一种透明的可分电子现金系统

刘 锋，张建中
（陕西师范大学 数学与信息科学学院，陕西 西安 710062）

摘 要：介绍了一种基于 PVSS 的可分电子现金系统。该系统将可公开验证的秘密分享引入电子现金系统，不仅能够在银行和注册商家协作下找出客户的真实身份，以防止客户利用电子现金的不确定性进行犯罪，而且实现了电子现金的多次合法的精确支付，提高了系统的效率。

关键词：可分电子现金 电子支付 可公开验证秘密分享

电子现金又称为数字现金，是能被客户和商家接受的、通过因特网购买商品或服务时使用的一种交易媒介。有效的电子现金系统必须满足下列安全要求：

（1）独立性，电子现金不依赖所使用的计算机系统；

（2）不可重复使用，电子现金一次花完后，就不能使用第二次；

（3）匿名性，电子现金不能提供用于跟踪持有者的信息；

（4）可传递性，电子现金可容易地从一个人传给另一个人，并且不能提供跟踪这种传递的信息；

（5）可分性，电子现金可用若干种货币单位，并且可像普通的现金一样，把大钱分为小钱；

（6）安全存储，电子现金能够安全地存储在客户的计算机或 Smart 卡中，而且客户以这种方式存的钱可方便地在网上传递。

其中，电子现金的可分性能够让客户进行多次合法的精确支付，减少提款次数，从而降低网络负载，提高系统效率，因此可分电子现金系统应是研究的重点。这类系统允许客户将电子现金分成任意大小的金额进行多次精确的支付，直到与该电子现金的总额相等为止；但是，目前电子现金的支付协议通信量大、计算复杂度高、效率低。

可公开验证秘密分享（PVSS）在信息安全和数据保密中起着非常重要的作用，是设计多方安全计算的基本工具；自从第一个 PVSS 方案被提出以来，受到了密码学和信息安全界的普遍关注，到目前为止已经取得了丰富的研究成果，其中的一些 PVSS 方案已经被广泛地应用于多方安全计算、密钥托管、门限密码学及电子选举等多个研究领域。1996 年，Stadler 指出 PVSS 技术能够应用于电子现金系统的设计，但是到目前为止还未看到基于 PVSS 的电子现金系统。

Chang 基于参与者的身份提出了一种安全、高效的秘密分享方案；利用 Chang 方案，笔者给出了一种新的秘密分享方案；新方案具有可公开验证性，并且只使用了参与者公钥的盲化值，必要时秘密分发者可在另外任一位参与者的协助下揭示出该参与者的公钥。将新方案进一步引入到电子现金系统的研究，得出了一种可分电子现金系统。在该系统中，每个客户只需在银行注册一次就可多次执行存款和取款协议，而每个电子现金都可实现多次合法的精确支付；系统无需可信的第三方，任一客户的犯罪行为都可由银行与当前的商家协作揭示出其真实身份，从而降低系统负担、增强跟踪的确定性。

1 签密方案

系统参数：r 是大素数，$r-1$ 是两个大素因子的乘积，g 是 Z_r 的一个生成元，h 表示输出至少为 128bits 的抗碰撞的 hash 函数，KH 表示有密钥控制的单向 hash 函数；E、D 表示一个对称密码体制的加解密算法。

（1）签密者 Alice 的密钥：

私钥 $x_a \in Z^*_{r-1}$，公钥 $y_a(=g^{x_a} \bmod r)$；

解签密者 Bob 的密钥：

私钥 $x_b \in Z^*_{r-1}$，公钥 $y_b(=g^{x_b} \bmod r)$；

（2）Alice 对消息 m 的签密过程：

随机选取 $x \in Z^*_{r-1}$，计算

$(K_1,K_2)=h(y_b^x \bmod r), C=E_{K_1}(m),$

$R=KH_{K_2}(m), G=x/(R+x_a) \bmod (r-1);$

签密密文为 (C,R,G)。

（3）Bob 对密文 (C,R,G) 的解签密过程：

计算 $(K_1,K_2)=h((y_a g^R)^{Gx_b} \bmod r)$，

$m=E_{K_1}(C)$，当且仅当 $KH_{K_2}(m)=R$ 时接受 m。

2 新的秘密分享方案

利用 Chang 方案和签密方案，给出了一种新的秘密分享方案。该方案具有可公开验证性，并且只使用参与者公钥的盲化值，必要时秘密分发者可在另外任一位参与者的协助下揭示出该参与者的公钥。

