Journal of System Simulation

Volume 27 | Issue 6 Article 27

1-15-2021

New Identify Based Proxy Signature Scheme

Xiaojing Hong
1. Department of Information Engineering, Jianghai Polytechnic College, Yangzhou 225101, China; ;

Bin Wang
2. Information Engineering College, Yangzhou University, Yangzhou 225127, China;

New Identify Based Proxy Signature Scheme

Abstract

Abstract: Proxy signature schemes allow a proxy signer to generate proxy signatures on behalf of an original signer. Mambo, et ah first introduced the notion of proxy signature and a lot of research work can be found on this topic nowadays. To simplify key management, many identity based proxy signature schemes were proposed. However, some existing schemes are vulnerable to proxy key exposure attack. *It is necessary to propose a security model for identity based proxy signature schemes against proxy key exposure attack. Then an efficient scheme based on pairings was presented, which is provably secure in the random oracle model. In particular, the new scheme is secure against proxy key exposure attack*

Keywords

digital signature, proxy signature, identity based signature, bilinear pairing, random oracle model

Recommended Citation

Hong Xiaojing, Wang Bin. New Identify Based Proxy Signature Scheme[J]. Journal of System Simulation, 2015, 27(6): 1338-1347.

第 27 卷第 6 期 系统仿真学报© Vol. 27 No. 6
2015 年 6 月 Journal of System Simulation Jun., 2015

一个新的基于身份的代理签名方案

洪晓静[1]，王斌[2]
(1.江海职业技术学院信息工程系，扬州 225101；2.扬州大学信息工程学院，扬州 225127)

摘要： 代理签名方案允许代理签名者代表原始签名人生成代理签名。Mambo 等人首次引入了代理签名的概念，目前在这个领域上有大量的研究工作。为了简化密钥管理，研究人员提出了许多基于身份的代理签名方案。但许多现有的方案容易受到基于代理密钥泄露的攻击。*有必要针对代理密钥泄露，提出一个基于身份的代理签名方案的安全模型。基于双线性映射提出了一个有效的方案，并在随机预言模型中证明是安全的。新方案在代理密钥泄露时仍然是安全的。*

关键词： 数字签名；代理签名；基于身份的签名；双线性映射；随机预言模型

中图分类号：TP309 文献标识码：A 文章编号：1004-731X (2015) 06-1338-10
DOI:10.16182/j.cnki.joss.2015.06.027

New Identity Based Proxy Signature Scheme

Hong Xiaojing[1], *Wang Bin*[2]

(1. Department of Information Engineering, Jianghai Polytechnic College, Yangzhou 225101, China;
2. Information Engineering College, Yangzhou University, Yangzhou 225127, China)

Abstract: Proxy signature schemes allow a proxy signer to generate proxy signatures on behalf of an original signer. Mambo, *et al.* first introduced the notion of proxy signature and a lot of research work can be found on this topic nowadays. To simplify key management, many identity based proxy signature schemes were proposed. However, some existing schemes are vulnerable to proxy key exposure attack. *It is necessary to propose a security model for identity based proxy signature schemes against proxy key exposure attack. Then an efficient scheme based on pairings was presented, which is provably secure in the random oracle model. In particular, the new scheme is secure against proxy key exposure attack.*

Keywords: digital signature; proxy signature; identity based signature; bilinear pairing; random oracle model

引言*

数字签名是电子商务环境下一种重要的安全服务。作为普通数字签名的一个变体，代理签名的概念在 1996 年被 Mambo, Usuda 和 Okamoto[1]首次提出来。在代理签名方案中，原始签名人可以将他的签名权力授权给指定的代理签名人，然后代理签名人可以代表原始签名人生成代理签名。代理签名已经有大量的实际应用，例如分布式系统、网格计算和移动通信等领域。

Goldwasser, Micali 和 Rivest 提出了数字签名方案的安全定义[2]。然而直到 2003 年才由 Boldyreva，Palacio 和 Warinschi[3]首先给出代理签名方案的形式化安全定义，并把代理签名方案的安全性归约到一些著名的难解问题。然而，Jacob C.N. Schdult 等人[4]指出，他们的方案[3]在代理密钥泄露的条件下容易受到攻击的。当代理签名密钥泄露的时候，敌手可以恢复对应的代理签名人的私钥。

在传统的公钥基础设施(PKI)中，通过可信 CA 颁发的证书来绑定用户公钥和用户身份。但部署和

收稿日期：2014-06-09 修回日期：2014-06-30；
基金项目：2014 年江苏省'青蓝工程'项目(62021157)；
作者简介：洪晓静(1977-)，女，江苏姜堰，硕士，副教授，研究方向为网络安全和通信技术；王斌(1976-)，男，江西萍乡，博士，副教授，研究方向为公钥密码学。

维护 PKI 的开销是昂贵的。在[5]中，Shamir 提出了基于身份的密码学的概念，用户的身份将被视为公钥。基于身份的密码方案的优势是不需要验证证书，简化对公钥证书的管理。其后，许多基于身份的密码方案被提出[6-7]。

2003 年，Zhang 等[8]通过双线性映射提出了一种基于身份的代理签名方案，然而没有正式分析他们方案的安全性。2005 年，Xu 等[9]也通过双线性映射提出了一种基于身份的代理签名方案，但在他们的论文中定义的安全模型没有考虑敌手 A 可以自适应地选择所攻击的身份。换句话说，敌手 A 在安全实验开始前就必须确定被攻击的目标身份 ID_1。后来，Shim[10]针对一个可以自适应地选择消息和身份的敌手，提出了一个基于身份的代理签名方案。然而，上述基于身份的代理签名方案[8-10]对于代理密钥泄露攻击是不安全的。

Wu 等[11]也针对一个可以自适应选择消息和身份的敌手，提出了一个基于身份的代理签名方案。由于在[11]中定义的敌手可以分为 3 种类型，要分析他们方案的安全性并不容易。此外，在[11]中定义的模型没有把代理密钥泄露攻击考虑进去。

因此，本文将首先定义一个基于身份的代理签名方案的安全模型。然后通过双线性映射提出一个有效的、基于身份的代理签名方案。接下来，表明即使敌手可以自适应地选择消息和身份，所提出的方案仍是不可伪造的。而且新方案可以防范代理密钥泄露攻击。最后比较了本文所提方案与文献[9-11]中方案的效率。

