密码学进展——CHINACRYPT'2006
第九届中国密码学学术会议论文集

王小云　杨义先　主编

中国科学技术出版社

密码学进展——CHINACRYPT'2006
第九届中国密码学学术会议论文集

王小云　杨义先　主编

中国科学技术出版社
·北京·

图书在版编目(CIP)数据

密码学进展:CHINACRYPT'2006 第九届中国密码学学术会议论文集/王小云,杨义先主编.
—北京:中国科学技术出版社,2006.8
ISBN 7-5046-2648-1

Ⅰ.密... Ⅱ.①王... ②杨... Ⅲ.密码—理论—学术会议—文集 Ⅳ.TN918.1—53

中国版本图书馆 CIP 数据核字(2006)第 102062 号

中国科学技术出版社出版
北京市海淀区中关村南大街 16 号 邮政编码:100081
电话:010—62103208 传真:010—62183872
http://www.kjpbooks.com.cn
科学普及出版社发行部发行
北京长宁印刷有限公司印刷
*
开本:889 毫米×1194 毫米 1/16 印张:20.5 字数:650 千字
2006 年 8 月第 1 版 2006 年 8 月第 1 次印刷
印数:1—700 册 定价:110 元

《密码学进展——CHINACRYPT'2006 第九届中国密码学学术会议论文集》

编　委　会

序　言

由中国密码学会主办、山东大学承办的第九届中国密码学学术会议——ChinaCrypt'2006于2006年10月13日至15日在中国济南山东大学举行。

本次会议共收到159篇投稿论文，每篇论文至少由两位专家评审。经程序委员会严格审阅，最后由程序委员会会议讨论决定，共录用其中的43篇形成此论文集。本论文集反映了近年来我国密码学领域的研究动态与学术水平。

本次会议得到了中国密码学会的大力支持。

我们衷心感谢为这次会议的成功举办作出贡献的所有人员。首先，感谢所有向本次会议投稿的科研人员对会议的关心与支持；感谢程序委员会的所有专家，他们在百忙之中从众多的投稿中遴选出最具代表性的论文作为本论文集的选编论文。我们还要特别感谢会议承办单位山东大学为本次会议的顺利召开所做出的精心安排与布置，感谢山东大学校长展涛教授对会议的大力支持与关注，同时感谢郑倩、王美琴、崔宝江老师和张海纳同学以及山东大学密码技术与信息安全教育部重点实验室（筹）的全体老师和研究生，他们为会议的筹备和组织安排付出了辛勤的劳动。最后还要感谢中国科学技术出版社责任编辑贾凤坡先生，他为本论文集的出版做了大量细致且繁琐的工作；本论文集的出版得到了中国科学技术出版社的大力支持，在此向他们表示衷心的感谢。由于这本论文集的编辑时间比较仓促，我们的经验和水平有限，论文集中难免出现纰漏，欢迎读者提出批评和指正。

王小云　杨义先

二〇〇六年八月

目　录

Pairing-based Proxy Ring Signature Scheme with Proxy Signer Privacy Protection

Lu Rongxing, Cao Zhenfu, Dong Xiaolei

Department of Computer Science and Engineering, Shanghai Jiao Tong University, 800 Dongchuan Road, Shanghai 200240, China

Email: rxlu.cn@gmail.com {cao-zf, dong-xl}@cs.sjtu.edu.cn

Abstract Proxy signature is a signature scheme that an original signer delegates his signing capability to a proxy signer, and then the proxy signer can create signatures on behalf of the original signer. Till now, various application requirements have been proposed and called for new proxy signature schemes. Among of them, the requirement of proxy signer privacy protection is quite important when the proxy signature scheme is applied to some practical applications where personal activities within organization should be kept secret to outside. However, to our best knowledge, most of the previously proposed proxy signature schemes with proxy signer privacy protection are insecure. Therefore, in this paper, aiming at providing the privacy protection for the proxy signer, we would like to present a new pairing-based proxy ring signature scheme and use techniques from provable security to analyze its security.

Key Words Proxy signature, ring signature, proxy ring signature, privacy protection, bilinear pairings, provable security

1 Introduction

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message, and possibly to ensure that the original content of the message remains to be unchanged. Due to its merits of easy transportability and security assurance, digital signature schemes have been widely used in the digital world. However, sheer simple digital signature schemes, such as RSA and ElGamal schemes, are not enough to satisfy some practical conditions. For instance, when an original signer is absent, he may wish to delegate his signing capability to a designated person. Therefore, to fulfill this requirement, the proxy signature was invented[14].

The concept of proxy signature was first introduced by Mambo, Usuda and Okamoto in 1996[14]. In a proxy signature scheme, an original signer delegates his signing capability to a proxy signer and then the proxy signer can sign messages on behalf of the original signer. Anyone accessible to the public keys of the original signer and proxy signer is able to verify the authenticity of the purported signature afterwards. Based on the delegation type in different applications, proxy signature schemes can be classified as full delegation, partial delegation and delegation by warrant scheme. On the other hand, depending on whether the original signer can generate the same proxy signatures as the proxy signer, they also can be classified into proxy-unprotected and proxy-protected scheme. In a proxy-protected scheme only the proxy signer can generate proxy signatures, while in a proxy-unprotected scheme either the proxy signer or the original signer can generate the same proxy signatures. Therefore, in many applications, proxy-protected schemes

are required to avoid the potential disputes between the original signer and the proxy signer.

