doi:10.11959/j.issn.1000-436x.2016107

基于无证书群签名方案的电子现金系统

梁艳，张筱，郑志明
（北京航空航天大学数学与系统科学学院，北京 100191）

摘 要：在经典方案 ACJT 群签名方案的基础上，提出了一种基于椭圆曲线的前向安全的成员可撤销无证书群签名方案，改进了 ACJT 计算复杂、参数较多、签名较长的不足，减小了计算量及参数个数，缩短了签名长度，提高了方案效率，并基于此群签名方案构建了一个离线公平高效的多银行电子现金系统，该电子现金系统不仅继承了群签名方案的安全性、高效性，还实现了不可伪造性、防止多重支付、防止金额篡改等多种性质，较同类方案具有明显优势。

关键词：椭圆曲线；无证书签名；前向安全；成员撤销；群签名；电子现金
中图分类号：TP309 **文献标识码：**A

Electronic cash system based on certificateless group signature

LIANG Yan, ZHANG Xiao, ZHENG Zhi-ming
(School of Mathematics and Systems Science, Beihang University, Beijing 100191, China)

Abstract: An efficient elliptic certificateless group signature ith forward security and member revocation based on ACJT group signature was proposed. Compared to ACJT which has complex computation, many parameters and long signature length, proposed scheme has less parameters and only involve a small amount of computation. The length of proposed signature is short and the efficiency is high. A fair off-line multi-bank e-cash system based on this group signature scheme was also proposed. The new e-cash system has not only the high security and efficiency, but the unforgeability.It also can avoid double-spending and tampering money. The scheme has a clear advantage compared with others.

Key words: elliptic curve, certificateless signature, forward security, member revocation, group signature, electronic cash

1 引言

随着互联网技术以及电子商务的快速发展，电子现金系统作为一种重要的支付手段，在现代生活中起到了日益重要的作用。构建离线公平的多银行电子现金系统是目前的主要目标，而如何在实现系统高效运转从而达到快捷支付，同时减少系统漏洞，防范信息伪造、多重支付、金额篡改等可能的网络经济犯罪行为是电子现金系统的发展瓶颈及研究热点。电子现金系统主要通过密码基础协议进行构建，数字签名是系统的技术支持与保障，构建高效安全的电子现金系统关键在于设计良好的密码协议，在降低计算复杂度的同时实现电子现金系统的实用性。

第一个电子现金系统是由 David Chaum 于 1982 年利用群盲签名构造而成[1]的，自此之后，基于不同数字签名技术的电子现金系统被相继提出，自 2000 年，群签名[2]中的经典方案 ACJT[3]被提出后，基于群签名的电子现金系统得以充分发展，由于群签名所具有的良好密码特性，如匿名性、匿名可撤销性、不可链接性、不可伪造性等，并且 ACJT 是首个实用性较强且可抵抗多种攻击的可证安全的群签名方案，所以，ACJT 在电子现金系统及其他领域有着广泛的应用，之后许多基于 ACJT 群签名方案的电子现金系统被相继提出[4~8]，但都存在

收稿日期：2015-07-09；修回日期：2016-01-21
通信作者：张筱，09621@buaa.edu.cn
基金项目：国家自然科学基金资助项目（No.11290141, No.61402030）；民机专项基金资助项目（No.MJ-F-2012-04）
Foundation Items: The National Natural Science Foundation of China (No.11290141, No.61402030); Foundational Research of Civil Aircraft (No.MJ-F-2012-04)

一些不足，比如不能防止金额篡改、实现效率较低等。如何构建基于群签名的高效安全的电子现金系统仍然是目前研究的重点。

电子现金系统的安全性及效率依托于其中所用到的数字签名技术，为更好地建立电子现金系统，需对其中所用的签名方案进行改进，由于 ACJT 是基于群签名的电子现金系统中常用的方案，如何对其改进以构建更高效安全的电子现金系统具有重要的研究价值与意义，自 ACJT 提出以来，学者们提出了许多对该方案的改进。针对 ACJT 中不具备成员撤销功能这一最主要的缺陷，学者们通过不同方法构建了成员可撤销的 ACJT 群签名方案，Song 等[9]提出的 2 个成员撤销方案中，方案计算量较大并且验证算法线性依赖于被撤销的成员个数，方案效率较低。Toru 等[10]提出的成员撤销方案中，由于方案引入动态累加器进行成员撤销，使方案计算量较大、效率同样较低。陈泽文等[11]通过引入乘积互素的零知识证明的方法设计了高效的可实现成员撤销的方案，但其方案中成员证书线性依赖于成员个数，不仅增加了计算量而且不适用于大群体。为使 ACJT 能够实现更高的安全性，Zhang 等[12]提出了一个新的支持成员撤销的前向安全群签名方案，虽然效率较高，但被证明是不安全的[13]。肖平安等[14]从克服 ACJT 方案防陷害性不高的方面进行改进，方案同样未考虑效率问题。

本文在近几年对 ACJT 方案[15~25]改进的启发下，设计了一个基于椭圆曲线的前向安全的成员可撤销无证书群签名方案，基于此方案构建的电子现金系统不仅继承了群签名方案的安全性、高效性，还是一个公平离线的多银行系统，并实现了不可伪造性、防止多重支付及防止金额篡改等多种实用性质。

