并发安全的紧凑多重息票方案

柳 欣[1,2,3],徐秋亮[1]
(1.山东大学计算机科学与技术学院,山东济南 250101; 2.山东青年政治学院信息工程学院,山东济南 250014;
3.山东省高校信息安全与智能控制重点实验室(山东青年政治学院),山东济南 250103)

摘 要: 已有多重息票方案的弱点是缺乏支持用户根据需要选择最大兑换数量的高效协议.另一个缺陷是并不满足并发安全性.为了克服这些困难,提出两个并发安全的改进方案.第一个方案是利用关于两个被承诺值的知识证明和2轮并发零知识论证的Sigma协议编译器对底层的Blanton方案进行扩展得到的.第二个方案(即前一个方案的增强版本)利用直线提取技术实现了更为高效的安全性归约过程,并借助基于同态加密的非交互零知识论证避免了对随机预言机的使用.与其他的强不可分割的方案相比,第一个方案具有更高的通信效率,且第二个方案的安全性并不依赖于随机预言模型.

关键词: 电子现金; 多重息票; 非交互的零知识; 并发安全性; 注册公钥模型
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 05-0877-06
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.05.003

Compact Multi-Coupon Schemes with Concurrent Security

LIU Xin[1,2,3], XU Qiu-liang[1]
(1. *School of Computer Science and Technology, Shandong University, Jinan, Shandong* 250101, *China*;
2. *School of Information Engineering, Shandong Youth University of Political Science, Jinan, Shandong* 250014, *China*;
3. *Key Laboratory of Information Security and Intelligent Control in Universities of Shandong (Shandong Youth University of Political Science), Jinan, Shandong* 250103, *China*)

Abstract: The disadvantage of previous multi-coupon schemes is the lack of efficient protocol in which users can decide the maximal number of redemption according to their demands. And another deficiency is that they cannot remain secure in the concurrent case. This article remedied these obstacles by providing two improved systems with concurrent security. The first scheme was obtained by extending the underlying scheme of Blanton with the proof of two committed values and the Sigma-compiler for two round concurrent zero-knowledge argument. The second scheme (i.e., the strengthened version of the first one) achieved more efficient security reduction by incorporating the straight-line extraction paradigm and removed random oracles by using the non-interactive zero-knowledge argument from homomorphic encryption. Compared with the other strongly unsplittable schemes, the first scheme has better communicational efficiency and the second one does not rely on the random oracle model.

Key words: e-cash; multi-coupon; non-interactive zero-knowledge; concurrent security; the registered public-key model

1 引言

电子息票(e-coupon)是纸质息票的对应物,其作用是通过向顾客提供折扣或礼品来刺激销售.多重息票[1](multi-coupon)可以视为由单张电子息票构成的列表.在实际应用中,发布一张兑换次数上界为 m 的多重息票比分别发布 m 张单独的息票要高效得多.多重息票方案并不等同于电子现金方案[2,3],因为此类方案并不要求银行参与以及对恶意用户进行追踪.然而,已有的方案[1,4~6]并不理想.这表现在,文献[1,4]方案仅满足弱不可分割性[5].同时,它们要求将兑换次数上界 m 作为固定的系统参数,因此并不实用.文献[5,6]提出了能灵活地设置该上界的方案,且所得方案满足更理想的强不可分割性[5],但缺点是息票发布协议的复杂度为 $O(m)$,同时息票的存储耗费与 m 同样满足 $O(m)$的关系.值得指出的是,Canard等人[7]提出了允许对息票进

收稿日期:2010-11-29;修回日期:2011-12-22
基金项目:国家自然科学基金(No.61173139);山东省自然科学基金(No.ZR2010FM045)

行分割使用的方案,但该方案并不符合文献[1,4~6]的安全模型.总之,已有方案并未解决在发布协议中实现对兑换次数上界的灵活设置并且能有效地控制协议复杂度的问题.同时,已有方案[1,4~7]要求商家以串行方式为客户发布息票,因此在互联网应用中存在弱点.原因是串行阶段构成系统的瓶颈,致使系统在拒绝服务攻击下变得脆弱[8].考虑到商家通常是由多线程服务器实现,应当允许服务器执行与多个用户间的并发会话.此外,已有方案的底层签名方案都是基于 q-SDH(q-Strong Diffie-Hellman)假设[4]或 SRSA(Strong RSA)假设[1,5~6].然而, q-SDH 假设存在安全隐患[9],而基于 SRSA 假设的方案通信效率不高.

为此,提出两个发布协议的复杂度均为 $O(1)$且满足紧凑性质的方案(简称方案Ⅰ与Ⅱ).新方案采用了如下的设计思路:为了能使用户根据需要设置兑换次数的上界和实现高效的息票更新协议,利用关于被承诺值之间可比较关系的知识证明技术[7]对文献[10]方案做出扩展.底层方案[10]使用了 Camenisch-Lysyanskaya 签名方案[11](简称 CL 方案)的对称版本,而本文使用了非对称的版本.原因是:(1)随着 AES(Advanced Encryption Standard)类型安全性等级的广泛使用,非对称的对已经日益成为基于对的密码协议的默认实现选择[12];(2)可以进一步降低所得方案的通信耗费;(3)可以使得本文方案的息票更新协议比底层方案[10]的令牌更新过程更简单,即用户可以减少一次指数运算.在方案Ⅰ中,使用 Furukawa[13]的编译器将发布协议的底层 Sigma 协议(简记为∑协议)编译为并发安全的 2 轮知识论证.在方案Ⅱ中,利用 Damgård 等人[14]的基于同态加密的编译技术将标准的∑协议转换为非交互的零知识(Non-interactive zero-knowledge,简记为 NIZK)证明.考虑到所得证明不具有知识提取器,因此引入了 Arita[15]的直线提取技术.此外,方案Ⅱ无需借助随机预言机.

2 方案Ⅰ

系统建立 令 (G_1, G_2)为双线性群对,满足 $\hat{e}: G_1 \times G_2 \to G_T$, $|G_1| = |G_2| = |G_T| = p$, $\psi: G_2 \to G_1$,其中 p 为素数.令 $H: \{0,1\}^* \to Z_p$ 为抗碰撞的散列函数.令 $g_1, h_0, \tilde{u}$ 分别为群 G_1, G_2, G_T 的生成元,计算 $g_0 = \psi(h_0)$.假设 g_0 与 g_1 间的离散对数为未知.商家 V 选取 $\alpha, \beta, \gamma_1, \gamma_2, \gamma_3 \in_R Z_p$,设置 CL 方案的公钥 $X = h_0^{\alpha}$, $Y = h_0^{\beta}$, $Z_i = h_0^{\gamma_i}(i = 1,2,3)$.方案的公钥为 $PK = (g_0, g_1, h_0, \tilde{u}, X, Y, Z_1, Z_2, Z_3)$,私钥为 $SK = (\alpha, \beta, \gamma_1, \gamma_2, \gamma_3)$.

息票发布 用户 U 与商家 V 执行如下过程:

(1) U 向 V 申请多重息票 M 的兑换次数上界 m.

