原始签名人匿名的代理环签名研究

鲍皖苏 隗 云 钟普查
(解放军信息工程大学电子技术学院 郑州 450004)

摘 要：环签名是一种新的匿名签名技术，能保证签名用户的无条件匿名性。代理环签名是将代理签名和环签名相结合产生的一种签名。已有的代理环签名方案都是利用环签名的思想实现代理签名人的身份匿名性，但原始签名人的身份始终是公开的。该文基于 RSA 问题的难解性提出了一种新的代理环签名方案，在保证代理签名人身份匿名性的同时，还能保证原始签名人身份匿名性，并证明该方案在随机预言模型下能抵抗适应性选择消息攻击。

关键词：环签名；代理环签名；身份匿名性
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2009)10-2392-05

Research on Proxy Ring Signature with Anonymity of the Original Signer

Bao Wan-su Wei Yun Zhong Pu-cha
(*Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou* 450004, *China*)

Abstract: Ring signature is a new kind of anonymous signature which can provide unconditional anonymity of the signer. Proxy ring signature is the combination of proxy signature and ring signature. Previous proxy ring signature schemes are constructed based on the idea of ring signature to provide the privacy protection for the proxy signer while the identity of the original signer is public. A new proxy ring signature scheme based on the difficulty of RSA problem is proposed in this paper, which can provide the privacy protection for both the proxy signer and the original signer. It proves that the proposed scheme can resist the adaptive chosen-message attack in the random oracle model.

Key words: Ring signature; Proxy ring signature; Privacy protection

1 引言

代理签名的概念是Mambo，Usuda和Okamoto[1]于1996年提出的，所谓代理签名是指：在一个签名方案中，一个被指定的代理签名人可以代表原始签名人生成有效的签名。他们在文献[1]中指出，代理签名方案应满足不可伪造性、可验证性、不可否认性、可区分性及可识别性等基本的安全要求。

Revist等[2]于2001年首次提出环签名的概念。环签名能保证签名者的无条件匿名性，且不需要预先建立群组以及撤销环成员等阶段，签名人只要知道某个用户的公钥，不需要其同意或者合作就可以将其加入到环中对消息进行签名，其唯一假设是所有用户都拥有支持某种标准签名方案的公钥。由于环签名的这些性质及其应用背景，很多学者对环签名进行了研究[3–16]。

代理签名的某些实际应用要求代理签名人身份是保密的(例如，通过所签署文件的重要性可推测各代理签名人在行使代理签名权时的优、劣势，若想隐藏该信息可采用代理环签名)，Zhang 等[3]首次利用环签名的思想实现了这一目的，提出了代理环签名的概念：某原始签名人将签名权利授权给多个代理签名人，任一代理签名人在代理原始签名人进行签名时，都能保证其自身身份的匿名性，即任何人都无法确定代理签名是哪个代理签名人所为。Awasthi 等[5]提出的代理环签名方案映射次数更少，但这两个方案都只能保证代理签名人的身份匿名性，原始签名人的身份始终是公开的。

本文基于 RSA 问题[17]的难解性提出了一个在随机预言模型[18]下能抵抗适应性选择消息攻击的代理环签名方案，在保证代理签名人身份匿名性的同时，还能保证原始签名人身份匿名性。

2 相关定义

2.1 环签名[1]

假设每个用户都拥有一对支持某种标准签名方案的公钥及私钥。一个环签名方案是包括以下算法的数字签名方案：

(1)签名算法：一个概率算法，给定消息m，n个环成员的公钥及一个成员(真正的签名人)的私

2008-09-22 收到，2009-06-18 改回
国家自然科学基金(10501053)资助课题

钥，输出关于消息 m 的环签名 σ 。

(2)验证算法：一个确定性算法，输入消息 m 和签名 σ (包含所有成员的公钥)，输出 0 或 1。

一个安全的环签名方案必须无条件匿名性和不可伪造性[1]。

2.2 代理环签名[5]