1 背景知识

1.1 双线性配对

若 $<G_1,+>$ 是由 P 所生成的一个循环加法群，其阶是一个大素数 q，$<G_2,\bullet>$ 是一个有相同阶的循环乘法群，并且 $e(\cdot)$ 具有以下属性：

1.双线性：对于任何 Q，R，$T \in G_1$，

$e(Q+R,T)=e(Q,T)\bullet e(R,T)$ 且

$e(Q,R+T)=e(Q,R)\bullet e(Q,T)$；

2.非退化的：$e(P,P)\neq 1$；

3.可计算的：对于任何的 R，$T \in G_1$，存在一个有效的算法来计算 $e(R,T)$。

1.2 计算型 Diffie-Hellman 假设

计算型 Diffie-Hellman(CDH)问题：若 G_1 是一个由 P 所生成的循环加法群，其阶是一个素数 q。给定 $<P,a\cdot P,b\cdot P>$，$a,b\in Z_q$，计算 $(ab)\cdot P$。

一个算法 A 解决 CDH 问题的成功概率定义为：

$$Succ_{P,G_1}^{CDH}(A)=\Pr[A(P,a\cdot P,b\cdot P)=ab\cdot P:\forall a,b\in Z_q]$$

一个 (t,ε) 的CDH求解器 A 是一个概率多项式时间(PPT)算法，运行时间最多为 t，且成功概率 $Succ_{P,G_1}^{CDH}(A)\geq\varepsilon$。如果给定一族 $\{G_{1,k}\}_k$，对任意多项式时间的 (t,ε) 的 CDH 求解器 A，ε 关于安全参数 k 是可忽略的，称 $\{G_{1,k}\}_k$ 满足 CDH 假设。

1.3 代理签名的安全性质

代理签名中有 3 种类型的委托方式：完全委托、部分委托和按授权证书委托。在一个完全委托方案中，原始签名人把他的签名密钥作为代理签名密钥给予代理签名人。因此，对于一个给定的消息，难以区分对应的签名究竟是由原始签名人还是由代理签名人生成的。在一个部分委托方案中，原始签名人通过自己的签名密钥计算代理签名密钥。但要从代理签名密钥导出原始签名人的签名密钥，从计算上来讲是不可行的。然而部分委托方案中无法限制代理签名人可以签署的消息类型。在一个按授权证书委托的方案中，原始签名人会创建和签发一个授权证书，用来检验代理签名人发布的代理签名的合法性。

自从 Mambo 等介绍了代理签名的概念后，多种代理签名方案被提出[12-13]。此外，还有许多方案对代理签名方案进行扩展，如门限代理签名[14]，对多签名的代理签名[15]等。通俗地说，代理签名方案基本的安全属性可以描述如下[13]：可验证性：

合法的代理签名使验证人相信代理签名人得到原始签名人的授权。

不可伪造性：只有指定的代理签名人可以代表原始签名人生成有效的代理签名。

强可识别性：任何人都可以从代理签名中确定对应的代理签名人的身份。

不可抵赖性：代理签名人生成一个有效的代理签名后不能再否认。

防止滥用：代理签名密钥除了用于生成有效的代理签名外不能用于其它目的。

2 一些现有方案的弱点

描述对基于身份的代理签名方案[9-10]的代理密钥泄露攻击。即当代理密钥暴露时，一个敌手可以恢复对应代理签名人的私钥。

2.1 Xu 等人的方案

在 Xu 等人的方案[9]中，代理密钥定义如下：

$skp = H_4(ID_i, ID_j, m_\omega, U_\omega)d_j + V_\omega$， m_ω 是对代理的授权证书，(U_ω, V_ω) 是由原始签名人 ID_i 在 m_ω 上所生成的签名，并且 d_j 是代理签名人 ID_j 的密钥。因为通常是在潜在的敌对环境中使用代理签名(特别是自代理签名的情形)，不能假定在原始签名人和代理签名人之间有一个安全的通道。即授权证书 (U_ω, V_ω) 可能被敌手截获。此时一旦代理密钥 skp 泄露，敌手就可以恢复代理签名人 ID_j 的密钥 d_j： $d_j = H_4(ID_i, ID_j, m_\omega, U_\omega)^{-1}(skp - V_\omega)$

2.2 Shim 的方案

我们简要概述一下 Shim 的方案[10]。

设置：

(1) 生成两个循环群 G_1, G_2，2 个不同的生成元 $P, Q \in G_1$ 和一个双线性映射 $e: G_1 \times G_1 \to G_2$。

(2) 选择一个随机数 $s \in Z_q^*$ 并设置主密钥对 $< sP, s >$。令主公钥 $P_{pub} = sP$。

(3) 选择 3 个安全散列函数 H_1, H_2, H_3，定义如下：$H_1: \{0,1\}^* \to G_1$，$H_i: \{0,1\}^* \to Z_q$，$i = 2,3$。

生成用户密钥：给定一个身份 ID，计算 $Q_{ID} = H_1(ID)$ 并设置用户密钥为 sQ_{ID}。

然后原始签名人 A 为授权信息 ω 生成一个签名如下：选择 $r_A \in Z_q^*$，然后计算 $U_A = r_A P \in G_1$，$h_A = H_2(\omega, U_A) \in Z_q$，$V_A = h_A S_A + r_A Q \in G_1$。

在验证了消息签名对 (ω, U_A, V_A) 的正确性后，代理签名人 B 计算 $h_B = H_3(\omega, U_A)$ 并设置代理密钥为 $\sigma_P = V_A + h_B S_B$，这里 $S_B = sQ_{ID_B}$，是 B 的秘密密钥。通过计算 $S_B = (h_B)^{-1}(\sigma_P - V_A)$，可以恢复 S_B。

3 基于身份的代理签名

3.1 基于身份的代理签名方案的定义

一个基于身份的代理签名方案(IBPS)包括以下多项式时间算法：

(1) MasterKeyGen(生成主密钥)：在输入一个安全参数 $k \in$ N 时，密钥生成中心(KGC) 运行该算法生成主密钥对 (mpk, msk) 和系统参数 params。

(2) UserKeyGen（生成用户密钥）：在输入 msk 时，用户身份 $ID \in \{0,1\}^*$，生成用户密钥 $Sk_{ID} \leftarrow$ UserKeyGen (ID, msk)。该算法由 KGC 为每个用户运行，并且认为用户密钥可以安全地分配给对应的用户。

