基于多级分布式银行的 Smart Card 电子支付系统 [1]

赵福祥 * ** 王育民 * 赵红云 **

*(西安电子科技大学 ISN 国家重点实验室 西安 710071)
**(西安通信学院 西安 710106)

摘 要 在电子支付系统中，采用分布式电子银行方案更适合于网络运行环境，然而在现行的分布式电子银行方案中，每个用户局限在所开帐户的电子银行取得签发的 Smart Card 和提取或存储电子货币，由于网络的瓶颈作用和安全缺陷，以及用户所处地域的分散性和流动性等因素的限制，使得单一开户的银行方案在实际应用中其分布式特性并未充分得以发挥。针对此，通过采用代理签字与群签字综合的方法，本文提出了多级电子银行的新方案，并对该方案的安全性进行了分析。

关键词 网络安全，电子商务，电子支付，群签字
中图号 TN919.3

1 引 言

在电子支付系统中，银行通过 Smart Card 这样存储载体记录用户所持资金数额，即用户在 Smart Card 上的帐户记录或者电子货币 (以下统称电子货币)。为了在使用中能够正确识别，防止违法者利用不合法手段窃取用户信息， Smart Card 通过硬件及有关的密码技术被设置成为防窜扰记录凭证。用户在网上使用 Smart Card 时，要向商店证实所拥有的电子货币是指定银行合法签发的，即必须向商店出示指定银行在该电子货币上的有效签字，并证明该电子货币是可支付的。在这一过程中，要求持卡人的身份对商家和其它银行是匿名的，银行和商店不能跟踪 Smart Card 上所拥有的电子货币。也就是说，银行和商店可以通过读卡器、电子钱包软件以及手持式电子钱包等设备验证该电子货币是合法的支付，但不应从用户所支付的款项找出用户的身份信息 (重复花费时例外)，也不应找出签发该电子货币的具体银行是谁；同时，当银行再次看见由它签发的电子货币时，不能确认该货币是由它签发的。虽然支付被分成在线和离线两种方式，但所有的电子货币的提款和支付都是基于网络操作的。网络本身缩短了银行、商店和顾客之间的距离，使支付活动变得简单快捷。但由于存在网络传输瓶颈和网络安全的制约，以及用户所处地域的分散性和流动性的制约，因而只有与其支持的网络环境相协调，与网络的特性相符合，所设计的电子支付系统才能发挥其潜在的效能。

为了增强电子支付系统的功能， A.Lysyanskaya 在文献 [1] 中给出了分布式电子银行的方案。所谓分布式电子银行是由某个 "中央" 银行监管的一群银行组成的银行组，该银行组中的每一个银行都能签发电子货币，而商家只需一个群公钥就可验证电子货币的有效性，并且银行商家都不能跟踪某个用户使用的电子货币，但该方案作为一个实用系统仍存在如下不足： (1) 用户的取款和存款被限制在某个开户电子银行中，由于网络传输瓶颈作用，限制了其服务规模，并且如果网络发生堵塞，则无法提款和存款； (2) 由于不同地域的差异与用户的流动性等因素造成网络服务分布不平衡，有可能无法提款和存款； (3) 某一个存取高峰时段中，其存取操作出现超过网络承受时，提款和存款困难； (4) 由于网络结构的复杂性，公众网络覆盖的范围越大要求其安全可靠性越高，这也限制电子银行所提供的服务，并且恶意的攻击更易破坏电子银行的独立服务网关。为了弥补这些不足，本文提出了多级分布式电子银行的新方案，即在分布电子银行中某个主电子银行可指定若干个代理银行为其签发 Smart Card 和代理提款和存款；旨在各电子银行服务的分布性，使得用户只用一张 Smart Card 就可在多个指定的电子银行提取和存储电子货币，降低对公众网络的依赖性，从而提高整个系统的效率和可靠性。

[1] 2000-05-30 收到， 2001-01-11 定稿
国家自然科学基金重点资助项目 (批号 69931010)

2 不可否认代理签字[2-4]

