A Certificateless Proxy Re-Signature Scheme

Guo Duntao
Key Laboratory of Network and Information Security, Engineering College of Chinese Armied Police Force, Xi’an 710086, China
yudan0830@163.com

Wei Ping
Key Laboratory of Network and Information Security, Engineering College of Chinese Armied Police Force, Xi’an 710086, China
Yudan1986@126.com

Yu Dan
Key Laboratory of Network and Information Security, Engineering College of Chinese Armied Police Force, Xi’an 710086, China
328237950@qq.com

Yang Xiaoyuan
Key Laboratory of Network and Information Security, Engineering College of Chinese Armied Police Force, Xi’an 710086, China
xxyangwj@126.com

Abstract—Proxy re-signature is greatly concerned by researchers recently. It is a very useful tool for sharing web certificates, forming weak group signatures, and authenticating a network path. In this paper, we propose the first certificateless proxy re-signature scheme. Based on certificateless public cryptosystem, the scheme solves the using of certificate in certificate-based scheme and removes key escrow in ID-based scheme. Analysis shows that the proposed scheme can satisfy the required properties of proxy re-signature, and it can avoid public key replacement attack and malicious KGC attack.

Keywords—Certificateless Public Key Cryptography; Proxy Re-Signature; Bilinear Pairing; Public Key Replacement Attack

I. INTRODUCTION

In Asiacrypt 2003, Certificateless Cryptography was first proposed by Al-Riyami and Paterson [1]. Certificateless cryptography does not require the use of certificate to ensure the authenticity of public keys. Instead, certificateless is similar to identity-based cryptography [2], which relies on a trusted third party KGC who has the master-key. But, certificateless cryptography removes the key escrow problem that seems to be inherent in identity-based cryptography. In the certificateless system, KGC only knows the partial private key of the user, the full private key must use a secret value, which is chosen by the user himself. So, the certificateless cryptography solves the using of certificate in certificate-based cryptography and removes key escrow in ID-based cryptography.

A. Proxy re-signature and related work

Proxy re-signature scheme was first introduced by Blaze, Bleumer, and Strauss [3] at Eurocrypt’98, in which a semi-trusted proxy acts as a translator between Alice and Bob. To translate, the proxy converts a signature from Alice into a signature from Bob on the same message. However, the proxy does not learn any signing key and cannot sign arbitrary messages on behalf of either Alice or Bob. Proxy re-signature is very useful in sharing web certificates, authenticating a network path and forming weak group signatures.

Proxy re-signature is different from proxy signature. Proxy signature allows Alice to delegate her signing rights to Bob but only if the proxy cooperates. However, in proxy re-signature system, the proxy translates a perfectly valid and publicly-verifiable signature from Alice on a certain message \( \sigma_A(m) \), into one from Bob on the same message \( \sigma_B(m) \). The two signatures can coexist and both can be publicly verified as being two signatures from two distinct people on the same message. But the proxy re-signature scheme of BBS has many problems and with limited features. So, Giuseppe Ateniese and Susan Hohenberger formalized the proxy re-signature over again in 2005, and provided three new proxy re-signature schemes (\( \mathcal{B} \), \( \mathcal{S} \), *\( \mathcal{S} \)) [4] which based on bilinear maps. And they give the eight desirable properties of a proxy re-signature scheme:

1) **Unidirectional**: In an unidirectional scheme, a re-signature key allows the proxy to transform A’s signature to B’s but not vice versa. In a bidirectional scheme, on the other hand, the re-signature key allows the proxy to transform A’s signature to B’s as well as B’s signature to A’s.

2) **Multi-use**: In a multi-use scheme, a transformed signature can be re-transformed again by the proxy. In a single-use scheme, the proxy can transform only the signatures that have not been transformed.

3) **Private Proxy**: The re-signature key can be kept secret by the proxy in a private proxy scheme, but can be recomputed by observing the proxy passively in a public proxy scheme.

