一种新的基于身份的公平离线电子现金方案*

崔 巍[1], 周玉建[1], 梁 建[1], 周游胜[2], 王尊亮[3a], 伍淳华[3b]
(1. 科学技术部 信息中心, 北京 100862; 2. 重庆邮电大学 计算机科学与技术学院,重庆 400065; 3. 北京邮电大学 a. 计算机学院; b. 信息安全中心, 北京 100876)

摘 要: 为了设计安全、高效的电子现金方案,基于受限部分盲签名提出了一种新的基于身份的公平离线电子现金方案。该方案使用知识证明签名有效地构造了重复花费检测协议,并实现了货币追踪协议和货币所有者追踪协议,给出了不可伪造性、匿名性、公平性和有效性证明。与已有方案相比,该方案能够有效地防止账户所有者进行重复消费,并且使用了较少的高耗时运算,提款协议和支付协议具有较高的计算效率。

关键词: 基于身份; 公平; 离线; 电子现金; 重复花费检测
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)07-2668-04
doi:10.3969/j.issn.1001-3695.2012.07.073

New ID-based fair off-line electronic cash scheme

CUI Wei[1], ZHOU Yu-jian[1], LIANG Jian[1], ZHOU You-sheng[2], WANG Zun-liang[3a], WU Chun-hua[3b]
(1. *Informaiton Center, Ministry of Science & Technology, Beijing* 100862, *China*; 2. *College of Computer Science & Technology, Chong qing University of Posts & Telecommunications, Chongqing*, 400065, *China*; 3. *a. School of Computer Science, b. Information Security Center, Beijing University of Posts & Telecommunications, Beijing* 100876, *China*)

Abstract: In order to design a secure and efficient electronic cash scheme, this paper proposed a new ID-based fair off-line electronic cash scheme based on restrictive partially blind signature. The scheme effectively constructed double-spending detection protocol by using signature of proof of knowledge and achieved coin tracing protocol and owner tracing protocol. The scheme was proved to be unforgeable, anonymous, fair and effective. Compared with the existing scheme, the proposed scheme can prevent the double-spending of account holder and has obvious advantages in withdrawal protocol and payment protocol by using less high time-consuming operation.

Key words: ID-based; fair; off-line; electronic cash; double-spending detection

0 引言

Chaum[1]提出了盲签名的概念,并将其应用于具有不可追踪性的匿名电子现金系统。该系统为了防止用户重复花费电子现金,需要银行在线检查商家的账户中是否存在已花费的电子现金。由于这种在线检查的方式往往成为交易的瓶颈,Chaum 等人[2]提出了离线匿名电子现金系统的概念,大大减少了在线交易的运算量。Camnisch 等人[3]和 Frankel 等人[4]分别提出了公平离线电子现金系统,通过嵌入部分与用户身份无关的公共信息,并且对电子现金的结构进行限制,能够在有效保护用户隐私的同时降低管理复杂度。

通过将身份的概念引入到电子现金系统中,Chen 等人[5]使用基于身份的受限部分盲签名构造了一个基于身份的公平离线电子现金系统,但是该方案没有给出安全性证明。Hu 等人[6]指出该方案存在严重的安全缺陷,该方案在账户所有者进行重复消费时不能被有效地追踪。此外,Wang 等人[7]还构造了第一个多银行的基于身份的公平离线电子现金系统,有效地解决了实际使用中多个银行发行电子现金的问题。

本文根据文献[8]提出的基于身份的受限部分盲签名方案,并借鉴 Brand 等人[9]和 Wang 等人[7]的思想构造了一个新的基于身份的公平离线电子现金系统,并给出了安全性证明。该系统能够有效地防止账户所有者进行重复消费,并实现了货币和货币所有者追踪,所提方案在签名过程中使用了较少的双线性对运算[10](运算效率较低),所以在系统建立、提款协议、支付协议三个阶段具有较高的效率。