(2) U 选取 $x, s, r \in_R Z_p$,计算 Pedersen 承诺 $C = g_0^x \psi(Z_1)^s \psi(Z_2)^m \psi(Z_3)^r$,并与 V 执行 2 轮并发安全的知识论证子协议 $\Pi_1 = PK\{(x, s, r): C/\psi(Z_2)^m = g_0^x \psi(Z_1)^s \psi(Z_3)^r\}$.该协议是通过将 Furukawa[13]的编译技术应用于底层∑协议而获得的,即(**a**) V 向 U 发送 $(\bar{C}, \bar{R}, \bar{\xi}_x, \bar{\xi}_s, \bar{\xi}_r)$,具体产生过程为: V 选取 $\bar{x}, \bar{s}, \bar{r} \in_R Z_p$,计算 $\bar{C} = g_0^{\bar{x}} \psi(Z_1)^{\bar{s}} \psi(Z_2)^m \psi(Z_3)^{\bar{r}}$.选取 $\theta_x, \theta_s, \theta_r \in_R Z_p$,计算 $\bar{R} = g_0^{\theta_x} \psi(Z_1)^{\theta_s} \psi(Z_3)^{\theta_r}$.设置 $\bar{e} = H(\bar{C}, \bar{R})$,并且在 Z_p 上计算 $\bar{\xi}_x = \theta_x + \bar{e}\bar{x}$, $\bar{\xi}_s = \theta_s + \bar{e}\bar{s}$, $\bar{\xi}_r = \theta_r + \bar{e}\bar{r}$;(**b**) U 向 V 返回 $(R, e, \xi_x, \xi_s, \xi_r)$, $(\bar{R}', \bar{e}', \bar{\xi}'_x, \bar{\xi}'_s, \bar{\xi}'_r)$.具体产生过程为: U 计算 $\bar{e} = H(\bar{C}, \bar{R})$并验证是否满足 $\bar{R} = g_0^{\bar{\xi}_x} \psi(Z_1)^{\bar{\xi}_s} \psi(Z_3)^{\bar{\xi}_r} (\bar{C}/\psi(Z_2)^m)^{-\bar{e}}$.选取 $\bar{e}', \bar{\xi}'_x, \bar{\xi}'_s, \bar{\xi}'_r \in_R Z_p$,计算 $\bar{R}' = g_0^{\bar{\xi}'_x} \psi(Z_1)^{\bar{\xi}'_s} \psi(Z_3)^{\bar{\xi}'_r} (\bar{C}/\psi(Z_2)^m)^{-\bar{e}'}$.选取 $\theta_x, \theta_s, \theta_r \in_R Z_p$,计算 $R = g_0^{\theta_x} \psi(Z_1)^{\theta_s} \psi(Z_3)^{\theta_r}$.设置 $d = H(C, R, \bar{C}, \bar{R}')$,并在 Z_p 上计算 $e = d \oplus \bar{e}'$, $\xi_x = \theta_x + ex$, $\xi_s = \theta_s + es$, $\xi_r = \theta_r + er$;(**c**) V 接受 U 的证明,当且仅当, $H(C, R, \bar{C}, \bar{R}') = e \oplus \bar{e}'$, $R = g_0^{\xi_x} \psi(Z_1)^{\xi_s} \psi(Z_3)^{\xi_r} (C/\psi(Z_2)^m)^{-e}$, $\bar{R}' = g_0^{\bar{\xi}'_x} \psi(Z_1)^{\bar{\xi}'_s} \psi(Z_3)^{\bar{\xi}'_r} (\bar{C}/\psi(Z_2)^m)^{-\bar{e}'}$.

(3)若 V 接受,则选取 $d' \in_R Z_p$,计算 $a = g_0^{d'}$, $b = a^{\beta}$, $A_i = a^{\gamma_i}$, $B_i = A_i^{\beta} (i = 1,2,3)$, $c = a^{\alpha} C^{\alpha\beta d'}$,向 U 发送 $\sigma_x = (a, b, c, A_1, A_2, A_3, B_1, B_2, B_3)$.

(4) U 检查 σ_x 是否为关于元组 (x, s, m, r)的 CL 方案签名,即是否满足

$\hat{e}(a, Z_i) = \hat{e}(A_i, h_0)$, $\hat{e}(a, Y) = \hat{e}(b, h_0)$, $\hat{e}(A_i, Y) = \hat{e}(B_i, h_0)$, $\hat{e}(ab^x B_1^s B_2^m B_3^r, X) = \hat{e}(c, h_0)$, $i = 1,2,3$.若是,则设置计数器 $J = 1$,同时保存 $M = ((x, s, m, r, J), \sigma_x)$.

息票兑换 U 与 V 执行如下过程(假设满足 $J < m$):

(1) U 计算序列号 $S = \tilde{u}^{\frac{1}{s+J}}$,选取 $r_1 \in_R Z_p$,计算 $\tilde{a} = a^{r_1}$, $\tilde{b} = b^{r_1}$, $\tilde{c} = c^{r_1}$, $\tilde{A}_i = A_i^{r_1}$, $\tilde{B}_i = B_i^{r_1} (i = 1,2,3)$,向 V 提供 $x, S, \hat{e}(\tilde{b}, X)^x, \tilde{a}, \tilde{b}, \tilde{c}, \tilde{B}_1, \tilde{B}_2, \tilde{B}_3$ 以及 Π_2: $SPK\{(s, m, J, r): (\hat{e}(\tilde{a}, X)\hat{e}(\tilde{b}, X)^x)/\hat{e}(\tilde{c}, h_0) = \hat{e}(\tilde{B}_1, X)^{-s} \hat{e}(\tilde{B}_2, X)^{-m} \hat{e}(\tilde{B}_3, X)^{-r} \wedge \tilde{u} = S^J S^s \wedge 0 \leqslant J < m\}(")$.其中,有关 $0 \leqslant J < m$ 的证明要求使用 Canard 等人[7]的关于被承诺值之间可比较关系的知识证明技术.此外,为了降低证明 Π_2 的运算耗费,需要使用关于掌握部分知识的批处理技术[16];(2) V 检查知识签名 Π_2 是否有效以及是否满足: $\hat{e}(\tilde{a}, Z_i) = \hat{e}(\tilde{A}_i, h_0)$, $\hat{e}(\tilde{a}, Y) = \hat{e}(\tilde{b}, h_0)$, $\hat{e}(\tilde{A}_i, Y) = \hat{e}(\tilde{B}_i, h_0)$, $(i = 1,2,3)$. V 检查 x, S 是否未使用过.若是,则接受 U 的兑换请求,并在数据库中保存 x, S.同时, U 设置 $J = J + 1$.