4) **Transparent**: In a transparent scheme, a signature on the same message signed by the delegator is computationally indistinguishable from a signature transformed by a proxy.
5) **Key-Optimal:** In a key-optimal scheme, a user is required to protect and store only a small constant amount of secrets no matter how many signature delegations the user gives or accepts.

6) **Non-interactive:** The delegatee is not required to participate in a delegation process.

7) **Non-transitive:** A re-signing right cannot be re-delegated by the proxy alone.

8) **Temporary:** A re-signing right is temporary.

In Indocrypt 2007, Shao Jun provided two proxy re-signature schemes without random oracle [5]. They first propose a multi-use bidirectional proxy re-signature scheme, denoted as $S_m$, which is existentially unforgeable in the standard model. And then, they extend $S_m$ to be a multi-use bidirectional ID-based proxy re-signature scheme, denoted by $S_{id-m}$, which is also existentially unforgeable in the standard model. Both of these two proposed schemes are computationally efficient, and their security bases on the Computational Diffie-Hellman (CDH) assumption.

**B. Our work**

In this paper, based on Jun's approach [5], we combine the proxy re-signature with certificateless cryptography, and first propose a certificateless bidirectional proxy re-signature scheme. Based on the certificateless cryptography, the new scheme removes key escrow in ID-based scheme and solves the using of certificate in certificate-based scheme. In addition, it avoids two tradition types of attack in certificateless system and satisfies the properties of proxy re-signature. So, the scheme possesses the merits of certificateless and proxy re-signature.

**C. The application of our scheme**

Our scheme can also be applied in many applications, including forming weak group signatures, simplifying key management, simplifying certificate management [4]. But our scheme has a better merit. For example, in the paper [4] gives an E-passports example. Suppose Eve from Eden arrives in New York and shows US border patrol a signature $\sigma_{\text{E}}$ from Eden. The border patrol officer checks this signature and translates it into $\sigma_{\text{E}}$, stating that Eve has passed the border patrol check. Eve next takes her passport to the customs officer. The customs officer need only verify passport against one public key – that of border patrol – and if it checks out and she passes customs, he can translate the signature into $\sigma_{\text{C}}$, etc. After that she can go in New York. But if somebody forges the primitive signature $\sigma_{\text{C}}$, he can also go in New York. In our scheme, the user’s private key is consisted of two parts, one is the partial private key $D_{\text{id}}$ generated by KGC and another is the secret value $\chi_{\text{id}}$ chosen by the user himself, so the security of private key and $\sigma_{\text{C}}$ can be ensured, nobody can forge the signature and cheat the checking.

**II. BILINEAR PAIRING AND DIFFIE-HELLMAN PROBLEM**

**A. Bilinear pairing**

Let $G_1$ and $G_2$ be additive and multiplicative cyclic groups of prime order $q$, and let $P$ be an arbitrary generator of $G_1$. Assume that the discrete logarithm in both $G_1$ and $G_2$ is hard. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ and satisfies the following properties:

- **Bilinear:** For all the $P, Q \in G_1$, and $a, b \in \mathbb{Z}_q^*$, the equation $e(aP, bQ) = e(P, Q)^{ab}$ holds;
- **Non-degenerate:** There exists $Q \in G_1$, if $e(P, Q) = 1$, then $P = 0$;
- **Computable:** For $P, Q \in G_1$, there is an efficient algorithm to compute $e(P, Q)$.

**B. Computational Diffie-Hellman problem**

Computational Diffie-Hellman (CDH) problem: Let $G$ be a group of prime order $p$ and let $g$ be a generator of $G$. The CDH problem is as follows: Given $(g, g^a, g^b)$ for any $a, b \in \mathbb{Z}_q^*$ compute $g^{ab}$.

**III. BIDIRECTIONAL PROXY RE-SIGNATURE**

In this subsection, we briefly review the definitions and the external security about bidirectional proxy re-signatures, which follow that in [4].

