# 标准模型下基于双线性对的前向安全环签名方案

王玲玲[①②]　张国印[①]　马春光[①]
[①](哈尔滨工程大学计算机科学与技术学院　哈尔滨　150001)
[②](青岛科技大学信息科学技术学院　青岛　266061)

**摘　要**：该文针对环签名存在的密钥泄漏问题，基于前向安全数字签名和双线性对，提出一种新的前向安全环签名方案。方案的前向安全性保证了签名密钥可定期更新，即使当前时间段的签名密钥被泄漏，敌手也不能伪造先前的签名。在全面考虑了实际攻击者的能力后，给出了方案在标准模型下的安全性证明。

**关键词**：环签名；前向安全；双线性对；标准模型；密钥更新
**中图分类号**：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2009)02-0448-05

# A Forward-Secure Ring Signature Scheme Based on Bilinear Pairing in Standard Model

Wang Ling-ling[①②]　Zhang Guo-yin[①]　Ma Chun-guang[①]
[①](*College of Computer Science and Technology*, *Harbin Engineering University*, *Harbin* 150001, *China*)
[②](*College of Information Science & Technology*, *Qingdao University of Science & Technology*, *Qingdao* 266061, *China*)

**Abstract**: Since the proposed ring signatures has the key exposure problem, a new forward-secure ring signature scheme based on bilinear pairings is proposed. Forward security of the scheme means that even if the secret key of current time period is compromised, some security remains. It is impossible to forge the signature relating to the past. Secret key is evolved with different period time while the public key is fixed in the life time. The scheme is proven to be secure against adaptive chosen message attack in the standard model.

**Key words**: Ring signature; Forward-secure; Bilinear pairings; Standard model; Key evolution

## 1　引言

普通签名方案都有一个严重的缺陷：一旦签名密钥泄露，先前用该密钥签署的所有文档均失效。为了降低因密钥等秘密泄露而带来的损失，1997年，Anderson[1]首次提出了前向安全的概念。前向安全就是把整个有效时间分成若干个周期，在每个周期开始时使用单向更新函数定时更新密钥，而验证签名的公钥在整个有效时间内保持不变。即使当前周期的签名密钥被泄露，也并不影响此周期前签名的有效性。Bellare和Miner[2]设计了第一个有效的前向安全签名方案。随后，文献[3–5]提出了更为简单、实用的新方案。

2001年，Rivest等[6]在如何匿名泄漏秘密的背景下提出了一种新型签名技术——环签名。环签名可以让用户以一种完全匿名的方式对消息进行签名。任何验证者都能确信这个签名是来自于环中的某个成员，但却不能确认实际签名者的身份。自环签名的概念被提出后，引起了各国学者的广泛关注[7–10]。环签名作为一种特殊的数字签名，也存在密钥泄漏的问题。2006年，Liu等[11]首次针对环签名存在的密钥泄漏问题，提出了采用前向安全和密钥封装技术的解决方案，并且在随机预言模型下证明了方案在分解Blum整数和强RSA问题困难的前提下的安全性。

随机预言模型[12]作为一种非标准化的计算模型，是由Bellare和Rogaway于1993年提出的。在这个模型中，任何具体的对象例如哈希函数，都被当作随机对象。它允许人们规约参数到相应的计算，哈希函数被作为一个预言返回值，对每一个新的查询，将得到一个随机的应答。然而，该模型没有全面考虑实际攻击者的能力，并且存在缺陷，如哈希函数是确定的，不能总是返回随机的应答等。已有环签名方案的安全性大都是在随机预言模型下考虑的。2006年，Chow等[13]首次在标准模型下提出了基于新安全假设的环签名方案(CLW)。Bender等[14]在陷门置换存在的前提下，也提出了标准模型下安全的环签名方案(BKM)，然而他们的方案只适用于环成员个数为2个的情况。随后，Shacham和Waters[15]在已有方案的基础上，提出了在标准模型下高效的环签名方案(SWR)。

本文在解决了环签名存在的密钥泄漏问题的同时，还全面考虑了实际攻击者的能力，提出了在标准模型下基于双线性对的前向安全环签名方案 FSRS-BP。由于双线性对上的计算简便和椭圆曲线上点的表示所需位数较短，使得本方案

