doi:10.11959/j.issn.1000-436x.2016175

基于 DAA 的轻量级多商家多重息票系统

柳欣[1,2]，徐秋亮[3]，张波[4]

（1. 山东青年政治学院信息工程学院，山东 济南 250103；
2. 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；
3. 山东大学计算机科学与技术学院，山东 济南 250101；4. 济南大学信息科学与工程学院，山东 济南 250022）

摘 要：基于 Brickell 等的 DAA（direct anonymous attestation）方案提出一个支持多商家环境的多重息票系统。新系统将多重息票中的关键元素与抗篡改的 TPM（trusted platform module）芯片进行绑定，从而能更有效地阻止用户的共享行为。新系统的构造过程使用了 Chow 等的服务器辅助签名验证技术、Yang 等的自盲化证书技术以及 Peng 等的区间证明技术，使用户在息票发布和兑换协议中均无需执行低效的对运算。相对于多个同类系统，新系统同时满足多个较理想的性质，而且与 ARM TrustZone 平台上的移动支付框架兼容。此外，新系统在通信和运算耗费方面具有明显优势。

关键词：多重息票；直接匿名证明；服务器辅助签名验证；区间证明；不可分割性

中图分类号：TN918.2 **文献标识码**：A

Lightweight multi-coupon system for multi-merchant environments with DAA

LIU Xin[1,2], XU Qiu-liang[3], ZHANG Bo[4]

（1. School of Information Engineering, Shandong Youth University of Political Science, Jinan 250103, China;
2. Key Laboratory of Information Security and Intelligent Control in Universities of Shandong
(Shandong Youth University of Political Science), Jinan 250103, China;
3. School of Computer Science and Technology, Shandong University, Jinan 250101, China;
4. School of Information Science and Engineering, University of Jinan, Jinan 250022, China）

Abstract: A multi-coupon system for multi-merchant environments was proposed by extending the DAA (direct anonymous attestation) scheme of Brickell etc. The new system bound the key elements in multi-coupon with the tamper-resistant TPM（trusted platform module）chip, so that it could prevent users from sharing behavior more effectively. By using the server-aided signature verification of Chow etc, the self-blindable credential technique of Yang etc, and range proof of Peng etc, the new system does not require customers to perform expensive pairing operations in the issue protocol and the redeem protocol. Compared with previous similar systems, the new system simultaneously satisfies several ideal properties and it is compatible with the mobile payment framework on the ARM TrustZone platform. Moreover, it has obvious advantages in aspects of communication and computation costs.

Key words: multi-coupon, direct anonymous attestation, server-aided signature verification, range proof, unsplittability

收稿日期：2015-09-24；**修回日期**：2016-07-07

基金项目：国家自然科学基金资助项目（No.61173139）；山东省自然科学基金资助项目（No.ZR2015FL023, No.ZR2014FL011）；山东省高等学校科技计划资助项目（No.J14LN61）；山东青年政治学院博士科研启动经费资助项目（No.14A007）

Foundation Items: The National Natural Science Foundation of China(No. 61173139), Shandong Provincial Natural Science Foundation(No.ZR2015FL023, No.ZR2014FL011),The Project of Shandong Province Higher Educational Science and Technology Program(No.J14LN61), The Doctoral Research Start-up Funding Project of Shandong Youth University of Political Science (No.14A007)

1　引言

息票（coupon）是一种传统的广告和促销手段。目前，电子息票（e-coupon）已在电子商务领域得到广泛应用，且能有效解决传统纸质息票的环境污染问题[1]。此外，还提出了移动息票[2]（m-coupon）和多重息票[3~9]（MC, multi-coupon）的概念。其中，MC 可视为包含 k 张可独立兑换息票的集合，它有助于商家与客户建立长期的购买关系，形成稳定的购买群体。出于安全性的考虑，多重息票系统（MCS, multi-coupon system）必须满足以下性质。为了保护商家利益，不允许顾客使用伪造的 MC 进行兑换，也不允许多名顾客对同一张 MC 进行分割使用。同时，为了保护顾客的隐私，应当确保顾客交易过程的机密性和同一名顾客的多个交易间的无关联性。

2005 年，Chen 等[3]提出 MCS 的安全模型，同时设计了一个实例化的系统。然而，该系统的最大缺点是息票发布和兑换阶段的复杂度线性依赖于 MC 的价值。此后，文献[4]提出了通信和运算复杂度均独立于 MC 价值的改进系统。但是，该系统的弱点是要求将 k 作为系统的固定参数。2007 年，Chen 等[5]指出已有系统[3,4]仅满足弱不可分割性（weak unsplittability），即只要客户 U_1、U_2 间存在完全信任关系，就可以通过复制操作实现对 MC 的分割使用。为此，Chen 等构造了满足强不可分割性（strong unsplittability）的改进系统，即只要客户 U_1、U_2 相互信任且 U_1 承诺在共享使用 MC 后与 U_2 执行某种交互，就能确保 U_2 可以继续使用 MC。由于要求顾客以固定顺序进行兑换，因此 Chen 等的系统仍无法满足实际应用的需要。文献[6]指出，已有的 MCS 仅考虑了单一商家的情况。为了实现客户友好性质，应当将此类系统推广至更具有一般性的环境，即允许不同类型的商家构成联合体，当获得由任何一个商家颁发的 MC 之后，顾客可以向联合体中的其他商家进行兑换。为此，文献[6]提出第一个支持多商家环境的 MCS，且无需限制兑换顺序。需要指出的是，文献[6]系统的缺点是联合体的公/私钥对是在商家间共享的，一旦某个商家退出联合体，将为 MCS 带来安全隐患。此外，联合体是以静态方式创建的，并未考虑商家的动态加入问题。最近，文献[7,8]提出多个满足额外性质的改进系统，如支持批量兑换、息票发布子协议满足并发安全性等。但是，这些系统[7,8]并不支持多商家环境。2015 年，Hinarejos 等[9]提出一个轻量级的多商家多重息票系统。然而，该系统的用户匿名性是借助群签名技术实现的，因此仅实现了较低的匿名性等级，即使客户保持诚实，也必须期望 MC 的发布者不与商家进行合谋。尽管采用群签名技术有利于通过揭示身份而实现对恶意用户的惩罚，但是最新的隐私增强匿名认证技术提倡采取“拒绝为欺诈用户提供服务而非损害其隐私”的宽容做法[10,11]。此外，该系统仅满足弱不可分割性。在文献[12]中，Canard 等指出 MC 可用于为病人开具药物处方，并提出允许用户分割使用 MC 的系统。本文认为，文献[12]系统与上述系统[3~9]的应用目标并不一致。

从实际角度考虑，MCS 应当同时满足以下性质：1)支持多商家应用环境，从而拓宽 MC 的使用范围，提高其兑换率；2)支持息票对象[5,6]的概念，即利用息票对象表示息票代表的商品或服务，因为不同商家提供的兑换服务是不同的；3)为顾客提供一定的灵活性，即允许顾客与发布者共同协商 MC 的价值以及商品类型；4)满足更强的不可分割性，因为已有系统[3~9]的不可分割性都是基于纯软件技术实现的，这种方式仅能为用户的共享行为设置障碍，而无法真正地阻止这种行为；5)系统的执行过程应当尽量避免用户执行低效的密码运算。已有系统[3~9]要求顾客执行 RSA 群上的模指数运算或者对运算。然而，这 2 类运算并不适合于移动设备[13~15]。

直接匿名证明（DAA, direct anonymous attestation）[16~19]是一类由可信计算组织（TCG, trusted computing group）提出的匿名证书系统，且适用于配置了专用安全芯片 TPM（trusted platform module）的计算平台。DAA 方案最初用于解决可信计算平台远程身份证明中的隐私保护问题[20]。当前，此类方案在众多应用系统的设计中同样得到广泛采用[19]。需要指出的是，标准的匿名证书系统（如文献[21]）往往难以杜绝用户复制和共享证书的行为。为此，Cesena 等[18]利用 DAA 技术构造了可以阻止此类行为的匿名认证方案。

本文基于 Brickell DAA 方案[16]提出一个改进的 MCS。该系统具有以下的显著特点：1)商家间无需共享秘密信息，当某个商家离开联合体时，不会带来安全性问题；2)用户在息票发布和息票兑换协议中均无需执行对运算，因此本文 MCS 在某种程度上是“轻量级的”；3)本文系统在新定义的多商家 MCS 模型下满足可证安全；4)在效率方面，本文系

统的通信和运算耗费较已有系统有明显优势；5)本文 MCS 与 Pirker 等[22]的基于 ARM TrustZone 技术的移动支付框架相兼容，因为 TPM 端与 Host 端分别对应于 TrustZone 系统的 Secure World 环境和 Normal World 环境。

