部分受限盲签名及在电子现金中的应用*)

彭 冰 杨宗凯 谭运猛

(华中科技大学电子与信息工程系 武汉430074)

摘 要 本文提出了一种有效的部分受限盲签名方案。该方案具有通信量少、计算量小等优点。分析了其安全性和有效性后,介绍了该方案在离线电子现金支付系统中的应用。

关键词 部分受限盲签名,表述问题,电子现金

Partially Restrictive Blind Signature and its Application to E-cash

PENG Bing YANG Zhong-Kai TAN Yun-Meng

(Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074)

Abstract In this paper, an efficient partially restrictive blind signature scheme is introduced. In our scheme, the siger can explicitly embed and control part of information to be signed, while the other part of information are blind transformed by user in a restrictive ways. After analyzing its security and efficiency, the application of our new scheme on off-line electronic cash (E-cash) payment system is presented. In the E-cash system, only a single key pair to issue E-cash is needed. At the same time, the storage size of payment transcript database is controllable.

Keywords Partially restrictive blind signature, Representation problem, Electronic cash, Double spend

1 引言

数字签名是信息社会中实现对原始信息进行鉴别和不可抵赖性确认的重要技术。一般的数字签名方案中,由于原始信息对签名者而言是可见的,它不适用于信息拥有者的匿名性需求。这类涉及到信息拥有者隐私的应用包括电子现金、电子投票选举、电子拍卖等。为了让签名者在不知道信息内容的情况下予以签名,或者说签名者签名时获得的信息与原始信息之间具有不可链接性,Chaum 提出了盲签名[1]的概念。盲签名的严格定义由 Juels 在文[2]中正式给出。早期的盲签名在应用到电子现金时往往采用低效的分割-选择的方法。后来,Brands 提出了受限盲签名的思想[3],并以此构造了一种高效的单条信息电子现金系统[4]。受限盲签名的实质是对签名申请者的原始信息的结构予以限制,无论申请者如何盲变换,原始信息和盲化后的信息是同构的。具体到电子现金中就是申请者必须将自己的身份信息嵌入原始信息中才能获得正确的签名。

不论是盲签名还是受限盲签名,其原始信息均由申请者交给签名者签名,然后申请者将收到的签名及全部原始信息盲变换得到签名者的盲签名。这样,签名者对盲化后的原始信息是无法控制的。在某些应用场合要求签名者能够控制部分盲化后的原始信息,例如在电子现金中,发行银行需要在每笔电子现金中嵌入相应的面额信息等;在电子投票中,发票机构需要嵌入每张选票的合法 ID 号等。以电子现金为例,目前提出的电子现金方案,不同面额的签名及验证是由银行不同的公私钥对来实现的,这不仅要求用户和商家保存大量的银行公钥,且对银行自身的密钥管理是一大挑战。针对这些情况,Abe M. 提出了部分盲签名的概念[5],在部分盲签名中,原始信息的一部分由申请者控制,另一部分信息则由签名者控制。此外,Maitland 进一步将部分盲签名与 Brands 的受限盲签名结合起来,给出了一个安全性可证明的部分受限盲签名协议[6],该协议是受限盲签名的扩展。

在离线电子现金支付系统中,一般用户端采用智能卡的形式,相对于银行和商家的服务器而言,其计算能力和存储空间都非常有限,有可能形成处理瓶颈。本文改进了 Maitland 的部分受限盲签名方案,通过简化盲变换的形式以减少签名申请者的计算量和存储量,并给出我们的高效部分受限盲签名在离线电子现金系统中的具体应用。

2 基本定义

为便于表述,以下给出本文涉及的有关符号:

p,q	充分大的素数,且 $q\|(p-1)$;
Z_q	小于 q 的非负整数集合;
G_q	乘法群 Z_p^* 的阶为 q 的循环子群;
$\|\|$	二进制位串级联;
$\in_R$	从某一集合中随机选择;
g,g_1,g_2	群 G_q 的生成元;
H,H_0	强碰撞自由的哈希函数,分别将任意长的二进制串映射为固定长度的串和 G_q 中的某一生成元;
$a \stackrel{?}{=} b$	验证 a 与 b 是否(模)相等。