2007-07-31 收到，2008-07-04 改回
黑龙江省自然科学基金(F2004-06)，哈尔滨工程大学基础研究基金(HEUFT05067)和黑龙江省博士后科研启动基金资助课题

的计算简便，并且可以得到简短的密钥和签名，从而减小了存储量和计算代价。

## 2　相关定义

本文将采用合数阶有限群构造双线性映射，其详细定义和性质可参见文献[16]。

**定义 1**(双线性对(bilinear pairing)[16])　令 $G$ 和 $G_T$ 分别是阶为合数 $N$ 的加法群和乘法群，其中 $N=pq$，$p$，$q$ 均为大素数，并且 $G$ 上的离散对数问题是难解的。$P$ 是 $G$ 的一个生成元，即 $G=<P>$。可定义两个群之间的双线性映射为 $e: G\times G\to G_T$，且满足以下性质：

(1)双映射性　$e(aP,bQ)=e(P,Q)^{ab}$，对所有的 $P,Q\in G$，$a,b\in Z_N^*$ 均成立。

(2)非退化性　存在 $P,Q\in G$，使得 $e(P,Q)\neq 1_{G_T}$，其中 $1_{G_T}$ 是 $G_T$ 的幺元。

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

本文构造的 FSRS-BP 安全性基于$(q, n)$-DsjSDH 问题，与文献[13]类似，我们将给出加法群 $G$ 上$(q, n)$-DsjSDH 问题的定义。

**定义 2**($(q, n)$-DsjSDH 问题[13])　给定 $P,Q,xQ\in G$，对于 $1\le i\le n$，选取互不相同的整数 $a_i\in Z_N^*$ 和单向哈希函数 $H_i(\cdot):\{0,1\}^*\to Z_N^*$。任选非零 $m_\tau$ 和 $\sigma_{i,\tau}$，其中 $1\le\tau\le q$，$1\le i\le n$ 且满足 $\sum_{i=1}^{n}(xa_i+H_i(m_\tau))\sigma_{i,\tau}=P$。计算满足等式 $\sum_{i=1}^{n}(xa_i+H_i(m^*)+r_i)\sigma_i^*=P$ 且 $H_i(m^*)+r_i\neq H_i(m_\tau)$ 的 $m^*$ 和 $(\sigma_i^*,r_i)$，$1\le i\le n$ 是困难的。

**定义 3**(前向安全环签名方案模型)　一个前向安全的环签名方案一般由 5 个多项式时间算法组成 FSRS =(SET, IKG, KE, SIG, VER)。

(1)系统设置算法 SET　给定安全参数，返回系统公共参数 params。

(2)初始密钥生成算法 IKG　输入 params 和用户选择的任意信息，返回该用户的初始私钥，和验证公钥。

(3)密钥进化算法 KE　输入系统所处的时段和前一时段的私钥，用户计算现时段的私钥，公钥保持不变。

(4)环签名算法 SIG　系统给定环成员的公钥集，签名用户代表环群体用其私钥对消息 $m$ 进行签名，最后输出签名。

(5)签名验证算法 VER　接收者收到环签名后，用公钥验证环签名是否合法。

**定义 4**　如果 FSRS 满足以下性质，则 FSRS 是安全的。

(1)正确性　如果按照正确的签名步骤对消息 $m$ 进行签名，并且在传播的过程中签名没有被篡改，那么环签名满足签名验证等式。

(2)不可伪造性　任何攻击者能代表一个不包括他自己的环，对消息 $m$ 成功伪造一个环签名的概率是可以忽略的。

(3)无条件匿名性　给定一个合法签名，任何验证者猜对代表环进行签名的真实签名者身份的概率是可以忽略不计的。

(4)前向安全性　用户的私钥定期更新，公钥保持不变。已知某用户第 $j$ 时段的私钥，得到该用户第 $j-1$ 时段私钥的概率是可以忽略的。

## 3　标准模型下基于双线性对的前向安全环签名方案

依照定义 3，本文设计了一种基于双线性对的前向安全环签名方案 FSRS-BP=(SET-BP, IKG-BP, KE-BP, SIG-BP, VER-BP)。假设环中有 $n$ 个成员 $U=\{U_1,\cdots,U_n\}$。