假设每个用户都拥有一对支持某种标准签名方案的公钥及私钥。一个代理环签名方案包括以下 3 个算法：代理签名密钥生成算法、代理签名算法和验证算法。由代理签名和环签名必须满足的安全性质可知，一个安全的代理环签名方案应满足：代理签名人的无条件匿名性和代理环签名的不可伪造性。

2.3 代理环签名的安全模型

本文考虑随机预言模型下的适应性选择消息攻击。对代理环签名的攻击分两种：对代理密钥的伪造和对代理签名的伪造。在对代理密钥的伪造攻击中，攻击者可以：向随机预言、签名预言和代理签名密钥预言询问，若在此条件下攻击者能以不可忽略的概率产生一个有效的签名(原始签名人的普通数字签名)或代理签名公钥(这里的有效指用原始签名人公钥验证有效)，则称其攻击成功。

同理，在对代理签名的伪造攻击中，攻击者可以向随机预言和代理签名预言提出询问，如果攻击者能以不可忽略的概率产生关于消息 m 的有效代理环签名，且未向代理签名预言询问过关于消息 m 的代理环签名，则称其攻击成功。

3　原始签名人匿名的代理环签名方案

3.1 用户密钥的生成

用户生成公、私钥对 $((n,e),d)$，其中 $n=pq$，p 和 q 为大素数，整数 e，d 满足 $ed=1\bmod\varphi(n)$，$\varphi(n)=(p-1)(q-1)$ 为欧拉函数。

3.2 代理密钥的生成

假设原始签名人 A 和代理签名人 B 的公、私钥对分别为 $((n_A,e_A),d_A)$ $((n_B,e_B),d_B)$。m_ω 为授权书，包含授权有效期等内容，但为保证签名人身份匿名性，授权书不包含与原始签名人或代理签名人身份相关的任何信息。$h:\{0,1\}^*\to[1,n_A)$ 为抗碰撞的单向散列函数。代理密钥的生成过程如下：

(1) A 选取整数 $e_p(0<e_p<\varphi(n_A))$ 且 $\gcd(e_p,\varphi(n_A))=1$，计算满足 $e_pd_{p_A}=1\bmod\varphi(n_A)$ 的 d_{p_A}，再计算 $\alpha=h(m_\omega)^{d_{pA}d_A}\bmod n_A$，并将 (m_ω,α,e_p) 传送给 B。

(2) B 首先判断 e_p 是否小于 $\varphi(n_B)$ 且 $\gcd(e_p,\varphi(n_B))=1$ 是否成立，任一条件不成立则要求 A 重新选择 e_p 并执行步骤(1)；否则验证 $h(m_\omega)=\alpha^{e_pe_A}\bmod n_A$ 是否成立，不成立则要求 A 重新执行步骤(1)，成立则计算满足 $e_pd_{p_B}=1\bmod\varphi(n_B)$ 的 d_{p_B}，d_{p_B} 即代理签名密钥，e_p 为对应的代理公钥。

3.3 代理签名

设原始签名人集合为 $\mathcal{OR}=\{A_1,A_2,\cdots,A_{n_1}\}$，代理签名人集合为 $\mathcal{PR}=\{B_1,B_2,\cdots,B_{n_2}\}$，对任意 $i\in\{1,2,\cdots,n_1\}$，$j\in\{1,2,\cdots,n_2\}$，B_j 是 A_i 的代理签名人，且对于同一原始签名人，所有代理签名人具有相同的代理权限。m_{ω_i} 为原始签名人 A_i 产生的授权书，$e_{p_{i,j}}$ 为原始签名人 A_i 为代理签名人 B_j 产生的代理公钥，$d_{p_{i,j}}$ 表示对应的代理签名密钥。$H:\{0,1\}^*\to\{0,1\}^l$，$G:\{0,1\}^*\to\{0,1\}^l$ 为抗碰撞的单向散列函数，假设模数 $n_{B_j}(j=1,2,\cdots,n_2)$ 的长度 l_{B_j} 都小于 l。定义 RSA 扩展函数

$$g_i^j(x)=\begin{cases}q_jn_{B_j}+f_i^j(r_j), & (q_j+1)n_{B_j}\le 2^l\\ x, & \text{其它}\end{cases}$$