2 多商家多重息票系统的定义及安全模型

2.1 多商家多重息票系统的定义

本文 MCS 定义是在文献[9]定义基础上修改得到的。具体地，多商家环境下的 MCS 可视为由以下算法/协议构成的集合，即 Setup、Affiliation、Disaffiliation、Issue、Redeem 和 Claim。其中，Setup 算法用于产生系统参数以及为发布者 I 产生公/私钥对。商家 V 通过与 I 执行 Affiliation 算法加入到联合体 *Fed* 中，且可以在今后通过与 I 执行 Disaffiliation 算法离开联合体。用户 U 利用 Issue 协议向发布者 I 申请 *MC*，且 *MC* 中的每张息票都是可以独立兑换的。当希望获得某类商品或服务时，U 通过执行 Redeem 协议向联合体 *Fed* 中的某个商家 V 兑换 *MC* 中的一张息票。此后，V 通过 Claim 协议向 I 证明自己为 U 提供了兑换服务，从而要求后者向自己支付费用。在本文模型下，安全的 MCS 应当满足如下安全性质。

1) 正确性：若诚实的用户 U 与发布者 I 执行 Issue 协议，并且获得由 I 提供的 *MC*，则 U 总是能利用 *MC* 中未曾使用的息票向联合体 *Fed* 中的商家 V 兑换商品或服务，且 V 总是能向 I 证明这个事实，使后者向自己支付相应的费用。

2) 不可伪造性：由恶意用户构成的联合与诚实商家 V 执行的兑换次数不能超过他们通过执行 Issue 协议而取得的合法息票数量之和。同时，由恶意商家构成的联合无法向 I 做出虚假声明，即声明的兑换次数超过他们实际为诚实用户提供兑换服务的次数。

3) 无关联性：好奇的商家 V 无法对用户 U 执行 Issue 协议和 Redeem 协议的行为进行关联，也无法对该用户 2 次执行 Redeem 协议的行为进行关联。

4) 可声明性：若诚实的商家 V 为用户 U 兑换了某张息票，则他总是能向 I 证明这个事实。

5) 不可分割性：用户 U_1 无法与另一个用户 U_2 分割使用自己的 *MC*。

2.2 多商家多重息票系统的安全模型

在文献[9]中，Hinarejos 等提出一个 MCS 安全模型。但是，Hinarejos 等[9]要求的防止息票重复兑换性质完全可以由不可伪造性所蕴含。此外，Hinarejos 等将无关联性实验分为 2 个模式，即分别在“由恶意商家构成联合”与“由恶意商家和发布者构成联合”2 种情况下进行分析。本文认为无需再对这 2 种情况进行细分，因为若 MCS 在后一种情况下满足无关联性，则在前一种情况下同样满足无关联性。为此，本文结合文献[6,9]的安全模型定义提出更为简洁的 MCS 安全模型。在本节的描述中，符号 *Adv* 与 *B* 分别表示安全性实验中的攻击者与归约算法，U、V、I 分别表示诚实用户、商家以及发布者，$\bar{U}$、$\bar{V}$、$\bar{I}$ 分别表示恶意（或被攻破的）用户、商家以及发布者，$\bar{\bar{U}}$ 表示部分被攻破的用户，即 $\bar{\bar{U}}$ 的 host 部分已经被攻破，但 TPM 部分仍然保持诚实。表 1 对 *Adv* 与 *B* 在不同安全性质实验中充当的角色进行了总结。

表 1 *Adv* 与 *B* 在不同安全性质实验中充当的角色

安全性质实验	*Adv* 充当的角色	*B* 充当的角色
不可伪造性（模式 1）	$\bar{U},\bar{\bar{U}}$(host)	$I,V,\bar{\bar{U}}$(TPM)
不可伪造性（模式 2）	$\bar{V}$	I,U
无关联性	$\bar{V},\bar{I},\bar{U}$	U
可声明性	$\bar{V},\bar{I},\bar{U}$	V
不可分割性	$\bar{U},\bar{\bar{U}}$(host)	$I,V,\bar{\bar{U}}$(TPM)

2.2.1 不可伪造性实验

该实验的执行过程分为以下 2 个模式。

1) 模式 1

① 初始化：*B* 执行 Setup 算法，产生 I 的公/私钥对 (w_I,γ) 以及 Fed_{pk} 中的其他参数，*B* 将 Fed_{pk} 提供给 *Adv*。

② 交互：*B* 为 *Adv* 提供以下的预言服务。

散列询问：当 *Adv* 提出关于散列函数 H_i 的询问 M，*B* 向 *Adv* 返回 $H_i(M)$。

Issue 询问：当 *Adv* 请求获得一张 *MC*，则 *B* 以 I 的身份与 *Adv* 执行 Issue 协议。

Semi-Issue 询问：当 *Adv* 请求获得一张 *MC*，则 *B* 以部分被攻破用户的 TPM 的身份与 *Adv* 联合执行同 I 的 Issue 协议。

Redeem 询问：当 *Adv* 请求向 V 兑换一张对象为 *ob* 的息票，则 *B* 以 V 的身份与 *Adv* 执行 Redeem 协议。

Semi-Redeem 询问：当 *Adv* 请求向 V 兑换一张

对象为 ob 的息票，则 B 以部分被攻破用户的 TPM 的身份与 Adv 联合执行同 V 的 Redeem 协议。

Corrupt 询问：当 Adv 请求攻破 U，则 B 向 Adv 返回 U 的私钥，同时将 U 标记为被攻破的用户。

③ 结束：Adv 输出 ob^*。若同时满足以下条件，则判定 Adv 在实验中获胜，即 Adv 向 B 兑换的“具有息票对象 ob^*”的息票数量大于它通过与 B 执行 Issue 协议而获得的“具有息票对象 ob^*”的息票数量。

2) 模式 2

① 初始化：B 执行模式 1 中描述的初始化操作。此外，B 定义计数器 Ctr_R，用于统计已经为诚实用户执行的兑换次数。

② 交互：B 为 Adv 提供以下的预言服务。

散列询问：描述方式同模式 1。

Issue 询问：当 Adv 请求为 U 发布一张 MC，则 B 以 I 的身份与 U 执行 Issue 协议。

Redeem 询问：当 Adv 请求为 U 兑换一张对象为 ob 的息票，则 B 以 U 的身份与 Adv 执行 Redeem 协议。

③ 结束：最终，Adv 输出由 Redeem 协议副本构成的列表 L_{trans}，并且请求 I 为 L_{trans} 中所含的交易支付费用，B 以 I 的身份与 Adv 执行 Claim 协议。若 Claim 协议执行成功且满足 $|L_{trans}|>Ctr_R$，则判定 Adv 在实验中获胜。

2.2.2 无关联性实验

该实验的具体过程分为以下阶段。

1) 初始化：B 执行不可伪造性实验中描述初始化操作，并且向 Adv 提供 $Fed_{pk},(w_1,\gamma)$。

2) 交互：B 为 Adv 提供以下的预言服务。

散列询问：描述过程同不可伪造性实验（模式 1）。

Issue 询问：B 以 U 的身份与 Adv 执行 Issue 协议，并且获得由 Adv 提供的 MC。

Redeem 询问：B 以 U 的身份与 Adv 执行 Redeem 协议。

Corrupt 询问：当 Adv 请求攻破 U，则 B 将 U 标记为被攻破的用户。

3) 挑战：Adv 输出 $(U_0,U_1,\alpha_0,\beta_0,\alpha_1,\beta_1,\overline{V})$，若不能同时满足以下条件，则 B 运行失败，即：① U_0 与 U_1 均未被攻破；② U_0 的第 α_0 张 MC 中的第 β_0 张息票与 U_1 的第 α_1 张 MC 中的第 β_1 张息票具有相同的状态，即要么均未兑换，要么均已得到兑换；③ U_0 的第 α_0 张 MC 中的第 β_0 张息票与 U_1 的第 α_1 张 MC 中的第 β_1 张息票含有相同的息票对象。否则，B 选取 $c\in_R\{0,1\}$，然后分别以 U_c 的身份向 $\overline{V}$ 兑换第 α_0 张 MC 中的第 β_0 张息票，以 U_{1-c} 的身份向 $\overline{V}$ 兑换第 α_1 张 MC 中的第 β_1 张息票。

4) 结束：Adv 输出猜测结果 b，若 $b=c$，则判定 Adv 在实验中获胜。

2.2.3 可声明性实验

该实验的具体过程分为以下阶段。

1) 初始化：B 执行无关联性实验中描述的初始化操作。

2) 交互：B 为 Adv 提供以下的预言服务。

散列询问：描述过程同不可伪造性实验。

Redeem 询问：当 Adv 请求向 V 兑换一张对象为 ob 的息票，B 以 V 的身份与 Adv 执行 Redeem 协议。

3) 结束：最终，Adv 请求向 V 兑换一张对象为 ob^* 的息票，若满足以下条件，则判定 Adv 在实验中获胜，即：① B 与 Adv 成功执行 Redeem 协议并且获得对应的交易副本 $trans^*$；②当 B 以 $trans^*$ 为输入与 Adv 执行 Claim 协议时，该协议总是失败，即 B 无法证明自己为用户提供兑换服务这个事实。