(1)系统设置算法 SET-BP　选择定义 1 所示的双线性对 $e: G\times G\to G_T$，$|G|=|G_T|=N$，$N$ 为合数，且 $G=<P>=<R>$。选择单向哈希函数 $H_i(\cdot):\{0,1\}^*\to Z_N^*$，$1\le i\le n$。签名密钥的有效期分为 $T$ 个时段。系统公共参数为 $\{e,P,R,H_1,\cdots,H_n,T\}$。

(2)初始密钥生成算法 IKG-BP　用户 $U_i$ 任选 $x_{i,0},y_{i,0}\in {}_RZ_N^*$，计算 $u_i=x_{i,0}^{2^T}R, v_i=y_{i,0}^{2^T}R$。$U_i$ 的验证公钥为 $PK_i=\{u_i,v_i\}$，初始私钥为 $SK_{i,0}=\{x_{i,0},y_{i,0}\}$。

(3)密钥进化算法 KE-BP　系统一旦进入第 $j(1\le j\le T)$ 时段，用户 $U_i$ 使用第 $j-1$ 时段的私钥 $SK_{i,j-1}=\{x_{i,j-1},y_{i,j-1}\}$，计算 $x_{i,j}=x_{i,j-1}^2 \bmod N$，$y_{i,j}=y_{i,j-1}^2 \bmod N$。由归纳法可知 $x_{i,j}=x_{i,0}^{2^j}$，$x_{i,0}^{2^T}=x_{i,j}^{2^{T-j}}$。此时，立刻从系统中删除第 $j-1$ 时段的私钥 $SK_{i,j-1}$。系统在第 $j$ 时段的签名密钥对为 $(SK_{i,j},PK_i)$，其中 $SK_{i,j}=\{x_{i,j},y_{i,j}\}$，$PK_i=\{u_i,v_i\}$。

(4)环签名算法 SIG-BP　用户 $U_s$ 希望代表群体对消息 $m$ 进行签名。并且系统现在进入了第 $j$ 时段。用户 $U_s$ 执行如下操作：

(a)对于 $i\in\{1,\cdots,n\}\setminus s$，选择 $z_i\in {}_RZ_N^*$，计算 $\sigma_i=z_iR$。

(b)对于 $i\in\{1,\cdots,n\}$，选择 $r_i\in {}_RZ_N^*$，通过以下等式计算 $W$。

$$P=W+\left[\sum_{i\in\{1,\cdots,n\}\setminus s} z_i\cdot(u_i+H_i(m)R+r_iv_i)\right]$$

(c)通过 $SK_{s,j}=\{x_{s,j},y_{s,j}\}$ 计算

$$\sigma_s=\left(1\Big/\left(x_{s,j}^{2^{T-j}}+H_S(m)+r_sy_{s,j}^{2^{T-j}}\right)\right)W$$

输出环签名为 $\{(\sigma_1,r_1),\cdots,(\sigma_n,r_n)\}$。

(5)签名验证算法 VER-BP　接收方收到消息 $m$ 的环签名 $\{(\sigma_1,r_1),\cdots,(\sigma_n,r_n)\}$，用 $n$ 个成员的公钥验证等式：

$$\prod_{i=1}^{n}[e(\sigma_i,(u_i+H_i(m)R+r_iv_i))]=e(P,R)$$

若等式成立则接收签名，否则拒绝。

## 4　安全性分析

**定理 1**　FSRS-BP 满足签名验证的正确性。

**证明** 接收方收到环签名$\{(\sigma_1,r_1),\cdots,(\sigma_n,r_n)\}$，若该签名是按照第 3 节步骤产生的，并且在传输的过程中没有改变，则有

$$\prod_{i=1}^{n}[e(\sigma_i,(u_i+H_i(m)R+r_iv_i))]=e(\sigma_s,(u_s+H_s(m)R+r_sv_s))\cdot\prod_{i\in\{1,\cdots,n\}/s}[e(\sigma_i,(u_i+H_i(m)R+r_iv_i))]$$

