一个可审计的离线电子现金方案*

李 进，王燕鸣
（中山大学数学与计算科学学院，广东 广州 510275）

摘 要：提出了一个高效率的可审计的离线电子现金方案，用户有权控制去除电子现金的匿名性，即使没有可信第三方的存在。相对于以前提出的可审计电子现金方案，方案的一个优点是银行在查询电子现金的花费者时，可以直接找到相应的用户帐号，而之前的方法都是从银行的整个提取现金的数据库去遍历搜索，导致效率很低。另一个贡献是构造了第一个多面值的可审计的离线电子现金方案。

关键词：电子现金；公平追踪；可审计性；多种面值
中图分类号：TP309 **文献标识码**：A **文章编号**：0529-6579（2005）05-0006-05

当前的电子支付系统可以分为如下4类：在线信用卡，电子支票，智能卡和电子现金。而前面3类支付方式都基本上没有考虑到保护用户的隐私，因为在这些系统中，银行很容易就可以知道谁什么时候在哪里支付了多少的金额等等很多的信息，而电子现金系统则很好地保护了用户的隐私。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（online）和离线支付（offline）。1982年，Chaum[1]提出了盲签名的概念并用它第一次构造了一个在线电子现金方案。然而因为在线电子现金方案需要银行在每次交易中都参与，因此效率非常低。1988年，Chaum和Fiat等[2]提出了第一个离线电子现金方案，然而他们需要用到公平分割协议，因此，虽然实现了离线功能，但是效率还是不高。1993年，Brands[3]克服了公平分割所带来的大量的计算，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，这种方案相对而言效率很高。

然而，尽管电子现金[2,3]可以很好地实现用户匿名性，但是完全匿名的电子现金在有些情况下是不可取的，文[4]指出完全匿名的电子现金系统不能解决金融犯罪如绑票洗钱等，基于这些问题，政府和银行提出了可取消匿名性的电子现金系统。从而如何构造在适当的时候可以取消匿名性成了电子现金设计的一个重点。公平性是指必要时银行可以实现电子现金追踪以及帐户追踪。

现金追踪：银行将提取时的数据交给可信第三方，可信方利用自己的私钥追踪到此电子现金。

帐户追踪：银行将某一次存储时的交易信息给可信方，由可信方追踪到此电子现金所对应的帐号。

Stadler等[5]提出了一个新的概念称为公平盲签名，利用这种新签名方案他们构造了一个公平的电子现金方案，然而，这个电子现金方案中的可信第三方是在线的，从而影响到银行的效率。随后出现一些更有效的公平电子现金方案[6-9]，在他们方案中，可信第三方是离线的。虽然公平电子现金系统可以提供追踪，但是很多时候可信第三方会有可能滥用自己的权利给用户隐私带来危险。在金融密码学会议FC'00上，Pfitzmann等[10]提出了一个新的自我托管密钥防止黑邮的方案，这个方案的实现只是在原来的公平电子现金方案的基础上将可信第三方的公钥换成用户自己的公钥来实现的。随后在金融密码学会议FC'02上，可审计的离线电子现金方案第一次被文[11]提出：在这样的方案中，用户可以审查自己花费的电子现金是否被追踪。银行或者可信第三方如果进行了非法的追踪，那么用户可以得到证据并且对他们提出控诉。对于现金追踪和帐户追踪都可以利用它来实现，方案[11]的缺点是当需要银行进行合法追踪时，它必须对整个提取的电子现金数据库进行遍历搜寻，从而降低系统的效率。

* 收稿日期：2004-11-01
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

本文提出了一个可审计的离线电子现金方案，使银行可以直接从花费的电子现金中找到相应的帐户，而不需要进行整个数据库的遍历。对于银行，在发放电子现金时肯定是需要发行多种面值的电子现金，本文的另外一个贡献是第一次提出了一个可审计的离线多面值电子现金方案，相比以前的直接使用多个私钥和公钥来完成这个工作，效率要高很多。本文最后一个工作是将一个优秀的离线电子现金方案[6]改变得到一个相应的可审计的离线电子现金方案。