Due to its wide applicability, research in proxy signature has become an active cryptographic area and many variations have been proposed in recent years. Following the first construction[14], a number of new schemes and variations have been presented, such as multi-proxy signature[6], proxy multi-signature[20], proxy blind signature[19], proxy blind multi-signature[9], and threshold proxy signature[21], and so on.

In 2002, Shum and Wei[18] extended Lee, Kim and Kim's scheme[10] and proposed a strong proxy signature scheme with proxy signer privacy protection. In Shum-Wei scheme, a proxy signer may sign messages on behalf of the original signer while protecting his privacy against any third party. Because of the proxy anonymity property, Shum-Wei scheme is suitable for some applications, in which it is necessary to protect the privacy of the participants. Unfortunately, both Sun and Hsieh[17] and Lee and Lee[11] showed that Shum-Wei scheme cannot maintain the property of strong unforgeability, since not only the proxy signer but also the original signer can generate valid proxy signatures.

The concept of ring signature was first formalized by Rivest, Shamir and Tauman[16] in 2001. A ring signature is considered to be a simplified group signature which consists of only users without managers. It protects the anonymity of signers since the verifier only knows that the signature comes from a member of a ring, but not whom the actually signer is. What's more, there is no way to revoke the anonymity of the signer. Therefore, ring signature is a useful tool to provide anonymity in many scenarios. For instance, if a member of a group wants to leak to the public media a secret information about the group, he can use ring signature scheme to sign this information and convince everyone outside that the information indeed comes from the group itself, without being accused of leaking the secret. In recent years, several ring signature schemes have been proposed (e.g., [4, 22, 7, and 24]).

In 2003, Zhang et al.[23] first proposed the concept of proxy ring signature. A proxy ring signature can be regarded as the combination (but not straightforward) of a general proxy signature scheme and a ring signature scheme, which allows an original signer to delegate his signing capability to a group of proxy signers and then any proxy signer can perform the signing operation for the original signer while preserve his anonymity. More precisely, a proxy ring signature scheme should satisfy the following properties①:

- **Distinguishability**: Proxy ring signatures are distinguishable from normal signatures by everyone.
- **Verifiability**: Any verifier can be convinced of the original signer's agreement on the signed message from a proxy signature.
- **Unforgeability**: Only those who belong to the proxy signers group delegated by the original signer can create a valid proxy ring signature for the original signer. Anyone else, including the original signer, cannot create a valid proxy signature.
- **Anonymity**: Any verifier cannot determine the identity of the real proxy signer who has computed a proxy ring signature on behalf of the original signer.
- **Prevention of misuse**: Any proxy signer cannot use the proxy key for other purposes other than generate a valid proxy signature. That is, she/he cannot sign messages that have not been authorized by the original signer.

Obviously, the proxy ring signature scheme provides the privacy protection on the proxy sign-

① To provide the anonymity of proxy signer, the properties of identifiability and undeniability are not considered in a proxy ring signature scheme.

er. Therefore, some specific personal activities within organization can be protected from outside. In these applications, when the proxy signer signs for the original signer, any verifier cannot tell the identity of the real proxy signer. In the literature[23], Zhang et al. proposed a proxy ring scheme from bilinear pairings[1]. However, due to the sequential operation in ring signature generation and verification phases, their scheme is not very efficient.

Motivated by previous work, in this paper, using the bilinear pairing, we would like to present a new proxy ring signature scheme with proxy signer privacy protection. Since our proposed scheme utilizes Zhang et al.'s new parallel ring signature[24], it is more efficient than the previous one[23]. Moreover, our proposed scheme is also provably secure in the random oracle model[3].

The rest of this paper is organized as follows. Section 2 introduces some notations used in the following scheme. Then, we give formal definitions for proxy ring signature scheme in Section 3 and review some basic concepts of bilinear pairings in Section 4. And in the next two sections, 5 and 6, we present our pairing-based proxy ring signature scheme with proxy signer privacy protection and use the techniques from provable security to analyze its security. Finally, we draw our conclusions in Section 7.

2 Notations

We let $N=\{1,2,3,\cdots\}$ be the set of positive integers. If x a string, then $|x|$ denotes its length, while if S is a set then $|S|$ denotes its cardinality. If $k\in N$ then 1^k denotes the string k ones. If S is a set then $s\rightarrow S$ denotes the operation of picking a random element s of S uniformly. We indicate that B is an original signer, and $PG=\{P_1,P_2,\cdots,P_n\}$ is a set of proxy signers delegated by B in the following scheme.

