一个改进的基于限制性盲签名的电子现金系统

王常吉[1], 裴定一[1], 蒋文保[2]
(中国科学技术大学研究生院信息安全国家重点实验室, 北京 100039; 中国科学院高能物理研究所计算中心, 北京 100039)

摘 要: 本文简述了电子现金系统的研究成果及其发展现状, 并对文 Brands 提出的基于限制性盲签名的电子现金系统作了改进, 提出了一个新的电子现金系统, 在用户提取的由银行盲签名的电子现金中, 嵌入有由银行规定的该电子现金的有效期, 银行只需保留所有已经使用过的、还未过期的电子现金, 这就大大地减少了银行的存储量.

关键词: 盲签名; 限制性盲签名; 知识证明的签名
中图分类号: TP393.08 文献标识码: A 文章编号: 0372-2112 (2002) 07-1083-03

An Improved E-Cash System Based on Restrictive Blind Signature

WANG Chang-ji[1], PEI Ding-yi[1], JIANG Wen-bao[2]
(1. *State Key Lab. of Information Security, Graduate School of USTC, Beijing* 100039, *China*;
2. *Computer Center of Institute of High Energy Physics of CAS, Beijing* 100039)

Abstract: In this paper, we reviewed the art of e-cash in brief, and improved the Brands' e-cash system based on the restrictive blind signature. In our new e-cash system, the withdrawal date and expiry date, prescribed by the bank are embedded in the withdrawn e-cash. Users cannot alter these information later, the bank only needs to keep all used and undue e-cash in his database to trace the double-spender. Thus it reduces the storage level and improves the querying efficiency of the bank to detect double-spending.

Key words: blind signature; restrictive blind signature; signature of proof of knowledge

1 引言

电子现金较传统现金的一个最显著的优点是它能够实现用户支付的匿名性. D. Chaum[2] 最早利用盲签名实现了匿名的电子现金系统, 电子现金容易被复制, 因此匿名的、离线电子现金系统, 必须具有能防止电子现金被重复花费的机制, D. Chaum 等[3] 提出一次显示盲签名的概念, 银行能够追踪电子现金的重复花费者, 而又不牺牲合法用户的匿名性. S. Brand[1] 提出盲签名的限制性假设, 有效实现了一次显示盲签名. 文[4] 在文[1] 的基础上, 最早提出匿名性可控制的所谓公正的电子现金系统, 之后文[5] 等对文[1]、[4] 作了改进. 文[6] 等提出利用群盲签名实现有多个银行参与发行的电子现金系统, 文[7] 提出利用二叉树结构实现可分电子现金系统, 这些系统都非常复杂, 并且需要引进一些新的安全性的假设.

对离线电子现金系统, 为了防止电子现金的重复花费, 目前主要有两种解决方法: 一是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; 二是通过密码技术, 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, 该数据库将无限制地增大, 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, 然而, 由于为实现电子现金的匿名性而采用盲签名的特性, 银行不能直接将有效期嵌入在电子现金中. 本文改进了文[1] 的电子现金系统, 银行计算电子现金的取款日期与有效日期的单向散列值, 作为文[1] 中的素数阶群 G_q 的生成元 g_2, 这样就能保证银行的电子现金数据库不会无限制地增大, 大大地减少了银行的存储压力.

第二节介绍文中出现的记号及基本工具; 第三节介绍系统的设置; 第四节详细讨论电子现金系统的取款、支付和存款协议, 以及重复花费者的跟踪协议, 并分析了系统的安全性; 第五节是本文所得出的结论.

2 记号与基本工具

$x \stackrel{?}{=} y$ 表示判断 x 是否等于 y, 如果 $x \neq y$, 协议随之终止; p, q 为两个大素数, 且 $q \mid p-1$, G_q 表示乘法群 Z_p^* 的一个 q 阶子群, 在 G_q 上求解离散对数是计算上不可行的; m 表示和知识证明的签名有关的消息, 可以是空串 ζ; 将 $x = y \bmod p$ 简记为 $x = y$.

