两种环签名方案的安全性分析及其改进

王化群[①②] 张力军[①] 赵君喜[③]
[①](南京邮电学院信息工程系 南京 210003)
[②](大连水产学院信息工程学院 大连 116023)
[③](南京邮电学院应用数理系 南京 210003)

摘 要：通过对 Xu(2004)和 Zhang(2004)提出的两种环签名方案进行分析，指出了这两种环签名方案都容易受到群成员改变攻击(group-changing attack)，并给出了攻击方法；另外，Zhang 的方案还容易受到多已知签名存在伪造(multiple-known-signature existential forgery)攻击。为防范这两种攻击，对这两种环签名方案进行了改进，改进后的方案在最强的安全模型(Joseph, 2004 提出)中仍是安全的。

关键词：环签名；双线性对；伪造攻击；GDP(Gap Diffie-Hellman)
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2007)01-0201-04

Cryptanalysis and Improvement of Two Ring Signature Schemes

Wang Hua-qun[①②] Zhang Li-jun[①] Zhao Jun-xi[③]
[①](*Department of Information Engineering*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)
[②](*Information Engineering Institute*, *Dalian Fisheries University, Dalian 116023*, *China*)
[③](*Department of Applied Mathematics and Physics*, *Nanjing University of Posts and Telecommunications*, *Nanjing* 210003, *China*)

Abstract: The security of the two ring signature schemes proposed by Xu(2004) and Zhang(2004) is analyzed, and it's found that both the ring signature schemes are susceptible to group-changing attack. In addition, Zhang's scheme can easily be attacked by multiple-known-signature existential forgery. To guard against the two attacks, the two ring signature schemes are improved, which can make the improved schemes is still secure even in the strongest security model (proposed by Joseph in 2004).

Key words: Ring signature; Bilinear pairings; Forgery attack; GDP (Gap Diffie-Hellman)

1 引言

2001年，Rivest，Shamir和Tauman在文献[1]中首次正式提出了环签名的概念，并且利用组合函数和对称密码体制给出了一种高效的环签名方案。环签名提出以后引起了广泛的关注，并提出了各种环签名方案[2-9]，也有的利用环签名的思想提出了新的签名类型[10]。环签名是一种新的匿名签名技术，因签名中参数根据一定的规则首尾相接组成环状而得名。环签名可以实现无条件匿名，即使攻击者拥有无限的计算能力，也无法追踪签名人的身份。环签名的这种无条件匿名性在对信息需要长期保护的一些特殊环境中非常有用，例如，即使RSA被攻破也须保护匿名的场合。对于环签名的存在不可伪造性分析，存在3种强度不同的安全模型[1,3,4]。对于环签名方案，可在不同的安全模型下进行分析。

最近，双线性对被广泛应用在各种密码方案的设计中，也设计出了许多环签名方案[2,5-9]。由于双线性对在密码学应用中具有良好的性质，所以最近得到广泛的关注。本文在3种不同安全模型中分析了文献[2]中的环签名方案，并利用双线性对的性质，指出了其存在的安全缺陷，然后对其进行了改进，弥补了这些安全缺陷。

本文第2节主要介绍了双线性对和环签名的基本概念，并给出了环签名的3种强度不同的安全模型；第3节简要介绍了文献[2]提出的环签名方案，针对该方案提出了群成员改变攻击，为防止这种攻击，提出了一种改进方案，使得改进的方案即使在最强的安全模型中也是存在不可伪造的；第4节简要介绍了文献[9]提出的环签名方案，针对该方案提出了两种攻击方法：群成员改变攻击和多已知签名存在伪造攻击。为防止这两种攻击，提出了两种改进方案，分别在Model2中和Model3中是安全的；第5节为结束语。

2 双线性对、环签名和安全模型

设 G 为一生成元为 P 的加法循环群，V 为乘法循环群，其阶都为素数 q。群 G，V 中的离散对数问题都是困难的。定义双线性对 $e:G\times G\to V$，e 满足如下条件：

