电子月票*

杨 波, 张 彤, 王育民

(西安电子科技大学 综合业务网国家重点实验室,陕西 西安 710071)

E-mail: yangbo@mail.xidian.edu.cn

摘要: 提出了一种电子月票系统.用户从银行提取一笔款项后,可在有效次数范围内购买网上的服务,其付费方式不是以购买的信息量的多少进行,而是以购买的次数进行.这样既方便了用户,又方便了网上的服务提供者.

关键词: 电子月票;电子钱包;提款;支付

中图法分类号: TP393 **文献标识码**: A

在大多数电子现金系统中,电子现金都是不可分割支付的.这样,用户一次需支付多少,就要在银行提取多少;或者一次提取很多不同面值的电子现金先存起来,以后根据需支付的款额,再决定支付哪种电子现金,参看文献[1~5].但这些系统都有不方便之处.

本文在文献[4]的基础上提出一种电子现金系统,用户在银行一次提取的电子现金可分若干次支付,比如说月票30次、季票90次.与可分的电子现金系统(如文献[6])相比,这种电子现金每次支付的数额是一定的,因此我们称其为电子月票.就像乘车时的月票一样,虽然这一次乘车距离较短,但可能下次距离较长,然而每次收费都是一样的.这样既方便了乘客又方便了公交公司,因而受到乘客和公交公司的欢迎.电子月票可用于客户定期或不定期访问某一网站时进行支付,如阅读电子报刊杂志、观赏影视作品,或享受网上的其他服务.用户按这种方式购买服务不是按购买的信息量的多少来支付,而是按购买的次数来支付,所以对用户和服务提供者(以下简称商家)都很方便.同时,本系统是不在线的,即提款、支付、存款都不同时进行.所以,本文提出的电子月票系统避免了不可分割电子现金系统使用中的不便之处,还避免了可分电子现金系统过于复杂的问题.

该方案中利用电子钱包[2,7,8]的方式,用户的提款是在自己的终端进行,所提款项存在自己的电子钱包中.提款协议使用盲签字技术,这可避免用户先获取银行颁发证书然后再提款这样两步进行.

为了防止用户在脱机支付时重复花费电子现金,物理上安全的设备(如防窜扰的Smart卡)通过去掉已花费过的电子现金或使其变得无效,从而可在一般情况下防止电子现金的重复花费,因为一般的用户并无修改防窜扰卡的资源.然而,实际中并无绝对防窜扰的卡.所以,即使使用防窜扰卡,我们仍然有必要提供密码保护来防止电子现金的重复花费.

1 系统设置

设系统中有银行B、用户U、商家M,U有一个电子钱包(其中的Smart卡S是用户在银行开户

* 收稿日期: 2000-04-15; 修改日期: 2001-01-25

基金项目: 国家自然科学基金资助项目(19931010,69972034)

作者简介: 杨波(1963—),男,陕西临潼人,博士,副教授,主要研究领域为电子商务中的安全理论与技术,密码学中的无条件安全,信息隐匿技术;张彤(1967—),男,陕西西安人,博士生,副研究员,主要研究领域为电子商务中的安全理论与技术,信息隐匿技术;王育民(1936—),男,北京人,教授,博士生导师,主要研究领域为信息论,密码,编码.

时由银行发放的).

又设 G_q 是素数阶 q 的循环群.

B 作如下设置:产生 $x,y\in_R Z_q$,$g_0\in_R G_q\setminus\{1\}$,并设 $h=g_0^x$,$g_1=g_0^y$,确定一个 Hash 函数 $H(\cdot)$,公开 h,g_0,g_1,H. 建立账目数据库以存储有关账目持有者的信息,建立存款数据库以存储与支付文本相关的信息.账目数据库中的数据是与用户的身份信息相联系的,存款数据库则不是,它仅出现于商家在银行的存款协议中,用于防止同一笔钱的重复花费.