如不另作说明,本文对群 G_q 中的运算省略模运算符 $(\bmod p)$。

定义1[5] 部分盲签名方案是如下所述的一个四元组(Gen,Signer,User,Ver):Gen 是概率型算法,Signer 和 User 分别为签名者和(签名)申请者,Ver 为确定型验证算法。Gen 的输入为系统参数,输出是签名者 Signer 的公私钥对(y,x);

*)基金项目:国家自然科学基金项目(90104033)。彭 冰 博士,主要研究领域为现代密码理论、网络信息安全、安全电子支付。杨宗凯 教授,博士生导师,主要研究领域为现代信息网络理论及应用、远程教育、信息安全。谭运猛 副教授,硕士生导师,主要研究领域为网络攻防技术、数字水印、隐藏信息检测。

Signer 的输入为公共信息 m_P 和私钥 x，输出为签名协议执行成功或失败；User 的输入为公共信息 m_P、隐私信息 m_S 和签名者的公钥 y，输出为签名者的签名 $\mathrm{Sign}_x(m_P,m_S)$；Ver 的输入为$(y,m_P,m_S,\mathrm{Sign}_x(m_P,m_S))$，输出为 True 或 False。

定义2[3]（表示问题(RP)） 给定有限循环群 G_q，一组生成元 $g_1,\cdots,g_k\in_R G_q$ 和元素 $m\in_R G_q$，在多项式时间内找到一个 k 元组$(a_1,\cdots,a_k)$（若 $m=1$，则要求$(a_1,\cdots,a_k)$不全为0）满足 $m=\prod_{i=1}^{k}g_i^{a_i}$。

表示问题实质上是离散对数问题(DLP)的推广。如果$(g_1,\cdots,g_k)$中各生成元是随机选择的，则在相同的有限群 G_q 中找到同一元素的两个不同表示与计算离散对数问题是一样困难的。

定义3[3] 设 $m\in_R G_q$，$(g_1,\cdots,g_k)$是 G_q 的一组生成元，盲签名协议开始时签名申请者知道 m' 对于$(g_1,\cdots,g_k)$的表示为$(a'_1,\cdots,a'_k)$，签名协议结束后 m' 被盲变换为 m，签名申请者知道 m 对于$(g_1,\cdots,g_k)$的表示为$(a_1,\cdots,a_k)$。如果对任意的消息 m' 和签名申请者的任意盲变换操作，存在函数 I' 和 I，使得 $I'(a'_1,\cdots,a'_k)=I(a_1,\cdots,a_k)$，那么盲签名协议称为受限盲签名协议；$I'$ 和 I 称为盲变换固定函数。

3 部分受限盲签名

在我们提出的高效部分受限盲签名协议中，原始消息由两部分构成：信息 m'_S 由签名申请者提供；信息 m_P 为申请者和签名者均知道的公共消息。签名者对 m'_S 和 m_P 用私钥 x 签名，申请者将签名 $\mathrm{Sign}_x(m_P,m'_S)$去盲处理后得到消息 m_P 和 m_S 的可用签名者公钥 y 验证的合法签名 $\mathrm{Sign}_x(m_P,m_S)$。这里，签名者并不知道 m'_S 的盲形式 m_S，他不能将消息 m_S 和申请者以后出示的签名 $\mathrm{Sign}_x(m_P,m_S)$联系起来。同时，签名者能够控制消息 m_P，或者说签名者能够确信只有包含 m_P 的消息的签名才是合法的签名。具体协议执行过程如下：

(1) 申请者计算 $y_2=H_0(m_P)$，将消息 m'_S 发给签名者；

(2) 签名者也计算 $y_2=H_0(m_P)$，随机选择 $\omega,c'_2\in_R Z_q$，计算并发送 $z'=(m'_S)^x,a'_1=g^{\omega},a'_2=y_2^{c'_2},b'=(m'_S)^{\omega}$ 给申请者；