(1) 双线性性 $e(aP,bQ)=e(P,Q)^{ab}$，其中 $P,Q\in G$，$a,b\in Z_q^*$。

(2) 非退化性 存在 $P,Q\in G$，满足 $e(P,Q)\neq 1$，其中 1 为循环乘法群 V 的幺元。

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

2005-05-23 收到，2006-03-02 改回
国家自然科学基金重点项目(60432040)资助课题

群 G 可取有限域上超奇异椭圆曲线或超椭圆曲线，双线性对可利用该曲线上的 Weil 配对或 Tate 配对改进后进行实现。

假设 G 为一加法群，在群 G 上定义以下密码学问题：

(1)离散对数问题(DLP) 任取 $Q\in G$，求满足 $Q=nP$ 的 $n\in Z_q^*$。

(2)计算 Diffie-Hellman 问题(CDHP) $\forall(P,aP,bP)\in G^3$，其中 $a,b\in Z_q^*$，求出 abP。

(3)决策 Diffie-Hellman 问题(DDHP) $\forall(P,aP,bP,cP)\in G^4$，其中 $a,b,c\in Z_q^*$，判断 $ab\equiv c \bmod q$ 是否成立。

(4)Gap Diffie-Hellman(GDH)问题 一类 CDHP 困难而 DDHP 容易的问题。

(5)q-Strong Diffie-Hellman(q-SDH)问题 $\forall(P,xP,x^2P,\cdots,x^qP)\in G^{q+1}$，求出一对 $(c,(1/(x+c))P)$，其中 $c\in Z_q$。

(6)k-CAA(Collusion Attack Algorithm with k traitors)问题 对于整数 k 和 $x\in_R Z_q$，$P\in G$，给出 $\{P,Q=xP,h_1,h_2,\cdots,h_k\in Z_q,(1/(h_1+x))P,(1/(h_2+x))P,\cdots,(1/(h_k+x))P\}$，输出 $\left(1/(h+x)\right)P,h\notin\{h_1,h_2,\cdots,h_k\}$。

假设DLP问题,CDHP问题，q-SDH问题和k-CAA问题是困难的，即不存在概率多项式时间算法以不可忽略的概率求解DLP问题，CDHP问题，q-SDH问题和k-CAA问题。群 G 的选取可满足DLP问题，CDHP问题难解，而DDHP问题易解的条件，即群 G 为GDH群。在GDH群中，假设q-SDH问题，k-CAA问题是困难的。

在一个环签名可能签名者的集合中，其中实际签名的环成员为签名者，其它的环成员为非签名者。签名者能够使得确认者相信消息的签名者为这个环中的一个成员，但该成员能够保持无条件匿名性，即攻击者即便非法获取了所有可能的签名者的私钥,他能确定出真正的签名者的概率不超过 $1/n$，这里 n 为环成员(可能的签名者) 的个数。环签名还有另外一个特征，即签名者可以在 n 个用户中自由地任意选取 $r>1$ 个用户(包括自己)产生一个环签名，也就是说，签名者可以指定自己的匿名范围，并且被指定的用户可能不知道自己被包含在其中。

对于环签名的不可伪造性，文献[1,3,4]提出了不同的模型，下面简要介绍一下：

一个环签名方案由一个三元算法组 (I,S,V) 组成，其中各自的作用如下：

$(x,u)\leftarrow I(1^k)$ 是一个概率多项式时间算法，k 为安全参数，输出 x 为私钥，u 为相应的公钥；$\sigma\leftarrow S(1^k,x,L,m)$ 是一个概率多项式时间算法，输入 k 为安全参数，x 为私钥，L 为 n 个环签名成员公钥的集合，其中含有实际签名者的公钥，m 为要求签名的消息，输出 σ 为签名；$1/0\leftarrow V(1^k,L,m,\sigma)$ 为确定的多项式时间算法,输入符号的含义跟前两个算法相同，输出 1 或 0 表示接受或拒绝，并要求 $V(1^k,L,m,S(1^k,x,L,m))=1$。为简化起见，本文其余部分将输入中的安全参数 1^k 省略。

