盲签名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)
E-mail:pbdhl@sina.com

摘　要　该文根据近年来国内外关于盲签名的研究背景及进展,阐述了盲签名的概念和基本思想,分析了两种电子现金实现方案,着重探讨了盲签名在电子现金取款协议中的应用。同时给出了检测重复花费电子现金的方法。

关键词　盲签名　电子现金　表示问题　重复花费

文章编号 1002-8331-(2003)19-0031-03　**文献标识码** A　**中图分类号** TP391

The Applications of Blind Signature in E-cash

Peng Bing　Yang Zongkai　Tan Yunmeng
(Department of Electronic & Information,HUST,Wuhan 430074)

Abstract: In this paper,the basic conceptions of blind signature are described according to its recent progress.The paper analyzes two schemes of e-cash and focuses on the application of blind signature to the withdrawal protocol of e-cash.It presents some methods to discover the double spending of e-cash as well.

Keywords: Blind signature,E-cash,Representation problem,Double spending

随着 Internet 电子商务的发展和金融电子化的普及,传统的交易方式正在发生着一场深刻的变革。电子现金作为电子商务中的一种重要支付手段,日益受到国内外学者的重视,其研究也在不断深入。普通数字签名技术是实现身份认证、数据完整性保障和非否认服务的基础,是开展电子商务的重要工具,但由于签名者能够获悉待签文件的内容而使其不适合于需要隐藏某些用户信息的电子现金系统。盲签名可以让签名者在不知道所签文件内容的情况下签名,而文件拥有者将该签名去盲后能够得到签名者关于真实文件的签名。

为便于叙述,文中||表示串连接,$\in_R$ 表示随机选择,Z_p 表示小于 p 的非负整数,Z_q^* 表示小于 q 的正整数。如不另作说明,签名者的公私钥分别为 x,y,σ_x 表示签名者用私钥 x 产生的盲签名。G_q 为 Z_p^* 的唯一循环子群,其阶为 q,$g\in Z_p^*$ 为 G_q 的生成元,其中 p 是二进制位大于 512 的大素数,q 是 $p-1$ 一个大素因子,其二进制位大于 160。$H()$ 为冲突自由的单向散列函数。

1　盲签名的基本概念

由于用户的个人消费信息(如时间、形式、内容等)对商家、银行或非法组织具有极其重要的意义,因此电子现金系统必须保护用户的隐私,即所谓的匿名性。实现匿名性的关键技术是 D.Chaum 提出的盲签名[1,2]。简单地说,盲签名是一个两方协议,接收者先对原始信息进行盲化然后发送给签名者;签名者对盲化后的信息进行签名并返还给接收者;接收者进行去盲化,最终得到签名者关于原始信息的正确签名。盲签名的正式定义如下:

定义 1　一个盲签名方案是一个算法的三元组 (gen,IP,ver),其中 gen 是概率型算法,IP 是签名者 S 和接收者 R 之间的交互协议 (R,S),ver 是确定型验证算法。gen 输入系统参数,输出签名者 S 的私钥 x 和公钥 y。协议 (R,S) 中 S 的输入是 x,R 的输入是消息 m 和 y,R 的输出是 m 的签名 σ_x。ver 输入消息 m、签名 σ_x 和 S 的公钥 y,输出 true 或 false。

盲签名方案应当具有如下性质:

(1)正确性:如果 R 和 S 都正确地执行 IP,则签名满足 ver。

(2)不可伪造性:任何不知道私钥 x 的人都不可能产生正确的签名 σ_x。

(3)盲性:签名者的协议信息和消息-签名对是不可链接的。即给定若干次签名会话的协议信息和若干个消息-签名对,S 不能确定协议信息与消息-签名对的对应关系。

假定盲变换和去盲变换分别为 ξ,θ,则在协议执行中,接收者看到的消息-签名对为 $(m,\sigma_x(m))$,而签名者看到的消息-签名对为 $(\xi(m),\sigma_x(\xi(m)))$,并且以下关系式成立:

$$\sigma_x(m)=\theta(\sigma_x(\xi(m)))$$

D.Chaum 在提出盲签名的同时,给出了盲签名的第一个实现方案:盲 RSA 签名方案。该方案从 RSA 公开密钥算法演变而来。设签名者 S 的私钥为 d,公钥为 (k,e),按如下步骤接收者 R 可以得到签名者 S 的盲签名。

