A Novel Unidirectional Proxy Re-Signature Scheme and Its Application for MANETs

Xuan Hong*
Computer Science Department, Shanghai Normal University, Shanghai, CHINA
Email: sh.xuanhong@gmail.com

Yu Long
Computer Science and Engineering Department, Shanghai Jiaotong University, Shanghai, CHINA
Email: longyu@sjtu.edu.cn

Abstract— **Mobile ad-hoc networks (MANETs) have received a lot of attention recently, adapting proxy re-signature to work in such environments is challenging. In this paper, we propose a novel and efficient proxy re-signature scheme, which provides a flexible and secure way for authorizing the new nodes of mobile ad-hoc networks. The proposed scheme is unidirectional, single-use and non-transitive. Compared with the previous schemes, we need only a few public parameters and no pairing operation in signature and re-signature algorithms. We will also give the concrete security analysis of the proposed scheme. Its security is based on the Computational Diffie-Hellman assumption in the random oracle model. Thus, the scheme is suitable for the mobile ad-hoc networks, for it is completely non-interactive and is very simple.**

Index Terms— **Proxy Re-Signature, Unidirectional, Mobile Ad-Hoc Network, CDH Assumption**

I. Introduction

In 1998, Blaze, Bleumer and Strauss [1], [2] proposed the *proxy re-signature*, in which a semi-trusted proxy converts a delegatee's signature into a delegator's signature on the same message. The proxy transforms the signature with some secure information, but cannot generate original signature on behalf of the delegatee and the delegator. The first proxy re-signature scheme proposed by Blaze et al. [1] is bidirectional, multi-use. However, the scheme is not secure. It is possible for everybody to recover the re-sign key that should be stored at the proxy. This precludes the possibility of anyone having the re-signing right and the delegator can recover the delegatee's secret key or vice versa. Dodis and Ivan [3] revisited the notion of proxy cryptography. However, the user in their constructions should store secret share for each signature delegation the user gives or accepts. Ateniese and Hohenberger [4] proposed another two proxy re-signature schemes. One is bidirectional multi-use, and another is unidirectional single-use. The schemes above did not proved secure. Later, Shao et al. [5] proposed the first bidirectional proxy re-signature which is existentially unforgeable in the standard model and the first ID-based proxy re-signature scheme. Both the schemes suffered from the relatively large size of public parameters and the considerable computation overheads. However, Kim et al. [6] discussed about Shao et al. [5]'s scheme, by presenting an attack and making improvements. Furthermore, Libert and Vergnaud [7] proposed multi-use unidirectional proxy re-signature schemes based on bilinear groups in random oracle model and in standard model. Sunitha et al. [5] proposed another unidirectional proxy re-signature scheme with forward-secure. Chow et al. [8] showed how to design a generic unidirectional proxy re-signature scheme, and how to incorporate the concept of forward-security into the proxy re-signature. Deng and Song [9] present a proxy re-signature scheme based on quadratic residues, which is bidirectional and is secure under the random oracle model. More and more experts focus on the study of proxy re-signature with kinds of properties [10], [11], such as certificateless, traceability and blindness.

Mobile ad-hoc networks (MANETs) have received a lot of attention for its rapid expanding range of capabilities and various uses. The mobile ad-hoc network [12], [13] is a collection of nodes, in which the nodes communicate amongst each other using wireless radios and operate in dynamic and ad-hoc manners. Applications of mobile ad hoc networks are very extensive, such as military tactical operations, civil rapid development, data collection, sensor networks, and meeting room applications. In these application, nodes may be dynamically added to the system, however their public keys and identities could not be signed by the certificate authority (CA) before deployment. If the authorized node can do the job instead, it will be interesting. When the certification is need, a semi-trusted third party can translate the authorized node's signature into the CA's certification. Such primitive is referred to as threshold signatures in cryptography.

Security of mobile ad hoc networks has become a more sophisticated problem than security in other networks. Blaze et al. categorized re-signature scheme [1]. If the re-sign key allows the proxy to transform A's

This work is supported by the National Natural Science Foundation of China(NSFC) under grant No. 61003215 and Innovation Program of Shanghai Municipal Education Commission No.12YZ072.