（1）系统建立

令 S 是任一待分享的秘密，D 是秘密分发者；$A_1A_2\cdots A_n$ 是 n 个参与者，ID_i 是参与者 $A_i(i=1,2,\cdots,n)$ 的身份信息。D 定义如下参数：

r、g 的选取如上文所述，e、d 是 RSA 密码体制中的公钥和私钥，其中 $e\cdot d\equiv 1\bmod(r-1)$；$x_a\in Z^*_{r-1}$ 是 D 的私钥，$y_a(=g^{x_a}\bmod r)$ 是 D 的公钥。

(2)子密分配

D 通过传统的身份信息 ID_i 确定参与者 A_i 的身份；然后，随机选取一个 $t-1$ 次多项式

$$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}\bmod(r-1)$$

这里 $a_k\in Z^*_{r-1}$；为该多项式的系数计算一个验证向量 $V=\{V_0,V_1,\cdots,V_{t-1}\}$，使得 $V_k=g^{a_k}\bmod r$，$k=0,1,\cdots,t-1$；计算参与者 A_i 的身份标识号：

$$X_i=f(ID_i)\cdot p_i^{-1}\bmod(r-1)$$

其中 $p_i=\prod_{k\neq i}(ID_i-ID_k)\bmod(r-1)$；计算 A_i 的公钥 $Y_i=g^{X_i}\bmod r$；最后，D 进行如下的签密运算：

随机选取 k_i、$l\in Z^*_{r-1}$，计算

$$(K_1,K_2)=h(Y^{k_i}\bmod r),\ z_i=E_{K_1}(X),$$

$$s_i=KH_{K_2}(X),t_i=k_i/(s_i+x_D)\bmod(r-1);$$

$$C=g^{l\cdot d}\bmod r,F=(g^{a_0\cdot l\cdot d}\bmod r)\oplus S;$$

把 (z_i,s_i,t_i,Y_i,C,F) 发送给 A_i；

A_i 收到上述数组后，进行解密和验证；若合法，则接受 (X_i,Y_i) 作为其身份标识号；否则，发出抱怨并返回收到的数组不合法的信息，并再次注册。

(3)秘密恢复

不妨设 t 个参与者 A_1、A_2、$\cdots$、A_t 同意共同合作恢复秘密 S，则 A_i 计算并提交

$$E_i=C^{X_i}\bmod r,\hat{Y}_i=Y_i^l\bmod r$$

任何人均可验证 E_i 的有效性：$E_i^e\stackrel{?}{=}\hat{Y}_i\bmod r$

如果 E_i 不能通过验证，则 D 通过计算

$$\hat{V}=l^{-1}\bmod(r-1)\text{ 和 }\hat{l}=\hat{Y}^{\hat{V}}\bmod r$$

得到 A_i 的公钥；否则，每个参与者均可恢复出秘密：

$$S=F\oplus(\prod_{i=1}^{t}(E_i^{\Delta i}\bmod r)$$

其中 $\Delta i=\prod_{k=1,k\neq i}^{n}(-ID_k)\cdot\prod_{k\in Z_n/Z_i}(ID_i-ID_k)$

3 基于 PVSS 的可分电子现金系统

将可公开验证的秘密分享引入电子现金系统的研究，首次给出了一个基于 PVSS 的具有可撤销匿名性的可分电子现金系统。

(1)系统设置

设置过程由银行 B 完成。其中参数的选取如前所述，X_B、$Y_B(=g^{X_B}\bmod r)$ 分别是 B 的私钥和公钥。

(2)注册协议

本节用 A 表示任何一个要注册的客户或商家，ID 表示 A 的身份信息。

B 首先通过传统的身份信息 ID 确定 A 的身份，然后随机选取 $f(x)=a_0+a_1x\bmod(r-1)$，这里 $a_i\in Z^*_{r-1}$；为 $f(x)$ 的系数计算一个验证向量 $V=\{V_0,V_1\}$，使得 $V_i=g^{a_i}\bmod r$ $(i=0,1)$；计算 A 的身份标识号：