2.2.4 不可分割性实验

该实验的具体过程分为以下阶段。

1) 初始化：B 执行不可伪造性实验（模式 1）中描述的初始化操作。

2) 交互：B 为 Adv 提供以下的预言服务。

散列询问：描述过程同不可伪造性实验（模式 1）。

Issue 询问：描述过程同不可伪造性实验（模式 1）。

Semi-Issue 询问：描述过程同不可伪造性实验（模式 1）。

Redeem 询问：描述过程同不可伪造性实验（模式 1）。

Semi-Redeem 询问：描述过程同不可伪造性实验（模式 1）。

3) 结束：Adv 输出 MC^*。若同时满足以下条件，则判定 Adv 在实验中获胜，即：① MC^* 是有效的；② MC^* 的剩余价值大于 0；③当 B 以 MC^* 为输入执行 Redeem 协议时，该协议总是失败，这表明 Adv 已经将 MC^* 的剩余价值转移至其他的 MC'，即实现了对 MC^* 的分割使用。

3 预备知识

令 G_1、G_2、G_T 分别为素数 p 阶循环群，满足 $G_1=\langle g_0\rangle, G_2=\langle h_0\rangle$。令 $\hat{e}$ 表示双线性映射，使 $G_1\times G_2\to G_T$。令 $\tilde{G}$ 表示素数 p 阶循环群，满足 $\tilde{G}=\langle\tilde{g}\rangle$。

3.1 复杂性假设

q-SDH（q-strong Diffie-Hellman）假设[23]：对于任何的 PPT（probabilistic polynomial time）算法 $\mathfrak{A}$，定义概率

$$Adv_{\mathfrak{A}}^{q\text{-SDH}}=\Pr[\mathfrak{A}\left((p,G_1,G_2,G_T,g_0,h_0,\hat{e}),h_0,h_0^{\gamma},\cdots,h_0^{\gamma^q}\right)=(g_0^{\frac{1}{\gamma+x}},x):\gamma,x\in\mathbb{Z}_p^*]$$

q-SDH 假设表明 $Adv_{\mathfrak{A}}^{q\text{-SDH}}$ 是可以忽略的。

y-DDHI（decisional Diffie-Hellman inversion）假设[12]。对于任何的 PPT 算法 $\mathfrak{A}$，定义概率

$$Adv_{\mathfrak{A}}^{y\text{-DDHI}}=\Pr[\mathfrak{A}\left(\tilde{g},\tilde{g}^{x},\tilde{g}^{x^2},\cdots,\tilde{g}^{x^y},\tilde{g}^{c}\right)=\begin{cases}1, c=\dfrac{1}{x}:\left(\tilde{g},\tilde{g}^{x},\tilde{g}^{x^2},\cdots,\tilde{g}^{x^y},\tilde{g}^{c}\right)\in\tilde{G}^{y+2}\\ 0,\text{其他}\end{cases}]$$

y-DDHI 假设表明 $Adv_{\mathfrak{A}}^{y\text{-DDHI}}$ 是可以忽略的。

G_1-DDH（G_1- decisional Diffie-Hellman）假设[19]：对于任何的 PPT 算法 $\mathfrak{A}$，定义概率

$$Adv_{\mathfrak{A}}^{G_1\text{-DDH}}=|\Pr[\mathfrak{A}\left((p,G_1,G_2,G_T,g_0,h_0,\hat{e}),X,Y,Z\right)=1:x,y,z\in\mathbb{Z}_p,X=g_0^x,Y=g_0^y,Z=g_0^z]-\Pr[\mathfrak{A}\left((p,G_1,G_2,G_T,g_0,h_0,\hat{e}),X,Y,Z\right)=1:x,y\in\mathbb{Z}_p,X=g_0^x,Y=g_0^y,Z=g_0^{xy}]|$$

G_1-DDH 假设表明 $Adv_{\mathfrak{A}}^{G_1\text{-DDH}}$ 是可以忽略的。

3.2 BBS+签名方案

令 $g_0,g_1,\cdots,g_{n+1}$ 为群 G_1 的生成元，令 h_0 为群 G_2 的生成元。签名者私钥为 $\gamma\in\mathbb{Z}_p$，公钥为 $w=h_0^{\gamma}$。给定待签名的消息 $m_1,\cdots,m_n$，所产生的 BBS+方案签名[23]为 (A,e,s)，其中，$A=(g_0g_1^{m_1}\cdots g_n^{m_n}g_{n+1}^{s})^{\frac{1}{\gamma+e}}$，$s,e\in\mathbb{Z}_p$。Au 等[23]指出，证明掌握该签名，等价于证明关系 $\hat{e}(A,wh_0^{e})=\hat{e}(g_0g_1^{m_1}\cdots g_n^{m_n}g_{n+1}^{s},h_0)$ 成立，且证明过程需要对元素 A 进行盲化。然而，该过程要求证明者执行低效的对运算以及群 G_T 上的指数运算。

3.3 自盲化证书技术

最近，Yang 等[24]提出了旨在减轻用户端运算耗费的自盲化证书技术。为了证明掌握 BBS+方案签名 (A,e,s)，证明者选取 $f\in\mathbb{Z}_p$，计算 $A'=A^f$，$A''=A'^{e},M'=M^f$，其中，$M=g_0g_1^{m_1}\cdots g_n^{m_n}g_{n+1}^{s}$。于是，证明掌握秘密元素 $A,e,m_1,\cdots,m_n,s$，使验证等式 $\hat{e}(A,wh_0^{e})=\hat{e}(g_0g_1^{m_1}\cdots g_n^{m_n}g_{n+1}^{s},h_0)$ 成立，等价于证明掌握秘密元素 $e,f,m_1f,\cdots,m_nf,sf$，使关系 $A''=A'^{e}$，$M'=g_0^fg_1^{m_1f}\cdots g_n^{m_nf}g_{n+1}^{sf}$ 成立。此外，要求验证者额外验证等式 $\hat{e}(A',w)=\hat{e}(M'A''^{-1},h_0)$ 是否成立以及是否满足 $A'\neq 1\in G_1$。

3.4 Peng-Yi 区间证明技术

本文系统的构造过程要求使用 Peng 等[25]的关于秘密元素 j 属于公开集合 $[1,J_i]$ 的准确区间证明协议，记为 $PK\{(j,r):\tilde{T}=\bar{g}^j\bar{h}^r\wedge j\in[1,J_i]\}$。其基本思想是首先将目标证明 $PK\{(j,r):\tilde{T}=\bar{g}^j\bar{h}^r\wedge j\in[1,J_i]\}$ 等价为 $PK\{(j-1,r):\tilde{T}'=\bar{g}^{j-1}\bar{h}^r\wedge j-1\in[0,J_i-1]\}$，其中，$\tilde{T}'=\dfrac{\tilde{T}}{\bar{g}}$。然后，计算秘密元素 $j-1$ 关于底数 $\upsilon(\upsilon>2)$ 的表达式 $(x_1,\cdots,x_l)_{\upsilon}$，满足 $j-1=\sum_{t=1}^{l}x_t\upsilon^{t-1}$，从而将关于 $j-1\in[0,J_i-1]$ 的证明约化为 l 个关于 $x_t\in[0,\upsilon-1](t=1,\cdots,l)$ 的更为简单的证明。现在，证明 $PK\{(j-1,r):\tilde{T}'=\bar{g}^{j-1}\bar{h}^r\wedge j-1\in[0,J_i-1]\}$ 进一步等价于证明

$$PK\{(r',(x_t,r_t)_{t=1}^{l}):\prod_{t=1}^{l}\frac{e_t^{\upsilon^{t-1}}}{\tilde{T}'}=\bar{h}^{r'}\wedge\{e_t=\bar{g}^{x_t}\bar{h}^{r_t}\wedge x_t\in[0,\upsilon-1]\}_{t=1}^{l}\}$$

其中，$r'=\sum_{t=1}^{l}r_t\upsilon^{t-1}-r \bmod p$。

3.5 对委托运算协议与服务器辅助签名验证技术

委托运算技术有利于用户将繁重的运算任务委托给不可信的服务器，且此类运算模式特别适合于当前的云计算应用环境。对委托运算（pairing delegation）协议是一种委托计算技术，使用户端无需再执行昂贵的对运算。Canard 等[15]指出，对委托运算协议应当满足完备性、可验证性和保密性。

服务器辅助签名验证（SASV, server-aided signature verification）技术的目标是帮助用户将数字签名验证过程中涉及的对运算任务委托给服务器。最近，Chow 等[14]提出了一般性的 SASV 框架，且允许将任何对委托运算协议作为该框架的底层

