An Efficient Short Blind Proxy Re-signatures Scheme

Xiaodong Yang, Tingchun Ma, Chunlin Chen, Yutong Li and Meiding Wang

College of Computer Science and Engineering Northwest Normal University Lanzhou, Gansu 730070, China
Email: y200888@163.com

Abstract. The existing proxy re-signature schemes have drawbacks in terms of privacy protection and signature efficiency. Our scheme is based on the proxy re-signature scheme, which combines the main idea of short blind signature and proposes the definition of short blind proxy re-signature scheme. Then, using the signature framework of the random oracle model, we propose a short blind proxy re-signature scheme based on the random oracle model, and prove the security of the scheme under the adaptive chosen-message attacks. The analysis shows that compared with the existing similar schemes, our scheme does not add additional verification information under the premise of shortening the signature length, and the applicability is better in the interactive transmission of devices with limited calculation and transmission performance.

1. Introduction

The concept of proxy re-signature was first proposed by Blaze et al. in 1998 at the EUROCRYPT [1]. In 2005, Ateniese and Hohenberger pointed out the drawbacks of this scheme [2], redefined proxy re-signature and proposed three different proxy re-signature schemes. In 2006, Sherman and Raphael constructed a new proxy re-signature scheme in the standard model [3]. At present, proxy re-signature is widely used in DRM authentication negotiation, path certification, and public key certificate management.

In 1982, Chaum put forward the concept of blind signature for the first time in the construction of electronic cash system [4]. Blind signature is a special kind of digital signature. Under this signature mechanism, the content of the message is unknown to the signer. Because of its blindness, this signature is widely used in the fields of electronic voting, electronic cash payment and electronic bill management. Usually, such devices have problems such as low computational efficiency, limited transmission capability and instability. To solve these problems, Boneh et al. proposed the concept of short signature in 2001 [5], which improves the storage space and transmission efficiency of the signature. In the case of low computing performance, this signature is highly applicable.

In general, proxy re-signature is not blind to messages. In the process of message transformation, message content is open to the re-signed agent, which also brings challenges to message hiding. In response to this challenge, Deng et al., on the framework of proxy re-signature, merged the main features of blind signature and proposed a blind proxy re-signature mechanism in 2010 [6], and proposed a blind proxy re-signature scheme based on standard model. However, this scheme is not suitable for high power wireless devices because of its complex operation and low efficiency in the process of signature and blindness.

In order to solve the problem of low efficiency and privacy in proxy re-signature. This paper combines the characteristics of short-blind signature and proxy re-signature, and proposes a short-blind proxy re-signature scheme. Under the premise that the length of the signature is shortened, no
additional authentication information is added. It not only improves the transmission efficiency of the signature, but also guarantees the blindness of the proxy signature in the transformation process.

2. Preliminaries

2.1. Bilinear Pairing
Let \( G_1 \) and \( G_2 \) be two multiplicative cyclic groups of prime order \( p \), and let \( g \) be a generator of \( G_1 \). A bilinear pairing map \( e : G_1 \times G_1 \rightarrow G_2 \) satisfies the following properties:

a) Bilinear: For any \( a, b \in \mathbb{Z} \), there is \( e(g^a, g^b) = e(g, g)^{ab} \).

b) Non-degeneracy: \( e(g, g) \neq 1 \).

c) Computability: There exists an efficient algorithm to compute \( e(g^a, g^b) \).

2.2. The Computational Diffie-Hellman Assumption (CDH)
In the random oracle model, the \( q \) order cyclic additive group generated by \( g \) is called \( G_1 \). Choose randomly \( a, b \in \mathbb{Z}_q \), \( g \in G_1 \), It is difficult to solve \( g^{ab} \) with known \( g^a \) and \( g^b \).

3. Our Short Blind Proxy Re-signatures Scheme

(1) System Initialization: Our scheme chooses two groups \( G_1 \) and \( G_2 \) whose order is prime \( q \), where the generator of \( G_1 \) is \( g \), a bilinear mapping \( e : G_1 \times G_1 \rightarrow G_2 \) and a secure hash function \( H : \{0, 1\}^* \rightarrow G_1 \), exposing the system parameter \( sp = (G_1, G_2, q, g, e, H) \).