**A. Definition**

A bidirectional proxy re-signature scheme is a tuple of (possibly probabilistic) polynomial time algorithms $(\text{KeyGen}, \text{REKey}, \text{Sign}, \text{RESign}, \text{Verify})$, where:

- $(\text{KeyGen}, \text{Sign}, \text{Verify})$ form the standard key generation, signing, and verification algorithms.
- On input $(sk_1, sk_2)$, the re-signature key generation algorithm $\text{REKey}$ outputs a key $rk_{sk, a}$ for the proxy where $sk_1$ and $sk_2$ are the secret key of A and B, respectively.
- On input $rk_{sk, a}$, a signature $\sigma$, a message $m$, and a public key $pk_1$, the re-signature function, $\text{RESign}$, outputs a new signature $\sigma'$ on message $m$ corresponding to $pk_a$, if $\text{Verify}(pk_a, m, \sigma) = 1$ and $\bot$ otherwise.

**B. Correctness**

For any message $m$ in the message space and any key pairs $(pk, sk), (pk', sk') \leftarrow \text{KeyGen}(1^t)$, let $\sigma = \text{Sign}(sk, m)$ and $rk \leftarrow \text{REKey}(sk, sk')$. Then the following two conditions must hold:

$$\text{Verify}(pk, m, \sigma) = 1 \quad \text{and} \quad \text{Verify}(pk', m, \text{RESign}(rk, pk, m, \sigma)) = 1$$
C. External Security

External security protects a user from adversaries outside the system (i.e., excluding the proxy and any delegation partners). This is the proxy-equivalent of strong existential unforgeability under adaptive chosen-message attack (where an adversary cannot create a new signature even for a previously signed message).

Formally, for any non-zero \( n \in \text{poly}(k) \) and all PPT algorithms \( A \),
\[
\Pr\{ (pk_i, sk_i) \leftarrow \text{KeyGen}(1^k) \} \in \text{poly}(k),
\]
\[
(t, m, \sigma) \leftarrow A^{\text{Setup},\text{Sign},\text{Verify}} (\{pk_i\}_{i \in \{1,\ldots,n\}}),
\]
\[
\text{Verify}(pk_i, m, \sigma) = 1 \land (t, m, \sigma) \notin Q \land (1 \leq t \leq n)
\]
where the oracle \( O_{\text{sign}} \) takes as input an index \( 1 \leq j \leq n \) and a message \( m \in M \), and produces the output of \( \text{Sign}(sk_j, m) \); the oracle \( O_{\text{session}} \) takes as input two distinct indices \( 1 \leq i, j \leq n \), a message \( m \), and a signature \( \sigma \), and produces the output of \( \text{ReSign}(\text{ReKey}(sk_i, pk_j, sk_j, pk_j), pk_j, m, \sigma) \); and \( Q \) denotes the set of (index, message, signature) tuples \( (t, m, \sigma) \) where \( A \) obtained a signature \( \sigma \) on \( m \) under public key \( pk_j \) by querying \( O_{\text{sign}} \) on \( (t, m) \) or \( O_{\text{session}} (t, m, \cdot) \).

In the above security notion, the proxy is required to keep the re-signature keys private (or it is easy for an adversary to "win").

IV. BIDIRECTIONAL CERTIFICATELESS PROXY RE-SIGNATURE

A. Definition

A bidirectional certificateless proxy re-signature scheme consists of the following six random algorithms: \text{Setup}, \text{Keygen}, \text{ReKey}, \text{Sign}, \text{ReSign}, and \text{Verify} where:

- \( \{\text{Setup}, \text{Keygen}, \text{Sign}, \text{Verify}\} \) are the same as those in a standard certificateless signature.
- On input \( (sk_i, sk_j) = ((x_i, D_i), (x_j, D_j)) \), the re-signature key generation algorithm, \text{REKey}, outputs a key \( rk_{i \rightarrow j} \) for the proxy, where \( x_i(x_j) \) is A’s (B’s) secret value, \( D_i(D_j) \) is A’s (B’s) private partial key.
- On input \( rk_{i \rightarrow j} \), a public key \( pk_j \), a message \( m \), and a signature \( \sigma \), the re-signature algorithm, \text{RESign}, outputs a new signature \( \sigma’ \) on message \( m \) corresponding to \( pk_j \), if \( \text{Verify}(pk_j, m, \sigma) = 1 \) and \( \bot \) otherwise.