模块。此类技术要求满足以下性质：1)适应性选择消息与验证攻击下的存在的不可伪造性；2)合谋的适应性选择验证攻击下的可靠性。

4　对本文系统的描述

4.1　本文系统的设计思想

用户获得形式为 $(mid,J_1,\cdots,J_n,cre)$ 的 *MC*，其中，*mid* 表示唯一的多重息票标识符，$\{J_i\}_{i=1}^n$ 表示每类对象 ob_i 所对应的最大服务次数或商品数量，*cre* 表示商家为元组 $(sk,mid,J_1,\cdots,J_n)$ 产生的用户证书，其中，*sk* 表示底层 DAA 方案的 TPM 私钥。为了实现更强的不可分割性，本文系统在兑换过程中要求使用与 *cre* 相绑定且仅为 TPM 所掌握的 *sk*。为了防止用户的重复兑换行为，要求用户在兑换过程中提供与每张息票唯一对应的重复检测标签 *S*，而该标签是利用底层 Dodis-Yampolskiy 伪随机函数[26]产生的。在 Issue 协议中，为了验证所得 *MC* 的有效性，用户需要执行 BBS+方案签名的验证过程。为了避免执行对运算，本文利用 Chow 等[14]的 SASV 技术将验证过程涉及的对运算委托给服务器。在 Redeem 协议中，用户需要证明掌握有效的 *MC*，而这等价于证明掌握有效的 BBS+方案签名。为了摆脱对运算，本文利用 Yang 等[24]的自盲化证书技术实现了用户与商家间运算任务的不平衡性[27]。最后，为了在兑换过程中证明自己的 *MC* 尚能兑换对象 ob_i 所对应的商品或服务，用户需要执行形式为“$j\in[1,J_i]$”的准确区间证明。为此，本文使用了高效的 Peng-Yi 区间证明技术[25]。

4.2　具体描述

4.2.1　系统中的参与方

在本文系统中，共涉及以下参与方，即由 TPM 和主机 host 构成的用户 U，由多个商家构成的联合体 $Fed=\{V_1,\cdots,V_m\}$ 以及发布者 I。

4.2.2　系统建立（Setup）

以安全参数 1^λ 作为输入，I 执行下列步骤。

1) 选取具有可计算同构 $\psi:G_2\to G_1$ 的素数 p 阶非对称群对 (G_1,G_2) 以及双线性映射 $\hat{e}:G_1\times G_2\to G_T$，其中，$G_1=\langle g_0\rangle,G_2=\langle h_0\rangle$。选取 $g_1,\cdots,g_{n+3}\in_R G_1$，选取 $\overline{g},\overline{h}\in_R G_1$。

2) 选取素数 p 阶椭圆曲线群 $\tilde{G}$，使 $\tilde{G}$ 上的 DDH 问题是难解的，选取 $\tilde{g}_3,\cdots,\tilde{g}_{n+2}\in_R\tilde{G}$。

3) 定义抗碰撞的散列函数 $H_i:\{0,1\}^*\to\mathbb{Z}_p$，$i=1,\cdots,4$。

4) 选取 $\gamma\in_R\mathbb{Z}_p^*$，计算 BBS+签名方案[23]公钥 $w_I=h_0^\gamma$。

5) 设置息票对象集合 $\overrightarrow{ob}=(ob_1,\cdots,ob_n)$。

6) 创建公共数据库 *DB*，并且为 *DB* 创建任意的标准数字签名方案 *SIG* 下的公/私钥对 (PK_{DB},SK_{DB})，用于为向 *DB* 中写入重复检测标签的商家产生收据。创建废除列表 *BL*，以及列表 *AL*、*ADL*。

7) 输出公开参数 $Fed_{pk}=(G_1,G_2,G_T,\tilde{G},\ p,\hat{e},\ \{g_i\}_{i=0}^{n+3},\ h_0,\{\tilde{g}_i\}_{i=3}^{n+2},\overline{g},\overline{h},w_I,\{H_i\}_{i=1}^4,\overrightarrow{ob},PK_{DB})$。

4.2.3　商家加入联合体（Affiliation）

希望加入 *Fed* 的商家 V 与 I 签署商业合作协议，其内容包括：规定 V 支持兑换的商品或服务类型，I 承诺为 V 提供兑换服务而支付费用等。然后，I 为 V 分配身份标识 id_V，执行 $AL\leftarrow AL\cup\{id_V\}$。

4.2.4　息票发布（Issue）

该协议由 U（host+TPM）和 I 共同执行。假设 TPM 已经与 I 建立起可信信道[16]。为了提高在线运算效率，假设 TPM 已事先选取 $\rho_{sk},\rho_{mid}\in_R\mathbb{Z}_p$，并计算 $R_1=g_1^{\rho_{sk}},R_2=g_2^{\rho_{mid}}$，具体步骤如下。

1) I 选取随机数 $n_I\in_R\{0,1\}^\lambda$，并且向 TPM 发送 $n_I,J_1,\cdots,J_n$。其中，$J_i(i=1,\cdots,n)$ 表示 host 此前向 I 申请的每类服务 ob_i 的访问次数。为了确保底层 Dodis-Yampolskiy 伪随机函数的抗碰撞性，要求满足 $\max\{J_1,\cdots,J_n\}<2^\lambda$ [28]。

2) TPM 计算私钥 $sk=H_1(DAASeed\|cnt\|K_I)$。选取 $mid\in_R\mathbb{Z}_p$，计算 $F_1=g_1^{sk},F_2=g_2^{mid}$，$c=H_2(Fed_{pk}\|n_I\|J_1\|\cdots\|J_n\|F_1\|F_2\|R_1\|R_2)$，在 $\mathbb{Z}_p$ 上计算 $\xi_{sk}=\rho_{sk}+c\cdot sk,\xi_{mid}=\rho_{mid}+c\cdot mid$。上述过程可以理解为 TPM 产生了知识签名 $SPK\{(sk,mid):F_1=g_1^{sk}\wedge F_2=g_2^{mid}\}(n_I\|J_1\|\cdots\|J_n)$。

上述的 *cnt* 是 TPM 内部计数器。本文允许用户通过多次执行当前协议而获得多个 *MC*，且假设在每次执行当前协议时，*cnt* 的取值不变。

3) TPM 向 I 发送 $(F_1,F_2,c,\xi_{sk},\xi_{mid},n_I)$。

4) I 验证 n_I。对于每个 $sk'\in BL$，I 验证是否满足 $F_1\neq g_1^{sk'}$。若满足，则计算 $\hat{R}_1=g_1^{\xi_{sk}}F_1^{-c}$，$\hat{R}_2=g_2^{\xi_{mid}}F_2^{-c}$，验证是否满足 $c=H_2(Fed_{pk}\|n_I\|J_1\|$

$\cdots \| J_n \| F_1 \| F_2 \| \hat{R}_1 \| \hat{R}_2)$。若不满足，则选取 $e,s \in {}_R\mathbb{Z}_p$，计算 $A = (g_0 F_1 F_2 g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s})^{\frac{1}{e+\gamma}}$，向 TPM 发送 $cre = (A,e,s)$。

5) TPM 向 host 发送 (F_1, mid, cre)，host 验证 cre 是否为关于 $(sk, mid, J_1, \cdots, J_n)$ 的有效 BBS+签名，即是否满足验证等式 $\hat{e}(A, w_I h_0^e) = \hat{e}(g_0 F_1 g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s}, h_0)$。

为了提高验证效率，host 利用 Chow 等[14]的 SASV 技术进行验证，具体过程如下。

① 设置 $C_1 = A, C_2 = w_I h_0^e, C_3 = g_0 F_1 g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s}$, $C_4 = h_0$，即将原始的 BBS+签名验证等式 $\hat{e}(A, w_I h_0^e) = \hat{e}(g_0 F_1 g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s}, h_0)$ 归结为 $\hat{e}(C_1, C_2) = \hat{e}(C_3, C_4)$ 的一般形式。

② 分别以 (C_1, C_2)、(C_3, C_4) 为输入，调用底层对委托运算协议 Φ。

③ 根据步骤②所得的委托运算结果 $\Phi(C_1, C_2)$、$\Phi(C_3, C_4)$，验证是否满足 $\Phi(C_1, C_2) = \Phi(C_3, C_4)$。若是，则接受 cre 为有效 BBS+签名。