2　设计原理及特点

为构建高效安全的电子现金系统，实现其在快捷支付的同时防范某些网络经济犯罪行为，本文将群签名与电子现金系统相结合，通过分析改进对群签名方案进行重新设计并利用该方案建立一个合理的电子现金系统，该群签名方案主要从以下几个方面进行设计。

1) 方案建立椭圆曲线模型，通过椭圆曲线上的点乘、点加等运算实现了整个方案的运行，提高了方案效率。由于椭圆曲线上的离散对数问题比标准的离散对数问题更加困难，并且从已知的最好求解方法来看，160 bit 的椭圆曲线密码算法的安全性相当于 1 024 bit 的 RSA 算法，所以椭圆曲线密码算法可以用更短小的密钥实现较高的安全性。方案通过重新设计并选择不同参数，克服了 ACJT 中模乘、模幂等运算计算复杂、计算量大的缺点，减少了运行过程中所用的参量个数，并且最终缩短了签名长度及整个方案运行的总时间。表 1 给出了本文方案与 ACJT 方案的对比。

2) 方案将无证书签名思想与群签名相结合，设计无证书签名算法简化了成员加入过程。A 在加入过程中使用部分密钥直接做出签名并发送给群管理员 GM 进行验证，实现了 A 与 GM 的一次交互认证。KGC 通过计算 $R_A=r_AP, s_A=r_A+xH(ID_A\|P_A\|R_A)$ 产生 A 的相应密钥。在成员加入过程，A 使用部分密钥对签名公钥做知识签名，产生 $(h_{A,i}, s_{A,i})$，并将 $(ID_A, Y_{A,i}, h_{A,i}, s_{A,i})$ 发送给 GM，GM 不直接从 A 处而是从 KGC 处获取 A 的部分公钥，对 A 发送的签名进行认证，既证明了 A 身份的合法性，也抵抗了公钥替换攻击。

3) 方案引入前向安全性，减小了密钥泄露带来的危害，提高了系统安全性。方案将系统时间进行分段，成员 A 第 i 时段的签名密钥 $x_{A,i}$ 通过安全算法 $x_{A,i+1}=x_{A,i}^{2^T+r} \bmod(q-1)$ 进行更新，在不增加系统计算量的同时使成员信息均得到更新，减小了系统负担。并且在最后生成的群签名 $(c, s_1, s_2, s_3, s_4, T_{A,i}, T_2, i)$ 中还加入了时段信息 i，使签名更具实时性，便于验证。

4) 方案加入了成员撤销算法，弥补了 ACJT 群签名方案的一大缺陷。方案中 KGC 及 GM 通过维护成员撤销列表的方式实现了群成员的高效安全撤离。当系统进入下一时段，KGC 及 GM 处存储的成员信息均会得到更新。

表 1　本文方案与 ACJT 方案对比

方案名称	群公钥参数个数	群公钥长度/bit	签名过程参数个数	签名长度/bit	签名、验证及打开算法总时间/ms
ACJT 方案	6	6 144	13	8 192	45 840
本文方案	2	320	11	1 136	43.21

3 高效的无证书群签名方案

本文所设计的群签名方案具体包括以下步骤：系统初始化、群管理员及群成员部分密钥提取、成员加入、签名、验证及打开、系统更新、成员撤销。设 F_q 是阶为 q 的有限域，椭圆曲线 E 为 $y^2=x^3+ax+b$，其中，$a,b\in F_q$ 并且满足 $\Delta=4a^3+27b^2\neq 0$。$P\in E(F_q)$ 是该椭圆曲线的生成元，它的阶为素数 $n, n>2^{160}$。

3.1 系统初始化

系统安全参数为 $k\in N$，选取安全的散列函数 $H:\{0,1\}^*\to Z_p$。KGC 秘密选择 $x\in Z_q^*$，计算 $P_{\text{pub}}=xP$。KGC 公钥为 P_{pub}，系统主密钥为 x，系统参数为 $(F_q,\frac{E}{F_q},q,P,P_{\text{pub}},H)$。

3.2 群管理员 GM 及群成员 A 部分密钥提取

群管理员 GM 的身份信息为 ID_{GM}，该密钥提取过程简记为 $Ext(\text{GM})$。GM 首先随机选取 $x_{\text{GM}}\in Z_q^*$ 作为其秘密值，计算 $P_{\text{GM}}=x_{\text{GM}}P$，将 $(ID_{\text{GM}},P_{\text{GM}})$ 发送给 KGC；KGC 随机选取 $r_{\text{GM}}\in Z_q^*$，计算 $R_{\text{GM}}=r_{\text{GM}}P, s_{\text{GM}}=r_{\text{GM}}+xH(ID_{\text{GM}}\|P_{\text{GM}}\|R_{\text{GM}})$，并将 $(R_{\text{GM}},s_{\text{GM}})$ 通过安全信道发送给 GM；GM 验证等式 $s_{\text{GM}}P=R_{\text{GM}}+P_{\text{pub}}H(ID_{\text{GM}}\|P_{\text{GM}}\|R_{\text{GM}})$ 是否成立，若成立，则接受部分密钥 s_{GM}，KGC 存储相应的信息 $(ID_{\text{GM}},P_{\text{GM}},S_{\text{GM}},s_{\text{GM}})$，并将 GM 公钥列入公开公钥表中。此时 GM 形成私钥对 $SK_{\text{GM}}=(x_{\text{GM}},s_{\text{GM}})$，相应的公钥对为 $PK_{\text{GM}}=(x_{\text{GM}}P,s_{\text{GM}}P)=(P_{\text{GM}},S_{\text{GM}})$。