(3) 申请者随机选择 $t,u_1,u_2,v\in_R Z_q$，对消息 m'_S 进行盲变换得 $m_S=(m'_S)^t$，同时分别将 z',a'_1,a'_2,b' 盲化为：$z=(z')^t$，$a_1=a'_1g^{u}y^{u_1},a_2=a'_2y_2^{v_2},b=[b'(m'_S)^{v}(z')^{u_1}]^t$，再计算 $c=H(y_2\|m_S\|z\|a_1\|a_2\|b)$并传送 $c'=c-u_1-u_2(\bmod q)$给签名者；

(4) 签名者计算 $r'=\omega-(c'-c'_2)x(\bmod q)$，然后传送 r'，c'_2给申请者；

(5) 申请者计算 $c'_1=c'-c'_2(\bmod q)$并检查：$a'_1\stackrel{?}{=}g^{r'}y^{c'_1},a'_2\stackrel{?}{=}y_2^{c'_2},b'\stackrel{?}{=}(m'_S)^{r'}(z')^{c'_1}$，如验证正确，则计算 c'_1,c'_2,r' 的盲形式：$c_1=c'_1+u_1(\bmod q),c_2=c'_2+u_2(\bmod q),r=r'+v(\bmod q)$从而得到签名 $\mathrm{Sign}_x(m_P,m_S)=(z,c_1,c_2,r)$。

验证消息 m_P,m_S 的签名(z,c_1,c_2,r)是否合法只须检查：

$$c_1+c_2\stackrel{?}{=}H(H_0(m_P)\|m_S\|z\|g^ry^{c_1}\|[H_0(m_P)]^{c_2}\|m_S^rz^{c_1})\bmod q$$

容易证明如果申请者与签名者成功地执行上述部分受限盲签名协议，由于：

$$c=c'+u_1+u_2=c'_1+c'_2+u_1+u_2=c_1+c_2(\bmod q)$$

$$g^{r'}y^{c'_1}=g^{r'+v}y^{c'_1+u_1}=g^{r'}y^{c'_1}g^{v}y^{u_1}=a'_1g^{v}y^{u_1}=a_1$$

$$[H_0(m_P)]^{c'_2}=[H_0(m_P)]^{c'_2+u_2}=y_2^{c'_2}y_2^{u_2}=a'_2y_2^{u_2}=a_2$$

$$m_S^rz^{c_1}=(m'_S)^{t(r'+v)}(z')^{t(c'_1+u_1)}=[(m'_S)^{r'}(z')^{c'_1}(m'_S)^{v}(z')^{u_1}]^t$$
$$=[b'(m'_S)^{v}(z')^{u_1}]^t=b$$

则申请者一定能获得合法的可用签名者公钥 y 验证的签名。

与 Maitland 的部分受限盲签名协议比较，本文的改进在于：a'_2,a_2,m_S,z 的计算均减少了一次模指数运算，且申请者的盲变换由 $a_1=(a'_1)^{u_1}g^{v_1},a_2=(a'_2)^{u_1}g^{v_1},b=a_1^{\beta_1}(b')^{\alpha_1}(m'_S)^{v_1}$转变为 $a_1=a'_1g^{v}y^{u_1},a_2=a'_2y_2^{v_2},b=[b'(m'_S)^{v}(z')^{u_1}]^t$；此外签名长度减少了一个变量。由于我们对 m'_S,z' 的盲变换是 Brands 受限盲签名的特例，它也满足文[3]的定理12，即申请者只有这样盲变换才能得到合法签名。在相同的 p,q 取值和随机选择生成元的条件下，离散对数问题(DLP)与表示问题(RP)的困难程度是相同的，又存在唯一的盲因子：$u_1=c_1-c'_1(\bmod q)$，$u_2=c_2-c'_2(\bmod q)$，$v=r-r'(\bmod q)$，$t=\log_{m'_S}m_S$ 将签名者在协议中获得的信息$(m_P,m'_S,z',a'_1,a'_2,b',c',c'_2,r')$映射到签在$(m_P,m_S,z,c_1,c_2,r)$，仿照文[6]的证明方法同样可以证明我们提出的协议具有部分盲的特性。