(1)R 在 1 至 n 之间选择一随机数 k,计算 $m'=mk^e \bmod n$,从而隐藏待签名消息 m;

(2)S 对 m' 签名,即计算 $(m')^d$ 并返还给 R;

(3)R 除以盲因子 k,即计算 $\sigma_d(m)=(m')^d/k \bmod n$,得到 S 关于 m 的盲签名 $\sigma_d(m)$。

容易证明:$\sigma_d(m)=\dfrac{(m')^d}{k}=\dfrac{(mk^e)^d}{k}=m^d \bmod n$。

基金项目:国家自然科学基金资助项目(编号:90104033)

作者简介:彭冰,男,博士,研究方向是网络安全与电子支付。杨宗凯,男,教授,博士生导师,研究方向是现代通信网络,电子商务。谭运猛,男,博士,副教授,研究方向是现代密码学与网络安全。

一般基于离散对数的盲签名方案如下所述：

(1)签名者 S 随机选择 $k_3 \in_R Z_q$，计算 $r_3=g^{k_3} \bmod p$ 并将 r_3 发送给接收者 R；

(2)R 随机选择 $k_1, k_2 \in_R Z_q$，计算 $r_1=g^{k_1} \bmod p$，$r_2=g^{k_2} \bmod p$；

(3)R 根据盲变换等式 $a_b m'+b_b m+c_b \equiv 0 \bmod q$，对 m 变盲得到 m'并将 m'发送给 S；

(4)S 根据签名等式 $a_s m'+b_s s'+c_s \equiv 0 \bmod q$ 计算签名 s'，并将签名 s'发送给 R；

(5)R 根据去盲变换等式 $a_m s+b_m s'+c_m \equiv 0 \bmod q$ 计算最后的签名结果 s；

(6)如果消息-签名对 (m,s) 满足 $g^{ma_s b_b b_m+sa_m a_b b_s+a_s b_m c_b+a_b b_s c_m}=g^{a_b b_m c_s} \bmod p$，则 R 接受 S 对消息 m 的签名，否则拒绝签名。

上述方案 9 个参数的不同取值可以演变为不同的基于离散对数的盲签名方案，例如取：$a_b=a_m=b_s=1$，$b_b=b_m=-1$，$a_s=x$，$c_b=k_2$，$c_s=-k_3$，$c_m=-k_1$，则得到 Schnorr 盲签名方案[3]。

在电子现金系统中目前常用的盲签名协议有 RSA 盲签名、Schnorr 盲签名、DSA 盲签名、Okamoto 盲签名、Nyberg-Rueppel 盲签名等。这些盲签名均从相应的普通数字签名协议中变换而来。

一个典型的电子现金支付系统包括取款、支付、存款三个协议，其中盲签名主要发生在取款阶段，以下将着重讨论在其取款协议中盲签名的应用，并假定发行电子现金的银行和商家的帐户银行为同一家银行。

2 基于分割选择的盲签名及应用

电子现金本质上是一个由用户（联合发行银行）产生的公钥和发行银行对该公钥的盲签名组成的数组。由于数字信息的拷贝是一件非常容易的事，而且拷贝与原始信息完全相同，所以无法象普通纸币那样在纸币本身采取众多防伪措施。目前比较成熟的方法是发行银行维护一个已发行的电子现金的数据库，当用户花费了一笔电子现金，接受该电子现金的商家需要定期（或立即）在发行银行（或通过其它清算系统）处存储电子现金，此时，银行将检索数据库确认该电子现金是“新鲜的”，即未曾被存储过。如果是用户通过复制的手段，得到另一个非法电子现金并花费之，则当商家存储该非法电子现金时，银行会发现数据库已经记载了合法电子现金的存储，从而得知用户企图“重复花费”。当然，商家也可能“重复花费”，所以银行也要采取措施防止商家的“重复花费”。

