第37卷 第17期 计 算 机 工 程 2011年9月
Vol.37 No.17 Computer Engineering September 2011

·安全技术· 文章编号：1000—3428(2011)17—0090—03 文献标识码：A 中图分类号：TP309

# 一种基于身份的高效代理环签名方案

张俊茸，任平安

(陕西师范大学计算机科学学院，西安 710062)

**摘 要**：结合代理签名和环签名方案的优点，以双线性对为基础，提出一种新的基于身份的代理环签名方案，并证明其满足代理环签名方案的所有安全性要求，即可区分性、不可伪造性、无条件匿名性、不可否认性和可验证性。与现有方案的效率相比，新方案中计算消耗最大的双线性对运算开销从 $O(n)$降到了 $O(1)$，效率得到提高。

**关键词**：环签名；代理签名；代理环签名；双线性对；安全性

# Efficient ID-based Proxy Ring Signature Scheme

ZHANG Jun-rong, REN Ping-an

(College of Computer Science, Shaanxi Normal University, Xi'an 710062, China)

**【Abstract】** Combining the advantages of proxy signature and ring signature, this paper proposes a new efficient ID-based proxy ring signature scheme based on bilinear pairings, and proves that it satisfies the security requirements of a proxy ring signature scheme, which contains distinguishability, unforgeability, unconditional ambiguity, undeniability and verifiability. At the same time, comparing with validity of the existing schemes, the computational cost of bilinear pairings which is the biggest is reduced from $O(n)$ to $O(1)$, the computational efficiency of the new scheme is obviously improved.

**【Key words】** ring signature; proxy signature; proxy ring signature; bilinear pairings; security

**DOI:** 10.3969/j.issn.1000-3428.2011.17.029

## 1 概述

代理签名[1]是1996年由Mambo提出的一种特殊的数字签名。在一个签名方案中，原始签名人将他的签名权授权给代理签名人，代理签名人接受授权后代表原始签名人生成的有效签名称为代理签名。

环签名[2-3]的概念是2001年由Rivest R L、Shamir A和Tauman F提出的，它是一种只有用户没有管理者的简化的类群签名，任何一个环中成员都可以代表整个环签名，而验证者并不知道谁是真正的签名者，只知道签名来自这个环。任何环中用户都可以用自己的私钥和其他环成员的公钥进行签名而不需要经过他们的同意，其他的环成员可能并不知道他们的公钥已被其他人(真实签名者)用于签名。所以，环签名对真实签名者来说是匿名的，它是一种以匿名方式透露可靠消息的好方法。代理环签名[4]的思想最早是为满足代理人代替原始签名者进行签名同时又能保护自己匿名性而提出的，它将代理签名和环签名的功能特点结合起来，广泛应用于保护代理签名者的隐私问题。

现有的代理环签名方案或多或少都有缺陷，主要有2点：(1)效率不高，如文献[5]方案(需要太多双线性对运算)；(2)不能满足代理环签名方案的安全需要，如文献[6]方案(代理密钥生成时运算域不合理)。因此，本文提出一个基于身份和双线性对的高效且安全的代理环签名方案PRS，该方案满足代理环签名方案的安全要求，很好地保护了代理签名者的利益，可以广泛用于泄露隐私信息、电子投票、电子现金和认证通信等场合。与其他方案相比，新方案明显降低了计算量。

## 2 双线性对的相关知识

双线性对是2个循环群之间相对应的线性映像关系。由于椭圆曲线上所有点形成的集合在代数几何学上会形成群的关系，因此双线性配对函数的运算能应用于椭圆曲线上。目前，在密码学中广泛应用的双线性对还只能由椭圆曲线上的Weil对或Tate对推导出来。

### 2.1 双线性对定义

设阶为素数 $q$ 的 $G_1$ 是由 $P$ 生成的加法群，阶为 $q$ 的 $G_2$ 是乘法群，双线性对是映射：$e:G_1\times G_1\to G_2$，其中，在 $G_1$ 和 $G_2$ 中求解离散对数是困难性问题。