环签名的 3 种不同的不可伪造性安全模型：设 S 为签名者，A 为攻击者。S 利用 I 产生一个大的公钥集合 $L=\{u_1,u_2,\cdots,u_N\}$，其中 N 为 k 的某个多项式。A 向 S 请求至多 k 的多项式次消息 m_i 关于 L_i 的环签名请求，在得到响应 (L_i,m_i,σ_i) 后，A 不能以不可忽略的概率产生消息 m 的环签名 (L',m,σ) ($L'\subseteq L$, $A\notin L'$, $m\notin\{$已请求环签名的消息$m_i\}$)，称该方案在安全模型Model1[1]中是安全的；当 A 不能以不可忽略的概率产生任一消息 m 的环签名 (L',m,σ) ($L'\subseteq L$, $(L',m)\notin\{$已请求环签名的消息、成员组对$(L_i,m_i)\}$)时，称该方案在安全模型Model2[4]中是安全的；当 A 不能以不可忽略的概率产生任一消息 m 的环签名 (L',m,σ) ($L'\subseteq L$, $(L',m,\sigma)\notin\{$已请求环签名的消息、成员组、签名对$(L_i,m_i,\sigma)\}$)时，称该方案在安全模型Model3[3]中是安全的。

容易看到，Model1，Model2 和 Model3 的安全性要求依次增强。Model1 没有考虑群改变,多已知签名存在伪造攻击；Model2 考虑了群成员改变攻击，没考虑多已知签名存在伪造攻击；Model3 考虑了这两种攻击。文献[2, 9]中所提出的环签名方案都是在 Model1 模型中考虑其安全性的。

3 文献[2]中的环签名方案及其安全性分析和改进

文献[2]给出了一种环签名方案，下面简要介绍一下：

设系统参数为 $\text{param}=\{G,V,P,q,e\}$，其中的符号含义跟第 2 节相同。

密钥产生 I 随机产生 $x_s,y_s\in_R Z_q{}^*$，计算 $u_s=x_sP$, $v_s=y_sP$。成员 U_s 的私钥为 (x_s,y_s)，公钥为 (u_s,v_s)。

环签名产生 成员 U_s 随机选取公钥集合，不妨设为 $L=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n)\}$，消息 $m\in Z_q{}^*$，其中 $(u_s,v_s)\in L$。随机选取 $r\in_R Z_q{}^*,\alpha_i\in_R Z_q{}^*$，$i=1,2,\cdots,s-1,s+1,\cdots,n$，计算 $\sigma_i=\alpha_iP$，$i\neq s$，$\sigma_s=\dfrac{1}{m+x_s+y_sr}\left(P-\sum_{i\neq s}\alpha_i(mP+u_i+rv_i)\right)$。当 $m+x_s+y_sr\equiv 0 \bmod q$ 时，重新选择一个不同的随机数 $r\in_R Z_q{}^*$，使得 $m+x_s+y_sr\neq 0 \bmod q$。输出环签名 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n,r)$，$L=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n)\}$ 及消息 m。

环签名确认 当接收到环签名 (L,m,σ) 后，确认式子 $\prod_{i=1}^{n}e(mP+u_i+rv_i,\sigma_i)=e(P,P)$ 是否成立；如果成立，输出 1，接受；否则，输出 0，拒绝。

环签名方案在Model1 中是存在不可伪造的 当 $n=1$ 时，该方案实际就是Boneh[11]提出的短签名方案，该短签名方案基于q-SDH假设在Model1 中是存在不可伪造的。文献[2]中所提环签名方案的不可伪造性证明类似于文献[11]中的证明方法[2]。