代理签字是签字者授权代理的一种方法。为了防止发生分歧，双方签字都应该是不可否认的。因此双方的签字密钥应是不同的，并且彼此应不知对方密钥。为此，设 p_0, q_0 是两个素数，G_{q_0} 是 $Z^*_{p_0}$ 的一个 q_0 阶子群。g_0 是 G_{q_0} 中的一个生成元。又设 (s_{OS}, v_{OS}) 和 (s_{PS}, v_{PS}) 分别表示原签字者和代理签字者的密钥对，则代理签字密钥为 $\sigma_p = H(m_w\|K)s_{OS} + H(m_w\|K)s_{PS} + k \bmod q_0$，其中 $s_{OS}, s_{PS} \in {}_RZ_{q_0}\backslash\{0\}$，而 $v_{OS} = g_0^{S_{OS}} \bmod p_0$, $v_{PS} = g_0^{S_{PS}} \bmod p_0$。那么对于信息 m_p 代理签字为 $(\mathrm{Sign}_{\sigma_p}(m_p), K, m_w)$ 三元组，其中 $\mathrm{Sign}_{\sigma_p}(m_p)$ 表示代理签字，$K = g_0^k \bmod p_0$，而 $k \in {}_RZ_{q_0}\backslash\{0\}$, m_w 原签字者授权证书。验证者可通过公钥 (c, v') 来对签字进行验证。其中 $c = H(m_w\|K)$, $v'_{PS} = (v_{OS} \cdot v_{PS})^c K$。

3 多级分布电子银行支付系统[5-8]

3.1 系统设置

设系统中有主银行 $\mathrm{B_M}$，代理银行 B_{Pi}，用户 U，商家 M，“中央”银行做为可信者 CT，进行分布电子银行支付系统的管理，主银行 $\mathrm{B_M}$ 指定 B_{Pi} 为其中一个代理银行，由多组 $\mathrm{B_M}$ 及 B_{Pi} 共同组成了多级分布式电子银行。“中央”银行在整个系统内选取下列参数：

(1) 选择安全参数 l；

(2) RSA 的公钥 (n, e) 和私钥 d。其中 n 的长度至少 $2l$ 位，我们要求 $n = pq$。其中 $p = 2P + 1, q = 2Q + 1$ 且 p, q, P, Q 全为素数。p, q 的选择应远大于 l 位，以确保对于模的分解不可实现；

(3) 一个 n 阶循环群 G，使得 G 中的任一元素计算离散对数是不可实现的，因此，可以选取 G 作为 Z^*_{p2} 的一个循环子群，其中 p_2 是一个素数并且 $n|(p_2 - 1)$；

(4) 一个元素 $a \in z^*_n$，其中 a 对所有 n 的素因子有大的乘法阶；

(5) 密钥长度的一个上限 λ；

(6) 每个要加入的银行都应该有与之相关的公钥设施的一部分，即每个银行都有自己的签字密钥对。设 $(s_{\mathrm{B_M}}, v_{\mathrm{B_M}})$ 和 $(s_{\mathrm{B}_{Pi}}, v_{\mathrm{B}_{Pi}})$ 分别为 $\mathrm{B_M}$ 和 B_{Pi} 签字密钥对。

该群的的公钥为 $Y = (n, e, G, g, a, \lambda)$。

3.2 代理密钥协调协议

$\mathrm{B_M}$ 选择其中一个 B_{Pi}, $\mathrm{B_M}$ 按 2 节所给出的方法与 B_{Pi} 协调代理密钥。设系统公钥设施的签字方法满足所给条件，即 $s_M, s_P \in {}_RZ_{q_0}\backslash\{0\}$，而 $v_M = g_0^{s_M} \bmod p_0$, $v_P = g_0^{s_P} \bmod p_0$。$\mathrm{B_M}$ 向 CT 注册其代理 B_{Pi} 并生成双方都不可否认的代理签字密钥对 $(s_{M,Pi}, V_{M,Pi})$，具体实现协议如图 1 所示。