B. Scheme Implement

Based on paper [5] and [6], we present a new certificateless bidirectional proxy re-signature scheme, denoted as \( S_{AB} \). The scheme is consisted of six algorithms.

- \( \text{Setup} \): We assume the given length identities and messages are \( n_i \) and \( n_j \) \( (n_i, n_j, n_j \in \mathbb{Z}) \), respectively. We choose two collision-resistant hash functions, \( H_1 : \{0,1\}^* \rightarrow \{0,1\}^n \) and \( H_2 : \{0,1\}^* \rightarrow \{0,1\}^{n_2} \). Furthermore, choose a random number \( \alpha \in \mathbb{Z}_q \), compute \( g_1 = g_\alpha \), and then choose \( g_2 \in G_t \), \( u_i \in G_r \), and \( \alpha = \{ G_t, g_2, g_\alpha, g_1, g_2, u_i, u_i \} \).

And the master secret key is \( g_\alpha^\alpha \).

- \( \text{Keygen} \) : Input the identity \( ID_1 \), choose a random number \( r_1 \in \mathbb{Z}_q \), KG computes partial private key:
\[
D_1 = (d_1^u, d_1^\alpha) = (g_\alpha^u, \prod_{u \in U} u_i)^\alpha, g_\alpha^u
\]

where \( u = H_2(ID_1) \), \( U \subseteq [1, \ldots, n_j] \) is the set of indices \( i \) such that \( u[i] = 1 \), and \( u[i] \) is the \( i \)-th bit of \( u \). The user A picks \( x_i \in \mathbb{Z}_q^* \) and computes
\[
\text{pk}_1 = (pk_1, pk_1^\alpha) = (g_\alpha, g_\alpha^\alpha)
\]
then he sets \( sk_1 = (x_i, D_1) \). The user B sets his key in the same way.

- \( \text{ReKey} \) : Input two private keys \( (x_i, D_i), (x_j, D_j) \), output the re-signature key:
\[
rk_{i \rightarrow j} = D_j^x, D_j^\alpha = (d_j^{x_i})^\alpha, (d_j^\alpha)^\alpha
\]

(Note that the way we get the re-signature key is the same method and assumptions in [3].)

- \( \text{Sign} \) : Input the message \( m \in \{0,1\}^* \), the identity \( ID_2 \) and the key (\( x_i, D_i \)), output the signature \( r_2 \in \mathbb{Z}_q \).
\[
R_{m} = g_\alpha, R_m = (d_j^\alpha)^u
\]
\[
m = H_1(m, R_1, R_m, pk_j)
\]
then, output the sign:
\[
\sigma_i = ((d_j^\alpha)^m \prod_{m \in M} m_i)^\alpha, (d_j^\alpha)^\alpha, g_\alpha^u
\]
\[
=(V, R_1, R_m)
\]
where \( M \subseteq [1, \ldots, n_j] \) is the set of indices \( i \) such that \( m[i] = 1 \), and \( m[i] \) is the \( i \)-th bit of \( m \).