1　基本工具和困难假设

给定如下的参数 q，p，$p-1=kq$；g 是 Z_p^* 上的 q 阶群 G_q 的生成元，考虑群在群 G_q 中如下的困难问题：

(1) 离散对数问题 (DLP)：给定群 G_q 中的任意两个元素 g，h 计算 $x\in Z_q$ 使得 $h=g^x$ 成立；

(2) 计算离散对数问题 (CDHP)：对于任意 x，$y\in Z_q$，给定 g^x，g^y，计算 g^{xy}；

(3) 决策离散对数问题 (DDHP)：对于任意 x，y，$z\in Z_q$，给定 g^x，g^y，g^z 判别 $z\equiv xy \bmod q$ 是否成立；

(4) 计算代表元困难问题 (RP)：给定群 G_q 中的 $k+1$ 个生成元 g_1，…，g_k 以及 h，计算出一个 k 元组 $(x_1,\cdots,x_k)$ 使得 $h=\prod_{i=1}^{k} g_i^{x_i}$ 成立。

在文章随后的方案中经常会用到如下的知识证明：两个离散对数相等的知识证明和代表性问题的知识证明。现在如下定义：

定义 1　[对数相等知识证明]：对于要证明群 G_q 中元素 h 关于 g 的指数和 h' 关于 g' 的指数相等，用如下的记号表示：$SPK\{\alpha: h=g^\alpha \wedge h'=g'^\alpha\}$。

简单的证明过程如下：首先证明者选择 $k\in Z_q$ 然后计算 $r_1=g^k$ 和 $r_2=g'^k$，接着计算 $s=k-cx \bmod q$，其中 $c=H(M,g,h,g',h',r_1,r_2)$。验证者只需要计算 $c=H(M,g,h,g',h',g^s h^c, g'^s h'^c)$ 是否成立即可。

定义 2　[代表元和对数相等知识证明]：对于要证明群 G_q 中元素 h 关于 g 和 g_1 的指数以及证明关于 g 上的指数和 h' 关于 g' 的指数相等，用如下记号表示：$SPK\{(\alpha,\beta): h=g^\alpha g_1^\beta \wedge h'=g'^\alpha\}$。

简单的证明过程如下：首先证明者选择 k，$k_1\in Z_q$，然后计算 $r_1=g^k g_1^{k_1}$ 和 $r_2=g'^k$，接着计算 $s_1=k-cx \bmod q$ 和 $s_2=k_1-cx \bmod q$，其中，$c=H(M,g,h,g',h',r_1,r_2)$。验证者只需要计算 $c=H(M,g,h,g',h',g^{s_1}g_1^{s_2}h^c, g'^{s_1}h'^c)$ 是否成立即可。

2　可审计的离线电子现金方案

2.1　系统初始化

银行：(假设银行需要发行 n 种面额的电子现金) 选定如下的参数：大素数 q，p，$p-1=kq$；g 是 Z_p^* 上的 q 阶群 G_q 的生成元。银行选择 $x\in Z_q$ 作为它的私钥，同时选择群 G_q 的生成元 g_1，g_2 (当然这两个值的离散对数值是未知的)。随后银行选择 n 个群 G_q 的生成元 g'_4，…，$g_4^{(n)}$。整个系统的公钥是 $h=g^x$，$h_1=g_1^x$，$h_2=g_2^x$，$h'_4=g_4'^x$，…，$h_4^{(n)}=g_4^{(n)x}$，(g'_4, h'_4) 表示第一种面额电子现金，(g''_4, h''_4) 表示第二种面额的电子现金，依次类推。银行还定义一个哈希函数 H：$\{0,1\}^* \to Z_q$。在新系统中，银行发放 n 个面额的电子现金时，只需要保存一个私钥，实现这一功能的原因是银行公开 n 个公开值 $\{g'_4,\cdots,g_4^{(n)}\}$ 作为相应面额的代表元。

