# 一种基于ECC的可恢复离线电子支付系统*)

郎为民[1] 杨宗凯[1] 吴世忠[2] 谭运猛[1]

(华中科技大学电子与信息工程系 武汉430074)[1] (中国国家信息安全测评认证中心 北京100091)[2]

**摘 要** 本文提出了一种高效的基于椭圆曲线密码体制(ECC)的可恢复电子支付系统,与传统的基于RSA及离散对数问题的电子支付系统相比,我们提出的系统所需安全参数字节较短且易于扩展,因而存储、计算和通信效率大大提高,同时也满足了所有的安全要求。此外,用户可以借助可信第三方(简称TTP)恢复因计算机崩溃或电子钱包遗失等原因而丢失的电子现金,并能有效防止重复花费、欺诈行为和高手段犯罪。

**关键词** 电子支付系统,椭圆曲线密码体制,盲签名,椭圆曲线离散对数问题

## A Recoverable Off-line Electronic Payment System Based on ECC

LANG Wei-Min[1] YANG Zong-Kai[1] WU Shi-Zhong[2] TAN Yun-Meng[1]

(Department of Electronic & Information, Huazhong University of Science and Technology, Wuhan 430074)[1]

(China National Information Security Testing Evaluation & Certification Center, Beijing 100091)[2]

**Abstract** This paper proposes an efficient recoverable electronic cash system. Compared with previous RSA based E-cash and Discrete Logarithm based E-cash systems, ECC possess fewer bits achieving the same security level as other public key cryptosystems, so our system requires much shorter security parameter size and it also scales better. That is to say, our new system improves the storage, computation and communication efficiency while keeping all the security features at the same time. With the help of Trusted Third Party(TTP), each consumer can recover the lost money even if the computer has crashed and all the files are removed accidentally, or his e-cash wallet has been lost. Furthermore, our system can prevent from double spending, fraud and perfect crime effectively.

**Keywords** Electronic payment systems, Elliptic curve cryptosystems, Blind signatures, Elliptic curve discrete logarithm problems(ECDLP)

## 1 引言

目前,电子现金支付已有不少协议和系统模型。Chaum等[3]提出了第一个不可追踪的离线电子现金支付系统。该系统中,一个电子现金包含多条信息,且每次用户从银行取款时,都采用分割选择技术。其安全性基于一些假设而且未作形式化的证明。该系统虽然不实用,但为后来的更安全、更高效的系统打下了基础。Ferguson[5]在电子现金支付系统中提出单条信息的概念。这意味着一个电子现金仅包含一条信息,而且用户在取款时不采用分割选择技术。Brands[2]提出第一个实用的单条信息电子支付系统。用户在取款过程中可将个人的身份信息通过零知识方法嵌入到盲签名中从而向银行证实自己的身份。Okomoto[4]提出了另一种实现单条信息的电子现金支付系统。该系统是通过用户在取款阶段由分割选择方法产生的电子证书来实现的。电子证书的更改可以通过再次执行开户协议来完成。银行可将同一电子证书产生的电子现金进行链接。Chan[1]提出的电子现金支付系统是迄今为止效率最高的电子现金支付系统。它将Okomoto[4]系统中执行开户协议时的效率提高了三个数量级,电子现金基于512字节的模的表示仅需要300个字节。但上述系统都是通过效率不高的模指数运算构建的,既需要进行大量的计算,又占用较大的系统空间。在Victor Miller[7]和Nei Koblitz[6]各自提出椭圆曲线加密算法后,ECC在密码领域得到了广泛的应用。Woei-Jiunn等[8]提出了一种基于PKI的安全电子支付系统,将ECC应用于电子现金支付系统,但其算法比较复杂。椭圆曲线密码体制与基于离散对数的传统公钥密码体制相比有两大优点:密钥长度较短和安全性更高。该算法在占有较小系统空间的情况下仍能达到与使用模指数运算的其他系统相同的安全水平。本文所提出的可恢复离线电子支付系统就是建立在椭圆曲线离散对数难解及散列函数单向性的基础上的。