最终，host 保存 $MC = (mid, J_1, \cdots, J_n, cre)$。

4.2.5 息票兑换（Redeem）

假设 U（host+TPM）希望向商家 $V \in Fed$ 兑换类型为 $ob_i \in \overrightarrow{ob}$ 的商品或服务。

1) V 向 U 发送 $id_V, n_V \in_R \{0,1\}^{\lambda}$。$U$ 检查是否满足 $id_V \in AL$，若满足，则向 V 发送 ob_i 以及符合如下形式的知识签名。

$$\pi = SPK\{(sk, s, j, r_s, r_j, \{J_i\}_{i=1}^{n}, \{r_{J_i}\}_{i=1}^{n}, A, mid, e):$$
$$K = B^{sk} \wedge S = \tilde{g}_{i+2}^{\frac{1}{s+j+1}} \wedge T = \overline{g}^{s} \overline{h}^{r_s} \wedge$$
$$\tilde{T} = \overline{g}^{j} \overline{h}^{r_j} \wedge \{T_i = \overline{g}^{J_i} \overline{h}^{r_{J_i}}\}_{i=1}^{n} \wedge$$
$$A = (g_0 g_1^{sk} g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s})^{\frac{1}{e+\gamma}} \wedge$$
$$j \in [1, J_i]\}(id_V \| n_V)$$

注意，群 $\tilde{G}$ 的生成元 $\tilde{g}_3, \cdots, \tilde{g}_{n+2}$ 分别固定地与息票对象 $ob_1, \cdots, ob_n$ 相对应，在兑换 ob_i 类型服务的情况下，序列号 S 是利用关系 $S = \tilde{g}_{i+2}^{\frac{1}{s+j+1}}$ 产生的。

2) 若 π 能通过验证，且对于每个 $sk' \in BL$，满足 $K \neq B^{sk'}$，则 V 向 DB 发送 S。

3) DB 检查是否满足 $S \notin DB$，若满足，则执行 $DB \leftarrow DB \cup (S)$，向 V 返回 $receipt = SIG_{SK_{DB}}(S)$ 作为收据；否则，DB 向 V 返回关于“序列号 S 因重复使用而无法写入数据库”的失败信息。

4) 若 V 接收到收据（$receipt$），则利用 PK_{DB} 验证 $receipt$ 的有效性，然后，V 为用户提供所请求的类型 ob_i 的服务，并且保存交易副本 $trans = (id_V, n_V, S, ob_i, \pi, receipt)$。相反，若 V 接收到的是出错信息，则拒绝为 U 提供兑换服务。

4.2.6 声明（Claim）

当 V 已经积累了由若干兑换交易副本构成的列表 $L_{trans} = \{trans_1, trans_2, \cdots\}$，且希望向 I 索取费用，则与 I 执行以下步骤。

1) V 向 I 发送 (L_{trans}, id_V)。

2) I 检查是否满足 $id_V \in AL$，若满足，则对于 L_{trans} 中的每个交易副本，I 执行如下检查：①验证知识签名 π 的有效性；②验证是否满足 $S \in DB$；③验证 $receipt$ 的有效性。若上述检查都通过，则 I 为 V 支付费用。相反，若满足 $S \notin DB$ 或 $receipt$ 验证失败，则判定 V 进行欺诈。

4.2.7 商家退出联合体（Disaffiliation）

若 V 请求退出 Fed，则 I 执行 $AL \leftarrow AL / \{id_V\}$，$ARL \leftarrow ARL \cup \{id_V\}$。

5 知识签名 π 的实现过程

为了便于理解，本文将 π 的执行过程分成 2 个子签名 π_1、π_2 进行描述。

$$\pi_1 = SPK\{(sk, s, j, r_s, r_j, \{J_i\}_{i=1}^{n}, \{r_{J_i}\}_{i=1}^{n}, A, mid, e):$$
$$K = B^{sk} \wedge S = \tilde{g}_{i+2}^{\frac{1}{s+j+1}} \wedge T = \overline{g}^{s} \overline{h}^{r_s} \wedge$$
$$\tilde{T} = \overline{g}^{j} \overline{h}^{r_j} \wedge \{T_i = \overline{g}^{J_i} \overline{h}^{r_{J_i}}\}_{i=1}^{n} \wedge$$
$$A = (g_0 g_1^{sk} g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s})^{\frac{1}{e+\gamma}}\}(id_V \| n_V)$$
$$\pi_2 = SPK\{(j, r_j): \tilde{T} = \overline{g}^{j} \overline{h}^{r_j} \wedge j \in [1, J_i]\}(id_V \| n_V)$$

5.1 子签名 π_1 的实现过程

在 π_1 的构造过程中，本文采用 Yang 等[24]的自盲化证书技术对 Au 等[23]的关于“掌握有效 BBS+方案签名”的方法进行了优化。π_1 的最终形式为

$$\pi_1 = SPK\{(sk, s, j, r_s, r_j, \{J_i\}_{i=1}^{n}, \{r_{J_i}\}_{i=1}^{n},$$
$$e, f, sk \cdot f, mid \cdot f, \{J_i \cdot f\}_{i=1}^{n}, s \cdot f):$$
$$K = B^{sk} \wedge \frac{\tilde{g}_{i+2}}{S} = S^{s+j} \wedge T = \overline{g}^{s} \overline{h}^{r_s} \wedge$$
$$\tilde{T} = \overline{g}^{j} \overline{h}^{r_j} \wedge \{T_i = \overline{g}^{J_i} \overline{h}^{r_{J_i}}\}_{i=1}^{n} \wedge A'' = A'^{e} \wedge$$
$$M' = g_0^{f} g_1^{sk \cdot f} g_2^{mid \cdot f} g_3^{J_1 \cdot f} \cdots g_{n+2}^{J_n \cdot f} g_{n+3}^{s \cdot f}\}(id_V \| n_V)$$

π_1 的具体产生过程如下。

在兑换协议开始之前，TPM 预先选取 $B\in_R G_1$, $\rho_{sk},\rho_{sk\cdot f}\in_R \mathbb{Z}_p$，计算 $R_1=B^{\rho_{sk}}, R_{7t}=g_1^{\rho_{sk\cdot f}}$。

1) TPM 计算 $sk=H_1(DAASeed\,\|\,cnt\,\|\,K_I)$，选取 $f\in_R\mathbb{Z}_p$，计算 $K=B^{sk}, R=g_1^{sk\cdot f}$，并且向 host 发送 (B,K,R_1,R_{7t},R,f)。

2) host 在 $[1,J_i]$ 中选取未使用过的序号 j，计算重复检测标签 $S=\tilde{g}_{i+2}^{\frac{1}{s+j+1}}$，选取 $r_s\in_R\mathbb{Z}_p$，计算 $T=\overline{g}^s\overline{h}^{r_s}$，选取 $r_j\in_R\mathbb{Z}_p$，计算 $\tilde{T}=\overline{g}^j\overline{h}^{r_j}$。对于 $i=1,\cdots,n$，选取 $r_{J_i}\in_R\mathbb{Z}_p$，计算 $T_i=\overline{g}^{J_i}\overline{h}^{r_{J_i}}$。

计算 $A'=A^f, A''=A'^e$，$M'=(g_0g_2^{mid}g_3^{J_1}\cdots g_{n+2}^{J_n}g_{n+3}^{s})^f R=g_0^f g_1^{sk\cdot f}g_2^{mid\cdot f}g_3^{J_1\cdot f},\cdots,g_{n+2}^{J_n\cdot f}g_{n+3}^{s\cdot f}$。选取 $\rho_s,\rho_j,\rho_{r_s},\rho_{r_j},\rho_e,\rho_f,\rho_{mid\cdot f},\rho_{J_1\cdot f},\cdots,\rho_{J_n\cdot f},\rho_{s\cdot f}\in_R\mathbb{Z}_p$。对于 $i=1,\cdots,n$，选取 $\rho_{J_i},\rho_{r_{J_i}}\in_R\mathbb{Z}_p$。

计算 $R_2=S^{\rho_s+\rho_j}, R_3=\overline{g}^{\rho_s}\overline{h}^{\rho_{r_s}}, R_4=\overline{g}^{\rho_j}\overline{h}^{\rho_{r_j}}, \{R_{5,i}=\overline{g}^{\rho_{J_i}}\overline{h}^{\rho_{r_{J_i}}}\}_{i=1}^n, R_6=A'^{\rho_e}, R_7=g_0^{\rho_f}R_{7t}g_2^{\rho_{mid\cdot f}}g_3^{\rho_{J_1\cdot f}}\cdots g_{n+2}^{\rho_{J_n\cdot f}}g_{n+3}^{\rho_{s\cdot f}}$。

3) host 计算 $c_h=H_3(Fed_{pk}\,\|\,S\,\|\,B\,\|\,K\,\|\,T\,\|\,\tilde{T}\,\|\,\{T_i\}_{i=1}^n\,\|\,A'\,\|\,A''\,\|\,M'\,\|\,R_1\,\|\cdots\|\,R_7\,\|\,id_V\,\|\,n_V)$，向 TPM 发送 c_h。