其中 $f_i^j(x)=x^{e_{p_{i,j}}}\bmod n_{B_j}$，$x=q_jn_{B_j}+r_j$，$q_j$，$r_j$ 都是整数且 $0\le r_j<n_{B_j}$。由文献[2]可知，当 $l-l_{B_j}$ 足够大时，x 在 g_i^j 的作用下保持不变的概率可忽略不计。

设代理签名人 $B_{k_2}(1\le k_2\le n_2)$ 欲代理原始签名人 $A_{k_1}(1\le k_1\le n_1)$ 对消息 m 进行签名，过程如下：

Step1　For $i=1,\cdots,n_1,i\ne k_1$, Do $v_i\in_R\{0,1\}^l$

Step2　For $i=1,\cdots,n_1,i\ne k_1$, Do

For $j=1,\cdots,n_2$, Do

$x_i^j\in_R\{0,1\}^l$, $y_i^j=g_i^j(x_i^j)$, $z_i=C_{v_i,m}(y_i^1,y_i^2,\cdots,y_i^{n_2})$, $\gamma_i=v_i\oplus z_i$

where $C_{v_i,m}(y_i^1,y_i^2,\cdots,y_i^{n_2})=H(m,y_i^{n_2}\oplus H(m,y_i^{n_2-1}\oplus\cdots H(m,y_i^1\oplus v_i)\cdots))$

Step3　Do $\sigma_1\in_R\{0,1\}^l$, and $u_{k_1+1}=G(\sigma_1)$

For $i=k_1+2,\cdots,n_1,1,\cdots,k_1$, Do $u_i=G(u_{i-1}\oplus\gamma_{i-1})$

Step4　Do $\gamma_{k_1}=\sigma_1\oplus u_{k_1}$

其中，step3 和 step4 利用 σ_1，单向函数 G 以及 $\gamma_i(i=1,\cdots,n_1,i\ne k_1)$ 构造了一个环以隐藏原始签名人身份，因为对 $i=1,\cdots,n_1$ 均有 $u_i=G(u_{i-1}\oplus\gamma_{i-1})$ 且 $u_1=G(u_{n_1}\oplus\gamma_{n_1})$，如图 1 所示。

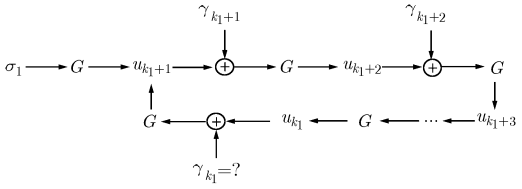

图 1　签名算法 step3 和 step4

Step5 For $i=k_1$, Do

For $j=1,\cdots,n_2$, $j\neq k_2$, Do

$\sigma_2\in_R\{0,1\}^l$, $x_{k_1}^j\in_R\{0,1\}^l$,

and $y_i^j=g_{k_1}^j(x_i^j)$

Step6 Do

$c_{k_2+1}=H(m,\sigma_2)$

$c_{k_2+2}=H(m,c_{k_2+1}\oplus y_{k_1}^{k_2+1})$

$\vdots\qquad\vdots$

$c_{n_2}=H(m,c_{n_2-1}\oplus y_{k_1}^{n_2-1})$

$c_1=H(m,c_{n_2}\oplus y_{k_1}^{n_2})$

$c_2=H(m,c_1\oplus y_{k_1}^1\oplus\gamma_{k_1})$

$c_3=H(m,c_2\oplus y_{k_1}^2)$

$\vdots\qquad\vdots$

$c_{k_2}=H(m,c_{k_2-1}\oplus y_{k_1}^{k_2-1})$

and $y_{k_1}^{k_2}=c_{k_2}\oplus\sigma_2$, $x_{k_1}^{k_2}=(g_{k_1}^{k_2})^{-1}(y_{k_1}^{k_2})$,