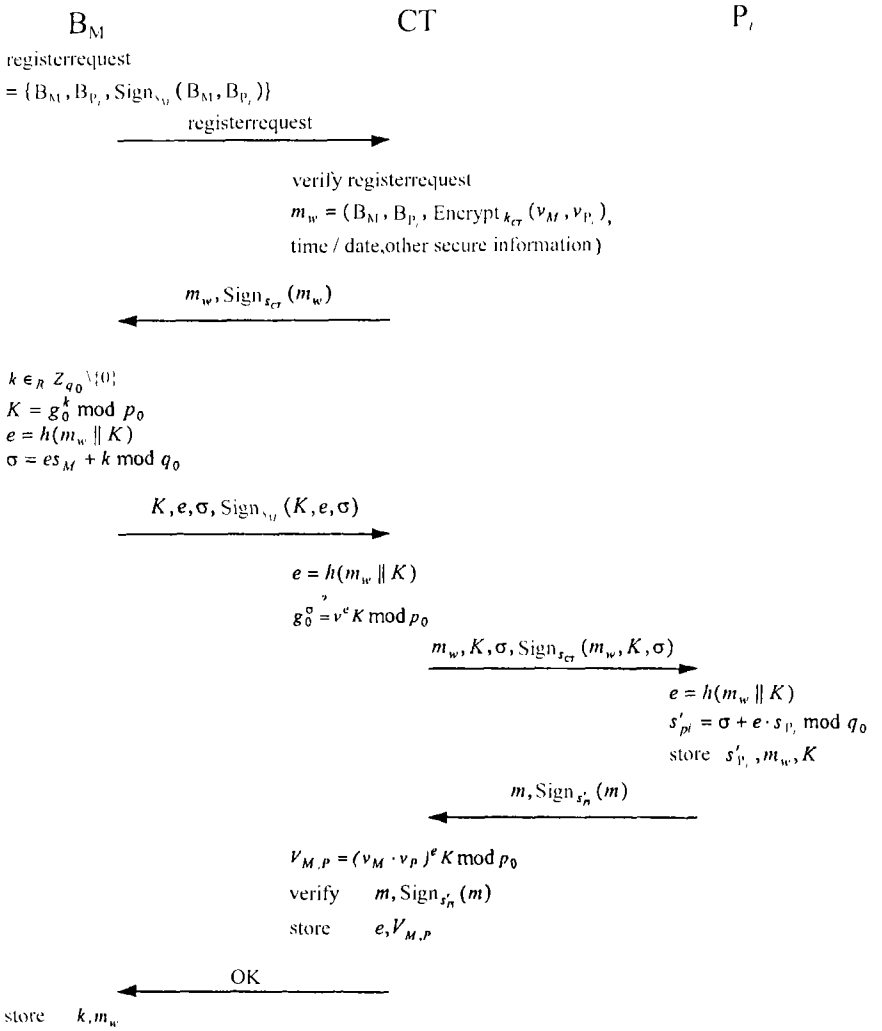

图 1 协议内容

3.3 成员注册

由“中央”银行 CT 管理着整个分布式电子银行，B_M 通过授权 B_{Pi} 后就以平等的身份向 CT 注册，B_M 用 s_M 而 B_{Pi} 用 $s_{M,Pi}$。注册时每个电子银行都作为成员在群内选择一个随机数 x 作为自己的密钥，并用该密钥作为种子密钥，通过向 CT 注册再生成成员签字密钥对 (y, z)，由 CT 签发的证书 $(y+1)^d$，其中 $y = a^x$，$z = g^y$。因此，电子银行所持的签字密钥与整个群的大小无关，用户用自己的成员签字密钥签发电子货币时，不受成员数的影响。为了防止银行间窜通，CT 要参与银行密钥的选择，并验证其生成密钥的合法性，最后用系统的公钥设施中银行签字协议担保其生成密钥的合法性，并向 CT 注册。具体注册过程如图 2 所示。

