一个公平的离线电子现金方案

蔡满春 赵海洋 马春光 杨义先
(北京邮电大学信息安全中心 国家重点实验室 北京 100876)

摘 要 基于双线性映射的群签名，设计了一个新的离线电子现金方案实现了公平性。该方案结构简单，可在椭圆曲线上实现，而且没采用传统的盲签名。该方案具有较高的安全性和效率以及无陷门的密码性质。

关键词 电子现金，公平性，双线性映射，群签名
中图分类号：TP393 **文献标识码**：A **文章编号**：1009-5896(2006)05-0820-03

A Fair Offline E-cash Scheme

Cai Man-chun Zhao Hai-yang Ma Chun-guang Yang Yi-xian
(*Information Center of Beijing Univ. of Posts and Telecommunications, Beijing* 100876, *China*)

Abstract Based on group signature scheme from bilinear pairings, a new offline fair cash scheme is presented. Because of setting up on the elliptic curve group and without using blind signature scheme , this scheme has many properties such as having simple structure, security, efficiency, trapdoor-free and so on.

Key words e-cash, fairness, bilinear pairings, group signatures

1 引言

群签名最早由Chaum和Van Heyst[1]提出，它允许群成员以群体的名义签名，而同时不会揭露签名者的信息和关联其他签名；当有争议时，指定的匿名撤销管理者又能打开签名和揭露签名者的信息。群签名也保证任何群成员和群管理者都不能仿造其他群成员的签名。由于群签名提供了用户的私有和匿名性，一些电子现金方案[2-4]引用了群签名。这些存在的方案以不同的方式使用群签名，在文献[2,3]中消费者作为群成员，同时在文献[2]中银行也作为群成员，在文献[4]中电子货币构成群。

普遍认为效率较高的利用群签名设计的电子现金[MB01][5]，利用了基于当时最有效的强RSA假设[ACJ00][6]签名方案实现一个消费者作为群成员的方案，但他们加入了盲签名用以实现匿名性和防止重复花费，因此结构比较复杂。

本文采用了基于双线性映射的群签名，设计了一个新的电子现金方案实现了公平性，与[MB01]比，本文采用的在椭圆曲线上的群签名，其160位的安全性相当于1024位的[MB01]用的强RSA假设[ACJ00]的安全性，而且本文的电子现金没采用盲签名，结构比[MB01]简单，效率更高。本文采用的群签名的公钥和签名长度与群成员的个数不相关，比较适合使用电子货币的消费者随时增加的实际情形。同时本文采用的群签名，没有RSA假设的陷门，便于群成员采用相同的系统参数，这点更适合真实世界，不同的成员和组织在匿名信任机制下交换大量信息而同时保证匿名性。

下面介绍本文设计的新的电子现金方案。

2004-09-17 收到，2005-01-24 改回
国家自然科学基金(90204017)资助课题

2 新的离线电子现金方案

新的离线公平电子现金方案是基于椭圆曲线上双线性映射的群签名而设计。本文对Lan Nguyen[7]提出的群签名做了一些改进，即本文在Lan Nguyen提出的群签名基础上引入一次性标记 P_i 及其验证，以适合本文设计的新电子现金方案。Lan Nguye提出的群签名在文献[7]中证明是安全的，本文改进群签名主要是加入约束条件来验证一次性标签，因而并不会使群签名的安全性降低。下面先给出双线性映射的概念描述。

双线性映射(Bilinear pairings)[7]：令 G_1，G_2 分别是 P_1, P_2 生成的 p 阶循环加群，G_M 是 p 阶循环乘法群。存在映射 ψ：$G_2 \to G_1$，使得 $\psi(P_2)=P_1$。若 e：$G_1 \times G_2 \to G_M$ 是一个双线性映射满足下面性质：

