第34卷 第17期 计 算 机 工 程 2008年9月
Vol.34 No.17 Computer Engineering September 2008
·安全技术· 文章编号：1000—3428(2008)17—0133—03 文献标识码：A 中图分类号：TP309

基于智能卡的含有效期的电子现金系统

刘文远[1]，郭丽芳[1]，王宝文[1]，王亚东[2]
(1. 燕山大学信息科学与工程学院，秦皇岛 066004；2. 哈尔滨工业大学计算机科学与技术学院，哈尔滨 150001)

摘 要：为防止银行数据库记录的无限膨胀，提高系统的执行效率，该文将有效期加入基于智能卡的电子现金系统中，提出基于智能卡的含有效期的离线电子现金系统。该系统采用基于椭圆曲线的数字签名技术来实现。智能卡由于容量有限，椭圆曲线需要较小长度的密钥就可以获得较高的安全性，相对离散对数，椭圆曲线更适合应用于基于智能卡的电子现金系统中。因为该系统基于椭圆曲线离散对数表示问题，所以其安全性也是基于椭圆曲线离散对数的安全性。

关键词：智能卡；有效期；椭圆曲线；盲签名

E-cash System with Validity Duration Based on Smart Card

LIU Wen-yuan[1], GUO Li-fang[1], WANG Bao-wen[1], WANG Ya-dong[2]
(1. Information Science and Engineering Institute, Yanshan University, Qinhuangdao 066004;
2. Computer Science and Technology Institute, Harbin Institute of Technology, Harbin 150001)

【Abstract】 In order to prevent the database of the bank expanding infinitely and improve the performance efficiency of the system, this paper proposes an off-line e-cash system with validity duration based on the smart card by adding the validity duration into electronic cash system. The system applies the signature based on the elliptic curve to realize. As the capability of the smart card is limited, and the elliptic curve can achieve much better security and only need much shorter keys, the elliptic curve is much more adapt to e-cash system based on smart card than the discrete logarithm. The system is based on expression question of elliptic curve dispersed number, so its security is based on the security of elliptic curve dispersed logarithm.

【Key words】 smart card; validity duration; elliptic curve; blind signature

1 概述

自Chaum提出盲签名和电子现金的概念以来[1]，国内外学者在现代密码学理论指导下提出了许多电子现金方案[2]。其中离线电子现金系统由于克服了银行在线验证这一传输“瓶颈”，提高了交易的处理效率，从而有可能得到更大范围的普及应用。但电子现金的离线验证也带来了“重复花费”的潜在危害。

为了防止电子现金的重复花费，目前主要有 2 种解决方法：

(1)依赖防篡改智能卡的物理安全性，以达到电子现金重复花费的事前阻止；

(2)通过密码技术，实现对重复花费者的事后检测，此时银行必须维护一个记录所有已经花费过的电子现金的数据库，通过搜查该数据库来判断某电子现金是否已经使用过。随着时间的推移，该数据库将无限量地增大，这不仅给银行带来存储压力，也降低了电子现金的查询效率。若电子现金含有有效期，则银行就只需保留所有已经使用过、还未过期的电子现金，从而可以控制银行数据库的无限量增大。

2004 年彭冰等人提出了一个具有有限流通期限的离线电子现金系统[3]，该系统在目前效率较高的Brands的单条电子现金方案的基础上，加进了电子现金有限流通期限的概念，使银行数据库不至于无限制的膨胀。该系统采用的是基于乘法群上的离散对数的数字签名技术，但对于基于智能卡的电子现金系统而言，由于智能卡的容量非常有限，而椭圆曲线只需要较小长度的密钥就可以获得较高的安全性，采用基于椭圆曲线的数字签名效率更高[4]，因此本文采用基于椭圆曲线的数字签名技术，构建了一个基于椭圆曲线的含有效期的离线电子现金系统。