- \( \text{Resign} \) : Input a re-signature key \( rk_{i \rightarrow j} \), the public key \( pk_j \), a message \( m \) and a signature \( \sigma_i = (V, R_1, R_m) \),
check that $\text{Verify}(pk_s, m, \sigma_s) = 1$, if $\sigma_s$ does not verify, output $\bot$; otherwise output

$$\sigma_b = \left( V_A \left( \prod_{i \in M} t_i \right)^{\gamma}, R_A, \left( \prod_{i \in M} t_i \right)^{\gamma}, R_m \right)$$

$$= \left( \prod_{i \in M} t_i, \left( \prod_{i \in M} t_i \right)^{\gamma}, R_m \right)$$

$$= \left( V_A, R_A, R_m \right)$$

Proof: Verify: Input the public key $pk$, the message $m$ and the signature $\sigma$, compute $\hat{m} = H_m(m, R, R_m, pk)$, if

$$\begin{align*}
\mathcal{e}(g, pk^\gamma) &= \mathcal{e}(g, pk^\gamma), \\
\mathcal{e}(V, g) &= \mathcal{e}(pk^\gamma, g) \mathcal{e}(u \prod_{i \in U} u_i, R) \mathcal{e}(m \prod_{i \in M} t_i, R_m)
\end{align*}$$

output 1 and 0 otherwise.

V. SECURITY ANALYSIS

In the standard model, our certificateless bidirectional proxy re-signature scheme $S_{id}$ is correct, achieves the property of certificateless system and the external security about bidirectional proxy re-signatures.

A. Correctness

The proposed certificateless bidirectional proxy re-signature scheme $S_{id}$ is correct.

Proof: We use the following equations to show correctness:

$$\begin{align*}
\mathcal{e}(V, g) &= \mathcal{e}(\left( \prod_{i \in M} t_i \right)^{\gamma}, g) \\
&= \mathcal{e}(u \prod_{i \in U} u_i)^{\gamma}, R) \mathcal{e}(m \prod_{i \in M} t_i, R_m)
\end{align*}$$

B. Unforgeable

The proposed certificateless bidirectional proxy re-signature scheme $S_{id}$ is unforgeable and achieves the property of certificateless signature.

Proof: Our scheme is based on certificateless, the user’s private key is consisted of secret value $x_{id}$ and the partial private key $D_{id}$, so the re-signature key is the same consisted of $x_{id}$ and $D_{id}$. Even if the proxy colludes with one user, they can not get another user’s private key. Also they can not forge the signature. Other bidirectional proxy re-signature schemes do not have this property of our scheme $S_{id}$.

The certificateless system has two tradition types of attack, the public key replacement attack [7] and the malicious KGC attack [8].

In our scheme $S_{id}$, put the public key into the signature $\hat{m} = H_m(m, R, R_m, pk_s)$. After the attacker chooses the $H_m, r_m, \sigma_s$, he can not compute and replace the public key, so the scheme avoids the public key replacement attack.

Although KGC knows the master secret key and user’s partial private key $D_{id}$, he does not know the secret value $x_{id}$, he can not compute the private key and re-signature key, so he can not forge the signature.

C. External Security

The proposed certificateless bidirectional proxy re-signature scheme $S_{id}$ achieves the external security about bidirectional proxy re-signatures.

Proof: In the external security notion, an adversary from outside the system can not collude with the proxy, delegatee and delegator. In paper [5] author have proved their scheme $S_{id-mb}$ was existentially unforgeable under the Computational Diffie-Hellman (CDH) assumption in $G_1$. Compare with the scheme $S_{id-mb}$, our scheme $S_{id}$ just makes the bidirectional proxy re-signature under the certificateless system. So the proof of external security is the same with the $S_{id-mb}$. In addition, the way of setting the private key of the user in the certificateless system makes our scheme has better external security.

VI. CONCLUSIONS

The appearance of certificateless cryptography solves the key escrow problem and the using of certificate. In the paper we propose the first certificateless proxy re-signature scheme which make use of the merits of certificateless and proxy re-signature. From the Analysis, we can see that the new scheme is secure and efficient. So our scheme has wide applications in many areas.

ACKNOWLEDGMENTS

This work is supported by the National Natural Science Foundation of China (N0.60842006).

REFERENCES