

# 具有委托、代理功能的可分割电子现金系统

叶振军<sup>1</sup>, 王春峰<sup>1</sup>, 张庆翠<sup>2</sup>

(1. 天津大学管理学院, 天津 300072; 2. 国家开发银行天津分行, 天津 300061)

**摘要:** 为使电子现金的使用更具安全性、便利性, 将代理签名与可分割电子现金技术相结合, 实现了一个具有委托、代理功能的电子现金系统。它一方面允许用户将电子现金分成任意金额进行多次支付, 另一方面又可以在电子现金所有者授权的情况下, 代理人代其执行取款以及支付等相关活动。

**关键词:** 电子现金; 代理签名; 二叉代表树

## Divisible E-cash System with the Function of Trust and Proxy

YE Zhenjun<sup>1</sup>, WANG Chunfeng<sup>1</sup>, ZHANG Qingcui<sup>2</sup>

(1. College of Management, Tianjin University, Tianjin 300072; 2. Tianjin Branch of China Development Bank, Tianjin 300061)

**【Abstract】** To use electronic cash more securely and conveniently, an E-cash system with the function of trust and proxy is proposed with the technologies of proxy signature and E-cash. It allows a cash user to subdivide the electronic coin into many pieces to allow each subdivided piece to be worthy any desired value less than the electronic coin and the total value of pieces equal to it. And on the other hand, the proxy can withdraw and pay a coin in place of the cash owner with his warrant.

**【Key words】** E-cash; Proxy signature; Binary representative tree

电子现金(E-cash)是一种重要的电子支付系统,其最简单的形式包括3个主体(商家、用户和银行)和4个安全协议过程(初始化协议、提款协议、支付协议和存款协议)。第一个电子现金方案是由Chaum于1982年提出并利用盲签名技术实现的,该方案在完全保护用户隐私的同时,也为不法分子利用电子现金的完全匿名性进行违法犯罪活动提供了方便。所以,合理的电子现金系统应该是不完全或条件匿名的。1995年,Stadler等人提出了公平盲签名(fair blind signature)的概念,可以用于条件匿名的支付系统。1996年,Camenisch等人 and Frankel等人分别提出了公平的离线电子现金(fair off-line electronic cash)的概念,同时给出了两个方案。公平电子现金中的用户的匿名性是不完全的,它可以被一个可信赖的第三方(TTP)撤消,从而可以防止利用电子现金的完全匿名性进行的犯罪活动。这些系统在很大程度上改进了Chaum的方案,但在这些系统中,电子现金只能作为整体使用,而不能被分为更小的部分多次使用。Okamoto和Ohta于1991年首次提出了一个可分割的电子现金系统,该系统允许用户将电子现金分成任意金额进行多次支付,极大地促进了电子现金的广泛使用。然而,在电子商务活动中,往往管理者并不亲自从事划账等财务工作,他们往往通过财务人员甚至专门的服务机构去从事这些活动,这就使得代理支付成为电子商务活动中必须实现的一个功能,它要求执行代理功能的人员或机构必须获得相应的支付权限,同时又必须受委托者的监督和控制。本文采用代理签名技术对Okamoto和Ohta的可分割电子现金系统进行改进,使其更好地适用于电子商务支付环境。

### 1 电子现金应具备的性质及其设计流程

电子现金与普通现金的作用一样,应该具备安全性、保密性、方便性、可传递性以及可分性等几个性质。其设计流

程一般包括如下几个步骤:

(1)开户协议(The opening account protocol):用户向银行申请一个账户。

(2)取款协议(Withdrawal Protocol):用户从自己的银行账户上提取电子现金。为了保证用户匿名的前提下获得带有银行签名的合法电子现金,用户将与银行交互执行盲签名协议,同时银行必须确信电子现金上包含必要的用户身份。一般取款协议分为如下两步子协议:

1)开户协议:这一步通常计算量大,用于向用户提供包含其身份信息的电子执照。

2)取款协议。这一步只是单纯的盲签名过程,用户能够从其账户中提取电子现金。

(3)支付协议(Payment Protocol):用户使用电子现金从商店中购买货物。通常也分为两个子协议:

1)验证协议:验证电子现金的签名,用于确认电子现金是否合法。

2)知识泄露协议:买方将向卖方泄露部分有关自己身份的信息,用于防止买方滥用电子现金。

(4)存款协议(Deposit Protocol):用户及商家将电子现金存入到自己的银行账户上。在这一步中银行将检查存入的电子现金是否被合法使用。

### 2 具有代理功能的电子现金系统

#### 2.1 系统采用的数据存储结构

在该电子现金系统中,采用二叉树作为数据存储结构,它使得电子现金C被分成若干碎片,这些碎片的总额恰好等

**基金项目:** 国家杰出青年科学基金资助项目(70225002)

**作者简介:** 叶振军(1976-),男,博士生,主研方向:金融工程与金融管理,电子金融等;王春峰,教授、博导;张庆翠,博士

**收稿日期:** 2006-03-20 **E-mail:** yie\_tju@126.com

于  $C$  (如图 1 所示, 这里  $C = \$100$ )。Okamoto 等人给这种二叉树的使用规则作了两点限制: (1) 当一个结点被用过, 无论它的孩子结点还是它的父亲结点都不可再次使用; (2) 任何一个结点都只能用一次, 而不能被多次使用。这些限制的目的在于防止超额消费。

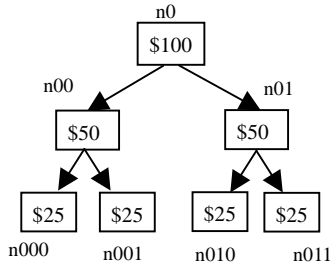


图 1 二叉代表树

## 2.2 系统参数

$p$  是一个大素数,  $q$  为  $q-1$  的大素因子,  $g \in Z_p^*$ , 且  $g^q \equiv 1 \pmod p$ 。Alice(原始签名者), Mike(代理签名者)的私钥为  $x_A, x_B \in \{1, 2, \dots, q-1\}$ , 公钥为  $y_A = g^{x_A} \pmod p$ ,  $y_B = g^{x_B} \pmod p$ 。

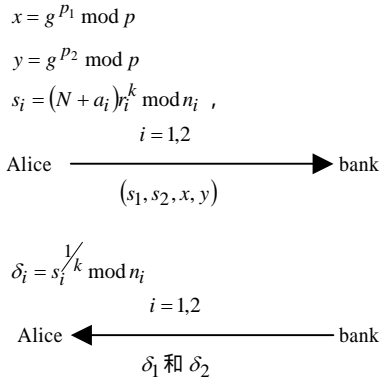
## 2.3 方案实施步骤

### (1) 开户协议

1) 银行公布它的公钥  $(n_1, k)$ 、 $(n_2, k)$  和  $(a_1, a_2)$ , 并发送一个素数  $p$  和一个生成元  $g$  ( $g \in Z_p^*$ )。

2) Alice 随机选择两个素数  $p_1$  和  $p_2$ , 计算  $x = g^{p_1} \pmod p$ ,  $y = g^{p_2} \pmod p$ , 并将  $x$  和  $y$  发送给银行。她同时还要发送  $s_1$  和  $s_2$  给银行(其中  $s_i = (N + a_i)r_i^k \pmod{n_i}$ , 这里  $i = 1, 2$ ,  $N = pq$ )。

3) 在 Alice 向银行证明了  $(s_1, s_2, x, y)$  是诚实产生的之后, 银行向 Alice 发送  $\delta_1$  和  $\delta_2$ , 其中  $\delta_i = s_i^{1/k} \pmod{n_i}, i = 1, 2$ 。具体过程如下所示:



### 4) Alice 计算

$$L_i = (N + a_i)^{1/k} \pmod{n_i} = \frac{\delta_i}{s_i} \pmod{n_i} \quad (i = 1, 2)$$

这时 Alice 便有了自己的电子许可证  $(N, L_1, L_2)$ 。

### (2) 委托取款协议(假设 Alice 的取款额为 $w$ )

1) Alice 随机选择一个数  $k \in Z_q^*$ , 计算  $r = g^k \pmod p$ , 然后计算代理签名密钥  $s = x_A + kr \pmod q$ 。并将  $(s, r)$  以安全的渠道发送给代理 Mike。

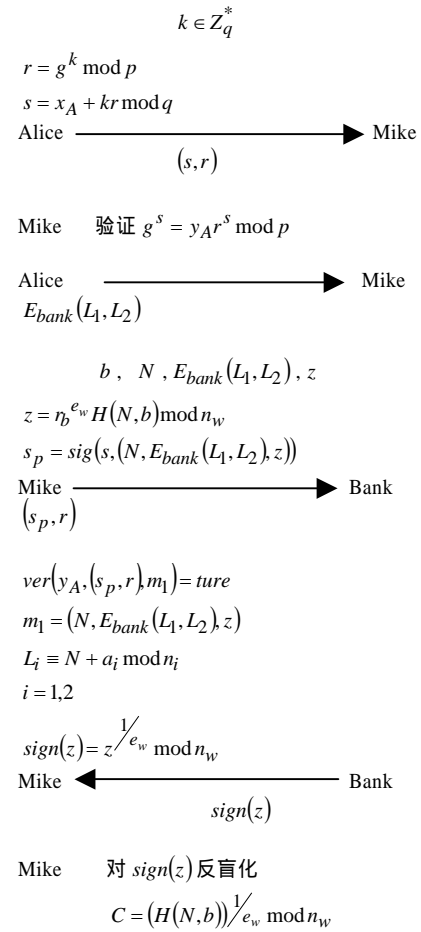
2) Mike 检查等式  $g^s = y_A r^s \pmod p$  是否成立, 如果成立则接受, 否则拒绝。

