一种签名长度固定的基于身份的环签名方案

王玲玲 张国印 马春光
(哈尔滨工程大学计算机科学与技术学院 哈尔滨 150001)

摘 要：环签名作为一种匿名通信技术，可以使签名人具有匿名性。在以往提出的环签名方案中，签名长度与环成员个数成正比，这是环签名的一个公开问题。该文使用双线性对，并基于累加器技术，提出了一种签名长度固定的基于身份的环签名方案，并证明了其安全性。方案既能保证消息发送者的匿名性，又可使得到的签名长度与环成员个数无关，解决了环签名的公开问题。

关键词：数字签名；环签名；基于身份密码体制；累加器；双线性对
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2007)11-2645-04

An Identity-Based Ring Signature Scheme with Constant-Size Signature

Wang Ling-ling Zhang Guo-yin Ma Chun-guang
(*College of Computer Science and Technology, Harbin Engineering University, Harbin* 150001, *China*)

Abstract: The ring signature is one of the anonymous techniques by virtue of its unconditional anonymity. Most proposed ring signature schemes have the problem that the size of ring signatures depends linearly on the group size. That is an open problem. In this paper, new scheme called constant-size ring signatures is presented. The scheme is based on bilinear pairings and accumulators. In the scheme, users can send messages anonymously, and the size of the signature is independent of the group size. Therefore, the scheme proposed can be used to solve the open problem.

Key words: Signature; Ring signature; ID-based cryptosystem; Accumulators; Bilinear pairings

1 引言

目前，匿名技术在现代网络通信中有着广泛的应用需求。公民隐私权是现代人的一项基本生活权利，商业秘密是商品经济社会的命根，政府事务和军事活动机密的泄漏会带来社会的动乱。匿名技术中的一个重要问题是匿名通信中的身份识别问题。虽然通信的一方或多方不需要知道对方的真实身份，但也要保证对方属于某个合法的匿名集，因此匿名签名和匿名认证就成为实现匿名通信的一个基本构件。

环签名是一种可以让用户完全匿名地对消息进行签名的匿名签名技术。任何验证者都能确信这个签名来自于环中的某个成员，但不能确认实际签名者的身份。2001 年，Rivest 和 Tauman [1] 首先提出了环签名的概念，并给出了在理想模型下可证安全的环签名方案。2002 年，对于文献[1]中的方案，Bresson 和 Stern [2] 等给出了在随机预言模型 [3] 下更加简单的安全性证明过程，并且还提出了门限环签名方案的概念。同年，Zhang 和 Kim [4] 首次提出了基于身份的环签名方案。

基于身份的公钥密码体制是由 Shamir [5] 首先提出。在这个密码体制中，用户的公钥为该用户的身份信息，用户的私钥是由一个可信密钥生成中心颁发的。这样，用户间的安全通信，不再需要交换安全证书，也不需要使用在线服务器。直到 2001 年，Boneh 和 Franklin [6] 才提出了一个实用的基于身份的签名方案。

由于验证者需要了解环成员的信息，所以在以往提出的环签名方案中，签名长度与环成员个数是成正比的。然而正如文献[7]所指出的，在很多情况下，环成员是固定不变的，此时就不需要对环成员信息进行描述，这样就可以得到签名长度固定的环签名方案。虽然文献[7, 8]提出可以应用 Fiat-Shamir 方法 [9] 将签名长度固定的认证方案转化为签名方案，但是他们并没有给出具体的转变过程，也没有给出转化后环签名方案的安全性证明。

本文考虑在为签名者提供匿名性的同时，还考虑了如何用最小的代价得到固定长度环签名的问题。在基于身份的 AD-hoc 匿名认证方案 [8] 的基础上，本文首次给出了签名长度固定的基于身份的环签名方案，并证明了其安全性。

2 符号及定义

为了叙述方便，首先进行一些符号约定。Z_p 表示所有小于 p 的正整数组成的集合，Z_p^* 表示整数模 p 的乘法群。$x \in_R X$ 表示从 X 中任取一元素 x。$\{0,1\}^*$ 为任意长的字符串，$\{0,1\}^l$ 表示长度为 l 的字符串。PT 表示多项式时间，PPT

2006-08-07 收到，2007-05-15 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)资助课题