群成员 A 的身份信息为 ID_A，该密钥提取过程简记为 $Ext(A)$。A 通过该过程私钥对 $SK_A=(x_A,s_A)$，相应的公钥对为 $PK_A=(P_A,S_A)$。

3.3 成员加入

当群成员 A 要加入群时，GM 生成签名有效期 T，设当前系统所处时段为 i，该成员加入过程简记为 $Join_{\text{GM}}(A)$。A 随机选取 $x_{A,i}\in Z_q^*$，计算 $Y_{A,i}=x_{A,i}P$，再随机选取 $u\in Z_q^*$，计算 $t=uP, h_{A,i}=H(ID_A\|PK_A\|Y_{A,i}\|t\|T), s_{A,i}=u-h_{A,i}SK_A=u-h_{A,i}(x_A+s_A)$。将 $(ID_A,Y_{A,i},h_{A,i},s_{A,i})$ 通过安全信道发送给 GM；GM 将 ID_A 发送给 KGC，KGC 将 A 对应的公钥 $PK_A=(P_A,S_A)$ 发送给 GM，GM 计算 $t'=s_{A,i}P+h_{A,i}PK_A=s_{A,i}P+h_{A,i}(P_A+S_A)$，验证等式 $h'_{A,i}=H(ID_A\|PK_A\|Y_{A,i}\|t'\|T)=h_{A,i}$ 是否成立，若成立，则为 A 生成成员证书。GM 随机选取 $e_A\in Z_q^*$，计算 $E_{A,i}=(SK_{\text{GM}}+Y_{A,i})e_A^{-1}$，并将 $(E_{A,i},e_A,PK_{\text{GM}})$ 发送给 A，同时将 $(ID_A,PK_A,Y_{A,i},E_{A,i},e_A,h_{A,i},s_{A,i})$ 存储到群成员信息列表中；A 验证 PK_{GM} 是否存在于 KGC 公开的公钥表中及等式 $E_{A,i}e_AP=PK_{\text{GM}}+PY_{A,i}$ 是否成立。

3.4 签名

该签名过程简记为 $Sig_A(m)$。A 随机选取 $w\in Z_q^*$，计算 $T_{A,i}=PE_{A,i}+wPPK_{\text{GM}}, T_2=wP$；随机选择 $r_1,r_2,r_3\in Z_q^*$，计算 $d_1=r_1T_{A,i}-r_2PPK_{\text{GM}}$，$d_2=r_1T_2-r_2P, d_3=r_3P, d_4=r_4T_2$，$c=H(Y_{A,i}\|PK_{\text{GM}}\|T_{A,i}\|T_2\|d_1\|d_2\|d_3\|d_4\|m\|i)$，$s_1=r_1-ce_A$，$s_2=r_2-ce_Aw, s_3=r_3-cw, s_4=r_4-cx_{A,i}w^{-1}$；输出签名为 $(c,s_1,s_2,s_3,s_4,T_{A,i},T_2,i)$。

3.5 验证及打开

验证过程简记为 $Verify_A(m)$。计算

$$c'=H(Y_{A,i}\|PK_{\text{GM}}\|T_{A,i}\|T_2\|c(PK_{\text{GM}}+PY_{A,i})+s_1T_{A,i}-s_2PPK_{\text{GM}}\|s_1T_2-s_2P\|cT_2+s_3P\|cY_{A,i}+s_4T_2\|m\|i)$$

当且仅当 $c=c'$ 时接受签名。

打开过程简记为 $Open(A)$。A 将 $T'_{A,i}=E_{A,i}+wPK_{\text{GM}}$ 发送给 GM；GM 通过私钥计算 $E_{A,i}=T'_{A,i}-SK_{\text{GM}}T_2$ 恢复 $E_{A,i}$，证明 $\frac{PK_{\text{GM}}}{P}=\frac{T'_{A,i}-E_{A,i}}{T_2}$。

3.6 系统更新

当系统从第 i 时段进入第 $i+1$ 时段时，系统信息更新，系统更新过程简记为 $Update(A)$。A 计算 $x_{A,i+1}=x_{A,i}^{2^T+r}\bmod(q-1), r\in Z_q^*$；GM 更新所存储的成员信息 $(ID_A,PK_A,Y_{A,i+1},E_{A,i+1},e_A,h_{A,i+1},s_{A,i+1})$。