Corresponding author:Xuan Hong. Mailing Address: Computer Science Department, Shanghai Normal University, 100 Guilin Road, Shanghai 200234, China.

doi:10.4304/jcp.7.7.1796-1800

signature to B's but not vice verse, then the scheme is called *unidirectional*. If re-sign key allows the proxy to transform A's signature to B's as well as B's to A's, then the scheme is called *bidirectional*. Depending on its application, a proxy re-signature scheme could satisfy other properties[5]: *multi-use, key optimal, non-transitive* and *temorary*. In a *multi-use* scheme, the re-signature can also be transformed, while in a *single-use* scheme, only the original signature can be transformed. In a *key optimal* scheme, a user is required to store only a small constant amount of secrets, regardless of how many signature delegations the user gives or accepts. In a *non-transitive* scheme, the proxy cannot delegate his re-signing right with itself alone. In a *temporary* scheme, the re-signing right is temporary. Nodes are receptive to being captured, compromised, and hijacked since they are units capable of roaming independently.

Proxy re-signatures provide a flexible and secure way for the nodes to join into the networks dynamically, all that is needed is the assurance that the authorized node can represent the CA. In the mobile ad-hoc networks, communication bandwidth may be constrained, expensive communication primitives like broadcast may not be available, and transmitting large amount of data or heavy interaction may be infeasible. Adapting proxy re-signature schemes to work in such environments is challenging.

In this paper, we make the following **contributions**. First, we give the formal definition of unidirectional proxy re-signature, which adopt Shao et al.'s game-based definition [5] and make some modifications to make it suitable for unidirectional proxy re-signature. Shao et al.'s model requires both two users are corrupted, or both are uncorrupted, which increase the failure possibility of the re-sign key oracle. Our game-based definition no longer restricts the corruption of proxies between corrupted and uncorrupted parties. We set original signature security as well as re-signature security. The original signature should remain secure even when the re-sign key is exposed. In other words, the colluding delegatee and proxy can not forge the delegator's original signature, either the colluding delegator and proxy. Moreover, Shao et al.'s game define the bidirectional proxy re-signature, while we define the unidirectional case.

Furthermore, we give a concrete implementation of proxy re-signature. The scheme is unidirectional, single use, key optimal and non-transitive. It is very attractive for its simplicity. Compared with the previous schemes, our scheme needs only a few public parameters and no pairing operation in signature and re-signature algorithms. The colluding delegatee and proxy can not forge the delegator's original signature and vice versa. We protect the signing key of the delegator and the delegatee. Security of this scheme can be reduced to Computational Diffie-Hellman (CDH) assumption in the random oracle model [14].

The rest of the paper is organized as follows. Section II introduces some preliminaries. Section III presents the unidirectional proxy re-signature scheme. Section IV analyzes its security and performance. Conclude in section V with a brief summary.

II. Preliminaries

A. Proxy Re-Signature

In this section, we will give the definitions of single-use unidirectional proxy re-signature primitive. The game-based definition adopt Shao et al.'s game-based definition [5] and make some improvements. We don't restrict the corruption of proxies between corrupted and uncorrupted parties. We set original signature security, while the original signature remains secure even when the re-sign key is exposed.

Throughout the paper, we focus on the unidirectional proxy re-signature scheme, where the re-sign key from pk_A to pk_B should not provide the ability of computing the re-sign key from pk_B to pk_A. The proxy re-signature scheme is a tuple of algorithms (**KeyGen,ReKey,Sign,ReSign,Verify**):

- **KeyGen**$(1^k) \rightarrow (pk, sk)$. On input the security parameter 1^k, the key generation algorithm, **KeyGen**, outputs a public key pk and a secret key sk.
- **ReKey**$(sk_A, sk_B) \rightarrow rk_{A\rightarrow B}$. In the single-use unidirectional proxy re-signature scheme, on input two secret keys sk_A and sk_B, the re-sign key generation algorithm, **ReKey**, outputs a re-sign key $rk_{A\rightarrow B}$.

Remarks: the bidirectional proxy re-signature scheme would output the bidirectional re-sign key $rk_{A\leftrightarrow B}$ instead of unidirectional re-sign key $rk_{A\rightarrow B}$.