$v_{k_1}=\gamma_{k_1}\oplus c_1$

以上两步通过前面计算出的 γ_{k_1} 求满足 $z_{k_1}=C_{v_{k_1},m}(y_{k_1}^1,y_{k_1}^2,\cdots,y_{k_1}^{n_2})$，$\gamma_{k_1}=v_{k_1}\oplus z_{k_1}$ 的 v_{k_1}，以隐藏代理签名人的身份。签名算法 Step6 如图 2 所示。

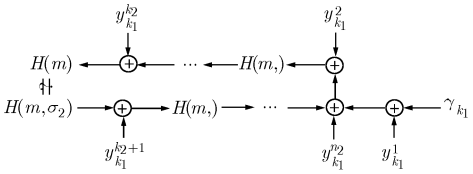

图 2 签名算法 step6

Step7 Do $\eta\in_R\{1,\cdots,n_1\}$

and output$\left(\eta,u_\eta,\mathcal{OR},\mathcal{PR},\bigcup_{1\le i\le n_1}\left(m_{\omega_i};e_{p_{i,1}},\cdots,e_{p_{i,n_2}};x_i^1,\cdots,x_i^{n_2};v_i\right)\right)$

3.3 代理签名的验证

代理签名验证算法如下：

Step1 For $i=1,\cdots,n_1$, Do

For $j=1,\cdots,n_2$, Do

$y_i^j=g_j(x_i^j)$, $z_i=C_{v_i,m}(y_i^1,y_i^2,\cdots,y_i^{n_2})$

and $\gamma_i=v_i\oplus z_i$

Step2 Verify $u_\eta\stackrel{?}{=}G(\gamma_{\eta-1}\oplus G(\cdots G(\gamma_\eta\oplus u_\eta)\cdots))$

4 方案分析

4.1 正确性

由签名算法 step6 可知

$$c_2=H\left(m,c_1\oplus y_{k_1}^1\oplus\gamma_{k_1}\right)=H\left(m,v_{k_1}\oplus y_{k_1}^1\right)$$

$$c_3=H\left(m,c_2\oplus y_{k_1}^2\right)=H\left(m,y_{k_1}^2\oplus H\left(m,v_{k_1}\oplus y_{k_1}^1\right)\right)$$

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

$$c_{k_2}=H\left(m,c_{k_2-1}\oplus y_{k_1}^{k_2-1}\right)=\cdots$$

$$=H\left(m,y_{k_1}^{k_2-1}\oplus H\left(m,y_{k_1}^{k_2-2}\oplus\cdots H\left(m,y_{k_1}^1\oplus v_{k_1}\right)\cdots\right)\right)$$

$$c_{k_2+1}=H\left(m,c_{k_2}\oplus y_{k_1}^{k_2}\right)=\cdots$$

$$=H\left(m,y_{k_1}^{k_2}\oplus H\left(m,y_{k_1}^{k_2-1}\oplus\cdots H\left(m,y_{k_1}^1\oplus v_{k_1}\right)\cdots\right)\right)$$

$$=H(m,\sigma_2)$$

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

$$c_{n_2}=H\left(m,c_{n_2-1}\oplus y_{k_1}^{n_2-1}\right)=\cdots$$

$$=H\left(m,y_{k_1}^{n_2-1}\oplus H\left(m,y_{k_1}^{n_2-2}\oplus\cdots H\left(m,y_{k_1}^1\oplus v_{k_1}\right)\cdots\right)\right)$$

$$c_1=H\left(m,c_{n_2}\oplus y_{k_1}^{n_2}\right)=\cdots$$

$$=H\left(m,y_{k_1}^{n_2}\oplus H\left(m,y_{k_1}^{n_2-1}\oplus\cdots H\left(m,y_{k_1}^1\oplus v_{k_1}\right)\cdots\right)\right)$$