(3) Sign（生成签名）：在输入一个用户身份 ID、用户密钥 Sk_{ID} 和一个消息 m 时，生成一个签名 $\sigma \leftarrow \text{Sign}(ID, Sk_{ID}, m)$。

(4) Verf（验证签名）：在输入用户身份 ID，mpk，签名的消息 m 和签名 σ 时，如果签名被接受，Verf(mpk, ID, m, σ) 返回 1，否则为 0。

(5) ProxyKeyGen(生成代理密钥)：由一对交互式算法 (D, V) 执行指定代理协议，D 和 V 分别代表原始签名人 ID_i 和代理签名人 ID_j。D，V 的公共输入包括身份 ID_i，ID_j。D 的保密输入包括原始签名人的密钥 Sk_{ID_i}，授权信息 m_w 包含身份 ID_i，ID_j 以及代理的有效期限、可以被代理的消息类型等。V 的保密输入包括代理签名人的密钥。通过交

互，V 的输出是一个代理签名密钥 $psk_{[i\to j]}$，通过它 ID_j 可以代表 ID_i 产生有效的代理签名。

(6) Proxy_Sign（生成代理签名）：给定代理签名人的身份 ID_j，代理签名密钥 $psk_{[i\to j]}$，代理签名人的密钥 Sk_{ID_j}，授权信息 m_w 和消息 m 时，可以生成代理签名如下：

$$p\sigma \leftarrow \text{Proxy\_Sign}(ID_j, psk_{[i\to j]}, Sk_{ID_j}, m_w, m)$$

(7) Proxy_Verf（验证代理签名）：在输入 mpk，授权信息 m_w，消息 m 和对应的代理签名 $p\sigma$，如果代理签名被接受，Proxy_Verf$(mpk, m_w, m, p\sigma)$ 返回 1，否则为 0。

(8) IDP（识别代理）：在输入一个授权信息 m_w 和一个代理签名 $p\sigma$ 时，在验证代理签名的正确性后，代理识别算法返回指定代理签名人的身份。

<MasterKeyGen，UserKeyGen，Sign，Verf>可以被视为一个标准的基于身份的签名方案。

正确性：要求对所有 m_w，$m\in\{0,1\}^*$，$ID\in\{0,1\}^*$，$k\in$N，(mpk,msk)=MasterKeyGen (1^k)，Sk_{ID} = UserKeyGen (ID,msk)，如果

(1) $psk_{[i\to j]}$ 由 $[D(ID_i, ID_j, Sk_{ID_i}, m_w) \leftrightarrow V(ID_i, ID_j, Sk_{ID_j})]$ 产生，且

(2) $p\sigma$ 由 Proxy_Sign $(ID_j, psk_{[i\to j]}, Sk_{ID_j}, m_w, m)$ 产生，且

(3) 消息 m 并不违反授权信息 m_w

则 Proxy_Verf$(mpk, m_w, m, p\sigma)$ 返回 1，且 IDP$(m_w, p\sigma)=ID_j$。

3.2 安全模型

在本节中，我们定义基于身份的代理签名方案的安全模型如下：

设 IBPS 是一个基于身份的代理签名方案，且 $k\in$N 是一个安全参数。定义一个安全实验 $Exp^{A}_{IBPS}(k)$，其中，一个敌手 A 与挑战者 S_1 相互交互。我们用 $\varnothing$ 来表示空集。

阶段 1：S_1 运行 MasterKeyGen (1^k) 得到 (mpk,msk) 和系统参数 params。$Corr$ 被初始化为空集，用于跟踪密钥已经被攻击者获取的用户身份的集合。S_1 提供 mpk，params 给 A。

阶段 2：A 向 S_1 发出对以下功能的查询：

(1) CreateUser：输入为用户身份 ID，如果 ID 已经被创建，S_1 返回指示消息来表明这一点。否则，S_1 执行 $Sk_{ID} \leftarrow$ UserKeyGen (ID,msk)，并建立一个空数组 $Pkey_{ID}$，用于存储由 ID 作为原始签名人参与生成的代理密钥。此时称已经创建 ID。

(2) RevealSecretKey：输入为用户身份 ID，如果 ID 已经被创建，S_1 返回对应的用户密钥 sk_{ID}。然后设置 $Corr \leftarrow Corr\cup\{ID\}$。否则返回一个特殊符号 $\perp$。

(3) Sign_Msg：在输入身份 ID 和由 A 自适应选择的消息 m 时，S_1 首先查询 RevealSecretKey (ID) 以获取 Sk_{ID}，然后返回一个标准签名 $\sigma \leftarrow$ Sign (ID, Sk_{ID}, m)。如果 $Sk_{ID}=\perp$，则返回 $\perp$。

(4) DesignateProxy：A 自适应地选择身份 ID_i (代表原始签名人)，ID_j (代表代理签名人)和一条授权信息 m_w。A 请求 S_1 根据输入 ID_i，ID_j，m_w 运行指定代理协议。然后 A 可以查看协议交互过程的通信记录。在协议成功运行之后，保密的代理密钥 $psk_{[i\to j]}$ 被存储在 $Pkey_i[j][t]$ 中，t 表示列表 $Pkey_i[j]$ 的当前未使用的位置。在这个过程中 A 可以控制在 $Corr$ 列表中用户的计算过程和查看其历史状态。

(5) Proxy_Sign_Msg：A 自适应地选择身份 ID_i (代表原始签名人)，ID_j (代表代理签名人)，授权信息 m_w，消息 m，以及 $t\in$N，并请求 S_1 生成 1 个代理签名。如果已经定义了 Sk_{ID_j} 和对应的代理签名密钥 $Pkey_i[j][t]$，则 S_1 返回 $p\sigma \leftarrow$ Proxy_ Sign $(ID_j, Pkey_i[j][t], Sk_{ID_j}, m_w, m)$。否则返回符号 $\perp$。

(6) Reveal_Proxy_Key：A 自适应地选择身份 ID_i (代表原始签名人)，ID_j (代表代理签名人)，$t\in$N。如果代理签名密钥 $Pkey_i[j][t]$ 被定义，则 S_1 返回 $Pkey_i[j][t]$。否则返回一个符号 $\perp$。

阶段 3：如果有下列事件之一发生，则 A 获胜：

(1) A 输出的 (ID^*, m^*, σ^*) 满足 Verf$(mpk, ID^*, m^*, \sigma^*)=1$。要求 A 没有用 (ID^*, m^*) 查询签名功能，