(a) 双线性 $P \in_R G_1$，$Q \in_R G_2$，$a,b \in_R Z_q$，都有 $e(aP,bQ)=e(P,Q)^{ab}$。

(b) 非退化 $e(P_1,P_2)\neq 1$。

(c) 可计算性 对任意 $P \in G_1, Q \in G_2$，存在有效算法计算 $e(P,Q)$。

有时为了方便，可使 $G_1=G_2$，$P_1=P_2$。

本文设计的电子现金协议分这样几个步骤：

(1)系统建立(Set Up) 系统参与者有：作为群管理者的银行 B，成为群成员的消费者 C，一个作为匿名性撤销者的

可信第三方 P，商家 S 作为群签名的验证者。消费者 C 和商家 S 在银行处有各自的帐户，并可通过身份认证过程确认自己的身份。

选取一组双线性参数 (p,G_1,G_M,e,P)，其中 p 为素数，G_1 为由 P 生成的 p 阶循环加群，G_M 为 p 阶乘法群，$e:G_1\times G_1\to G_M$ 双线性映射。$H:\{0,1\}^*\to Z_p$ 为无碰撞的 hash 函数。选取 $P_0,G,H\in_R G_1$，$x,x'\in_R Z_p^*$，计算 $P_{\text{pub}}=xP$，$\theta=e(G,G)^{x'}$，其中群管理员银行 B 的公钥为 (P,P_0,P_{pub},H) 和密钥 x，群成员撤销管理员 P 的公钥为 (G,θ) 和密钥为 x'。

(2)取款阶段(Withdrawal)　消费者 C 从银行的取款过程，就是加入群、获得关系证书的过程。消费者 C 首先向银行 B 证明自己的身份，向银行提出取款申请，即加入群，包括下面过程：

(a) 消费者选取 $x_i\in_R Z_p^*$，计算 $P_i=x_iP$，再取 $n\in_R Z_p^*$。

(b) $C\to B$：$P_i'=\dfrac{1}{n}(P_i+P_0)$。

(c) $C\leftarrow B$：$\left(a_i,S_i'=\dfrac{1}{a_i+x}P_i'\right)$，其中 $a_i\in_R Z_p^*$。

(d) C 计算 $S_i=n\cdot S_i'=\dfrac{1}{a_i+x}(P_i+P_0)$，并验证 $e(a_iP+P_{\text{pub}},S_i)\stackrel{?}{=}e(P_i+P_0,P)$，如验证通过，进行下一步。

(e) $C\to B$：S_i，nP。

(f)　B 验证 $e(S_i,P)=e(S_i',nP)$，如验证通过则记 $\Delta_i=e(S_i,P)$，并在数据库中记录 (C, Δ_i，a_i，S_i，S_i', nP, Jointranscript)，再将消费者帐户余额通知消费者。消费者 C 验证余额正确，保存自己的证书 (a_i,S_i), (x_i,P_i) 和 Δ_i。

(3)支付阶段(Payment)　消费者向商家的支付过程，就是交给商家一个群签名，即证明自己有一个合法关系证书 (a_i,S_i), (x_i,P_i) 的过程。为了能够检测出重复花费者的身份，群签名应该是一次性的，即如果同一证书使用两次将被发现。同时也为了区别消费者和商家中谁进行的重复花费，群签名加入只有消费者 C 才知道的秘密信息 P_i，并证明它的正确性。消费者 C 先选择 $t\in_R Z_p^*$，计算 $E=tG$，$\Lambda=\Delta_i\theta^{-t}$。

下面是对购物信息 m 的签名过程：

(a) 消费者 C 选择 $r_1,\cdots,r_3,k_0,\cdots,k_5\in_R Z_p^*$ 且 $k_2=r_1\cdot r_2$，计算：$U=r_1(a_iP+P_{\text{pub}})$，$V=r_2S_i$，$W=r_1r_2(x_iP+P_0)$，$X=r_2U+r_3H$，$T_1=k_1P+k_2P_{\text{pub}}+k_0H$，$T_2=k_3P+k_2P_0$，$T_3=k_4U+k_0H$，$T_4=k_5G-K_4E$，$T_5=k_3P-k_2P_i$，$\Pi=\theta^{k_5}\Lambda^{k_4}$。

(b) C 计算

$$c=H(P\|P_0\|P_{\text{pub}}\|H\|G\|P_i\|\theta\|\Lambda\ \|E\|U\|V\|T_1\|\cdots\|T_5\|\Pi\|m)$$

(c) C 在 Z_p 中计算：$s_0=k_0+cr_3$，$s_1=k_1+cr_1r_2a_i$，$s_2=k_2+cr_1r_2$，$s_3=k_3+cr_1r_2x_i$，$s_4=k_4+cr_2$，$s_5=k_5+cr_2t$。

(d) C 提交电子现金给商家，即输出对 m 的签名 $(c,s_0,\cdots,s_5,P_i,U,V,W,X,E,\Lambda)$。

商家验证过程：

(a) 商家计算：$N_1=s_1P+s_2P_{\text{pub}}+s_0H-cX$，$N_2=s_3P+s_2P_0-cW$，$N_3=s_4V+s_0H-cX$，$N_4=s_5G-s_4E$，$N_5=s_3P-s_2P_i$，$\Pi'=\theta^{s_5}\Lambda^{s_4}(e(cV,P))^{-1}$。