即有 $\gamma_{k_1}=v_{k_1}\oplus c_1=v_{k_1}\oplus C_{v_{k_1},m}(y_{k_1}^1,y_{k_1}^2,\cdots,y_{k_1}^{n_2})$。由签名算法 step3 和 step4 知，对任意 $\eta\in\{1,\cdots,n_1\}$ 有 $u_\eta=G(\gamma_{\eta-1}\oplus G(\cdots G(\gamma_\eta\oplus u_\eta)\cdots))$。

4.2 匿名性

由签名算法及正确性证明可知，对 $i=1,\cdots,n_1$，均有 $z_i=C_{v_i,m}(y_i^1,y_i^2,\cdots,y_i^{n_2})$，$\gamma_i=v_i\oplus z_i$。其中 v_i $(i\neq k_1)$ 由代理签名人随机选择，v_{k_1} 通过 σ_2 计算而得，σ_2 的随机性使得 v_{k_1} 不泄露原始签名人的身份信息。同时，$y_{k_1}^{k_2}$ 也由 σ_2 计算而得，故 $x_{k_1}^{k_2}=(g_{k_1}^{k_2})^{-1}\cdot(y_{k_1}^{k_2})$ 不泄露原始签名人和代理签名人的身份信息。

4.3 不可伪造性

定理 1 3.2 小节中的代理密钥生成协议在适应性选择消息攻击下是安全的。

证明 考虑 2.3 节中的安全模型，攻击者可以向随机预言 h 提出 q_h 询问，并能分别向签名预言和代理签名密钥预言提出 q_s 次签名询问和 q_p 次代理签名公钥询问(其中 $q_h>q_s+q_p$)。假设存在算法 $\mathcal{A}$，能以不可忽略的概率 ε 成功地对 3.2 小节中的代理密钥生成协议进行适应性选择消息攻击。下面证明可利用算法 $\mathcal{A}$ 构造一个新的算法 $\mathcal{B}$，能以不可忽略的概率解 RSA 问题。

设给定的 RSA 问题输入为 (n_A,e_A,y)。$\mathcal{B}$ 对随机预言 h 进行模拟时，为其建立一个询问和回答相对应的关系列表 L_h，并随机选择 $\eta\in[1,q_h)$，保证对 h 的第 η 次询问所对应的回答为 y。当算法 $\mathcal{A}$ 对随机预言 h 提出询问，$\mathcal{B}$ 首先检查 L_h 中是否存在该询问，若存在，输出对应的回答；否则，随机选择一个值输出。

当算法 $\mathcal{A}$ 询问关于消息 m 的签名时，$\mathcal{B}$ 随机选择 $\sigma\in[1,n_A)$，计算 $\sigma^{e_A}\bmod n_A$，若 $\sigma^{e_A}=y\bmod n_A$，重新选择 σ，否则输出 σ 作为消息 m 的签名，并将 (σ^{e_A},m) 保存到关系列表 L_h，即 $h(m)=\sigma^{e_A}\bmod n_A$。

当算法 $\mathcal{A}$ 询问关于授权书 m_ω 的授权代理公钥

时，$\mathcal{B}$ 随机选择 $e_p,\alpha\in[1,n_A)$，计算 $\alpha^{e_Ae_p}\bmod n_A$，若 $\alpha^{e_Ae_p}=y\bmod n_A$，重新选择 e_p，α，否则输出 (e_p,α)，并将 $(\alpha^{e_Ae_p},m_\omega)$ 保存到关系列表 L_h，即 $h(m_\omega)=\alpha^{e_Ae_p}\bmod n_A$。