同时 $ID^* \notin Corr$ (这种情况称为对一个标准签名的伪造)。

(2) A 把 (ID_i, ID_j, m_w^*) 作为输入提供给 Designate Proxy 功能后，输出 $(ID_i, ID_j, m_w^*, m^*, p\sigma^*)$，满足 $\text{Proxy\_Verf}(mpk, m_w^*, m^*, p\sigma^*)=1$，$\text{IDP}(m_w^*, p\sigma^*)=ID_j$。

要求 A 没有用 $(ID_i, ID_j, t, m_w^*, m^*)$ 作为输入查询 Proxy_Sign_Msg 功能，其中 $t \in \mathrm{N}$，同时满足 $ID^* \notin Corr$。但允许 A 用 ID_i 作为输入查询 RevealSecretKey 功能(即 ID_j 被 ID_i 指定为代理后，通过 ID_i 伪造由 ID_j 生成的代理签名)。这种类型的攻击考虑的是在原始签名人的密钥泄露条件下的安全性。

(3) A 没有用 (ID_i, ID_j, m_w^*) 访问 DesignateProxy 功能，且输出 $(ID_i, ID_j, m_w^*, m^*, p\sigma^*)$，满足 $\text{Proxy\_Verf}(mpk, m_w^*, m^*, p\sigma^*)=1$，且 $\text{IDP}(m_w^*, p\sigma^*)=ID_j$。

要求满足 $|\{ID_i, ID_j\} \cap Corr| \leqslant 1$。这种类型的攻击考虑了敌手试图越过指定代理协议而设法伪造一个代理签名（例如 ID_j 伪造代表 ID_i 的代理签名；但 ID_j 未被 ID_i 指定为代理）。

最后，该安全实验返回 1 来表示敌手成功。定义敌手在该安全实验成功的概率为

$$Succ_{IBPS}(A)=\Pr[Exp_{IBPS}^{A}(k)=1]。$$

如果任何 PPT 敌手 A 在上述安全实验的成功概率 $Succ_{IBPS}(A)$ 是可以忽略的，则称该基于身份的代理签名方案满足签名不可伪造性。

在文献[11]中定义的敌手可以分为 3 种类型：

类型 I：这种类型的敌手只有关于原始签名人和代理签名人身份的信息。

类型 II：这种类型的敌手既有原始签名人和代理签名人身份的信息，也有代理签名人的密钥。

类型 III：这种类型的敌手既有原始签名人和代理签名人身份的信息，也可以有原始签名人的密钥。

很明显，在我们的安全模型中定义的敌手可以模拟在[11]中定义的所有攻击类型。例如，类型 I 的敌手对应我们安全模型中定义的不发出任何对 RevealSecretKey 功能进行查询的敌手。此外，在文献[11]中定义的模型没有考虑代理密钥泄露攻击。而且一个统一的安全模型可能导致更简洁的安全证明。

4 本文的方案

在本节中，我们基于双线性映射提出一个基于身份的代理签名方案。该方案包括以下算法：

MasterKeyGen：设 k 是系统的安全参数。令 $<G_1, +>$ 为一个由 P 生成的循环加法群，其阶是一个大素数 q，$<G_2, \cdot>$ 是一个具有相同阶的循环乘法群，令 $e: G_1 \times G_1 \to G_2$ 为对应的双线性映射。然后 KGC 执行以下操作：

(1) 选择一个随机数 $s \in Z_q^*$ 并设置主密钥对 $<mpk, msk>=<s \cdot P, s>$。

(2) 选择 3 个安全的单向函数 H_1, H_2, H_3，定义如下：$H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \times G_1 \to G_1$，$H_3: \{0,1\}^* \times G_1 \to G_1$。

(3) 设置系统参数 params 为 $<(G_1, +), (G_2, \cdot), e, q, P, mpk, H_1, H_2, H_3>$。

UserKeyGen：给定输入为身份 ID_i，KGC 计算 $Q_i = H_1(ID_i)$，$Sk_i = msk \cdot Q_i$。然后 KGC 通过安全的信道分发密钥 Sk_i 给由身份 ID_i 所对应的用户。用户可以通过检验 $e(Sk_i, P) = e(Q_i, mpk)$ 是否成立来验证密钥的正确性。

Sign：为了对消息 m 进行签名，由身份 ID_i 所对应的用户应执行以下步骤：

(1) 选择一个随机数 $k_i \in Z_q^*$ 并计算 $K_i = k_i \cdot P$。

(2) 计算 $V_i = H_2(ID_i, m, K_i)$，$U_i = k_i \cdot V_i + Sk_i$。

(3) 签名是 $\sigma = <U_i, K_i>$。

Verf：给定主公钥 mpk，身份 ID_i，已签署的消息 m，可以如下验证标准签名 σ 的正确性：

(1) 计算 $V_i = H_2(ID_i, m, K_i)$。

(2) 返回 1，当且仅当 $e(U_i, P) = e(V_i, K_i) \cdot e(Q_i, mpk)$，这里 $Q_i = H_1(ID_i)$。

很容易检验上述验证方程的正确性。

ProxyKeyGen：为了授予代理签名人 ID_j 代表自己签名的权力，原始签名人 ID_i 应该首先生成一个授权证书 m_w，其中包括原始签名人和代理签名人的身份，代理的有效期，委托签名的消息类型等信息。然后指定代理的协议可描述如下：

(1) 原始签名人 ID_i 输出 $\sigma'=\text{Sign}(ID_i,Sk_i,m_w)$，这里 $\sigma'=<U_i',K_i'>$。然后，$<\sigma',m_w>$ 发送给代理签名人 ID_j。

(2) 如果 $\text{Verf}(mpk,ID_i,m_w,\sigma')=1$，$ID_j$ 执行下一步。否则 ID_j 请求 ID_i 提供一个对 m_w 有效的签名。

(3) ID_i 的代理签名密钥是 $psk_{[i\to j]}=<U_i',K_i'>$。

Proxy_Sign：设代理签名密钥 $psk_{[i\to j]}=<U_i',K_i'>$，为了代表 ID_i 生成一个关于消息 m 的代理签名，代理签名人 ID_j 应该执行以下步骤：