息票更新 在兑换结束后, U 与 V 执行如下过程:

(1) U 选取 $\hat{x}, \hat{r} \in_R Z_p$,计算承诺 $\hat{C} = \tilde{a}^{\hat{x}} \tilde{A}_3^{\hat{r}}$,并向 V 提供 $\hat{C}$ 以及 Π_3: $SPK\{(\hat{x}, \hat{r}): \hat{C} = \tilde{a}^{\hat{x}} \tilde{A}_3^{\hat{r}}\}(")$;(2)若 Π_3 有效, V 选取 $\xi \in_R Z_p$,计算 $(\tilde{a}^{\xi}, \tilde{b}^{\xi}, (\tilde{c}\hat{C}^{\alpha\beta})^{\xi}, \tilde{A}_1^{\xi}, \tilde{A}_2^{\xi}, \tilde{A}_3^{\xi}, \tilde{B}_1^{\xi},$

$\tilde{B}_2^{\xi},\tilde{B}_3^{\xi})=(\tilde{a}',\tilde{b}',\tilde{c}',\tilde{A}'_1,\tilde{A}'_2,\tilde{A}'_3,\tilde{B}'_1,\tilde{B}'_2,\tilde{B}'_3)$,并将其提供给 U;(3) U 设置 $\tilde{x}=x+\hat{x}\bmod p$, $\tilde{r}=r+\hat{r}\bmod p$,并检查 $\sigma_{\tilde{x}}=(\tilde{a}',\tilde{b}',\tilde{c}',\tilde{A}'_1,\tilde{A}'_2,\tilde{A}'_3,\tilde{B}'_1,\tilde{B}'_2,\tilde{B}'_3)$是否为关于元组$(\tilde{x},s,m,\tilde{r})$的有效 CL 方案签名.若是,则保存 $M'=((\tilde{x},s,m,\tilde{r},J),\sigma_{\tilde{x}})$.

3　方案Ⅱ

公共参考字符串　可信功能算法 F_{CRS}^{D}选取 $e_1,d_0,d_1\in_R Z_p$, 选取 $\tilde{g}_0\in_R G_1$,计算 $\tilde{g}_1=\tilde{g}_0^{e_1},\tilde{h}_0=\tilde{g}_0^{d_0},\tilde{h}_1=\tilde{g}_1^{d_1}$,设置 $CRS=(\tilde{g}_0,\tilde{g}_1,\tilde{h}_0,\tilde{h}_1)$,删除陷门$(e_1,d_0,d_1)$.

商家的密钥注册　V 与可信功能算法 F_{reg}^{KS}执行文献[14]中的密钥建立过程,从而获得注册的公钥(pk_P,c)以及私钥(sk_P,e).其中,(pk_P,sk_P)是由 V 选取的底层 Paillier 加密方案[17]的公/私钥对,即 pk_P 为 RSA 模数 n, sk_P 为 n 的因子分解.另外,c 为关于底层∑协议的挑战 e 的 Paillier 方案密文.

用户的密钥注册　U 采用相同方式获得注册的公钥(pk_U,c_U)以及私钥(sk_U,e_U).系统建立.与方案Ⅰ的区别是在公钥中增加元素 $\tilde{g}_0,\tilde{g}_1,\tilde{h}_0,\tilde{h}_1$.

息票发布　U 与 V 执行如下过程:

(1) U 向 V 申请兑换次数上界 m. V 选取 $b_0,b_1\in_R Z_p$,计算 $\tilde{j}_0=\tilde{g}_0^{b_0},\tilde{k}_0=\tilde{h}_0^{b_0},\tilde{j}_1=\tilde{g}_1^{b_1},\tilde{k}_1=\tilde{h}_1^{b_1}$,向 U 发送 $\tilde{j}_0,\tilde{k}_0,\tilde{j}_1,\tilde{k}_1$ 及证明

$$\begin{aligned}\Pi_4=NIZK\{(b_0,b_1):\tilde{j}_0&=\tilde{g}_0^{b_0}\wedge\tilde{k}_0=\tilde{h}_0^{b_0}\wedge\tilde{j}_1\\&=\tilde{g}_1^{b_1}\wedge\tilde{k}_1=\tilde{h}_1^{b_1}\}\end{aligned}$$

(2)若 Π_4 有效,则 U 选取 $a_1,a_2\in_R Z_p$,计算 $\tilde{g}'_1=\tilde{g}_1^{a_1},\tilde{h}'_1=\tilde{h}_1^{a_2},\tilde{j}'_1=\tilde{j}_1^{a_1},\tilde{k}'_1=\tilde{k}_1^{a_2}$. U 选取 $x,s,r\in_R Z_p$,计算承诺 $C=g_0^x\psi(Z_1)^s\psi(Z_2)^m\psi(Z_3)^r$. U 选取 $r_x,r_s,r_r\in_R Z_p$,并分别计算对元素 x,s,r 的文献[15]方案承诺 $M_{i,0},M_{i,1},L_{i,0},L_{i,1}(i=0,1,2)$. U 向 V 发送$\tilde{g}'_1,\tilde{h}'_1,\tilde{j}'_1,\tilde{k}'_1,C,M_{i,0},M_{i,1},L_{i,0},L_{i,1}(i=0,1,2)$及证明

$$\begin{aligned}\Pi_5=NIZK\{(x,s,r,r_x,r_s,r_r):\\C/\psi(Z_2)^m=g_0^x\psi(Z_1)^s\psi(Z_3)^r\wedge M_{0,0}=\tilde{g}_0^x\tilde{h}_0^{r_s}\wedge M_{0,1}=\\\tilde{g}'^x_1\tilde{h}'^{r_x}_1\wedge L_{0,0}=\tilde{j}_0^x\tilde{k}_0^{r_s}\wedge L_{0,1}=\tilde{j}'^x_1\tilde{k}'^{r_s}_1\wedge M_{1,0}=\tilde{g}_0^s\tilde{h}_0^{r_s}\wedge M_{1,1}=\\\tilde{g}'^s_1\tilde{h}'^{r_s}_1\wedge L_{1,0}=\tilde{j}_0^s\tilde{k}_0^{r_s}\wedge L_{1,1}=\tilde{j}'^s_1\tilde{k}'^{r_s}_1\wedge M_{2,0}=\tilde{g}_0^r\tilde{h}_0^{r_r}\wedge M_{2,1}=\\\tilde{g}'^r_1\tilde{h}'^{r_r}_1\wedge L_{2,0}=\tilde{j}_0^r\tilde{k}_0^{r_r}\wedge L_{2,1}=\tilde{j}'^r_1\tilde{k}'^{r_r}_1\}.\end{aligned}$$

(3)若 Π_5 有效且满足 $\tilde{j}'_1=\tilde{g}'^{b_1}_1,\tilde{k}'_1=\tilde{h}'^{b_1}_1$,则 V 选取 $d'\in_R Z_p$,计算 $a=g_0^{d'},b=a^{\beta},A_i=a^{\gamma_i},B_i=A_i^{\beta}(i=1,2,3),c=a^{\alpha}C^{\alpha\beta d'}$,向 U 发送 $\sigma_x=(a,b,c,A_1,A_2,A_3,B_1,B_2,B_3)$.

(4) U 检查 σ_x 是否为关于元组(x,s,m,r)的 CL 方案签名.若是,则设置计数器 $J=1$,并且保存 $M=((x,s,m,r,J),\sigma_x)$.