但是，这个方案在 Model2 中存在群成员改变攻击：

设（$\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n,r)$，$L=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,$

$v_n)\}$, m)为 m 的环签名，伪造者 A 在未知任何成员私钥情况下，可以增加 U_{n+1} 进入成员集，但仍能够通过签名确认：

伪造者 A 任取 $t\in_R Z_q{}^*$，计算 $\sigma'_n=\sigma_n+t(mP+u_{n+1}+rv_{n+1})$，$\sigma'_{n+1}=-t(mP+u_n+rv_n)$，令 $\sigma'_i=\sigma_i$, $i=1,2,\cdots,n-1$，则消息 m 关于 $L=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n),(u_{n+1},v_{n+1})\}$ 的新签名为 $\sigma=(\sigma'_1,\sigma'_2,\cdots,\sigma'_n,\sigma'_{n+1},r)$，新签名能够通过确认。证明如下：

$$\begin{aligned}
&\prod_{i=1}^{n+1}e(mP+u_i+rv_i,\sigma'_i)\\
&=\left(\prod_{i=1}^{n-1}e(mP+u_i+rv_i,\sigma'_i)\right)e(mP+u_n+rv_n,\sigma'_n)\\
&\quad\cdot e(mP+u_{n+1}+rv_{n+1},\sigma'_{n+1})\\
&=\left(\prod_{i=1}^{n-1}e(mP+u_i+rv_i,\sigma'_i)\right)e(mP+u_n+rv_n,\sigma_n\\
&\quad+t(mP+u_{n+1}+rv_{n+1}))e(mP+u_{n+1}+rv_{n+1},\\
&\quad-t(mP+u_n+rv_n))\\
&=\left(\prod_{i=1}^{n-1}e(mP+u_i+rv_i,\sigma_i)\right)e(mP+u_n+rv_n,\sigma_n)\\
&\quad\cdot e(mP+u_n+rv_n,t(mP+u_{n+1}+rv_{n+1}))\\
&\quad\cdot e(mP+u_{n+1}+rv_{n+1},-t(mP+u_n+rv_n))\\
&=\prod_{i=1}^{n}e(mP+u_i+rv_i,\sigma_i)=e(P,P)
\end{aligned}$$

由于 Model3 是比 Model2 更强的安全模型，文献[2]中的方案在 Model2 中是存在伪造的，当然在 Model3 中也是存在伪造的。为防止这种攻击，对该环签名方案进行改进，令 $r=H(m,L,t)$，其中 $t\in_R Z_q$，即 t 为长度为 $|q|$ ($|q|$ 为 q 的二进制表示长度)的随机二进制串。这样，在每次产生新的签名时，随机选取新的 $t\in_R\{0,1\}^{|q|}$；当 $m+x_s+y_sr\equiv 0 \bmod q$ 时，重新选择 t，使得 $m+x_s+y_sr\neq 0 \bmod q$。环签名的产生同原方案类似，仅 r 取值时不同。这样就能防止群成员改变攻击，在 Model2 中是安全的。

与文献[2]中的方案相比较，改进后的方案将哈希函数作用于消息 m、成员集 L 和一个随机数 t 上，所得到的哈希值用作原方案中的随机值 r。原方案存在群成员改变攻击的原因就在于确认方程中，攻击者能够在保持一个环签名的随机值 r 不变的情况下，改变环成员的数目。改进后的方案使得 r 要随着 L 的改变而改变，这样就防止了这种攻击方式。由于原方案在 Model1 中是安全的，对于每次环签名，由于随机值 t 不同，因而哈希值也是随机的，其安全性证明跟原方案类似。如果成员集 $L=\{(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n)\}$ 变为 $L'\neq L$，由于 $r'=H(m,L',t)\neq H(m,L,t)$，对于上面给出的群成员改变攻击，则

$$\begin{aligned}
\prod_{i=1}^{n+1}e(mP+u_i+r'v_i,\sigma'_i)&=\prod_{i=1}^{n}e(mP+u_i+r'v_i,\sigma_i)\\
&\neq\prod_{i=1}^{n}e(mP+u_i+r'v_i,\sigma_i)=e(P,P)
\end{aligned}$$