1 背景知识

1.1 双线性群组

定义 1 非对称双线性群组。设 k 是一个安全参数,p 是一个 k bit 长的安全大素数,设$(G_1,+)$、$(G_2,+)$和$(G_T,\cdot)$是 p 阶循环群,P、Q 分别是 G_1 和 G_2 的生成元。(G_1,G_2,G_T)是非对称双线性映射群组,如果双线性映射 $e:G_1\times G_2\rightarrow G_T$ 存在,并满足以下条件:

a)双线性性。$\forall(S,T)\in G_1\times G_2$, $\forall a,b\in Z_p$,均有 $e(aS,$

收稿日期: 2011-11-11; **修回日期**: 2011-12-26 **基金项目**: 国家"973"重点基础研究发展计划资助项目(2007CB311203); 国家自然科学基金资助项目(60821001)

作者简介:崔巍(1982-),男,山东聊城人,工程师,博士,主要研究方向为网络安全、数字签名(dacui635@163.com);周玉建(1964-),男,北京人,工程师,主要研究方向为网络管理、信息安全;梁建(1980-),男,北京人,工程师,硕士,主要研究方向为计算机网络、网络安全;周游胜(1979-),男,湖北利川人,讲师,博士,主要研究方向为网络安全、可信计算;王尊亮(1980-),男,山东聊城人,讲师,博士,主要研究方向为人工智能、可信计算;伍淳华(1977-),女,湖北黄岗人,讲师,博士,主要研究方向为数字水印、数字信息隐藏.

$bT) = e(S,T)^{ab}$成立。

b)非退化性。$\exists (S,T) \in G_1 \times G_2$,满足 $e(S,T) \neq 1$。

c)可计算性。存在有效算法,对于 $\forall (S,T) \in G_1 \times G_2$,$e(S,T)$能够被有效地计算。

d)存在有效并可以公开计算的同构映射。$\psi: G_2 \to G_1$,使得 $\psi(Q) = P$。

上述非对称双线性群组可以通过文献[10]中所建议的方法来构造椭圆曲线,并根据该椭圆曲线来获得双线性映射群。

1.2　知识签名

所谓的知识签名是这样一个密码学工具:它是通过签名的方法,使得一方可以向另外一方证明知道一个秘密值,而不泄露任何有关该秘密值的有用信息。下面对本文所提方案涉及到的知识签名进行了定义,这些知识签名可以在文献[11]中找到。

定义 2　两个离散对数相等的知识签名。(d, r)称为是两个离散对数 $A_1 = xP$ 和 $A_2 = xQ$ 的知识对消息 m 的签名,如果它满足方程 $d = H(m \| A_1 \| A_2 \| P \| Q \| rP + dA_1 \| rQ + dA_2)$,用 $SPK\{a \mid A_1 = aP \cap A_2 = aQ\}(m)$来表示。

定义 3　离散对数和表示相等的知识签名。三元组$(d, r_1, r_2) \in \{0,1\}^s \times (Z_p)^2$ 称为是离散对数 $A_1 = x_1 P$ 并且 $A_2 = x_1 P_1 + x_2 P_2$ 关于基于 P_1, P_2 的表示对消息 m 的知识签名,如果它满足方程

$$d = H(m \| A_1 \| A_2 \| P_1 \| P_2 \| r_1 P + dA_1 \| dA_2 + r_1 P_1 + r_2 P_2)$$

用 $SPK\{(a, b) \mid A_1 = aP \cap A_2 = aP_1 + bP_2\}(m)$来表示。

1.3　安全性

定义 4　基于身份部分盲签名的不可伪造性。在随机预言模型中,如果一个算法 F 以至少 ε 的概率输出一个对基于身份的部分盲签名方案伪造的签名,并且其运行时间最多是 t,最多进行过 q_{HID}次 ID 哈希询问,q_{HM}次消息哈希询问,q_E 次提取询问,q_S 次发行询问,则算法 F 可以$(t, q_{HID}, q_{HM}, q_E, q_S, \varepsilon)$攻破该方案。如果不存在这样的算法,则称该方案是$(t, q_{HID}, q_{HM}, q_E, q_S, \varepsilon)$存在性不可伪造的。