息票兑换　U 与 V 执行如下过程:

(1) V 选取 $b'_0,b'_1\in_R Z_p$,计算 $\tilde{j}'_0=\tilde{g}_0^{b'_0},\tilde{k}'_0=\tilde{h}_0^{b'_0},\tilde{j}'_1=\tilde{g}_1^{b'_1},\tilde{k}'_1=\tilde{h}_1^{b'_1}$,向 U 发送$\tilde{j}'_0,\tilde{k}'_0,\tilde{j}'_1,\tilde{k}'_1$ 以及证明

$$\Pi_6=NIZK\{(b'_0,b'_1):\tilde{j}'_0=\tilde{g}_0^{b'_0}\wedge\tilde{k}'_0=\tilde{h}_0^{b'_0}\wedge\tilde{j}'_1=\tilde{g}_1^{b'_1}\wedge\tilde{k}'_1=\tilde{h}_1^{b'_1}\}.$$

(2)若 Π_6 有效,则 U 计算序列号 $S=\tilde{u}^{\frac{1}{s+J}}$,选取 $r_1\in_R Z_p$,计算 $\tilde{a}=a^{r_1},\tilde{b}=b^{r_1},\tilde{c}=c^{r_1},\tilde{A}_i=A_i^{r_1},\tilde{B}_i=B_i^{r_1}(i=1,2,3)$. U 选取 $a'_1,a'_2\in_R Z_p$,计算 $\tilde{g}''_1=\tilde{g}_1'^{a'_1},\tilde{h}''_1=\tilde{h}_1'^{a'_2},\tilde{j}''_1=\tilde{j}'^{a'_1}_1,\tilde{k}''_1=\tilde{k}'^{a'_2}_1$. U 选取 $r_s,r_m,r_r\in_R Z_p$,分别计算对元素 s,m,r 的文献[15]方案承诺,即 $M'_{i,0},M'_{i,1},L'_{i,0},L'_{i,1}(i=0,1,2)$.

(3) U 向 V 提供 $x,S,\hat{e}(\tilde{b},X)^x,\tilde{a},\tilde{b},\tilde{c},\tilde{B}_1,\tilde{B}_2,\tilde{B}_3,\tilde{g}''_1,\tilde{h}''_1,\tilde{j}''_1,\tilde{k}''_1-M'_{i,0},M'_{i,1},L'_{i,0},L'_{i,1}(i=0,1,2)$以及证明

$$\begin{aligned}\Pi_7:&NIZK\{(s,m,r,J,r_s,r_m,r_r):\\&(\hat{e}(\tilde{a},X)\hat{e}(\tilde{b},X)^x)/\hat{e}(\tilde{c},h_0)\\&=\hat{e}(\tilde{B}_1,X)^{-s}\hat{e}(\tilde{B}_2,X)^{-m}\hat{e}(\tilde{B}_3,X)^{-r}\wedge\tilde{u}\\&=S^JS^s\wedge M'_{0,0}=\tilde{g}_0^s\tilde{h}_0^{r_s}\wedge M'_{0,1}\\&=\tilde{g}''^s_1\tilde{h}''^{r_s}_1\wedge L'_{0,0}=\tilde{j}'^s_0\tilde{k}'^{r_s}_0\wedge L'_{0,1}\\&=\tilde{j}''^s_1\tilde{h}''^{r_r}_1\wedge M'_{1,0}=\tilde{g}_0^m\tilde{h}_0^{r_m}\wedge M'_{1,1}\\&=\tilde{g}''^m_1\tilde{h}''^{r_m}_1\wedge L'_{1,0}=\tilde{j}'^m_0\tilde{k}'^{r_m}_0\wedge L'_{1,1}\\&=\tilde{j}''^m_1\tilde{k}''^{r_m}_1\wedge M'_{2,0}=\tilde{g}_0^r\tilde{h}_0^{r_r}\wedge M'_{2,1}\\&=\tilde{g}''^r_1\tilde{h}''^{r_r}_1\wedge L'_{2,0}=\tilde{j}'^r_0\tilde{k}'^{r_r}_0\wedge L'_{2,1}\\&=\tilde{j}''^r_1\tilde{k}''^{r_r}_1\wedge 0\leqslant J<m\}.\end{aligned}$$

(4) V 检查 Π_7 的有效性以及是否满足:$\tilde{j}''_1=\tilde{g}''^{b'_1}_1,\tilde{k}''_1=\tilde{h}''^{b'_1}_1,\hat{e}(\tilde{a},Z_i)=\hat{e}(\tilde{A}_i,h_0),\hat{e}(\tilde{a},Y)=\hat{e}(\tilde{b},h_0),\hat{e}(\tilde{A}_i,Y)=\hat{e}(\tilde{B}_i,h_0),(i=1,2,3)$. V 检查 x,S 是否未使用过.若是,则接受 U 的兑换请求,并保存 x,S.同时, U 设置 $J=J+1$.

息票更新　与方案Ⅰ的区别是,需要将知识签名 Π_3 替换为证明 $\Pi_8:NIZK\{(\hat{x},\hat{r}):\hat{C}=\tilde{a}^{\hat{x}}\tilde{A}_3^{\hat{r}}\}$.

4　NIZK 证明的编译过程

方案Ⅱ中的 *NIZK* 证明 $\Pi_4,\cdots,\Pi_8$ 是利用 Damgård 等人[14]的技术对底层∑协议(分别记为 $\Phi_4,\cdots,\Phi_8$)进行编译而得到的.限于篇幅,本节仅提供证明 Π_5 的编译过程.

4.1　底层 Σ 协议构造过程

(1) U 选取 $\theta_x,\theta_s,\theta_r,\theta_{r_x},\theta_{r_s},\theta_{r_r}\in_R Z_p$,计算

$R_1=g^{\theta_x}\psi(Z_1)^{\theta_s}\psi(Z_3)^{\theta_r}$, $R_2=\tilde{g}_0^{\theta_x}\tilde{h}_0^{r_{\theta_x}}$, $R_3=\tilde{g}'^{\theta_s}_1\tilde{h}'^{\theta_{r_x}}_1$, $R_4=\tilde{j}_0^{\theta_x}\tilde{k}_0^{\theta_{r_x}}$, $R_5=\tilde{j}'^{\theta_s}_1\tilde{k}'^{\theta_{r_x}}_1$, $R_6=\tilde{g}_0^{\theta_r}\tilde{h}_0^{\theta_{r_x}}$, $R_7=\tilde{g}'^{\theta_r}_1\tilde{h}'^{\theta_{r_x}}_1$, $R_8=\tilde{j}_0^{\theta_r}\tilde{k}_0^{\theta_{r_x}}$, $R_9=\tilde{j}'^{\theta_r}_1\tilde{k}'^{\theta_{r_x}}_1$, $R_{10}=\tilde{g}_0^{\theta_s}\tilde{h}_0^{\theta_{r_x}}$, $R_{11}=\tilde{g}'^{\theta_s}_1\tilde{h}'^{\theta_{r_r}}_1$, $R_{12}=\tilde{j}_0^{\theta_s}\tilde{k}_0^{\theta_{r_r}}$, $R_{13}=\tilde{j}'^{\theta_s}_1\tilde{k}'^{\theta_{r_r}}_1$,向 V 发送$(R_1,\cdots,R_{13})$.