- **Sign**$(sk, m) \rightarrow \sigma$. On input the secret key sk and the message m, the signature algorithm, **Sign**, outputs a signature σ.
- **Resign**$(rk_{A\rightarrow B}, pk_A, m, \sigma) \rightarrow \sigma'$. On input the re-sign key $rk_{A\rightarrow B}$, the message m and the signature σ on m corresponding to pk_A, the re-signature algorithm, **Resign**, outputs a new signature σ' on m under pk_B.
- **Verify**$(pk, m, \sigma) \rightarrow f$. On input the public key pk, the message m and the signature σ, the verification algorithm, **Verify**, outputs 1 or 0.

1) Game-based Definition: In this section, we give the game-based definition. The game-based definition is proposed by formulating the requirements for correctness and consistency of proxy re-signature scheme.

The security notions we discussed here are existential unforgeability under adaptive chosen message attack (CMA). We adopt Shao et al.'s game-based definition but make some improvements. firstly, They require both two users are corrupted, or both are uncorrupted, Which increase the failure possibility of the re-sign key oracle. Our game-based definition no longer restricts the corruption of proxies between corrupted and uncorrupted parties. Secondly, we set original signature security as well as re-signature security. The original signature should remain secure even when the re-sign key is exposed. In other words, the colluding delegatee and proxy can not forge the delegator's original signature, either the colluding delegator and proxy. Furthermore, Shao et al.'s

game define the bidirectional proxy re-signature, while we define the unidirectional case.

PRS Correctness. The proxy re-signature scheme is perfectly correct if: For any $(pk, sk) \leftarrow \mathbf{KeyGen}(1^k)$, any m, it holds that $\mathbf{Verify}(pk, m, \mathbf{Sign}(sk, m)) = 1$; For any (pk_A, sk_A), (pk_B, sk_B) output by $\mathbf{KeyGen}(1^k)$, any m, $rk_{A\to B} \leftarrow \mathbf{ReKey}(sk_A, sk_B)$, $\sigma \leftarrow \mathbf{Sign}(m, sk_A)$, it holds $\mathbf{Verify}(pk_B, m, \mathbf{ReSign}(rk_{A\to B}, m, \sigma)) = 1$.

PRS Consistency. The proxy re-signature scheme is consistent if: For any message m, any signature σ, invokes the verification algorithms **Verify** twice get the same response.

(PRS-CMA game) The game consists of adversary $\mathcal{A}$ querying the following oracles, which can be invoked multiple times in any order:

- Corrupted Key Generation $\mathcal{O}_{CKeyGen}$: On input pk from $\mathcal{A}$, where pk was generated legally, return its corresponding secret key sk.

- Re-Sign Key Generation $\mathcal{O}_{ReKey}$: On input (pk_A, pk_B) from the adversary $\mathcal{A}$, where pk_A, pk_B were generated legally, return the re-sign key $rk_{A\to B} \leftarrow$ **ReKey**(sk_A, sk_B), where sk_A, sk_B are the secret keys that correspond to pk_A, pk_B.

- Signature $\mathcal{O}_{Sign}$: On input (pk, m) from the adversary $\mathcal{A}$, where pk was generated before by **KeyGen**, return the signature $\sigma \leftarrow$ **Sign**(sk, m), where sk is the secret keys corresponding to pk.

- Re-Signature $\mathcal{O}_{ReSign}$: On input (pk_A, pk_B, m, σ) from the adversary $\mathcal{A}$, where pk_A, pk_B were generated before by **KeyGen**, return the re-signature $\sigma' \leftarrow$ **ReSign** (**ReKey**$(sk_A, sk_B), m, \sigma)$, where sk_A, sk_B are the secret keys that correspond to pk_A, pk_B.

Original Signature Secure: $\mathcal{A}$ obtains a forgery (pk^*, m^*, σ^*), we say that $\mathcal{A}$ wins the PRS-CMA game with original signature secure if the followings hold: σ^* is a valid original signature on m^* under pk^*. pk^* is not a query to $\mathcal{O}_{CKeyGen}$. (pk^*, m^*) is not a query to $\mathcal{O}_{Sign}$.