定义 1 (限制性盲签名协议)[1]: 令 $\tilde{m} \in G_q$ (通常是一个向量) 为 m 的被盲化后的值, 请求者在盲签名开始时, 知道 $\tilde{m}$ 关于生成元组 $(g_1, g_2, \cdots, g_k)$ 的表示为 $(a_1, a_2, \cdots, a_k)$, 签名

收稿日期: 2001-04-02; 修回日期: 2001-07-07
基金项目: 国家自然科学基金(No. 19931010)

者验证 $\tilde{m}$ 的内部结构, 协议结束后, 请求者知道 m 关于$(g_1, g_2, \cdots, g_k)$的表示记为$(b_1, b_2, \cdots, b_k)$, 若存在函数 I_1 和 I_2, 使得不管请求者采用何种盲变换以及 m 的形式, 都有 $I_1(a_1, a_2, \cdots, a_k) = I_2(b_1, b_2, \cdots, b_k)$, 则称此协议为限制性盲签名协议. 并称函数 I_1 和 I_2 为协议关于$(g_1, g_2, \cdots, g_k)$的盲不变函数.

若证明者想向验证者证明他知道 h 关于底g 的离散对数(即 $x = \log_g h$)的知识, 并用这个离散对数对消息 $m \in \{0,1\}^*$ 做签名, 他可以通过以下的步骤来实现:

® 证明者→验证者: 选择 $s \in_R Z_q^*$ (表示 s 在 Z_q^* 中随机选取), 计算 $h' = g^s$, $c = H(m \| g \| h \| h')$和 $r = s - cx \bmod q$ ($\|$表示串的连接操作, H 表示无碰撞单向散列函数), 传送 (c, r)给验证者.

® 验证者: 检验 $c \stackrel{?}{=} H(m \| g \| h \| g^r h^c)$.

定义 2[4,5] 满足 $c = H(m \| h \| g^r h^c)$ 的二元组(c, r)称为是 h 关于底g 的离散对数的知识, 对于消息 $m \in \{0,1\}^*$ 的签名, 记为: $SPK\{\alpha \mid h = g^\alpha\}(m)$.

3 系统设置

银行设置: 选群 G_q 以及 G_q 的一个生成元组(g, g_1), 签名私钥 $x \in Z_q^*$, 无碰撞单向散列函数 H_0、H_1 和 $\Psi: \{0,1\}^* \mid \rightarrow \{0,1\}^{len}$ ($len < |p|$, $|p|$ 表示 p 的比特长度), 公开其公钥 $y = g^x$, 以及 H_0、H_1、Ψ(为简单起见, 只考虑单一面额和单一有效期, 不同签名私钥对应电子现金的不同面额, 不同单向散列函数 Ψ 对应电子现金的不同有效期.)

用户设置(开户协议): 选取 $u_1 \in_R Z_q^*$, 计算 $I_U = g_1^{u_1}$ 作为用户的银行账号, 并将知识证明的签名 $SPK\{\alpha \mid I_U = g^\alpha\}(m)$ 传给银行, 这里 m 表示用户的身份识别信息, 银行验证此知识证明的签名, 若验证成功, 存储 I_U 与用户的身份识别信息.

4 离线的电子现金系统

4.1 取款协议

(1) 用户→银行: 用户先通过身份识别协议(如 Schnoor 协议), 向银行证明自己是其账号的持有者, 然后将取款需求 (W_date, E_date, 面值, 数量等)传送给银行.

(2) 银行→用户: 银行先验证用户提交的身份识别协议, 然后选取 $w \in_R Z_q^*$, 计算 $a_0 = g^w$, $\hat{g}_2 = \Psi(W\_date \| E\_date)^{(p-1)/q}$, $b_0 = (I_U \hat{g}_2)^w$, $Z_0 = (I_U \hat{g}_2)^x$, 传送 a_0, b_0, z_0 和 W_date 与 E_date 给用户.

(3) 用户→银行: $x_1, x_2, s, u, v \in_R Z_q^*$, 计算 $\hat{g}_2 = \Psi(W\_date \| E\_date)^{(p-1)/q}$, $B = g_1^{x_1} \hat{g}_2^{x_2}$, $A = (I_U \hat{g}_2)^s$, $z = z_0^s$, $a = a_0^u g^v$, $b = b_0^{su} A^v$, $c = H_0(A \| B \| z \| a \| b)$, $c_0 = c/u \bmod q$, 传送 c_0 给银行.

(4) 银行→用户: 计算 $r_0 = w + c_0 x \bmod q$, 传送 r_0 给用户, 同时借记用户的账号.