用户：用户最开始的时候注册一个公钥 $I=g_1^u$ (也就是他的帐号)，同时他选择一个私钥 $x_c\in Z_q$ 并且计算 $g_c=g_2^{x_c}$ 作为他的另外一个公钥。为了实现现金追踪，银行给用户一个追踪公钥 y_c，分为 2 种情况：第一种是如果用户被追踪，这时银行这样计算 y_c，首先选择 $x_c\in Z_q$ 然后计算 $y_c=g_2^{x_c}$ 作为用户的证书；第二种情况是用户没有被追踪，这时的 $y_c=g_c^{x_c}$。

商家：在开始交易之前，商家选择 g_M 作为它的一个公钥，银行为商家另外注册一个公钥：首先银行选择 x_M，计算公钥为 $y_M=g_2^{x_M}$，如果商家被追踪；否则银行计算 $y_M=g_M^{x_M}$；

2.2　提取阶段

在用户 U 和银行 B 开始协议之前，用户首先向银行认证使银行确信自己就是用户 U (也就是说确信他有相应的帐号，这一步可以利用 Schnorr 鉴别或者签名方案)。假设用户想提取第 i 个面值的电子现金 (当然很容易地就可以拓展到同时提取多个面值的现金)。

(用户 U)：用户 U 首先选择一个秘密值 $s\in Z_q$ 然后计算 $h_p=Ig_4^{(i)}g_2^s$ 以及 $z_p=[Ig_4^{(i)}g_2^s]^x$，计算 $d=y_c^s$。用户要得到银行对这些信息的盲签名，U 盲化 (h_p, z_p) 为 $(h_\omega=h_p^{s^{-1}}, z_\omega=z_p^{s^{-1}})$ 并且进行如下的知识证明：$SPK\{\alpha: h_\omega/g_2=[Ig_4^{(i)}g_2^s]^\alpha \wedge y_c^c=d^\alpha\}$；

（银行 B）：银行选择一个秘密值 $r' \in Z_q$ 然后计算并发送 $t'_g = g^{r'}$ 和 $t'_h = h_\omega^{r'}$ 给用户 U；

（用户 U）：收到银行发送过来的值以后，用户随机选择 x_1，x_2，β，γ，$\in Z_q$ 并且计算 $a = g_1^{x_1} g_2^{x_2}$（这个值的目的是用来防止双重花费）然后盲化 t'_g，t'_h 为：$t_g = t'_g g^{\beta} h^{\gamma}$ 以及 $t_h = t'_h h_p^{\beta} z_p^{\gamma}$。最后，计算并且发送 $c' = c - \gamma \bmod q$ 给银行，其中 $c = H(g_4^{(i)}, a, h_p, z_p, t_g, t_h)$；

（银行 B）：接收到 c' 后计算 $\sigma' = r' - c'x \bmod q$ 发送给用户；

（用户 U）：收到 σ' 后验证 $t'_g = g^{\sigma'} y^{c'}$ 以及 $t'_h = h_\omega^{\sigma'} z_\omega^{c'}$ 是否成立，如果成立，则计算 $\sigma = \sigma' + \beta \bmod q$，则用户拥有的电子现金为（$c$，$\sigma$，$a$，$g_4^{(i)}$，$h_p$，$z_q$，$t_g$，$t_h$）。

2.3 支付阶段

假设用户购买商家 I_s 的物品并且知道商家的公钥是 y_M，不妨假设交易的时间为 T。

用户首先将电子现金（c，σ，a，$g_4^{(i)}$，h_p，z_q，t_g，t_h）发送给商家，商家验证如下的几个等式是否成立：$c = H(g_4^{(i)}, a, h_p, z_q, t_g, t_h)$，$t'_g = g^{\sigma} y^{c'}$ 以及 $t'_h = h_\omega^{\sigma} z_\omega^{c'}$，如果上述 3 个验证等式都成立，商家则要求用户证明此电子现金确实属于用户 U 的，即要求用户进行知识证明：用户首先计算 $d' = y_M^s$ 和 $\alpha' = y_M^{x_s}$，用这 2 个值进行如下证明 $SPK\{(\alpha, \beta): h_p / g_4^{(i)} = g_1^{\alpha} g_2^{\beta} \wedge d' = y_M^{\beta}\}$，其实也就是计算 $\sigma_1 = x_1 - H(I_s, T)u$ 和 $\sigma_2 = x_2 - H(I_s, T)s$。