表示概率多项式时间。敌手 A 用一个交互式图灵机表示。

定义 1[10] (双线性对) 假设 G_1 和 G_2 分别是阶为 p 的加法群和乘法群，其中 p 是大素数，并且 G_1 和 G_2 上的离散对数问题是难解的。P 是 G_1 的一个生成元。两个群之间的双线性映射 $e: G_1 \times G_1 \to G_2$ 是满足以下性质的映射：

(1)双映射性 $e(aP,bQ)=e(P,Q)^{ab}$，对所有的 $P,Q \in G_1$，所有的 $a,b \in Z_p$ 成立。

(2)非退化性 存在 $P,Q \in G_1$，使得 $e(P,Q) \neq 1_{G_2}$，其中 1_{G_2} 是 G_2 的幺元。

(3)可计算性 存在有效的算法，对于 $P,Q \in G_1$，可计算 $e(P,Q)$。

定义 2[11] (q-SDH 问题) 设 G_1 和 G_2 分别是如上所述的循环群，e 是双线性映射。已知 $(P,sP,\cdots,s^qP)$，其中 $s \in_R Z_p^*$，计算 $(c,1/(s+c)P)$，$c \in Z_p$。

定义 3[8] (累加器) 累加器是一个二元组 $(\{X_l,F_l\})$，其中 $l \in N$，$\{X_l\}$ 为累加器的值域，$\{F_l\}$ 为函数对族，即：$(f,g) \in F_l$，其中 $f: U_f \times X_f \to U_f$，$g: U_f \to U_g$ $(U_f = U_g)$。此外，累加器满足以下属性：

(1)生成有效性 对于给定的安全参数，存在一个 PT 算法，可以随机生成一个函数对 $(f,g) \in F_l$。

(2)计算有效性 存在一个多项式 P，对每个给定的整数 k，对所有的 $x \in U_f$ 以及所有的 $y \in X_f$，$f(x,y)$ 是在时间 $P(k)$ 内可计算的。

(3)准交换性 对所有 $x \in U_f$，y_1，$y_2 \in X_f$，有 $f(f(x,y_1),y_2)=f(f(x,y_2),y_1)$。

本文采用文献[8]提出的基于双线性映射的动态累加器构造了签名长度固定的环签名方案。文献[8]中选择了定义 1 所示的双线性映射 $e: G_1 \times G_1 \to G_2$，参数 $t=(P,P_{\text{pub}}=sP,\cdots,s^qP)$，其中 $s \in_R Z_p^*$，q 是可以累加的最大成员个数。函数对 (f,g) 定义为 $f: Z_p \times Z_p \to Z_p$，$g: Z_p \to G_1$，即 $f: (u,x) \mapsto (x+s)u$，$g: u \mapsto uP$。具体可参见文献[8]。

3 签名长度固定的基于身份的环签名方案

3.1 签名长度固定的基于身份的环签名方案模型

定义 4 一个签名长度固定的基于身份的环签名方案一般由 6 个 PT 算法组成，IR=(SET, KG, GPK, GSK, SIG, VER)。

(1)系统设置算法 SET 给定安全参数，返回公共参数 params 和系统主密钥 mk。其中只有密钥生成中心知道 mk。

(2)用户私钥生成算法 KG 输入 params，mk 和任意用户的身份信息，返回该用户的私钥，同时身份信息作为相应公钥。

(3)环公钥生成算法 GPK 输入 params 和一群用户的身份信息，输出唯一的一个环公钥。环公钥的计算代价与群用户的个数成正比。

(4)环私钥生成算法 GSK 输入 params，用户的身份信息集和某一用户的密钥对，输出一个环私钥。环私钥的计算代价与群用户的个数成正比。同一个环公钥可以对应多个环私钥。

(5)环签名算法 SIG 系统给定环私钥，相应的用户验证环私钥的合法性。若环私钥合法，则该用户代表环群体对消息 m 进行签名，最后输出签名。

(6)验证算法 VER 接收者收到签名后，用环公钥和公开参数验证签名是否合法。

定义 5 环签名方案 IR 是安全的，如果 IR 满足：

(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 成功伪造一个合法环签名的概率是可以忽略的。

(3)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。

3.2 签名长度固定的基于身份的环签名方案

按照定义 4 提出的签名长度固定的基于身份的环签名方案一般模型，本文提出了一种基于双线性对和身份密码体制的签名长度固定的环签名方案(IRBP)。具体方案可表示为 IRBP=(SET-BP,KG-BP,GPK-BP,GSK-BP,SIG-BP,VER-BP)。