3.7 成员撤销

若需撤销第 j 时段成员 A 的信息，该成员撤销过程简介为 $Revoke(A)$，则 GM 将其对应的信息 $(ID_A,PK_A,Y_{A,j},E_{A,j},e_A,h_{A,j},s_{A,j})$ 存储到内部撤销列表中，将部分信息 $(PK_A,Y_{A,j},T_{A,j},T_2,j)$ 存储到公开撤销列表中，并将成员撤销信息发送给 KGC；KGC 将 A 所对应的信息存储到内部撤销列表中。

4 离线公平多银行电子现金系统

银行电子现金系统的主要步骤如下。

4.1　开户协议

设当前所处时段为 i，发币行 B_i 生成有效期 T。用户 U_i 的身份信息为 ID_U，私钥对 $SK_U=(x_U,s_U)$，公钥对 $PK_U=(P_U,S_U)$，随机选取 $x_{U,i}\in Z_q^*$，计算 $Y_{U,i}=x_{U,i}P$；U_i 通过 $Join_{B_i}(U_i)$ 过程获得成员证书 $(E_{U,i},e_U)$，发币行 B_i 存储 $(ID_U,PK_U,\ Y_{U,i},E_{U,i},e_U,h_{U,i},s_{U,i})$。

4.2　取款协议

用户 U_i 以取款金额 m 作为签名信息，通过 $Sig_{U_i}(m)$ 过程，产生群签名 $(c,s_1,s_2,s_3,s_4,T_{U,i},T_2,i)$，并且计算 $T'_{U,i}=E_{U,i}+wPK_{B_i}$，将取款请求 req，及 $T'_{U,i}\ (c,s_1,s_2,s_3,s_4,T_{U,i},T_2,i),T'_{U,i},Y_{U,i},PK_{B_i},m$，全部发送给交易银行 B_j；B_j 查看 PK_{Bi} 是否存在于中央银行 B 公布的公钥列表中及通过 $Verify_{U_i}(m)$ 过程验证签名是否合法；分行 B_j 对交易金额 m 产生序列号 m_time，记 $M=(m,m\_time,T_{U,i},T_2)$。B_j 随机选取 $v\in Z_q^*$，计算 $t_2=vP,h_{i2}=H(PK_{B_j}\|M\|t_2\|T\|i),s_{i2}=v-h_{i2}SK_{B_j}$，将 $(m,m\_time,h_{i2},s_{i2},PK_{B_j})$ 通过安全信道发送给 U_i；U_i 计算 $t'_2=s_{i2}P+h_{i2}PK_{B_j}$，验证等式 $h'_{i2}=H(PK_{B_j}\|M\|t'_2\|T\|i)=h_{i2}$ 是否成立。

4.3　支付协议

设当前系统处于第 j 时段，用户将 $(c,s_1,s_2,s_3,s_4,T_{U,i},T_2,i),h_{i2},s_{i2},T'_{U,i},m',Y_{U,i},PK_{B_i},PK_{B_j}$ 发送给商家；商家验证电子现金有效期、成员是否被撤销及通过 $Verify_{U_i}(m)$ 验证群签名是否正确，最后验证银行对电子现金的认证签名是否成立，计算 $t'_2=s_{i2}P+h_{i2}PK_{B_j}$，验证等式 $h'_{i2}=H(PK_{B_j}\|M\|t'_2\|T\|i)=h_{i2}$ 是否成立，若成立，则产生交易时间 pay_time。

4.4　存款协议

商家 D_i 将所有信息 $(c,s_1,s_2,s_3,s_4,\ T_{U,i},T_2,i),h_{i2},s_{i2},\ T'_{U,i},m',Y_{U,i},PK_{B_i},PK_{B_j},pay\_time$ 全部发送给分行 B_l，记当前处于第 k 时段；分行 B_l 验证电子现金有效期、用户和商家身份是否被撤销、商家是否存在非法行为。若验证通过，则分行 B_l 将金额 m 存入商家账户。

4.5　用户追踪

验证时，若有一项验证未通过，则验证者可将用户对应信息中的 PK_{B_i} 发送给中央银行 B，中央银行查找其发币行，由其发币行根据群签名及 $T'_{U,i}$ 打开其身份信息，实现对用户的追踪，对其所持有的电子现金进行标注，记录在非法现金库中，不从用户账户上扣除 m。