2 用户在银行的开户

U 在银行开户时,执行如下过程:

B 产生 $x_i\in_R Z_q$,以 $I_i=x+yx_i$ 作为 U 的身份号,B 在 U 的账目数据库中存 I_i 及 U 的余款数 balance′.

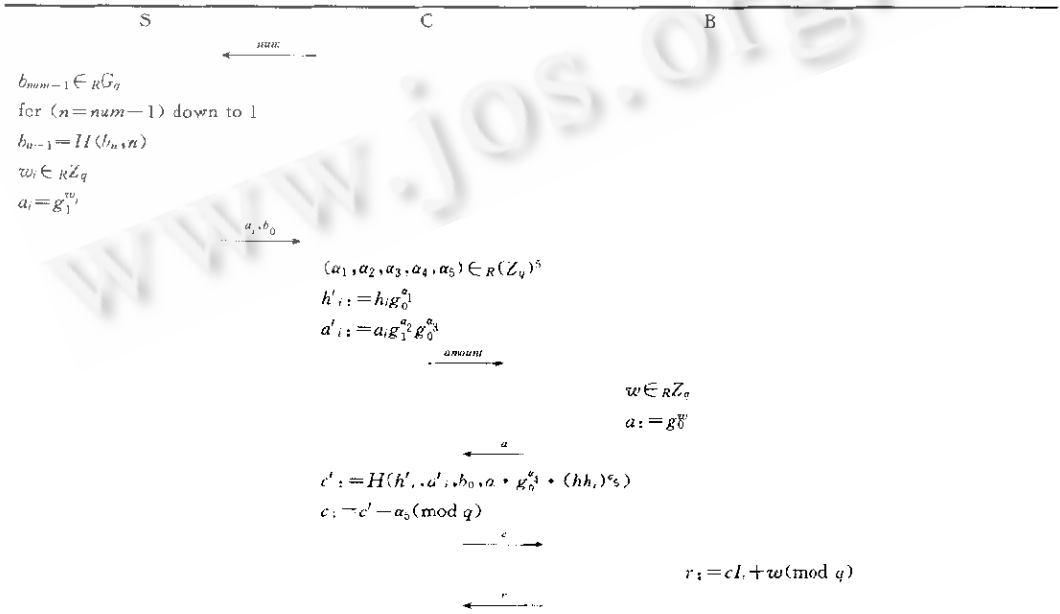
B 发给 U 一个防窜扰的 Smart 卡,该卡存有如下信息:

- x_i,g_1,G_q 和 $H(\cdot)$的描述.
- 记数器 balance,用于记录用户所持有的款数.
- 银行的密钥 z.
- 顺序号 seq,用于记录提款的次数.初始值设置为 0.
- 单向函数 $f(\cdot)$.该函数可取某一分组密码,如 DES.

同时,B 将 $h_i=g_1^{x_i}$ 发给 U,U 在其计算机 C 中存 h_i,g_c,g_1,h 以及 G_q 和 $H(\cdot)$的描述.

3 提款协议

设用户 U 欲在 B 购买一笔电子月票,包括 num 张,其金额为 $amount$(由每张的金额及 num 而定),U 首先向 B 出示自己的身份及身份号 I_i,B 检查 I_i 是否与 U 的账目数据库中的 I_i 一致.若一致,则执行下面的提款协议:



$g_0^{f_0}(hh_i)^{-c'} \stackrel{?}{=} a$

$r' := r + c'\alpha_1 + \alpha_4 \pmod q$

$balance' := balance' - amount$

$v := f(z, seq, amount)$

$seq := seq + 1$

$\xleftarrow{v, amount, date/time}$ $v, amount, date/time$ $\xleftarrow{v, amount, date/time}$