(b) 商家验证 $N_2-N_5\stackrel{?}{=}W$，$e(U,V)\stackrel{?}{=}e(W,P)$，$c\stackrel{?}{=}H(P\|P_0\|P_{\text{pub}}\|H\|G\|P_i\|\theta\|\Lambda\ \|E\|U\|V\|N_1\|\cdots\|N_5\|\Pi'\|m)$

如果上面条件都成立，则商家接受此签名，将货物发送给消费者。

(4)存款阶段(Deposit)　存款过程就是商家 S 将群签名交给银行 B，银行验证正确性并检查是否重复花费的过程。商家将在支付协议中得到 m 的群签名 $(c,s_0,\cdots,s_5,P_i,U,V,W,X,E,\Lambda)$ 交给银行。银行首先验证 P_i 是否与已有的存款记录中的 P_i 相同，如有相同者，再检查其他项是否相同，如都相同则说明商家企图重复花费；如果只有 P_i 相同，则说明消费者企图重复花费，银行请求可信第三方(匿名性撤销者)P 确认该消费者的身份；如果 P_i 没有相同者，则银行像商家在支付协议中所作的一样，验证群签名的正确性，如通过，则在商家的帐户上增加一项，并记录该群签名，将帐户金额通知商家。

(5)身份恢复(Identity Revocation)　匿名性撤销者 P 因为知道密钥 x'，所以能够计算 $\Delta_i=\Lambda e(E,G)^{x'}$，从而可以确定用户身份。对于钱币(coin)跟踪，即从取款者身份到存款记录的跟踪，以及对于所有者跟踪，即从存款记录到取款记录的跟踪，只要匿名性撤销者 P 和银行的取款记录比较 Δ_i，就可得到取款者身份 C。

3 新方案的性能分析

以下证明基于El Gamal公钥体系的双线性映射以及Diffie-Hellman假设[7]，证明大都是基于群签名方案的性质。

(1)　正确性　取款阶段银行签名的可验证性如下：

$e(a_iP+P_{\text{pub}},S_i)=e(P_i+P_0,P)$ 成立，这是因为

$$e(a_iP+P_{\text{pub}},S_i)=e\left(a_iP+xP,\frac{1}{a_i+x}(p_i+P_0)\right)$$

$$=e(P,P_i+P_0)^{(a_i+x)\cdot\frac{1}{a_i+x}}=e(P_i+P_0,P)$$

支付过程中消费者所作的群签名的可验证性如下：

$$N_1=s_1P+s_2P_{\text{pub}}+s_0H-cX$$
$$=(k_1+cr_1r_2a_i)P+(k_2+cr_1r_2)xP+(k_0+cr_3)H$$
$$-c(r_2(r_1(a_iP+P_{\text{pub}}))+r_3H)=T_1$$

同理，$N_2=s_3P+s_2P_0-cW=T_2$，$N_3=s_4V+s_0H-cX=T_3$

$N_4=s_5G-s_4E=T_4$，$N_5=s_3P-s_2P_i=T_5$

$$\Pi' = \theta^{s_5} \Lambda^{s_4} \ (e(cV,P))^{-1} = \Pi$$

(2)不可伪造性　由于不知道银行的密钥 x，由q-SDH假定[7]，用户不能伪造银行 $S_i, S_i^{'}$；由于群签名是零知识证明，不会泄漏关于证书的知识，所以商家不能伪造用户的群签名；由于群签名的无陷害性质，银行也不能伪造消费者的群签名；再由于重复花费的可检查性，因此系统不能存在one-more伪造。

(3)匿名性　由于群签名的匿名性质，所以商家不知道消费者的身份，银行也不能将存款记录和取款记录联系起来。即使商家和银行合谋也不能确定消费者身份。

(4)检测重复花费和可撤销匿名性　消费者C不能重复花费，也就是C只能用一个群成员证书进行唯一的有效签名，这是因为 $P_i = x_i P$ 包含用户C的秘密信息，成为签名的唯一标志。并且，C在签名时，也不可能构造一个 $P_i' = lP_i$ 代替 P_i，这是由于 $e(U,V) = (W,P)$ 以及验证者所知的 N_2 的表达式等，W 一定是 $t(x_i P + P_0)$ 形式。若假定 $T_5 = k_3 P - k_2 P_i' = k_3 P - k_2 l P_i$，因 $W = T_2 - T_5 = k_2(lP_i + P_0)$，故只能 $l = 1$，说明C签名时构造一个 $P_i^{'} = lP_i$ 代替 P_i 是不可能的，不能重复花费。