Re-Signature Secure: $\mathcal{A}$ obtains a forgery (pk^*, m^*, σ^*), we say that $\mathcal{A}$ wins the PRS-CMA game with re-signature secure if the followings hold: σ^* is a valid re-signature on m^* under pk^*. pk^* is not a query to $\mathcal{O}_{CKeyGen}$. (pk^*, m^*) is not a query to $\mathcal{O}_{Sign}$. $(\diamondsuit, pk^*)$ is not a query to $\mathcal{O}_{ReKey}$, where $\diamondsuit$ denotes any public key. $(\diamondsuit, pk^*, m^*, \heartsuit)$ is also not a query to $\mathcal{O}_{ReSign}$, $\heartsuit$ denotes any signature.

Denote $\mathcal{A}$'s probability to forge a valid original signature or a valid re-signature by $Adv_{\mathcal{A}} = Pr[\mathcal{A}succeeds]$. A proxy re-signature scheme is existential unforgeable under adaptive chosen message attack if for every adversary $\mathcal{A}$, $Adv_{\mathcal{A}}$ is negligible.

B. The Computational Diffie-Hellman Assumption (CDH)

Let $\mathbb{G}$ be a group of prime order p and g be a generator of $\mathbb{G}$. Given $\langle g, g^a, g^b\rangle$ for some $a, b \in {\mathbb{Z}_p}^*$, compute g^{ab}. An algorithm $\mathcal{A}$ has advantage ε in solving CDH in $\mathbb{G}$ if $Pr[\mathcal{A}(g, g^a, g^b)] \geq \varepsilon$, where the probability is over the random choice of a, b in ${\mathbb{Z}_p}^*$ and the random choice of $g \in \mathbb{G}^*$.

It will simplify the reading our proof by using the following equivalent problem of CDH, modified CDH. The mCDH assumption is identical to the CDH assumption, except also be given h, h^a. The mCDH problem is as follows: given $\langle g, g^a, g^b, h, h^a\rangle$ for some $a, b \in {\mathbb{Z}_p}^*$, compute g^{ab}, where g, h be generators of $\mathbb{G}$.

Theorem 2.1. *If mCDH is solved in $\mathbb{G}$ with probability ε, then CDH is solvable in $\mathbb{G}$ with probability ε; and vice versa.*

Proof. (CDH $\Rightarrow$ mCDH) It is observable.

(mCDH $\Rightarrow$ CDH) On CDH input $\langle g, g^a, g^b\rangle$, randomly select $t \in {\mathbb{Z}_p}^*$, let $h = g^t, h^a = (g^a)^t$, query the mCDH solver on input $\langle g, g^a, g^b, h, h^a\rangle$. Observe that when the mCDH solver outputs its response g^{ab} with probability ε, by substitution, we have g^{ab} for the CDH solver with probability ε. □

III. Proxy Re-Signature Scheme

A. Proxy Re-Signature Scheme

Our scheme requires a bilinear map, $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ operates over two groups $\mathbb{G}_1$, $\mathbb{G}_2$ of prime order $p = \Theta(2^k)$. The global parameters are $(e, p, \mathbb{G}_1, \mathbb{G}_2, g, h, H)$, where g and h are generators of $\mathbb{G}_1$, and H is a hash function from arbitrary strings to elements in $\mathbb{Z}_p$. Scheme $\prod_{PRS}$=(**KeyGen, ReKey, Sign, ReSign, Verify**) is described as follows:

- KeyGen: On input the security parameter 1^k, select a random $a \in {\mathbb{Z}_p}^*$, and output the key pair $pk = g^a$ and $sk = a$.

- ReKey: On input two secret keys $sk_A = a$, $sk_B = b$, output the re-sign key $rk_{A\to B} = h^{b/a}$ and $rk_{A\to B}{}' = h^{1/a}$.

- Sign: On input secret key $sk = a$ and message m, select a random $r \in {\mathbb{Z}_p}^*$, set $R = g^r, K = h^{r/a}$, $\delta = a \cdot H(m||R||K) + r$, and output triple $\sigma = (\delta, R, K)$. We call this form *the original signature*.