2　基于身份的公平离线电子现金系统模型

基于身份的公平离线电子现金系统主要包含五个参与方:用户 U、银行 B、商家 S、可信第三方 TTP 与中央银行 CB(CB 的作用和在签名中使用的 PKG 作用基本相同)。在系统建立过程中,银行与可信第三方需要进行初始化操作,如设定系统安全参数、选取并公布系统取款公钥与追踪公钥。可信第三方的作用是协助银行完成对货币或货币所有者的追踪。银行用来管理用户的身份与发行货币,根据支付信息实现商家的存款。并要求用户与商家在银行处都建有账户。

系统建立。该算法由中央银行 CB 运行,输入一个安全参数 k,返回系统参数 params,并自己秘密保存主密钥 MK。可信第三方 TTP 使用密钥生成算法,生成自己的公私钥对(pk_T, sk_T)。

注册算法。它是一个概率性的多项式时间算法,由 CB 运行,输入安全参数 k、系统参数 params、公钥 PK、主密钥 MK 和银行 B 的身份 ID,返回银行 B 的公私钥对(pk_B, sk_B)。

开户协议。该算法由用户 U 运行,U 使用密钥生成算法,生成自己的公私钥对(pk_U, sk_U)并将自己的账户信息 I_u(一般情况下 $pk_U = I_u$)提供给银行 B,B 对该信息进行存储。

提款协议。在该协议中,用户 U 从银行 B 处提取电子现金,U 的输入是 pk_B、pk_T 和 sk_U,B 的输入是 pk_U、pk_T 和 sk_B,其输出是电子现金 W 或错误(error)的消息以及可以追踪电子现金或检测重复消费的消息 T_W,银行 B 维持一个数据库 D 保持追踪信息(pk_U, T_W)。

支付协议。在该协议中,用户 U 的输入是 W、pk_T,商家 S 的输入是 pk_T、pk_B 以及自己的秘密信息,用户 U 向商户 S 提交电子现金 W 以及电子现金的有效性证明 π,输出是成功或失败。

存款协议。在该协议中商户 S 的输入是 sk_S、pk_T、π、W、pk_B,银行 B 的输入是 pk_S、pk_T、sk_B。S 将(W, π)存入自己的账户。对与用户共同执行过支付协议的诚实商户来说,银行肯定会接受该电子现金。银行 B 把(W, π)添加到已使用过的电子现金列表中。如果成功,则商家没有输出,否则输出一个错误消息 error。

检测算法。该算法输入 params、W、π_1、π_2 并输出(pk_U, Π_T),如果商家提交的 π_1、π_2 是两个不同且有效的签名时,Π_T 就是关于 pk_U 是 W 的取款者的公钥证明,从而能够确定重复消费者的身份。

货币追踪协议。该协议的输入是 T_W、sk_T、pk_T、pk_U,输出是 W',W'是提款协议算法中与用户 U 输入相关的信息,通过 W′ 银行可以把某个取款视图及其电子现金联系起来。

货币所有者追踪协议。该算法的输入是 W、π、sk_T、pk_T,输出是 W'',通过 W'',银行可以获得与之对应的取款视图。

3　方案描述

首先用 B 来表示发币银行,CB 表示中央银行用来生成和分发密钥,TTP 表示可信的第三方,一个普通账户的所有者 U,以及一个普通的商户 S。

系统建立。给定安全参数 k,CB 选出 $p(p > 2^k)$阶非对称双线性群组(G_1, G_2, G_T)(其中 G_1、G_2 是加法群,G_T 是乘法群),Q 为 G_2 中的生成元,Q_1、Q_2、Q_3 是 G_2 中的元素,$P = \psi(Q) \in G_1$,CB 选择主密钥 $s \in_R Z_p^*$,$Q_{pub} = sQ \in G_2$,哈希函数 $H_1: \{0,1\}^* \to Z_p^*$、$H_2: \{0,1\}^* \times G_T^* \to Z_p^*$、$H_3: \{0,1\}^* \to Z_p^*$ 并公布系统参数 params = $\{G_1, G_2, G_T, P, Q, Q_1, Q_2, Q_3, Q_{pub}, e, \psi, H_1, H_2, H_3\}$, TTP 随机选择 $x_T \in Z_p^*$ 作为自己的私钥,计算并公布$Q_T = x_T Q_2$ 和 $\hat{Q}_T = x_T^{-1} Q_2$。