从而防止了群成员改变攻击，在 Model2 中是安全的。由于 $e(mP+u_i+r'v_i,\sigma'_i),1\le i\le n$ 中的 $mP+u_i+r'v_i$, $1\le i\le n$ 在每次签名中都是不同的，无法从同一个消息的多个环签名产生新的环签名，因而也避免了文献[4]中提出的多已知签名存在伪造攻击，因而在 Model3 中也是安全的。

新方案的匿名性证明　假设 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n,t)$ 是签名者 U 关于成员集 L ($U\in L$) 和消息 m 的环签名，那么，对于任意算法 A，算法 A 能够输出签名者 U 的概率至多为 $1/|L|$，其中 $|L|$ 表示成员集 L 中的成员数。这是因为，在签名 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n,t)$ 中，除 σ_U 外，其余的 σ_i 都是随机从 G 中选取的，$\sigma_i=a_iP,a_i\in_R Z_q{}^*$，$\sigma_U$ 由 m,a_i,x_U,y_U,t 确定，但是在 a_i,x_U,y_U 保密的情况下，σ_U 并不能由 $(\sigma_1,\sigma_2,\cdots\sigma_{U-1},\sigma_{U-1},\cdots,\sigma_n,t)$ 计算出来，并且环签名过程也暗示了环签名满足 $\sum_{i=1}^{n}(m+x_i+ry_i)\sigma_i=P$。所以，$\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$ 共有 q^{n-1} 个可能的取值，每种可能取值都是等概率的。这就保证了环签名的匿名性。

4　文献[9]中的环签名方案及其安全性分析和改进

文献[9]给出了一种环签名方案，下面简要介绍一下，其中系统参数的符号含义跟第 2 节相同：

密钥产生　I 随机产生 $x_s\in_R Z_q{}^*$，计算 $u_s=x_sP$。成员 U_s 的私钥/公钥对为 (x_s,u_s)。

环签名产生　对于消息 $m\in Z_q{}^*$，成员 U_s 随机选取公钥集合 $L=\{u_1,u_2,\cdots,u_n\}$，其中 $u_s\in L$。随机选取 $\alpha_i\in_R Z_q{}^*$，$i=1,2,\cdots,s-1,s+1,\cdots,n$，计算 $\sigma_i=\alpha_iP$，$i\neq s$，$\sigma_s=-\frac{1}{H(m)+x_s}\sum_{i\neq s}(\alpha_i(H(m)P+u_i))+\frac{1}{H(m)+x_s}P$。输出消息 m 关于成员集 $L=\{u_1,u_2,\cdots,u_n\}$ 的环签名 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$。

环签名确认　当接收到环签名 (L,m,σ) 后，确认式子 $\prod_{i=1}^{n}e(H(m)P+u_i,\sigma_i)=e(P,P)$ 是否成立；如果成立，输出 1，接受；否则，输出 0，拒绝。

该方案的存在不可伪造安全模型为文献[1]中的安全模型，即Model1。在k-CAA问题困难性假设下，Zhang等人在随机预言模型中给出了确切的存在不可伪造性安全性证明[9]。但是，该方案在签名产生时，如果 $H(m)+x_s=0 \bmod q$，则签名失败；由于 H 的随机性，签名失败的概率很小，但即便如此，这个方案在Model2中存在群成员改变攻击：

设($\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$，$L=\{u_1,u_2,\cdots,u_n\}$，$m$)为 m 的环签名，伪造者 A 在未知任何成员私钥情况下，可以增加 U_{n+1} 进入成员集，但仍能够通过签名确认：