- ReSign: On input the re-signature key $rk_{A\to B}$, public key pk_A, original signature $\sigma = (\delta, R, K)$, and message m, check that **Verify**$(pk_A, m, \sigma) = 1$. If it holds, choose $r' \in {\mathbb{Z}_p}^*$, compute $K' = (rk_{A\to B}{}')^{r'}$, set $\delta' = (rk_{A\to B})^{\delta + r'}$, and output $\sigma' = (\delta', R, K, K')$; otherwise, output $\perp$. We call this form *the re-signature*. Since $\delta = a \cdot H(m|R|K) + r$, the re-signature $\delta' = (rk_{A\to B})^{\delta} = h^{b\cdot H(m|R|K)} \cdot K^b \cdot K'^b$.

- Verify: On input public key pk, message m and the purported signature σ, set $\omega = H(m|R|K)$, do:

1) If $\sigma = (\delta, R, K)$ is an original signature, δ here equals $a \cdot H(m|R|K) + r$. That is to say, if $g^{\delta} \equiv {pk_B}^{\omega} \cdot R \mod p$, it is a correct original signature, the scheme outputs 1, otherwise outputs 0 for instead.
2) If $\sigma = (\delta, R, K, K')$ is a re-signature, δ here equals $h^{b\cdot H(m|R|K)} \cdot K^b \cdot K'^b$. That is to say, if $e(\delta', g) = e(h, pk_B)^{\omega} \cdot e(K, pk_B) \cdot e(K', pk_B)$, it is a correct re-signature, the scheme outputs 1, otherwise output 0 for instead.

The proposed scheme is composed of these five algorithms. they may be executed by the same parties or other parties, they may have potentially related inputs and the scheduling of message delivery may be adversarily coordinated. Furthermore, the local outputs of a protocol execution may be used by other protocols in an unpredictable way.

B. Security

The correctness and consistency properties are easily observable. We now show that our scheme is PRS-CMA secure in the random oracle model, where cryptographic hash functions are replaced by a random oracle. This model was rigorously formalized and fully exploited by Bellare and Rogaway [15], and thereafter used in numerous papers.

Theorem 3.1. *If Computational Diffie-Hellman (CDH) assumption holds in $\mathbb{G}_1$, then the proposed unidirectional proxy re-signature is correct and existentially unforgeable under PRS-CMA game in the random oracle model.*

Proof. Recall that CDH and mCDH are equivalent, the theorem can also be proved as follows. If there exists an adversary $\mathcal{A}$ that can break the above proxy re-signature scheme with non-negligible probability ε in time t after making at most q_S sign queries, q_{RS} resign queries, q_K corrupted key queries, q_{RK} rekey queries and q_H hash queries, then there also exists an adversary $\mathcal{B}$ that can solve the mCDH problem in $\mathbb{G}_1$ with probability $\frac{1}{\sqrt{q_H}}$ in time $t + O(t(k) + q_H \cdot \tau)$.

On input (g, g^a, g^b, h, h^a), the mCDH adversary $\mathcal{B}$'s goal is to compute g^{ab}. $\mathcal{B}$ sets up the global parameters for $\mathcal{A}$: the security parameter $k \geq |p|$, the groups $\mathbb{G}_1 = \langle g \rangle$, $\mathbb{G}_2$, their prime order p, and the mapping e. The system parameters are $(e, p, \mathbb{G}_1, \mathbb{G}_2, g, h, H)$, where H is random oracle.

Queries: $\mathcal{B}$ builds the following oracles:

$\mathcal{O}_{Hash}$: On input (m, R, K), $\mathcal{B}$ checks if (m, R, K) is recorded in database $\mathcal{D}_H$. If not, selects random $\omega \in \mathbb{Z}_p$ and record (m, R, K, ω). $\mathcal{B}$ outputs ω.

$\mathcal{O}_{CKeyGen}$: $\mathcal{B}$ chooses random $x_i \in \mathbb{Z}_p$, and outputs $(pk_i, sk_i) = (g^{x_i}, x_i)$.

$\mathcal{O}_{ReKey}$: On input (pk_i, pk_j), $\mathcal{B}$ returns $rk_{i \to j} = h^{j/i} = (h^j)^{1/i}$. if pk_i and pk_j are both corrupted, or pk_i is uncorrupted and $pk_j$is corrupted, B returns $rk_{i \to j} = h^{j/i} = (h^j)^{1/i}$; else, this input is illegal.