本文第2节介绍相关的符号及其定义;第3节全面描述我们所提出的高效可恢复离线电子支付系统;第4节对系统进行安全性和效率分析;最后总结得出结论。

## 2 符号描述

本文中所用符号的意义:$x\in_R N$ 表示 $x$ 在集合 $N$ 中随机地选取,$H(\cdot)$表示碰撞自由的单向散列函数,$\|$表示字符串连接操作符,$R_x(A)$,$R_y(A)$表示取 $A$ 点的 $x$,$y$ 坐标。$p$,$q$ 表示大素数,$q$ 是 $p-1$的一个大的素因子(即 $q|(p-1)$),$Z_p^*$ 表示小于 $p$ 的正整数的集合,$G_q$ 表示乘法群 $Z_p^*$ 的一个 $q$ 阶子群,并且假定在 $G_q$ 上求解椭圆曲线离散对数是困难的。$Z_q$ 表示小于 $q$ 的非负整数的集合。$E$ 是椭圆曲线,其方程为 $y^2=x^3+$

*)基金项目:国家自然科学基金资助项目(90104033)。郎为民 博士研究生,研究方向为电子支付、信息安全和应用密码学。杨宗凯 博士生,教授,博士生导师,研究方向为电子商务、远程教育和网络安全。吴世忠 教授,主要从事网络攻防技术、应用密码学等研究。谭运猛 博士,副教授,研究方向为电子支付、信息安全和应用密码学。

$ax+b(4a^3+27b^2\neq 0)$，$B$ 为 $E$ 上一个阶为 $n$ 的基点(生成元)。

## 3 基于 ECC 的可恢复离线电子支付系统

具有可恢复性的离线电子支付系统除了银行、用户和商店等三个基本的参与方外，还包括可信第三方(Trusted Third Party，简称 TTP)。TTP 是一个具有电子认证功能的参与者，它不需知道任何与用户有关的隐私信息，仅仅是协助用户恢复丢失的电子现金而不参与用户和商店的支付活动。

### 3.1 初始设置

银行选择大素数 $p$，$q$ 且 $q|(p-1)$。$H(\cdot)$ 表示碰撞自由的单向散列函数。$G_q$ 表示乘法群 $Z_p^*$ 的一个 $q$ 阶子群，并且假定在 $G_q$ 上求解椭圆曲线离散对数是困难的。记 $B$ 为 $E$ 上一个阶为 $n$ 的基点(生成元)，选取 $x_B\in_R Z_p^*$ 作为银行的私钥，其对应的公钥 $P_B=x_BB$。银行公布 $p,q,B,H$ 和 $P_B$。

用户选取 $x_u\in_R Z_q^*$，计算 $I_u=x_uB=(R_x(I_u),R_y(I_u))$ 并将其发送给银行，作为用户的帐号，同时向银行出示其身份证或护照等来唯一标识其身份。银行验证其证明，并在其用户帐号数据库中存储用户的身份识别信息及 $I_u$，帐号 $I_u$ 与用户的身份信息必须一一对应。这样，在用户实施重复花费后，银行才能通过计算得到该用户帐号，进而确定其身份。

商店选取 $x_i\in_R Z_q^*$，计算 $I_i=x_iB=(R_x(I_i),R_y(I_i))$ 并将其发送给银行，作为商店的银行帐号。银行验证后存储商店帐号。

### 3.2 取款协议

(1)用户随机选取 $l\in_R Z_q^*$，计算 $a=lB=(R_x(a),R_y(a))$，$M=lP_B+dI_u=(R_x(M),R_y(m))$($d$ 是由银行和用户共同计算的电子现金的私钥)，$e'=H(R_x(M)\|R_y(M),R_x(a)\|R_y(a))$ 和 $\sigma=l-x_ue'$，这样一个电子现金 $c$ 就可以用一个二元组$(a, M)$来表示，$e'$，$\sigma$ 是签名，将 $M,e',\sigma$ 连同 $I_u$ 的值发送给银行。

(2)银行计算 $a'=\sigma B+e'I_u=(R_x(a'),R_y(a'))$，并验证 $e'\stackrel{?}{=}H(R_x(M)\|R_y(M),R_x(a')\|R_y(a'))$，若通过，则在调整用户帐面余额后，发送 $Cert_c$ 给用户。