(1) 选择一个随机数 $k_j\in Z_q^*$ 并计算 $K_j=k_j\cdot P$。

(2) 计算 $V_j=H_3(ID_i,ID_j,m_w,m,(K_j+K_i'))$。

(3) 计算 $U_j=U_i'+Sk_j+k_j\cdot V_j$

代理签名是 $p\sigma=<U_j,K_j,K_i'>$。

Proxy_Verf：收到消息 m，授权证书 m_w 和代理签名 $p\sigma=<U_j,K_j,K_i'>$ 后，验证算法应该执行以下步骤：

(1) 如果授权证书 m_w 是无效的，(例如，已经过期)，则 $p\sigma$ 被拒绝。否则验证者从 m_w 中提取身份 ID_i，ID_j，并继续下一步。

(2) 计算 $V_j=H_3(ID_i,ID_j,m_w,m,(K_j+K_i'))$，$V_i'=H_2(ID_i,m_w,K_i')$。

(3) 返回 1 当且仅当下式成立：

$$e(U_j,P)=e(V_i',K_i')\cdot e(V_j,K_j)\cdot e(Q_i+Q_j,mpk)$$

验证方程的正确性可以证明如下：

$$e(U_j,P)=e(U_i',P)\cdot e(Sk_j,P)\cdot e(k_j\cdot V_j,P)=$$
$$e(V_i',K_i')\cdot e(V_j,K_j)\cdot e(Q_i,mpk)\cdot e(Q_j,mpk)=$$
$$e(V_i',K_i')\cdot e(V_j,K_j)\cdot e(Q_i+Q_j,mpk)$$

IDP：在输入一个授权证书 m_w 和一个代理签名 $p\sigma$ 时，在验证了代理签名 $p\sigma$ 的正确性后，代理识别算法返回包含在 m_w 中的代理签名人的身份。

5 安全分析

5.1 安全证明

假设一个运行时间最多为 t 的 PPT 敌手 A 能以不可忽略的概率 ε 成功破解我们的 IBPS 方案，通过使用来自文献[16]的技术构建一个 PPT 算法 B，它调用 A 并以不可忽略的概率求解 CDH 问题。

若 $(X=a\cdot P,Y=b\cdot P)\in G_1\times G_1$，$a,b\in Z_q$，为输入给 B 的 CDH 问题的一个实例。然后 B 通过下述方式与 A 交互(B 模拟安全实验中的挑战者)。

系统参数 params 是

$$<(G_1,+),(G_2,\bullet),e,q,P,mpk,H_1,H_2,H_3>,$$

这里 mpk 被设置为 X，H_1,H_2,H_3 是由 B 控制的随机 oracle。在模拟过程中，B 按如下的方式回答 A 的查询：

对 H_1 的查询：B 保存一个列表 $H_1^{list}=\{<ID,Q_{ID},l,coin>\}$，其中 $coin\in\{0,1\}$。如果 H_1^{list} 中的一个元组 $\{<ID,Q_{ID},l,coin>\}$ 已包含被查询的身份 ID，B 返回 $H_1(ID)=Q_{ID}$ 给 A。否则 B 选择一个随机的 $l\in Z_q^*$，以概率 δ 设置 $(Q_{ID}=l\cdot P$，$coin=0)$，或以概率 $1-\delta$ 设置 $(Q_{ID}=l\cdot Y$，$coin=1)$。然后 B 添加 $<ID,Q_{ID},l,coin>$ 到 H_1^{list} 并返回 $H_1(ID)=Q_{ID}$ 给 A。

CreateUser：B 保存 1 个列表 $L=\{<ID,Sk_{ID}>\}$。设被查询的身份为 ID，B 执行如下步骤：

(1) 如果列表 L 已经包含 $<ID,Sk_{ID}>$，B 返回一个消息来表明这一点。

(2) 否则，B 先查询 $H_1(ID)$。然后 B 查找 H_1^{list} 提取一个元组 $<ID,Q_{ID},l,coin>$。如果 $coin=1$，B 添加 $<ID,\perp>$ 到列表 L。如果 $coin=0$，B 计算 $Sk_{ID}=l\cdot mpk$，添加 $<ID,Sk_{ID}>$ 到列表 L，并创建一个空数组 $Pkey_{ID}$ 用于存储由 ID 参与生成的代理密钥。

RevealSecretKey：设被查询的身份为 ID。B 首先查找列表 L，如果 L 包含 $<ID,Sk_{ID}>$ 且 $Sk_{ID}\neq\perp$，B 返回 Sk_{ID}。否则，B 返回 $\perp$ 并中止运行。

第 27 卷第 6 期 系统仿真学报 Vol. 27 No. 6
2015 年 6 月 Journal of System Simulation Jun., 2015

对 H_2 的查询：B 保存一个列表 H_2^{list}。设给定的输入为 $<ID,m,K>$，如果 $<ID,m,K,h_{ID}^{(2)}>$ 已经在 H_2^{list} 中，B 返回 $h_{ID}^{(2)}\cdot P$。否则 B 选择一个随机的 $h_{ID}^{(2)}\in Z_q^*$，并返回 $H_2(ID,m,K)=h_{ID}^{(2)}\cdot P$ 给 A。然后 $<ID,m,K,h_{ID}^{(2)}>$ 被添加到 H_2^{list} 中。

Sign_Msg：设给定的输入为 $<ID,m>$。B 应执行如下步骤：

(1) 执行 $Sk_{ID}\leftarrow$ RevealSecretKey(ID)。如果 $Sk_{ID}=\perp$，B 返回 $\perp$ 并中止运行。

(2) 否则 B 选择一个随机数 $k\in Z_q^*$ 并计算 $K=k\cdot P$。

(3) 执行 $V\leftarrow H_2(ID,m,K)$ 计算 $U=k\cdot V+Sk_{ID}$。

(4) B 返回 $\sigma=<U,K>$ 给 A。

DesignateProxy：设 A 选择的输入为 ID_i(原始签名人)、ID_j(代理签名人)和授权证书 m_w。如果 $Sk_{ID_i}=\perp$，B 返回 $\perp$ 并中止运行。否则，B 通过输入 (ID_i,m_w) 调用 Sign_Msg。如果一个有效的签名 $\sigma'=<U_i',K_i'>$ 被 Sign_Msg 功能生成，B 会发送 σ' 到 A。最后，B 设置 $Pkey_i[j][t]\leftarrow\sigma'$，这里 t 指示列表 $Pkey_i[j]$ 最后空闲的位置。显然，代理签名密钥仅是对授权证书的签名，在这种情况下向敌手提供代理密钥是没有必要的，因为敌手可以通过查询 Sign_Msg 来完成这一功能。

