*Machine Learning and Artificial Intelligence*
*A.J. Tallón-Ballesteros and C. Chen (Eds.)*


*doi:10.3233/FAIA200813*

# An Identity-Based Directed Proxy Multi-Signature Scheme

Weiping ZUO[1]
*Department of Mathematics, Tianshui Normal College, Tianshui, China*

**Abstract.** Directed signature is introduced when the signed message contains privacy which is sensitive to the receiver, it is widely used in some special occasions involving signature privacy, such as electronic bidding, electronic voting, personal business activities, etc. This paper presents a new directed proxy multi-signature scheme, which integrated the directed signature and proxy multi-signature. In the proposed scheme, the agent generate a signature on behalf of the delegators, only a receiver specified by the delegator convince whether the truth of signature or not. At last, we analyze the characteristics and discuss the security of the scheme.

**Keywords.** Identity, Directed signature, Bilinear map

## 1. Introduction

Shamir[1] proposed identity based cryptosystem, in this type of cryptosystem, the public key of user is obtained directly from his basic information, such as username, ID number, Electronic mailbox, address and so on, while the secret key is obtained from private key generator which is called PKG and it is a trusted third party. The identity based cryptosystem has many advantages by comparison with public key cryptosystem, which make the acquisition of the public key simply, reduce the key management burden greatly and bring great convenience in practical application.

In the real world, people often need to delegate their signing rights to a reliable agent, which ensures the agent can sign on documents on behalf of the delegator, the same as in the electronic information society. In order to solve this problem, In 1996, Mambo[2] introduced the notion of proxy signature, in this type of schemes, an agent obtain the signing right form a delegator, and then the agent generates a signature on behalf of the delegator. Due to the technology of proxy signature is widely used in many fields, the study on proxy signature has attracted more and more attention. But in many electronic scenarios, sometimes it may be necessary to allow an agent to sign on behalf of the delegators at same time, for example, many departments of a company need to appoint an agent to sign on documents jointly at the same time, which is the concept of proxy multi-signature in fact, and the first concrete scheme was given by Yi[3]. Later, more and more concrete schemes [4-8] were introduced.

In the traditional signature, the signer has no restrictions on a verifier of the signature, anyone who obtains the signature convince whether the truth of signature or not. But, the public validity of signature is undesirable in some special occasions

[1] Corresponding Author; E-mail: wpzuo@126.com.

involving signature privacy, such as electronic bidding, electronic voting, personal business activities, etc. In order to protect signature privacy, Lim[9] introduced the concept of directed signature, in this type of schemes, only the receiver specified by the delegator convince whether the truth of signature or not with his secret key, while the others cannot convince it. Later, more and more concrete directed schemes [10-14] were introduced. Motivated with the above, we present a new concrete directed scheme which integrated the directed signature and proxy multi-signature. The new scheme has the characteristic of designated verifiability and it is widely used in many electronic scenarios.

The rest part of our paper has been organized as follows. The second section introduces the bilinear pairings and complexity assumption. In the third section, a new concrete directed proxy multi-signature scheme is proposed. We discuss the security of our scheme in the fourth section. The fifth section concludes remarks.

## 2. Preliminaries

Some preliminaries which include bilinear map and complexity assumption are given in this section.

### *2.1. Bilinear Map*

Suppose $G_1$ be a group with addition, $G_2$ be a group with multiplication, where $G_1$ has a generator $P$ and a prime order $q$, the same as $G_2$. bilinear map $e: G_1 \times G_1 \to G_2$, which has characteristics as follows.

- Bilinearity: $\forall a, b \in Z_q^*$, $P, Q \in G_1$, $e(aP, bQ) = e(P, Q)^{ab}$.
- Nondegeneracy: $\exists P \in G_1$, such that $e(P, P) \neq 1$.

### *2.2. Complexity Assumption*

This section revisits the computational Diffie-Hellman problem.

- Computational Diffie-Hellman(CDH) Problem: $\forall a, b \in Z_q^*$, $P, aP, bP \in G_1$, compute $abP$, where $G_1$ is a group with addition and it has a generator $P$ and a prime order $q$.
- Computational Diffie-Hellman Assumption: Suppose that $\mathrm{A}$ is a adversary, if no such $\mathrm{A}$ can solve CDH problem in polynomial time at most $t$ with probability at least $\varepsilon$.

## 3. Our Scheme

There are three type of entities which include the delegators $A_1 \ldots A_n$, the agent $B$ and the designated receiver $C$. $A_i$ ($i$=1...$n$) with identity $ID_i$, $B$ with identity $ID_B$, $C$ with identity $ID_C$. Our scheme is described as follows.