3 Definitions

In this section, following[5, 16], we formally define the proxy ring signature scheme, together with its security notions. A proxy ring signature (PRS) scheme is considered to be the combination of a general proxy signature scheme and a ring signature scheme, which consists of five algorithms: Key Generation, Delegation Signing, Delegation Verification, PRS Issuing and PRS Verification.

Definition 1 *A PRS scheme consists of the following five algorithms KG, DS, DV, PS, PV:*

(1) *Key Generation KG: On input of an unary string 1^k where k is a security parameter, outputs a personal public-private key pair (pk, sk). It is a probabilistic polynomial time (PPT) algorithm.*

(2) *Delegation Signing DS: On input of a delegation warrant m_w and an original signer B's private key sk_B, outputs a signature δ on m_w.*

(3) *Delegation Verification DV: On input of an original signer B's public key pk_B and his signature δ on m_w, outputs "accept" if (m_w,δ) is valid with respect to pk_b, and "reject" otherwise. Then, with valid (m_w,δ) and the proxy signer's private key sk_{p_j} to produce a secure proxy secret key psk_j.*

(4) *PRS Issuing PS: On input of a message m, the public keys $pk_B, pk_{p_1}, pk_{p1}, \cdots, pk_{p_n}$, of the original signer and proxy signers, the delegation warrant m_w and some proxy signer P_j's proxy secrete key psk_{p_j}, outputs a ring signature for a message m.*

(5) *PRS Verification PV: On input of a message m and a ring signature sig, a set of pubic keys $pk_B, pk_{p_1}, \cdots, pk_{p_n}$, of the original signer and proxy signers, and a delegation warrant m_w, outputs "accept" if (m_w, sig) is valid with*

respect to $pk_B, pk_{p_1}, \cdots pk_{p_n}, m_w$, *and "reject" otherwise.*

The above algorithms should satisfy the consistency constraint of PRS, that is

$$\forall m_w: DV(pk_B, m_w, \delta) = accept,$$
$$where\ \delta = DS(m_w, sk_B)$$
$$\forall m: PV(pk_B, pk_{p_1}, \cdots, pk_{p_n}, m, m_w, sig) = accept,$$
$$where\ sig = PS(pk_B, pk_{p_1}, \cdots, pk_{p_n}, psk_{p_j}, m, m_w)$$

In 2003, Boldyreva et al[2] first formally defined the security model for proxy signature, where the delegation is only one level. In 2004, Malkin et al[12] also provided the security model for fully hierarchical proxy signatures with warrants, which can support chains of several levels of delegation. However, since the proxy ring signature is not an ordinary proxy signature, the security of which cannot be directly proved under these models. As shown in Section 1, the unforgeability and anonymity properties are two main security requirements for PRS scheme. When we say a PRS scheme is secure if it by and large satisfies these two requirements: (i) the delegation signing protocol and PRS signature issuing protocol in a PRS scheme are unforgeable; (ii) Anyone (include the original signer) cannot tell the identity of the real proxy signer, even he has unlimited computing resources.

Definition 2 (*Unforgeability* − 1): *Let A be an adversary and B be an original signer that involved in the following game.*

(1) $(pk_B, sk_B) \leftarrow KG(1^k)$; *where* (pk_B, sk_B) *is the public-private key pair of B.*

(2) *A is given the public key* pk_B *of B and allowed to make signing oracle query to B adaptively.*

(3) *Finally, outputs a signature* $\delta_B(m)$. *A wins the game if* $\delta_B(m)$ *is accepted. We define the success probability of A as*

$$Succ_{PRS}^{UF-1}(A) = Pr\begin{bmatrix}(pk_B, sk_B) \leftarrow KG(1^k);\\ \delta_B(m) \leftarrow A^{O_S}(pk_B)\\ :\delta \quad is\ accepted\end{bmatrix}$$

We say the delegation signing protocol in PRS scheme is unforgeable if the probability $succ_{PRS}^{UF-1}(A)$ *is negligible in the game.*

Definition 3 (*Unforgeability* − 2): *Let A be an adversary, B be an original signer and* $P = \{P_1, P_2, \cdots, P_n\}$ *be n proxy signers that involved in the following game.*

1. $(pk_B, sk_B, pk_{p1}, sk_{p1}, \cdots, pk_{p_n}, sk_{p_n}) \leftarrow KG(1^k)$, $pk_B \neq pk_{p_i}$ *for* $1 \leqslant i \leqslant n$

2. $\left(m_w, \delta_B(m_w)\right) \leftarrow B(1^k, pk_B, sk_B)$

3. *A is given the* $pk_B, sk_B, pk_{p_1}, \cdots, pk_{p_n}, m_w$, $\delta_B(m_w)$, *and allowed to make PRS signing oracle query to P adaptively.*

4. *Finally, A outputs a PRS sig* (m). *A wins the game if isg* (m) *is accepted. We define the success probability of A as*

$$succ_{PRS}^{UF-2}(A) =$$
$$\Pr\begin{bmatrix}(pk_B, sk_B, pk_{p_1}, sk_{p_1}, \cdots, pk_{p_n}, sk_{p_n}) \leftarrow P(1^k);\\ sig(m) \leftarrow A^{O_{PS}}\left(pk_B, sk_B, pk_{p1}, \cdots, pk_{pn}, m_w, \delta_B(m_w)\right)\\ :sig(m)\ is\ accepted\end{bmatrix}$$