(1)系统设置算法 SET-BP 给定安全参数 l，生成累加器 (f,g)。选择双线性映射：$e: \hat{G}_1 \times \hat{G}_1 \to \hat{G}_2$，其中 $\hat{G}_1$ 和 $\hat{G}_2$ 同为 p 阶的加法群和乘法群，P 是 $\hat{G}_1$ 的一个生成元。生成 $t=(P,P_{\text{pub}}=sP,\cdots,s^qP)$，其中 $s \in_R Z_p^*$，q 是可以累加的最大成员个数。同时，选择参数 $G_1,G_2,K,Q \in_R \hat{G}_1^*$，$u,s_m \in_R Z_p^*$，计算 $Q_{\text{pub}}=s_mQ$。选择哈希函数：$H_1: \{0,1\}^* \to Z_p$。公布系统参数 $\text{params}=(l,e,P,t,f,g,G_1,G_2,K,Q,Q_{\text{pub}},u,H_1)$，对系统主密钥 $\text{mk}=s_m$ 保密。

(2)用户私钥生成算法 KG-BP 对于身份信息为 id 的用户，密钥生成中心生成该用户对应的私钥 $s_{\text{id}}=R_{\text{id}}$，其中 $R_{\text{id}}=1/(H_1(\text{id})+s_m)Q$。

(3)环公钥生成算法 GPK-BP 假设环中有 $k(k \leq q)$ 个成员，其身份信息集 $U=\{\text{id}_1,\text{id}_2,\cdots,\text{id}_k\}$。计算 $X=\{H_1(\text{id}_i)\}_{i=1}^k$，生成环公钥 $\text{gpk}=V=g(f(u,X))$。

(4)环私钥生成算法 GSK-BP 给定某用户的身份信息 id_j 和身份信息集合 $\{\text{id}_i\}_{i=1}^k$，计算 $X'=\{H_1(\text{id}_i)\}_{i=1}^k$，其中 $i \neq j$，$h_{\text{id}_j}=H_1(\text{id}_j)$ 和证据 $W=g(f(u,X'))$，则该用户对应的环私钥为 $\text{gsk}=(h_{\text{id}_j},R_{\text{id}_j},W)$。

(5)环签名算法 SIG-BP 假设用户 u_{id} 希望代表群体对消息 m 进行签名，他将执行如下操作：

首先，对于给定的环私钥 $\text{gsk}=(h_{\text{id}},R_{\text{id}},W)$，用户 u_{id} 验证以下两个等式是否成立：$e(h_{\text{id}}Q+Q_{\text{pub}},R_{\text{id}})=e(Q,Q)$，

$e(h_{\mathrm{id}}P+P_{\mathrm{pub}},W)=e(P,V)$。若等式不成立，则环私钥不合法，用户要求密钥生成中心重新生成合法环密钥。

若环私钥合法，则用户随机选择 $r_1,r_2,r_3,k_1,\cdots,k_7\in_R Z_p$，计算 $U_1=R_{\mathrm{id}}+r_1K$；$U_2=W+r_2K$；$R=r_1G_1+r_2G_2+r_3K$；$T_1=k_1G_1+k_2G_2+k_3K$；$T_2=k_4G_1+k_5G_2+k_6K-k_7R$；$\Pi_1=e(Q,U_1)^{-k_7}e(Q,K)^{k_4}e(Q_{\mathrm{pub}},K)^{k_1}$；$\Pi_2=e(P,U_2)^{-k_7}e(P,K)^{k_5}e(P_{\mathrm{pub}},K)^{k_2}$。

随机选择 $a_1,a_2\in_R Z_p^*$，计算 $c=H_1(m\,||\,e((P_{\mathrm{pub}}+a_1P)/(a_2+r_2),R_{\mathrm{id}}))$；$s_1=k_1+cr_1$；$s_2=k_2+cr_2$；$s_3=k_3+cr_3$；$s_4=k_4+cr_1h_{\mathrm{id}}$；$s_5=k_5+cr_2h_{\mathrm{id}}$；$s_6=k_6+cr_3h_{\mathrm{id}}$；$s_7=k_7+ch_{\mathrm{id}}$。