### 2.2 双线性对性质

(1)双线性：设 $P,Q,R\in G_1$，则有：

$e(aP,bQ)=e(P,Q)^{ab}=e(abP,Q)=e(P,abQ)$，其中，$a,b\in Z_q$

$e(P,Q+R)=e(P,Q)e(P,R)$

$e(P+Q,R)=e(P,R)e(Q,R)$

(2)非退化性：$\exists P,Q\in G_1$，使 $e(P,Q)\neq 1$。

(3)可计算性：存在有效算法计算 $e(P,Q)$，其中，$P,Q\in G_1$。

### 2.3 与双线性对有关的数学问题

在对该方案进行安全性分析之前，先给出与双线性对有关的3个数学问题：

(1)离散对数问题(Discrete Logarithm Problem, DLP)：给定 $P,Q\in G_1$，寻找 $n\in Z_q^*$，使 $Q=nP$。

(2)计算性Diffie-Hellman问题(Computational Diffie-Hellman Problem, CDHP)：设 $P\in G_1$，$a,b\in Z_q^*$，已知 $P$、$aP$、$bP$，计算 $abP$。

(3)双线性对Diffie-Hellman问题(Double-linear Diffie-Hellman Problem, BDHP)：设 $P\in G_1$，$a,b,c\in Z_q^*$，已知 $P$、

**作者简介**：张俊茸(1984－)，女，硕士研究生，主研方向：代理签名，网络与信息安全；任平安，副教授、博士

**收稿日期**：2011-02-16 **E-mail**：zhangjunrong0502@163.com

$aP$、$bP$，$cP$，计算 $e(P,P)^{abc}$ 。

## 3 代理环签名的预备知识

代理环签名方案一般包括 4 个参与方：密钥生成中心(Key Generation Center, KGC)，授权人(原始签名者)，代理人(真实签名者)和验证者。

### 3.1 代理环签名产生步骤

代理环签名方案是包含以下 4 个步骤的数字签名方案：

(1)系统创建：一个用于产生授权人密钥对、代理人密钥对和系统参数的多项式时间概率算法。

(2)代理密钥产生：用于产生代理签名密钥对的算法。

(3)签名生成：一个概率算法，当输入待签消息、系统参数、身份集合和真实签名者的代理签名私钥后，输出对该消息的签名。

(4)签名验证：一个输入对消息的签名、系统参数和身份集合后确定签名是否有效的算法。

### 3.2 代理环签名的安全性需求

代理环签名在安全性方面有 5 点要求。

(1)可区分性：代理环签名区别于代理者一般的环签名。

(2)不可伪造性：一个授权的代理签名者可以产生一个合法的代理环签名，但是原始签名者和第三方不能产生一个合法的代理环签名。

(3)无条件匿名性：攻击者甚至原始签名者不知道谁是真正的代理环签名者。

(4)不可否认性：代理签名者一旦生成一个合法的环签名，就不能再否认。

(5)可验证性：任何人都可以从代理环签名中验证签名的正确性。

## 4 新的代理环签名方案 PRS

设 $G_1$ 是由 $P$ 生成的加法群，它的阶为素数 $q$；$G_2$ 是乘法群，阶为 $q$；映射 $e:G_1\times G_1\to G_2$ 是双线性对。有 2 个安全哈希函数：$H_1$，$H_2$，其中，$H_1:\{0,1\}^*\to G_1$；$H_2:\{0,1\}^*\to Z_q^*$。

(1)系统参数生成阶段

1)KGC 随机选择秘密参数 $x\in_R Z_q^*$，并将其作为系统主密钥，$P_{\text{pub}}=xp$ 为对应的系统公钥，然后公布系统参数 $params=\{G_1, G_2, H_1, H_2, P, P_{\text{pub}}, q, e\}$。