(3)用户保存$\{l,d,Cert_c\}$的值。

### 3.3 标记协议

用户从银行端取得电子现金后，即可在 TTP 的帮助下，为每一个电子现金 $c$ 获取一个唯一的“身份标识”。此过程具体描述如下：

(1)用户发送 $c$，$Cert_c$ 给 TTP。

(2)TTP 在保存了 $c$ 的电子现金序列表中检测这些电子现金是否出现过(即 TTP 是否已经处理过)，若没出现，则检查电子现金 $c$ 和证书 $Cert_c$ 的合法性，对于每个电子现金，给定一个附加的数字 $x_i(1\leqslant i\leqslant n)$，$n$ 为用户一次从银行所取电子现金的个数，记

$$H(x_1)=y_1,H(x_2)=y_2,\cdots,H(x_n)=y_n$$

并对 $y_1,y_2,\cdots,y_n$ 和 $n$ 进行签名得到

$$S_T=sign_T\{y_1,y_2,\cdots,y_n,n\}$$

然后发$\{S_T,y_1,y_2,\cdots,y_n,n\}$给用户。

(3)用户保存$\{S_T,y_1,y_2,\cdots,y_n,n\}$用于恢复丢失的电子现金。

### 3.4 支付协议

(1)用户发送 $m$($m$ 是包含电子现金 $c$、数字证书 $Cert_c$ 和时戳等信息的数据段)和 $x_i$($x_i$ 为用户支付给商店的电子现金所对应的附加数字)给商店。

(2)商店验证电子现金和证书的合法性，并计算 $H(x_i)$，检查其是否在黑名单中(黑名单是丢失或者失效电子现金 $x_i$ 散列值的列表)。选择 $\varepsilon\in_R Z_q^*$，计算

$$r=H(date\|time\|\varepsilon,R_x(I_i)\|R_y(I_i))$$

其中 $date$、$time$ 分别为交易的日期和时间，并发送 $r$ 给用户。

(3)用户计算 $s=rP_B+dB=(R_x(s),R_y(s))$，$e=H(m,R_x(s)\|R_y(s))$，$u=r-le$，$v=d-x_ue$，$t_1=(d-1)x_ueB=(R_x(t_1),R_y(t_1))$，$(e,u,v,t_1)$即签名 $S$，发$(e,u,v,t_1)$及 $m$ 给商店。

(4)商店计算 $t'=uP_B+vB+eM=(R_x(t'),R_y(t'))$，并检查：

$$t'\stackrel{?}{=}s+t_1,e\stackrel{?}{=}H(m,R_x(t'-t_1)\|R_y(t'-t_1))。$$

### 3.5 存款协议

(1)商店发送支付协议的副本给银行，包括$(e,u,v,t_1)$及证书 $Cert_c$，电子现金 $c$、挑战 $r$ 和时戳。

(2)银行验证其合法性，并检查电子现金的 $H(x_k)$是否在黑名单中(银行在 TTP 的协助下也维护着一个记录丢失电子现金 $x_k$ 散列值的黑名单)。

### 3.6 恢复协议

如果用户选择了匿名性升级且丢失了电子现金，他可以通过执行如下协议加以恢复：

(1)用户将自己的身份信息公布给银行，并将$\{S_T,y_1,y_2,\cdots,y_n,n\}$和 $Cert_c$ 提供给银行。

(2)银行检查 TTP 在$\{y_1,y_2,\cdots,y_n,n\}$上的签名 $S_T$ 的合法性，并在支付信息数据库中查找序列号散列值为 $y_i(1\leqslant i\leqslant n)$的电子现金，其最大数目是 $n$，此即用户已花费的电子现金。

(3)银行计算用户所取电子现金总额与已花费电子现金的差，此即用户丢失的电子现金总额。

为防止用户伪挂失(即未丢失电子现金而向银行挂失)，银行可在用户挂失后采取如下步骤：

(1)银行将数字 $y_i(1\leqslant i\leqslant n)$加到黑名单中，并通过广播告知所有商店。

(2)商店将 $y_i(1\leqslant i\leqslant n)$加到黑名单中，如果用户使用电子现金 $x_i$ 的散列值 $y_i$ 等于黑名单中所列的散列值时，商店不再接受这个电子现金。

## 4 安全性和效率分析

本系统的安全性是建立在椭圆曲线离散对数难解和散列函数单向性基础上的。它具有不可重用性，即在用户实施重复花费后，银行可通过计算得到该用户帐号，进而确定其身份。其过程如下：