(5) 用户: 检查 $g^{r_0} \stackrel{?}{=} y^{c_0} a_0$ 和 $(I_U \hat{g}_2)^{r_0} \stackrel{?}{=} z_0^{c_0} b_0$, 若验证通过, 则计算 $r = v + r_0 u \bmod q$.

取款协议实际上是一个盲签名协议, 一个签名 $Sign(A, B) = (z, a, b, r)$ 有效, 当且仅当 $g^r = y^{H_0(A \| B \| z \| a \| b)} a$ 和 $A^r = z^{H_0(A \| B \| z \| a \| b)} b$ 成立. 用户得到的电子现金为 $Coin = \{A, B, Sign(A, B), W\_date, E\_date\}$.

4.2 支付协议

(1) 用户→商家: 用户将电子现金 $Coin$ 发送给商家.

(2) 商家→用户: 验证电子现金 $Coin$ 上银行的签名, 若验证通过, 则计算质询串 $d = H_1(A \| B \| I_S \| P\_date/time)$ 然后将质询串 d 传送给用户. 其中 I_S 表示商家在银行的账户, $P\_date/time$ 表示支付的日期与时间.

(3) 用户→商家: 用户计算出应答 $r_1 = d(u_1 s) + x_1 \bmod q$, $r_2 = ds + x_2 \bmod q$, 将(r_1, r_2)发送给商家.

(4) 商家: 计算 $\hat{g}_2 = \Psi(W\_date \| E\_date)^{(p-1)/q}$, 然后检验 $g_1^{r_1} \hat{g}_2^{r_2} \stackrel{?}{=} A^d B$, 若检验通过, 则接受用户的支付, 否则拒绝.

4.3 存款协议

商家传送支付协议的一个副本给银行, 银行先检查电子现金是否已经过期, 然后(如商家一样地)检验电子现金上银行的盲签名 $Sign(A, B) = (z, a, b, r)$ 是否有效, 若检验都通过, 则在其维护的记录有所有已经支付过、未到期的电子现金数据库中搜索 A, 有两种可能:

(1) 搜索失败, 即在此数据库中不存在 A, 表明此电子现金是第一次使用, 银行在此数据库中存储(A, r_1, r_2, I_S)和 $P\_date/time$, 并且为商家入账.

(2) 搜索成功, 即在存款数据库中找到了 A, 此时, 用户或商家定有欺诈者, 比较新发送来的电子现金记录与数据库中电子现金记录的字段 I_S 与 $P\_date/time$, 若相同, 则商家试图在银行存储同一电子现金两次, 否则是用户重复支付电子现金(此时质询串一定不同), 银行计算出数据库中 A 相应的质询串 d' (可以由商家的账号 I_S 与交易日期 $P\_date/time$ 计算出), 记数据库中记录 A 对应的元组为(d', r'_1, r'_2), 新提交的电子现金记录对应的元组为 (d, r_1, r_2), 银行计算出 $g_1^{(r_1 - r'_1)/(r_2 - r'_2)} = I_U$, 银行由此在其账号数据库中查找与账号 I_U 对应的用户的实际身份识别信息, 从而找到了试图两次支付同一电子现金的用户.

4.4 安全性分析

本文的工作主要是用 $\hat{g}_2 = \Psi(W\_date \| E\_date)^{(p-1)/q}$ 替换文[1]中的生成元 g_2, 其中 Ψ 是一个单向散列函数(如 SHA_1, $MD5$ 等, 它将任意比特长度的数字串映射为固定长度$< |p|$ 的串), 只要 $\hat{g}_2 \neq 1$(这很容易判断), 则 $\hat{g}_2$ 是 G_q 的一个生成元. 和文[1]作相同的假设, 即假设在 G_q 中求离散对数问题是计算上困难的, 就可以保证电子现金的不可伪造性; 取款协议实质上是限制性盲签名协议($I_U \hat{g}_2$ 相当于限制性盲签名定义中的 m, $(I_U \hat{g}_2)^s$ 相当于限制性盲签名定义中的$\tilde{m}$, 关于$(g_1, \hat{g}_2)$的盲不变函数 $I_1(a_1, a_2) = I_2(a_1, a_2) = a_1 : a_2$), 在电子现金中嵌入有用户的识别信息(即账号 I_U), 商家和银行在支付和存款协议中, 获得的数据有 A, B, $Sign(A, B)$, r_1, r_2, 其中 B, r_2 不含用户的识别信息 I_U, 而 A, r_1, $Sign(A, B)$ 都是 I_U 盲化后的结果, 商家和银行若想从接收到数据中得到用户的识别信息(即 I_U), 必须知道盲因子 s, 而 s 是用户随机选取

并保密的,这就保证了电子现金的匿名性.