$\mathcal{O}_{Sign}$: On input (pk, m), if pk is corrupted, $\mathcal{B}$ returns the signature $\sigma = (\delta, R, K)$, where $\delta = a \cdot H(m|R|K) + r$. Otherwise, $\mathcal{B}$ randomly selects u, v. Sets $R = g^u pk^v \mod p$, $\delta = u$, and $K = h^{r/a} = g^b$. The challenger records $\omega = H(m|R|K) = -v$ to the $\mathcal{D}_H$ as the hash response to (m, R, K). $\sigma = (\delta, R, K)$ has the correct signature as in the actual scheme.

$\mathcal{O}_{ReSign}$: On input (pk_i, pk_j, m, σ), if **Verify**$(pk_i, m, \sigma) = 1$, $\mathcal{B}$ invokes the re-signature algorithm **ReSign**$(\mathcal{O}_{ReKey}(pk_i, pk_j), pk_i, m, \sigma)$ and outputs the result; otherwise, outputs $\perp$.

Forgery: If $\mathcal{B}$ does not abort as a consequence of one of the queries above, $\mathcal{A}$ will, with probability at least ε, return a message m^* and a valid σ^* on m^*. If the forgery is the original signature, we have the conclusion that the triplet ElGamal-family signature which is provably unforgeable under ROM following the forking lemma. If the forgery is the re-signature, the forgery must be of the form $\delta^* = (h^\omega \cdot K)^a = (h^a)^\omega \cdot g^{ab}$. To solve the mCDH instance, $\mathcal{B}$ outputs $g^{ab} = \delta^* \cdot (h^a)^{-\omega}$.

To conclude, we analyze the probability that $\mathcal{B}$ completes the simulation without aborting. The probability of $\mathcal{B}$ is $Pr[\mathcal{B}succeeds] = Pr[E_1 \vee E_2]$, where E_1 denotes forge the original signature and E_2 denotes forge the re-signature, respectively. $Pr[E_1] = \frac{1}{\sqrt{q_H}}$, $Pr[E_2] = \frac{1}{q_H}$, hence $Pr[\mathcal{B}succeeds] \geq \frac{1}{\sqrt{q_H}}$. The time complexity of $\mathcal{B}$ is $t + O(t(k) + q_H \cdot \tau)$.

Thus, the theorem follows. □

IV. Discussion

A. Performance

This scheme is unidirectional, single-use and non-transitive. The proxy transforms manager B's signature to company A's signature, and the verifier can be convinced that the signature contains the manager B's signature and the seal maintainer (semi-trusted proxy) of the company.

With our best knowledge, there is few provable secure proxy re-signature scheme. Ateniese and Hohenberger [4] proposed unidirectional single-use scheme, which did not proved secure. Kim et al. [6] discussed about Shao et al. [5]'s scheme, by presenting an attack and making improvements. Thus, we compare our security definition with Shao et al.'s.

Compared with the previous schemes, it is simple and efficient. In the signature algorithm and re-signature algorithms, the parties only need modular and multiplicative operations within the group $\mathbb{G}_1$. The scheme does the time consuming paring operation only when verifying the re-signature. Unlike Kim et al.'s scheme, which has relatively large size of public parameters. We have a few public parameters $(e, p, \mathbb{G}_1, \mathbb{G}_2, g, h, H)$. The security of our scheme can be reduced to Computational Diffie-Hellman (CDH) assumption in the random oracle model. Furthermore, since each user just stores one signing key, the scheme is also key optimal.

B. Application

Mobile ad-hoc networks (MANETs) have received a lot of attention for its rapid expanding range of capabilities and various uses. The mobile ad-hoc network is a collection of nodes, in while the nodes communicate amongst each other using wireless radios and operate in dynamic and ad-hoc manners. Applications of mobile ad hoc networks are very extensive, such as military tactical operations, civil rapid development, data collection, and sensor networks. In these application, nodes may be dynamically added to the system, however their public key and identification could not be signed by the certificate

authority (CA) before deployment. If the authorized node can do the job instead, it will be interesting. When the certification is need, a semi-trusted third party can translate the authorized node's signature into the CA's certification.

Proxy re-signatures provide a flexible and secure way for the nodes to join into the networks dynamically, all that is needed is the assurance that the authorized node can represent the CA. In the mobile ad-hoc networks, communication bandwidth may be constrained, expensive communication primitives like broadcast may not be available, and transmitting large amount of data or heavy interaction may be infeasible. Adapting proxy re-signature schemes to work in such environments is challenging.