图 1 所示为成员加入过程，图 2 所示为签名及验证过程。

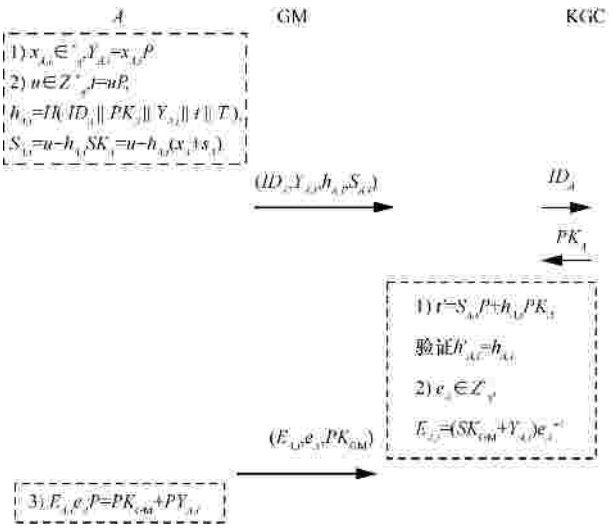

图 1　成员加入过程

图 2　签名及验证过程

5　方案分析

该部分主要对上述群签名方案及电子现金系统的正确性、安全性及效率做相应分析。

5.1　群签名方案分析

5.1.1　正确性

1) KGC 分发部分密钥时签名的正确性

群成员 A 在收到 (R_A,s_A) 之后，验证等式 $s_AP=R_A+P_{\text{pub}}H(ID_A\|P_A\|R_A)$ 是否成立。由于 $s_AP=r_AP+xPH(ID_A\|P_A\|R_A)=R_A+P_{\text{pub}}H(ID_A\|P_A\|R_A)$，所以验证过程与签名产生过程算法一致，且仅用到群成员 A 所拥有的信息，在保证 KGC 密钥安全的情况下完成了验证过程，原签名方案满足正确性。

同理，群成员 GM 在收到 $(R_{\text{GM}},s_{\text{GM}})$ 之后，验证等式 $s_{\text{GM}}P=R_{\text{GM}}+P_{\text{pub}}H(ID_{\text{GM}}\|P_{\text{GM}}\|R_{\text{GM}})$ 是否成立。由于 $s_{\text{GM}}P=r_{\text{GM}}P+xPH(ID_{\text{GM}}\|P_{\text{GM}}\|R_{\text{GM}})=R_{\text{GM}}+P_{\text{pub}}H(ID_{\text{GM}}\|P_{\text{GM}}\|R_{\text{GM}})$，所以原签名方案满

足正确性。

2) 成员加入过程签名的正确性

GM 在得到信息 $(ID_A, Y_{A,i}, h_{A,i}, s_{A,i}, PK_A)$ 之后，若 $(h_{A,i}, s_{A,i})$ 为合法签名，则有 $s_{A,i}P + h_{A,i}PK_A = (u - SK_A h_{A,i})P + h_{A,i}PK_A = uP = t$，GM 通过 A 发送的信息计算得出的 $t' = t$，利用 t' 再计算 $h'_{A,i} = H(ID_A \| PK_A \| Y_{A,i} \| t' \| T)$，则 $h'_{A,i} = h_{A,i}$，通过此等式，GM 得出原签名是有效的，即用户身份合法。从而签名产生及验证过程的算法是正确的。

3) 群签名的正确性

若 $(c, s_1, s_2, s_3, s_4, T_{A,i}, T_2, i)$ 为合法签名，则有

$$c(PK_{\mathrm{GM}} + PY_{A,i}) + s_1 T_{A,i} - s_2 PPK_{\mathrm{GM}} = c(PK_{\mathrm{GM}} + PY_{A,i}) + (r_1 - ce_A)(PE_{A,i} + wPPK_{\mathrm{GM}}) - (r_2 - ce_A w)PPK_{\mathrm{GM}} = d_1$$

$$s_1 T_2 - s_2 P = (r_1 - ce_A)wP - (r_2 - ce_A w)P = r_1 wP - r_2 P = d_2$$

$$cT_2 + s_3 P = cwP + (r_3 - cw)P = r_3 P = d_3$$

$$cY_{A,i} + s_4 T_2 = cY_{A,i} + (r_4 - cx_{A,i} w^{-1})wp = r_4 wp = d_4$$

当签名有效时，上述式子均成立，则验证者通过已有及公开信息计算得 $c' = H(Y_{A,i} \| PK_{\mathrm{GM}} \| T_{A,i} \| T_2 \| c(PK_{\mathrm{GM}} + PY_{A,i}) + s_1 T_{A,i} - s_2 \cdot PK_{\mathrm{GM}} \| s_1 T_2 - s_2 P \| cT_2 + s_3 P \| cY_{A,i} + s_4 T_2 \| m \| i) = H(Y_{A,i} \| PK_{GM} \| T_{A,i} \| T_2 \| d_1 \| d_2 \| d_3 \| d_4 \| m \| i) = c$，所以签名的验证算法是正确的。

5.1.2 不可伪造性

在无证书签名体制[26]中，定义存在 2 类拥有不同能力的敌手，分别为第 Ⅰ 类敌手和第 Ⅱ 类敌手，第 Ⅰ 类敌手进行公钥替换攻击，第 Ⅱ 类敌手进行恶意 KGC 攻击。

1) 第 Ⅰ 类敌手—公钥替换攻击

敌手 A_1 知道除 x_A 之外的所有信息，当获知用户 P_A 之后，敌手 A_1 模拟用户与 KGC 交互过程，获得部分私钥 s_A，A_1 用自己的秘密值 x_{A_1} 代替用户秘密值，A_1 签名密钥为 (x_{A_1}, s_A)，A_1 用自己的公钥 (P_A, S_{A_1}) 替换原先用户的公钥 (P_A, S_A)。在成员加入阶段，A_1 产生签名密钥 $x_{A_1,i}$，对 $Y_{A_1,i}$ 用 (x_{A_1}, s_A) 进行签名，并将 $(ID_A, h_{A_1,i}, s_{A_1,i})$ 发送给 GM 进行验证，由于 GM 需与 KGC 进行交互获得用户公钥，GM 计算 $t'_1 = s_{A_1,i}P + h_{A_1,i}PK_A$，验证 $h'_{A_1,i} = H(ID_A \| PK_{A_1} \| Y_{A_1,i} \| t'_1 \| T)$，显然 $h'_{A_1,i} \neq H(ID_A \| PK_{A_1} \| Y_{A_1,i} \| t'_1 | T)$，所以敌手伪造失败，方案可以抵抗公钥替换攻击。