$$X=f(ID)\cdot(ID_B-ID)^{-1}\bmod(r-1)$$

相应的公钥 $Y=g^X\bmod r$；然后，B 对 A 的身份标识号进行如下的签密运算：

随机选取 $k\in Z^*_{r-1}$，计算

$$(K_1,K_2)=h(Y^k\bmod r),z=E_{K_1}(X),$$

$$s=KH_{K_2}(X),t=k/(s+x_B)\bmod(r-1);$$

把 (z,s,t) 发送给 A；A 收到上述数组后，进行解密和验证；若合法，则接受 X 作为其身份标识号；否则，发出抱怨并返回收到的数组不合法的信息，再次注册。

(3)提款协议

客户 U 将数组 (X_U,M) 签密，并将秘文 (z,s,t) 出示给 B；其中 X_U 是客户的身份标识号，M 是提款金额；B 验证客户 U 及 M 后，随机选取 $l\in Z^*_{r-1}$，计算

$$\hat{Y}=Y^l\bmod r,C=g^{l\cdot d}\bmod r,L=C^{X_B}\bmod r,$$

$$D=(g^{a_0\cdot l\cdot d}\bmod r)\oplus M;$$

然后，B 将数组 (l,C,D,L) 发送给客户 U；

客户 U 收到上述数组后，验证：$L^e\stackrel{?}{=}Y^l\bmod r$。如果验证成立，则计算：

$$M'=((C^{X_U})^{ID_BID_S(ID_U-ID_S)}\cdot L^{ID_UID_S(ID_U-ID_S)}\bmod r)\oplus D$$

比较 $M'\stackrel{?}{=}M$，如果验证成立，即得到数字现金为：

$$N=(ID_B,ID_U,l,C,D,M,Y_U,A_U(=C^{X_U}\bmod r))$$

(4)付款协议

客户 U 发送电子现金 N 给商店 S，并由 ID_B 知道系统的公共参数 e；验证 $A_U^e\stackrel{?}{=}Y_U^l\bmod r$，如果验证成立，则计算：$M'=((C^{X_S})^{ID_UID_S(ID_S-ID_U)}\cdot L^{ID_UID_S(ID_U-ID_S)}\bmod r)\oplus D$

比较是否有 $M'\stackrel{?}{=}M$，$M'\geq M_T$（M_T 为应支付金额）同时成立；若上述两式同时成立，则计算：

$$M_1=M-M_T,D_1=M_1\oplus(A_S,A_U);$$

并将数组 (M_1,D_1) 发送给 U；客户 U 验证：

$$M_1'=((C^{X_U})^{ID_BID_S(ID_U-ID_S)}\cdot L^{ID_UID_S(ID_U-ID_S)}\bmod r)\oplus D\stackrel{?}{=}M_1$$

如果通过验证，则接受支付，并保存数组：

$$N_1=(ID_B,ID_U,l,C,D_1,M_1,Y_U,A_U);$$

商家 S 保存数组：

$$F=(ID_U,l,C,D_1,M_T,Y_U,A_U)。$$

(5)存款协议

商家 S 将数组 F 发送银行 B。B 执行与 S 相同的验证功能，即验证：$A_U^e\stackrel{?}{=}Y_U^l\bmod r$，

$$M_T'=((C^{X_B})^{ID_B ID_S(ID_U-ID_S)}\cdot L^{ID_U ID_S(ID_B-ID_S)} \bmod r)\oplus D \stackrel{?}{=} M_T$$

若上述两式都能通过验证，则接受商家 S 的存款请求。

4 系统分析

(1) 安全性

本电子现金系统的安全性是建立在计算离散对数问题和因子分解问题困难性之上的；此外，采用无碰撞的 hash 函数保证了客户必须诚实地构造电子现金。一般假设银行随意地控制客户的账号，它是可信的。

(2) 不可重用性

由于银行为任意一份电子现金均产生了一个承诺值，而这个承诺值来源于 B 随机选取的一个整数，因此，客户支付的任何一份电子现金金额的标递各不相同；否则，商家可以容易地检测出客户 U 对某一电子现金金额的重复使用。

(3) 有效性

由于采用明文方式直接表示电子现金金额，使得电子现金的计算复杂性为常数；又因为每一份电子现金金额均有一个公开的承诺值，这使得客户与商家之间的支付协议是公平的，保护了商家的利益。