注册。给定银行 B 的身份信息 ID_B,CB 生成私钥:$S_{ID} = \frac{1}{s + H_1(ID_B)} P$,如果 $s + H_1(ID_B) \equiv 0$,则放弃 s,返回建立算法,重新选择 s。为了使用方便,用户可以在协议执行前对 $g = e(P,Q)$进行计算。

开户协议。当用户 U 在银行 B 开户时,B 要求用户 U 鉴别自己的身份,U 产生随机数 $u_1 \in_R Z_p$,并且计算唯一的账号信息 $I_U = u_1 Q_1$ 并且 $u_1 Q_1 + Q_2 \neq O$。用户 U 将 I_U 发送给银行 B,并且保持 u_1 为自己的秘密。银行 B 把用户 U 的账号信息和 I_U 一起保存在自己的账号数据库中,这里的信息 I_U 可以用来鉴别用户 U,防止该用户进行重复花费。

提款协议。当用户 U 需要提取电子货币时,首先需要证明他对自己账户的所有关系,并且和银行协商他们之间的公共信息 info。用户 U 和银行 B 之间的取款协议如下:

a)用户 U 随机选择 $a \in Z_p^*$,计算 $M = Q_2 + a^{-1}(I_U + Q_3)$ 和 $M_2 = a\hat{Q}_T$,然后用户 U 根据定义 2 构造知识签名 $V_1 = SPK\{a \mid I_U + Q_3 = a(M - Q_2) \cap M_2 = a\hat{Q}_T\}(\text{info})$,并将 M、M_2、V_1 发送给银行 B。

b)银行 B 首先验证 V_1,如果验证通过,则 B 随机选择 $x \in Z_p^*$,并且计算 $R = g^x \in G_T$,$R_2 = e(S_{\text{ID}}, M)$,$R'_2 = R_2^x$,并将 R、R_2、R'_2,发送给用户 U。

c)用户 U 随机选择 $\alpha, \beta, x_1, x_2 \in Z_p^*$,计算:

$$M_1 = aM,\ W = x_1 Q_1 + x_2 Q_2$$

$$Z = R_2^a (= e(S_{\text{ID}}, M_1))$$

$$t_2 = R'^{a\alpha}_2 \times Z^{\alpha\beta H_3(\text{info})} (= e(\alpha x S_{\text{ID}}, M_1) \times Z^{\alpha\beta H_3(\text{info})}$$

$$t_1 = R^\alpha g^{\alpha\beta H_3(\text{info})}$$

$$c' = H_2(H_3(\text{info}) \parallel M_1 \parallel Z \parallel W \parallel t_2 \parallel t_1),\ c = \alpha^{-1}c' + \beta$$

并将 c 发送给银行 B。

d)银行 B 计算 $V = (x + cH_3(\text{info}))S_{\text{ID}}$,并将 V 发送给用户 U。

e)用户 U 计算 $V' = \alpha V$,其中 $(\text{ID}_B, M_1, \text{info}, Z, W, c', V')$ 是一个有效的电子现金,并且里面嵌有与银行 B 协商的公共信息。该电子货币满足以下等式:

$$c' = H_2(H_3(\text{info}) \parallel M_1 \parallel Z \parallel W \parallel e(V', M_1) \times Z^{-c'H_3(\text{info})} \parallel e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'H_3(\text{info})})$$

支付协议。当用户 U 想要使用他的电子货币在商家 S 那里进行消费时,将会执行下面的支付协议:

a)商户 S 发送给用户 U 一个挑战 $PI = H_1(\text{ID}_B, I_S, \text{date/time}, \text{TID})$。其中 I_S 表示商户 S 的账号信息,date/time 表示日期以及交易的时间,TID 表示交易业务的其他信息。

b)用户 U 计算 $E_2 = aQ_T$ 并根据定义 3 构造知识签名 $V_2 = SPK\{(a,b) \mid aQ_2 + bQ_1 = M_1 - Q_3 \cap E_2 = aQ_T\}(PI)$,将 $(\text{ID}_B, M_1, \text{info}, Z, W, c', V', E_2, V_2)$ 发送给商家 S。

c)商户 S 首先验证签名 $(\text{ID}_B, M_1, \text{info}, Z, W, c', V')$ 和知识签名 V_2 的有效性,如果通过验证则商户 S 接受这笔交易,否则,商户 S 拒绝这次交易。