2) 第 Ⅱ 类敌手—恶意的 KGC 攻击

敌手 A_2 进行恶意的 KGC 攻击，即知道 KGC 系统主密钥，但无法替换用户的公钥，当 A_2 知道用户公钥 (P_A, S_A)，由于椭圆曲线上离散对数的困难性，他将无法计算出用户秘密值 x_A，假设他伪造的用户私钥为 (x_{A_2}, s_A)，计算 $t_2 = uP, h_{A_2,i} = H(ID_A \| PK_A \| Y_{A_2,i} \| t_2 \| T), s_{A_2,i} = u - h_{A_2,i} SK_{A_2}$，GM 计算 $t'_2 = s_{A_2,i}P + h_{A_2,i}PK_A$，验证 $h'_{A_2,i} = H(ID_A \| PK_A \| Y_{A_2,i} \| t'_2 \| T)$，显然 $h'_{A_2,i} \neq H(ID_A \| PK_A \| Y_{A_2,i} \| t_2 \| T)$，所以敌手伪造失败，方案可以抵抗恶意的 KGC 攻击。

5.1.3 前向安全性

在方案更新过程中，使群成员 A 的签名密钥随时间更新，从而使其相应的公钥、证书及签名随之更新，并且若用户在当前时段被撤销，其之前的签名仍然有效，满足前向安全性。设群成员 A 当前所处时段为 j，其签名密钥为 $x_{A,j}$。若敌手得到该时段的签名密钥，则他无法伪造上一阶段的密钥，由密钥更新算法 $x_{A,i+1} = x_{A,i}^{2^T + r} \bmod(q-1)$ 得，求解前一阶段的密钥是基于求模 $q-1$ 的 $2^T + r$ 方根的难度，其困难性等价于因子分解问题，由于无法获得上一阶段的签名密钥，所以无法伪造成员证书，从而不能产生有效的群签名。

若敌手根据第 j 时段的签名密钥，伪造出第 $j+1$ 时段的签名密钥，则由于在成员加入过程中，需要 A 用自己的私钥 SK_A 对 $Y_{A,j}$ 进行签名，由于不知道 A 的私钥 SK_A，所以无法完成成员加入阶段的认证，也无法获得群成员证书，从而无法伪造正确的群签名。

5.1.4 效率分析

所提出的方案建立在椭圆曲线模型上，可以用更短小的密钥保持较高的安全性，从已知的最好求解方法来看，160 bit 的椭圆曲线密码算法的安全性相当于 1 024 bit 的 RSA 算法。

有限域上的模乘、模幂运算计算复杂度高，有限域上的加法等计算复杂度相对较低，可以忽略。只对复杂度较高的运算进行衡量，表 2 给出了本方案与 ACJT[3]、文献[9]及文献[27] 3 种方案的对比。

由文献[28]中方法，在 CPU:1.6 GHz，RAM：2.0 GB，使用 C++语言的环境下，实现指数运算的平均时间为 1 910 ms，实现群中的点乘运算，使用密钥长度为 160 bit 时，所需时间为 1.49 ms，

表 2　群签名方案对比

方案	模数大小/bit	Sign 计算量	Verify 计算量	Open 计算量	签名长度/bit	群公钥长度/bit	是否具有成员撤销过程	是否具有前向安全性
ACJT	≥1 024	12E+11M	11E+7M	1E+1M	8 192	6 144	×	×
文献[9]	≥1 024	20E+17M	(22+k)E+13M	2E+1M	7 168	6 144	v	v
文献[20]	≥1 024	12E+11M	11E+7M	1E+1M	9 232	6 144	v	v
本文方案	≥160	17C+7J	11C+6J	1C+1J	1 136	320	v	v

其中，E、M 分别表示有限域上模幂、模乘运算，C、J 表示椭圆曲线点乘、点加运算，k 表示被撤销的成员个数，“×”表示不具备该过程，“v”表示具备该过程。并且假定有限域 G 中元素为 1 024 bit，ECC 中元素为 160 bit，时间长度为 16 bit。

经过计算，实现 ACJT[3]、Song 方案 I [9]及 Shi 方案[27]3 种方案的签名、验证及打开过程的总时间分别为 45 840 ms、(84 080+1 910k) ms、45 840 ms，而本方案只需 43.21 ms 即可实现，相比之下效率显著提高。