同时注意到，在签名者将 z',a'_1,a'_2,b' 传送给申请者后，将在线等待申请者一系列盲变换操作，直到收到挑战 c' 才继续执行协议。本文提出的部分受限盲签名协议无论总的计算量还是在线计算量均少于 Maitland 的方案，且协议执行过程中的通信量也有所减少，二者之间的对比详见表1（取 p,q 分别为512和160 bits）。

表1 部分受限盲签名计算量与通信量对比

	总计算量(次)		在线计算量(次)		通信量
	模幂	模乘	模幂	模乘	(Bytes)
文[6]	22	20	11	9	356
本文	17	8	8	5	316

4 离线电子现金系统

我们以离线电子现金为例，阐述部分受限盲签名的应用。目前广泛使用的电子支付系统大多为在 Internet 上基于信用卡的支付系统，其安全性主要建立在一系列复杂的安全协议基础上，如 SSL 和 SET 协议等。这类支付系统存在的问题主要是：

(1) 交易涉及复杂的签名与加/解密技术，用户支付时其信用卡号及口令要保密地由商家传送到发卡银行，要从公网经支付网关跨跃到金融内部网络；

(2) 银行在线验证每个用户信用卡号和口令的合法性，在大量用户支付的情况下，银行端易形成交易瓶颈；

(3) 用户支付的稳私性得不到保证，银行根据信用卡号知道每个用户的每一笔交易情况。

在日常生活中，用户交易的金额一般都不大（例如小于500元），为提高这种小额交易的系统效率，Chaum，Fiat 和 Naor 首先提出了离线不可追踪的电子现金支付系统[7]。然而由于采用了低效的分割选择技术，他们的系统运行效率极低。随后 Brands，Ferguson，Franklin 和 Yung 等学者提出了单一符号的电子现金协议[8~10]，大大提高了支付系统的效率，为电子现金实用化奠定了基础。

离线电子现金系统主要涉及用户、银行、商家三方（在有的系统中可能还有可信方）。用户和商家在发行电子现金的银行开设有帐户，用户与银行执行取款协议可以提取若干面额不等的电子现金存储到本地计算机或智能卡中；用户与商家执行支付协议，用电子现金购买商家提供的商品或服务。支付时不需要银行在线验证每笔交易，商家则保存接受的电子现金然后经过一定的时间间隔（如1周，或营业额达1万元）与银行执行存款协议，以便将电子现金所代表的价值转移到它的帐户上。

目前提出的各种电子现金方案[11~13]描述的都是单一面额的电子现金，其不同现金面额是由银行不同的私钥盲签名

来实现。此外，用户的电子现金没有流通期限的限制。这些方案均存在下述不足之处：

(1) 用户需要保存众多对应于不同面额的银行公钥，用户端的存储需求较大；

(2) 银行本身要对众多签名公、私钥对进行管理与更新，密钥管理复杂；

(3) 电子现金支付后，它要与商家的付款请求信息一起永远保存在银行付款说明数据库中以便在存款协议中对电子现金支付的唯一性进行核查，从而银行付款说明数据库的规模日益庞大。

上述缺陷的根源在于银行发行电子现金时不能控制电子现金的面额和有效期等信息。我们提出的新型部分受限盲签名可以高效地实现银行在执行取款协议时将这些公用信息嵌入到合法电子现金中。

为叙述简洁，以下协议描述忽略开始的双向身份认证(在支付协议，由于用户是匿名消费，因此只需用户验证商家的身份)。

4.1 系统初始化与注册

银行随机选择512 bits 大素数 p 和160 bits 大素数 q 并确保 $k=(p-1)/q$ 为素数，随机选择 $g,g_1,g_2\in_R Z_q$，然后选择碰撞自由的单向 Hash 函数 $H:\{0,1\}^*\rightarrow Z_q$，$H':\{0,1\}^*\rightarrow Z_p$。银行用于签名的私、公钥为：$x\in_R Z_q$，$y=g^x$。