若算法 $\mathcal{A}$ 输出一个有效的消息签名对 (m^*,σ^*)，即 $h(m^*)=(\sigma^*)^{e_A}\bmod n_A$，$m^*$ 为对 h 的第 η 次询问的概率不小于 $1/q_h$，此时有 $y=(\sigma^*)^{e_A}\bmod n_A$，即 σ^* 为所求 RSA 问题的输出；若算法 $\mathcal{A}$ 输出有效的代理签名公钥信息 $(e_p^*,\alpha^*,m_\omega^*)$，即 $h(m_\omega^*)=(\alpha^*)^{e_Ae_p^*}\bmod n_A$，$m_\omega^*$ 对 h 的第 η 次询问的概率也不小于 $1/q_h$，此时有 $y=((\alpha^*)^{e_p^*})^{e_A}\bmod n_A$，即 $(\alpha^*)^{e_p^*}$ 为所求 RSA 问题的输出。

由此可以看出，当 $\mathcal{A}$ 输出有效的签名或代理签名公钥时，$\mathcal{B}$ 能以不可忽略的概率求解 RSA 问题。

定理 2　上述代理环签名方案在适应性选择消息攻击下是不可伪造的。

证明　假设存在攻击算法 $\mathcal{A}$，能以不可忽略的概率 ε 成功地对上述方案进行适应性选择消息攻击。下面证明可利用算法 $\mathcal{A}$ 构造一个新的算法 $\mathcal{B}$，能以不可忽略的概率求某一 RSA 扩展函数关于某给定值 y_0 的逆。在适应性选择消息攻击下，算法 $\mathcal{A}$ 可向随机预言 H，G 提出的询问次数分别为 q_H，q_G，并可询问 q_S 个消息的签名。

给定值 y_0，$\mathcal{B}$ 首先随机选择 $i_0\in_R[1,n]$，$h_0,h_0'\in[1,q_H]$ 及 $g_0,g_0'\in[1,q_G]$，满足 $g_0<g_0'<h_0<h_0'$。

在对随机预言 H 进行模拟时，$\mathcal{B}$ 为其产生一个关于询问、回答的关系列表 L_H。当 $\mathcal{A}$ 向随机预言 H 提出询问时，$\mathcal{B}$ 首先检查 L_H 中是否存在该询问，若存在，输出对应的回答；否则，从 $\{0,1\}^l$ 中随机选择一个值输出。类似地，对随机预言 G 进行模拟，产生关系列表 L_G。除此之外，保证：若 $i_0>1$，对 H 的第 h_0' 次询问所对应回答为 $y_0\oplus x_0$；若 $i_0=1$，回答为 $y_0\oplus x_0\oplus\gamma_0$。其中，$(m,x_0)$ 为对 H 的第 h_0 次询问，$\gamma_0=\Lambda\oplus\Gamma$，而 Λ 为对 G 的第 g_0 次询问，Γ 为对 G 的第 g_0' 次询问所对应的回答。