(2) V 返回挑战 $e\in {}_R Z_p$.

(3) U 在 Z_p 上计算 $\xi_x=\theta_x+ex$, $\xi_s=\theta_s+es$, $\xi_r=\theta_r+er$, $\xi_{r_x}=\theta_{r_x}+er_x$, $\xi_{r_s}=\theta_{r_s}+er_s$, $\xi_{r_r}=\theta_{r_r}+er_r$,并向 V 发送 $(\xi_x,\xi_s,\xi_r,\xi_{r_x},\xi_{r_s},\xi_{r_r})$. V 验证是否满足

$R_1=h_0^{\xi}\psi(Z_1)^{\xi_s}\psi(Z_3)^{\xi_r}(C/\psi(Z_2)^m)^{-e}$, $R_2=\tilde{g}_0^{\xi}\tilde{h}_0^{\xi_{r_r}}M_{0,0}^{-e}$,

$R_3=\tilde{g}'^{\xi}_1\tilde{h}'^{\xi_{r_x}}_1 M_{1,0}^{-e}$, $R_4=\tilde{j}'^{\xi}_0\tilde{k}^{\xi_{r_x}}_0 L_{0,0}^{-e}$, $R_5=\tilde{j}'^{\xi}_1\tilde{k}'^{\xi_{r_x}}_1 L_{0,1}^{-e}$,

$R_6=\tilde{g}_0^{\xi}\tilde{h}_0^{\xi_{r_s}}M_{1,0}^{-e}$, $R_7=\tilde{g}'^{\xi}_1\tilde{h}'^{\xi_{r_s}}_1 M_{1,1}^{-e}$, $R_8=\tilde{j}_0^{\xi}\tilde{k}_0^{\xi_{r_s}}L_{1,0}^{-e}$,

$R_9=\tilde{j}'^{\xi}_1\tilde{k}'^{\xi_{r_s}}_1 L_{1,1}^{-e}$, $R_{10}=\tilde{g}_0^{\xi}\tilde{h}_0^{\xi_{r_r}}M_{2,0}^{-e}$, $R_{11}=\tilde{g}'^{\xi}_1\tilde{h}'^{\xi_{r_r}}_1 M_{2,1}^{-e}$,

$R_{12}=\tilde{j}_0^{\xi}\tilde{k}_0^{\xi_{r_r}}L_{2,1}^{-e}$, $R_{13}=\tilde{j}'^{\xi}_1\tilde{k}'^{\xi_{r_r}}_1 L_{2,2}^{-e}$.

4.2 将底层 Σ 协议编译为 NIZK 证明

(1) U 根据 F_{reg}^{KS} 获得 V 的注册公钥 (pk_P,c),并根据底层协议 Φ_5 计算 $R=(R_1,\cdots,R_{13})$. 计算

$c_{\xi_x}=randomize(E_{pk_P}(\theta_x)\cdot c^x)$, $c_{\xi_s}=randomize(E_{pk_P}(\theta_s)\cdot c^s)$,

$c_{\xi_r}=randomize(E_{pk_P}(\theta_r)\cdot c^r)$, $c_{\xi_{r_x}}=randomize(E_{pk_P}(\theta_{r_x})\cdot c^{r_x})$,

$c_{\xi_{r_s}}=randomize(E_{pk_P}(\theta_{r_s})\cdot c^{r_s})$, $c_{\xi_{r_r}}=randomize(E_{pk_P}(\theta_{r_r})\cdot c^{r_r})$.

(符号 $E_{pk_P}(m)$ 表示在公钥 pk_P 下对消息 m 执行 Paillier 加密, $randomize(m)$ 表示计算 Paillier 密文的乘积 $E_{pk_P}(m)\cdot E_{pk_P}(0)$)并且向 V 发送 $\Pi_5=(R_1,\cdots,R_{13},(c_{\xi_x},c_{\xi_s},c_{\xi_r},c_{\xi_{r_x}},c_{\xi_{r_s}},c_{\xi_{r_r}}))$.

(2) V 利用私钥 sk_P 解密 $(c_{\xi_x},c_{\xi_s},c_{\xi_r},c_{\xi_{r_x}},c_{\xi_{r_s}},c_{\xi_{r_r}})$,获得 $(\xi_x,\xi_s,\xi_r,\xi_{r_x},\xi_{r_s},\xi_{r_r})$. 然后,执行底层协议 Φ_5 的验证过程.

5 方案的安全性分析

在文献[14]中,Damgård 等人引入了一个基于复杂度的假设(简称 DFN 假设,即 Damgård-Fazio-Nicolosi). 该假设表明,给定能在 $T(k)$ 时间内求解模数长度为 k 的离散对数问题的算法 **A**,则并不存在能在 $O(T(k)+poly(k))$ 时间内攻破模数长度为 $2k$ 的 Paillier 加密方案的算法 **B**. 此后,Kristian 等人[18]将该假设推广到素数阶双线性群上. 采用文献[4,10,15,19]中的技术,可以得出以下结论.

定理 1 随机预言模型下,若 DBDHI(Decisional Bilinear Diffie-Hellman Inversion)假设[4]、XDDH(External Decisional Diffie-Hellman)假设[19]、LRSW(Lysyanskaya-Rivest-Sahai-Wolf)假设[11]和离散对数假设成立,则方案Ⅰ满足正确性、无关联性、不可伪造性和强不可分割性.

定理 2 在注册公钥模型[14]下,若 DFN 假设[14]、KEA1(Knowledge of Exponent Assumption 1)假设[15]、DBDHI 假设[4]、XDDH 假设[19]、LRSW 假设[11]和离散对数假设成立,则方案Ⅱ满足正确性、无关联性、不可伪造性和强不可分割性.

正确性. 限于篇幅,仅证明息票更新协议是正确的. 在更新之前, U 拥有有效签名 $(\tilde{a},\tilde{b},\tilde{c},\tilde{A}_1,\tilde{A}_2,\tilde{A}_3,\tilde{B}_1,\tilde{B}_2,\tilde{B}_3)$,这是对其在发布阶段所获签名 σ_x 的随机化处理结果,即是关于秘密元组 (x,s,m,r) 的有效 CL 方案签名. 在更新阶段, V 向 U 提供 $\sigma_{\tilde{x}}=(\tilde{a}',\tilde{b}',\tilde{c}',\tilde{A}'_1,\tilde{A}'_2,\tilde{A}'_3,\tilde{B}'_1,\tilde{B}'_2,\tilde{B}'_3)=(\tilde{a}^{\xi},\tilde{b}^{\xi},(\tilde{c}\hat{C}^{\alpha\beta})^{\xi},\tilde{A}^{\xi}_1,\tilde{A}^{\xi}_2,\tilde{A}^{\xi}_3,\tilde{B}^{\xi}_1,\tilde{B}^{\xi}_2,\tilde{B}^{\xi}_3)$,其中

$\tilde{c}'=(\tilde{c}\hat{C}^{\alpha\beta})^{\xi}=((a^{\alpha+\alpha\beta(x+s\gamma_1+m\gamma_2+r\gamma_3)})^{r_1}((\tilde{a}^{\hat{x}+\hat{r}\gamma_3}))^{\alpha\beta})^{\xi}$

$=(\tilde{a}^{\alpha+\alpha\beta[(x+\hat{x})+s\gamma_1+m\gamma_2+(r+\hat{r})\gamma_3]})^{\xi}$.