$$=e\left(\left(1\Big/\left(x_{s,j}^{2^{T-j}}+H_S(m)+r_sy_{s,j}^{2^{T-j}}\right)\right)W,x_{s,0}^{2^T}R+H_s(m)R+r_sy_{s,0}^{2^T}R\right)\cdot\prod_{i\in\{1,\cdots,n\}/s}\left[e\left(z_iR,x_{i,0}^{2^T}R+H_i(m)R+r_iy_{i,0}^{2^T}R\right)\right]$$

$$=e(W,R)\cdot e\left(\sum_{i\in\{1,\cdots,n\}/s}z_i\left(x_{i,j}^{2^{T-j}}+H_i(m)+r_iy_{i,j}^{2^{T-j}}\right)R,R\right)$$

$$=e\left(W+\sum_{i\in\{1,\cdots,n\}/s}z_i\left(x_{i,j}^{2^{T-j}}+H_i(m)+r_iy_{i,j}^{2^{T-j}}\right)R,R\right)$$

$$=e(P,R)$$

所以 FSRS-BP 的验证算法是正确有效的。

**定理 2** 如果$(q, n)$-DsjSDH 问题是难解的，则在标准模型下 FSRS-BP 满足环签名的不可伪造性。

**证明** 假设在第 $j$ 时段，敌手 $A$ 成功伪造了消息 $m$ 的签名，则存在多项式时间算法 $B$，可以通过与 $A$ 合作来解决$(q, n)$-DsjSDH 问题。

给定$(q, n)$-DsjSDH 问题的一个实例：$P,S,zS\in G$，$a_i^{2^{T-j}}\in Z_N^*$，单向哈希函数：$H_i(\cdot):\{0,1\}^*\to Z_N^*$，$m_\tau^{'}$，$\sigma_{i,\tau}^{'}$，其中$i\in\{1,\cdots,n\}$，$\tau\in\{1,\cdots,q\}$。$B$ 首先令 $R=S$，运行密钥生成算法生成用户 $U_i$ 的签名公钥$(u_i=x_{i,j}^{2^{T-j}}R,v_i=y_{i,j}^{2^{T-j}}R)$，并将其发送给 $A$。敌手 $A$ 通过询问消息$m_1,\cdots,m_{q_S}\in Z_N^*$ 的签名$(\sigma_t,r_t)$，其中$1\le t\le q_s$，$q_s\le q$，可以伪造$U_i$ 的一个合法消息签名对$(m^*,\sigma_i^*,r_i^*)$。这里，敌手 $A$ 可以通过以下两种方式来伪造签名：

(1)敌手 $A$ 询问消息 $m$ 的签名，而恰好有 $H_i(m)=-x_{i,j}^{2^{T-j}}$；或者对于敌手 $A$ 伪造的签名$(m^*,\sigma_i^*,r_i^*)$，满足$H_i(m^*)+r_i^*y_{i,j}\notin\{H_i(m_\tau)\}_{\tau=1}^{q_s}$。

(2)敌手 $A$ 所询问的所有消息 $m$，均不满足 $H_i(m)=-x_{i,j}^{2^{T-j}}$，并且对于 $(m^*,\sigma_i^*,r_i^*)$，满足 $H_i(m^*)+r_i^*y_{i,j}\in\{H_i(m_\tau)\}_{\tau=1}^{q_s}$。

下面将证明 $B$ 如何解决$(q, n)$-DsjSDH 问题。假设对于第 $\tau$ 次询问，$B$ 生成 $m_\tau$ 的签名。

对于(1)，$B$ 随机选择 $y,b_1,\cdots,b_n\in Z_N^*$，令用户 $U_i$ 的公钥为$(u_i,v_i)=(a_i^{2^{T-j}}\cdot zS,(yb_i)^{2^{T-j}}\cdot S)$。若存在$i\in\{1,\cdots,n\}$，使得$a_i^{2^{T-j}}\cdot zS=-H_i(m_\tau)S$，则 $B$ 可以计算出 $z$ 的值，进而解决$(q, n)$-DsjSDH 问题。