存款协议。商户 S 在规定的时间前向银行 B 支取现金时,向银行 B 发送支付业务的相关信息:$(\text{ID}_B, M_1, \text{info}, Z, W, c', V')$、$E_2$、$PI$、$d$、$r_1$、$r_2$,其中 PI 表示此项业务的相关信息,d、r_1、r_2 是根据定义 2 得到的知识签名的信息。银行 B 首先检查电子货币的有效性和使用时间 date/time 是否超过了使用的有效日期 T_{expire}。如果验证通过,银行 B 将会在它的存款数据库中去查找 $\{M_1, \text{info}, \text{date/time}, d, r_1, r_2\}$ 是否存在。如果该条信息没有被存储过,则银行 B 将信息 $\{M_1, \text{info}, \text{date/time}, d, r_1, r_2\}$ 存储到它的存款数据库中,并将相应的金额存到商户 S 的账户上。

重复花费检测协议。在存款时,B 首先查找该电子现金是否已被使用,如果已被使用,再继续分析支付脚本是否相同,如果相同,则表明是该商家企图多次存入收到的同一电子现金。如果不同,则说明了用户 U 多次使用同一个电子现金,那么他必将在不同的商户那里消费超过一次,或是在不同的时间在同一个商户那里消费。根据定义 3 可知 $d \neq d'$,所以 V_2 中 PI 的信息总是不同的,因为 $r_2 \equiv_p k_2 - du_1$ 和 $r'_2 \equiv_p k_2 - d'u_1$,所以银行 B 可以计算 $u_1 \equiv_p (r'_2 - r_2)/(d - d')$ 的值,这样就可以确定进行过重复消费的用户身份 $I_U = u_1 P_1$。

货币追踪协议。在需要对 U 所取出的货币进行追踪时,B 向可信第三方 TTP 传送提款协议中 $M_2 = a\hat{Q}_T$,TTP 计算 $x_T M_2 = aQ_2$,并将其发回给 B。B 计算 $M_1 = I_U + aQ_2 + Q_3$ 并在其存款数据库中查找相应的电子货币信息。

货币所有者追踪协议。当需要对货币所有者进行追踪时,银行 B 向可信第三方 TTP 传送取款信息 (M_1, E_2),TTP 计算 $I_U = M_1 - Q_3 - x_T^{-1}E_2$ 并把它发回给银行 B,B 在自己的账户数据库中查找相应的 I_U 信息,就完成了货币所有者的信息追踪。

4 安全性证明

根据第 3 章的受限部分盲签名方案提出了一个新的基于身份的公平离线电子现金系统,在这里给出其不可伪造性、匿名性、公平性以及相关的效率分析。

4.1 正确性

当用户与银行正确执行完取款协议后,用户获得了一个有效的电子现金。

因为等式:

$$e(V', M_1)Z^{-c'H_3(\text{info})} = e((\alpha x + \alpha c H_3(\text{info}))S_{\text{ID}}, M_1) \times Z^{-c'H_3(\text{info})} =$$

$$e(S_{\text{ID}}, M_1)^{\alpha x} \times e(S_{\text{ID}}, M_1)^{c'H_3(\text{info}) + \alpha\beta H_3(\text{info})} \times Z^{-c'H_3(\text{info})} =$$

$$e(S_{\text{ID}}, aM)^{\alpha x} \times e(S_{\text{ID}}, M_1)^{\alpha\beta H_3(\text{info})} = R'^{a\alpha}_2 \times Z^{\alpha\beta H_3(\text{info})} = t_2$$

和等式:

$$e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'H_3(\text{info})} =$$

$$e((\alpha x + \alpha c H_3(\text{info}))P, Q) \times g^{-c'H_3(\text{info})} =$$

$$e(P, Q)^{\alpha x} \times e(P, Q)^{\alpha c H_3(\text{info})} \times g^{-c'H_3(\text{info})} =$$

$$e(P, Q)^{\alpha x} \times e(P, Q)^{c'H_3(\text{info}) + \alpha\beta H_3(\text{info})} \times g^{-c'H_3(\text{info})} =$$

$$R^\alpha \times g^{\alpha\beta H_3(\text{info})} = t_1$$

成立。所以:

$$c' = H_2(H_3(\text{info}) \parallel M_1 \parallel Z \parallel W \parallel e(V', M_1) \times Z^{-c'H_3(\text{info})} \parallel e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'H_3(\text{info})} \parallel$$