We say the PRS signature issuing protocol in PRS scheme is unforgeable if the probability $Succ_P^{UF-2}RS(A)$ *is negligible in the game.*

Definition 4 (*Anonymity*): *Let A be an adversary, B be an original signer and* $PG = \{P_1, P_2, \cdots, P_n\}$ *be n proxy signers that involved in the following game.*

1. $(pk_B, sk_B, pk_{p_1}, sk_{p_1}, \cdots, pk_{p_n}, sk_{p_n}) \leftarrow KG(1^k)$

2. $\left(m_w, \delta_B(m_w)\right) \leftarrow B(1^k, pk_B, sk_B)$, *A is given the* $pk_B, pk_{p_1}, \cdots, pk_{p_n}, m_w, \delta_B(m_w)$

3. *Select* $P_j \leftarrow P$, P_j, *then outputs a valid PRS sig* (m) *on message m and sends it to A*

4. *A outputs* $P_j \in P$, *A wins the game if* $P_j = P_j$ *We define the success probability of A as*

$$Succ_{PRS}^{AN}(A) = \Pr[A\left(sig(m)\right) = P_{j'} = P_j] = \frac{1}{|PG|} + \varepsilon$$

We say a PRS scheme is unconditionally anonymous if ε *is zero in the game.*

4 Basic Concepts on Bilinear Pairings

Bilinear pairing is an important cryptographic primitive and has recently been applied in many positive applications in cryptography. Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of the same prime order q. We assume that the discrete logarithm problems in both G_1 and G_2 are hard. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ which satisfies the following properties: (i) Bilinear: For any $P,Q \in G_1$ and $a,b \in Z_q^*$, we have $e(aP,bQ)=e(P,Q)^{ab}$; (ii) Non-degenerate: There exists $P \in G_1$ and $Q \in G_1$ such that $e(P,Q) \neq 1$; (iii) Computable: There is an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$. From the literature[1], we note that such a bilinear pairing may be realized using the modified Weil pairing associated with supersingular elliptic curve.

Next, we consider the following related mathematic problems in G_1, namely the Discrete Logarithm Problem (DLP), Decisional Diffie-Hellman Problem (DDHP), Computational Diffie-Hellman Problem (CDHP) and Collusion Attack Algorithm with k traitors (k-CAA)[13, 24].

Definition 5 (DLP): For $a \in Z_q^*$, given $P, aP \in G_1$, compute such an a. An algorithm A is said to solve the DLP with an advantage of ε if

$$Adv_{G_1}^{DLP}(A)=\Pr[A(P,aP)=a] \geqslant \varepsilon$$

Definition 6 (DDHP): For $a,b,c \in Z_q^*$, given $P,aP,bP,cP \in G_1$, decide whether $c=ab \in Z_q$.

A DDHP is easy in G_1[1], since it is easy to compute $e(aP,bP)=e(P,P)^{ab}$ and decide whether $e(P,P)^{ab}=e(P,P)^{c}$.

Definition 7 (CDHP): For $a,b \in Z_q^*$, given $P,aP,bP \in G_1$, compute $abP \in G_1$. An algorithm A is said to solve the CDHP with an advantage of ε if

$$Adv_{G_1}^{CDH}(A)=\Pr[A(P,aP,bP)=abP] \geqslant \varepsilon$$

Definition 8 (k-CAA): For an integer $k \in N$, and $a \in Z_q^*$, $P \in G_1$, given

$$\left\{P, Q=aP, h_1, \cdots, h_k \in Z_q^*, \frac{1}{h_1+a}P, \cdots, \frac{1}{h_k+a}P\right\}$$

compute $\frac{1}{h+a}$ for some $h \notin \{h_1, \cdots, h_k\}$. An algorithm A is said to solve the k-CAA with an advantage of ε if

$$Adv_{G_1}^{k-CAA}(A)=\Pr\left[\begin{array}{l} A(P,Q=aP,\frac{1}{h_1+a}P,\cdots,\frac{1}{h_1+a}P,\cdots, \\ \frac{1}{h_K+a}P)=\frac{1}{h+a}P \mid a \in Z_q^*, P \in G_1, \\ h_1,\cdots,h_k \in Z_q^*, h \notin \{h_1,\cdots,h_k\} \end{array}\right] \geqslant \varepsilon$$

We have the relationship of the CDHP and k-CAA in[30] that the k-CAA in G_1 is no harder than the CDHP. Therefore, we assume throughout this paper that k-CAA is intractable, which means there is no polynomial time algorithm to solve k-CAA, CDHP and DLP in G_1 with nonnegligible probability.

5 Our Proposed Scheme

In this section, based on the formal definition in Section 3, we will introduce our PRS scheme from bilinear pairings.