### *3.1. Setup*

Assume $G_1$ be a group with addition , $G_2$ be a group with multiplication, where $G_1$ has a generator $P$ and a prime order $q$ , the same as $G_2$ . bilinear map $e: G_1 \times G_1 \to G_2$ , $k$ is a system security parameter. $H_i : \{0,1\}^* \to G_1 (i = 1..3)$ , $H_4 : \{0,1\}^* \to Z_q^*$ are cryptographic hash functions. **PKG** randomly chooses $s \in Z_q^*$ and regards it as secret key, then computes $P_{pub} = sP$ and keep $s$ secretly.

### *3.2. Extraction*

According to $ID_i$ of a user, **PKG** generates $Q_{ID_i} = H_1(ID_i)$ and $s_{ID_i} = sQ_{ID_i}$ , where $Q_{ID_i}$ is public key, $s_{ID_i}$ is private key. Thus, delegator $A_i$ ($i$=1...$n$) has the key pair $(Q_{ID_i}, s_{ID_i})$ respectively, the agent $B$ has the key pair $(Q_{ID_B}, s_{ID_B})$, the designated receiver $C$ has the key pair $(Q_{ID_C} = s_{ID_C})$ .

### *3.3. Proxy Key Generation*

$A\{A_i \ldots A_n\}$ and $B$ do the following steps to finish delegation under $w$, where $w$ is the warrant for signed message. Finally, $B$ generates the proxy key $s_P$ .

- For all $i$=1...$n$ , $A_i$ computes $R = \sum_{i=1}^{n} R_i$ , $V_i = s_{ID_i} + r_i H_2(w \| \mathrm{R})$ , sends $(w, R_i, V_i)$ to $B$.
- For all $i$=1...$n$ , $B$ confirms $(w, R_i, V_i)$ by an equation such that $e(P, V_i) = e(P_{pub}, Q_{ID_i}) e(R_i, H_2(w \| R))$. If the equation holds, he accepts signature, otherwise rejects.
- For all $i$=1...$n$ , If $B$ confirms $(w, R_i, V_i)$ , he computes $s_P = \sum_{i=1}^{n} V_i + H_4(w \| R \| ID_B) s_{ID_B}$ .

### 3.4. Proxy Multi-Signature Generation

$B$ can sign a message $m \in \{0,1\}^*$ on behalf of $A\{A_i...A_n\}$ by using $s_P$, he performs the following steps.

- Randomly chooses $u_1, u_2 \in Z_q^*$ and computes $U = u_1 P$, $W = u_2 Q_{ID_B}$.
- Computes $V = s_P + u_1 H$, where $H = H_3(m \| w \| R \| e(s_{ID_B}, u_2 Q_{ID_C}))$.
- The directed proxy multi-signature is $\sigma = (w, R, U, W, V)$.

### 3.5. Proxy Multi-Signature Verification

In order to verify $\sigma = (w, R, U, W, V)$, $C$ checks the signed message $m$ and the delegation, if $m$ accords with $w$ and the delegation which $A\{A_i...A_n\}$ authority $B$ is effective, $C$ performs the following computations with his private key $s_{ID_C}$.

- Computes $H = H_3(m \| w \| R \| e(s_{ID_C}, W))$ and convince whether the equation as follows holds or not.□
- $e(P,V) = e(P, \sum_{i=1}^{n} (Q_{ID_i}) e(P,R)^{H_2(w\|R)} e(P_{pub}, Q_{ID_B})^{H_4(w\|R\|ID_B)} e(U,H)$

## 4. The Analysis of Our Scheme

This section analyze our scheme in detail, the analysis shows that our scheme satisfies the unforgeability, the designated verifiability and the nonrepudiation.

### 4.1. Correctness

We can put the mathematical formula of proxy multi-signature generation phase (section 3.4) into the equation of proxy muti-signature verification phase (section 3.5), and confirm whether the equation as follows holds or not.

$$
\begin{aligned}
e(P,V) &= e(P, s_P + u_1 H) = e(P, \sum_{i=1}^{n} (V_i + H_4(w \| R \| ID_B)) + u_1 H) \\
&= e(P, \sum_{i=1}^{n} (s_{ID_i}) e(P, \sum_{i=1}^{n} r_i H_2(w \| R)) e(P, H_4(w \| R \| ID_B) s_{ID_B}) e(P, u_1 H) \\
&= e(P, \sum_{i=1}^{n} (Q_{ID_i}) e(P,R)^{H_2(w\|R)} e(P_{pub}, Q_{ID_B})^{H_4(w\|R\|ID_B)} e(U,H)
\end{aligned}
$$

where $H = H_3(m \| w \| R \| e(s_{ID_C}, W))$.