5 结论

本文改进了文[1]的基于盲签名限制性假设的电子现金系统,使得在用户从银行提取的由银行盲签名的电子现金中,嵌入有银行载明的该电子现金的有效期,从而银行只需保留所有已经使用过的、还未过期的电子现金,大大地减少了银行的存储量.

参考文献:

[1] S Brands. Untraceable Off line Cash in Wallets with Observers [A]. In Advance in Cryptology-Crypto'93 [C]. German: Springer-Verlag, 1993. 302-318.

[2] D Chaum. Blind signatures for untraceable payments [A]. Proc. of CRYPTO'82 [C]. Berlin: Plenum Press, 1983. 199-203.

[3] D Chaum, A Fiat, M Naor. Untraceable Electronic Cash [A]. In Advance in Cryptology-Crypto'88 [C]. German: Springer-Verlag, 1988. 319-327.

[4] Y Frankel, Y Tsiounis, M Yung. Indirect discourse proof: achieving fair off-line e-cash [A]. Proc. of Asiacrypt'96 [C]. German: Springer-Verlag, 1996. 286-300.

[5] Frankel Y, Tsiounis Y, Yung M. Fair off-line e-cash made easy [A]. Proc. of Asiacrypt'98 [C]. Berlin: Springer-Verlag, 1998. 257-270.

[6] L Anna, R Zulfikar. Group Blind Digital Signatures: A scalable solution to electronic cash [A]. In Financial Cryptography'98 [C]. German: Springer-Verlag, 1998. 184-191.

[7] Okamoto T. An efficient divisible electronic cash scheme [A]. Proc. of Crypto'95 [C]. German: Springer-Verlag, 1995. 438-451.

[8] 王常吉,裴定一. 一类公正的离线的电子现金方案 [J]. 计算机应用, 2001, 21(3): 9-11.

作者简介:

王常吉　男,1972 年 2 月出生于湖南省衡山县,1990 年 9 月至 1994 年 7 月,就读于湖南吉首大学数学系,获理学学士学位;1994 年 9 月至 1997 年 7 月,就读于广州中山大学应用数学系,获理学硕士学位;1997 年 7 月至 1999 年 7 月,任教于广州业余大学计算机系;1999 年 9 月至今,就读于中国科技大学研究生院信息安全国家重点实验室,师从裴定一教授,研究方向为电子支付和密码学理论与应用.

裴定一　男,1941 年 8 月出生于江苏省常州市,博士生导师,1964 年毕业于中国科技大学应用数学专业,同年考入该系研究生,师从华罗庚教授,1978 年 12 月至 1981 年 3 月在美国普林斯顿大学数学系进修,现为信息安全国家重点实验室学术委员会主任,主要研究方向为认证码,椭圆曲线等理论与应用.

蒋文保　男,1969 年 11 月出生,1989 年~1993 年,武汉水电大学自动化系学习,获工学学士学位,1993~1996 年,武汉水电大学自动化系学习,获工学硕士学位,1996 年~1999 年,深圳华为工作,1999 年至今,中国科学院高能物理研究所计算中心攻读博士学位,研究方向为电子商务.

勘误

《电子学报》30 卷 2002 年第 4 期 586 页中图 6 应改为下图

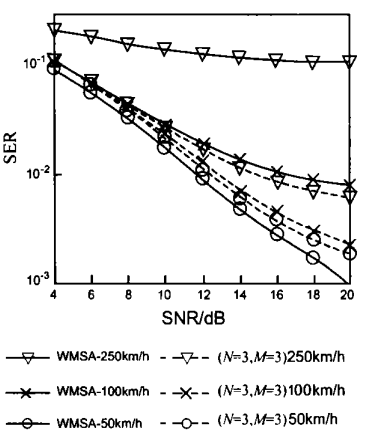

图 6　多项式重建算法与 WMSA 算法的性能比较