(2) Key Generation (KeyGen): On input the security parameter \( 1^k \), select a random \( x \in \mathbb{Z}_q \), and output a public-private key pair \((sk, pk)\), where \( sk = x \), \( pk = g^x \).

(3) Re-Signature Key Generation (ReKey): Given that the trustee Alice's private key is \( sk_a \) and the trustee Bob's private key is \( sk_b \), the proxy's re-signature key \( rk_{a+sb} = x_{a+sb} \mod q \) is generated.

(4) Message Blind: The user randomly selects \( u, v \in \mathbb{Z}_q \), calculates \( h = H(m) \), \( v = g^v \), and \( \lambda = h^V \), and then sends the blinded message \( \lambda \) to Alice.

(5) Signature Generation: After receiving the blind message \( \lambda \), Alice calculates \( S_{\lambda} = \lambda^{x_a} \) and sends \((\lambda, S_{\lambda})\) to the agent.

(6) Signature Conversion: The agent verifies that \( e(S_{\lambda}, g) = e(\lambda, y_a) \) is true. If the equation does not hold, the agent refuses to convert the signature; otherwise, the agent calculates the blind signature \( S_g = S_{\lambda}^{x_b} \mod q \) and sends \((\lambda, S_g)\) to the user.

(7) Unblind: After receiving the \((\lambda, S_g)\), the user calculates \( S_{\lambda} = S_{\lambda} / (y_a) \) and \( S = (S_g)^{x_a} \) and outputs the final re-signature \( S \) of the message \( m \).

(8) Message Verification: On input message and signature \((m, S)\), calculate \( h = H(m) \), verify the equality \( e(S, g) = e(h, y_a) \) is established. If the equation is true, the verifier accepts that the signature \( S \) is a legal signature of the message \( m \); otherwise, \( S \) is rejected.
(9) Correctness analysis: According to $\lambda = h^xV = H(m)^yg^x$, $S_d = \lambda^x$ and $S_n = S_d^{x_1} = (\lambda^x)^{x_1} = \lambda^{x_1}$, get:

$$S_z = \frac{\lambda^x}{(y^x)^y} = \frac{(H(m)^yg^x)^x}{(g^x)^y}$$

Therefore, we have; $e(S, g) = e(H(m)^x, g) = e(h, y^x)$. 

4. Security Analysis

4.1. Message Blindness
In this scheme, given a valid signature $(m, S)$, and the median value $(\lambda, \lambda^x, \lambda^y)$ of the signature phase, the randomly selected blinding factors $u$ and $v$ satisfy: $uV = \lambda$ and $vV = \lambda^y$. It can be concluded that: $v = \log_e V$ and $u = \log_e \lambda$. When signing, $S = \lambda^x$. Since the blindness factor $u$ and $v$ is random and unique, it is difficult to calculate the value of $u$ and $v$ according to the signature. It is concluded that the calculation of this scheme message is difficult and has message blindness.

4.2. Security proof
Based on the random prediction model, this scheme proves the existence of forgery attacks against adaptive chosen-message attacks from the external security certification and internal security under the assumption of CDH problem.

(1) External Security
External security refers to the fact that the user's legal signature will not be forged by non-legitimate users outside the scheme. In this scheme, except the trustee, the principal and the agent, other users can not generate the signatures of the trustee and the principal.

Theorem 1 For external security, assume that any adversary $A$, At most, after $q_h$ hash queries, $q_S$ signature queries, and $q_{resign}$ re-signature queries, break the above short-blind proxy re-signature scheme with a non-negligible advantage $\varepsilon$, then build an adversary $A'$ solves the CDH problem with a probability of approximately $\varepsilon \geq e(\frac{1}{2q_h})(\frac{1}{2q_S})$.

Proof. The adversary $A$ solves the above problem by calling the algorithm $\mathcal{R}$. It is assumed that the target public key is $y_i = g^x$, the message challenged is $m^x$, and the public key of other identities is $y_i = g^x$, where $x_i \in Z_q$ is random. After the system is initialized, the adversary $A$ sends the system parameter $\{G_1, G_2, k, q, g, H\}$ and the public key $a$ of the target identity $y_i$ to the algorithm $\mathcal{R}$.