5.2　电子现金系统分析

5.2.1　防止金额篡改和多重支付

在用户取款阶段，发币行发放电子现金，其中包括电子现金金额、序列号以及银行所做的认证签名，可在后续验证过程中进行查找，在电子现金库中也可以进行查找，从而确定用户是否存在多重支付行为，并确定用户或商家是否对金额有所篡改。在用户和商家交易的过程中，产生交易时间 pay_time，即对电子现金的又一重标记，可通过核对交易时间是否重复检验商家是否存在多重支付的行为。

5.2.2　方案对比

表 3 是本方案与其他基于 ACJT 群签名方案建立的电子现金系统 Zhang 方案[7]及 FEI 方案[8]的对比，由于该电子现金系统是根据前述的群签名方案设计而成，所以满足正确性及高效性。通过对比可知，本方案建立在椭圆曲线模型上，较之同类方案模数大小由 1 024 bit 减小为 160 bit，即通过更短小的密钥保证了较高的安全性；方案加入了成员撤销算法，成员可以自由地加入和撤离群体，更符合实际；方案实现了前向安全性，使电子现金系统中成员信息随时间进行更新，减少了密钥泄露带来的危害，提高了系统安全性；为防止一些网络经济犯罪行为，方案通过一定算法实现了防止金额篡改及防止多重支付的特点，弥补了同类方案的缺陷。

6　结束语

为了提高电子现金系统效率，实现快捷支付，防范信息伪造、多重支付、金额篡改等可能的网络经济犯罪行为，本文将群签名与电子现金系统相结合，构建了一个基于高效安全的群签名方案的电子现金系统，安全性及效率较之同类系统具有明显优势，并且实现了系统不可伪造性、防止多重支付、防止金额篡改等多种实用性质。本文设计的群签名方案利用椭圆曲线上的离散对数问题比标准的离散对数问题更加困难的特点，选定特殊的椭圆曲线，通过椭圆曲线上的点乘、点加等运算实现了整个方案的建立及运行，相较于 ACJT 中的模乘、模幂运算，计算复杂度大大降低，并且方案运行过程所用参量个数明显减少，使签名长度减少了 86.13%，方案主要过程运行时间由不小于 40 000 ms 缩短为不大于 45 ms，系统效率明显提升，用更短小的密钥保持了较高的安全性。引入无证书签名的思想，通过设计签名算法使群成员利用从密钥生成中心 KGC 处提取的部分密钥在加入过程中直接生成签名，群管理员 GM 直接验证，避免了两者多次交互，简化了成员加入的过程，并且成员信息分储在 KGC 和 GM 两处，在减小 GM 存储压力的同时增强了系统防陷害的能力，使方案可以抵抗联合攻

表 3　电子现金方案对比

方案	理论基础	模数大小/bit	成员可撤销	前向安全性	防止金额篡改	防止多重支付
Zhang 方案	有限域离散对数问题	≥1 024	v	×	×	×
FEI 方案	有限域离散对数问题	≥1 024	×	×	v	v
本文方案	椭圆曲线离散对数问题	≥160	v	v	v	v

注：其中“v”表示具备该性质，“×”表示不具备该性质。

击，提高了效率及安全性。方案使成员签名密钥通过特定算法随时间进行更新，由于更新算法的安全性，系统满足前向安全性，减少了密钥泄露带来的危害。并且系统具备成员撤销功能，弥补了 ACJT 方案中成员不可撤销的缺陷，使方案更具实用性。文中还对方案的安全性及高效性做出了相应证明。

参考文献：

[1] CHAUM D. Blind signature for untraceable payments[C]//Advances in Cryptology-CRYPTO'82. New York, c1983: 199-203.

[2] CHAUM D, HEYST F. Group signature[C]//EUROCRYPT'91, LNCS. Springer-Verlag. c1991: 257-265.

[3] ATENIESE G, CAMENISCH J, JOYE M, et al. A practical and provably secure coalition-resistant group signature scheme[C]//Advances in Cryptology-CRYPTO'00, LNCS 1880, Springer-Verlag, c2000: 255-270.

[4] MAITLAND G, BOYD C. Fair electronic cash based on a group signature scheme[C]//Proc of ICICS'01. c2001: 461-465.

[5] CONSTANTIN P. An off-line electronic cash system with revokable anonymity[C]//The 12th IEEE Mediterranean Electro-Technical Conference. Dubrovnik, Croatia, c2004: 763-767.

[6] HOU X S, TAN C H. A new electronic cash model [J]. Information Technology : Coding and Computing, 2005,1(4-6):374-379.

[7] ZHANG J L, MA L Z, WANG Y M. Fair e-cash system without trustees for multiple banks[C]//International Conference on Computational Intelligence and Security Workshops. c2007: 585-587.

[8] FEI X W, LI Q L. New electronic cash system with higher security and efficiency[J]. Application Research of Computers, 2008, 25(5): 1543-1545.

[9] SONG D X. Practical forward secure group signature schemes[C]//The 8th ACM Conf on Computer and Communications Security(CCS 2001). New York, ACM Press, c2001: 225-234.

[10] TORU N, NOBUO F. Revocable group signature with compact revocation list using accumulators[C]//Springer International Publishing Switzerland. c2014: 435-451.