Key Generation: Let G_1 be a cyclic additive group of prime order q, and P be a generator of G_1. Let G_2 be a cyclic multiplicative group of the same prime order. Then, the bilinear pairing is given as $e: G_1 \times G_1 \to G_2$. H, H_1 denote two secure cryptographic hash functions where $H: \{0,1\}^* \to Z_q^*$ and $H_1: \{0,1\}^* \to Z_q^*$. Then, the public system parameters are $\{G_1, G_2, q, e, P, H, H_1\}$.

The original signer B selects $x_B \leftarrow Z_q^*$ as his private key, and sets the public key $Y_B = x_B P$. Similarly, each proxy signer $P_i \in PG$ selects a random number $x_{P_i} \leftarrow Z_q^*$ as his/her private key, and sets the corresponding public key $Y_{P_i} = x_{P_i} P$.

Delegation Signing: First, the original signer B makes a delegation warrant m_w, which records the necessary proxy information, such as the identities of the original signer B and the set of

proxy signers $PG=\{P_1,P_2,\cdots,P_n\}$, the expiration time of the delegation of signing power and so on.

$m_w=[B\|P=\{P_1,P_2,\cdots,P_n\}\|\text{Authority}\|\text{ValidPeriod}]$

Then, B chooses a random number $r\leftarrow Z_q^*$ and uses his private key x_B to compute $\left[R=rP, S=r+H(m_w,R)x_B \bmod q\right]$. At last, B sends (R,s,m_w) to proxy signers $PG=\{P_1,P_2,\cdots,P_n\}$.

Delegation Verification: Upon receiving (R,s,m_w), each proxy signer $P_i\in PG$ first checks them by the equality $sP=R+H(m_w,R)Y_B$. If it does hold, (R,s,m_w) will be accepted, otherwise rejected, since

$$\begin{aligned}&R+H(m_w,R)Y_B\\&=rP+H(m_w,R)x_BP\\&=\left(r+H(m_w,R)x_B\right)P=sP\end{aligned}$$

If (R,s,m_w) is valid, P_i then, with his private key x_{P_i}, computes the proxy secret key psk_i, where

$psk_i=s+x_{P_i}H(m_w,R)=r+H(m_w,R)(x_B+x_{P_i})\bmod q$

Obviously, the proxy secret key psk_i is only known by the proxy signer P_i.

PRS Issuing: A proxy signer $P_j\in PG$ wants to sign a message on behalf of the original signer in an anonymous way, the following steps will be executed:

1. P_j first chooses $n-1$ random numbers $a_1,\cdots,a_{j-1},a_{j+1},\cdots,a_n\leftarrow Z_q^*$

2. Then, P_j computes $\delta_1,\cdots,\delta_n$, where

$$\delta_j=\frac{1}{H_1(m)+psk_j}\left\{P-\sum_{i\neq j}a_i\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i})\right]\right\}$$

$$\delta_i=a_iP,\ 1\leqslant i\leqslant n,\ i\neq j$$

3. Finally, P_j sends $sig=(\delta_1,\delta_2,\cdots,\delta_n,m,m,R)$ as a PRS to a verifier.

PRS Verification: The verifier can check the validity of a PRS by the following equality

$$\prod_{i=1}^{n}e\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i}),\delta_i\right]=e(P,P)$$

If it does hold, $sig=(\delta_1,\delta_2,\cdots,\delta_n,m,m_w,R)$ is accepted as valid, otherwise rejected, since

$$\begin{aligned}&\prod_{i=1}^{n}e\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i}),\delta_i\right]\\&=\prod_{i=1,i\neq j}^{n}e\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i}),\delta_i\right]\\&\quad\times e\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_j}),\delta_j\right]\\&=\prod_{i=1,i,\neq j}^{n}e\left\{a_i\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i})\right],P\right\}\\&\quad\times e\left\{\left[H_1(m)+psk_j\right]P,\delta_j\right\}\\&=\prod_{i=1,i,\neq j}^{n}e\left\{a_i\left[H_1(m)P+R+H(m_w,R)(Y_B+Y_{P_i})\right],P\right\}\\&\quad\times e\left\{P,P-\sum\nolimits_{i\neq j}a_i\left[H_1(m)P+R\right.\right.\\&\quad\left.\left.+H(m_w,R)(Y_B+Y_{P_i})\right]\right\}\\&=e(P,P)\end{aligned}$$

6 Security Analysis

In this section, we will analyze the security of our proposed PRS scheme. First, we focus on the unforgeablity and anonymity by using the following three theorems. Then, we also discuss other security properties stated in Section 1.

Theorem 1 *Let A be an adversary who can, with a time bound τ, perform an existential forgery under an adaptively chosen message attack against the delegation signing protocol with probability ε in random oracle model*[4]. *A is allowed to query the random oracle H and signing oracle at most q_h and q_s times, respectively. Then assume that $\varepsilon\geqslant 10(q_s+1)(q_s+q_h)/q$, the DLP can be solved within expected time $\tau'\leqslant 12068q_h\tau/\varepsilon$, where $|q|$ is equal to the security parameter k*[15].