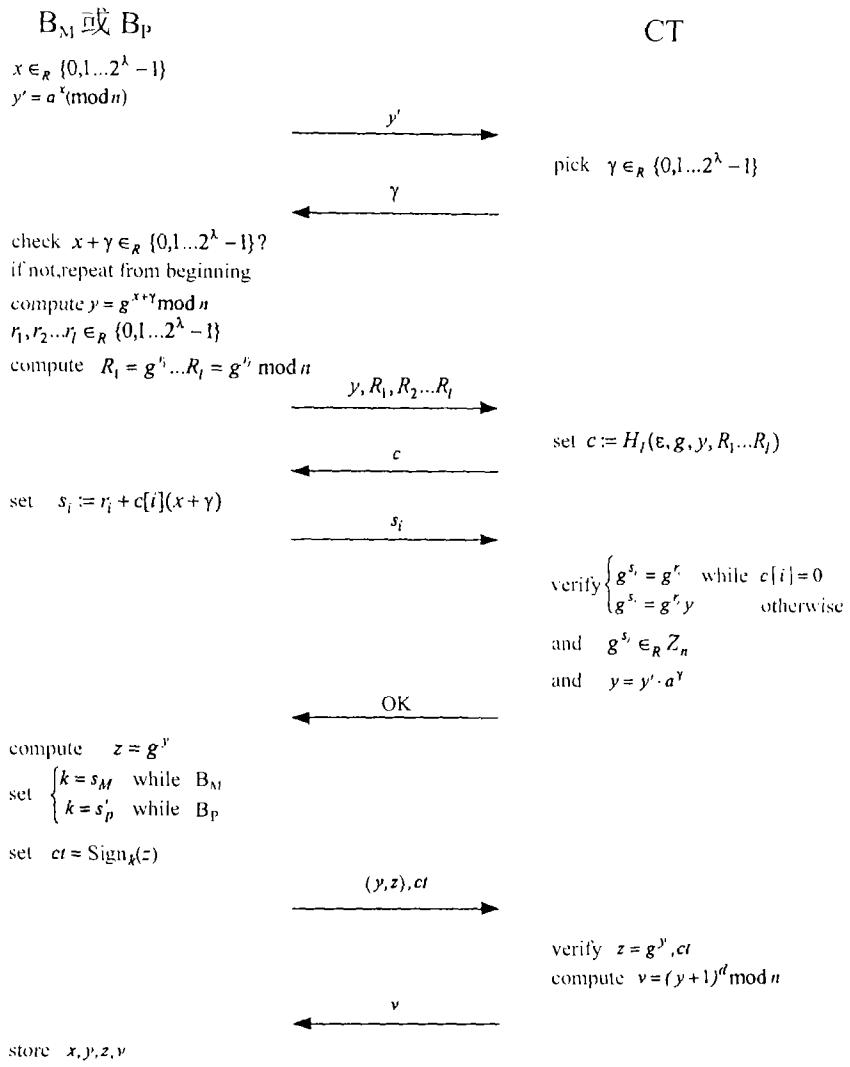

图 2　注册过程

3.4 用户开户

用户可在任何一个主电子银行设立帐户，而在代理电子银行的帐户是由其主电子银行设立的。设 $g_1, g_2 \in G$ 是 CT 公布的两个生成元，U 选择 $u_1 \in {}_R Z_n$ 作为自己的秘密，使得 $I_U = g_1^{u_1}$ 作为与用户身份相关的数。B_M 用 I_U 与 U 的帐户 $A_M = (B_M, U)$ 相关连。通过用户开户操作，B_M 把 $ZI = (I_u g_2)^y$ 交付给 U 作为用户生成电子货币的一个参数，并把用户的存款数 count′ 记入用户帐户 count_M。B_M 通过用 $I_{Pi} = g_1^{H_p(I_u, i)}$ 替换 I_u 执行相同的过程，为 U 在 B_{Pi} 帐户 $A_P = (B_P, P)$，使得 B_{Pi} 不知道 U 是谁，但其信誉由 B_M 来担保。如此重复，直到为用户在其所有代理电子银行都开设了帐户。然后在用户的 Smart Card 上存入如下数据：(1) 与用户帐户相关的用户身份 $(I_U g_2)$、ZI；(2) 分布式电子银行公布参数 g, g_1, g_2, a, e；(3) 置换函数 $\sigma : \{1 \cdots l\} \to \{1 \cdots l\}$ 及逆置换 σ^{-1}；(4) Hash 函数 $H_p(\cdot)$ 及代理电子银行标识 i；(5) 加密函数 Encrypt$(\cdot)$ 及密钥 k_u；(6) 签字函数 Sign$(\cdot)$ 及签字密钥 s_u。

3.5 提款协议

为了使提出的电子货币能够取得实际币值的支付，提款时所采用电子货币 Brands 方案的电子货币形式，即电子货币 $(A,B_1,\cdots,B_m)$ 和银行在 $(A,B_1,\cdots,B_m)$ 签字组成。其中 $A=(I_U g_2)^w$ 为盲化后的用户身份，w 是用户选取的秘密盲化数；$B_i=g_1^{y_1^i}g_2^{y_2^i}$ 是与币值相关的数，$B_1,\cdots,B_m$ 是按树型结构排列的一组值，其组合可构成从最小精度的货币到提款总值 count' 的任意面值电子货币组，从而避免了在支付中“找零”操作。而 $Y_R=y_1^1\|y_2^1\|\cdots\|y_1^m\|y_2^m$ 是一个足够长的随机数，$B=(H'(B_1),\cdots,H'(B_m))$ 表示一个确定的币值，由用户在提款时计算出的，并包含在货币的签字中，支付时每个分量可从其在货币中的顺序决定。提款时用户先向银行证明自己的身份，然后提取总值为 count' 的货币 $(A,B_1,\cdots,B_m)$，具体的提款协议如图 3 所示。

用户在代理电子银行 $\mathrm{B}_{\mathrm{P}i}$ 提款时，采用与主电子银行相同的方法，只是代理电子银行这时要保存用户提款的票据及其签字，并在以后将其交付给主电子银行，清算相互之间的帐务。