否则，对于$i\in\{1,\cdots,n\}$，$B$ 令$r_{i,\tau}=[H_i(m_\tau^{'})-H_i(m_\tau)]/(yb_i)^{2^{T-j}}$，此时若 $r_{i,\tau}=0$，则 $B$ 宣布失败。$B$ 生成签名对$(\sigma_{i,\tau}^{'},r_{i,\tau})$，并且签名满足：

$$\prod_{i=1}^{n}[e(\sigma_{i,\tau}^{'},u_i+H_i(m_\tau)R+r_{i,\tau}v_i)]=\prod_{i=1}^{n}[e(\sigma_{i,\tau}^{'},u_i+(H_i(m_\tau)+r_{i,\tau}^{'}(yb_i)^{2^{T-j}})R)]=\prod_{i=1}^{n}[e(\sigma_{i,\tau}^{'},u_i+H_i(m_\tau^{'})R)]=\prod_{i=1}^{n}[e(\sigma_{i,\tau}^{'},(za_i^{2^{T-j}}+H_i(m_\tau^{'}))R)]=e(P,R)$$

对于(2)，$B$ 随机选择 $x,b_1,\cdots,b_n\in Z_N^*$，令用户 $U_i$ 的公钥为$(u_i,v_i)=((xb_i)^{2^{T-j}}\cdot S,a_i^{2^{T-j}}\cdot zS)$。对于$i\in\{1,\cdots,n\}$，令$r_{i,\tau}=[(xb_i)^{2^{T-j}}+H_i(m_\tau)]/H_i(m_\tau^{'})$，$\sigma_{i,\tau}=(1/r_{i,\tau})\sigma_{i,\tau}^{'}$。$B$ 生成签名对$(\sigma_{i,\tau},r_{i,\tau})$，并且签名满足：

$$\prod_{i=1}^{n}[e(\sigma_{i,\tau},u_i+H_i(m_\tau)R+r_{i,\tau}v_i)]=\prod_{i=1}^{n}\left[e\left(\sigma_{i,\tau},\left((xb_i)^{2^{T-j}}+H_i(m_\tau)\right)R+r_{i,\tau}v_i\right)\right]=\prod_{i=1}^{n}[e(\sigma_{i,\tau},r_{i,\tau}H_i(m_\tau^{'})R+r_{i,\tau}v_i)]=\prod_{i=1}^{n}\left[e\left((1/r_{i,\tau})\sigma_{i,\tau}^{'},r_{i,\tau}\left(H_i(m_\tau^{'})+za_i^{2^{T-j}}\right)R\right)\right]=\prod_{i=1}^{n}\left[e\left(\sigma_{i,\tau}^{'},\left(H_i(m_\tau^{'})+za_i^{2^{T-j}}\right)R\right)\right]=e(P,R)$$

所以，对于(1)和(2)，$B$ 都可以生成合法签名。

假设敌手 $A$ 生成消息 $m^*$ 的合法签名$(\sigma_i^*,r_i^*)$，$i\in\{1,\cdots,n\}$，并且 $m^*$ 从未被询问过。

对于 (1)，$H_i(m^*)+r_i^*\cdot(yb_i)^{2^{T-j}}\notin\{H_i(m_\tau^{'})\}_{\tau=1}^{q_S}$，令$R_i=r_i^*\cdot(yb_i)^{2^{T-j}}$，可得$(q, n)$-DsjSDH 问题的一个解$(\sigma_i^*,R_i)$，其中$i\in\{1,\cdots,n\}$。

对于(2)，因为存在某个$i\in\{1,\cdots,n\}$和$\tau\in\{1,\cdots,q\}$，满足 $H_i(m^*)+r_i^*za_i^{2^{T-j}}=H_i(m_\tau^{'})$，所以有 $H_i(m^*)+r_i^*za_i^{2^{T-j}}=H_i(m_\tau)+r_{i,\tau}za_i^{2^{T-j}}$。

又因为$(m^*,r_i^*)\ne(m_\tau,r_{i,\tau})$，可以解得$z=(H_i(m^*)-H_i(m_\tau))/(a_i^{2^{T-j}}(r_{i,\tau}-r_i^*))$。