4.2 不可伪造性

定理 1 如果恶意用户可以有效地伪造出一个新的有效的电子现金,则该用户也可以伪造在文献[8]中提出的基于身份的部分盲签名。

证明 在本文提出的电子现金系统中,$(\text{ID}_B, M_1, \text{info}, Z, W, c', V')$ 是一个有效的电子货币,并且里面嵌有与银行 B 协商的公共信息。该电子货币满足以下等式:

$$c' = H_2(H_3(\text{info}) \parallel M_1 \parallel Z \parallel W \parallel e(V', M_1) \times Z^{-c'H_3(\text{info})} \parallel e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'H_3(\text{info})})$$

假设恶意用户可以伪造电子货币,由于 H_2 是随机预言机,恶意用户必须得到 $H_3(\text{info})$、M_1、Z、$e(V', M_1) \times Z^{-c'H_3(\text{info})}$、$e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'H_3(\text{info})}$ 去计算 c',这就表示恶意用户可以计算出满足等式的 V'。令 $H_3(\text{info}) = 1$,$m = M_1 \parallel Z \parallel e(V', M_1) \times Z^{-c'H_3(\text{info})}$,攻击者可以伪造签名

$$(\text{ID}, m = M_1 \parallel Z \parallel e(V', M_1) \times Z^{-c'H_3(\text{info})}, \text{info}, c', V')$$

并满足

$$c' = H_2(m, e(V', Q_{\text{pub}} + H_1(\text{ID})Q) \times g^{-c'})$$

此时说明文献[8]提出的基于身份的部分盲签名被攻破,与其文中基于身份的部分盲签名的不可伪造性相冲突,因此,该方案是不可伪造的。

4.3 匿名性

假设 $(\text{ID}_B, M_1, \text{info}, Z, W, c', V')$ 是有效的电子现金,$(M,$

R, R_2, R'_2, c, V)为签名者执行协议时观察到的数据,对于(α, β)有等式 $c = \alpha^{-1}c' + \beta$, $V' = \alpha V$ 成立。显然,可以得到 $\alpha = \log_V V'$,$\beta = c - \alpha^{-1}c'$,且 α、β 是唯一存在的。因为电子现金是有效的,所以有 $R_2 = e(S_{ID}, M)$ 和 $Z = e(S_{ID}, M_1)$ 成立,可以得到 $Z = e(S_{ID}, M_1) = R_2^a$,因此必然存在关于 M_1 的表示 $M_1 = aM$。所以银行不能把某个电子现金与其对应的提款协议联系起来。

4.4　公平性

在本文方案里,TTP 可以执行货币所有者追踪协议和货币追踪协议。货币的提取协议本质上是一个基于身份的受限部分盲签名方案,所以银行 B 能够确保用户 U 以格式 $M_1 = aM + bQ$ 执行盲转换协议,并且通过 V_1 得到 $M = Q_2 + \xi^{-1}(I_U + Q_3)$,其中 $a, b, \xi \in Z_p^*$。用户 U 被要求在支付阶段提供带有特殊结构的电子货币,这就强迫用户必须使用带有盲因子的承诺值。也就是说,如果在支付阶段用户 U 通过 V_2 向商户 S 证明存在 $\lambda, \mu \in Z_p^*$,使得 $M_1 = \mu Q_1 + \lambda Q_2 + Q_3$,那么可以推出 $b \equiv_p 0$、$\mu \equiv_p u_1$ 和 $a \equiv_p \xi \equiv_p \lambda$,所以,$M_2 = a\hat{Q}_T$,$E_2 = aQ_T$ 并且 $M_1 = u_1 Q_1 + aQ_2 + Q_3$。