可信第三方(匿名性撤销者)因为知道密钥 x'，所以能够计算 $\Delta_i = \Lambda e(E,G)^{x'}$，通过与数据库中的$(C, \Delta_i, a_i, S_i, S_i^{'}, nP$, Jointranscript)比较，就能揭露重复花费的消费者的身份，撤销匿名性。

(5)关于银行的非法行为　首先，由于群签名的无陷害特性，即使银行与其他成员合谋，也不能以取款协议中的消费者名义进行群签名，故银行不能盗用用户的钱币；其次，我们可使银行不能诬陷消费者取过钱：类似实际的从存折中取款过程，在取款时用户提交一个有自己签名的取款申请，说明取多少钱。取款之后银行将发给消费者一个有自己签名的余额记录，消费者检查正确性。但银行的后一种行为将严重影响银行的信誉，因此一般情况下不会发生，这种签名交换过程是一种可选项。

(6)效率　同[MB01]比，本文采用的在椭圆曲线上的群签名，其160位的安全性相当于1024位的[MB01]用的强RSA假设[ACJ00]的安全性，其规模大小相当于[ACJ00]的1/3 [7]，并且由于[MB01]在群签名中使用了盲签名，因此与本文方案效率比，低得多。

4　结束语

本文采用了基于双线性映射的群签名，设计了一个新的电子现金方案实现了公平性，由于本文采用的群签名建立在椭圆曲线上，其 160 位的安全性相当于 1024 位的强 RSA 假设的安全性，双线性映射也具有较高的知识证明的效率，而且没采用盲签名，结构简单，本方案具有较高的安全性和效率。而且本文采用的群签名的公钥和签名长度与群成员的个数不相关，比较适合使用电子货币的消费者随时增加的实际情形。同时本文采用的群签名，没有 RSA 假设的陷门，便于群成员采用相同的系统参数，这点更适合真实世界，不同的成员和组织在匿名信任机制下交换大量信息而同时保证匿名性。然而，本文方案像所有的一次性消费电子现金一样，每次花费时需从银行提取货币，实际应用中存在效率问题；以及如何增加较小的信息冗余度的情况下使得现金实现找零和再次花费，都是我们今后设计电子现金进一步研究的问题。

参 考 文 献

[1] Chaum D, Van Heyst E. Group signatures. CRYPTO 1991, LNCS 547, Springer-Verlag，1991: 410 – 424.

[2] Lysyanslaya A, Ramazan Z. Group blind digital signature: A scalable solution to electronic cash. In Financial Cryptography, Second International Conference, FC’98, LNCS 1465, Springer-Verlag, 1998: 184 – 197.

[3] Traore Jacques. Group signatures and their relevance to privacy-protecting off-line electronic cash systems. In Australasian Confererce on Information Security and Privacy (ACISP’99)， LNCS 1587. Springer-Verlag, 1999: 228 – 243.

[4] Nakanishi Toru, Haruna Nobuaki, Sugiyama Yuji. Unlinkable electronic coupon protocol with anomymity control. On International Workshop on Information Security (ISW’99), LNCS 1729: 1999: 37 – 46.

[5] Mailland G, Boyd C. Fair electronic cash based on a group signature scheme, Tech. Report, Queensland University of Technology, Australia, 2001.

[6] Ateniese G, Camenisch J, Joye M, *et al*.. A practical and provably secure coalition-resistant group signature scheme, Crypto’00: 204 – 216 .http://citeseer.ist.psu.edu/cache/papers/cs/21124/http:zSzzSzwww.zurich.ibm.comzSz~jcazSzpaperszSzgroup2000.pdf/ateniese00practical.pdf.

[7] Nguyen Lan. A trapdoor-free and efficient group signature scheme from bilinear pairings. http://eprint. iacr.org/2004/104.pdf.

蔡满春： 男，1972 年生, 博士生，研究方向为密码学、网络安全、电子商务.

赵海洋： 男，1978 年生, 博士生，研究方向为计算机通信、信息安全技术.

马春光： 男，1974 年生, 博士生，研究方向为密码学、网络安全、电子商务.

杨义先： 男，1961 年生, 教授，博士生导师，主要研究方向为密码学、通信网络、 信息安全技术.