一个公正的电子货币方案*)

A Fair e-cash Scheme

王常吉　裴定一

(中国科技大学研究生院信息安全国家重点实验室　北京 100080)

Abstract In this paper, we propose a fair e-cash scheme based on [1]. On the one hand, User's anonymity is protected in our system, On the other hand, bank can trace e-coin and owner of e-coin with the help of the group manager, so it can prevent laundering, corruption and kidnapping, and the security of the scheme is based on strong RSA assumption and decision Diffie-Hellman assumption.

Keywords Blind signature, Group signature, Signature of knowledge

一、引言

盲数字签名方案最初由 Chaum 在文[2]中提出，一个盲数字签名方案是一个发送者和签名者之间的密码协议，该协议允许发送者选择一个消息，从签名者处获得对该消息的数字签名，而签名者看不到他所签名的消息的内容。

文[3]最早提出了一类基于盲数字签名限制性假设的匿名的电子支付系统，大家知道，匿名的电子支付系统，在保护用户的个人隐私的同时，也给犯罪分子带来了可乘之机，如洗钱、贪污和敲诈等问题。如何防止这一问题，已成为电子支付研究的一个热点，文[5]在文[3]的基础上，最早提出了匿名性受控制的(即所谓公正的)离线的电子货币的实现方案，在特定的条件(如法律要求)下，用户的匿名性可以被撤消，而在其余的条件下，用户的所有支付依然是匿名的。之后，不少人对此系统作了进一步的改进，然而，他们所考虑的公正系统，都是建立在盲数字签名的限制性假设之上，而这一点目前还没有严格证明此假设的正确性。

群数字签名最早由 Chaum 和 van Heyst 在文[4]中引进，在群数字签名方案中，群的任何一个成员都可以代表群进行签名，接收者使用单一的群公钥来验证群成员的签名，除了群管理中心，没有人能够确定出签名者的身份，同时没有人(包括群管理中心)能够假冒某个群成员进行签名。文[4]提出了四种群数字签名的实现方案，之后不少人对这些方案作了改进，然而这些群数字签名有一个共同的缺陷，就是群签名的长度与群公钥的长度都线性依赖于群成员的多少，这就使得这些方案不适用于成员多的大群。最近文[1]提出了一个实用的可抵抗合谋攻击的、且群的公钥和群签名的长度都固定不变，与群成员的多少无关的群数字签名方案，并且在强 RSA 假设与确定的 Diffie-Hellman 假设的前提下，所提出的群数字签名是安全的。

本文利用文[1]的结果，提出了一个公正的离线的电子货币方案：所有用户形成一个群，用户从群管理中心处领取成员证书，然后从银行提取由银行盲签名的电子货币，在支付时，用户须向商家证明他拥有一个合法的成员证书，并且证书已嵌入在电子货币中，本文的系统实现了跟踪重复花费者、货币所有者以及电子货币的功能。

在第二节，我们介绍文[1]中出现的假设与基本工具；第三节详细讨论公正的电子货币方案的取款、支付和存款协议，以及跟踪重复花费者、电子货币和货币所有者的协议，并分析了系统的安全性；第四节是本文所得出的结论。

二、假设与基本工具

为方便起见，我们引进如下的记号：

$x\in_R E$ 表示 x 在集合 E 中随机地选取；$\|$ 表示字符串的连接操作；H 表示为无碰撞的 hash 函数，它把任意比特长度的串映射为 k 比特的串；m 表示与知识签名有关的信息，可以是空串 ζ；循环群 $G=\langle g\rangle$ 的阶 $\#G$ 未知，但阶的比特长度 $\lceil\log_2(\#G)\rceil=l_G$ 是公开的；假定安全参数 $\varepsilon>1$。

强 RSA 问题：记 $n=pq$ 是一个 RSA 型模，G 是 Z_n^* 的一个阶为 $\#G$ 的循环子群，$\lceil\log_2(\#G)\rceil=l_G$，给定 n 和 $z\in G$，寻找满足 $z=u^e \bmod n$ 的 $u\in G$ 和 $e\in Z_{>1}$。