3) 如果 Mike 接受, 则 Alice 用银行的公钥加密  $(L_1, L_2)$ , 得到  $E_{bank}(L_1, L_2)$  并将其与  $N$  一起通过安全渠道发送给 Mike。

4) Mike 选择一个随机数  $b$ , 然后计算  $z = r_b^{e_w} H(N, b) \pmod{n_w}$  (其中  $r_b \in Z^{n_w}$  是一个随机整数,  $H$  是一个单向 Hash 函数)。对于  $N$ 、 $E_{bank}(L_1, L_2)$  和  $z$ , Mike 产生普通签名  $s_p = \text{sig}(s, (N, E_{bank}(L_1, L_2), z))$ , 然后以  $(s_p, r)$  作为他代表 A 对于消息  $N$ 、 $E_{bank}(L_1, L_2)$  和  $z$  的数字签名(即代理签名)并通过安全渠道发送给银行。

5) 银行收到消息  $m_1$  和代理签名  $(s_p, r)$ , 并验证  $\text{ver}(y_A, (s_p, r), m_1) = \text{ture}$ , 验证  $m_1 = (N, E_{bank}(L_1, L_2), z)$  以及  $L_i \equiv N + a_i \pmod{n_i}$  ( $i = 1, 2$ ) 是否成立, 如果成立则认为代理签名成立, 对  $z$  签字并在 Alice 的账户上扣除  $w$ , 然后银行将  $\text{sign}(z)$  发送给 Mike (其中  $\text{sign}(z) = z^{1/e_w} \pmod{n_w}$ ), 否则拒绝。

6) 这时 Mike 可以对  $\text{sign}(z)$  反盲化并将其用作自己的现金  $C$ , 其中  $C = (H(N, b))^{1/e_w} \pmod{n_w}$ 。实现过程如下所示:



### (3) 支付协议

支付协议由两个部分组成, 即现金认证和币值显示。在现金认证阶段, Bob 验证现金合法性。

1) Alice 用 Bob 的公钥加密  $(L_1, L_2)$ , 得到  $E_{Bob}(L_1, L_2)$ , 并以安全渠道送给代理 Mike。

2) Mike 向 Bob 发送  $(s_p, r)$ 、 $E_{Bob}(L_1, L_2)$ 、 $N$ 、 $(C, b)$  和  $w$ 。

3) Bob 通过验证  $\text{ver}(y_A, (s_p, r), m) = \text{ture}$ , 其中  $m = (N, E_{Bob}(L_1, L_2), (C, b), w)$ , 并计算  $L_i \equiv N + a_i \pmod{n_i}$  ( $i = 1, 2$ ), 来验证电子许可证的合法性。

4) Bob 通过计算  $C^{e_w} \equiv H(N, b) \pmod{n_w}$  来验证电子现金上银行的 RSA 签名。

5) Bob 验证  $J(-1, N) = 1$  和  $J(2, N) = -1$ 。操作步骤如下：

Alice  $\xrightarrow{E_{Bob}(L_1, L_2)}$  Mike

Mike  $\xrightarrow{(s_p, r), E_{Bob}(L_1, L_2)}$  Bob  
 $N, (C, b), w$ 。

Bob 验证  $ver(y_A, (s_p, r), m) = true$

其中

$m = (N, E_{Bob}(L_1, L_2), (C, b), w)$

$L_i = N + a_i \bmod n_i \quad (i = 1, 2)$

$C^e_w = H(N, b) \bmod n_w$

验证  $J(-1, N) = 1$  和  $J(2, N) = -1$

#### (4)存款协议

这个协议很简单，Bob 仅需发送一个支付副本给银行。

### 2.4 性能分析

由于 Okamoto 和 Ohta 的可分割电子现金系统基于 RSA 机制建立，因此其安全性来源于大数分解的困难性。同时，将代理功能绑定到电子现金的取款、支付等步骤中，使其在保证安全的情况下增添委托代理的机能，从而更好地实现电子现金安全、灵活、便捷的特性。