4) TPM 选取 $n_T\in\{0,1\}^\lambda$，计算 $c=H_4(c_h\,\|\,n_T\,\|\,ob_i)$，在 $\mathbb{Z}_p$ 上计算 $\xi_{sk}=\rho_{sk}+c\cdot sk$, $\xi_{sk\cdot f}=\rho_{sk\cdot f}+c\cdot sk\cdot f$。TPM 向 host 返回 $(c,n_T,\xi_{sk},\xi_{sk\cdot f})$。

5) host 在 $\mathbb{Z}_p$ 上计算

$$\xi_s=\rho_s+c\cdot s,\xi_j=\rho_j+c\cdot j,$$
$$\xi_{r_s}=\rho_{r_s}+c\cdot r_s,\xi_{r_j}=\rho_{r_j}+c\cdot r_j,$$
$$\{\xi_{J_i}=\rho_{J_i}+c\cdot J_i\}_{i=1}^n,\{\xi_{r_{J_i}}=\rho_{r_{J_i}}+c\cdot r_{J_i}\}_{i=1}^n,$$
$$\xi_e=\rho_e+c\cdot e,\xi_f=\rho_f+c\cdot f,\xi_{mid\cdot f}=\rho_{mid\cdot f}+c\cdot mid\cdot f,$$
$$\{\xi_{J_i\cdot f}=\rho_{J_i\cdot f}+c\cdot r_{J_i\cdot f}\}_{i=1}^n,\xi_{s\cdot f}=\rho_{s\cdot f}+c\cdot s\cdot f$$

最终，host 输出 $(S,B,K,T,\tilde{T},\{T_i\}_{i=1}^n,A',A'',M',c,n_T,\xi_{sk},\cdots,\xi_{s\cdot f})$。

π_1 的验证过程如下。

1) V 验证是否满足 $S,B,K,T,\tilde{T},\{T_i\}_{i=1}^n,A',A'',M'\in G_1$ 以及 $\xi_{sk},\cdots,\xi_{s\cdot f}\in\mathbb{Z}_p$。检查是否满足 $S\notin DB$ 以及 $A'\neq 1\in G_1$。

2) 验证是否满足 $\hat{e}(A',w_I)=\hat{e}(M'A''^{-1},h_0)$。

3) 计算 $\hat{R}_1=B^{\xi_{sk}}K^{-c}$，$\hat{R}_2=S^{\xi_s+\xi_j}\left(\frac{\tilde{g}_{i+2}}{S}\right)^{-c}$，$\hat{R}_3=\overline{g}^{\xi_s}\overline{h}^{\xi_{r_s}}T^{-c}$, $\hat{R}_4=\overline{g}^{\xi_j}\overline{h}^{\xi_{r_j}}\tilde{T}^{-c}$, $\{\hat{R}_{5,i}=\overline{g}^{\xi_{J_i}}\overline{h}^{\xi_{r_{J_i}}}T_i^{-c}\}_{i=1}^n$, $\hat{R}_6=A'^{\xi_e}A''^{-c}$, $\hat{R}_7=g_0^{\xi_f}g_1^{\xi_{sk\cdot f}}g_2^{\xi_{mid\cdot f}}g_3^{\xi_{J_1\cdot f}}\cdots g_{n+2}^{\xi_{J_n\cdot f}}g_{n+3}^{\xi_{s\cdot f}}M'^{-c}$。验证是否满足 $c=H_4(H_3(Fed_{pk}\,\|\,S\,\|\,B\,\|\,K\,\|\,T\,\|\,\tilde{T}\,\|\,\{T_i\}_{i=1}^n\,\|\,A'\,\|\,A''\,\|\,M'\,\|\,\hat{R}_1\,\|\cdots\|\,\hat{R}_7\,\|\,id_V\,\|\,n_V)\|\,n_T\,\|\,ob_i)$。

5.2 子签名 π_2 的实现过程

根据 3.4 节可知，可以利用 Peng 等[25]的小区间准确区间证明技术将 $\pi_2=SPK\{(j,r_j):\tilde{T}=\overline{g}^j\overline{h}^{r_j}\wedge j\in[1,J_i]\}(id_V\,\|\,n_V)$ 转换为

$$\pi_2=SPK\{(r',(x_t,r_t)_{t=1}^l):\prod\nolimits_{t=1}^l\frac{e_t^{\upsilon^{t-1}}}{\tilde{T}'}=\overline{h}^{r'}\wedge\{e_t=\overline{g}^{x_t}\overline{h}^{r_t}\wedge x_t\in[0,\upsilon-1]\}_{t=1}^l\}(id_V\,\|\,n_V)$$

其中，$r'=\sum_{t=1}^l r_t\upsilon^{t-1}-r \bmod p$。在文献[25]中，Peng 等指出可以利用文献[29]中的关于“秘密元素属于公开集合 $\mathbb{S}$”的证明技术实现关于 $\{e_t=\overline{g}^{x_t}\overline{h}^{r_t}\wedge x_t\in[0,\upsilon-1]\}_{t=1}^l$ 的证明，但并未提供具体过程。在下面，本文定义公开集合 $\mathbb{S}=\{0,1,\cdots,\upsilon-1\}$，并通过对文献[29]证明技术的 l 次迭代实现了这项证明，即对于 $t=1,\cdots,l$，证明 $e_t=\overline{g}^{x_t}\overline{h}^{r_t}\wedge x_t\in\mathbb{S}$ 成立。同时，为了提高效率，本文对这 l 次迭代执行了并行合成。π_2 的产生过程如下。

1) host 计算 $\tilde{T}'=\frac{\tilde{T}}{\overline{g}}$。计算 $j-1$ 在底数 $\upsilon(\upsilon>2)$ 的编码系统中的表达式 $(x_1,\cdots,x_l)_\upsilon$，满足 $j-1=\sum_{t=1}^l x_t\upsilon^{t-1}$。

2) 定义公开集合 $\mathbb{S}=\{s_1,\cdots,s_\upsilon\}=\{0,1,\cdots,\upsilon-1\}$。显然，host 掌握秘密元素 $\{x_t\}_{t=1}^l\in\mathbb{S}$。现在，host 将 υ 阶多项式 $F(X)=\prod_{i=1}^{\upsilon}(X-s_i)\bmod p$ 扩展为 $F(X)=\sum_{i=0}^{\upsilon}a_iX^i \bmod p$（满足 $F(s_i)=0,\ i=1,\cdots,\upsilon$），从而得到系数 $(a_0,\cdots,a_\upsilon)$。对于 $t=1,\cdots,l$，host 选取 $r_t\in_R\mathbb{Z}_p$，计算 $e_t=\overline{g}^{x_t}\overline{h}^{r_t}$。对于 $t=1,\cdots,l,i=2,\cdots,\upsilon$，host 计算 $e_{t,i}=e_{t,i-1}^{x_t}\overline{h}^{r_{t,i}}$，其中，$e_{t,1}=e_t, r_{t,i}\in_R\mathbb{Z}_p$。现在，可以将 $e_{t,i}$ 表示为 $e_{t,i}=\overline{g}^{x_t^i}\overline{h}^{R_{t,i}}, i=1,\cdots,\upsilon$，其中

$$R_{t,i}=\begin{cases}x_tR_{t,i-1}+r_{t,i}, & i=2,\cdots,\upsilon\\ r_t, & i=1\end{cases}$$

3) 将 π_2 细化为如下形式

$$\pi_2 = SPK\{(r',(x_t,r_t,r_{t,2},\cdots,r_{t,\upsilon})_{t=1}^{l},$$

$$(\eta_1,\eta_2,\cdots,\eta_l)):\prod_{t=1}^{l}\frac{e_t^{\upsilon^{t-1}}}{\tilde{T}'}=\bar{h}^{r'}\wedge$$

$$\left\{e_t=\bar{g}^{x_t}\bar{h}^{r_t}\wedge e_{t,2}=e_{t,1}^{x_t}\bar{h}^{r_{t,2}}\wedge\cdots\wedge e_{t,\upsilon}=e_{t,\upsilon-1}^{x_t}\bar{h}^{r_{t,\upsilon}}\right\}_{t=1}^{l}\wedge$$

$$(u_1=\bar{h}^{\eta_1}\vee u_2=\bar{h}^{\eta_2}\vee\cdots\vee u_l=\bar{h}^{\eta_l})\}(id_V\|n_V)$$

其中，$r'=\sum_{t=1}^{l}r_t\upsilon^{t-1}-r \bmod p,\eta_t=\sum_{i=1}^{\upsilon}a_iR_{t,i}$，$u_t=\prod_{i=0}^{\upsilon}e_{t,i}^{a_i},e_{t,1}=e_t,e_{t,0}=\bar{g},t=1,\cdots,l$。