2)每个身份为 $ID\in\{0,1\}^*$ 的环成员可以通过计算 $Q_{ID}=H_1(ID)\in G_1$ 生成公钥 $Q_{ID}$。为了得到对应私钥，环成员向 KGC 提交个人身份，KGC 计算对应私钥 $S_{ID}=xQ_{ID}$，并将私钥安全发送给该成员。在该方案中，原始签名者的公私钥为 $Q_{ID_0}$、$S_{ID_0}$，代理签名者的公私钥为 $Q_{ID_s}$、$S_{ID_s}$，身份为 $ID_i$ 的环成员的公私钥为 $Q_{ID_i}$、$S_{ID_i}$。

(2)生成代理密钥阶段

1)原始签名人生成委托状 $\omega$，$\omega$ 记录了将原始签名权利委托给代理签名人的相关信息，如授权期限和范围。

2)原始签名人计算出 $S_\omega=S_{ID_0}H_2(\omega)$ 后，将 $\omega$ 和 $S_\omega$ 的值发送给代理签名人。

3)代理签名人验证 $e(S_\omega,P)=e(H_2(\omega)Q_{ID_0},P_{\text{pub}})$，如果不成立，则拒绝委托代理，否则，代理签名人计算 $S_{pi}=S_\omega+S_{ID_i}H_2(\omega)(i=1,2,\cdots,n)$，$S_{pi}$ 为代理签名私钥。

(3)生成签名阶段

对于 $L=\{ID_1,ID_2,\cdots,ID_n\}$，$L$ 为 $n$ 个环成员身份的集合，序号 $t$ 为真实代理签名人，其公私钥为 $Q_{ID_t}$、$S_{ID_t}$，代理签名私钥为 $S_{pt}$。

1)对于消息 $m$，首先随机选择 $r_i\in_R Z_q^*$，计算 $A_i=r_iP$，$h_i=H_2(m\|L\|A_i)$(其中，$i=1,2,\cdots,n$ 且 $i\neq t$)，如果 $A_i$ 中有相等的，则重新选择 $r_i$。

2)随机选择 $r_t\in_R Z_q^*$ 并计算 $A_t=r_tP-\sum_{i\neq t}h_iH_2(\omega)Q_{ID_i}$(如果 $A_t$ 与 $A_i$ 相同，则重新选择 $r_t$)、$h_t=H_2(m\|L\|A_t)$ 和 $V=(\sum_{i=1}^{n}r_i)P_{\text{pub}}+h_tS_{pt}$ 的值。

3)计算 $Z=h_tH_2(\omega)Q_{ID_0}$。

4)得到签名 $\sigma=(m,A_1,A_2,\cdots A_n,V,Z)$。

(4)验证签名阶段

1)计算 $h_i=H_2(m\|L\|A_i)(i=1,2,\cdots,n)$。

2)检查等式 $e(P_{\text{pub}},\sum_{i=1}^{n}A_i+\sum_{i=1}^{n}h_iH_2(\omega)Q_{ID_i}+Z)=e(P,V)$ 是否成立，如成立，该签名是合法正确的，否则，该签名是非法的。

## 5 PRS 方案安全性分析

下面从代理环签名安全性需要满足的若干方面证明 PRS 方案的安全性。

**定理 1** PRS 方案是正确的。

证明：如果代理签名人对消息 $m$ 的签名为 $\sigma=(m,A_1,A_2,\cdots,A_n,V,Z)$，则有：

$$e(P_{\text{pub}},\sum_{i=1}^{n}A_i+\sum_{i=1}^{n}h_iH_2(\omega)Q_{ID_i}+Z)=$$

$$e(P_{\text{pub}},\sum_{\substack{i=1\\i\neq t}}^{n}A_i+r_tP-\sum_{\substack{i=1\\i\neq t}}^{n}h_iH_2(\omega)Q_{ID_i}+$$

$$\sum_{\substack{i=1\\i\neq t}}^{n}h_iH_2(\omega)Q_{ID_i}+H_2(\omega)h_tQ_{ID_t}+Z)=$$

$$e(P_{\text{pub}},(\sum_{\substack{i=1\\i\neq t}}^{n}r_i+r_t)P+h_t(H_2(\omega)Q_{ID_t}+H_2(\omega)Q_{ID_O}))=$$