### 3 讨论

本文结合代理签名技术对 Okamoto 和 Ohta 的可分割电子现金系统进行改进，使其成为一个具有委托、代理功能的电子现金系统，它可以使得商家或用户在交易或使用过程中委托他人进行相应的交易或支付活动，从而可以更好地应用于电子商务支付环境，为商业软件的开发提供了一种可选择的方案。此外，该方案中给出的实现步骤相对较细，在项目实施过程中可以灵活使用所给出的步骤，为方案的实施提供了一定的灵活性。

(上接第 139 页)

防护。认证通过后的应用通信阶段，驱动可以随时进行重新认证，而设备内部也可根据授权有效期的定时长度来进行重新认证，实现了对 USB 信道的安全维护。

### 5 结论

普通 USB 存储设备的识别方式不能满足身份锁设备的安全性要求，身份锁只有在此基础上，继续完成驱动软件和设备可信身份确认，才能确保在主机与身份锁之间建立起一条真正安全可靠的 USB 传输信道。本文提出的厂商认证协议能够为身份锁驱动和设备提供可靠的身份认证质量，有效地实现主机对身份锁设备的强化识别，目前正在以 Cygnal 公司的 F320 型 8 位 51 单片机和飞利浦的 LPC2104 型 32 位 ARM7 单片机为核心处理器的身份锁设备中实现应用。该协议也可以应用于具有高安全性要求的 USB 设备中，进一步加强设备的识别，为实现设备功能提供可靠的基本保证。

### 参考文献

- 1 Chaum D. Blind Signature for Untraceable Payments[C]//Proceedings of Crypto'82, Plenum. 1983: 199-203.
- 2 Chaum D, Fiat A, Naor M. Untraceable Electronic Cash[C]//Advances in Crypto'88. Springer-Verlag. 1988: 319-327.
- 3 Chaum D. On-line Cash Checks[C]//Proceedings of Eurocrypt'89. Springer-Verlag. 1990: 288-293.
- 4 Camenisch J, Maurer U, Stadler M. Digital Payment Systems with Passive Anonymity-revoking Trustees[C]//Proceedings of Esorics'96. Springer-Verlag. 1996: 33-43.
- 5 Brands S. Untraceable Off-line Cash in Wallets with Observers[C]//Advances in Cryptology Crypto '93. Springer-Verlag. 1993: 302-318.
- 6 Eng T, Okamoto T. Single-term Divisible Electronic Coins[C]//Advances in Cryptology Eurocrypt'94. Springer-Verlag. 1994: 311.
- 7 Okamoto T. An Efficient Divisible Electronic Cash Scheme[C]//Advances in Cryptology Crypto'95. Springer-Verlag. 1995: 438-451.
- 8 Okamoto T, Ohta K. Universal Electronic Cash[C]//Advances in Cryptology Crypto'91, Lecture Notes in Computer Science. Springer-Verlag. 1992: 324-337.
- 9 Brickell E, Gemmell P, Kravitz D. Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change[C]//Proc. of the 6<sup>th</sup> ACM-SIAM Symposium on Discrete Algorithms. New York: ACM Press. 1995: 457-466.
- 10 Ferguson N T. Single Term Off-line Coins[C]//Advances in Cryptology Eurocrypt'93, Lecture Notes in Computer Science. Springer-Verlag. 1993: 318-328.
- 11 Sander T, Ta-Shma A. Auditible, Anonymous Electronic Cash[C]//Advances in Cryptology Crypto'99, Lecture Notes in Computer Science. Springer-Verlag. 1999: 555-572.
- 12 Varadharajan V, Nguyen K Q, Mu Y. On the Design of Efficient RSA Based Off-line Electronic Cash Schemes[J]. Theoretical Computer Science. 1999, 226(1/2): 173-184.

### 参考文献

- 1 Universal Serial Bus Specification[R]. Compaq, Intel, Microsoft, NEC, 1998.
- 2 Simpson W. PPP Challenge Handshake Authentication Protocol (CHAP)[S]. RFC1994, 1992-10.
- 3 周立功. PDIUSB12 USB 固件编程与驱动开发[M]. 北京: 北京航空航天大学出版社, 2002.
- 4 Microsoft Corportio. Windows 2000 驱动程序开发大全(第 1 卷)——设计指南[M]. 冯博琴, 译. 北京: 机械工业出版社, 2001.
- 5 刘 阳, 朱方金, 史清华. 一个 CHAP 认证协议的改进方案[J]. 计算机工程, 2005, 31(5): 168-169.
- 6 任传伦, 李远征, 杨义先. CHAP 协议的分析 and 改进[J]. 计算机应用, 2003, 23(6): 36-37.
- 7 李 丹, 龙毅宏. MD5 算法破解对实际应用的影响[J]. 信息安全与通信保密, 2005, (4): 91.