Due to the space limitation, the proof is omitted. Please refer to the full version of the paper[8] for details.

Theorem 2 *Suppose that the q_s-CAA in G_1 is (τ',ε')-secure. Then, the proxy ring signature issuing protocol in the proposed scheme is $(\tau,q_s,q_h,\varepsilon)$-secure in the random oracle*

model, where

$$\varepsilon \leqslant \left(\frac{q_s}{q_h}\right)^{-q_s} \cdot (q_h - q_s) \cdot \varepsilon'$$

$$\tau \geqslant \tau' - (q_s n + 3n - 2) \cdot T_{pmul} - (3n-1)T_{padd} - nT_{inv} - (2n-2)T_{mul}$$

and q_h, q_s denote the number of queries to the random oracle H_1 and to the signing oracle, and q_h, q_s denotes the time of one point scalar multiplication in G_1, T_{padd} the time of one addition in G_1, T_{inv} the time of one inversion in Z_q^* and T_{mul} the time of one multiplications in Z_q^*.

Proof: Adopting the security model of Rivest, Shamir and Tauman[16], using the similar idea in[24], we consider the challenge game defined in Definition 3. Suppose A is an adversary who can $(\tau, q_h, q_s, \varepsilon)$-break the ring signature issuing protocol in the proposed scheme. Without loss of generality, we assume that q_h queries to H_1 are all distinct. Then, we will use A to construct another algorithm S, who can break the q_s-CAA with another non-negligible ε' and within a running time τ',

$$\varepsilon' \geqslant \left(\frac{q_s}{q_h}\right)^{q_s} \cdot \frac{1}{q_h - q_s} \cdot \varepsilon$$

$$\tau' \leqslant \tau + (q_s n + 3n - 2) \cdot T_{pmul} + (3n-1)T_{padd} + nT_{inv} + (2n-2)T_{mul}$$

At first, the algorithm S is given a challenge as follows: Given $P \in G_1, Q = aP, h_1, \cdots, h_{q_s} \in Z_q^*$, and $\frac{1}{h_1 + a}P, \cdots, \frac{1}{h_{q_s} + a}P$, compute $\frac{1}{h+a}P$ for some $h \notin \{h_1, \cdots, \cdots, h_{q_s}\}$.

simulates the challenger of A and interacts with A as follows:

Setup: S first makes a delegation warrant m_w that includes the original signer B and n proxy signers $P_1, P_2, \cdots, P_n$①. Then, S chooses a random number $x_B \leftarrow Z_q^*$, computes $Y_B = x_B P$ and determines R and Y_{P_1} in G_1 such that $R + v(Y_B + Y_{P_1}) = ap$. In the end, S computes $H(m_w, R) = v$.

S picks up $n-2$ random numbers, $b_2, \cdots, b_{n-1} \leftarrow Z_q^*$, and computes $b_n \in Z_q^*$ such that

$$\frac{1}{b_n} = n - 1 - \frac{1}{b_2} + \cdots + \frac{1}{B_{n-1}} \bmod q$$

then sets

$$Y_{P_2} = Y_{P_1} + V^{-1}\left[(b_2 - 1)aP + h(b_2 - 1)P\right]$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$Y_{P_n} = Y_{P_1} + V^{-1}\left[(b_n - 1)aP + h(b_n - 1)P\right]$$

From the delegation signing protocol, the implied verification key ppk_i for p_i, $1 \leqslant i \leqslant n$, are

$$ppk_1 = R + H(m_w, R)(Y_B + Y_{P_1}) = aP = Q$$

$$ppk_2 = R + H(m_w, R)(Y_B + Y_{P_2}) = b_2 Q + h(b_2 - 1)P$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$ppk_n = R + H(m_w, R)(Y_B + Y_{P_n}) = b_n Q + h(b_n - 1)P$$

S then keeps $\{b_2, \cdots, b_n\}$ secretly and gives other parameters (including the original signer's private key x_B) to A. To achieve the perfect simulation, the hash function $H_1 : \{0,1\}^* \rightarrow Z_q^*$ behaves as a random oracle controlled by S here.

H_1-Queries: At any time, A provides a message M_i for H_1 oracle query. To respond to such q_h times H_1-queries, S should maintain a H_1-list, which is initially empty and records all responses to, previous H_1-queries. S selects a random number w_i in Z_q^* or from $\{h, h_1, \cdots, h_{q_s}\}$, then adds (m_i, w_i) to H_1-list, and responds to A with $H_1(m_i) = w_i$.