*)国家自然科学基金资助项目，批准号 19931010。

强 RSA 假设：存在一个概率多项式时间算法 A，输入安全参数 l_G，输出 (n,x)，使得对所有的概率多项式时间的算法 P，P 能解决强 RSA 问题的概率是可忽略不计的。

确定的 Diffie-Hellman 问题：记 $G=\langle g\rangle$ 是一个由 $\#G$ 阶元素 g 生成的循环群，$\lceil\log_2(\#G)\rceil=l_G$，给定 g,g^x,g^y 和 $g^z\in G$，确定元素 g^{xy} 是否等于 g^z。

确定的 Diffie-Hellman 假设：不存在多项式时间的算法 P，P 能以不可忽略的概率区分两个分布 D 和 R，其中 $D=(g,g^x,g^y,g^z),x,y,z\in_R Z_{\#G},R=(g,g^x,g^y,g^{xy}),x,y\in_R Z_{\#G}$。

记 n 是一个强 RSA 型模，即 $n=pq,p\neq q,p=2p'+1,q=2q'+1,p',q',p,q$ 均为素数，记 $QR(n)$ 为由 $p'q'$ 阶元素所生成的循环群，下面的引理指出了如何寻找 $QR(n)$ 的生成元 g。

引理：记 $n=pq$，其中 $p\neq q,p=2p'+1,q=2q'+1,p',q',p,q$ 均为素数，则 Z_n^* 中元素的阶一定属于集合 $\{1,2,p',q',2p',2q',p'q',2p'q'\}$，并且元素 $a\in Z_n^*$ 的阶等于 $p'q'$ 或 $2p'q'$ 等价于 $\gcd(a\pm1,n)=1$。

推论：令 n 如上引理所述，对任何 $a\in Z_n^*$，使得 $\gcd(a\pm1,n)=1$，则 $\langle a^2\rangle\subset Z_n^*$ 是一个由阶等于 $p'q'$ 的元素所生成的循环群。

如果 n 的分解未知，要确定一个元素 y 是否属于 $QR(n)$，通常认为是计算上不可行的。

定义 1：$y,g\in G$，二元组 $(c,r)\in\{0,1\}^k\times\pm\{0,1\}^{l(l+k)+1}$ 满足 $c=H(m\|g\|y\|g^r y^c)$ 是离散对数 $\log_g y$，且 $\log_g y\in[X-2^{l(l+k)},X+2^{l(l+k)}]$ 的关于 $m\in\{0,1\}^*$ 的一个知识签名。

证明者如果知道一个整数 $x=\log_g y\in[X-2^l,X+2^l]$，可以按如下步骤计算出这一知识签名。

- 选择 $s\in_R\{0,1\}^{n(l+k)}$，计算 $y'=g^s$
- $c=H(m\|g\|y\|y')$
- 在 Z 中计算 $r=s-c(x-X)$

定义 2：$y_1,y_2,g,h\in G$，二元组 $(c,y)\in\{0,1\}^k\times\pm\{0,1\}^{n(c+k)+1}$ 满足 $c=H(m\|g\|h\|y_1\|y_2\|g^r y_1^c\|h^r y_2^c)$ 是离散对数 $x=\log_g y_1$ 和 $x=\log_h y_2$ 关于信息 $m\in\{0,1\}^*$ 的一个知识签名。

证明者如果知道一个整数 $x=\log_g y_1=\log_h y_2$，可以按如下步骤计算出这一签名。

- 选取 $s\in_R\{0,1\}^{n(c+k)}$，计算 $y_1'=g^s,y_2'=h^s$
- $c=H(m\|g\|h\|y_1\|y_2\|y_1'\|y_2')$
- 在 Z 中计算 $r=s-cx$