3.6 支付协议

商家首先用挑战 $d_i=H_0(A,B_i,ID_s,\mathrm{date/time})$ 获取点信息 (r_1^i,r_2^i)，其中 $r_1^i=d_iu_1w+x_1^i$，$r_2^i=d_iw+x_2^i$，然后验证 $\mathrm{Sign}(A,B_i)$ 的有效性和 $A^{d_i}B=g_1^{x_1^i}g_2^{r_2^i}$ 是否成立，并检查币值的数址，最后保存 A,B_i,d_i,r_1^i,r_2^i，从而取得第 i 块电子货币的支付。

3.7 存款协议

用户在向银行存款时，银行必须检查该电子货币是否发生重复花费。即如果用户重复花费了，就会基于不同的挑战 d_i 和 d_i' 产生在同一直线的两个点信息 (r_1,r_2) 和 (r_1',r_2')，银行通过检查已花费货币数据库查询是否已存在这样的点，如果存在，则有 $g_1^{(d_iu_1w-d_i'u_1w)/(d_iw-d_i'w)}=g_1^{u_1}=I_U$，从而确定出重复花费的用户。然后再把该电子货币以及相应签字交给 CT，执行公开协议。代理银行只能取得货币的加密形式和用户存款签字担保，实际存款在主银行执行。

3.8 公开协议

给定一个在电子货币 $(A,B_1\cdots B_m)$ 上的签字 $(\hat{g},\hat{z},a,e,c,s_1^{SKL},\cdots,s_l^{SKL},s_1^{SKR},\cdots,s_l^{SKR})$. CT 可以通过对所有的成员测试是否 $\hat{g}^y=\hat{z}$ 成立，从而确定出产生签字的银行。用该银行的成员公钥 z、以及该银行对 z 的签字和非交互式证明，即 $\log_g z=\log_{\hat{g}}\hat{z}$，而不用泄露 y。