2 椭圆曲线的有关知识

2.1 有限域上的椭圆曲线

令F_q表示q个元素的有限域，$q = p^r$, p是素数，$r \geq 1$，令$E(F_q)$表示定义在F_q上的一个椭圆曲线，一般将$E(F_q)$简记为E。这里取r=1, p>3。

令$a, b \in F_q$满足 $4a^3+27b^2 \neq 0$，由参数a和b定义的F_q上的一个椭圆曲线为由方程$y^2=x^3+ax+b$的所有解(x, y), $x \in F_q$, $y \in F_q$连同一个称为“无穷远点”(计为O)的元素组成的点集合。$E(F_q)$的点数用$\#E(F_q)$表示，由Hasse定理可知公式：

$$p+1-2\sqrt{p} \leq \#E(F_q) \leq p+1+2\sqrt{p}$$

其中，$E(F_q)$的点集合对应加法规则构成一个群。

基金项目：国家电子信息发展基金及河北省信息产业发展计划基金资助项目(2005035025)；国家科技部高新技术计划基金资助项目(2005EJ000017)；河北省自然科学基金资助项目(F2005000368)
作者简介：刘文远(1968－)，男，教授、博士后，主研方向：虚拟企业，电子商务，数据挖掘；郭丽芳，硕士；王宝文，副教授；王亚东，教授、博士生导师
收稿日期：2007-10-20 **E-mail：**guolifang2005@163.com

2.2 椭圆曲线上的离散对数问题

令E是定义在F_q上的椭圆曲线，由椭圆曲线上的基本运算可知，椭圆曲线E上类似于F_q^*中 2 个元素乘积的运算是两点相加。在椭圆曲线上求一个点$P\in E$的k倍点$kP\in E$可用“重复加倍和加”方法来计算。椭圆曲线$E(F_q)$中所有点按点的加法规则组成一个有限阿贝尔群。

因此，在椭圆曲线点群上，有这样的问题：$E(F_q)$同上，P是$E(F_q)$上一个点，假设点Q是$E(F_q)$上为P的倍数的点，即存在整数$x>0$，使得$Q=xP$，则椭圆曲线离散对数问题就是给定的P和Q，确定出x。

2.3 椭圆曲线上离散对数的表示问题

令E是定义在有限域F_q上的椭圆曲线，椭圆曲线上的离散对数表示问题为：给定椭圆曲线上的一组阶数相同的公共基点$(P_1,P_2,\cdots,P_m)$和元素a，设其阶为L，找到整数组成的m元组$(x_1, x_2,\cdots, x_m)$，对所有 $1\le I\le m$，$0<x_i<L$，满足：

$$a = x_1P_1 + \cdots + x_iP_i + \cdots x_mP_m$$

椭圆曲线离散对数表示问题是椭圆曲线离散对数问题的推广。如果基点是随机选择的，则找到同一元素的两个不同表示和椭圆曲线离散对数一样困难。

3 基于智能卡的含有效期的电子现金方案

3.1 系统参数的建立

银行随机产生阶为L的一组基点(G,G_1,G_2,G_3)和一个正整数s $(0<s<L)$，作为银行签署电子现金的私钥匙，将s保密， 银行计算签名的公钥为 $P=sG$ ，用于有效期签名的公钥为 $P_e=sG_3$，银行公开$E(F_p)$、基点(G, G_1, G_2, G_3)、H和H_0，其中，H和H_0为无碰撞单向哈希函数，H用来构建和确认银行的签名以及在支付协议中计算质询串，H_0用来产生电子现金标识，记号||表示 2 个比特串的级联。

3.2 开户协议

开户协议是用户在发币银行进行账户登记的过程。当用户申请在银行处开户时，要先证明自己的真实身份，如出示身份证或护照等有效证件。在银行确认有效后，双方签署相应的合同。然后，用户的PC机产生一个随机数S_C $(0<S_C<L)$，作为PC机的私钥秘密保存，并计算PC机的公钥 $P_C=S_CG_1$，发给银行。