以上的假设与知识证明均引自于文[1]。

三、公正的离线电子货币系统

3.1 系统设置

令 $\varepsilon>1,k,l_p$ 为安全参数，$\lambda_1,\lambda_2,\gamma_1,\gamma_2$ 表示比特长度，其中 $\lambda>\varepsilon(\lambda_2+k)+2,\lambda_2>4l_p,\gamma_2>\varepsilon(\gamma_2+k)+2,\gamma_2>\lambda_1+2$，定义范围 $I_1=[2^{\gamma_1}-2^{\gamma_2},2^{\gamma_1}+2^{\gamma_2}],I_2=[2^{\gamma_1}-2^{\gamma_2},2^{\gamma_1}+2^{\gamma_2}]$。

群管理中心随机选取 l_p 比特的素数 p',q'，使得 $p=2p'+1,q=2q'+1$ 均为素数，置 RSA 模 $n=pq$；随机选取元素 $a,a_0,g,h\in_R QR(n),x\in_R Z_{p'q'}^*$，计算 $y=g^x \bmod n$，则群私钥 $S_{GM}=(p',q',x)$，群管理中心公开群公钥 $Y_{GM}=(n,a,a_0,g,h,y)$。

银行选取大素数 p_B,q_B，计算相应的 RSA 模 $n_B=p_Bq_B$，然后选取合适的整数 e_B，使得 $(e_B,\phi(n_B))=1$，计算出满足 $e_Bd_B=1 \bmod \phi(n_B)$ 的 d_B，则银行的私钥 $S_B=(p_B,q_B,d_B)$，银行公开其公钥 $Y_B=(n_B,e_B)$。

3.2 用户到群管理中心处领取证书

1）用户传递身份识别信息给群管理中心，同时选取 $\bar{x}_i\in_R[0,2^{\lambda_2}]$，$\bar{r}\in[0,n^2]$，计算并传送 $C_1=g^{\bar{x}_i}h^{\bar{r}} \bmod n$ 给群管理中心，并向群管理中心证明知道 C_1 关于底 g 和 h 的表示。

2）群管理中心验证用户的身份识别信息和知识证明，检查 $C_1\in QR(n)$，若验证成功，则随机选取 $\alpha_i,\beta_i\in_R[0,2^{\gamma_2}]$，并把 (α_i,β_i) 传送给用户。

3）用户计算 $x_i=2^{\gamma_1}+(\alpha_i\bar{x}_i+\beta_i \bmod 2^{\gamma_2})$，并发送 $C_2=a^{x_i} \bmod n$，并向群管理中心证明知道 C_2 关于底 a 的离散对数，且该离散对数属于 I_1。同时用户也向群管理中心证明他知道整数 u,v,ω_i，满足：①$u=\log_a C_2-2^{\gamma_1}\in[-2^{\gamma_2},2^{\gamma_2}]$，②$C_1g^{\bar{r}}=g^ug^{2^{\gamma_2}}h^v$，这就证明了用户的成员密钥 x_i 的确是由 C_1,α_i,β_i 计算出来的。

4）群管理中心验证上面的证明，检查 $C_2\in QR(n)$，若验证通过，群管理中心选择一个随机素数 $e_i\in I_2$，并计算 $A_i=(C_2a_0)^{1/e_i} \bmod n$，最后群管理中心给用户发送新成员证书 $[A_i,e_i]$，同时存储新成员的身份识别信息与证书。

5）用户验证 $a^{x_i}a_0=A_i^{e_i} \bmod n$。

3.3 用户从银行取款

1）用户通过任何的身份识别协议向银行证实自己是某帐号的合法持有者。

2）用户随机选取 $w\in_R\{0,1\}^{|p|}$，计算 $T_1=A_iy^w \bmod n,T_2=g^w \bmod n,T_3=g^rh^w \bmod n,s=r^{e_B}H(T_1\|T_2) \bmod n_B$，用户把 s,T_2 传递给银行。