Signing-Queries: When A makes a signature oracle query on a message m_i, S looks up the H_1-list. If $H_1(m_i) = w_i = h_j, 1 \leqslant j \leqslant q_s$, S responds $sig_i = \{\delta_{i1}, \delta_{i2}, \cdots, \delta_{in}\}$ to A, where

$$\delta_{i1} = (2-n)\frac{1}{h_j + a}P$$

$$\delta_{i2} = \frac{1}{b_2}\frac{1}{h_j + a}P$$

$$\vdots \qquad \vdots$$

$$\delta_{in} = \frac{1}{b_n}\frac{1}{h_j + a}P$$

From the construction of, $\delta_{i1}, \delta_{i2}, \cdots, \delta_{in}$, we can verify that sig_i can pass the ring verification:

$$\prod_{l=1}^{n} e\left[H_1(m_i)P + R + H(m_w, R)(Y_B + Y_{P_l}), \delta_{il}\right]$$

① Here, the number of proxy signers n is not limited as an odd number as that in Zhang et al.'s scheme[30].

$$= \prod_{l=1}^{n} e(h_j P + ppk_l, \delta_{il})$$

$$= e\left(h_j P + Q, (2-n)\frac{1}{h_j + a}P\right)$$

$$\prod_{l=2}^{n} e\left(h_j P + b_l Q + h(b_l - 1)P, \frac{1}{b_l}\frac{1}{h_j + a}P\right)$$

$$= e\left((2-n)(h_j P + Q), \frac{1}{h_j + a}P\right)$$

$$\prod_{l=2}^{n} e\left(\frac{h_j}{b_l}P + Q + hP - \frac{h}{b_l}P, \frac{1}{h_j + a}P\right)$$

$$= e\left((2-n)(h_j P + Q), \frac{1}{h_j + a}P\right)$$

$$e\left((n-1)(h_j P + Q), \frac{1}{h_j + a}P\right)$$

$$= e\left(h_j P + Q, \frac{1}{h_j + a}P\right)$$

$$= e(P, P)$$

solving q_s-CAA: Finally, the adversary A terminates the game and outputs a valid forgery $\{m, sig = (\delta_1, \cdots, \delta_n)\}$. S looks up the hash value of in H_1-list. If the hash value $H_1(m) \neq h$, S stops and reports failure. Otherwise,

$$\prod_{i=1}^{n} e\left(H_1(m)P + ppk_i, \delta_i\right)$$

$$= e\left(H_1(m)P + Q, \delta_1\right)$$

$$\prod_{i=2}^{n}\left(H_1(m)P + b_i Q + h(b_i - 1)P, \delta_i\right)$$

$$= e(hP + Q, \delta_1)\prod_{i=2}^{n} e\left(b_i(hP + Q), \delta_i\right)$$

$$= e(hP + Q, \delta_1 + \sum_{i=2}^{n} b_i \delta_i) = e(P, P)$$

S then outputs the challenge $\frac{1}{h + a}P$ as $\delta_1 + \sum_{i=2}^{n} b_i \delta_i$.

S will not fail in signing oracle queries with probability at least $\left(\frac{q_s}{q_h}\right)^{q_s}$, and the probability of $H_1(m) = h$ in $A's$ output is $\frac{1}{q_h - q_s}$. Therefore, S resolves the q_s-CAA with probability

$$\epsilon' \geq \left(\frac{q_s}{q_h}\right)^{q_s} \cdot \frac{1}{q_h - q_s} \cdot \epsilon$$

In the simulation, the main running time of algorithm S is that of the adversary A, plus nT_{inv} $+(2n-2)T_{mul} + (2n-1)T_{pmul} + 2nT_{padd}$ in Setup, q_s nT_{pmul} in Signing-Queries, and $(n-1)(T_{pmul} + T_{padd})$ in Solving q_s-CAA, i. e. ,

$$\tau' \leqslant \tau + (q_s n + 3n - 2) \cdot T_{pmul} + (3n-1)$$
$$T_{padd} + nT_{inv} + (2n-2)T_{mul}$$

Thus, the proof is completed.

Theorem 3 *For any algorithm A, any set of proxy signers $PG = \{P_1, P_2, \cdots, P_n\}$ delegated by an original signer B, and a random $P_j \in P$, the success probability of A to guess P_j is at most $\frac{1}{|PG|}$, that is, $Pr[A(sin) = P_j] \leqslant \frac{1}{|PG|}$ where $sin = (\delta_1, \delta_2, \cdots, \delta_n, m, m_w, R)$ is a ring signature on P generated by P_j with proxy secret key psk_j.*

Due to the space limitation, the proof is also omitted. Please refer to the full version of the paper [1] for details.

Now we will show that our proposed PRS scheme satisfies other properties stated in Section 1.

- Distinguishability: Since there is a delegation warrant m_w in a valid proxy ring signature, m_w and this warrant and the public keys of the original signer and some proxy signers must occur in the verification equation of a proxy ring signature, the distinguishability is obvious.
- Verifiability: The valid proxy ring signature for message m will be the tuple $sig = (\delta_1, \delta_2, \cdots, \delta_n, m, m_w, R)$, and from the verification phase, the verifier can be convinced that the real proxy signer has the original signer's signature on the warrant m_w. So the verifiability follows.
- Prevention of misuse: Since the delegation warrant m_w contains the capability scope of the delegation, any proxy signer cannot sign some messages that have not been authorized by the original signer.