4.5　有效性

银行使用根据基于身份的受限部分盲签名得到的电子现金方案,这使得用户和商户并不需要从 LDAP 服务器上取回银行的公钥或是将银行的公钥存储在本地的数据库中。在使用基于群盲签名的电子现金系统中,当一个商家接受了一个用户的电子现金。由于群签名的匿名性,他并不知道这个电子现金是从哪个银行中所提取的。所以商家必须将收到的电子现金发回到中央银行去检测双消费,这样将会导致中央银行的存储和计算的操作瓶颈。在提出的电子现金方案中,当一个商户在支付阶段接收了用户的电子现金后,知道是哪个银行发布了他接收的电子现金,并且可以把这些电子现金发送给发布它们的银行去检测重复消费。

4.6　效率分析

设 P 表示双线性对运算,E 和 M_t 分别表示 G_T 中的指数运算和乘法运算,M 和 A 分别表示 G_1 和 G_2 的标量乘和加法运算。其中配对运算是最为耗时的运算,由表 1 可以看出,本文所提方案使用了较少的双线性对运算,所以在系统建立、提款协议、支付协议三个阶段和已有方案相比具有明显的优势。

表 1　两种公平离线电子现金系统的效率比较

签名方案	系统建立	提款协议(用户)	提款协议(银行)	支付协议
本方案	$P+4M$	$8M+3A+5E+2M_t$	$P+5M+2A+2E$	$8M+3A$
文献[5]方案	$4P+M$	$3P+9M+7E+3M_t$	$P+5M+2A+2E$	$6P+6E+4M_t$

5　结束语

本文基于受限部分盲签名方案提出了一个新的基于身份的公平离线电子现金系统,并给出了不可伪造性、匿名性、公平性和有效性证明。该系统使用知识签名有效地构造了重复花费检测协议,并实现了货币追踪和货币所有者追踪,由于所提方案在签名过程中使用了较少的高耗时运算,所以在提款协议、支付协议具有较高的效率。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]//Proc of CRYPTO on Advances in Cryptology. New York: Plenum Press, 1982: 199-203.

[2] CHAUM D, FIAT A, NAOR M. Untraceable electronic cash[C]// Proc of the 8th Annual International Cryptology Conference on advances in Cryptology. London: Springer-Verlag, 1988: 319-327.

[3] CAMENISCH J, MAURER U M, STADLER M. Digital payment systems with passive anonymity-revoking trustees[C]//Proc of the 4th European Symposium on Research in Computer Security. London: Springer-Verlag, 1996: 33-43.

[4] FRANKEL Y, TSIOUNIS Y, YUNG M. Indirect discourse proofs: achieving efficient fair off-line E-cash[C]//Proc of the International Conference on the Theory and Appliations of Cryptology and Information Security advances in Cryptology. London: Springer-Verlag, 1996: 286-300.

[5] CHEN Xiao-feng, ZHANG Fang-guo, LIU Sheng-li. ID-based restrictive partially blind signatures and applications[J]. Journal of Systems and Software, 2007, 80(2): 164-171.

[6] HU Xiao-ming, HUANG Shang-teng. Analysis of ID-based restrictive partially blind signatures and applications[J]. Journal of Systems and Software, 2008, 81(11): 1951-1954.

[7] WANG Chang-ji, TANG Yong, LI Qing. ID-based fair off-line electronic cash system with multiple banks[J]. Journal of Computer Science and Technology, 2007, 22(3): 487-493.

[8] 崔巍,辛阳,胡程瑜,等. 高效的基于身份的(受限)部分盲签名[J]. 北京邮电大学学报, 2008, 31(4): 53-57.

[9] BRANDS S A. An efficient off-line electronic cash system based on the representation problem, CS-R9323[R]. Netherlands: CWI Amsterdam, 1993.

[10] BARRETO P S L M, NAEHRIG M. Pairing-friendly elliptic curves of prime order[EB/OL]. (2006-02-28). http://eprint.iacr.org/2005/133.

[11] ATENIESE G, CAMENISCH J, JOYE M, *et al*. A practical and provably secure coalition-resistant group signature scheme[C]//Proc of the 20th Annual International Cryptology Conference on advances in Cryptology. London: Springer-Verlag, 2000: 255-270.