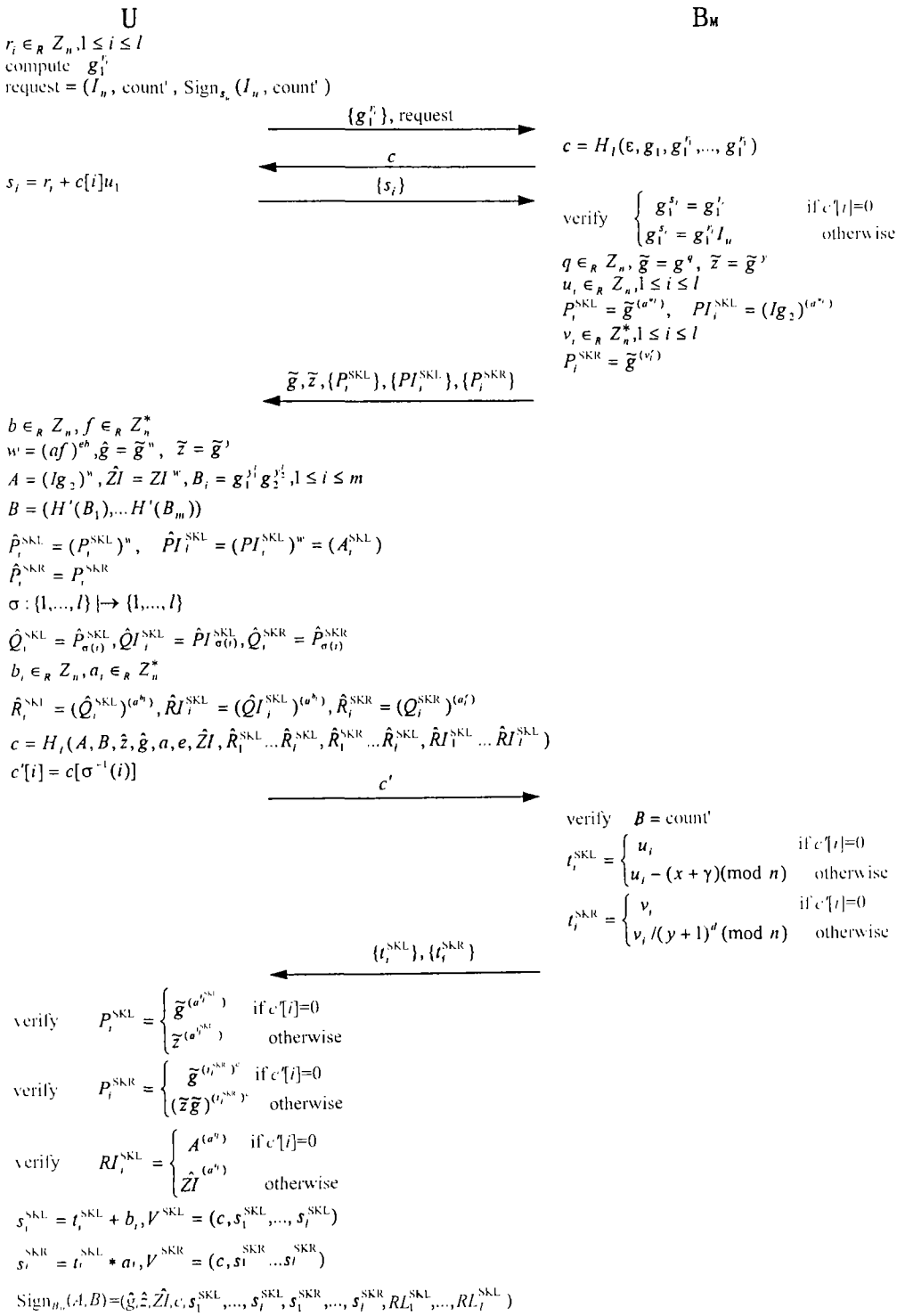
U
BM
$r_i \in_R Z_n, 1 \le i \le l$
compute $g_1^{r_i}$
request = $(I_u$, count', $\mathrm{Sign}_{s_u}(I_u$, count'$)$
$\{g_1^{r_i}\}$, request
$c = H_1(\varepsilon, g_1, g_1^{r_1}, \ldots, g_1^{r_l})$
c
$s_i = r_i + c[i]u_1$
$\{s_i\}$
verify $\begin{cases} g_1^{s_i} = g_1^{r_i} & \text{if } c'[i]=0 \\ g_1^{s_i} = g_1^{r_i} I_u & \text{otherwise} \end{cases}$
$q \in_R Z_n, \tilde{g} = g^q, \tilde{z} = \tilde{g}^y$
$u_i \in_R Z_n, 1 \le i \le l$
$P_i^{SKL} = \tilde{g}^{(a^{u_i})}$, $PI_i^{SKL} = (Ig_2)^{(a^{u_i})}$
$v_i \in_R Z_n^*, 1 \le i \le l$
$P_i^{SKR} = \tilde{g}^{(v_i)}$
$\tilde{g}, \tilde{z}, \{P_i^{SKL}\}, \{PI_i^{SKL}\}, \{P_i^{SKR}\}$
$b \in_R Z_n, f \in_R Z_n^*$
$w = (af)^{eh}, \hat{g} = \tilde{g}^w$, $\tilde{z} = \tilde{g}^y$
$A = (Ig_2)^w, \hat{ZI} = ZI^w, B_i = g_1^{s_i} g_2^{t_i}, 1 \le i \le m$
$B = (H'(B_1), \ldots H'(B_m))$
$\hat{P}_i^{SKL} = (P_i^{SKL})^w$, $\hat{PI}_i^{SKL} = (PI_i^{SKL})^w = (A_i^{SKL})$
$\hat{P}_i^{SKR} = P_i^{SKR}$
$\sigma : \{1, \ldots, l\} \mapsto \{1, \ldots, l\}$
$\hat{Q}_i^{SKL} = \hat{P}_{\sigma(i)}^{SKL}, \hat{QI}_i^{SKL} = \hat{PI}_{\sigma(i)}^{SKL}, \hat{Q}_i^{SKR} = \hat{P}_{\sigma(i)}^{SKR}$
$b_i \in_R Z_n, a_i \in_R Z_n^*$
$\hat{R}_i^{SKL} = (\hat{Q}_i^{SKL})^{(a^{b_i})}, \hat{RI}_i^{SKL} = (\hat{QI}_i^{SKL})^{(a^{b_i})}, \hat{R}_i^{SKR} = (Q_i^{SKR})^{(a_i')}$
$c = H_1(A, B, \hat{z}, \hat{g}, a, e, \hat{ZI}, \hat{R}_1^{SKL} \ldots \hat{R}_i^{SKL}, \hat{R}_1^{SKR} \ldots \hat{R}_i^{SKL}, \hat{RI}_1^{SKL} \ldots \hat{RI}_i^{SKL})$
$c'[i] = c[\sigma^{-1}(i)]$
c'
verify B = count'
$t_i^{SKL} = \begin{cases} u_i & \text{if } c'[i]=0 \\ u_i - (x+\gamma) (\mathrm{mod}\ n) & \text{otherwise} \end{cases}$
$t_i^{SKR} = \begin{cases} v_i & \text{if } c'[i]=0 \\ v_i / (y+1)^d (\mathrm{mod}\ n) & \text{otherwise} \end{cases}$
$\{t_i^{SKL}\}, \{t_i^{SKR}\}$
verify $P_i^{SKL} = \begin{cases} \tilde{g}^{(a^{t_i^{SKL}})} & \text{if } c'[i]=0 \\ \tilde{z}^{(a^{t_i^{SKL}})} & \text{otherwise} \end{cases}$
verify $P_i^{SKR} = \begin{cases} \tilde{g}^{(t_i^{SKR})^e} & \text{if } c'[i]=0 \\ (\tilde{z}\tilde{g})^{(t_i^{SKR})^e} & \text{otherwise} \end{cases}$
verify $RI_i^{SKL} = \begin{cases} A^{(a^{t_i})} & \text{if } c'[i]=0 \\ \hat{ZI}^{(a^{t_i})} & \text{otherwise} \end{cases}$
$s_1^{SKL} = t_1^{SKL} + b_1, V^{SKL} = (c, s_1^{SKL}, \ldots, s_l^{SKL})$
$s_l^{SKR} = t_l^{SKL} * a_1, V^{SKR} = (c, s1^{SKR} \ldots s_l^{SKR})$
$\mathrm{Sign}_{B_M}(A, B) = (\hat{g}, \hat{z}, \hat{ZI}, c, s_1^{SKL}, \ldots, s_l^{SKL}, s_1^{SKR}, \ldots, s_l^{SKR}, RL_1^{SKL}, \ldots, RL_l^{SKL})$