用于映射公用信息(面额、有效期)的 Hash 函数可定义为：$H_0(m_P)\triangleq[H'(m_P)]^{(p-1)/q} \bmod q$，根据欧拉定理易知：$H_0:\{0,1\}^*\rightarrow G_q$。

银行公布系统参数 $p,q,g,g_1,g_2,H(\cdot),H'(\cdot)$、公钥 y 以及电子现金自取款日起至失效的最大天数 D_V。

银行创建两个数据库，其一为帐户信息数据库，记录帐号、帐面余额及用户真实身份(如身份证号或数字证书)等信息；其二为付款说明数据库，记录每个合法电子现金的支付信息。

部分受限盲签名应用到离线电子现金系统时，信息 m 分为 pk_1,pk_2 两部分：

(1) pk_1 中嵌入有用户的身份信息(用户开户注册时产生的私钥，它构成了电子现金的一部分私钥)；

(2) pk_2 中嵌入电子现金的另外一部分私钥。

由于用户开户只需一次，为最大限度提高取款协议时的效率，可以将 z' 的计算放入注册阶段。于是，用户的注册过程为：用户随机产生标识身份信息的私钥 $S_U\in_R Z_q$，计算 $pk_0=g_1^{S_U}g_2$ 并确保它不等于1，将公钥 $p_U=g_1^{S_U}$ 告之银行，同时用 Schnorr 零知识证明协议[14]向银行证明他知道 p_U 关于 g_1 的离散对数 $\log_{g_1}p_U=s_U$。银行计算并验证 $pk_0=p_Ug_2\neq1$ 后将 $z'=pk_0^x$ 发给用户，并在帐户信息数据库中新增一条记录，保存 pk_0,z'。

商家按常规注册流程在银行处开户即可。

4.2 取款协议

假定用户帐户上已预存了一定量的现金。用户通过与银行执行取款协议以提取各种不同面额的电子现金。取款协议实质上是部分受限盲签名的具体应用。取款的过程就是用户构造电子现金的公私钥，其公钥及面额、有效期将由银行签名。由于 $pk_1=pk_0'=g_1^{S_U}g_2'$，它满足盲不变性，即用户对 pk_0 盲变换后得到的电子现金公钥的一部分 pk_1 的表示中关于 g_1 的指数与关于 g_2 的指数的商固定为用户注册时生成的私钥 S_U。这也就是限制用户必须将自己的身份信息嵌入到电子现金中去。因为使用了受限盲变换，所以如果用户诚实地花费电子现金，则他嵌入的身份信息将不会暴露，反之，如他重复花费电子现金，则银行可以在多项式时间内计算出他的私钥 S_U 从而揭露不诚实用户的身份，具体细节我们将在存款协议中给出。

协议开始时，用户传送他想要提取电子现金的面额 d 后，银行和用户双方均知道并可计算电子现金有效期 λ 及公共信息 d,λ 的 Hash 值 y_2。我们采用前后处理的方法以尽量减少用户在线计算量，即在前处理阶段，银行和用户并行进行各自的计算，这样当用户收到银行发送的 a_1',a_2',b' 后只需1次模幂运算和3次模乘运算(模加和求 Hash 值的计算量相对较少，可忽略不计)。取款协议的具体过程详见图1。