$$e(P,(\sum_{\substack{i=1\\i\neq t}}^{n}r_i+r_t)xP+h_t(H_2(\omega)xQ_{ID_t}+H_2(\omega)xQ_{ID_O}))=$$

$$e(P,(\sum_{\substack{i=1\\i\neq t}}^{n}r_i+r_t)P_{\text{pub}}+h_t(H_2(\omega)S_{ID_t}+H_2(\omega)S_{ID_O}))=$$

$$e(P,(\sum_{i=1}^{n}r_i)P_{\text{pub}}+h_tS_{pt})=e(P,V)$$

因此，PRS 方案是正确的。

**定理 2** PRS 方案满足代理环签名安全性需要的可区分性。

证明：

代理环签名不同于其他一般的环签名，它们是比较容易区分的，因为代理密钥 $S_{pi}$ 中包含了原始签名者的信息，代理签名人的代理密钥 $S_{pi}$ 与普通 KGC 分发的私钥 $S_{ID_i}$ 是不同的，所以 PRS 方案满足可区分性。

**定理 3** PRS 方案满足代理环签名安全性需要的不可伪造性。

证明：

(1)原始签名人的密钥是安全的：因为攻击人或代理签名人由 $S_{ID_0}H_2(\omega)$ 得出 $S_{ID_0}$ 是 $G_1$ 上的一个离散对数难题。

(2)不可能伪造代理签名人的代理密钥：因为代理密钥 $S_{pi}=S_\omega+S_{ID_i}H_2(\omega)$ 是 2 个签名之和，所以要解出 $S_{pi}$ 就需知

道 $S_{ID_0}$ 和 $S_{ID_i}$，而用 $S_\omega$ 和 $S_{ID_i}H_2(\omega)$ 求 $S_{ID_0}$ 和 $S_{ID_i}$ 是 $G_1$ 上的一个离散对数难题。

(3)不可能伪造签名：即使攻击者可以随机选择 $r_i$，计算出 $A_i$ ($i \neq t$)，也不能伪造 $V$，因为计算 $V$ 需要代理密钥 $S_{pi}$，而由(2)可知 $S_{pi}$ 是安全的；另外，也不能伪造签名 $\sigma$，令其满足签名验证等式，因为这是一个计算性 Diffie-Hellman 问题。

综上所述，PRS 方案满足不可伪造性。

**定理 4** PRS 方案满足代理环签名安全性需要的无条件匿名性。

证明：在一个合法的签名 $\sigma$ 中，因为 $r_i$ 是随机选择的，所以由 $r_i$ 计算出的 $A_i$ 在 $G_1$ 上分布均匀，而 $A_t$ 由 $r_t$ 计算得到，$r_t$ 也是随机选择的，所以 $A_t$ 也在 $G_1$ 上分布均匀，由签名 $\sigma$ 猜出代理签名人的概率不会高于 $1/n$；另外，$V$ 中含有随机选择的 $r_i$ 和 $r_t$，真实签名人的身份不会被泄露，因此，PRS 方案满足无条件匿名性。

**定理 5** PRS 方案满足代理环签名安全性需要的不可否认性。

证明：由于代理签名密钥 $S_{pi}$ 中包含代理签名人的身份信息，一旦真正的代理签名人生成一个合法签名，就不能对授权人否认由他生成的此有效的代理环签名，因此 PRS 方案满足不可否认性。