当 $\mathcal{A}$ 询问关于消息 m 的代理签名时，$\mathcal{B}$ 执行以下步骤：

(1)For $i=1,\cdots,n_1$, Do $v_i\in_R\{0,1\}^l, z_i\in_R\{0,1\}^l$

　For $j=1,\cdots,n_2$, Do $x_i^j\in_R\{0,1\}^l$, $y_i^j=g_i^j(x_i^j)$

(2)For $j=1,\cdots,n_2-1$, Do $c_i^j\in_R\{0,1\}^l$

　For $j=1,\cdots,n_2-2$,

　　sets $c_i^{j+1}=H\left(m,y_i^{j+1}\oplus c_i^j\right)$,

　　$z_i=H(m,y_i^{n_2}\oplus c_i^{n_2-1})$ and $\gamma_i=v_i\oplus z_i$

(3) For $i=1,\cdots,n_1-1$, Do $u_i\in_R\{0,1\}^l$

　　and sets $u_{i+1}=G(u_i\oplus\gamma_i)$, $u_1=G(u_{n_1}\oplus\gamma_{n_1})$

最后，将等式 $c_i^{j+1}=H(m,y_i^{j+1}\oplus c_i^j)(j=1,\cdots,n_2-2)$，$z_i=H(m,y_i^{n_2}\oplus c_i^{n_2-1})$ 中 H 的输入、输出对保存于关系列表 L_H 中，将等式 $u_{i+1}=G(u_i\oplus\gamma_i)(i=1,\cdots,n_1-1)$，$u_1=G(u_{n_1}\oplus\gamma_{n_1})$ 中 G 的输入、输出对保存于列表 L_G 中，并选择 $\eta\in_R\{1,\cdots,n_1\}$，输出代理签名。

假设算法 $\mathcal{A}$ 以不可忽略的概率 ε 成功地伪造了一个代理签名

$$\left(m^*,\eta^*,u^*,\mathcal{OR},\mathcal{PR},\bigcup_{1\le i\le n_1}(m_{\omega_i};e_{p_{i,1}},\cdots,e_{p_{i,n_2}};x_i^1,\cdots,x_i^{n_2};v_i)\right)$$

则有 $u^*=G(\Gamma_{\eta^*-1}\oplus G(\Gamma_{\eta^*-2}\oplus\cdots G(\Gamma_{\eta^*}\oplus u^*)\cdots))$，其中对 $i=1,2,\cdots,n_1$，有 $\Gamma_i=z_i\oplus v_i$，$z_i=C_{v_i,m}(y_i^1,\cdots,y_i^{n_2})$，$y_i^j=g_i^j(x_i^j)(j=1,\cdots,2,n_2)$。如果存在某个 $j_0\in\{1,2,\cdots,n_2\}$ 使得 $y_0=g_{i_0}^{j_0}(x_{i_0}^{j_0})$，则 $\mathcal{B}$ 输出 $x_{i_0}^{j_0}$；否则，输出“失败”。

下面分析 $\mathcal{B}$ 成功的概率。考虑对 G 提出的询问，在签名过程中要形成环则必存在序号 s，使得询问 $G(u_s\oplus\Gamma_s)$ 发生在询问 $G(u_{s-1}\oplus\Gamma_{s-1})$ 之前[19]，这两次询问分别是第 g_0，g_0' 次询问的概率不小于 $1/q_G^2$。

同理，在对 H 提出的询问中，必存在序号 t^* 和 s^*，使得询问 $H(m,w_{t^*}\oplus y_{s^*}^{t^*})$ 发生在询问 $H(m,w_{t^*-1}\oplus y_{s^*}^{t^*-1})$ 之前，这两次询问分别是第 h_0，h_0' 次询问的概率不小于 $1/q_H^2$，且 $s^*=s$，$t^*=i_0$ 的概率分别不小于 $1/n_1$，$1/n_2$。由此可以看出，$\mathcal{B}$ 能以不小于 $\varepsilon/(q_G^2q_H^2n_1n_2)$ 的概率求解某一 RSA 扩展函数关于某给定值 y_0 的逆。

5　结束语

代理环签名是将代理签名和环签名相结合产生的一种新的签名。已有的代理环签名方案都是利用环签名的思想实现代理签名身份保密，但原始签名人的身份却是公开的。本文基于 RSA 问题的难解性提出了一个代理环签名方案，在保证代理签名人身份匿名性的同时，还能保证原始签名人的身份匿名性，任何人都无法从代理签名确定原始签名人或代理签名人的身份。

参 考 文 献

[1] Mambo M, Usuda K, and Okamoto E. Proxy signature for delegating signing operation [C]. Proceedings of the 3rd ACM Conference on Computer and Communication Security. ACM Press, 1996: 48–57.

[2] Rivest R, Shamir A, and Tauman Y. How to leak a secret [C]. Advance in ASIACRYPT 2001, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2001, 2248: 552–565.

