对 Brands 电子现金方案的一种改进*

李 进，林 群，王燕鸣
（中山大学数学与计算科学学院，广东 广州 510275）

摘 要：电子现金支付系统是电子商务发展的关键，目前出现的电子现金方案在银行发行多种面值的电子现金时都是使用最直接的方法：即银行选择不同的私钥和公钥对来发行不同面值的电子现金，从而导致银行需要对多个私钥进行保密。利用限制性盲签名的特点，提出了一种基于 Brands 离线电子现金方案的高效的多种面值电子现金方案，银行只用保密一个私钥即可发行不同面额的电子现金，从而提高银行以及整个系统的安全和效率。

关键词：电子现金；多种面值；限制性盲签名
中图分类号：TP 309 文献标识码：A 文章编号：0529-6579（2005）03-0114-03

电子现金支付系统是电子商务发展的关键，目前为止出现了很多优秀的电子现金系统。相对于信用卡支付以及支票支付等形式，电子现金支付方式具有提供用户匿名性以及便捷性的特点，从而是未来电子支付的一种重要的手段。电子现金系统一般需要 3 方的参与：银行（Bank B），消费者（Customer C），商家（Merchant S）。一个完整的支付过程一般需要 3 个过程：提取过程（withdraw），支付过程（payment）和存储过程（deposit）。

根据消费者在支付给商家时是否需要银行的参与又可分为：在线支付（on line）和离线支付（off-line）。1982 年，Chaum[1] 提出了一种基于 RSA 的盲签名方法，并且构造了第一个在线的电子现金系统。在线电子现金在每次支付时都需要银行的参与，从而降低了效率，增加银行的成本。因此设计一个离线的电子现金系统是电子现金系统研究的重点，然而由于电子现金的可复制性，因此如何防止双重花费是设计离线电子现金系统的一个难点。1988 年，Chaum 等[2] 在文 [1] 的基础上提出了第一个离线电子现金方案，它使用公平分割的方法来防止双重花费，但是由于公平分割协议计算的复杂性大大降低了效率。1993 年，Brands 克服了公平分割所带来的大量计算，文中使用了一种基于离散对数问题的限制性盲签名方法设计出了一种高效的单一（single term）离线电子现金方案，这种方案由于它的高效和安全性已经成为一个经典的电子现金方案（到目前为止还没有发现对它的有效攻击方法），后来很多别的电子现金系统以及对电子现金的一些性质的补充如公平性和可分性[4-6] 等都是在文 [3] 的基础上进行改进的。

一个电子现金系统中银行必须要能够发行多种不同面值的电子现金，然而目前的离线电子现金方案中银行进行多种面值现金的发行时都是直接采用银行使用不同的公钥和私钥对进行区分，使用这种方法银行就必须对更多的私钥进行保密，而且如果电子现金面额种类比较多的时候，银行需要保密的私钥的长度是比较大的。对于一个电子现金支付系统而言，银行用来发行电子现金的私钥是整个系统安全与否的关键，所以保密更多的私钥显然不利。虽然构造了一种部分盲签名方法来达到同样的目的，但是部分盲签名效率太低而且对于防止双重花费以及公平性和可分性都很难实现。在本文中，我们使用一种新的方法在基于 Brands 电子现金系统提出了一种简单的多面值方案：银行保存一个私钥即可实现多种面值电子现金的发行，而且效率以及安全性和原方案一样。

1 多面值的 Brands 电子现金方案

银行参数设置：（假设银行需要发行 n 种不同面值的电子现金）银行选择大素数 q，p 满足 $p-1=kq$；g，g_1 是 Z_p 上的两个 q 阶生成元（q 阶生成元 g 的产生可以如下来进行：在 Z_p^*，即与 p 互素的元素集合中，一共存在 $\varphi(p-1)$ 个生成元。因此首先选择任意一个元素 h，$\varphi(p-1)$ 与 $(p-1)$ 比较接近，则 h 是一个 $p-1$ 阶生成元的概率很大，找到一个之后，计算 $g=h^k$，则 g 就是一个 q 阶生成元），同时随机再选择另外 n 个 q 阶生成元 g'_2，g''_2，…，$g_2^{(n)}$。本文用 g'_2 代表第 1 种面额的电子现金，g''_2 代表第 2 种面额的电子现金，依次类推，银行用 $g_2^{(n)}$ 代表发行的是第 n 种面额的电子现金。另外银行再选择 2 个