银行发给用户一张智能卡，卡内存有卡私钥S_T(由银行随机产生，不可伪造或篡改，$0<S_T<L$)和$a, b, G, G_1, G_2, G_3, T_e$等公开参数，其中，$T_e$为电子现金自取款日起有效的最大天数。卡公钥 $P_T=S_T+G_1$ 可印在卡的表面。

PC机计算并保存用户的公钥 $P_U=P_C+P_T$。可以看出，P_U同时含有PC机和智能卡的信息，银行不能模仿用户提取电子现金。同时，用户在支付电子现金时，如果没有智能卡的参加，PC机不能独立完成支付协议。用户和智能卡合成的公私钥匙分别为

$$S_U = S_C + S_T$$

银行同样计算 $P_U=P_C+P_T$ ，并将P_U作为用户的账号。账号的唯一性是很必要的，因为在多重花费的情况下，它能使银行唯一地识别用户。

随后，银行计算 $pk_0=P_U+G_2$ 并告之用户 $z_0=spk_0$。银行在账户数据库中新增一条记录，记载pk_0账户余额和用户的身份标识(身份证号或数字证书)。用户则保存pk_0, z_0以备后用。商家开户时，银行告之最大离线存储天数T_d。

3.3 提取协议

当用户想要从银行处自己的账户上提取电子现金时，就和银行一起执行提取协议，该提取协议实际上就是一个受限盲签名协议。

(1)智能卡随机选择$\xi_0$$(0<\xi_0<L)$，计算 $B=\xi_0G_1$ ，将B, T_e发送给用户PC机，同时保存ξ_0以备后用；

(2)PC机随机产生$t, \theta, \xi_1, \xi_2$$(0< t,\theta,\xi_1,\xi_2<L)$，计算有效期 $\lambda=current\_date+T_e$ 以及 $\overline{pk_0}=pk_0+\lambda G_3$ ， $\overline{z_0}=z_0+\lambda G_3$ 和电子现金的公钥 $pk_1=t\overline{pk_0}$ ， $pk_2=t\theta B+\xi_1G_1+\xi_2(G_2+\lambda G_3)$ ，随后PC机计算 $\overline{z_0}$ 的盲变换 $z=t\overline{z_0}$ ；

(3)银行在账户数据库中检索对应于用户的pk_0，同样计算λ和 $\overline{pk_0}$ ，随机产生$\omega_0$$(0<\omega_0<L)$，并计算 $a_0=\omega_0G$ ， $b_0=\omega_0\overline{pk_0}$ ，将它们发送给用户；

(4)PC机随机产生$u, v$$(0<u,v<L)$，将$a_0, b_0$盲变换为

$$a=a_0+uG+vQ\ ,\quad b=t(b_0+u\overline{pk_0}+v\overline{z_0})\ ,$$

然后，计算挑战 $c=H(pk_1\|pk_2\|z\|a\|b)$ 并在发送给银行前将其盲变换为

$$c_0=c-u(\mathrm{mod}\,L)\ ;$$

(5)银行计算并发送响应

$$r_0=\omega_0-c_0s(\mathrm{mod}\,L)$$

然后，从用户账户上扣除相应的数额；

(6)PC 机验证下列等式是否成立：

$$a_0=r_0G+c_0P \tag{1}$$

$$b_0=r_0\overline{pk_0}+c_0\overline{z_0} \tag{2}$$

若均成立，则计算$r=r_0+v(\mathrm{mod}\ L)$，最终用户得到经银行盲签名的电子现金$[pk_1, pk_2, \lambda, (z, c, r)]$；PC机保存电子现金和$B, t, \theta, \xi_1, \xi_2$以备后用。

从提取协议可以看出，Bank 从未看过(z, c, r)，本质上该协议是一个受限盲签名协议，因此，用户可以匿名地花钱。

3.4 支付协议

当用户在商家购物时，就和商家一起执行支付协议，支付协议的过程如下：

(1)用户将电子现金$[pk_1, pk_2, \lambda, (z, c, r)]$发送给商家并检索在取款时保存的$B, t, \theta, \xi_1, \xi_2$；