[3] Zhang F G, Reihaneh S N, and Lin C Y. New proxy signature,

proxy blind signature and proxy ring signature scheme from bilinear pairings [EB/OL]. http://eprint.iacr.org/2003/104, 2005. 4.

[4] Lin C Y and Wu T C. An identity based signature scheme from bilinear pairing [EB/OL]. http://eprint.iacr.org/2003/117, 2005.4.

[5] Awasthi A K and Lal S. ID-based ring signature and proxy ring signature scheme from bilinear pairings [EB/OL]. http://eprint.iacr.org/2004/184, 2005.4.

[6] Chow S S M and Yap W S. Certificateless ring signature [EB/OL]. http://eprint.iacr.org/2007/236, 2007.9.

[7] Chu C K and Tzeng W G. Identity-committable signatures and their extension to group-oriented ring signatures [EB/OL]. http://eprint.iacr.org/2007/354, 2007.9.

[8] 张国印, 王玲玲, 马春光. 环签名研究进展[J]. 通信学报, 2007, 28(5): 109–117.
Zhang G Y, Wang L L, and Ma C G. Survey on ring signature [J]. *Journal on Communications*, 2007, 28(5): 109–117.

[9] 禹勇, 杨波, 李发根等. 一个有效的代理环签名方案[J]. 北京邮电大学学报，2007, 30(3): 23–26.
Yu Y, Yang B, and Li F G, *et al*.. An efficient proxy ring signature scheme [J]. *Journal of Beijing University of Posts and Telecommunication*, 2007, 30(3): 23–26.

[10] Wang C H and Liu C Y. A new ring signature scheme with signer-admission property [J]. *Information Sciences*, 2007, 177(3): 747–754.

[11] Chow S S M, Hui L C K, and Yiu S M. Identity based threshold ring signature [C]. In Proceedings of the 7th International Conference on Information Security and Cryptology 2004, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2005, 3506: 218–232.

[12] Jakimoska K M, Jakimoski G, and Burmester M. Threshold ring signatures efficient for large sets of signers [EB/OL]. http://eprint.iacr.org/2005/227, 2006.10.

[13] Au M H, Liu J K, and Yuen Y H, *et al*.. ID-based ring signature scheme secure in the standard model [EB/OL]. http://eprint.iacr.org/2006/205, 2006.10.

[14] Liu J K, Wei V K, and Wong D S. Linkable spontaneous anonymous group signature for Ad hoc groups [C]. Australian Conference on Information Security and Privacy 2004, Lecture Notes in Computer Science 2004, Berlin: Springer-Verlag, 3108: 325–335.

[15] Tsang P P, Wei V K, and Chan T K, *et al*.. Separable linkable threshold ring signature [EB/OL]. http://eprint.iacr.org/2004/267, 2006.10.

[16] Zhang M M, Chen G L, and Li J H. ID-based ring signature for RSA scenario [C]. Advance in Cryptography — CHINACRYPT'2006, Jinan Shandong, Oct, 2006: 142–154.

[17] Alfred J M, Oorschot P C and Vanstone S A 著胡磊, 王鹏等译. 应用密码学手册[M]. 北京: 电子工业出版社, 2005, 98.

[18] Bellare M and Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols [C]. In Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM Press, 1993: 62–73.

[19] Bresson E, Stern J, and Szydlo M. Threshold ring signatures and applications to ad-Hoc groups (Extended abstract)[C]. Advance in Cryptology- Proceedings of CRYPTO'02, Lecture Notes in Computer Science, Berlin: Springer-Verlag, 2002, 2442: 465–480.

鲍皖苏： 男，1966 年生，教授，博士生导师，研究方向为信息安全与密码理论等.

隗 云： 女，1982 年生，博士生，研究方向为密码理论、数学签名.

钟普查： 男，1982 年生，硕士生，研究方向为密码理论.