* 收稿日期：2004-06-07
基金项目：国家自然科学基金资助项目（10271119）
作者简介：李进（1981 年生），男，博士研究生；E-mail：sysjinli@yahoo.com.cn

无碰撞的哈希函数 H, H_1。银行的私钥为 x, 公钥为 $y = g^x$; 银行同时公布 $y' = g'^x_2$, $y'' = [g''_2]^x$, …, $y^{(n)} = [g_2^{(n)}]^x$。

用户参数设置: 用户 U 首先在银行开户, 银行帐号 $I = g_1^{u_1}$, 其帐号所对应的私钥为 u_1。开户时用户必须使用签名或鉴别方法向银行认证自己知道相应的私钥 u_1。因此用户的公钥为 I, 而私钥为 u_1。

1.1　提取阶段　用户 U 首先向银行 B 证明他拥有帐号 I, 这一步可以使用 Schnorr 鉴别或者签名方案, 同时告诉银行需要提取多大面额的电子现金(每次可能会同时提取多个不同面额的电子现金, 为简洁计, 假设用户提取第 i 个面值的电子现金)。对于每个提取的电子现金和银行进行以下的交互协议:

步骤 1 (B→U): 银行首先选择 $\omega \in_R Z_q^*$, 同时由于用户要提取第 i 个面额的电子现金, 银行选择代表第 i 个面额的生成元 $g_2^{(i)}$, 同时计算 $a = g^\omega$, $b = (Ig_2^{(i)})^\omega$, $Z = (Ig_2^{(i)})^x$; 银行将 a, b, Z 发给用户;

步骤 2 (U→B): 用户产生 5 个随机数 $s \in Z_q^*$, x_1, x_2, u, $v \in_R Z_q$; 计算 $A = (I g_2^{(i)})^s$, $Z' = Z^s$; $B = g_1^{x_1} [g_2^{(i)}]^{x_2}$, $a' = a^u g^v$, $b' = b^{su} A^v$, $c' = H(A, B, Z', a', b')$; 然后计算 $c = c'/u$, 将 c 发送给银行;

步骤 3 (B→U): 银行计算 $r = \omega + cx \pmod q$ 并且将 r 发给用户;

步骤 4 (U): 验证 $g^r = ay^c$ 和 $(Ig_2^{(i)})^r = bZ^c \pmod p$; 若成立, 则表示银行的签名有效, 否则通知银行签名无效。

1.2　支付阶段　用户 U 计算 $r' = ru + v$, 得到电子硬币 $(A, B, Z', a', b', c', r')$, 其中 (Z', a', b', c', r') 可以看成银行对 (A, B) 的签名 $\mathrm{Sig}_B(A, B)$。用户将 $(A, B, Z', a', b', c', r')$ 以及这个电子现金的面额 i 发给商家, 假设商家的代号是 I_s, 交易时间为 T。用户同时使用失败—终止签名 (fail—stop signature) 进行一次性的签名: $\sigma_1 = x_1 - us\,H(I_s, T)$, $\sigma_2 = x_2 - s\,H(I_s, T)$。

商家验证 $\mathrm{Sig}_B(A, B)$ 为银行的签名, 并且用户的一次性签名成立, 即 $B = A^{H(I_s, T)} g_1^{\sigma_1} [g_2^{(i)}]^{\sigma_2}$, 若都通过, 则进行交易; 否则, 通知用户此次为无效交易。

1.3　存储阶段　商家可以自己选择一个适当的时候将收到的这些交易数据都转给银行, 银行和商家进行类似的验证, 同时银行检查数据库中是否有此电子现金的记录以防止双重花费, 银行然后在商家的帐号存入相应的数目。若此电子现金被双重花费, 银行利用和 Brands 相同的方法就可以计算出这个电子现金对应的帐号 I。

1.4　安全性分析　本文方案中使用了和 Brands 方案相同的限制性盲签名的方法, 即用户在提取第 i 种面值的电子现金时, 银行计算 $a = g^\omega$, $b = (Ig_2^{(i)})^\omega$ 发给用户, 然后使用 ω, x 对 c 签名, 由于限制性盲签名的特点, 用户只能得到形如 $(I g_2^{(i)})^s g^t$ 形式的签名。由于在支付时商家要对用户是否知道此电子现金基于 g_1, $g_2^{(i)}$ 的离散对数进行验证, 而银行选择的生成元之间的关系 $\log_g g_1$ 和 $\log_g g_2$ 用户是不知道的, 从而限制用户只能得到 $(Ig_2^{(i)})^s$ 形式的盲签名, 这种形式的电子现金被用户双重花费时就可以被追踪到相应的帐号 I。所以说我们的电子现金方案安全性和 Brands 的完全一样。