① host 选取 $\rho_{r'}\in_R\mathbb{Z}_p$，计算 $\bar{R}=\bar{h}^{\rho_{r'}}$。对于 $t=1,\cdots,l$，选取 $\rho_{x_t},\rho_{r_t},\rho_{r_{t,2}},\cdots,\rho_{r_{t,\upsilon}}\in_R\mathbb{Z}_p$，计算 $\bar{R}_t=\bar{g}^{\rho_{x_t}}\bar{h}^{\rho_{r_t}},\bar{R}_{t,2}=e_{t,1}^{\rho_{x_t}}\bar{h}^{\rho_{r_{t,2}}},\cdots,\bar{R}_{t,\upsilon}=e_{t,\upsilon-1}^{\rho_{x_t}}\bar{h}^{\rho_{\eta,\upsilon}}$，选取 $\rho_{\eta_1},\xi_{\eta_2},\cdots,\xi_{\eta_l}\in_R\mathbb{Z}_p,\tilde{c}_2,\cdots,\tilde{c}_l\in_R\mathbb{Z}_p$，计算 $\tilde{R}_1=\bar{h}^{\rho_{\eta_1}}$，$\tilde{R}_i=\bar{h}^{\xi_{\eta_i}}u_i^{-\tilde{c}_i},i=2,\cdots,l$。

② host 计算 $c_h=H_3(Fed_{pk}\|\tilde{T}'\|(e_t\|e_{t,2}\|\cdots\|e_{t,\upsilon})_{t=1}^{l}\|u_1\|\cdots\|u_l\|\bar{R}\|(\bar{R}_t\|\bar{R}_{t,2}\|\cdots\|\bar{R}_{t,\upsilon})_{t=1}^{l}\|\tilde{R}_1\|\cdots\|\tilde{R}_l\|id_V\|n_V)$，并向 TPM 发送 c_h。

③ TPM 选取 $n_T\in_R\{0,1\}^{\lambda}$，向 host 返回 $c=H_4(c_h\|n_T\|ob_i)$，host 在 $\mathbb{Z}_p$ 上计算 $\xi_{r'}=\rho_{r'}+cr'$。

对于 $t=1,\cdots,l$，host 计算 $\xi_{x_t}=\rho_{x_t}+cx_t,\xi_{r_t}=\rho_{r_t}+cr_t,\xi_{r_{t,2}}=\rho_{r_{t,2}}+cr_{t,2},\cdots,\xi_{r_{t,\upsilon}}=\rho_{r_{t,\upsilon}}+cr_{t,\upsilon}$。host 计算 $\tilde{c}_1=c-\sum_{i=2}^{l}\tilde{c}_i \bmod p$，并且在 $\mathbb{Z}_p$ 上计算 $\xi_{\eta_1}=\rho_{\eta_1}+\tilde{c}_1\eta_1$。

④ host 输出 $(\tilde{T}',(e_t,e_{t,2},\cdots,e_{t,\upsilon})_{t=1}^{l},c,\tilde{c}_1,\cdots,\tilde{c}_l,\xi_{r'},(\xi_{x_t},\xi_{r_t},\xi_{r_{t,2}},\cdots,\xi_{r_{t,\upsilon}})_{t=1}^{l},\xi_{\eta_1},\cdots,\xi_{\eta_l})$。

π_2 的验证过程如下。

1) 验证是否满足 $\tilde{T}',(e_t,e_{t,2},\cdots,e_{t,\upsilon})_{t=1}^{l}\in G_1$ 以及 $\tilde{c}_1,\cdots,\tilde{c}_l,\xi_{r'},(\xi_{x_t},\xi_{r_t},\xi_{r_{t,2}},\cdots,\xi_{r_{t,\upsilon}})_{t=1}^{l},\xi_{\eta_1},\cdots,\xi_{\eta_l}\in\mathbb{Z}_p$。

2) 采用 π_2 产生过程中的方式计算系数 $(a_0,\cdots,a_\upsilon)$。对于 $t=1,\cdots,l$，计算 $u_t=\prod_{i=0}^{\upsilon}e_{t,i}^{a_i}$。计算 $\hat{\bar{R}}=\bar{h}^{\xi_{r'}}(\prod_{t=1}^{l}\frac{e_t^{\upsilon^{t-1}}}{\tilde{T}'})^{-c}$，$(\hat{\bar{R}}_t=\bar{g}^{\xi_{x_t}}\bar{h}^{\xi_{\eta_t}}e_t^{-c},\ \hat{\bar{R}}_{t,2}=e_{t,1}^{\xi_{x_t}}\bar{h}^{\xi_{r_t,2}}e_{t,2}^{-c},\cdots,\hat{\bar{R}}_{t,\upsilon}=e_{t,\upsilon-1}^{\xi_{x_t}}\bar{h}^{\xi_{r_t,\upsilon}}e_{t,\upsilon}^{-c})_{t=1}^{l},\hat{\bar{R}}_1=\bar{h}^{\xi_{\eta_1}}u_1^{-\tilde{c}_1},\cdots,\ \hat{\bar{R}}_l=\bar{h}^{\xi_{\eta_l}}u_l^{-\tilde{c}_l}$。验证是否满足 $c=H_4(H_3(Fed_{pk}\|\tilde{T}'\|(e_t\|e_{t,2}\|\cdots\|e_{t,\upsilon})_{t=1}^{l}\|u_1\|\cdots\|u_l\|\hat{\bar{R}}\|\ (\hat{\bar{R}}_t\|\ \hat{\bar{R}}_{t,2}\|\cdots\|\hat{\bar{R}}_{t,\upsilon})_{t=1}^{l}\|\hat{\bar{R}}_1\|\cdots\|\hat{\bar{R}}_l\|id_V\|n_V)\|n_T\|ob_i)$。

5.3 子签名 π_1 与 π_2 的合成

知识签名 π 是通过对子签名 π_1、π_2 执行并行合成而得到的。最终的合成结果为

$$\pi=(S,B,K,T,\tilde{T},\{T_i\}_{i=1}^{n},A',A'',M',n_T,$$

$$\tilde{T}',(e_t,e_{t,2},\cdots,e_{t,\upsilon})_{t=1}^{l},c,\tilde{c}_1,\cdots,\tilde{c}_l,\xi_{sk},\cdots,\xi_{s\cdot f},\xi_{r'},$$

$$(\xi_{x_t},\xi_{r_t},\xi_{r_{t,2}},\cdots,\xi_{r_{t,\upsilon}})_{t=1}^{l},\xi_{\eta_1},\cdots,\xi_{\eta_l})$$

在验证过程中，验证者需要根据 5.1 节和 5.2 节的方式计算 $\hat{R}_1,\cdots,\hat{R}_7,\hat{\bar{R}},(\hat{\bar{R}}_t,\hat{\bar{R}}_{t,2},\cdots,\hat{\bar{R}}_{t,\upsilon})_{t=1}^{l},\hat{\bar{R}}_1,\cdots,\hat{\bar{R}}_l$，且最终的验证等式为

$$c=H_4(H_3(Fed_{pk}\|S\|B\|K\|T\|\tilde{T}\|\{T_i\}_{i=1}^{n}\|A'\|A''\|M'\|\hat{R}_1\|\cdots\|\hat{R}_7\|\tilde{T}'\|(e_t\|e_{t,2}\|\cdots\|e_{t,\upsilon})_{t=1}^{l}\|u_1\|\cdots\|u_l\|\hat{\bar{R}}\|\ (\hat{\bar{R}}_t\|\ \hat{\bar{R}}_{t,2}\|\cdots\|\hat{\bar{R}}_{t,\upsilon})_{t=1}^{l}\|\hat{\bar{R}}_1\|\cdots\|\hat{\bar{R}}_l\|id_V\|n_V)\|n_T\|ob_i)$$

6 安全性分析

定理 1 若群对 (G_1,G_2) 上的 q-SDH 假设，群 $\tilde{G}$ 上的 y-DDHI 假设以及群 G_1 上的 DDH 假设都成立，则本文系统在 2.2 节定义的多商家 MCS 模型下满足可证安全。

证明 限于篇幅，省略了正确性的证明过程。

1) 不可伪造性。当前实验分为以下 2 个模式。

① 模式 1。B 以某个 BBS+签名方案的实例 $(G_1,G_2,G_T,p,\hat{e},\{g_i\}_{i=0}^{n+3},h_0,w)$ 作为输入，B 设置 $w_I=w$，并且采用 Setup 算法中的方式产生 Fed_{pk} 中的剩余参数。需要指出的是，B 并不掌握 I 的私钥 γ_I。B 定义计数器 $CtrD_{ob_i},i=1,\cdots,n$，用于统计“由 I 发布且含有对象 ob_i 的”息票数量与“已经得到兑换的由 I 发布且含有对象 ob_i 的”息票数量之差。B 设置列表 Reg，用于保存用户注册信息。在 Reg 的每个表目中，B 用标识位 c 表示该用户是否被攻破（c=1 表示已经被攻破，c=0 表示未被攻破）。在实验执行过程中，B 为 Adv 提供以下的预言服务。