在本系统中，如果用户实施了重复花费，则同一电子现金在支付过程中将有两个签名 $S_1=(e_1,u_1,v_1,t_{11})$，$S_2=(e_2,u_2,v_2,t_{12})$，且有：

$$u_1=r_1-le_1,v_1=d-x_ue_1$$

$$u_2=r_2-le_2,v_2=d-x_ue_2$$

得到$(v_2-v_1)=x_u$，即用户 $I_u$ 的私钥。因此，在本系统中用户的电子现金是不可重用的。

本系统具有受限的不可追踪性。当用户构造一个电子现金时，要用到私钥 $x_u$，该参数在支付过程中对任何其他人是不可知的。因此没有人能够根据电子现金的支付信息来追踪

(下转第83页)

$A7$: $A$ Receives $x$ TimestampedWith $t$ SignedWith $K_T^{-1}$
$K_T$ Authenticates $T$
$A$ CanProve ($T$ IsTrustedOn $t$)
⇒$A$ CanProve ($A$ Receives $x$ At $t$)

$A8$: $M$ CanProve ($M$ Receives $x$ At $t$)
$x$ in $m$
$N$ CanProve($N$ Receives $m$ SignedWith $K_M^{-1}$)
$K_M$ Authenticates $M$
⇒$N$ CanProve ($M$ Receives $x$ At $t$)

4.2.4 协议目标的证明 由 $M$ Receives $M6$ TimestampedWith $T_1$ SignedWith $K_T^{-1}$

$A5$, $A1$ $\{A7\}$⇒$M$ CanProve ($M$ Receives $M6$ At $T_1$)

由 $N$ Receives $M8$ TimestampedWith $T_2$ SignedWith $K_T^{-1}$

$A5$, $A1$ $\{A7\}$
⇒$N$ CanProve ($N$ Receives $M8$ At $T_2$)
($M7$ SignedWith $K_M^{-1}$)in $M8$
$M6$ in $M7$
$M$ CanProve ($M$ Receives $M6$ At $T_1$)
$A3$ $\{A8\}$
⇒$N$ CanProve ($M$ Receives $M6$ At $T_1$)
⇒$N$ CanProve ($M$ Submit during $T_p$)

## 参考文献


1 Sirbu M, Tygar J D. NetBill: an internet commerce system optimized for network delivered services [J]. IEEE Personal Communications, 1995, 2(4): 34～39
2 Cox B, Tygar J D, Sirbu M. NetBill Security and Transaction Protocol. In: Proc. of the First USENIX Workshop on Electronic Commerce, July 1995. 77～88
3 Tygar J D. Atomicity in Electronic Commerce, ACM-Mixed Media, April 1998
4 Heintze N, Tygar J D, Wing J, Wong H C. Model checking electronic commerce protocols. In: Proc. USENIX 1996 Workshop on Electronic Commerce, Nov. 1996
5 Lichota R W, Hammonds G L, Brackin S H. Verifying Cryptographic Protocols for Electronic Commerce. In: Proc. of the 2nd USENIX Workshop on Electronic Commerce, 1996. 53～65
6 郭云川,古天龙,董荣胜,蔡国永. NetBill 协议原子性的符号模型检验分析. 计算机工程与应用,2003,39
7 梁坚, 敖青云, 尤晋元. 安全协议的时限责任分析. 电子学报, 2002,30(10):1450～1454
8 Kailar R. Accountability in electronic commerce protocols [J]. IEEE Trans. on Software Engineering, 1996, 22(5): 313～328
9 Syverson P. Adding time to a logic of authentication [A]. In: Proc. of the 1st ACM Conf. on Computer and Communications Security [C]. Fair-fax: ACM, 1993. 97～101
10 Burrows M, Abadi M, Needham R M. A logic of authentication. Report. 39[R]. Palo Alto, CA: DEC System Research Center, 1989
11 Abadi M, Tuttle M R. A semantics for a logic of authentication [A]. In: Proc. of the 10th Annual ACM Symposium on Principles of Distributed Computing [C]. 1991. 201～216
12 Kudo M. Electronic submission protocol based on temporal accountability [A]. In: Proc. of 14th Annual Computer Security Application Conf. [C]. Phoenix: ACSA, 1998. 353～363
13 Papa M, Bremer O, Hale J, Shenoi S. Formal Analysis of E-Commerce Protocols. In: Proc. of the 5th Intl. Symposium on Autonomous Decentralized Systems. 2001. 19～28


(上接第75页)