容易验证 $\sigma_{\tilde{x}}=(\tilde{a}',\tilde{b}',\tilde{c}',\tilde{A}'_1,\tilde{A}'_2,\tilde{A}'_3,\tilde{B}'_1,\tilde{B}'_2,\tilde{B}'_3)$ 是关于秘密元组 $(\tilde{x},s,m,\tilde{r})$ 的有效 CL 方案签名,其中 $\tilde{x}=x+\hat{x}\bmod p$, $\tilde{r}=r+\hat{r}\bmod p$.

无关联性. 定义归约算法 **B**,该算法的运行过程分为以下两个模式:

模式 1 **B** 以参数 $(p,G_1,G_2,G_T,\psi,\hat{e})$ 和元组 $\theta=(\bar{g}_0,\bar{h}_0,\bar{h}_0^{\gamma},\cdots,\bar{h}_0^{\gamma^q},\Theta)$ 为输入,其中 $\theta\in {}_R S_0,S_1$,且 $S_0=\{(\bar{g}_0,\bar{h}_0,\bar{h}_0^{\gamma},\cdots,\bar{h}_0^{\gamma^q},\hat{e}(\bar{g}_0,\bar{h}_0)^{1/\gamma}\mid\gamma\in {}_R Z_p^*\}$, $S_1=\{(\bar{g}_0,\bar{h}_0,\bar{h}_0^{\gamma},\cdots,\bar{h}_0^{\gamma^q},\Lambda\mid\gamma\in {}_R Z_p^*,\Lambda\in {}_R G_T^*\}$. **B** 选取 $b\in {}_R\{0,1\}$,设置 $b'=\{0,1\}/b$, $J_i=i(i=1,\cdots,m-1,m<q)$, $s_b=\gamma-J_{m-1}$,设置 $F=s_b\Pi_{i=1}^{m-2}(s_b+J_i)=\Sigma_{i=0}^{m-1}A_i\gamma^i$, $\tilde{u}=\hat{e}(\bar{g}_0,\bar{h}_0)^F$. **B** 定义集合 $H_b=\{\tilde{u}^{\frac{1}{s_b+J_1}},\cdots,\tilde{u}^{\frac{1}{s_b+J_{m-2}}}\}$,设置 $\bar{\Theta}=\hat{e}(\bar{g}_0,\bar{h}_0)^{\Sigma_{i=1}^{m-1}A_i\gamma^{i-1}}\Lambda^{A_0}$. 选取 $s_{b'}\in {}_R Z_p^*$,定义集合 $H_{b'}=\{\tilde{u}^{\frac{1}{s_{b'}+J_1}},\cdots,\tilde{u}^{\frac{1}{s_{b'}+J_{m-1}}}\}$. **B** 产生剩余的系统参数,并与敌手 **A** 执行无关联性游戏[4]. 在游戏中, **B** 为 **A** 提供以下的预言服务: $O_{Issue}('user')$ 询问. 若 $user=U_b$,则 **B** 向 **A** 申请兑换次数上界 m_b,并验证 Π_4 的有效性. 若是,则选取 $C\in {}_R G_1$,并且向 **A** 发送 $C,\tilde{g}'_1,\tilde{h}'_1,\tilde{j}'_1,\tilde{k}'_1,M_{i,0},M_{i,1},L_{i,0},L_{i,1}(i=0,1,2)$, Π_5. (Π_5 模拟过程为:选取 $a_1,a_2\in {}_R Z_p$,计算 $\tilde{g}'_1=\tilde{g}_1^{a_1}$, $\tilde{h}'_1=\tilde{h}_1^{a_2}$, $\tilde{j}'_1=\tilde{j}_1^{a_1}$, $\tilde{k}'_1=\tilde{k}_1^{a_2}$. 选取 $C,M_{i,0},M_{i,1},L_{i,0},L_{i,1}(i=0,1,2)\in {}_R G_1$. 选取 $\xi_x,\xi_s,\xi_r,\xi_{r_x},\xi_{r_s},\xi_{r_r}\in {}_R Z_p$,根据底层 Σ 协议的验证等式计算 $R_1,\cdots,R_{13}$. 计算 $c_{\xi_x}=randomize(\xi_x)$, $c_{\xi_s}=randomize(\xi_s)$, $\cdots$, $c_{\xi_{r_r}}=randomize(\xi_{r_r})$. 设置 $\Pi_5=(R_1,\cdots,R_{13},(c_{\xi_{r_x}},c_{\xi_{r_s}},c_{\xi_r},c_{\xi_{r_x}},c_{\xi_{r_s}},c_{\xi_{r_r}}))$.)在获得 **A** 返回的 CL 方案签名 $\sigma_{b,x}$ 后, **B** 设置 $M_b=((x_b,s_b,m_b,r_b,J),\sigma_{b,x})$,其中 (x_b,s_b,r_b) 是未知的. 若 $user=U_{b'}$,则 **B** 向 **A** 申请兑换次数上界 $m_{b'}$,选取 $x_{b'},s_{b'},r_{b'}\in {}_R Z_p$,计算 $C=g_0^{x_{b'}}\psi(Z_1)^{s_{b'}}\psi(Z_2)^{m_{b'}}\psi(Z_3)^{r_{b'}}$,以诚实方式与 **A** 完成剩余协议,并获得 $M_{b'}=((x_{b'},s_{b'},m_{b'},r_{b'},J),\sigma_{b',x})$.

$O_{Redeem}('user')$询问.若 $user = U_b$,则 **B** 在 H_b 中选取未使用的元素 $S = \tilde{u}_{s_b+J}^{\frac{1}{}}$,将 $\sigma_{b,x}$随机化为 $\tilde{\sigma}_{b,x}$,并且在 S,$\tilde{\sigma}_{b,x}$的基础上与 **A** 完成兑换协议,其中证明 Π_7 是模拟产生的.然后,**B** 以诚实方式与 **A** 完成更新协议.若 $user = U_{b'}$,则 **B** 在集合 $H_{b'}$中选取未使用的元素,并以诚实方式与 **A** 完成兑换和更新协议.

$Ch(\cdot)$询问.**B** 设置 $S = \bar{\Theta}$,并为 **A** 提供基于 S 产生的模拟证明 Π_7.最后,**A** 返回猜测值 b^*.若 $b = b^*$,则 **B** 判定 $\theta \in S_0$;否则,判定 $\theta \in S_1$.