商家验证如下的 2 个等式是否成立：$\alpha = h_p^{H(I_s, T)} g_1^{\sigma_1} g_2^{\sigma_2}$ 以及 $\alpha' = y_M^{\sigma_2} d'^{H(I_s, T)}$。如果成立，则进行交易；否则取消本次交易并通知用户。

2.4 存储阶段

商家收到电子现金之后，因为方案是离线的，所以可以隔一段时间存储电子现金，他只需要将支付阶段的交互数据给银行，银行进行和商家一样的验证，如果通过，则将相应的金额存入商家的帐户。

2.5 追踪阶段

如果在以上的过程中用户或者银行哪一方需要对电子现金进行追踪，则分为以下几种情况分别进行不同的运算：

（1）双重花费者身份追踪：如果一个用户对某一个电子现金进行了双重花费，那么他要么在不同的商家 I_s 和 I'_s 处进行了不同花费，要么在同一个商家 I_s 在不同时间做了 2 次花费，那么他肯定要计算如下 2 个不同的值：$\sigma_1 = x_1 - H(I_s, T)u$ 和 $\sigma'_1 = x_1 - H(I'_s, T')u$，只要 I_s 和 I'_s 或者 T 和 T' 有一个不同，那么相应哈希值将几乎不同。从而银行或者任何人都可以计算 $u = (\sigma'_1 - \sigma_1)/(c - c') \bmod q$ 并找到相应的帐号 $I = g_1^u$；

（2）电子现金追踪：如果在初始化时用户已经被银行追踪了，那么银行就知道 $x_c = \log_{g_2} y_c$，因此从提取数据银行可以计算 $h_p = I g_4^{(i)} d^{x_c^{-1}}$，从而追踪到相应的电子现金；

（3）帐户追踪：如果在初始化时商家被银行追踪了，那么银行就知道了 $x_M = \log_{g_2} y_M$，因此可以通过交易数据计算出 $I = h_p / d'^{x_M^{-1}} g_4^{(i)}$，即追踪到相应的身份；

（4）匿名性消除：在这个新方案中，用户有权控制和去除将来使用电子现金的匿名性，即如果在初始化用户选择了 x_s 并且计算了 $g_c = g_2^{x_s}$。一旦发生黑邮事件，用户需要从提取的电子数据中追踪到相应花费的电子现金时可以如下运算：从提取数据 $d = y_c^s$ 中，用户可以计算 $d^{x_s^{-1}}$ 并交给银行，如果在初始化中银行没有追踪用户，那么此时银行计算 $h_p = I g_4^{(i)} d^{x_c^{-1} x_s^{-1}}$ 就是相应的电子现金；如果在初始化时银行已经追踪了用户，那么银行只需要计算 $h_p = I g_4^{(i)} d^{x_c^{-1}}$；

（5）审计：如果设置了某一天为审计日，那么这一天银行就需要向用户证明自己是否已经追踪过用户或者商家。如果用户没有被追踪，银行就向用户证明他知道一个私钥 x_c 使得 $x_c = \log_{g_c} y_c$，其中 y_c 是用户在初始化时银行给的一个公钥；否则就表明用户被银行追踪。对于商家，如果银行要向商家证明没有追踪商家，只需要证明银行知道 $x_M = \log_{g_M} y_M$；否则就表明商家被银行追踪。

2.6 安全性分析

在新方案中，仍然使用限制性盲签名方案，到目前为止，限制性盲签名方案还没有受到什么攻击，因此比较安全。在这个协议中，用户得到银行的一个限制性盲签名，从限制性盲签名角度看，用户只能拥有 $h_\omega^{s'} g^{t'}$ 形式的签名（这也就是为何称这种盲签名为限制性盲签名的原因）。同时，由于商家最后验证用户知道 h/g 关于 g_1，g_2 的离散对数问题，从而可以确保用户选择 $s' = s$，这也保证了后面的双重花费和电子现金追踪以及用户追踪的正确性。