[11] **陈泽文**, **王继林**, **黄继武**, **等**. ACJT **群签名方案中成员撤销的高效实现**[J]. **软件学报**, 2005, 16(1): 151-157.
CHEN Z W, WANG J L, HUANG J W, et al. An efficient revocation algorithm in ACJT group signature[J]. Journal of Software, 2005,16(1): 151-157.

[12] ZHANG J, WU Q, WANG Y. A novel efficient group signature scheme with forward security [C]//Int'l Conf on Information and Communications Security(ICICS'03). Berlin, c2003: 292-300.

[13] WANG G. On the security of a group signature scheme with forward security[C]//Int'l Conf on Information Security and Cryptology-ICISC 2003. Berlin: Springer-Verlag, c2003: 27-39.

[14] **肖平安**, **杨凌**. **基于群签名的身份认证方案研究**[D]. **兰州**: **兰州大学**, 2013 :6-9.
XIAO P A, YANG L. Study on identity authentication scheme based group signature[D]. Lanzhou: Lanzhou University, 2013: 6-9.

[15] **李如鹏**, **于佳**, **李国文**, **等**. **高效撤销成员的前向安全群签名方案**.[J] **计算机研究与发展**, 2007, 44(7):1219-1226.
LI R P, YU J, LI G W, et al. Forward secure group signature schemes with efficient revocation[J]. Journal of Computer Research and Development, 2007, 44(7): 1219-1226.

[16] **陈少真**, **李大兴**. **有效取消的向前安全群签名体制**[J]. **计算机学报**, 2006, 29(6): 998-1003.
CHEN S Z, LI D X. An efficient revocable group signature schemes with forward security[J]. Chinese Journal of Computers, 2006, 29(6): 998-1003.

[17] CAMENISH J, STADLER M. Efficient group signature schemes for large groups[C]//Advances in Cryptology-CRPTO'97, LNCS 1294. Berlin: Springer-Verlag, c1997: 410-424.

[18] **张德栋**, **马兆丰**, **杨义先**, **等**. **群签名中成员撤销问题解决方案**[J]. **通信学报**, 2014, 35(3): 193-200.
ZHANG D D, MA Z F, YANG Y X, et al. New solution scheme for the member revocation in group signature[J]. Journal on Communications, 2014, 35(3): 193-200.

[19] **黎茂棠**, **杨晓元**, **韩益亮**, **等**. **基于** ACJT **的广义群签密方案**[J]. **计算机工程与应用**, 2008,44(31): 128-131.
LI M T, YANG X Y, HAN Y L, et al. New ACJT based generalized group signcryption[J]. Computer Engineering and Applications, 2008, 44(31): 128-131.

[20] **张兴兰**. **一种高效的群签名方案**.[J] **计算机应用研究**, 2009, 26(11): 4276-4278.
ZHANG X L. Efficient group signature scheme[J]. Application Research of Computers, 2009, 26(11): 4276-4278.

[21] **韩晓花，李乔良，袁遇晴**. **基于椭圆曲线群签名方案的多银行电子现金系统**[J]. **计算机研究与发展**, 2009, 46(Suppl.):306-310.
HAN X H, LI Q L, YUAN Y Q. An electronic cash system with multiple banks based on ECC group signature scheme[J]. Journal of Computer Research and Development, 2009, 46(Suppl.): 306-310.

[22] HE D, CHEN J, ZHANG R. An efficient and provably-secure certificateless signature scheme without bilinear pairings[J]. International Journal of Communication Systems, 2012, 25: 1432-1442.

[23] SUJATA M, BANSIDHAR M, SUBHALAXMI D.A secure electronic cash based on a certificateless group signcryption scheme[J]. Mathematical and Computer Modelling, 2013, 15(1-2): 186-195.

[24] ATENIESE G, SONG D, TSUDIK G. Quasi-efficient revocation in group signature[C]//Financial Crypotography(FC'02), LNCS 2357. Berlin: Springer-Verlag, c2002: 183-197.

[25] SUJATA M, BANSIDHAR M, SUBHALAXMI D. A secure electronic cash based on a certificateless group signcryption scheme[J]. Mathematical and Computer Modelling, 2013, 58: 186-195.

[26] SATTAM S. AL-RIYAMI, KENNETH G. Certificateless public key cryptography[C]//International Association for Cryptologic Research. c2003: 452-473.

[27] **施荣华**, **龙成胜**. **一种前向安全的** ACJT **群签名方案**.[J] **计算机工程与应用**, 2008, 44(7): 126-128.
SHI R H, LONG C S, ACJT group signature scheme with forward security[J]. Computer Engineering and Application, 2008, 44(7): 126-128.

[28] XU X, ZHU P, WEN Q Y, et al. A secure and efficient authentication and key agreement scheme based on ECC for telecare medicine information systems[J]//Journal of Medical Systems, 2014,38(1): 1-7.

作者简介：

梁艳（1991-），**女，山西阳泉人，北京航空航天大学硕士生，主要研究方向为信息安全与密码学。**

张筱（1984-），**女，山东济南人，博士，北京航空航天大学副教授，主要研究方向为密码学、信息安全及复杂信息系统。**

郑志明（1953-），**男，上海人，博士，北京航空航天大学教授，主要研究方向为信息安全、复杂信息系统及动力系统。**