模式 2　**B** 以参数$(p, G_1, G_2, G_T, \psi, \hat{e})$和给定的 DDH(Decisional Diffie-Hellman)问题实例$(\bar{g}_0, \bar{g}_1, \bar{g}_2, \bar{g}_3) = (g_0, g_0^{\mu}, g_0^{\nu}, g_0^{\omega}) \in G_1^4$ 为输入,满足 $g_0 = \psi(h_0)$.**B** 产生剩余的系统参数并与 **A** 共同执行无关联性游戏[4].在游戏开始前,**B** 选取 $b \in_R \{0,1\}$,设置 $b' = \{0,1\}/b$.

$O_{Issue}('user')$询问.若 $user = U_b$,则 **B** 向申请 **A** 兑换次数上界 m_b,选取 $\tau \in_R Z_p$,设置 $C = \bar{g}_1^{\tau} = g_0^{\mu\tau}$.**B** 向 **A** 发送 $C, \tilde{g}'_1, \tilde{h}'_1, \tilde{j}'_1, \tilde{k}'_1, M_{i,0}, M_{i,1}, L_{i,0}, L_{i,1}(i = 0,1,2)$以及模拟的证明 Π_5.在获得 **A** 返回的签名 $\sigma_{b,x}$后,**B** 设置 $M_b = ((x_b, s_b, m_b, r_b, J), \sigma_{b,x})$,其中$(x_b, s_b, r_b)$是未知的.满足 $\sigma_{b,x} = (g_0^{d'}, (g_0^{d'})^{\beta}, (g_0^{d'})^{\alpha+\alpha\beta\mu\tau}, (g_0^{d'})^{\gamma_1}, (g_0^{d'})^{\gamma_2}, (g_0^{d'})^{\gamma_3}, (g_0^{d'})^{\gamma_1\beta}, (g_0^{d'})^{\gamma_2\beta}, (g_0^{d'})^{\gamma_3\beta})$.若 $user = U_{b'}$,则 **B** 以诚实方式与 **A** 执行发布协议,从而获得 $M_{b'} = ((x_{b'}, s_{b'}, m_{b'}, r_{b'}, J), \sigma_{b',x})$.

$O_{Redeem}('user')$询问.若 $user = U_b$,则 **B** 将 $\sigma_{b,x}$随机化为 $\tilde{\sigma}_{b,x}$,并且在 $\tilde{\sigma}_{b,x}$的基础上与 **A** 执行兑换协议,其中证明 Π_7 是模拟产生的.然后,**B** 以诚实方式与 **A** 完成更新协议.若 $user = U_{b'}$,则 **B** 将 $\sigma_{b',x}$随机化为$\tilde{\sigma}_{b',x}$并以诚实方式与 **A** 完成兑换和更新协议.

$Ch(\cdot)$询问.**B** 设置 $\tilde{a} = \bar{g}_2 = g_0^{\nu}, \tilde{b} = \bar{g}_2^{\beta} = (g_0^{\nu})^{\beta}, \tilde{c} = \bar{g}_2^{\alpha}\bar{g}_3^{\alpha\beta\tau} = (g_0^{\nu})^{\alpha}(g_0^{\omega})^{\alpha\beta\tau}, \tilde{A}_i = \tilde{a}^{\gamma_i}, \tilde{B}_i = \tilde{A}_i^{\beta}(i = 1,2,3)$.**B** 为 A 提供基于$(\tilde{a}, \tilde{b}, \tilde{c}, \tilde{A}_1, \tilde{A}_2, \tilde{A}_3, \tilde{B}_1, \tilde{B}_2, \tilde{B}_3)$产生的模拟证明 Π_7.最后,A 返回猜测值 b^*.若 $b = b^*$,则 **B** 判定$(\bar{g}_0, \bar{g}_1, \bar{g}_2, \bar{g}_3)$为 *DDH* 元组;否则,判定$(\bar{g}_0, \bar{g}_1, \bar{g}_2, \bar{g}_3)$并非 *DDH* 元组.显然,若 **A** 能以不可忽略的概率获胜,则 **B** 将攻破 DBDHI 或 XDDH 假设.

不可伪造性.定义归约算法 **B**,该算法以参数$(p, G_1, G_2, G_T, \psi, \hat{e})$和 CL 方案公钥$(X, Y, Z_1, Z_2, Z_3)$为输入.**B** 产生剩余的系统参数,并与敌手 **A** 执行不可伪造性游戏[4].在游戏中,**B** 为 **A** 提供以下的预言服务:

$O_{Issue}('vendor')$询问.**A** 与 **B** 并发地执行发布协议的多个实例.在其中的任意一个实例中,**B** 向 **A** 提供 $\tilde{j}_0, \tilde{k}_0, \tilde{j}_1, \tilde{k}_1$ 及证明 Π_4.然后,**A** 返回 $\tilde{g}'_1, \tilde{h}_1', \tilde{j}'_1, \tilde{k}'_1, C, M_{i,0}, M_{i,1}, L_{i,0}, L_{i,1}(i = 0,1,2)$及证明 Π_5.此时,**B** 借助 KEA1 提取器[15]从 Π_5 中提取出秘密证据(x, s, r).最后,**B** 借助 CL 方案的签名预言机 $O_{CL}(\cdot)$为 **A** 提供签名 σ_x,同时保存 $M = ((x, s, m, r, J), \sigma_x)$.

$O_{Redeem}('vendor')$询问.**B** 与 **A** 共同执行兑换和更新协议,并借助 KEA1 提取器从证明 Π_7 中提取出秘密证据(s, m, r).最终,若 **A** 能以不可忽略的概率获胜,则 **B** 能获得秘密证据(s^*, m^*, r^*)以及对元组(x^*, s^*, m^*, r^*)的有效签名$(\tilde{a}^*, \tilde{b}^*, (\tilde{c}^*), \tilde{A}_1^*, \tilde{A}_2^*, \tilde{A}_3^*, \tilde{B}_1^*, \tilde{B}_2^*, \tilde{B}_3^*)$.此时分为两种情况:

情况 1　**B** 此前并未向预言机 $O_{CL}(\cdot)$提出询问(x^*, s^*, m^*, r^*).表明$(\tilde{a}^*, \tilde{b}^*, (\tilde{c}^*), \tilde{A}_1^*, \tilde{A}_2^*, \tilde{A}_3^*, \tilde{B}_1^*, \tilde{B}_2^*, \tilde{B}_3^*)$是由 **A** 产生的有效伪造签名,从而违背了 CL 方案的不可伪造性,即得出与底层 LRSW 假设的矛盾.

情况 2　**B** 此前曾经向预言机 $O_{CL}(\cdot)$提出询问(x^*, s^*, m^*, r^*).这表明 **A** 在伪造证明 Π_7 的过程中使用了利用 s^* 与 J^*(满足 $J^* \geqslant m^*$)构造的非法序列号 S^*,从而违背了底层知识证明协议[7]的可靠性,即得出与底层离散对数假设的矛盾.