输出环签名 $(c,U_1,U_2,R,T_1,T_2,\Pi_1,\Pi_2,s_1,\cdots,s_7)$。

(6)验证算法 VER-BP　接收方收到环签名 $(c,U_1,U_2,R,T_1,T_2,\Pi_1,\Pi_2,s_1,\cdots,s_7)$，可以验证以下等式：$T_1=s_1G_1+s_2G_2+s_3K-cR$；$T_2=s_4G_1+s_5G_2+s_6K-s_7R$；$\Pi_1=e(Q,U_1)^{-s_7}e(Q,K)^{s_4}e(Q_{\mathrm{pub}},K)^{s_1}e(Q,Q)^ce(Q_{\mathrm{pub}},U_1)^{-c}$；$\Pi_2=e(P,U_2)^{-s_7}e(P,K)^{s_5}e(P_{\mathrm{pub}},K)^{s_2}e(P,V)^ce(P_{\mathrm{pub}},U_2)^{-c}$；若以上等式均成立，则接收方认为签名有效，否则拒绝环签名。

4　方案的安全性

定理 1　IRBP 满足正确性，匿名性和不可伪造性。

下面对定理 1 的各个子命题分别进行讨论。

定理 2　IRBP 满足正确性。

证明　接收方收到环签名 $(c,U_1,U_2,R,T_1,T_2,\Pi_1,\Pi_2,s_1,\cdots,s_7)$，若该签名是按照 3.2 节步骤产生的，并且在传输的过程中没有改变，则有

$s_1G_1+s_2G_2+s_3K-cR=(k_1+cr_1)G_1+(k_2+cr_2)G_2+(k_3+cr_3)K-c(r_1G_1+r_2G_2+r_3K)=k_1G_1+k_2G_2+k_3K=T_1$；$s_4G_1+s_5G_2+s_6K-s_7R=(k_4+cr_1h_{\mathrm{id}})G_1+(k_5+cr_2h_{\mathrm{id}})G_2+(k_6cr_3h_{\mathrm{id}})K-(k_7+ch_{\mathrm{id}})R=k_4G_1+k_5G_2+k_6K-k_7R=T_2$；还有 $e(Q,U_1)^{-s_7}e(Q,K)^{s_4}e(Q_{\mathrm{pub}},K)^{s_1}e(Q,Q)^ce(Q_{\mathrm{pub}},U_1)^{-c}=e(Q,U_1)^{-(k_7+ch_{\mathrm{id}})}e(Q,K)^{(k_4+cr_1h_{\mathrm{id}})}e(Q_{\mathrm{pub}},K)^{(k_1+cr_1)_1}e(Q,Q)^ce(Q_{\mathrm{pub}},U_1)^{-c}$。

将 $U_1=R_{id}+r_1K$ 代入上式，则可得上式 $=e(Q,U_1)^{-k_7}\cdot e(Q,K)^{k_4}e(Q_{\mathrm{pub}},K)^{k_1}=\Pi_1$；

同理，将 s_2,s_5,s_7 和 $U_2=W+r_2K$ 代入 Π_2 的验证等式，有 $e(P,U_2)^{-s_7}e(P,K)^{s_5}e(P_{\mathrm{pub}},K)^{s_2}e(P,V)^ce(P_{\mathrm{pub}},U_2)^{-c}=e(P,U_2)^{-k_7}e(P,K)^{k_5}e(P_{\mathrm{pub}},K)^{k_2}=\Pi_2$，所以该方案的验证算法是有效的，即 IRBP 满足正确性要求。　证毕

定理 3　在 ROM 下，如果 q-SDH 问题是难解的，则 IRBP 满足签名人的匿名性。

证明　假设存在一个 PPT 敌手 A，可以成功地从一个环签名中猜测出签名人的身份信息，那么存在 PPT 算法 B 可以解决 q-SDH 问题。给定 q-SDH 问题的一个实例 $(\widehat{P},z\widehat{P},\cdots,z^q\widehat{P})$，其中 $z\in_R Z_p^*$，B 可以计算 $(x,1/(z+x)\widehat{P})$，$x\in Z_p$。