**定理 6** PRS 方案满足代理环签名安全性需要的可验证性。

证明：由 5.1 节可知，环中任何成员都可以验证签名是否正确。

## 6 PRS 方案效率分析

在讨论 PRS 方案的计算效率时，仅考虑一些计算消耗比较大的操作，主要是双线性对配对运算 Paring、群 $G_1$ 中的加法运算 $G_1$ add、群 $G_1$ 中的数乘运算 $G_1$ mul 和群 $G_2$ 中的数乘运算 $G_2$ mul，与文献[4]和文献[5]方案的比较，结果如表 1 所示，其中，$n$ 代表代理签名人选定的代理子集合中的代理人个数。表 1 只给出了计算和验证 1 个代理环签名所需要的运算量。从表中可以得出，PRS 方案的 $G_1$ add 和 $G_1$ mul 的计算复杂度与文献[4]方案和文献[5]方案相同，都是 $O(n)$，但是文献[4]方案和文献[5]方案中计算消耗最大的 Paring 运算的计算复杂度都是 $O(n)$，而 PRS 方案中只需要 2 次 Paring 运算，计算复杂度降到了 $O(1)$，计算效率更高。

**表 1 3 种方案效率比较**

| 方案 | $G_1$ add | $G_1$ mul | $G_2$ mul | Paring |
|---|---|---|---|---|
| 文献[4]方案 | $2n$ | $2n$ | $n$-1 | $4n$-1 |
| 文献[5]方案 | $5n$-1 | $3n$-1 | 2 | $n$+2 |
| PRS 方案 | $3n$ | $3n$+2 | 0 | 2 |

## 7 结束语

本文提出了一种基于身份的有效的代理环签名方案 PRS，该方案以双线性对为基础，结合了代理签名和环签名的优点，满足代理环签名的安全性需求，与文献[6]方案相比，PRS 方案的安全性更高；与文献[4]方案和文献[5]方案相比，PRS 方案具有更高的计算效率。

## 参考文献


[1] Mambo M, Usuda K, Okamoto E. Proxy Signatures for Delegating Signing Operation[C]//Proc. of the 3rd ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 1996: 48-57.

[2] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[C]//Proc. of Conf. on Advances in Croptology. New York, USA: Springer-Verlag, 2001: 552-565.

[3] 罗大文，何明星，李 娓. 无证书的可验证环签名方案[J]. 计算机工程, 2009, 35(15): 135-137.

[4] Zhang Feng, Naini R S, Lin Chih-Yin. New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Scheme from Bilinear Pairings[EB/OL]. (2003-10-04). http://eprint.iacr.org/2003/104/.

[5] Amit K, Sunder L. ID-based Ring Signature and Proxy Ring Signature Schemes Form Bilinear Pairings[J]. Internal Journal of Network Security, 2007, 4(2): 187-192.

[6] 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.


编辑 张正兴

(上接第 77 页)

## 参考文献


[1] Floyd S, Jacobson V. Random Early Detection Gateways for Congestion Control[J]. IEEE/ACM Trans. on Networking, 1993, 1(4): 397-413.

[2] Tan Xianhai, Huang Yuanhui. Parameters Setting Scheme of RED with Long-range Dependent Traffic Input[C]//Proc. of the 5th International Conference on Wireless Communications, Networking and Mobile Computing. Piscataway, USA: IEEE Press, 2009.

[3] Ohsaki H, Murata M. Steady State Analysis of the RED Gateway: Stability, Transient Behavior, and Parameter Setting[J]. IEICE Trans. on Communications, 2002, 85(1): 107-115.

[4] Seok W, Kiseon K. Parameter Setting and 2-D Stability Conditions for TCP/RED Networks[C]//Proc. of Global Telecommunications Conference. [S. l.]: IEEE Press, 2009.

[5] 孙丽珺，王立宏，逯昭义. 基于多优先级的动态阈值 RED 算法[J]. 计算机工程, 2008, 34(9): 115-118.

[6] Padhye J, Firoiu V. Modeling TCP Reno Performance: A Simple Model and Its Empirical Validation[J]. IEEE/ACM Trans. on Networking, 2000, 8(2): 133-145.

[7] Abouzeid A, Roy S. Analytic Understanding of Red Gateways with Multiple Competing TCP Flows[C]//Proc. of IEEE Global Telecommunication Conference. San Francisco, USA: IEEE Press, 2000.

[8] 林 闯，单志广，任丰原. 计算机网络的服务质量[M]. 北京：清华大学出版社, 2004.


编辑 顾逸斐