另一方面，用户不能更改电子现金的面额，这是因为用户不知道 $g_4^{(i)}$ 和 $g_4^{(j)}$ 之间的离散对数值，

而电子现金中有 $h_p = g_4^{(i)} g_2^s$ 以及 $z_p = [Ig_4^{(i)} g_2^s]^x$，由于用户不知道 $g_4^{(i)}$，$g_4^{(j)}$ 之间的离散对数值，从而用户也就不可能将 h_p，z_p 改变成为面值 j。

3　另一个可审计的电子现金方案

1998 年，Solages 等[6]提出了一个高效的公平离线电子现金方案。本节将它转换成一个可审计的同时保持离线的公平电子现金方案。

3.1　系统初始化

(1) 银行：仍然假设银行需要发行 n 种面额的电子现金，选定如下的参数：大素数 q，p，$p-1=kq$；g 是 Z_p^* 上的 q 阶群 G_q 的生成元。银行选择 $x\in Z_q$ 作为它的私钥，同时选择群 G_q 的生成元 g_1，g_2，随后银行选择 n 个群 G_q 的生成元 g'_4，…，$g_4^{(n)}$。整个系统的公钥是 $h=g^x$，$h_1=g_1^x$，$h_2=g_2^x$，$h_4=g_4^{'x}$，…，$h_4^{(n)}=g_4^{(n)x}$，(g'_4, h'_4) 表示第一种面额电子现金，(g''_4, g''_4) 表示第二种面额的电子现金，依次类推。银行还定义一个哈希函数 H：$\{0,1\}^* \to Z_q$。

(2) 用户：注册一个公钥 $I=g_1^u$ 作为他的帐号，同时他选择一个私钥 $x_s\in Z_q$ 计算 $g_c=g_2^{x_s}$ 作为他的另外一个公钥。银行给用户一个追踪公钥 y_c 决定用户是否被追踪，方式和前面方案相同，在此省略。

(3) 商家：商家选择 g_M 作为它的一个公钥，银行给商家另外一个公钥 y_M 决定其是否被追踪，方式也是和上面方案相同；

3.2　提取阶段

用户首先选择 2 个秘密值 s，$t\in Z_q^*$ 计算 $E_1=g_2^s y_c^t$ 和 $E_2=g_2^t$，然后进行如下的知识证明 $SPK\{(\alpha,\beta): E_1=g_2^\beta y_c^\alpha \wedge E_2=g_2^\alpha\}$。同时用户也计算 $D=g_1^a g_2^b$，$h_p=Ig_2^s g_4^{(i)}$，其中 a，b 是用户自己选择的秘密值。

接着银行计算 $t'_g=y_c^\omega$ 和 $t'_h=(IE_1 g_4^{(i)})^\omega$ 以及 $z'_p=(IE_1 g_4^{(i)})^x$ 和 $P=y_c^x$ 发送给用户；收到银行发送过来的值以后，用户随机选择 x_1，x_2，β，$\gamma\in Z_q$ 并且计算 $a=g_1^{x_1} g_2^{x_2}$ 并且盲化 t'_g，t'_h 为：$t_g=t'_g y_c^\beta P^{c'}$ 以及 $t'_h=(t'_h/t'^{t}_g)\, h_p^\beta z_p^\gamma$。最后，计算并且发送 $c'=c-\gamma \bmod q$ 给银行，其中 $c=H(g_4^{(i)}, a, h_p, z_p, t_g, t_h)$；银行 B 接收到 c' 后计算 $\sigma'=\omega-c'x \bmod q$ 发送给用户；用户 U 收到 σ' 后验证 $t'_g=y_c^{\sigma'} P^{c'}$ 以及 $t'_h=(IE_1 g_4^{(i)})^{\sigma'} z_p^{c'}$ 是否成立，如果成立，则计算 $\sigma=\sigma'+\beta \bmod q$，则用户拥有的电子现金为 $(c, \sigma, a, g_4^{(i)}, h_p, z_p, t_g, t_h)$。