3）银行计算并把 $s'=s^{d_B} \bmod n_B,H(T_2)^{d_B} \bmod n_B$ 传送给用户，同时在取款数据库中为用户存储 T_2。

4）用户计算出 $H(T_1\|T_2)^{d_B}=s'^{d_B}/r \bmod n_B$，并存储 $T_2,T_3,H(T_1\|T_2)^{d_B} \bmod n_B,H(T_2)^{d_B} \bmod n_B$。

3.4 用户向商店支付电子货币 C_S

1）记 $msg=I_S\|date/time$，其中 I_S 表示商店在银行的帐号，$date/time$ 表示交易的日期与时间，用户随

机选取 $r_1 \in_R \pm\{0,1\}^{\varepsilon(r_2+k)}$，$r_2 \in_R \pm\{0,1\}^{\varepsilon(\gamma_2+k)}$，$r_3 \in_R \pm\{0,1\}^{\varepsilon(\gamma_2+k+2l_p+1)}$，$r_4 \in_R \pm\{0,1\}^{\varepsilon(2l_p+k)}$，计算 $d_1 = T_1^{r_1}/(a^{r_2}y^{r_3}) \bmod n$，$d_2 = T_2^{r_1}/g^{r_3} \bmod n$，$d_3 = g^{r_1} \bmod n$，$d_4 = g^{r_1}h^{r_4} \bmod n$，$c = H(msg \| g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \| d_1 \| d_2 \| d_3 \| d_4)$，并在 Z 中计算 $s_1 = r_1 - c(e - 2^{\gamma_1})$，$s_2 = r_2 - c(x_1 - 2^{\gamma_1})$，$s_3 = r_3 - ce_1w$，$s_4 = r_4 - cw$，最后用户把 $H(T_2)^{d_B} \bmod n_B$，$H(T_1 \| T_2)^{d_B} \bmod n_B$，以及 $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$ 传递给商家。

2）商家先验证银行的签字，若验证成功，则计算 $c' = H(msg \| g \| h \| y \| a_0 \| a \| T_1 \| T_2 \| T_3 \| a_0^{c}T_1^{-c2^{\gamma_1}}/(a^{s_2-c2^{\gamma_1}}y^{s_3}) \bmod n \| T_2^{c-c2^{\gamma_1}}/g^{s_3} \bmod n \| T_2^{c}g^{s_4} \bmod n \| T_3^{c}g^{s_1-c2^{\gamma_1}}h^{s_4} \bmod n)$，当且仅当 $c = c'$，$s_1 \in \pm\{0,1\}^{\varepsilon(\gamma_2+k+1)}$，$s_2 \in \pm\{0,1\}^{\varepsilon(\gamma_2+k+1)}$，$s_3 \in \pm\{0,1\}^{\varepsilon(\gamma_1+k+2l_p+1+1)}$，$s_4 \in \pm\{0,1\}^{\varepsilon(2l_p+k+1)}$ 时，商家接受用户的支付。

3.5 商家到银行存款电子货币

商家传送 $msg = I_S \| date/time$ 以及支付协议的一个副本给银行，银行如商家一样非交互地验证，若验证成功，则在其存款数据库中搜索 (T_1, T_2, T_3)，有两种可能：(1)搜索失败，即存款数据库中不存在这组值，此时银行在存款数据库中为商家存储 $(T_1, T_2, T_3, date/time)$，并且在帐目数据库中为商家入帐；(2)搜索成功，即在存款数据库中找到了这组值，此时，用户或商家定有欺诈者，若商家新发送的文本中的 $date/time$ 与存款数据库中已有文本的 $date/time$ 相同，则商家试图在银行存储同一文本两次，否则则是用户在不同的商家处两次支付同一电子货币，银行将 (T_1, T_2) 传递给群管理中心，群管理中心计算 $T_2^{w_2} (= y^w) \bmod n$，$T_1/T_2^{w_2} = A_i$，然后群管理中心传回 A_i 对应的用户的身份识别信息，从而找到了试图两次支付同一电子货币的用户。