伪造者 A　任取 $t\in_R Z_q{}^*$，计算 $\sigma'_n=\sigma_n+t(H(m)P+u_{n+1})$，$\sigma'_{n+1}=-t(H(m)P+u_n)$，令 $\sigma'_i=\sigma_i,i\neq n$。这个新签名为 $\sigma=(\sigma'_1,\sigma'_2,\cdots,\sigma'_n,\sigma'_{n+1})$，$L=\{u_1,u_2,\cdots,u_n,u_{n+1}\}$，

m，新签名能够通过确认。能通过确认检测证明，证明过程类似于第 3 部分中群成员改变攻击的证明过程，容易得证。

在 Model3 中存在多已知签名存在伪造攻击：

设 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n)$，$\sigma'=(\sigma'_1,\sigma'_2,\cdots,\sigma'_n)$ 是消息 m 关于成员集 $L=\{u_1,u_2,\cdots,u_n\}$ 的两个环签名。因而，有

$$\prod_{i=1}^{n}e(H(m)P+u_i,\sigma_i)=e(P,P)$$

$$\prod_{i=1}^{n}e(H(m)P+u_i,\sigma'_i)=e(P,P)$$

任取 $a,b\in Z_q^*$，并且 $a+b\neq 0 \bmod q$，令 $\hat{\sigma}_i=\dfrac{a}{a+b}\sigma_i+\dfrac{b}{a+b}\sigma'_i,\quad i=1,2,\cdots,n$，则 $\hat{\sigma}=(\hat{\sigma}_1,\hat{\sigma}_2,\cdots,\hat{\sigma}_n)$ 也是消息 m 关于成员集 $L=\{u_1,u_2,\cdots,u_n\}$ 的环签名，即能通过确认过程，证明如下：

$$\begin{aligned}&\prod_{i=1}^{n}e(H(m)P+u_i,\hat{\sigma}_i)\\&=\left(\prod_{i=1}^{n}e\left(H(m)P+u_i,\frac{a}{a+b}\sigma_i\right)\right)\left(\prod_{i=1}^{n}e\left(H(m)P+u_i,\frac{b}{a+b}\sigma'_i\right)\right)\\&=\left(\prod_{i=1}^{n}e(H(m)P+u_i,\sigma_i)^{\frac{a}{a+b}}\right)\left(\prod_{i=1}^{n}e(H(m)P+u_i,\sigma'_i)^{\frac{b}{a+b}}\right)\\&=e(P,P)^{\frac{a}{a+b}}e(P,P)^{\frac{b}{a+b}}=e(P,P)\end{aligned}$$

为防止群成员改变攻击，令 $H(m)$ 变为 $H(m,L)$，H 为哈希函数；当 L 改变时，将导致 $H(m,L)$ 的改变，在不知道某一成员私钥的情况下，群成员改变攻击不能成功，因而在 Model2 中是安全的。但此时在 Model3 中仍然存在多已知签名存在伪造攻击，其攻击方式与上面提出的攻击方式一样，仅将 $H(m)$ 换为 $H(m,L)$。

为防止多已知签名存在伪造攻击，对改进后的环签名方案再作进一步改进，令 $r=H(m,L,t)$，其中 $t\in_R Z_q$，即 t 为长度为 $|q|$（$|q|$ 为 q 的二进制表示长度)的随机二进制串。这样，在每次产生新的签名时，随机选取新的 $t\in_R\{0,1\}^{|q|}$，当 $H(m,L,t)+r_s=0 \bmod q$ 时，重新选择 $t\in_R Z_q$。环签名的产生同原方案类似，仅 $H(m)$ 变为了 $H(m,L,t)$，这样就能防止多已知签名存在伪造攻击。