H_3 查询：B 保存一个列表 H_3^{list}。设 A 选择的输入为 $<ID_i,ID_j,m_w,m,K_{i,j}>$，如果 $<ID_i,ID_j,m_w,m,K_{i,j},h_{i,j}^{(3)}>$ 已经在 H_3^{list} 中，B 返回 $h_{i,j}^{(3)}\cdot P$。否则，B 选择一个随机的 $h_{i,j}^{(3)}\in Z_q^*$，并设置 $H_3(ID_i,ID_j,m_w,m,K_{i,j})=h_{i,j}^{(3)}\cdot P$ 作为对 A 的响应。$<ID_i,ID_j,m_w,m,K_{i,j},h_{i,j}^{(3)}>$ 被添加到 H_3^{list} 中。

Proxy_Sign_Msg：不失一般性，设 A 选择输入 $<ID_i,ID_j,m_w>$ 请求指定代理功能，并得到成功的响应后，我们假设 A 总是选择输入 $<ID_i,ID_j,t,m_w,m>$ 作为对 Proxy_Sign_Msg 功能的查询。然后 B 执行如下：

(1) 如果对应的表项 $Pkey_i[j][t]$ 没有定义，B 返回 $\perp$。否则设 $Pkey_i[j][t]=\sigma'$，$\sigma'=<U_i',K_i'>$，B 进行下一步。

(2) B 执行 $Sk_{ID_j}\leftarrow$ RevealSecretKey(ID_j)。如果 $Sk_{ID_j}=\perp$，B 返回 $\perp$ 并中止运行。

(3) 选择一个随机数 $k_j\in Z_q^*$ 并计算 $K_j=k_j\cdot P$。

(4) 执行 $V_j\leftarrow H_3(ID_i,ID_j,m_w,m,(K_j+K_i'))$。

(5) 计算 $U_j=U_i'+Sk_{ID_j}+k_j\cdot V_j$。

(6) B 返回 $p\sigma=<U_j,K_j,K_i'>$。

最终，A 结束运行并输出一个伪造的签名(为了成功地伪造签名，在安全模型中定义的对 A 的限制必须满足)。考虑以下情况：

(1) 假设 A 为已创建的身份 ID^*，针对一个消息 m^* 伪造的签名结构为 $\sigma^*=<U^*,K^*>$。然后 B 查找 H_1^{list} 去提取一个元组 $<ID^*,Q_{ID^*},l,coin>$。

如果 $coin=0$，B 报告失败并终止运行。如果 $coin=1$，B 查找 H_2^{list} 去提取一个元组 $<ID^*,m^*,K^*,h_{ID^*}^{(2)}>$。$A$ 没有发出输入为 $<ID^*,m^*,K^*>$ 对 H_2 的查询，且满足伪造成功的条件，其事件的概率最多是 $1/q$，这是可以忽略的。因此我们知道 $H_2(ID^*,m^*,K^*)=h_{ID^*}^{(2)}\cdot P$ 至少以概率 $1-1/q$ 成立。所以我们有：

$$e(U^*,P)=e(V^*,K^*)\cdot e(Q_{ID^*},mpk),$$

这里的 $V^*=h_{ID^*}^{(2)}\cdot P=e(h_{ID^*}^{(2)}\cdot P,K^*)\cdot e(l\cdot Y,X)$

因此 $e(Y,X)^l=e(U^*-h_{ID^*}^2\cdot K^*,P)$。

然后 B 输出 $l^{-1}\cdot(U^*-h_{ID^*}^2\cdot K^*)$ 作为对 G_1 上给定的 CDH 问题实例的解。

(2) 在完成对输入为 (ID_i,ID_j,m_w) 的指定代理功能的查询后，假设 A 对消息 m^* 伪造签名 $<ID_i,ID_j,m_w,U_j,K_j,K_i'>$。然后 B 查找 H_1^{list} 提取 $<ID_i,Q_{ID_i},l_i,coin_i>$ 和 $<ID_j,Q_{ID_j},l_j,coin_j>$。

如果 $coin_i=0\wedge coin_j=0$，B 报告失败并终止运行。

否则，其中一项至少为 1。B 查找 H_2^{list}，H_3^{list} 分别提取 $<ID_i,m_w,K_i',h_{ID_i}^{(2)}>$，$<ID_i,ID_j,m_w,m,K_i'+K_j,h_{i,j}^{(3)}>$。

因为伪造是成功的，A 并未查询 H_2 或 H_3，这事件发生的概率最多是 $2/q$。因此我们知道这些元组已经在 H_2^{list}，H_3^{list} 中的概率至少为 $1-2/q$。所以我们有：

$$e(U_j,P)=e(V_i',K_i')\cdot e(V_j,K_j)\cdot e(Q_{ID_i},mpk)\cdot e(Q_{ID_j},mpk)$$

其中 $V_j \leftarrow H_3(ID_i,ID_j,m_w,m,(K_j+K_i'))$，$V_i' \leftarrow H_2(ID_i,m_w,K_i')$

然后考虑以下子情况：

(2.1) $coin_i=1 \wedge coin_j=0$。

$$e(U_j,P)=e(h_{ID_i}^{(2)}\cdot P,K_i')\cdot e(h_{i,j}^{(3)}\cdot P,K_j)\cdot e(l_i\cdot Y,X)\cdot e(l_j\cdot P,X)$$

因此 $e(Y,X)^{l_i}=e(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j-l_j\cdot X,P)$。

然后 B 输出 $(l_i)^{-1}\cdot(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j-l_j\cdot X)$ 作为对 G_1 上给定的 CDH 问题实例的解。

(2.2) $coin_i=0 \wedge coin_j=1$。

$$e(U_j,P)=e(h_{ID_i}^{(2)}\cdot P,K_i')\cdot e(h_{i,j}^{(3)}\cdot P,K_j)\cdot e(l_i\cdot P,X)\cdot e(l_j\cdot Y,X)$$

因此 $e(Y,X)^{l_j}=e(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j-l_i\cdot X,P)$。

然后 B 输出 $(l_j)^{-1}\cdot(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j-l_i\cdot X)$ 作为对 G_1 上给定的 CDH 问题实例的解。