图 3　提款协议

4 安全分析

系统的安全性依赖 3 个部分的安全性：指定代理银行及代理签字的安全性；分布式电子银行所使用的盲签字的安全性；电子货币的安全性。由于采用了不可否认代理签字协议，原签字者不可伪造代理签字者，不可抵赖其签字。其安全性等价于求离散对数的难度[9]。另外，在代理签字的公钥中包含了代理者的委托证书，在其上将指明代理密钥的使用期限等说明信息，因此，不需要再使用撤消协议。

其次，分布式电子银行对电子货币所做的签字是不可伪造的和盲签字。这个结论可通过下面两个定理予以证明。

定理 1 在 3.5 节中的提款协议所生成的电子货币签字是不可伪造的。

证明 为了在电子货币产生一个有效签字，签字者一定是分布式电子银行的群成员。也就是说，$(c, s_1^{SKL}, \cdots, s_l^{SKL})$ 证明 $\hat{z} = \hat{g}^{(a^x)}$，因此有 $\hat{z}\hat{g} = \hat{g}^{(a^x+1)} = \hat{g}^{(y+1)}$，签字者知道成员密钥 x 是成立的。另一方面，$(c, s_1^{SKR} \cdots s_l^{SKR})$ 证明 $\hat{z}\hat{g} = \hat{g}^{((a^x+1)^d)^e} = \hat{g}^{(y+1)}$，签字者知道的成员密钥 $(y+1)^d$ 是成立的。只有在签字者执行了交互式协议，成为分布式电子银行的成员，取得 x 和 $(y+1)^d$ 之时。 证毕

定理 2 在 3.5 节中的提款协议所生成的电子货币签字是盲签字。即根据其签字不能确定签字者在协议中的参数。

证明 签字者利用随机盲因子 w 通过把 $\tilde{g}$ 和 $\tilde{z}$ 盲化为 $\hat{g}$ 和 $\hat{z}$ 而对输入进协议的参数进行了盲化。并且所构造的两个签字 $(c, s_1^{SKL}, \cdots, s_l^{SKL})$ 和 $(c, s_1^{SKR} \cdots s_l^{SKR})$ 也是盲签字。这些签字在有效值区间是均匀分布的，并且独立于 $\hat{g}$ 和 $\hat{z}$。电子货币上的签字与 $(c, s_1^{SKL}, \cdots, s_l^{SKL})$ 是相同参数。因此，从签字不能确定出签字者在协议中的参数。 证毕

最后可通过检验电子货币上的签字有效性来识别它，同时通过商家提供挑战来防止用户的重复花费。下面定理将证明，如果用户能正确响应商家的挑战，则用户知道其电子货币 A 和 B 相对于 (g_1, g_2) 的表示。

定理 3 如果用户在支付协议能够响应商家的挑战，那么用户知道电子货币 A 和 B 相对于 (g_1, g_2) 的表示。

证明 由于 H_0 是随机化 hash 函数，这使得如果用户不知道电子货币 A 和 B 相对于 (g_1, g_2) 的表示，那么用户接受电子货币的概率是可忽略的[9]。 证毕