为了尽量杜绝“重复花费”，银行应当揭露出实施了“重复花费”的用户的身份，所以用户产生的公钥必须嵌入他的个人身份信息，变盲后发送给银行进行盲签名。银行如何知道用户是否如实地将个人信息嵌入到了盲消息中，一种可选方案是采用分割-选择技术[4]。

这里银行 B 为签名者，该银行的某一用户 U 为接收者，在系统注册阶段，U 在 B 处开户，B 在用户数据库中添加一条记录，记载 U 的真实身份 ID_R 及其它相关信息。为了取得一电子现金 C，U 与 B 执行取款协议，如图 1 所示。

(1)用户与银行进行双方身份验证，银行根据用户提交的身份承诺检索用户数据库，得到用户的身份信息 ID_R；

(2)用户构造 l 个电子现金公私钥 $(\$_i,\omega_i)$，$(P_i,a_i)$，其中每一个 S_i 均嵌入身份信息 ID_R，用户通过银行的签名公钥 e_b 对待签信息 $red \| H(P_i \| a_i)$ 变盲，然后发送所有的盲消息 M_i 给银行，其中 red 为填充字段，从而使待签信息长度为 n_b；

(3)银行提出质询，在 1 至 l 中随机选取一个数 k 发送给用户；

(4)用户向银行揭示除下标为 k 外的所有 $(\$_i,\omega_i,\rho_i)$；

(5)银行验证除下标为 k 外的所有 $(\$_i,\omega_i,\rho_i)$ 是否满足 $M_i \overset{?}{=} \rho_i^{e_b}[red \| H(\$_i^{(ID_U \| r_i)} \| g^{\omega_i})]$，如果这 $k-1$ 个验证全部通过，银行有 $1-l^{-1}$ 的把握确信用户在构造过程中如实地嵌入了 ID_R；

(6)银行用私钥 d_b 对盲消息 M_k 签名，并发送给用户，同时在电子现金数据库中记录 ID_R 和 σ'，从用户帐户上扣除一笔数额，其等于已提取电子现金的数额；

(7)用户通过除以盲因子 ρ_k 对签名 σ'去盲，得到银行关于 $[red \| H(P_k \| a_k)]$的盲签名 $\sigma_{d_b}(P_k,a_k)=[red \| H(P_k \| a_k)]^{d_b}$，用户验证该盲签名的正确性，最后用户存储已取得的电子现金 $C=\{(P_k,a_k),\sigma_{d_b}(P_k,a_k)\}$，相应的私钥为 $(\$_k,\omega_k)$。

可以看出，分割-选择的效率是很低的。例如为了使发现用户没有如实嵌入身份信息的概率小于 0.001，则用户必须构造 1000 个电子现金公私钥对，而银行也必须要验证 999 个消息，由于构造和验证过程中都用到了模指数运算，从而大量的运算时间用在了确保用户正确构造盲消息之中，而真正盲签名的时间和用户验证盲签名的时间几乎可以忽略。