(2.3) $coin_i=1 \wedge coin_j=1$。

$$e(U_j,P)=e(h_{ID_i}^{(2)}\cdot P,K_i')\cdot e(h_{i,j}^{(3)}\cdot P,K_j)\cdot e(l_i\cdot Y,X)\cdot e(l_j\cdot Y,X)$$

因此 $e(Y,X)^{l_i+l_j}=e(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j,P)$。

然后 B 输出 $(l_i+l_j)^{-1}\cdot(U_j-h_{ID_i}^{(2)}\cdot K_i'-h_{i,j}^{(3)}\cdot K_j)$ 作为对 G_1 上给定的 CDH 问题实例的解。

(3) 假设 A 对一个消息 m^* 伪造签名 $<ID_i,ID_j,m_w,U_j,K_j,K_i'>$ 且未对输入 (ID_i,ID_j,m_w) 发出一个指定代理功能查询。对这种情况的分析与情形(2)是完全类似的。

引理 1 如果在模拟过程中算法 B 不中止运行，那时在模拟安全实验中敌手 A 的视图与在真正安全实验中的视图是不可分辨的。

证明 首先，对于 H_1，H_2，H_3 查询的响应与在真正的安全实验中的响应是同分布的，因为每个响应均匀分布在 G_1 中。如果算法 B 不中止运行，对于 RevealSecretKey，Sign_Msg，DesignateProxy，Proxy_Sign_Msg 查询的响应也与真正的安全实验中的响应是同分布的。因此，结论成立。

定理 1 假设有一个 PPT 敌手 A 可以针对我们的 IBPS 方案存在性地伪造一个标准签名，其成功概率至少为 ε，运行时间最多为 t。设 A 进行了至多 q_c 次的 CreateUser 查询，q_{H_i} 分别代表对随机 oracles H_i，$i=1$，2 的查询次数，q_{sig} 次对 Sign_Msg 的查询和 q_{rev} 次对 RevealSecretKey 的查询。那么就有一个算法 B 以概率 ε 解决基于 G_1 的 CDH 问题：

$$\varepsilon \approx \frac{\varepsilon}{q_{sig}+q_c}\left(1-\frac{1}{q_{sig}+q_c+1}\right)^{q_{sig}+q_c+1}$$

证明 在这种情况下，B 不中止运行的概率(即 B 能回答所有标准签名查询和 RevealSecretKey 查询)至少为 $\delta^{q_{sig}+q_{rev}}$。原因在于如果 B 能够获得一个用户的密钥，他可以完全地回答关于该用户的签名查询。当 B 回答 CreateUser 查询时，易见他能以概率 δ 正确地生成用户的密钥。因此，B 可以以概率 δ 正确地回答 1 个签名查询或 Reveal SecretKey 查询。

然后 B 以概率 $(1-\delta)(1-1/q)$ 输出关于 CDH 问题实例的解。因此 B 解决 CDH 问题的成功概率至少为：$\varepsilon\ (1-\delta)(1-1/q)\ \delta^{q_{sig}+q_{rev}} \approx \varepsilon\ (1-\delta)\ \delta^{q_{sig}+q_{rev}}$。让 $\lambda=\varepsilon\ (1-\delta)\ \delta^{q_{sig}+q_{rev}}$，$a=q_{sig}+q_{rev}$，通过使用 Coron 提出的技术[16]进行分析，成功概率 λ 在 $\delta_{opt}=\frac{a}{a+1}$ 取最大值。

因此，B 成功的概率 $\varepsilon \approx \frac{\varepsilon}{a}\left(1-\frac{1}{a+1}\right)^{a+1}$，而且对于充分大的 a，$\varepsilon \approx \frac{\varepsilon}{\exp(1)\cdot a}$。

B 的运行时间可以估计为：

$t+(q_c+q_{H_1}+q_{H_2}+q_{sig})t_m+q_{rev}q_cO(1)$

t_m 是在 G_1 中用来计算一个标量乘法的时间。

定理 2 假设有一个多项式时间的敌手 A 可以针对我们 IBPS 方案存在性地伪造一个代理签名，其成功概率至少为 ε 且运行时间至多为 t。设 A 进行至多 q_c 次的 CreateUser 查询，q_{H_i} 分别代表对随机 oracles H_i，$i=1$，2，3 的查询，q_{sig} 次 Sign_Msg 查询，q_{psig} 次 Proxy_Sign_Msg 查询，q_{desg} 次 DesignateProxy 查询和 q_{rev} 次

RevealSecretKey 查询。那么就有一个算法 B 以概率 ε 解决基于 G_1 的 CDH 问题：

$\varepsilon' \approx \frac{\varepsilon}{b}(1-\frac{1}{1+b})^{1+b}$，其中

$b=\frac{(q_{sig}+q_{desg}+q_{psig}+q_{rev})}{2}$。

证明 在这种情况下，B 不中止运行的概率(即 B 能回答所有标准签名查询，指定代理查询，代理签名查询和 RevealSecretKey 查询)至少是 $\delta^{q_{sig}+q_{desg}+q_{psig}+q_{rev}}$。原因在于如果 B 获得代理签名人的密钥，B 可以成功地响应一个代理签名查询，我们同样假设 A 总是在成功地查询指定代理功能之后，发出一次对代理签名功能查询。因此，B 能以概率 δ 成功地回答一次代理签名查询。

只要不出现 $coin_i=0 \wedge coin_j=0$ 这种情形，B 以概率 $(1-\delta^2)(1-2/q)$ 输出关于 CDH 问题的解。因此 B 能够以如下概率解决 CDH 问题：

$\varepsilon\ (1-\delta^2)(1-2/q)\ \delta^{q_{sig}+q_{desg}+q_{psig}+q_{rev}} \approx$

$\varepsilon\ (1-\delta^2)\ \delta^{q_{sig}+q_{desg}+q_{psig}+q_{rev}}$

令 $\lambda=\varepsilon\ (1-\delta^2)\ \delta^{q_{sig}+q_{desg}+q_{psig}+q_{rev}}$，