用户。而且,由于 $I_u$ 的椭圆曲线离散对数 $x_u$ 是难解的,对用户进行非法攻击从而伪造签名是不可能的。但如果用户丢失电子现金并试图进行恢复时,他必须向银行公开其身份信息,另外,除非用户实施了重复花费,用户身份将不可能被追踪。

本系统能够有效地防止欺诈行为和高手段犯罪。一是如果用户向银行伪报失。虽然系统不能预防此类现象的发生,但当用户恢复得到电子现金时,原有的电子现金因为被列入黑名单而失效。二是商店可能持有用户的电子现金,直到用户丢失其电子现金后他才将其存入银行。表面看来,用户挂失时可能会取得比其丢失数额更大的电子现金。但事实并非如此,若商店迟迟不将电子现金存入银行,银行将拒绝接受,因为它们已经被列入了黑名单。三是对高手段犯罪的预防。高手段的犯罪是电子支付领域出现的一个新问题,由于电子现金的持有者可能被绑架或杀害,犯罪分子将会使用受害人的电子现金。当犯罪分子胁迫用户将电子现金从银行中取出并企图进行花费时,用户可以向银行挂失,通过将这些被盗电子现金列入黑名单且广播告知所有商店,商店都将不会再接收已经失效了的电子现金。

与基于 RSA 和离散对数问题的电子支付系统(如 Okamoto[4]和 Chan[1]提出的电子现金支付系统)相比,本文所提出的可恢复离线电子支付系统由于采用了椭圆曲线密码体制,故所需的安全参数字节较短且易于扩展,在占有较小系统空间的情况下仍能达到与使用模指数运算等其他系统相同的安全水平,因而存储、计算和通信效率大大提高。如 RSA 加密体制进行模指数运算时需要1024比特的密钥,在 ECC 中若要达到相同要求则只需160比特即可。因此 ECC 中密钥的长度较短,内存空间和计算能力都可以降低,尤其适用于存储容量有限的基于智能卡的电子钱包。而且在提取协议中,可以采用将 $a=lB=(R_x(a),R_y(a))$, $M=lP_B+dI_u$, $e'=H(R_x(M)\|R_y(M)$, $R_x(a)\|R_y(a)$和 $\sigma=l-x_ue'$等运算进行前置处理的方法来提高在线处理速度,以减小银行执行取款协议时的计算和通信开销。

**结论** 本文设计了一个基于 ECC 的高效可恢复离线电子现金系统。与传统的基于效率不高的模指数运算的电子支付系统相比,ECC 具有密钥长度较短和安全性更高的特点,从而使得本系统的存储、计算和通信效率大大地提高。而且用户在丢失电子现金后,通过向银行挂失,并与其执行恢复协议,仍然可以继续使用剩余的未花费的电子现金,而不必向 TTP 公开自己的身份信息。此外,本系统还能有效地防止重复花费、窃听、篡改、非法攻击和犯罪。

## 参考文献


1 Chan A, Frankel Y. Easy come-easy go divisible cash. In Advances in Cryptology - Eurocrypt 98, LNCS, Springer-Verlag, 1998. 561～575
2 Brand S. Untraceable Off-line Cash in Wallet with Observers. In Advances in Cryptology - Crypto 93, LNCS, Springer-Verlag, 1994. 302～318
3 Chaum D, Fiat A, Naor M. Untraceable electronic cash. In Advanced in Cryptology - Crypto 88, volume 403 of Lectures Notes in Computer Science, Springer-Verlag, 1990. 319～327
4 Eng T, Okamoto T. Single-Term Divisible Coins. In Advances in Cryptology-Eurcrypt 94, LNCS, Springer-Verlag, 1994. 306～313
5 Ferguson N T. Single Term Off-line Coins. In Advances in Cryptology-Eurcrypt 93, LNCS, Springer-Verlag, 1994. 318～328
6 Koblitz N. Elliptic curve cryptosystems, Mathematics of Computation, 1987, 48(17): 203～209
7 Miller V S. Use of elliptic curves in cryptography. In Advances in Cryptology - Crypto 85, LNCS, Springer-Verlag, 1985. 417～462
8 Tsaur W-J, Ho C-H. A Secure Electronic Payment System Based on Efficient Public Key Infrastructure. In: Proc. of the 2002 Intl. Workshop for Asian Public Key Infrastructures (IWAP 2002), Taipei, Taiwan, 2002