强不可分割性.方案Ⅱ显然满足强不可分割性[5],因为若 U 与他人共享使用自己的息票 M,则此后将无法利用 M 进行兑换,否则将必须面对伪造 CL 签名的困难性.

6　方案的性能分析

我们在表 1~2 中对本文方案与两个满足强不可分割性的方案[5,6]进行了通信耗费(单位为比特)以及运算耗费(即乘法次数)的对比.对于文献[5,6]方案,选取其底层签名方案(即 CL 方案的 RSA 群版本)的模数为 1024 比特,消息长度为 160 比特,商家在签名过程中选取的随机素数和随机数分别为 160 与 1344 比特.对于本文方案,选取群 G_1, G_2, G_T 的阶数为 170 比特,这些群上元素的长度分别为 171,1020 与 1020 比特.选取抗

表 1　通信耗费比较(*U* 表示用户,*V* 表示商家)

方案	发布协议(*U*)	发布协议(*V*)	兑换协议(*U*)	兑换协议(*V*)
[5]	166400	129088	26912	2528
[6]	161408	129088	33888	2528
本文方案Ⅰ	1873	852	18048	1539
本文方案Ⅱ	29706	11099	336229	11099

表 2　运算耗费比较(*U* 表示用户,*V* 表示商家)

方案	发布协议(*U*)	发布协议(*V*)	兑换协议(*U*)	兑换协议(*V*)
[5]	360896	380896	40900	39188
[6]	435664	283072	53120	48400
本文方案Ⅰ	63905	4335	82644	78649
本文方案Ⅱ	107715	37674	439795	339380

碰撞散列函数的输出为 170 比特.选取底层 Paillier 方案的模数长度为 2048 比特[14,18].在表 2 的比较过程中,将所涉及的 RSA 群上的长指数运算耗费,群 G_1, G_2, G_T 上的短指数运算耗费和对运算耗费都近似地等价为模乘次数,具体方法可以参考文献[20,21].最后,取兑换次数上界为 50.

7 结语

提出两个支持紧凑存储的多重息票方案,新方案不仅克服了已有方案要求将兑换次数上界作为系统的固定参数或者发布协议的复杂度与该上界满足线性关系的弱点,而且满足强不可分割性和并发安全性.新方案因避免使用 q-SDH 假设而满足更强的安全性,其中方案Ⅰ在通信效率上优于基于 SRSA 假设的方案,且方案Ⅱ在设计方法上摆脱了随机预言机.

参考文献

[1] Chen L, Enzmann M, Sadeghi A -R, et al. A privacy-protecting coupon system [A]. Proceedings of Financial Cryptography 2005[C]. Berlin: Springer-Verlag, 2005. 93 – 109.

[2] 刘文远,张江霄,胡庆华,谷秀芝.可直接计算的高效的可分电子现金系统[J].电子学报,2009,37(2):367 – 371.
LIU Wen-yuan, et al. Divisible e-cash system with direct computation and efficiency[J]. Acta Electronica Sinica, 2009, 37(2):367 – 371. (in Chinese)

[3] 徐国胜,谷利泽,杨义先,李忠献.新的可转移电子现金方案[J].通信学报,2008,29(5):1 – 5.
XU Guo-sheng, GU Li-ze, YANG Yi-xian, LI Zhong-xian. New transferable electronic cash scheme[J]. Journal on Communications, 2008, 29(5):1 – 5. (in Chinese)

[4] Nguyen L. Privacy-protecting coupon system revisited[A]. Proceedings of Financial Cryptography 2006[C]. Berlin: Springer-Verlag, 2006. 266 – 280.

[5] Chen L, Escalante A, Löhr H, and et al. A privacy-protecting multi-coupon scheme with stronger protection against splitting [A]. Proceedings of Financial Cryptography 2007[C]. Berlin: Springer-Verlag, 2008. 29 – 44.

[6] Armknecht F, Escalante A, Löhr H, and et al. Secure multi-coupons for federated environments: privacy-preserving and customer-friendly[A]. Proceedings of ISPEC 2008[C]. Berlin: Springer-Verlag, 2008. 29 – 44.

[7] Canard S, et al. A handy multi-coupon system[A]. Proceedings of ACNS 2006[C]. Berlin: Springer-Verlag, 2006. 66 – 81.

[8] Au M H. Contribution to privacy-preserving cryptographic techniques[D]. Wollongong: School of Computer Science and Software Engineering, University of Wollongong, 2009.

[9] Jao D, Yoshida K. Boneh-Boyen signatures and the Strong Diffie-Hellman problem[A]. Proceedings of Pairing 2009[C]. Berlin: Springer-Verlag, 2009. 1 – 16.

[10] Blanton M. Online subscriptions with anonymous access[A]. Proceedings of ASIA-CCS 2008[C]. New York: ACM Press, 2008. 217 – 227.

[11] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps [A]. Proceedings of CRYPTO 2004[C]. Berlin: Springer-Verlag, 2004. 56 – 72.

[12] Chen L, et al. Pairings in trusted computing[A]. Proceedings of Pairing 2008[C]. Berlin: Springer-Verlag, 2008. 1 – 17.

[13] Furukawa J. Efficiency enhancement of secure multi-party protocols for privacy and privilege protection[D]. TOKYO: the University of TOKYO, 2006.

[14] Damgård I, Fazio N, Nicolosi N. Non-interactive zero-knowledge from homomorphic encryption[A]. Proceedings of TCC 2006[C]. Berlin: Springer-Verlag, 2006. 41 – 59.

[15] Arita S. A straight-line extractable non-malleable commitment scheme[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2007, E90-A(7):1384 – 1394.

[16] Chida K, Yamamoto G. Batch processing for proofs of partial knowledge and its applications[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2008, E91-A(1):150 – 159.

[17] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[A]. Proceedings of EUROCRYPT 1999[C]. Berlin: Springer-Verlag, 1999. 223 – 238.

[18] Gjøsteen K, Kråkmo L. Round-optimal blind signatures from Waters signatures[A]. Proceedings of ProvSec 2008[C]. Berlin: Springer-Verlag, 2008. 112 – 126.

[19] Bichsel P, Camenisch J, Neven G, and et al. Get shorty via group signatures without encryption[A]. Proceedings of SCN 2010[C]. Berlin: Springer-Verlag, 2010. 381 – 398.

[20] Peng K, Boyd C, Dawson E. Batch zero knowledge proof and verification and its applications[J]. ACM Transactions on Information and System Security, 2007, 10(2):1 – 28.

[21] Le D P, et al. Multisignatures as secure as the Diffie-hellman problem in the plain public-key model[A]. Proceedings of Pairing 2009[C]. Berlin: Springer-Verlag, 2009. 35 – 51.

作者简介

柳 欣 男,山东广饶人,1978 出生,硕士,山东大学博士生,山东青年政治学院讲师,主要研究方向为安全协议设计与分析.
E-mail: lxonne@163.com

徐秋亮 男,山东淄博人,1960 年出生,博士,山东大学教授、博士生导师、计算机科学与技术学院副院长,主要研究方向为密码协议、可证明安全性等.