(2)商家首先核查用户提供的电子现金中的有效期λ是否不小于协议执行时的日期，其次验证银行对电子现金盲签名的正确性，即验证等式(3)是否成立：

$$c=H(pk_1\|pk_2\|z\|rG+cP\|rpk_1+cz) \tag{3}$$

若成立，则计算付款要求pay_claim，它包括商家身份ID_S、交易的时间pc_t、日期pc_d、交易金额pc_a以及一个随机数ε，将pay_claim传给用户；

(3)用户计算

$$m=H(pk1\|pk2\|pay\_claim),\ m_0=\theta m(\mathrm{mod}\,L)$$

并将m_0传给智能卡T；

(4)智能卡检索ξ_0，判断$\xi_0\neq0$ 和$m_0\neq0$ 是否成立，如果不成立则终止协议，成立则计算

$$\rho_0=S_T-m_0\xi_0(\mathrm{mod}\,L)$$

并把ρ_0传给用户，然后智能卡清除ξ_0；

(5)用户验证等式(4)是否成立：

$$P_T=\rho_0G_1+m_0B \tag{4}$$

若成立，则用户用私钥对消息m进行签名，得到(ρ_1, ρ_2)，其中，$\rho_1 = t(\rho_0 + S_C) - m\xi_1 (\mathrm{mod}\, L)$，$\rho_2 = t - m\xi_2 (\mathrm{mod}\, L)$，然后将签名传给商家；商家计算 $m = H(pk1 \| pk2 \| pay\_claim)$，然后验证用户提交的签名，即验证等式(5)是否成立：

$$\rho_1 G_1 + \rho_2 G_2 + \rho_3 G_3 = pk_1 - mpk_2 \quad (5)$$

若成立，则接收此电子现金，否则拒绝。

3.5 存储协议

商家将用户的付款信息传给银行，银行首先从商家提供的付款说明的pay_claim中提取pc_d，然后验证当前日期$current_date$是否不大于$\lambda+T_d$以及取款日期pc_d是否不大于λ。如果验证通过，则按商家相同的方式检验电子现金的有效性以及用户对付款要求pay_claim签名的正确性，若检验都通过，则在银行维护的记录有所有支付过、未到期的电子现金数据库中搜索pk_1，有 2 种可能：

(1)搜索失败。

即在此数据库中不存在pk_1，表明此电子现金是第 1 次使用，用户和商家都没有发生重复行为，则银行执行转账工作。

(2)搜索成功。

即在存款数据库中找到了pk_1，此时，用户或商家定有欺诈者，比较新发送来的电子现金与数据库中电子现金记录的字段，如果发现对电子现金的签名有相同的记录，则说明此电子现金被重复花费，银行进一步比较这 2 个记录的pc_d，如果相同，则说明商家企图重复存储，否则为用户重复花费，这时，银行会根据 2 次花费记录追踪出用户的身份信息。

4 安全性分析

本文提出协议的安全性是基于椭圆曲线密码体制的，椭圆曲线具有“密钥短，安全性高”的特点，更有利于用在处理能力较低的智能卡上，可以降低其复杂度和成本，同时又可提高协议的执行效率。

4.1 匿名性

此系统满足匿名性的要求。合法用户是匿名的，与具体的电子现金无关。本文的提取协议实质上是受限盲签名协议。在电子现金中加入了用户账号信息

$$pk_1 = t\overline{pk_0} = t(pk_0 + G_2 + \lambda G_3)$$

由于用户选择了盲因子 t 进行盲化，银行和商家都看不到用户的账号信息，因此用户对商家和银行来说满足了匿名性。银行不能根据一次支付的电子现金计算出用户的账号信息；如果商家重复存储或用户重复支付电子现金，那么银行可根据新发送来的信息和数据库已有的对应信息，查出商家或用户的账号，所以，协议满足公平匿名性。