We suggest that the proposed scheme can minimize the damage caused by agents' misuse. In this scheme, all the signing is still done by the mobile agent, all the mobile agents hold its secret sharing. Only when more than t mobile agents are corrupted, the mobile agents system was insecure. Compared with the previous threshold proxy signature schemes, the proposed scheme reduces large amounts of modular exponential computations and communications. Therefore, it can be applied to the mobile agent. The security of this scheme depends on the underlying threshold signature schemes. The proposed scheme is suitable for the mobile ad-hoc networks, for it is completely non-interactive and has simple algorithm.

V. Conclusion

In this paper, we formally present a novel proxy re-signature scheme, which is unidirectional, single-use, key optimal and non-transitive. The proposed scheme is simpler, and the security can be reduced to Computational Diffie-Hellman assumption in the random oracle model.

Acknowledgment

We thank Mi Wen and Xiaomin Hu for their numerous discussions concerning this work, and the reviewers for their detailed comments.

References

[1] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *EUROCRYPT 1998*, vol. LNCS, no. 1403, 1998, pp. 127–144.

[2] M. Blaze and M. Strauss, "Atomic proxy cryptography," in *Technical reports*. AT&T Research, 1997.

[3] Y. Dodis and A. Ivan, "Proxy cryptography revisited," in *Network and Distributed System Security Symposium 2003*, 2003.

[4] G. Ateniese and S. Hohenberger, "Proxy re-signatures: New definitions, algorithms, and applications," in *ACM CCS 2005*, 2005, pp. 310–319.

[5] J. Shao, Z. Chao, L. Wang, and X. Liang, "Proxy re-signature schemes without random oracles," in *Indocrypt 2007*, vol. LNCS, no. 4859, 2007, pp. 197–209.

[6] K. Kim, I. Yie, and S. Lim, "Remark on shao et al's bidirectional proxy re-signature scheme in indocrypt 2007," *International Journal of Network Security*, vol. 8, pp. 308–311, 2009.

[7] B. Libert and D. Vergnaud, "Multi-use unidirectional proxy re-signatures," in *the 15th ACM conference on Computer and communications security 2008*, 2008.

[8] S. Chow and R. Phan, "Proxy re-signatures in the standard model," in *ISC 2008*, vol. LNCS, no. 5222, 2008, pp. 260–276.

[9] Y. Deng and G. Song, "Proxy re-signature scheme based on quadratic residues," *Journal of Networks*, vol. 6, pp. 1459–1465, 2011.

[10] D. Guo, P. Wei, D. Yu, and X. Yang, "A certificateless proxy re-signature scheme," in *Proceedings - 2010 3rd IEEE International Conference on Computer Science and Information Technology, ICCSIT 2010*, vol. 8, 2010, pp. 157–161.

[11] Y. Deng, "A blind proxy re-signatures scheme based on random oracle," *Advanced Materials Research*, vol. 204-210, pp. 1062–1065, 2011.

[12] E.Huang, J. Crowcraft, and I. Wassell, "Rethinking incentives for mobile ad hoc networks," in *Proc. SIGCOMM'04 Workshops 2004*, 2004, pp. 191–196.

[13] J. Schiller, *Mobile Communication*. Addison-Wesley Professional, 2008.

[14] M. Bellare and P. Pogaway, "Random oracles are practical: A paradigm from designing efficient protocols," in *ACM 1993*, 1993, pp. 62–73.

[15] N. Sunitha and B. Amberker, "Proxy re-signature schemes," in *ICISS 2008*, vol. LNCS, no. 5352, 2008, pp. 156–157.

Xuan Hong currently a lecture in the computer sciences department of Shanghai normal university. She received her PhD degrees in computer science from Shanghai Jiaotong University, shanghai, China, in 2009.

Her research interests include encryption, digital signature, cryptographic protocol and digital right management.

Yu Long currently a assistant researcher in the department of computer science and engineering of Shanghai Jiaotong Univeristy. She received her PhD degree in information security from Shanghai Jiaotong University, Shanghai, China, in 2008.

Her research interests include network security, cryptography and distributed systems.