• Hash query: The message $m$ input by the algorithm $\mathcal{R}$ is compared with the list $LH$. If the value exists in the list $LH$, the corresponding $h$ value is returned to the algorithm $\mathcal{R}$; otherwise, the relationship between $m$ and $m^x$ is judged: If $m = m^x$, the $y_i$ value is returned to algorithm $\mathcal{R}$ and $(y_i, m^x, m^x)$ is saved in the $LH$. If $m \neq m^x$, randomly select $x_i \in Z_q$, calculate $y_i = g^x$, return to the algorithm $\mathcal{R}$, and calculate the value of $h = H(m)$, and save the $(y_i, m, h)$ array to list $LH$.

• Signature Query (Osign): Input $(l, m)$, if $l \neq t$, then randomly select $u, v \in Z_p$, calculate $V = g^x$, $h = H(m)$, and $\lambda = h^xV$ according to the formula, and return the calculated signature $S = \lambda^x$ to algorithm $\mathcal{R}$; otherwise, judge the relationship between $m$ and $m^x$: If $m = m^x$, abort; If $m \neq m^x$, then randomly select $u, v \in Z_p$, calculate $h = H(m)$, $V = g^x$, and $\lambda = h^xV$ according to the formula, and return the computed signature $S = \lambda^x$ to the algorithm $\mathcal{R}$.

• Re-signature Query (Oresign): Input $(i, j, m, S)$, if $(y_i, m, S) = 1$, then by calling the re-signature Query, output $(y_j, m)$; otherwise, abort.
• Forgery: after completing adaptive query, adversary $A$ outputs forgery information $(y_i, m, S) = 1$, if $(y_i, m, S) \neq 1$ or $(m, S)$ is directly obtained by signature query and re-signature query, then the adversary $A$ forgery fails and abort; if $j \neq t$, it indicates that the target user guessed by algorithm $\mathcal{R}$ is wrong and abort; otherwise, the equality $e(S', g) = e(h', y_s)$ is verified and output the signature $S' = H(m')^a = g^{ab}$.

According to the above process, we can see: the adversary successfully calculated the $S' = g^{ab}$, output $S'$, that is, to solve the CDH problem, The following is an analysis of the advantages of adversaries in solving difficult problems:

In this scheme, the answers obtained by hash query are uniformly distributed, independent and efficient. When the signature is queried, the case where $m = m'$ occurs is counted as event $E_1$; in the forgery stage, the phenomenon that the forged message and the $m'$ are inconsistent, called the event $E_2$; and the case where the verification error occurs during the re-signature inquiry phase is called event $E_3$. When the events $E_1$, $E_2$, and $E_3$ do not occur, it indicates that the signature falsified by the adversary is legal. The probability that event $E_1$ does not occur is $\frac{1}{q_H}$, and that event $E_3$ does not occur is $\frac{1}{2}$.

Therefore, $\Pr(E_1 \land E_2 \land E_3) = (\frac{1-2^{\frac{q_H}{q_H}}}{q_H}) \cdot (\frac{1}{q_H}) \cdot \frac{1}{2} = (\frac{1-2^{\frac{q_H}{q_H}}}{q_H}) \cdot (\frac{1}{2q_H})$.

(2) External Security
The scheme is bidirectional, so the internal security considers only the limited agent.

Theorem 2 Assuming that any proxy $A$, in the identity attack algorithm $\mathcal{R}$, passes through at most $q_H$ hash query, $q_S$ signature query, $q_R$ re-signature key query, and breaks through the scheme with an undeniable advantage $\varepsilon$, an adversary $A_0$ can be constructed to solve the CDH problem with a probability of about $\varepsilon \geq (1 - \frac{1}{q_H})^{\frac{q_H}{q_H}} \cdot (\frac{1}{2q_H})$.

Proof. It is assumed that algorithm $A$ can perform the related work of the re-signature proxy and know the private keys of users other than user $A$. Here Agent $A$ falsifies the signature of User $A$ by means of the algorithm $\mathcal{R}$. In this proof process, other assumptions, hash query, forgery process and external security proof are consistent and will not be repeated.$\mathcal{R}$; otherwise, abort.