4.2 不可伪造性

用户在取款时，要产生电子现金的公钥pk_1和pk_2，其中，pk_2是由PC机和智能卡共同产生的序列号。因为椭圆曲线上 $b = kP$ 是已知b求k的难解问题，而对于pk_2的表示

$$\begin{aligned} pk_2 &= t\theta B + \xi_1 G_1 + \xi_2 (G_2 + \lambda G_3) = \\ &(t\xi_0 + v\xi_0 + \xi_1 G_1 + \xi_2 G_2 + \lambda \xi_2 G_3) = \\ &x_1 G_1 + x_2 G_2 + x_3 G_3 \end{aligned}$$

它是已知pk_2求$x_1,\ x_2,\ x_3$的更难解问题，因此，其安全性与椭圆曲线离散对数问题的安全性等同，这就保证了其他人无法假扮这个用户来伪造电子现金的序列号。银行对用户产生的电子现金公钥进行受限盲签名，只有银行自己知道签署的私钥。因此，在椭圆曲线离散对数的条件下，其他人无法伪造银行的签名。

4.3 不可重复花费性

在本协议中，可以采用预先阻止和事后检测 2 种方法来有效解决重复花费问题。

如果智能卡的防篡改性没被破坏，那么用户不能重复花费电子现金。因为智能卡与 PC 机共同合作参与提取和支付协议，PC 机无法单独完成整个交易，用户不能用同一电子现金对应的私钥对不同的付款要求进行 pay_claim 签名。

即使用户成功破解智能卡中的监视程序，如果他重复花费电子现金，银行可以揭示出重复花费者的身份。因为在存储阶段，当银行发现用户或商家可能存在欺诈行为时，银行可以将商家新传递过来的pc_d与数据库中的交易时间进行比较，如果相同则说明商家企图在银行对重复存储同一电子现金；否则就是用户在商家重复花费同一电子现金，此时不论用户是否在同一商家处多次花费同一电子现金，都会使pay_claim不同，因此 2 次存储的记录不同，设新旧记录分别为(m,ρ_1,ρ_2)和(m',ρ_1',ρ_2')，银行可以计算出

$$S_U = (m'\rho_1 - m\rho_1')/\ (m'\rho_2 - m\rho_2'),\quad pk_0 = S_U G_1 + G_2$$

然后查询账户数据库对应于pk_0的记录，得到用户的真实身份，从而确保系统的安全性。

5 结束语

本文将基于椭圆曲线的离散对数的数字签名应用于基于智能卡的电子现金系统中，提出了一个基于智能卡的含有效期的离线电子现金系统。由于椭圆曲线密钥短的运算位数远小于传统离散对数的运算位数，而智能卡的存储空间又非常宝贵，因此将椭圆曲线应用于智能卡是一个很好的结合。系统对用户和商家使用电子现金的期限提出了限制，使银行可以定期删除数据库中过期的电子现金的记录，防止了银行数据库记录的无限制膨胀，提高了执行的效率，但是如何尽可能减少这种限制以处理诚实用户和商家由于不经意而造成的电子现金过期仍需进一步深入的研究。

参考文献

[1] Chaum D. Blind Signature for Untraceable Payment[C]// Proceedings of Advances in Cryptology-Eurocrypt’82. [S. 1.]: Plenum Press, 1983: 199-203.

[2] Yacobi Y. Efficient Electronic Money[C]//Proceedings of Asiacrypt’94. Wollongong, Australia: [s. n.], 1994: 153-163.

[3] 彭 冰, 杨宗凯, 谭运猛. 一个具有有限流通期的离线电子现金系统[J]. 通信学报, 2004, 25(6): 33-39.

[4] 郭 涛, 李之棠, 彭建芬, 等. 基于椭圆曲线的盲签名与离线电子现金协议[J]. 通信学报, 2003, 24(9): 142-146.