3.6 电子货币的跟踪

银行提供用户的身份识别信息以及 T_2 给群管理中心，群管理中心根据用户的身份识别信息找到对应的证书 $[A_i, e_i]$，并计算出 $T_1 = A_iT_2^{x_1}$，将 T_1 传送给银行，从而银行得到 $T_1 \| T_2$，再计算出 $H(T_1 \| T_2)^{d_B} \bmod n_B$，$H(T_2)^{d_B} \bmod n_B$，这样就实现了电子货币的跟踪。

3.7 电子货币所有者的跟踪

银行将存款协议中的 (T_1, T_2) 传递给群管理中心，群管理中心计算出 $T_1/T_2^{x_1} = A_i$，群管理中心找到 A_i 所对应的用户的身份识别信息并回传给银行，这样就实现了货币所有者的跟踪。

3.8 安全性分析

本文所提出的电子货币方案的安全性是建立在强 RSA 假设与确定的 Diffie-Hellman 假设之上的。

文[1]已经证明在强 RSA 假设与确定的 Diffie-Hellman 假设下，文[1]中的群数字签名方案是安全的，即群成员不能自己产生，也不能够合谋产生成员证书，并且签名协议是一个关于成员证书和相应的成员密钥的统计零知识的知识证明。用户要在商家支付电子货币，必须向商家证明拥有成员证书，并且成员证书已嵌入在电子货币中，用户不能伪造成员证书，所以用户不能伪造电子货币；因为 RSA 盲签名是一个完备的盲签名体制，银行在取款协议中只是能够得到 T_2，$rH(T_1 \| T_2)^{d_B}$，而其中 r 是用户随机选取的盲因子，$T_2 = g^w$，w 也是由用户随机选取的数，不同的用户可能选取了相同的 w，即根据 $T_2 = g^w$ 并不能确定出取款人的身份识别信息，银行并不知道用户所提取的电子货币 $C_S = (T_1 \| T_2, H(T_1 \| T_2)^{d_B} \bmod n_B)$，另外，容易发现商家和银行从接收到的支付文本 $(c, s_1, s_2, s_3, s_4, T_1, T_2, T_3)$，都不能使银行和商家建立某次支付与某次取款之间的联系，从而用户的匿名性得到保护；由上面重复花费者的检测知，如果用户重复花费某电子货币，其身份识别信息将显露出来；由上面的电子货币的跟踪与电子货币所有者的跟踪的分析可知，群管理中心具有跟踪功能。

结论 本文利用文[1]中群数字签名的结果，提出了一个公正的电子货币系统，一方面，系统能够保证合法用户的匿名性，另一方面，在特定的情况下，通过一个可信方，用户的匿名性可以被撤消，从而可以防止洗钱、贪污和敲诈等问题，本文方案的安全性是建立在强 RSA 假设与确定的 Diffie-Hellman 假设之上的。

参 考 文 献

1 Atemse G, et al. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. CRYPTO'2000, Santa Barbara, California, USA, P. 255～270

2 Chaum D. Blind signatures for untraceable payments. In: Proc of CRYPTO'82, Plenum Press, 1983. 199～203

3 Brands S. Untraceable Off-line Cash in Wallets with Observers. In Advance in Cryptology-Crypto'93, Proceedings(Lecture Notes in Computer Science 773). Springer-Verlage, 1993. 302～318

4 Chaum D, Heyst V. Group Signatures. In Advance in Cryptology-Eurocrypt'91, Proceeding (Lecture Notes in Computer Science 547). Springer-Verlag, 1991. 257～265

5 Frankel Y, Tsioums Y, Yung M. Indirect discourse proof: achieving fair off-line e-cash. In Advance in Cryptology, Proc. of Asiacrypt'96(Lecture Notes in Computer Science 1163). Springer-Verlag, 1996. 286～300