2　结　论

本文提出了一种基于 Brands 电子现金方案的多种面值的电子现金方案, 我们的方案相比以前的多种面值方案的设计要更有效和安全。在本文方案中, 银行如果要发行不同面值的电子现金只需要选择同一个私钥, 相比之前一个系统如果有 n 种面值的电子现金那么银行就要选择 n 个不同的私钥的设计, 显然整个系统的安全性更高, 而且在文中已经证明了新方案的安全性和 Brands 方案相同。

参考文献:

[1] CHAUM D. Blind signatures for untraceable payments[C]. Advances in Cryptology Crypto'82. Springer-Verlag, 1982: 99—203.

[2] CHAUM D, FIAT A, NAOR M. Untraceable electronic cash [C]. Advances in Cryptology Crypto'88. Springer-Verlag, 1988: 319—327.

[3] BRANDS S. An efficient off-line electronic cash system based on the representation problem[C]. Report CS—R9323, Workshop on information, 1993.

[4] ENG T, OKAMOTO T. Single-term divisible electronic coins [C]. Advances in Cryptology EUROCRYPT'94, Springer-Verlag, 1994: 311—323.

[5] FRANKEL Y, TSIOUNIS Y, YUNG M. Fair off-line e-cash made easy[C]. Proceedings of ASIACRYPT'98, Springer-Verlag, 1998: 257—270.

[6] GAUD M, TRAORE J. On the anonymity of fair off-line E-cash systems[C]. Proceedings of Financial Cryptography'03, Springer-Verlag, 2003: 34—50.

[7] ABE M, OKAMOTO T. Provably secure partially blind signatures[C]. Proceedings of Crypt'2000, Springer-Verlag, 2000: 271—286.

(下转第 118 页)

汉字（它们的时域特征均为浊音）开头或结尾，则平均过零率判别也无能为力。

参考文献：

[1] 李祖鹏, 佩阳. 一种语音段起止端点检测新方法[J]. 电讯技术, 2000(3): 68－71.
[2] 刘庆升, 徐霄鹏, 黄文浩. 一种语音端点检测方法的探究[J]. 计算机工程, 2003, 29(3): 27－31.
[3] 董小刚, 秦喜文. 信号消噪的小波处理方法及 Matlab 实现[J]. 长春工业大学学报, 2003, 24(2): 13－15.
[4] 胡昌明. 基于 Matlab 的系统分析与设计: 小波分析[M]. 西安: 西安电子科技大学出版社, 1999.
[5] 陈怀琛, 吴大正. 高西全, Matlab 及在电子信息课程中的应用[M], (第二版). 北京: 电子工业出版社, 2003.

A Wavelet-Based Algorithm for Detecting the Beginning and End Points of Voice Segments

DONG Li, CHEN Hong-qin, MA Zheng-ming
(Deptartment of Electronics and Communication Engineering, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: A wavelet-based algorithm for detecting the beginning and end points of voice segments was proposed. The common-used algorithms are mostly based on their energy differences in time domain and therefore only suitable for the high SNR situation. For the low SNR, the common-used algorithms have to be strengthened by making use of some additional features such as average across-zero rates. This improvement will increase the algorithm complexity and still be possible to fail in some cases such as those Chinese characters with sonant consonants. A new wavelet-based algorithm has been proposed for the situation with white noise environment. White noise environment can remain unchanged across various subbands of wavelet transform domain and therefore can be detected and removed from voice signal. The experimental results show that this new algorithm can efficiently distinguish the beginning and end points of voice segments even in the low SNR environments.

Key words: wavelet transform; voice signal process; white noise

---

（上接第 115 页）

An Improvement to Brands E-cash Scheme

LI Jin, LIN Qun, WANG Yan-ming
(School of Mathematics, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: It is suggested that the bank just directly use different private and public key pairs to issue different denominations cash in previous e-cash schemes. An efficient multi-denomination off-line e-cash scheme is presented, in which the bank only needs one private key other than n different private keys when issuing n kinds denominations e-cash. The new scheme is more efficient than previous multi-denomination schemes.

Key words: e-cash; multi-denomination; restrictive blind signature