$v \stackrel{?}{=} f(z, seq, amount)$

$seq := seq + 1$

$balance := balance + amount$

store $w_i, amount, date/time$

其中 $balance'$ 是在 B 建立的账目数据库中 U 的记数器,用于记录 U 在银行的余款数. $date/time$ 是用户在银行提款的日期和时间.银行为了保证其账目数据库不致无限大,应定期更新,即用户所提款项在一定时间内有效.用户应在所提款项的有效期内支付.协议中假定用户所持的卡具有透支功能,若不具有透支功能,则 B 在收到 $amount$ 时应先判断 $amount \leqslant balance'$ 是否成立,如果不成立,协议则停止执行.协议由 3 部分组成,首先 S 产生 num 个值 $b_{num-1}, b_{num-2}, \ldots, b_1, b_0$,称为支付链,其中每一值称为支付字,表示一张月票,b_0 称为链头[9~11].第 2 部分,S 产生 $a_i = g_1^{w_i}$,用于它拥有 x_i 的零知识证明. C 将 h_i, a_i 变盲,并获得 B 的盲签字 (r', c').第 3 部分,U 将所提款项存于 S,其中 $v = f(z, seq, amount)$ 和 $seq = seq + 1$ 用于防止重放攻击.

4 用户在商家的支付协议

S C M

$\xleftarrow{(h'_i, a'_i)}$

w_i present?

IF $n = 1$ **THEN BEGIN**

$d := H(h'_i, a'_i, b_0, amount, date/time)$

$r_{i1} := dx_i + w_i \pmod q$

$n := n + 1$

$\xrightarrow{r_{i1}}$

$d := H(h'_i, a'_i, b_0, amount, date/time)$

$g_1^{r_{i1}} h_i^{-d} \stackrel{?}{=} a_i$

$r'_{i1} := r_{i1} + \alpha_2 \pmod q$

$r_{i2} := d\alpha_1 + \alpha_3 \pmod q$

$\xrightarrow{h'_i, (r', c'), (a'_i, r'_{i1}, r_{i2}), b_0, amount, date/time}$

$c' \stackrel{?}{=} H(h'_i, a'_i, g_0^{r'}(hh'_i)^{-c'})$

$d := H(h'_i, a'_i, b_0, amount, date/time)$

$g_1^{r_{i1}} g_0^{r_{i2}} (h'_i)^{-d} \stackrel{?}{=} a'_i$

store $h'_i, (r', c'), (a'_i, r'_{i1}, r_{i2}), amount, date/time$

ENDIF

IF $1 <= n$ **AND** $n <= (num - 1)$ **THEN BEGIN**

w_i present?

$\xrightarrow{b_n, n}$ b_n, n $\xrightarrow{b_n, n}$ $b_{n-1} \stackrel{?}{=} H(b_n, n)$

$n := n + 1$

store b_n, n

ENDIF

IF $n = num$ **THEN**

erase w_i

用户在商家的支付协议如上所示.用户首先建立一个化名及相应的地址,并向商家出示自己的化名及地址.在第1次支付时,U 向 M 出示 B 的肯签字、支付链的链头以及 S 拥有 x_i 的零知识证明.以后每次支付时仅需向 M 出示一个支付字,当 n 等于 num 时,月票用完.

5 商家在银行的存款协议

M 在 B 存款时,向 B 发送文本 $h'_i,(r',c'),(a'_i,r'_{i1},r_{i2}),b_0,b_1,\ldots,b_{num-1},amount,date/time$,$B$ 首先作如下检查:

$$\text{for } (n=num-1) \text{ down to } 1$$

$$b_{n-1}=H(b_n,n)$$

然后在存款数据库中搜索(h'_i,r',c').这存在两种可能:

(1) 搜索失败,即存款数据库中不存在这组值.B 计算 $d:=H(h'_i,a'_i,b_0,amount,date/time)$,验证 $c'=H(h'_i,a'_i,b_0,g_0^{r'}(hh'_i)^{-c'}$ 和 $g_1^{r'_{i1}}g_0^{r_{i2}}(h'_i)^d=a'_i$.如果验证成功,$B$ 在存款数据库中为 M 存 $d,r_{i1}',date/time$,并在账目数据库中为 M 入账 $amount$.