7 Conclusions

In this paper, in order to provide the proxy signer privacy protection, we have proposed a

new parallel proxy ring signature scheme from bilinear pairings. Our scheme allows an original signer delegates his signing capability to a group of proxy signers and then any proxy signer can perform the signing operation of the original signer while preserving his anonymity. In addition, our scheme is provably secure in the random oracle model and more efficient than Zhang et al.'s sequential proxy ring signature scheme[23]. Therefore, our proposed scheme is suitable for some practical applications where personal activities within organization should be protected from outside.

Acknowledgment

The authors would like to thank anonymous reviewers for their valuable comments. This work is supported in part by the National Natural Science Foundation of China for Distinguished Young Scholars under Grant No. 60225007 and 60572155, the Science and Technology Research Project of Shanghai under Grant Nos. 04JC14055 and 04DZ07067, and the Special Research Funds of Huawei.

References

1 D Boneh, M Franklin. Identity-based encryption from the Weil pairing. In: Advances in Cryptology—Crypto'01, LNCS 2139, pp. 213 — 229, Springer — Verlag, 2001

2 A Boldyreva, A Palacio, B Warinschi. Secure proxy signature scheme for delegation of signing rights. Cryptology ePrint Archive, Report 2003/096

3 M Bellare, P Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In: Proc. of the 1st CCS, ACM Press, New York, pp. 62 — 73, 1993

4 E Bresson, J Stern, M Szydlo. Threshold ring signatures and applications to ad-hoc groups. In: Advances in Cryptology—Crytpto'02, LNCS 2442, pp. 465—480, Springer—Verlag, 2002

5 S Goldwasser, S Micali, R Rivest. A digital signature scheme secure against adaptively chosen message attacks, SIAM Journal on Computing, 17 (2): 281—308, 1988

6 S Hwang, C Shi. A simple multi-proxy signature scheme, In: Proceedings of the Tenth National Conference on Information Security, pp. 134—138, 2000

7 J Herranz, G Saez. Forking lemmas for ring signature schemes. In: Advances in Cryptology—Indocrypt'03, LNCS 2904, pp. 266—279, Springer—Verlag, 2003

8 R Lu, Z Cao, X Dong. Pairing-Based Proxy Ring Signature Scheme with Proxy Signer Privacy Protection, The full version, available on http://tdt.sjtu.edu.cn/~rxlu

9 R Lu, Z Cao, Y Zhou. Proxy blind multi-signature scheme without a secure channel. Applied Mathematics and Computation, 164, pp. 179—187, 2005

10 B Lee, H Kim, K Kim. Strong proxy signer and its applications. In: Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01), Vol 2(2), pp. 603—608, 2001

11 N. Lee, M Lee. The security of a strong proxy signature scheme with proxy signer privacy protection. Applied mathematics and computation, 161 (2005) 807—812

12 T Malkin, S Obana, M Yung. The hierarchy of key evolving signatures and a characterization of proxy signatures. In: Advance in Cryptography—Eurocrypt'04, LNCS 3027, pp. 306—322, Springer—Verlag, 2004

13 S Mitsunari, R Sakai, M Kasahara. A new traitor tracing. IEICE Trans. Vol. E85 — A, No. 2, pp. 481—484, 2002

14 M Mambo, K Usuda, E Okamoto. Proxy signatures: delegation of the power to sign messages. IEICE Transaction Foundational, E79—A(9), pp. 1338—1353, 1996

15 D Pointcheval, J Stern. Security arguments for digit signatures and blind signatures. Journal of Cryptology, 13(3): 361—396, 2000

16 R Rivest, A Shamir, Y Tauman. How to leak a secret. In: Advances in Cryptology — Asiacrypt 2001, LNCS 2248, pp. 552—565, Springer—Verlag, 2001

17 H Sun, B Hsieh. Cryptanalysis of a strong proxy signature scheme with proxy signer privacy protection. IEEE Int. Carnahan Conf. on Security Technology, 2003

18 K Shum, V K Wei. A strong proxy signature scheme with proxy signer privacy protection. In: Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises 2002 (WETICE' 02), 2002, Pittsburgh, PA, pp. 55—56.

19 Z Tan, Z Liu, C Tang. Digital proxy blind signature schemes based on DLP and ECDLP, MM Research Preprints, No. 21, December 2002, MMRC, AMSS, Academia, Sinica, Beijing, pp. 212—217

20 L Yi, G Bai, G Xiao. Proxy multi-signature scheme: A new type of proxy signature scheme. Electronics Letter, 36(6), pp. 527—528, 2000

21 K. Zhang. Threshold proxy signature schemes. In: Proceedings of 1997 Information Security Workshop, 1997, pp. 191—197.

22 F Zhang , K Kim. ID-based blind signature and ring signature from pairings. In: Proceedings of Cryptology — Asiacrypt 2002, LNCS 2501, pp. 533 — 547, Springer—Verlag, 2002

23 F Zhang, R Safavi-Naini, C Lin. New proxy signature, proxy blind signature and proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive, Report 2003/104

24 F Zhang, R Safavi-Naini, W Susilo. An efficient signature scheme from bilinear pairings and its applications. PKC 2004, Singapore. LNCS 2947, pp. 277—290, Springer—Verlag, 2004