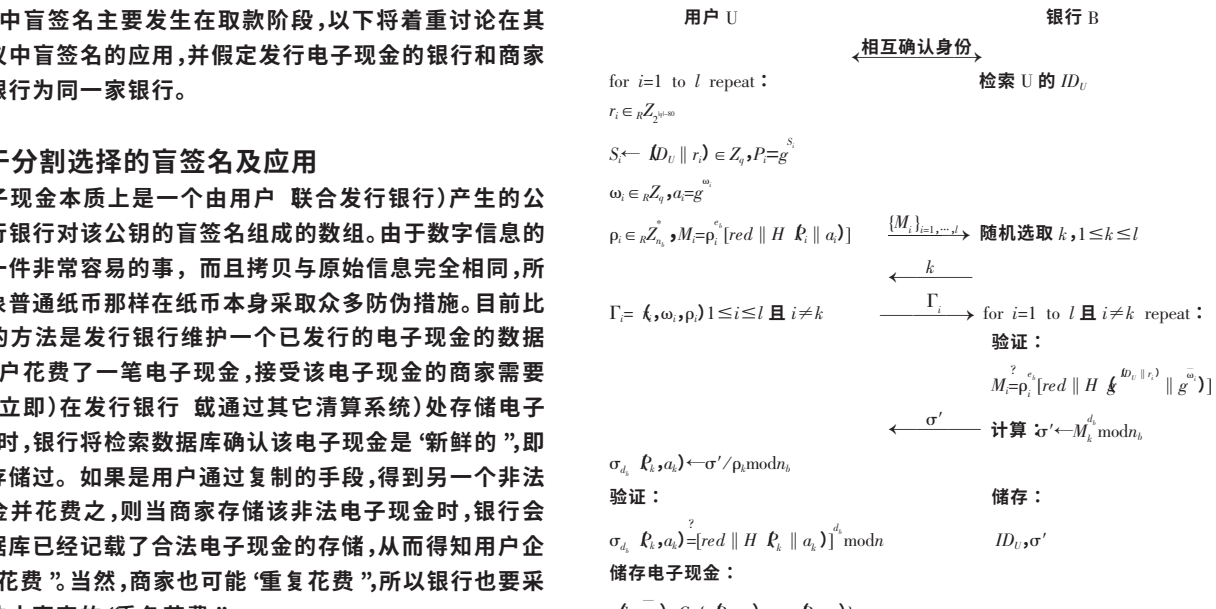

图 1 基于分割-选择的取款协议

3 基于表示问题的盲签名及应用

迄今为止提出的离线不可分电子现金方案中，S.Brand 提出的单条信息系统[5]是效率最高的，许多后续电子现金方案都建立在他的研究成果上，该方案的安全性主要基于有限素数阶群上的表示问题。

定义 2 设常数 $k \ge 2$，长度为 k 的生成重为 $(g_1,\cdots,g_k)$，其中 $g_i \in G_q \backslash \{1\}$ 且对于任何 $i,j \in \{1,\cdots,k\}$，$i \ne j$ 有 $g_i \ne g_j$，长度为 k 的指数重为 $(a_1,\cdots,a_k) \in Z_q^k$。任给 $h \in G_q$，则 h 关于 $(g_1,\cdots,g_k)$ 的表示是满足 $\prod_{i=1}^{k} g_i^{a_i}=h$ 的一个指数重 $\{a_1,\cdots,a_k\}$。

定义 3 表示问题（RP）：给定有限循环群 G_q，生成重 $(g_1,\cdots,g_k)$ 和整数 $h \in G_q$，找到一个特定的指数重 $\{a_1,\cdots,a_k\}$ 满足

$\prod_{i=1}^{k} g_i^{a_i}=h$。

表示问题是离散问题的推广，对于任一给定的 $h\in G_q$，存在着 q^{k-1} 个不同表示。解决表示问题就是在多项式时间内，在这 q^{k-1} 个不同表示中寻找某个特定的指数重。

基于表示问题的电子现金方案其基本思路是用户只有将身份信息嵌入到电子现金中，才能在随后的支付协议中花费，而用户与银行执行取款协议时，只需提交一条关于身份的信息，如果用户花费该合法电子现金一次，则其匿名性与不可追踪性将无条件得到满足，但用户如重复花费的话，银行可根据两次花费时支付阶段产生的信息揭示用户的身份。具体取款协议执行如图 2 所示。