结合多秘密分享的特点可知，任一客户在银行只需一次注册就可以实现所有金额的电子现金的提取；并且支付协议的计算量等同于秘密分享的一次恢复算法的计算量；另外，商家只需利用接收到的数组执行一个简单的验证过程，就可以确定该电子现金的合法性，这大大减轻了商家的计算量，方便了验证。因此，本系统是高效的。

参考文献

1 Tsiounis Y. Efficient electronic cash:New notations techniques [M].Boston:College of Computer Science,Northeaster University, 1997:50~51

2 陈 恺，胡予濮，肖国镇. 可撤销匿名性的可分电子现金系统[J].西安电子科技大学学宝(自然科学版)，2001;28(1):57~61

3 Camenisch J, Maurer U, Stadler M. Digital payment systems with passive anonymity-revoking trustees[A].Computer Security-ESORICS'96[C]. Berlin: Springer-Verlag,1996;31~43

4 Davida G, Trankel Y, et al. Anonymity control ine-cash systems[A].Financial Cryptography-FC'97[C].Berlin:Springer-Verlag,1997;1~16

5 Frankel Y, Tsiounis Y, Yung M. Indirect discourse proofs: Achieving efficient fair off-line e-cash[A]. Advances in Cryptology-ASIACRYPT'96[C]. berlin: Springer-Verlag, 1996:286~300

6 Carpentieri M. A perfect threshold secret sharing scheme to identify cheaters[J]. Des. Code Cryptography. 1995;5(3):183~187

7 Stadler M. Publicly verifiable secret sharing[A]. Advances in Cryptology-EUROCRYPT'96[C]. Berlin: Spring-Verlag,1996;190~199

8 Chang T-Y, Hwang M-S, Yang W-P.A. An improvement on the Lin-Wu threshold verifiable multi-secret sharing scheme. Applied Mathematics And Computation.2005;163:169~178

9 Yuliang Zheng. Signcrypytion and its applications in efficient public key solutions. Proc. Of Information Security Workshop (ISW'97), Berlin;1997;201~218

(收稿日期:2005-06-14)

(上接第 7 页)

对标定参数所在的内存区域进行初始化、数据改写及保存。根据标定参数所在不同地址空间（ROM、FLASH 或 EEPROM），CANape 规定了不同的标定方法。

当标定参数需要存放在 FLASH 或 ROM 中时，在 E-CU 上电初始化后，程序首先将标定参数的初始值复制到 RAM 中，在 CANape 中该段用来存放标定参数的 RAM 称为 Calibration RAM。标定过程中，CANape 修改 Calibration RAM 中的参数值。标定全部结束后，再将该段 RAM 中的内容复制回 FLASH 或 ROM 中。

当标定参数存放在 EEPROM 中，有两种标定方法。第一种与上述方法相同，首先将标定参数复制到 RAM 中，标定结束后再将 RAM 中的数据覆盖到 EEPROM。此外，也可对 EEPROM 中的参数直接进行改写，实现这种方法需要对 EEPROM 进行频繁擦写操作，但不占用额外的 RAM 空间。

由于汽车电子网络系统已开始得到广泛的使用，基于网络连接的电子控制单元的匹配标定和传统的匹配标定方法已有了很大的不同，特别是基于 CAN 总线的匹配标定技术，目前已成为研究和应用的重点。

采用 CANape 进行基于 CCP 的匹配标定，实现了标定工具和内容的统一。根据这种方法能够快速有效地进行汽车电子控制单元的匹配标定，在实际开发应用中取得了良好的效果。

参考文献

1 CCP CAN Calibration Protocol. H.Kleinknecht, Rev. 2.1, 1999;(2)

2 CCP Driver (Implementation in Electronic Control Units CCP Version 2.1). Vector Informatik GmbH, Rev. 1.37.2002;(7)

3 Application Note: Integration of the Vector CCP Driver with a free CAN Driver. Marco Konrad, Marcel Iannizzi. Rev. 1.1.3.2001;(10)

4 CANape/CANape Graph User Manual.Vector Informatik GmbH, Rev. 4.0. 2002CANape

5 CCP Communication. Application Note AN-AMC-1-100.Kim Lemon, Rev. 1.1. 2003;(3)

(收稿日期:2005-05-11)