首先，对于给定的安全参数 l，B 运行 SET-BP 生成系统参数 $\mathrm{params}=(l,e,P,t,f,g,G_1,G_2,K,Q,Q_{\mathrm{pub}},u,H_1)$，并将其发送给 A，其中 $t=(\widehat{P},P_{\mathrm{pub}}=z\widehat{P},\cdots,z^q\widehat{P})$，$H_1$ 作为随机预言。A 可以获得所有人的身份-私钥对 $(\mathrm{id}_i,\mathrm{gsk}_i)_{i=1}^k$，并从其中选择 $(\mathrm{id}_1,\mathrm{gsk}_1)$ 和 $(\mathrm{id}_2,\mathrm{gsk}_2)$。$B$ 在 $(\mathrm{id}_1,\mathrm{gsk}_1)$ 和 $(\mathrm{id}_2,\mathrm{gsk}_2)$ 中随机选择一对 $(\mathrm{id}_i,\mathrm{gsk}_i)$，$i\in\{1,2\}$，$B$ 可以模拟 A 要访问的所有预言。B 运行签名预言对消息 m 签名，得到签名值 σ，并将 σ 发送给 A。A 根据 σ 猜测出签名人身份为 id。若 $\mathrm{id}=\mathrm{id}_i$，则 B 就认为 $(x,1/(z+x)\widehat{P})$ 可解。因为对于 id，B 再次运行签名预言，通过选择不同的 $a_1,a_2\in_R Z_p^*$，得到一个与 σ 相同的签名值，则有 $c=c_i$。又因为 $\mathrm{id}=\mathrm{id}_i$，则有 $R_{\mathrm{id}}=R_{\mathrm{id}_i}$。根据式 $c=H_1(m\,||\,e((P_{\mathrm{pub}}+a_1P)/(a_2+r_2),R_{\mathrm{id}}))$ 可得 $(P_{\mathrm{pub}}+a_1P)/(a_2+r_2)=(P_{\mathrm{pub}}+a_{1i}P)/(a_{2i}+r_2)$，将 $P_{\mathrm{pub}}=z\widehat{P}$ 代入可解出 z 值，这样 B 就解决了 q-SDH 问题的一个实例。　证毕

定理 4　在 ROM 下，如果 q-SDH 问题是难解的，则 IRBP 满足环签名的不可伪造性。

证明　假设存在一个 PPT 敌手 A 可以成功伪造一个环签名 $(c',U_1',U_2',R',T_1',T_2',\Pi_1',\Pi_2',s_1',\cdots,s_7')$，那么存在 PPT 算法 B 可以解决 q-SDH 问题。给定 q-SDH 问题的一个实例 $(\widehat{P},z\widehat{P},\cdots,z^q\widehat{P})$，$z\in_R Z_p^*$，$B$ 可以计算出 $(x,1/(z+x)\widehat{P})$，$x\in Z_p$。

首先，对于给定的安全参数 l，B 运行 SET-BP 生成系统参数 $\mathrm{params}=(l,e,P,t,f,g,G_1,G_2,K,Q,Q_{\mathrm{pub}},u,H_1)$，并将其发送给 A，其中 $t=(\widehat{P},P_{\mathrm{pub}}=z\widehat{P},\cdots,z^q\widehat{P})$，$H_1$ 作为随机预言。B 选择用户群 $U=\{\mathrm{id}_i\}_{i=1}^k$，运行 GPK-BP，生成环公钥 $\mathrm{gpk}=V$。对于身份信息为 id 的成员 u_{id}，B 可以通过 A 对消息 m 的伪造签名，计算出新的环私钥 $(h_{\mathrm{id}}^*,R_{\mathrm{id}}^*,W^*)$。$B$ 可以模拟 A 要访问的所有预言。

若 (h',S',W') 为 B 成功计算出的一个新环私钥，在这个过程中环公钥 V 始终保持不变，并且由环 $U=\{\mathrm{id}_i\}_{i=1}^k$ 很容易计算出 $X=\{h_i\}_{i=1}^k$，$h'\notin X$。据累加器的性质，有

$$(h'+z)W'=\prod_{i=1}^k(h_i+z)uP \tag{1}$$

令 $f(z)=\prod_{i=1}^k(h_i+z)$，可将 $f(z)$ 扩展为 $f(z)=\sum_{i=0}^k c_iz^i$，其中 $c_0\neq 0$。

由式(1)可得 $(h'+z)W'=uf(z)P$，即

$$\frac{1}{u}W'=\frac{f(z)}{h'+z}P \tag{2}$$

此时，可以将 $f(z)$ 表示为 $f(z)=a(z)(z+h')+r$，其中 $a(z)=a_0+a_1z+\cdots+a_{k-1}z^{k-1}$，$r\in Z_p^*$。则有 $\dfrac{f(z)}{h'+z}=a(z)+\dfrac{r}{h'+z}$。所以式(2)可表示为 $\dfrac{1}{u}W'=a(z)P+\dfrac{r}{h'+z}P$，也可表示为 $\dfrac{1}{z+h'}P=\dfrac{1}{ur}W'-\dfrac{a(z)}{r}P$。