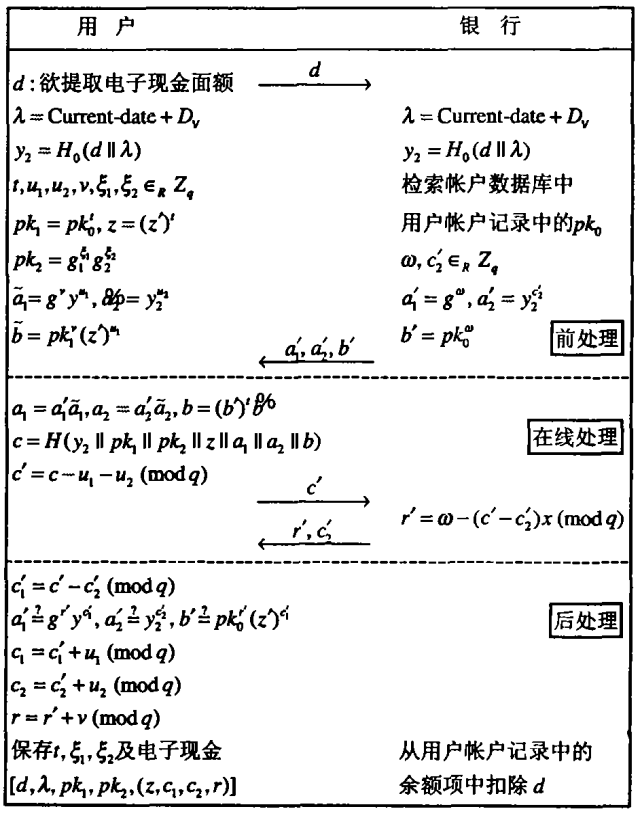

图1 离线电子现金系统取款协议

最终，用户获得电子现金：$[d,\lambda,pk_1,pk_2,(z,c_1,c_2,r)]$，其中 (z,c_1,c_2,r) 为银行对电子现金的面额 d、有效期 λ、公钥 pk_1,pk_2 的签名。电子现金的私钥为 (S_U,t,ξ_1,ξ_2)。银行则从用户帐户余额中扣款。

4.3 支付协议

用户可以用他提取的电子现金匿名地购买商家提供的商品或服务。用户支付电子现金给商家本质上是用电子现金的私钥对商家的付款请求进行签名。

商家首先检查电子现金有效期是否超过了本次支付发生的日期及 $pk_1\overset{?}{\neq}1$，接着用银行的公钥 y 验证电子现金的合法性，如验证通过则产生本次交易的付款请求 Pay-claim，它包括商家身份 ID_{Shop}、交易日期 T_d、交易金额 T_a、所购货物号 ID_{goods} 以及一个随机数 $\varepsilon\in_R Z_q$。商家在验证用户对电子现金公钥 pk_1,pk_2 和付款请求的 Hash 值签名的正确性后保存电子现金，付款请求及用户签名，组织发送货物。支付协议的具体过程详见图2。

由于 $g_1^{r_1}g_2^{r_2}=g_1^{s_U+k\xi_1}g_2^{t+k\xi_2}=(g_1^{S_U}g_2)^t(g_1^{\xi_1}g_2^{\xi_2})^k=pk_1pk_2^k$，因此用户提取的合法电子现金对 h 的签名必定能通过商家的验证。基于有限循环群 G_q 中表示问题的困难性，只有知道电子现金私钥 (S_U,t,ξ_1,ξ_2) 的用户才能产生合法签名；另一方面 $H(\cdot)$ 为强碰撞自由的 Hash 函数，支付协议要求用户对 Pay-claim 及公钥 pk_1,pk_2 的 Hash 值进行签名，基于表示问题和 $H(\cdot)$ 的单向性，强抗碰撞性，即使用户与商家串通也不能伪

