis

Theorem 3 This scheme has strong anonymity.

Proof. Assume that the ring signature \( \sigma' = (\alpha; h_i, v_i; \beta_1', \ldots, \beta_{\nu}^') \) is a legal signature generated by the signed user. According to the signature algorithm, \( \alpha \in \mathbb{Z}_{N_i}^* \), \( r_i \in \mathbb{Z}_{N_i}^* \) is randomly distributed in \( \mathbb{Z}_{N_i} \). When the ring formation process is \( i = 1, 2, \ldots, n \), \( j = H(y_1 \parallel y_2 \parallel \ldots \parallel y_{t-1} \parallel y_{t+1} \parallel \ldots \parallel y_{t+\gamma}, y_i) \), \( v_{i+1} = H(m \parallel j; v_i) \), \( v_i \in \mathbb{Z}_{N_i}^* \), \( \gamma \in \mathbb{Z}_{N_i}^* \) also randomly selected, therefore \( \sigma' \) is also randomly distributed in \( \mathbb{Z}_{N_i} \). As can be seen from the above, the distribution of the signature over the entire domain is uniform and does not include the identity of the signer and other information. For the server participating in the signature, a random password \( pw_i \) is used in the process of signing the message, and processes by the hash function \( G : \{0, 1\}^* \rightarrow \mathbb{Z}_{N_i}^* \) to get \( G(pw_i) \), the distribution on the signature domain also has indistinguishability over polynomial time.
In summary, the password-based selectable linkable convertible ring blind signature scheme, since the user private key is jointly generated by the PKI and the server participating in the signature, the server password selection is random, and the parameters \( v_i \in Z_N^* \), \( r_i \in Z_N^* \), \( \gamma \in Z_N^* \) and hash function are randomly selected in the signature algorithm. So for an arbitrary polynomial time algorithm \( P \), the signature \( \sigma_i \), \( i \) can be obtained, and the probability of satisfying \( sk = sk_i \) \( (i = 1,2,...,n) \) is only \( 1/n \), so the scheme has strong anonymity.

### 3.4. Blindness Analysis

**Theorem 4** This scheme has blindness.

**Proof.** For the signer, it is impossible to recover the original message \( m \) from the blinded message \( m' \), since the blinding process equation is \( m = ma^{\sigma_i} \), the blinding factor \( a \) is a randomly selected unknown. In addition, even after the message \( m \) to be signed is published, the signer cannot associate \( m \) and \( m' \), and therefore the signature of the blind message cannot be associated with the original message \( m \), so the scheme satisfies the blindness throughout the signature process.

### 4. Advantage and Performance Analysis

This scheme and the existing ring signature scheme are analysed and compared from various aspects. The symbols in the operation are shown in Table 1.

#### Table 1. Operator symbol definition.

| symbol | Interpretation          |
|--------|-------------------------|
| \( n \) | Total number of ring members |
| \( M \) | Power exponential operation overhead |
| \( E \) | Modulus exponential operation time complexity |
| \( OTV \) | One-time signature overhead |

Table 2 shows the specific analysis and comparison of the anonymity, signature length, signature time complexity and verification time complexity of the scheme and the existing ring signature scheme.

#### Table 2. Anonymity and efficiency comparison.

| Scheme | Signature Length | Anonymity         | Signature Time Complexity | Verification Time Complexity |
|--------|------------------|-------------------|---------------------------|----------------------------|
| Scheme [7] | \( O(n) \) | weak anonymity | \( (4n-1)E + (2n-1)M \) | \( 4nE + 2nM \) |
| Scheme [8] | \( O(n) \) | Calculated anonymous | \( E + (4 + 2n)/2)M \) | \( 2M + (n-1)E \) |
| Scheme [11] | \( O(n) \) | Strong anonymity | \( 2nE + M \) | \( 2nE \) |
| Our Scheme | \( O(n) \) | Strong anonymity | \( nE + 2M \) | \( 2nM \) |

Under the advantage of its strong anonymity, the difficult problem that the implementation process relies on is the decomposition of large integers. Compared with the literature [7], the complexity of signature and verification time is significantly improved, while the literature [7] only has weak anonymity. In the case of the same signature length, the literature [8] only achieves computational anonymity compared to this scheme. Compared with the scheme [11], although they have strong
anonymity, the operational efficiency is higher than the scheme [11]. In summary, the password-based
ring-blind signature increases the blindness of the signed message while ensuring its unforgeability
and strong anonymity. The signature user can also choose the relevance and conversion. In addition,
performance analysis shows that signature and verification have higher operational efficiency.