(2) 搜索成功,即在存款数据库中搜索到了这组值.此时 U 或 M 必定有欺诈者,若 M 新发送的文本中的 $date/time$ 与存款数据库中已有文本的 $date/time$ 一样,则 M 试图在 B 存储同一文本两次.否则,U 在 M 两次支付同一款项,设存款数据库中已存有 M 的一对数(d,r'_{i1}),M 现在正要存的一对数是(d',r''_{i1}),则由

$$\begin{cases}r'_{i1}=dx_i+w_i+\alpha_2 \pmod q\\ r''_{i1}=d'x_i+w_i+\alpha_2 \pmod q\end{cases}.$$

B 可得 $x_i=(r'_{i1}-r''_{i1})/(d-d') \pmod q$,则 $I_i=x+yx_i$ 是试图两次支付同一款项的用户的身份号.

6 安全性分析

在支付协议和存款协议中,M 和 B 得到 $h'_i,(r',c'),(a'_i,r'_{i1},r_{i2}),b_0,b_1,\ldots,b_{num-1},amount,date/time$,其中 $h'_i,(r',c'),(a'_i,r'_{i1},r_{i2})$ 是 h_i,a_i,r,c 变盲后的结果,而 $b_0,b_1,\ldots,b_{num-1},amount,date/time$ 不包含 U 的身份信息.可以证明(证明过程略),有惟一的一组盲因子 $\alpha_1,\alpha_2,\alpha_3,\alpha_4,\alpha_5$ 满足以下关系:

$$h'_i=h_ig_0^{\alpha_1},c'=c+\alpha_1 \pmod q,r'=r+c'\alpha_1+\alpha_4 \pmod q,$$

$$r'_{i1}=dx_i+w_i+\alpha_2,r_{i2}=d\alpha_1+\alpha_3,a'_i=a_ig_1^{\alpha_2}g_0^{\alpha_3},$$

其中 r,c 满足 $g_0^r(hh_i)^{-c}=a;h'_i,(r',c'),(a'_i,r'_{i1},r_{i2})$ 满足

$$g_1^r(hh'_i)^{-c'}=a\cdot g_0^{\alpha_4}\cdot(hh_i)^{\alpha_5},$$

$$g_1^{r'_{i1}}g_0^{r_{i2}}(h'_i)^d=a'_i.$$

M 和 B 若想从他们所接收到的支付文本中获得 U 的身份信息,只能惟一地通过这一组盲因子,但由于这一组盲因子是 U 秘密选取的,因此 M 和 B 无法得到 U 的身份信息.所以,支付协议和存款协议可以有效地保护合法用户的匿名性.

M 需要记录用户的 $b_0,b_1,\ldots,b_{num-1}$,一方面是因为 U 在每次支付其中一个值 $b_n(n=1,\ldots,num-1)$时,M 需要检查这个值以前是否用过以及 $H(b_n,n)$ 是否等于前一个值,这样可以防止 U

伪造并重复使用b_n,而且U如果伪造b_0,那么M和B得到的$d=H(h'_i,a'_i,b_0,amount,date/time)$就不可能满足$c'=H(h'_i,a'_i,b_0,g_0^{r'}(hh'_i)^{-c'})$和$g_1^{r'_{i1}}g_0^{r_{i2}}(h'_i)^{-d}=a'_i$.因此,假的$b_0$也将被检测出.$U$伪造$h'_i,(r',c'),(a'_i,r'_{i1},r_{i2})$的困难性与破译Schnorr签字[12]是一样的.所以得出结论:用户不能伪造电子月票.

至于商家得到电子月票而不提供服务或者用户得到服务却声称没有得到,这是有关公平交易的问题,本文不予考虑.

本方案有一个限制,即用户的一笔款项只能购买同一商家的服务.用户如果对另一商家的网上服务感兴趣的话,则需购买另一电子月票.