即解决了$(q, n)$-DsjSDH 问题的一个实例。

**定理 3** FSRS-BP 满足签名人的无条件匿名性。

**证明** 该方案是完全对称的，仅从签名来看，由于匿名集合中任何成员的地位是一样的，即便所有人的私钥泄露也无法确定具体签名人。任何一个用户是消息签名者的可能性是相等的，均为$1/n$。因此方案满足签名人的无条件匿名性。

**定理 4** 如果模 $N$ 的二次剩余问题是难解的，则 FSRS-BP 满足前向安全性。

**证明** 由密钥进化算法 $x_{i,j}=x_{i,j-1}^2\bmod N$，$y_{i,j}=y_{i,j-1}^2\bmod N$ 可知，用户私钥定期更新。用户公钥始终保持不变，这是因为 $u_i=x_{i,0}^{2^T}R$，$v_i=y_{i,0}^{2^T}R$，且 $x_{i,0},y_{i,0}\in_R Z_N^*$ 是初始密钥生成阶段选定的。

密钥进化算法涉及模 $N$ 的二次剩余问题。由于 $N$ 是合数，模 $N$ 的二次剩余问题是难解的，所以已知$(x_{i,j},y_{i,j})$，由式 $x_{i,j}=x_{i,j-1}^2\bmod N$，$y_{i,j}=y_{i,j-1}^2\bmod N$ 推导出$(x_{i,j-1},$

$y_{i,j-1}$) 的概率是可以忽略的。因此，FSRS-BP 满足前向安全性。

## 5　性能分析

下面，将从计算代价、存储代价和前向安全性 3 个方面来考虑方案 FSRS-BP 的性能，并和已有标准模型下可证安全的环签名方案进行比较。

这里假定环成员个数是 $n$。$k$ 为 SWR 方案中哈希函数 $H$ 输出值的长度。令 $l_G$ 表示群 $G$ 中元素的长度。$l_{Z_N^*}$ 表示 $Z_N^*$ 中元素的长度。对于 Bender 等提出的环签名方案 BKM，由于参与签名的环成员个数只有 2 个，其存储代价和计算代价与其他方案不具可比性，因此不再给出。

根据表 1 可以看出，方案 FSRS-BP 是唯一一个在标准模型下可证安全且具有前向安全性的环签名方案。此外，FSRS-BP 的签名计算不需要任何模幂运算，仅需要 $4n$−3 次的 $G$ 中的模乘运算，$2n$−2 次 $G$ 中的模加运算，2 次 $Z_N$ 中的模加运算，2 次 $Z_N^*$ 中的模乘运算和 $n$ 次哈希计算，并且验证算法中的配对运算也比 SWR 方案减少了。由于方案中最费时的就是模幂运算和配对运算。因此从总体上来说，本文提出的方案在性能上优于已有方案。特别是当环成员个数 $n$ 很大时，优势更加明显。

**表 1 标准模型下的环签名方案性能比较**

| 方案 | 签名计算代价 | 验证签名计算代价 | 存储代价 | 前向安全性 |
|---|---|---|---|---|
| CLW | $3n$−2 次 $G_1$ 中的模幂；$n$−1 次 $G_2$ 中的模幂；$n$−1 次 $G_1$ 中的模乘；$2n$−2 次 $G_2$ 中的模乘；$n$ 次哈希计算 | $n$+1 次配对计算 | $n(l_G + l_{Z_p^*})$ | 无 |
| BKM | — | — | — | 无 |
| SWR | $5n+k$+3 次 $G$ 中的模幂；$4n+k$+3 次 $G$ 中的模乘；$n$+1 次 $Z_n$ 中的模加；1 次哈希计算； | $2n$+3 次配对计算 | $(2n+2)\,l_G$ | 无 |
| FSRS-BP | $4n$−3 次 $G$ 中的模乘；$2n$−2 次 $G$ 中的模加；2 次 $Z_N$ 中的模加；2 次 $Z_N^*$ 中的模乘；$n$ 次哈希计算 | $n$+1 次配对计算 | $n(l_G + Z_N^*)$ | 有 |

## 6　结束语

本文采用前向安全数字签名和双线性对构造了一种新的前向安全环签名方案，并给出了其在标准模型下的安全性证明及性能分析。方案采用双线性对，简化了整个计算过程，并且得到的密钥和签名简短，从而减小了存储量和计算代价。标准模型下基于双线性对的前向安全环签名方案对于安全性要求高，计算能力有限或低带宽的情况将非常适用。

本方案的安全性证明基于求解($q$, $n$)-DsjSDH 问题的困难性。可以看出($q$, $n$)-DsjSDH 问题是为了证明在标准模型下环签名的安全性而提出的，结构比较复杂。因此，如何基于经典数学难题构造标准模型下前向安全的环签名方案将是我们下一步要研究的问题。此外，将标准模型下的前向安全环签名方案用于可转移电子现金系统[17]和公平电子支票系统[18]也是我们感兴趣的研究问题。

## 参 考 文 献


[1] Anderson R. Two remarks on public key cryptology [R]. Invited Lecture, ACM-CCS'97, 1997.