• Re-signature key Query (Orekey): On input $(i,j)$, if $i = A$ or $j = A$, abort; otherwise output $rk_{i,j} = \frac{x_j}{x_i}$.

The final analysis is similar to before. Only when agent $A$ correctly guesses the message $m'$ that needs to be forged and the target user that needs to be forged, can an adversary $A\theta$ be constructed to solve the CDH problem with a probability of about $\varepsilon \geq (1 - \frac{1}{q_H})^{\frac{q_H}{q_H}} \cdot (\frac{1}{2q_H})$.

5. Performance Analysis
Following from the four algorithms of signature, blind, re-signature and unblind, the overhead of the proposed scheme and the existing three bidirectional blind proxy re-signature schemes are compared. Assume that the selected four schemes have the same length, the bilinear pairing operation is represented by P, and the exponential operation is represented by E. In the process of comparison, the addition and modular multiplication operations with small calculation amount are ignored, and the comparison results are shown in Table 1.
Table 1. Performance comparison of four similar schemes

| Scheme          | Signature | Blind | Re-Signature | Unblind |
|-----------------|-----------|-------|--------------|---------|
| Deng’s Scheme[6]| 3E        | 2E    | 2E+3P        | 1E+3P   |
| Hu’s Scheme[7]  | 4E        | 5E+3P | 2E+3P        | 1E+3P   |
| Li’s Scheme[8]  | 3E        | 1E    | 4E+3P        | 1E+3P   |
| Our scheme      | 1E        | 2E    | 1E+P         | 2E      |

According to Table 1, the new scheme reduces the number of exponential and pairing operations in both signature and re-signature algorithms compared with the other three schemes. Compared with Hu scheme, the new scheme also reduces the number of exponential and triple pairing operations in the blind algorithm. Therefore, the efficiency of this scheme is much better than that of other schemes in signature and signature conversion process.

6. Conclusions
In this paper, a short blind proxy re-signature scheme based on random oracle model is proposed, which is proved to be existential unforgeable under adaptive chosen-message attacks. Compared with the typical proxy re-signature scheme, the proposed scheme has message blindness; compared with several existing blind proxy re-signature schemes, the proposed scheme efficiently shortens the signature length, and is more applicable in the interactive transmission of devices with limited computational and transmission performance. However, this scheme needs to be improved in practical application. In further research, we should focus on expanding the application field of this scheme to realize anonymous protection of electronic bills and secure interaction of devices in wireless environment.

7. Acknowledgments
This work was partially supported by the National Natural Science Foundation of China (61662069), China Postdoctoral Science Foundation (2017M610817), Science and Technology Project of Lanzhou City of China (2013-4-22), Foundation for Excellent Young Teachers by Northwest Normal University (NWNU-LKQN-14-7).

8. References
[1] Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. Lecture Notes in Computer Science, 1998, 1403: 127-144.
[2] Ateniese G, Hohenberger S. Proxy re-signatures: new definitions, algorithms, and applications. ACM Conference on Computer and Communications Security, 2005: 310-319.
[3] Sherman C, Raphael P. Proxy resignatures in the standard model. Proceedings of 11th International Conference on Information Security, Taipei, China, 2008: 260-276.
[4] Chaum D. Blind Signatures for Untraceable Payments. Advances in Cryptology. Springer US, 1983: 199-203.
[5] Dan B, Lynn B, Shacham H. Short Signatures from the Weil Pairing. International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2001: 514-532.
[6] Deng Y, Du M, You Z. A blind proxy re-signature scheme based on standard model. Journal of Electronics and Information, 2010, 32 (5): 1219-1223.
[7] Hu X, Yang Y, Liu Y. Security analysis and improvement of a blind proxy re-signature scheme based on standard model. Minicomputer System, 2011, 32 (10): 2008-2011.
[8] Li X, Yang X. An improved bidirectional blind proxy re-signature scheme. Computer Applications, 2013, 33 (2): 447-449.
[9] Deng Y. A blind proxy re-signature scheme based on quadratic residual difficulty. Journal of Computer Applications and Software, 2011, 28(6): 293-295.
[10] Shao J, Wei G, Ling Y, et al. Unidirectional Identity-Based Proxy Re-Signature. IEEE International Conference on Communications, 2011: 1-5.