由于支付协议是完整的，因此可得到如下定理。

定理 4 用户能够花费电子货币当且仅当用户知道电子货币 A 和 B 相对于 (g_1, g_2) 的表示。

证明 假设用户不知道电子货币 A 和 B 相对于 (g_1, g_2) 的表示，则由 A 和 B 的签字获得 A 和 B 的概率是可忽略的[9]，这与用户能够花费电子货币相矛盾；另外，若用户知道电子货币 A 和 B 相对于 (g_1, g_2) 的表示，则能顺利通过电子货币上的签字检验和正确响应商家的挑战，因此，能够花费电子货币。 证毕

5 结 论

电子支付系统是基于网络而发展的，网络本身的结构极其复杂。用户使用一个 Smart Card 能够在多个电子银行提款和存款可以降低对网络的依赖性。同时，现代经济社会中快速扩展其业务也要求充分利用现有的基础设施。而指定代理可以充分利用现有基础设施。同样地，代理银行也可以代替主银行签发 Smart Card。拓展多级分布式的电子银行的目的就在于增强其分布性，均衡网络结构及网络安全等因素而形成的传输瓶颈，从而达到更合理利用网络这一基础设施的目的。

参 考 文 献

[1] A. Lysyanskaya, Z. A. Ramzon, Group blind digital signature: A scalable solution to electronic cash, Proc. of 2nd Int. Conf. on Financle Crypto(FC'98), Anguilla, British West Indies, LNCS No.1465, Februray, 1998, 184-197.

[2] K. Zhang, Threshold proxy signature schees, Proc. of 1st Int. Workshop on Information Security(ISW'97), Tatsunokuchi, Ishikawa, Japan, LNCS No.1396, September, 1997, 282-290.

[3] H. Ghodsi, J. Pieprzyk, Repudiation of cheating and non-repudiation of Zhang's proxy signature schemes, Proc. of 4th Australasian Conf. on Information Security and Privacy(ACISP'99). Wollongong, NSW, Australia, LNCS No.1587, April, 1999, 129-134.

[4] M. blaze, G. Beumer, M. Strauss, Divertible protocols and atomic proxy cryptography, Advances in Cryptology, Proc. of EUROCRYPT'98, Espoo, Finland, LNCS No.1403, May31-June4, 1998. 127-144.

[5] J. Camenisch, M. Michels, A group signature with improved efficiency, Proc. of Int. Conf. on the Theory and Application of Cryptology and Information Security(ASIACRYPT'98), Springer-Verlag, LNCS No.1514, 1998, 160-174.

[6] J. Camenisch, M. Stadler, Efficient group signatures for large groups, Advances in crytology, Proc. of Crypto'97, Santa Barbara, California, USA, August 17-21, 1997, Springer-Verlag, LNCS No.1294, 1997, 410-424.

[7] S. Brands, Untraceable off-line cash in wallets with observers, Advances in crytology, Proc. Crypto' 93, Santa Barbara, California, USA, LNCS No.773, August, 1993, 302-318.

[8] M. Franklin, M. Yung, Secure and efficient off-line digital money, Proc. of 12th. Int. Colloqium on Automata, Languages and Programming(ICALP'93), Lund, Sweden, LNCS No.700, July, 1993. 265-276.

[9] 王育民，刘建伟，通信网的安全——理论与技术，西安，西安电子科技大学出版社，1999, 233-297.

A HIERARCHICALLY DISTRIBUTED BANK BASED ELECTRONIC PAYMENT SYSTEM WITH SMART CARDS

Zhao Fuxiang*,** Wang Yumin* Zhao Hongyun**

*(*The National Key Lab on ISN, Xidian University, Xi'an* 710071, China)

**(*Xi'an Institute of Telecommunication, Xi'an* 710106, China)

Abstract In electronic payment system, it is more suitable to introduce the distributed electronic bank scheme in networks environment. However, in current scheme, the users obtain their cards issued by the bank in which they have opened their accounts and withdraw and store their e-coin at the bank. Due to limits of current network neckbottle and security, dispersed and mobile users in different areas, there are some defects in a practical monadic account e-bank scheme. To solve this, a hierarchically distributed bank scheme is proposed by using an integrated method in which the group signature technique is combined with the proxy signature technique and analysis of the scheme security is given.

Key words Networks security, Electronic commerce, Electronic payment, Group signature

赵福祥：　男，1964 年生，博士生，研究方向：电子商务和网络安全.

王育民：　男，1936 年生，教授，博士生导师，研究方向：通信理论，信息论，编码和密码学.

赵红云：　女，1965 年生，讲师，硕士，研究方向：网络管理和管理信息系统.