造电子现金及其签名。

对于商家或其他潜在攻击者而言，计算签名(ρ_1,ρ_2)的两个表达式中共有4个未知参数，他们除了穷举之外别无它法以获取用户合法电子现金的私钥。

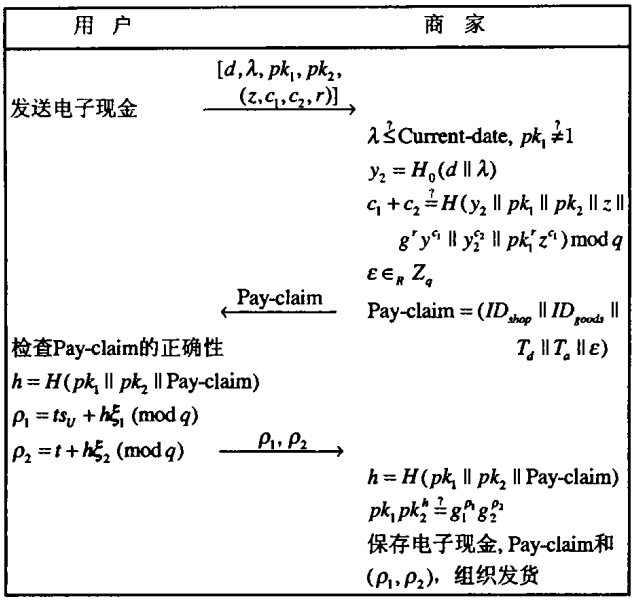

图2 离线电子现金系统支付协议

4.4 存款协议

商家定期将收取的电子现金存入银行，通过与银行执行存款协议实现电子现金价值的转移。首先，商家将电子现金、对应的付款请求 Pay-claim 及签名(ρ_1,ρ_2)传给银行，随后银行执行与商家在支付协议中相同的电子现金合法性，用户签名正确性的验证，如果检验无误，则执行重复行为的检测。

由于电子现金为具有一定价值的(二进制)数字信息，而信息的拷贝是非常容易的，且拷贝品完全是原电子现金的克隆，没有1 bit 的差错。不诚实的用户可能将某一合法电子现金拷贝多份进行花费，而不诚实的商家也有可能在接受了用户支付的电子现金后，将其拷贝多份予以存款。这些非法的重复行为均由银行在存款阶段予以揭示。因为支付协议要求商家对每一电子现金的支付均要在 Pay-claim 中含入一随机数 ε，正常情况下，不同电子现金支付时，经 $H(\cdot)$作用后得到的 h 是不同的。银行检索付款说明数据库，如果存在与根据商家传送的支付交易信息计算出的 h 相同的记录，则商家试图重复存储电子现金，银行拒绝对商家转帐。

银行检索付款说明数据库时，如果存在与商家传送的电子现金相同的记录存在，说明某用户已经重复花费了该电子现金，即用户用同一电子现金及其拷贝对不同商家或同一商家的不同付款请求进行了签名。

假设数据库中记录的和商家存款时传送的付款请求及 Hash 值、用户签名分别为 Pay-claim′，h'，(ρ_1',ρ_2')和 Pay-claim，h，(ρ_1,ρ_2)，满足 $pk_1 pk_2^{h'} = g_1^{\rho_1'} g_2^{\rho_2'}$，$pk_1 pk_2^{h} = g_1^{\rho_1} g_2^{\rho_2}$，其中：Pay-claim′≠ Pay-claim，$h' \neq h$，则银行可以计算出：

$$pk_1 = g_1^{(h\rho_1' - h'\rho_1)/(h-h')} g_2^{(h\rho_2' - h'\rho_2)/(h-h')}$$

又由 $pk_1 = pk_0^t = (p_U g_2)^t = g_1^{ts_U} g_2^t$ 得 $ts_U = (h\rho_1' - h'\rho_1)/(h-h')$，$t = (h\rho_2' - h'\rho_2)/(h-h')$。注意到用户注册时银行要计算并核查 $pk_0 \neq 1$，商家在支付协议中及银行在存款协议的前期均要检查 $pk_1 \neq 1$，从而 $t \neq 0$，最终银行计算出嵌入到电子现金中的标识用户身份的私钥 $S_U = (h\rho_1' - h'\rho_1)/(h\rho_2' - h'\rho_2)$，据此可以得到 $pk_0 = g_1^{S_U} g_2$，查询帐户信息数据库，揭示出重复花费者的真实身份。