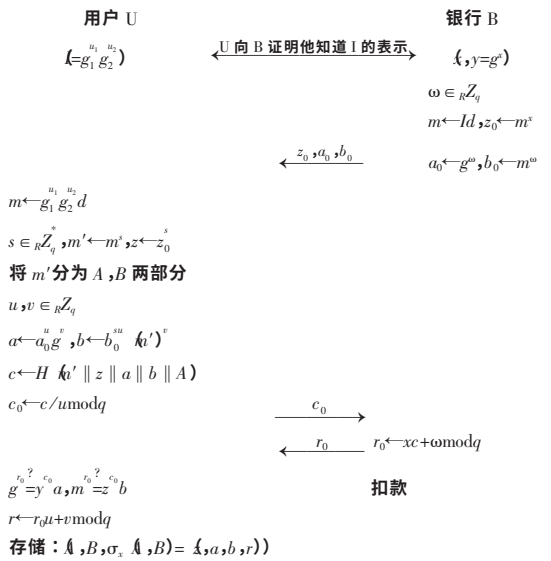

图 2　基于表示问题的取款协议

在系统建立及开户阶段，用户随机产生 u_1,u_2 并计算 $I=g_1^{u_1}g_2^{u_2}$，用户向银行公布 I，从而银行为用户存储一条记录，记载 I、用户真实身份、帐户号等。只有用户知道 I 的表示，但银行可以在用户重复花费电子现金后，计算出 u_1,u_2，从而揭示用户身份。此外，$d\neq g_1,g_2$ 为“哑元”，它也是 G_q 的生成元，用于在支付过程中阻止商家计算出诚实用户的身份信息。

(1)用户与银行进行双方身份验证，从而银行确信用户知道 I 关于 (g_1,g_2) 的表示；

(2)银行计算 $m=Id$，以及 a_0,b_0,z_0 并发送给用户；

(3)用户也计算 m，并随机选取 s 将 m,z_0 变盲为 m',z，同时将 m' 分割成 A,B 两部分，然后随机选取 u,v 对 a_0,b_0 变盲，通过单向散列函数 H ()计算询问 c，在发送给银行之前，将 c 变盲为 c_0；

(4)银行计算响应 $r_0=xc+\omega \bmod q$ 并发送给用户，同时从用户帐户上扣除一笔数额，其等于已提取电子现金的数额；

(5)用户验证 $g^{r_0}\stackrel{?}{=}y^{c_0}a, m^{r_0}\stackrel{?}{=}z^{c_0}b$，然后将响应 r_0 变换为 r，并在电子钱包中存储电子现金 $(A,B,\sigma_x(A,B)=(a,b,r))$。

用户在支付电子现金给商家时，要出示 $(A,B,\sigma_x(A,B))$，商家将 A,B 合并为 m' 并确信 $AB\neq 1$，然后根据 $\sigma_x(A,B)$ 计算 $c=H(AB\|z\|a\|b\|A)$，验证 $g^r\stackrel{?}{=}y^c a$，$(m')^r\stackrel{?}{=}z^r b$ 从而判断用户支付的电子现金是否合法。从取款协议中可看出，因 z_0,b_0 的计算均包含 m，c 中包含 A，而银行通过 Id 得到 m，所以必然包含用户身份 I，如果用户不如实将 I 包含在 m' 中，或在将 m' 分成 A,B 两部分时有意不包含身份信息，则他不可能获得合法电子现金（在支付时不能验证通过），除非他能在多项式时间内解决表示问题。