### 4.2. Designated Verifiability

In phase of verification, $C$ must use secret key $s_{ID_C}$ compute $H$, but $H=H_3(m \| w \| R \| e(s_{ID_C}, W))$ includes the private key $s_{ID_C}$ of $C$. Only $C$ verify the whether the truth of signature or not, any third party is unable to verify the truth of signature without the private key $s_{ID_C}$. Therefore, the proposed scheme satisfies the designated verifiability.

### 4.3. Unforgeability

The others tend to fake a valid directed signature is unfeasible without the proxy key $s_P$, Since $s_P = \sum_{i=1}^{n} V_i + H_4(w \| R \| ID_B) s_{ID_B}$ includes the private key $s_{ID_B}$ of $B$, however, $s_{ID_B}$ is kept secretly by $B$, Solving $s_{ID_B}$ from $s_p$ is equivalent to solving discrete logarithm problem. Therefore, the proposed scheme satisfies the unforgeability.

## 5. Conclusion

Due to the directed signature is applicable where the signed message contains privacy which is sensitive to the receiver and it is used in many electronic scenarios which including electronic transaction and personal business activities. Considering the significance of directed scheme, this paper present a new directed scheme. The new scheme is secure and it satisfies the security requirements of the unforgeability, the designated verifiability and the nonrepudiation.

## References

[1] A. Shamir. Identity-based cryptosystems and signature schemes, Advances in Cryptology: CRYPTO 1984, LNCS 196, Springer-Verlag Press, Berlin,1984, pp. 47-53.
[2] M. Mambo, K. Usuda and E. Okamoto. Proxy signature for Delegating signing operation, Proc of the 3rd ACM Conference on Computer and Communications Security, ACM Press, New York,1996, pp. 48-57.
[3] L. J. Yi, G. Q. Bai and G. Z. Xiao. Proxy Multi-Signature Scheme: a New Type of Proxy Signature Scheme, Electronics Letter, vol. 36, Jun. 2000, pp. 527-528.
[4] F. Cao, Z. F. Cao. A secure identity-based proxy multi-signature scheme, Information Sciences, vol. 179, Mar. 2009, pp.192-302.
[5] C. Hsu, T. Wu and W. He. New proxy multi-signature scheme, Applied Mathematics and Computation, vol. 162, Mar. 2005, pp.1201-1206.
[6] J. Ji, D. Li. A new proxy multi-signature scheme, Journal of Computer Research and Development, vol. 41, Apr. 2004, pp. 715-719.
[7] X. X. Li, K. H. Chen. Multi-proxy signature and proxy multi-signature schemes from bilinear pairings, LNCS 3320, Springer-Verlag Press, Singapore, 2004, pp. 591-595.
[8] H. Du, J. Wang, Y. N. Liu. Independent verification of proxy multi-signature scheme, International Journal of Computational Science and Engineering Vol. 9, Apr. 2014, PP. 301-311.
[9] C. H. Lim, P. J. Lee. Modified Maurer-Yacobi's Scheme and its applications,Proceedings of the Australasian Conference on Information Security and Privacy. Berlin: Springer-Verlag, 1992, pp. 308-323.

[10] J. Zhang, Y. Yang, X. Niu. Efficient Provable Secure ID-Based Directed Signature Scheme without Random Oracle, Advances in Neural Networks-ISSN 2009, LNCS 5553,Springer-Verlag Press, Berlin, pp. 318–327.
[11] Q. Wei, J. He, H. Shao. A directed signature scheme and its application to group key initial distribution, Proceedings of the International Conference on Interaction Sciences: Information Technology, Culture and Human. Seoul, Korea: ACM Press, 2009, pp. 265-269.
[12] D. X. Wang, H.M. Zhu,J.K. Teng. Directed signature scheme based on identity with Fairness, Journal of Yunnan University: Natural Sciences Edition, Vol. 33, Nov. 2011, pp. 658-661.
[13] W. P. Zuo, Y. F. Liu, S. F. Wang. An ID-based Designated-Verifier Proxy Multi-signature Scheme, Fourth International Conference on Multimedia, Information Networking and Security, 2012, pp. 576-579.
[14] N. B. Gayathri, R. V. Rao, P. V. Reddy. Efficient and Provably Secure Pairing Free ID-Based Directed Signature Scheme, International Symposium on Security in Computing and Communication, 2017, pp. 28-38.