$b=\frac{(q_{sig}+q_{desg}+q_{psig}+q_{rev})}{2}$。

成功的概率 λ 在 $\delta_{opt}=\sqrt{\frac{b}{b+1}}$ 取最大值。

因此，B 的成功概率为 $\varepsilon' \approx \frac{\varepsilon}{b}(1-\frac{1}{1+b})^{1+b}$，

对于充分大的 b，$\varepsilon' \approx \frac{\varepsilon}{\exp(1)\cdot b}$。

B 的运行时间可以估计如下：

$t+(q_c+q_{H_1}+q_{H_2}+q_{H_3}+q_{sig}+q_{psig}+q_{desg})t_m + q_{rev}q_cO(1)$

这里 t_m 是在 G_1 中计算一个标量乘法的时间。

为了简单起见，我们只考虑前面分析中的情形 (2)，因为情形(3)与情形(2)是完全类似的。

5.2 讨论

可验证性：由于授权证书由身份信息、代理权限的有效期、可被代理签名的消息类型组成，第 4 节的代理签名验证方程的正确性能推出可验证性。

不可伪造性：它是由定理 2 的结论建立的。

强可识别性：在验证了代理签名的正确性后，代理签名人的身份可以从授权证书中提取。

不可抵赖性：它来自于不可伪造性和强可识别性。

防止滥用：由于需要验证授权证书的合法性，代理签名人只能在不违反由原始签名人签署的授权证书 m_w 情况下生成代理签名。此外代理签名密钥只是对授权证书 m_w 的标准签名。根据定理 1，在我们方案中的标准签名方案是不可伪造的。因此代理签名人不能对未被原始签名人授权的消息进行代理签名。

代理密钥泄露：当代理签名密钥只是基于授权证书的签名时，此时即使提供代理签名密钥给敌手也是无害的。因此我们的方案对代理密钥泄露攻击是安全的。

6 性能分析

在本节中，根据签名长度和计算开销评估了所提方案和在文献[9-11]中提出的相关方案的性能。$|G_1|$ 代表 G_1 中一个元素的位长。Mu 和 Ad 在 G_1 中分别表示标量乘法和加法。H 代表一个散列函数的操作。Exp 和 P 分别表示 G_2 中的幂运算和双线性运算，它们是方案中最耗时的运算。比较结果列在表 1 中。在文献[9-10]中所提方案易受代理密钥泄露攻击。从表中可以看出，相比于文献[11]提出的方案，本文的方案降低了计算开销。

表 1 方案性能比较

方案	代理签名位长	代理签名的计算开销	验证代理签名的计算开销	防范代理密钥泄露攻击
Xu 的方案[9]	$3\|G_1\|$	$2Mu+1Ad+1H$	$5P+Exp$	否
Shim 的方案[10]	$3\|G_1\|$	$3Mu+1Ad+1H$	$3P$	否
Wu 的方案[11]	$3\|G_1\|$	$4Mu+3Ad+2H$	$5P$	能
本文的方案	$3\|G_1\|$	$2Mu+3Ad+1H$	$4P$	能

7 结论

本文针对代理密钥泄露攻击提出了 1 个基于身份的代理签名方案。首先建立 1 个基于身份的代理签名方案的安全模型。然后基于双线性映射提出了 1 个基于身份的代理签名方案。接下来提供了 1 个安全证明来说明该方案的安全可以归约到求解 CDH 问题的困难性，而且新方案对代理密钥泄露攻击是安全的。虽然 Wu 等人的方案[11]也能防范代理密钥泄露攻击，性能分析表明相比于文献[11]提出的方案，本文的方案降低了计算开销。

参考文献：

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation [C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security. USA: ACM, 1996: 48-57.

[2] Goldwasser S, Micali S, Rivest R L. A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks [J]. SIAM Journal on Computing (S1064-8275), 1988, 17(2): 281-308.

[3] Boldyreva A, Palacio A, Warinschi B. Secure proxy signature schemes for delegation of signing rights [J]. Journal of Cryptology (S0933-2790), 2012, 25(1): 57-115.

[4] Schuldt Jacob C N, Matsuura K, Paterson K G. Proxy Signatures secure against proxy key exposure [C]// Public Key Cryptography – PKC 2008. Berlin, Germany: Springer, 2008: 141-161.

[5] Shamir A. Identity based cryptosystems and signature schemes [C]// Advances in Cryptology-CRYPTO'84. Berlin, Germany: Springer-Verlag, 1984: 47-53.

[6] Boneh D, Franklin M. Identity based encryption from the Weil pairing [C]// Advances in Cryptology - CRYPTO 2001. Berlin, Germany: Springer-Verlag, 2001: 213-229.

[7] Hess F. Efficient identity based signature schemes based on pairings [C]// Selected Areas in Cryptography-SAC'2002. Berlin, Germany: Springer-Verlag, 2002: 310-324.

[8] Zhang Fangguo, Kim K. Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings [C]// 8th Australasian Conference, ACISP 2003. Berlin, Germany: Springer, 2003: 312-323.

[9] Xu Jing, Zhang Zhenfeng, Feng Dengguo. ID-based Proxy Signature using Bilinear Pairing [C]// ISPA 2005 International Workshops. Berlin, Germany: Springer-Verlag, 2005: 359-367.

[10] Shim K A. An Identity-Based Proxy Signature Scheme from Pairings [C]// 8th International Conference, ICICS 2006. Berlin, Germany: Springer, 2006: 60-71.

[11] Wu Wei, Mu Yi, Susilo W, et al. Identity-based Proxy Signature from Pairing [C]// 4th International Conference, ATC 2007. Berlin, Germany: Springer-Verlag, 2007: 22-31.

[12] Kim S, Park S, Won D. Proxy signature, revisited [C]// ICICS '97 Proceedings of the First International Conference on Information and Communication Security. London, UK: Springer-Verlag, 1997: 223-232.

[13] Lee B, Kim H, Kim K. Strong proxy signature and its applications [C]// Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01). Japan: The Institute of Electronics, Information and Communication Engineers, 2001: 603-608.

[14] Hsu Chien-Lung, Wu Tzong-Sun, Wu Tzong-Chen. New nonrepudiable threshold proxy signature scheme with known signers [J]. Journal of Systems and Software (S0164-1212), 2001, 58(2): 119-124.

[15] Jiang Guanxiong. A new proxy multi-signature scheme [C]// Networking and Digital Society - ICNDS '09. USA: IEEE, 2009: 134-138.

[16] Coron J S. On the exact security of full domain hash [C]// Advances in Cryptology-CRYPTO 2000. Berlin, Germany: Springer-Verlag, 2000: 229-235.

DOI: 10.16182/j.cnki.joss.2015.06.027