与文献[9]中的方案相比较，改进后的方案 1 将哈希函数作用于消息 m 和成员集 L 上，将所得到的哈希值用作原方案中的哈希值。这样就避免了群成员改变攻击。改进后的方案 2 将哈希函数作用于消息 m，成员集 L 和随机值 t 上，使得每次的签名所用的随机值不同，防止了多已知签名存在伪造攻击。多已知签名存在伪造攻击产生的原因在于 $H(m,L)P+u_i,1\le i\le n$ 在每次签名中固定不变，通过加入随机数，使得每次签名 $H(m,L,t)P+u_i,1\le i\le n$ 都不同，避免了该种攻击。

新方案匿名性　对于每个确定的环签名方案 $\sigma=(\sigma_1,\sigma_2,\cdots,\sigma_n,m,L,t)$ 而言，由于 m,L,t 是确定的，因而 $H(m,L,t)$ 也是确定的，并没有破坏原环签名方案中的匿名性要求。类似于 Zhang 等人的证明，可得到新方案的匿名性证明。

5 结束语

本文对文献[2, 9]提出的环签名方案进行了分析，给出了不同的攻击方法。文献[2]中的方案存在群成员改变攻击，文献[9]中的方案存在群成员改变攻击和多已知签名存在伪造攻击。针对这两种不同的攻击方法，对原签名方案进行了改进，使得改进后的环签名方案即便在最强的安全模型中仍是安全的。

参 考 文 献

[1] Rivest R L, Shamir A, and Tauman Y. How to leak a secret[A]. In Advances in ASIACRYPT 2001, LNCS[C], Berlin : Springer-Verlag, 2001,Vol. 2248: 552–565.

[2] Xu Jing, Zhang Zhenfeng, and Feng Dengguo. A ring signature scheme using bilinear pairings[A]. WISA2004, LNCS[C], 2004, Vol.3325: 160–170.

[3] Masayuki abe, Miyako ohkubo, and Koutarou suzuki. 1-out-of-n signatures from a variety of keys[J]. IEICE Trans fundamentals. 2004, E87-A: 131–140.

[4] Liu J K and Wong D S. On the security models of (Threshold) ring signature schemes[A]. ICISC 2004, LNCS[C], Springer-Verlag, 2004, Vol.3506: 204–217.

[5] Zhang Fangguo and Kim Kwangjo. ID-based blind signature and ring signature from pairings[A]. In Advances in ASIACRYPT 2002. LNCS[C]. Berlin: Springer-Verlag, 2002, Vol.2501: 548–566.

[6] Lin ChihYin and Wu TzongChen. An identity-based ring signature scheme from bilinear pairings. Cryptology ePrint Archive, 2003. http://eprint.iacr.org/2003/117

[7] Herranz J and Saez G. New identity-based ring signature schemes[A]. ICICS 2004, LNCS[C]. Berlin: Springer-Verlag, 2004, Vol.3269: 27–39.

[8] Awasthi A K and Lal S. ID-based ring signature and proxy ring signature schemes from bilinear pairings. Cryptology ePrint Archive, 2004. http://eprint.iacr.org/2004/184.pdf

[9] Zhang Fangguo, Naini R S, and Susilo W. An efficient signature scheme from bilinear pairings and its applications[A]. Public Key Cryptography 2004, LNCS[C]. Berlin: Springer-Verlag, 2004, Vol. 2947: 277–290.

[10] 王继林, 张键红, 王育民. 基于环签名思想的一种类群签名方案. 电子学报, 2004, 32(3): 408–410.
Wang Ji-lin, Zhang Jian-hong, and Wang Yu-min. A group signature scheme based on ring signature idea. Acta Electronica Sinica, 2004, 32(3): 408–410.

[11] Boneh D and Boyen X. Short signatures without random oracles[A]. Eurocrypt 2004, LNCS [C], Berlin: Springer-Verlag, 2004, Vol. 3027: 56–73.

王化群： 男，1974 年生，博士生, 研究方向为无线网络的安全.
张力军： 男，1942 年生，教授，博士生导师, 目前研究方向为无线数据、移动计算网络等.
赵君喜： 男，1963 年生，副教授，硕士生导师, 目前研究方向为信号处理等.