后面的支付过程和存储以及追踪协议和前面的方案都是相同的，在此不再详细描述。对于这个方案的安全性分析，由于也是使用了限制性盲签名方法，从而对于电子现金的签名形式和前面的方案也是同样的讨论，可以证明是一个安全的可审计的离线电子现金方案。

4　结论

如何更有效地设计一个公平追踪的电子现金方案一直都是电子现金研究的一个重点，而对于可审计的电子现金方案研究的还不多。本文提出了一个效率很高的方案，相对于以前提出的可审计的电子现金方案，新方案的一个优点是银行在追踪电子现金的帐户时可以直接找到，而不需要对整个的提取现金的电子数据库进行遍历。新方案的另一个贡献是提出了第一个银行只需要一个私钥就可以实现多面额电子现金发放，最后文章对一个一般的公平电子现金方案转换为一个可审计的方案。

参考文献：

[1] CHAUM D. Blind signatures for untraceable payments[C]. Advances in Cryptology Crypto'82. New York: Springer-Verlag, 1982: 199 - 203.

[2] CHAUM D, FIAT A, NAOR M, Untraceable electronic cash [C]. Advances in Cryptology Crypto'88. New York: 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] SOLMS S von, NACCACHE D. On blind signatures and perfect crimes[J]. Computer and Security, 1992, 11: 581 - 583.

[5] STADLER M, PIVETEAU J M, CAMENISCH J. Fair Blind Signatures[C]. Advances in Cryptology-EUROCRYPT'95. New York: Springer-Verlag, 1996: 209 - 219.

[6] SOLAGES A de, TRAORE J. An Efficient Fair Offline Electronic Cash System with extensions to Checks and Wallets with Observers[C]. In Financial Cryptography - FC'98. New York: Springer-Verlag, 1988: 275 - 295.

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

[8] ABE M, OKAMOTO T. Provably Secure Partially Blind Signatures [C]. Proceedings of Crypt'2000. New York: Springer-Verlag, 2000: 271 - 286.

[9] GAUD M, TRAORE J. On the Anonymity of Fair Off-line E-cash Systems[C]. Proceedings of Financial Cryptography'03. New York: Springer-Verlag, 2003 : 34 - 50.

[10] PFITZIMANN B, SADEGHI A R. Self-escrowed cash against user blackmailing [C]. Proceedings of Financial Cryptography'00. New York: Springer-Verlag, 2001: 42 - 52.

[11] KUGLER D, VOGT H. Offline payments with Auditable Tracing[C]. In Financial Cryptography - FC2002. New York: Springer-Verlag, 2003: 269 - 281.

（下转第 13 页）

estimates for Schrödinger equations[J]. J Func Anal, 2004, 208:122 - 139.

[8] YAJIMA K. A multichannel scattering theory for some time-dependent Hamiltonians, charge transfer problem[J]. Comm Math Phys, 1980, 75:153 - 178.

[9] IORIO R J, MARCHESIN D. On the Schrödinger equation with time-dependent electric fields[J]. Proc R Soc Edinb, 1984, 96A:117 - 134.

Solutions for Higher-order Schrödinger Equation with Potentials

GUO Cui-hua, CUI Shang-bin

(Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: The existence, uniqueness and the regularity for the solutions of the initial value problem for the higher-order Schrödinger equation with the time dependent potentials are discussed. The sufficient conditions on potential function are given so that this equation has classical solutions. Under the first assumption, the local solution is obtained by using fixed point theorem; the global solution is obtained by using the energy conservation laws. Under the second assumption, the solution is obtained by making moliphier functions.

Key words: Schrödinger equation; initial value problem; potential function

(上接第 9 页)

An Auditable Offline E-cash Scheme

LI Jin, WANG Yan-ming

(School of Mathematics and Computational Science, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Fair tracing is one of the most important aspects in electronic cash (e-cash). An efficient auditable offline e-cash scheme is proposed in which customers have power to control the deanonymization without the third party. The advantage of this scheme is that the bank can directly find the owner when owner tracing is necessary. Another contribution is that an efficient multi-denominations auditable offline e-cash scheme is first presented, in which the bank only needs one private key to issue different denominations.

Key words: e-cash; fair tracing; auditability; multi-denomination