因为 $P=\widehat{P}$，已知 q-SDH 问题的一个实例 $(\widehat{P},z\widehat{P},$

$\cdots, z^q\widehat{P})$)，则 $a(z)\widehat{P}$ 可解。代入上式可得 $(h', 1/urW' - a(z)/r\widehat{P})$ 为 q-SDH 问题的一个解。 证毕

5 结束语

本文在文献[7, 8]提出的签名长度固定的环签名方案概念基础上，对基于身份的 AD-hoc 匿名认证方案进行 Fiat-Shamir 转化，首次给出了签名长度固定的基于身份的环签名方案，并给出了方案的安全性证明。由于在很多情况下，环成员是固定不变的，因此对于同一个群体来说，签名者和验证者只需要计算一次相关的环密钥，就可以用其在以后的一段时间内生成其它的环签名。这将节省每次生成环签名时，计算环密钥的时间代价和存储代价。此外，签名长度固定的环签名方案在低带宽的情况下将更加适用。

本方案是对基于身份的AD-hoc匿名认证方案进行Fiat-Shamir 转化得来的，可以看出，转化后得到的签名方案仍比较复杂。如何构造形式简洁、安全高效的签名长度固定的环签名方案是下一步要继续研究的问题。此外，将签名长度固定的环签名方案用于可转移电子现金系统[13]，公平电子支票系统[14]及可传递签名[15]等也是我们感兴趣的研究问题。

参 考 文 献

[1] Rivest R, Shamir A, and Tauman Y. How to leak a secret. Advances in Cryptology-Asiacrypt'01, Gold Coast, Australia. Springer-Verlag, 2001, LNCS 2248, 552–565.

[2] Bresson E, Stern J, and Szydlo M. Threshold ring signatures for Ad-hoc Groups. Advances in Cryptology-Crypto'02, Santa Barbara, California, USA. Springer-Verlag, 2002, LNCS 2442, 465–480.

[3] Bellare M and Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols. First ACM Conference on Computer and Communications Security, Fairfax, Virginia, USA, ACM Press, 1993: 62–73.

[4] Zhang F G and Kim K. ID-based blind signature and ring signature from pairings. Advances in Cryptology –Asiacrypt'02, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, Springer-Verlag, 2002, LNCS 2501, 533–547.

[5] Shamir A. Identity based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, Santa Barbara, California, USA. Springer-Verlag, 1984. LNCS 196, 47–53.

[6] Boneh D and Franklin M. Identity based encryption from the Weil pairing. SIAM J. of Computing, 2003, 32(3): 586-615. Extended abstract in proceedings of Crypto '2001, Springer-Verlag. LNCS 2139, 213–229.

[7] Dodis Y, Kiayias A, and Nicolosi A, *et al.*. Anonymous identification in Ad Hoc groups. Eurocrypt'04, Interlaken, Switzerland, Springer-Verlag, 2004: 609–626.

[8] Nguyen L. Accumulator from bilinear pairings and application to ID-based ring signatures and group membership revocation. CT-RSA 2005, San Francisco, CA, USA, Springer-Verlag, 2005, LNCS 3376, 275–292.

[9] Fiat A and Shamir A. How to prove yourself: practical solutions to identification and signature problems. Crypto'86, Santa Barbara, California, USA, Springer-Verlag, 1987. LNCS 263, 186–194.

[10] Menezes A J, Okamoto T, and Vanstone S A. Reducing elliptic curve logarithms to a finite field. *IEEE Trans. on Info. Theory*, 1993, 39(5):1636–1646.

[11] Dutta R, Barua R, and Sarkar P. Pairing-based cryptographic protocols: a survey. http://eprint.iacr.org/2004/064.pdf, 2004.

[12] Pointcheval D and Stern J. Security proofs for signature schemes. Advanced in Cryptology – Eurocrypt'96. Springer-Verlag, 1996, LNCS 1070, 387–398.

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

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

[15] 张国印, 王玲玲, 马春光. 可传递签名研究综述, 计算机科学, 2007, 34(1): 6–11.
Zhang G Y, Wang L L, and Ma C G. Survey on transitive signature schemes. 2007, 34(1): 6–11.

王玲玲： 女，1982 年生，博士生，研究方向为密码学、网络与信息安全.

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.