[2] Bellar M and Miner S. A forward-secure digital signature scheme [C]. CRYPIO'99, Springer-Verlag, 1999. LNCS 1666: 431−448.

[3] Abdalla J M and Reyzin L. A new forward-secure digital signature scheme [C]. Asia crypt 2000, Springer-Verlag, 2000, LNCS 1976: 116−129.

[4] Itkis G and Reyzin L. Forward-secure signatures with optimal signing and verifying [C]. CRYPTO 2001, Springer-Verlag, 2001, LNCS 2139: 499−514.

[5] Kozolov A and Reyzin L. Forward-secure signatures with fast key update [C]. Security in communication networks, Springer-Verlag, 2002, LNCS 2576: 247−262.

[6] Rivest R, Shamir A, and Tauman Y. How to leak a secret [C]. Advances in Cryptology-Asiacrypt'01, Springer-Verlag, 2001, LNCS 2248: 552−565.

[7] Gao C Z, Yao Z A, and Li L. A ring signature scheme based on the Nyberg-Rueppel signature scheme [C]. ACNS 2003, Springer-Verlag, 2003, LNCS 2846: 169−175.

[8] Liu J K, Wei V K, and Wong D S. Linkable spontaneous anonymous group signature for Ad hoc groups [C]. Proc. ACISP'04, Springer-Verlag, 2004, LNCS 3108: 325−335.

[9] Awasthi A K and Sunder L. ID-based ring signature and proxy ring signature schemes from bilinear pairings [EB/OL]. http://eprint.iacr.org/2004/184.

[10] 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, Ma C G. Survey on ring signature [J]. *Journal on Communications*, 2007, 28(5): 109−117.

[11] Liu J K and Wong D S. Solutions to key exposure problem in

ring signature [EB/OL]. http://eprint.iacr.org/2005/427.

[12] Bellare M and Rogoway P. Random oracles are practical: A paradigm for designing efficient protocols [C]. Proceedings of the First Conference on Computer and Communications Security, Fairfax, 1993: 62–73.

[13] Chow S S M, Liu J K, and Wei V K, *et al*.. Ring signature without random oracles [C]. ASIACCS'06, Taiwan, 2006: 297–302.

[14] Bender A, Katz J, and Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles [C]. TCC 2006. Springer-Verlag, 2006, LNCS 3876: 60–79.

[15] Shacham H and Waters B. Efficient ring signatures without random oracles [EB/OL]. http://eprint.iacr.org/2006/289.

[16] Boneh D, Goh E J and Nissim K. Evaluating 2-DNF formulas on ciphertexts [C]. Proceedings of TCC 2005, Springer-Verlag, 2005, LNCS 3378: 325–341.

[17] 马春光, 杨义先. 可转移离线电子现金[J]. 计算机学报, 2005, 28(3): 301–308.
Ma C G and Yang Y X. Transferable off-line electronic cash [J]. *Chinese Journal of Computers*, 2005, 28(3): 301–308.

[18] 马春光, 杨义先, 胡正名. 可直接花费余额的电子支票系统[J]. 电子学报, 2005, 33(9): 1562–1566.
Ma C G, Yang Y X, Hu Z M. A fair electronic check systems with reusable refund [J]. *Acta Electronic Sinica*, 2005, 33(9): 1562–1566.

王玲玲： 女，1982 年生，博士生，研究方向为密码学、信息安全.

张国印： 男，1962 年生，博士，教授，博士生导师，主要研究方向为信息安全、嵌入式系统.

马春光： 男，1974 年生，博士，副教授，主要研究方向为密码学、网络与信息安全.