7 结 论

本文利用电子钱包提出了一种电子月票系统,一方面它可方便交易的各方.另一方面,能有效地保护合法用户的匿名性,并且防止电子月票的伪造及重复使用.

References:

[1] Yang, Bo, Zheng, Dong, Wang, Yu-min. A new kind of electronic cash system. Journal of Xidian University, 1998,25(5):616~620 (in Chinese).

[2] Yang, Bo, Wang, Yu-min. A fair payment system by electronic wallet. Chinese Journal of Computers, 1999,22(8):792~796 (in Chinese).

[3] Yang, Bo, Liu, Sheng-li, Wang, Yu-min. An anonymity-revoking electronic payment system. Journal of Xidian University, 1999,26(4):420~422 (in Chinese).

[4] Yang, Bo, Liu, Sheng-li, Wang, Yu-min. An anonymity-revoking electronic payment system by smart card. Acta Electronica Sinica, 1999,27(10):83~86 (in Chinese).

[5] Brands, S. Off-Line cash transfer by smart cards. Technical Report, CS-R9455, Amsterdam: CWI (Centre for Mathematics and Computer Science), 1994. http://www.cwi.nl/static/publications/reports/CS-R9455.

[6] Okamoto, T., Ohta, K. Universal electronic cash. In: Feigenbaum, J., ed. Proceedings of the Crypto'91. LNCN 576, Berlin: Springer-Verlag, 1992. 324~337.

[7] Brands, S. Untraceable off-line cash in wallets with observers. In: Stinson, D. R., ed. Advanced in Cryptology Crypto'93. Berlin: Springer-Verlag, 1994. 302~312.

[8] Chaum, D., Pedersen, T. Wallet database with observers. In: Brickell, E. F., ed. Proceedings of the Crypto'92. Berlin: Springer-Verlag, 1992. 89~105.

[9] Anderson, R., Manifavas, C., Sutherland, C. NetCard——a practical electronic cash system. In: Christianson, B., ed. Proceedings of the 4th Cambridge Workshop on Security Protocols. Cambridge: Springer-Verlag, 1996. 49~57.

[10] Rivest, R., Shamir, A. Payword and micromint: two simple micropayment schemes. In: Christianson, B., ed. Proceedings of the 4th Cambridge Workshop on Security Protocols. Cambridge: Springer-Verlag, 1996.

[11] Lipton, R., Ostrovsky, R. Micro-Payments via efficient coin-flipping. In: Hirschfeld, R., ed. Proceedings of the Financial Cryptography'98 Conferences. Heidelberg: Springer Verlag, 1998. 1~15.

[12] Schnorr, C.P. Efficient signature generation by smart cards. Journal of Cryptology, 1991,4(3):161~174.

附中文参考文献:

[1] 杨波,郑东,王育民. 一种新的电子货币系统.西安电子科技大学学报,1998,25(5):616~620.

[2] 杨波,王育民.利用电子钱包的可撤销匿名性的电子支付系统.计算机学报,1999,22(8):792~796.

[3] 杨波,刘胜利,王育民.一种可撤销匿名性的电子支付系统.西安电子科技大学学报,1999,26(4):420~422.

[4] 杨波,刘胜利,王育民.利用Smart卡的可撤销匿名性的电子支付系统.电子学报,1999,27(10):83~86.

An Electronic Monthly Ticket*

YANG Bo, ZHANG Tong, WANG Yu-min

(*National Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*)

E-mail: yangbo@mail.xidian.edu.cn

Abstract: In this paper, an electronic monthly ticket system is proposed. After a user makes a withdrawal from a bank, he can purchase the serve over the Internet within the scope of effective times. The payment is done according to the times purchased by the user instead of the information amount. So it is convenient both for users and service providers.

Key words: electronic monthly ticket; electronic wallet; withdrawal; payment

* Received April 15, 2000; accepted January 25, 2001

Supported by the National Natural Science Foundation of China under Grant Nos. 19931010, 69972034