5. Conclusion
In the public key cryptosystem, the password is used as an important part of the key. The signature
message is blinded and the optional linkable convertible feature is added. The ring signature improves
the security of the scheme based on strong anonymity. In the case of rapid development of blockchain,
information security and privacy protection, ring signatures show great research and use value. How to
design a signature scheme that guarantees anonymity while having a certain degree of supervision in
the blockchain is the next research direction.

6. Acknowledgments
Foundation Items: The National Natural Science Foundation of China (61163038, 61262056,
61262057). The Higher Educational Scientific Research Foundation of Gansu Province (2017A-
003,2018A-207).

7. References
[1] Rivest R, Shamir A and Auman Y 2001 How to leak a secret Proc.Advances in Cryptology-
ASIACRYPT (Australia: Gold Coast) pp 552–65
[2] Zhang Fan, Huang Nianyan and Gao Sheng 2018 Privacy data scheme of ring signature based
on Borromean (Cryptography Journal vol 5) chapter 5 pp 529–37
[3] Wang Huaqun and Wu Tao 2017 Cryptographic technology in block chain (Journal of Nanjing
University of Posts and Telecommunications vol 37) chapter 6 pp 61–7
[4] Shacham H and Waters B 2007 Efficient ring signatures without random oracles Proc. of the
Public Key Cryptography2007 (PKC 2007) (Beijing:China) pp 166–80
[5] Zheng D, Li X and Chen K 2007 Code-based Ring Signature Scheme (IJ Network Security vol 5)
chapter 2 pp 154–57
[6] Melchor CA, Cayrel PL and Uaborit P 2008 A new efficient threshold ring signature scheme
based on coding theory Proc.2nd Int. Workshop on Post-Quantum Cryptography(USA: Cincinnati) pp 1–16
[7] Liu J, Wei V and Wong D 2004 Linkable spontaneous anonymous group signature for ad hoc
groups Proc.9th Australasian Conf.on st.chinasensor@vip.126.com Information Security and
Privacy(ACISP 2004) (Australia: Sydney) pp 325–35
[8] Liu J K, Man H A and Susilo W 2013 Linkable and/or threshold ring signature without random
oracle[J](IEEE Transcations on Knowledge vol 16) chapter 1 pp 157–65
[9] Tsang P, Wei V and Chan T 2005 Separable linkable threshold ring signatures Proc.the Progress
in Cryptology-INDOCRYPT 2004 (India: Chennai) pp 384–98
[10] Fujisaki E 2011 Su-linear size traceable ring signatures without random oracles Proc.11th Int.
Conf. on Topics in Cryptology (CT-RSA’11) (American: San Francisco) pp 393–415
[11] Zhang Wenfang, Xiong Dan 2017 Optional convertible association ring signature based on RSA
public keycryptosystem (Journal of Computer Science vol 40) chapter 5 pp 1168–80
[12] Kristian Gjosteen and oysteinThuen 2012 Password-based Signatures Euro PKI 2011
LNCS7136 pp17–33
[13] Okamoto T 1992 Provable secure and practical identification schemes and corresponding digital
signature scheme[C] CRYPTO ’92 (New York:Springer-Verlag) pp 31–52
[14] Yao Chifeng, Zhu Huafei and Chen Kangsheng 2001 A generalized ELGamal type blind
signature scheme based on binary radiation variables [J] (Acta ElectronicaSinica vol 28) chapter
7 pp 128–29
[15] Wang Yihong, Lu Mingxin and Xiao Guozhen 2005 Cryptographic analysis based on discrete
logarithmic proxy blind signature [J] (Journal of Software vol 16) chapter 5 pp 777–80