如果没有检测到重复存储或重复花费，则银行保存商家发送的电子现金，付款请求，用户签名至付款信息数据库中，并增加商家的帐户余额。需要说明的是，商家一般会存储大量的电子现金，实际应用中，可以让银行服务器在半夜成批完成商家存款，正常工作时间则接受用户注册与取款，这样一方面满足了用户(其数量远大于商家数量)的服务请求，另一方面整个系统效率达到最大化。此外银行每日要从数据库中删除已过期的电子现金的记录，从而银行通过制定电子现金的最大流通天数 D_V 可以将付款说明数据库的存储大小限定在一个合理的范围内。

电子现金是一种小额支付方式，如果用户重复花费电子现金，则银行事后检测出来后的惩罚将使这些不诚实用户得不偿失。另外根据文[4,7]的思想，部分受限盲签名也可以应用到采用防窜改智能卡的电子现金系统中，从而"事先阻止"用户重复花费电子现金。

结束语 本文提出了一种改进的部分受限盲签名方案，该方案具有通信量少、(在线)计算量小的优点。同时，我们给出了部分受限盲签名在离线电子现金系统中的具体应用。本文的电子现金系统对不同面额电子现金只需同一银行私钥签发且银行付款说明数据库大小可控制。本文的工作为电子现金的走向实用化提供了一种新的思路。

参 考 文 献

1 Chaum D. Blind signatures for untraceable payments. In: Proc. of Crypto'82, Santa Barbara. Springer-Verlag, 1983. 199～203
2 Juels A, Luby M, Ostrovsky R. Security of blind digital signatures. In: Kaliski J, ed. Advances in Cryptology-Crypto'97. Santa Barbara, volume 1294 of LNCS, Springer- Verlag, 1997. 150～164
3 Brands S. An efficient off-line electronic cash system based on the repre- sentation problem: [Technical Report CS-R9323]. Centre for Mathematics and Computer Science, Amsterdam, Mar. 1993. 24～67
4 Brands S. Untraceable off-line cash in wallet with observers. In: D. Stinson, ed. Advances in Cryptology-Crypto'93. Springer-Verlag, volume 773 of LNCS, Aug. 1993. 302～318
5 Abe M, Okamoto T. Provably secure partially blind signatures. In: Bellare M, ed. Advances in Cryptology-Crypto 2000. Santa Barbara, volume 1880 of LNCS, Springer-Verlag, 2000. 271～286
6 Maitland G, Boyd C. A provably secure restrictive partially blind signature scheme. In: Naccache D, Paillier P, eds. Public key crypto- graphy, International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002. Paris, Feb. 2002, volume 2274 of LNCS, Springer-Verlag, 2002. 99～114
7 Chaum D, Fiat A, Naor M. Untraceable electronic cash. In: Goldwasser S, ed. Advances in Cryptology-Crypto'88. Santa Barbara, Springer-Verlag, volume 403 of LNCS, California, Aug. 1988. 319～327
8 Ferguson N. Single term off-line coins. In: Helleseth T, ed. Advances in Cryptology- Eurocypt'93. Berlin, Springer-Verlag. Volume 765 of LNCS, 1994. 318～328
9 Ferguson N. Extensions of single-term off-line coins. In: Advances in Cryptology-Crypto'93. Volume 773 of LNCS, Springer-Verlag, 1993. 292～301
10 Franklin M, Yung M. Secure and efficient off-line digital money. In: Lingas A, Karlsson R, Carlsson S, eds. Proc. of ICALP'93, Lund, Sweden, volume 700 of LNCS. Springer-Verlag, 1993. 265～276
11 Yacobi Y. Efficient electronic money. In: Pieprzyk J, Safavi-Naini R, eds. Proc. of Asiacrypt'94, Wollongong, volume 917 of LNCS, Springer-Verlag, 1994. 153～163
12 Camenisch J, Maurer U, Stadler M. Digital payment systems with passive anonymity-revoking trustees. Journal of Computer Security, 1997, 5(1): 69～89
13 Chaum D, Pedersen T. Wallet databases with observers. In: Brickell E, ed. Proc. of Crypto 92, Berlin, Springer-Verlag, volume 740 of LNCS, 1992. 89～105
14 Schnorr C. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4 (3): 161～174