如果用户重复花费了某合法电子现金，则银行可以按以下方法揭示他的真实身份（即通过计算出他的私钥 u_1,u_2，从而能够在数据库中检索出他的真实身份）。

设 $u_1s=\alpha_1+\beta_1, u_2s=\alpha_2+\beta_2, s=\gamma_1+\gamma_2$ 则 $A=g_1^{\alpha_1}g_2^{\beta_1}d^{\gamma_1}$，$B=g_1^{\alpha_2}g_2^{\beta_2}d^{\gamma_2}$，当商家验证完电子现金合法性后，随机选择 $\varepsilon\in {}_RZ_q^*$ 作为询问，用户响应 $r_1=\alpha_1+\varepsilon\alpha_2 \bmod q$，$r_2=\beta_1+\varepsilon\beta_2 \bmod q$，$r_3=\gamma_1+\varepsilon\gamma_2 \bmod q$，此即为电子现金对支付信息产生的信息，商家验证响应的正确性后保存电子现金 $(A,B,\sigma_x(A,B))$和交互信息 ε,r_1,r_2,r_3。在存款阶段，商家会出示这些信息。银行在验证完电子现金的合法性后将检索数据库，核实是否有相同的电子现金存在于数据库中，如有，说明有人重复花费。假定是用户重复花费（即 $\varepsilon\neq\varepsilon'$），显然有两笔不同的支付信息，即有 $AB^{\varepsilon}=g_1^{r_1}g_2^{r_2}d^{r_3}$，$AB^{\varepsilon'}=g_1^{r_1'}g_2^{r_2'}d^{r_3'}$，从而

$$A=g_1^{(\varepsilon' r_1-\varepsilon r_1')(\varepsilon'-\varepsilon)^{-1}}g_2^{(\varepsilon' r_2-\varepsilon r_2')(\varepsilon'-\varepsilon)^{-1}}d^{(\varepsilon' r_3-\varepsilon r_3')(\varepsilon'-\varepsilon)^{-1}}$$

$$B=g_1^{(r_1-r_1')(\varepsilon'-\varepsilon)^{-1}}g_2^{(r_2-r_2')(\varepsilon'-\varepsilon)^{-1}}d^{(r_3-r_3')(\varepsilon'-\varepsilon)^{-1}}$$

于是：

$$\begin{cases}\alpha_1=\dfrac{\varepsilon' r_1-\varepsilon r_1'}{\varepsilon'-\varepsilon},\ \beta_1=\dfrac{\varepsilon' r_2-\varepsilon r_2'}{\varepsilon'-\varepsilon},\ \gamma_1=\dfrac{\varepsilon' r_3-\varepsilon r_3'}{\varepsilon'-\varepsilon}\\ \alpha_2=\dfrac{r_1-r_1'}{\varepsilon'-\varepsilon},\ \beta_2=\dfrac{r_2-r_2'}{\varepsilon'-\varepsilon},\ \gamma_2=\dfrac{r_3-r_3'}{\varepsilon'-\varepsilon}\end{cases}$$

因为 s 不可能为 0，否则 $AB=1$，商家将视该电子现金为非法而不予接受。最终银行计算出：

$u_1=(\alpha_1+\beta_1)(\gamma_1+\gamma_2)^{-1}$，$u_2=(\alpha_2+\beta_2)(\gamma_1+\gamma_2)^{-1}$

如果银行没有检测重复花费行为，则将电子现金及支付信息存入数据库中。

4　结束语

该文探讨了盲签名的基本概念以及在电子现金取款协议中的具体应用。应当指出，盲签名是实现电子现金匿名性的有力工具，但用户身份的隐藏也带来无法从一次花费中就发现洗钱、敲诈、绑架勒索等犯罪份子身份的弊端，于是可撤消匿名性的盲签名被提出来。此外，构造多银行发行电子现金系统又提出了群盲签名的要求。如何对原有的盲签名方案加以改造以满足各种新的需求及在保证安全的前提下，进一步提高盲签名的在线处理效率还有待于进一步研究。（收稿日期：2002 年 9 月）

参考文献

1.D Chaum.Blind signatures for untraceable payments[C].In:Advanced in Cryptology,Proc Crypto'82,Springer-Verlag,1983:199~203

2.D Chaum.Security without identification:transaction systems to make big brother obsolete[J].Communications of the ACM,1985;(28):1030~1044

3.B Schneier.Appliced cryptography-protocols,algorithms and source code in C[M].New York:Wiley Press Inc,1994

4.C Radu,M Vandenwauver,R Govaerts et al.An efficient traceable payment system[C].In:Proc of the 16th Symposium on Information Theory in the Benelux,1995:61~67

5.S Brands.An efficient off-line electronic cash system based on the representation problem[R].Reprot CS-R9323,Centrum voor Wiskunde en Informatica,1993-03