散列询问：根据文献[16]的结论，无需将散列函数 H_1、H_3 视为随机预言机，因为它们都是内部函数。因此，B 只需提供对函数 H_2、H_4 的模拟，即对于 Adv 提出的询问，B 返回在 $\mathbb{Z}_p$ 上随机选取的元素作为应答，同时确保所提供的应答满足一致性。

Issue 询问：当接收到 Adv 的询问内容 $(U_i,J_1,\cdots,J_n)$，B 通过对 Adv 执行重绕操作而提取出 Adv 的秘密知识 sk、mid，并且借助 BBS+方案签名预言机 $O_{\mathrm{BBS+}}(\gamma)$ 产生相应的证书 $cre=(A,e,s)$。

对于 $i=1,\cdots,n$，B 设置 $CtrD_{ob_i}\leftarrow CtrD_{ob_i}+J_i, Reg\leftarrow Reg\cup\{(U_i,sk,mid,F_1,F_2,cre,c=1)\}, BL\leftarrow BL\cup\{sk\}$。

Semi-Issue 询问：当接收到 Adv 的询问内容 $(U_i,J_1,\cdots,J_n)$，B 选取 $sk,mid\in_R\mathbb{Z}_p$，借助 $O_{\text{BBS+}}(\gamma)$ 产生 $cre=(A,e,s)$，并且向 Adv 提供 mid,cre。对于 $i=1,\cdots,n$，B 设置 $CtrD_{ob_i}\leftarrow CtrD_{ob_i}+J_i, Reg\leftarrow Reg\cup\{(U_i,sk,mid,F_1,F_2,cre,c=0)\}$。

Redeem 询问：当接收到 Adv 提出的询问 (V,ob_i)，B 以 V 的身份与 Adv 执行 Redeem 协议，从而获得由 Adv 提供的有效知识签名 $\pi=(S,B,K,\cdots,c,\tilde{c}_1,\cdots,\tilde{c}_l,\xi_{sk},\cdots,\xi_{\eta_1},\cdots,\xi_{\eta_l})$。此时，$B$ 通过对 Adv 执行重绕而获得另一个有效知识签名 $\pi'=(S,B,K,\cdots,c',\tilde{c}'_1,\cdots,\tilde{c}'_l,\xi'_{sk},\cdots,\xi'_{\eta_1},\cdots,\xi'_{\eta_l})$。利用标准的知识提取技术，可以从 π 与 π' 中提取出秘密知识 $sk^*,s^*,j^*,r_s^*,r_j^*,\{J_i^*\}_{i=1}^n,\{r_{J_i}^*\}_{i=1}^n,e^*,f^*,mid^*\cdot f^*$ 满足

$$K=B^{sk^*},\frac{\tilde{g}_{i+2}}{S}=S^{s^*+j^*},T=\bar{g}^{s^*}\bar{h}^{r_s^*},$$
$$\tilde{T}=\bar{g}^{j^*}\bar{h}^{r_j^*},\{T_i=\bar{g}^{J_i^*}\bar{h}^{r_{J_i}^*}\}_{i=1}^n,A''=A'^{e^*},$$
$$M'=g_0^{f^*}g_1^{sk^*\cdot f^*}g_2^{mid^*f^*}g_3^{J_1^*f^*}\cdots g_{n+2}^{J_n^*f^*}g_{n+3}^{s^*f^*}$$

显然

$$\hat{e}(A',w_I)=\hat{e}(M'A''^{-1},h_0)$$
$$\Leftrightarrow\hat{e}(A',w_I)\ \hat{e}(A'^{e^*},h_0)$$
$$=\hat{e}(g_0^{f^*}g_1^{sk^*f^*}g_2^{mid^*f^*}g_3^{J_1^*f^*}\cdots g_{n+2}^{J_n^*f^*}g_{n+3}^{s^*f^*},h_0)$$

由 $A'\neq 1\in G_1$，可以确保 $f^*\neq 0 \bmod p$。于是，可以提取出秘密知识 $A^*=A'^{(f^*)^{-1}}$，$mid^*=mid^*\cdot f^*(f^*)^{-1}$，使 $\hat{e}(A^*,w_I h_0^{e^*})=\hat{e}(g_0g_1^{sk^*}g_2^{mid^*}g_3^{J_1^*}\cdots g_{n+2}^{J_n^*}g_{n+3}^{s^*},h_0)$。显然，$(A^*,e^*,s^*)$ 构成关于 $(sk^*,mid^*,J_1^*,\cdots,J_n^*)$ 的 BBS+签名。

在 Redeem 询问的末尾，B 设置 $CtrD_{ob_i}\leftarrow CtrD_{ob_i}-1$，检查是否满足 $(A^*,e^*,s^*)\in Reg$。

Semi-Redeem 询问：当接收到 Adv 提出的询问 (V,ob_i)，B 以 TPM 的身份与 Adv 联合执行 Redeem 协议，即采用 5.1 节中的做法为 Adv 提供元组 $(B,K,R_1,R_{7t},R,f,c,n_T,\xi_{sk},\xi_{sk\cdot f})$。

Corrupt 询问：当 Adv 请求攻破用户 U_i，若 U_i 在 Reg 的对应表目中的标识位满足 $c=0$，则 B 向 Adv 返回 U_i 的私钥 sk_i，设置 $c=1, BL\leftarrow BL\cup\{sk_i\}$。

Adv 在当前实验中获胜的条件是 $\exists i\in[1,n]$，使 $CtrD_{ob_i}<0$。根据底层区间证明协议[25]的可靠性以及伪随机函数[26]的抗碰撞性，Adv 不可能实现对 MC 的透支使用，也不可能利用使用过的重复检测标签 S 执行兑换而不被发觉。因此，若 Adv 在实验中获胜，则它必然在某次兑换过程中成功实现了对 BBS+签名方案实例的伪造攻击。于是，B 可以利用上述的重绕技术提取出关于秘密元组 $(sk^{**},mid^{**},J_1^{**},\cdots,J_n^{**})$ 的 BBS+方案签名 $(A^{**},e^{**},s^{**})\notin Reg$ 且 $sk^{**}\notin BL$，即违背了 q-SDH 假设。

② 模式 2。B 执行当前实验模式 2 下的初始化操作，并且定义计数器 Ctr_R。在当前实验中，B 为 Adv 提供以下的预言服务。

散列询问：描述方式同模式 1。

Issue 询问：当 Adv 请求为 U 发布一张 MC，则 B 自行模拟 I 与 U 执行 Issue 协议的过程。

Redeem 询问：当 Adv 要求为用户 U 兑换一张对象为 ob_i 的息票，B 以 U 的身份与 Adv 执行 Redeem 协议。若该协议执行成功，则 B 设置 $Ctr_R\leftarrow Ctr_R+1$。

最终，Adv 输出由 Redeem 协议副本构成的列表 L_{trans}，若 L_{trans} 中的每个副本都能通过 Claim 协议的验证过程且满足 $|L_{trans}|>Ctr_R$，则表明 $\exists(id_V^*,n_{V^*},S^*,ob^*,\pi^*,receipt^*)\in L_{trans}$，且该副本并非通过与 B 执行 Redeem 协议而获得的。此时，B 对 Adv 执行重绕，必然能从 π^* 中提取出关于秘密元组 $(sk^*,mid^*,J_1^*,\cdots,J_n^*)$ 的 BBS+方案签名 (A^*,e^*,s^*)，即违背了 q-SDH 假设。

2) 无关联性。在当前实验中，B 以四元组 $(u,v=u^a,w=u^b,z)\in G_1^4$ 作为输入，其中，$a,b\in\mathbb{Z}_p$。B 执行无关联性实验的初始化操作。在该过程中，对于 Fed_{pk} 中的参数 g_1，B 设置 $g_1=u$。B 选取 $i^*\in_R\{1,\cdots,N\}$，其中，N 表示当前实验中的最大用户数量。此外，B 设置列表 Reg，用于保存用户注册信息。同时，B 为每个诚实用户 U_i 定义如下的数据结构。Ctr_{U_i} 用于存储 U_i 获得的 MC 的数量。CL_{U_i} 为二维数组，其中，$CL_{U_i}[i',j']=1$ 表示 U_i 的第 i' 张 MC 中的第 j' 张息票尚未得到兑换，$CL_{U_i}[i',j']=0$ 表示已经得到兑换。OL_{U_i} 为二维数组，其中，$OL_{U_i}[i',j']$ 表示 U_i 的第 i' 张 MC 中的第 j' 张息票的息票对象。在实验执行过程中，B 为 Adv 提供以下的预言服务。

散列询问：描述过程同不可伪造性实验（模式 1）。

Issue 询问：当接收到 Adv 的询问内容 $(U_i, J_1, \cdots, J_n)$，B 分以下 2 种情况进行处理。

情况 1：若满足 $i = i^*$，B 设置 $F_1 = v$ 且自己并不掌握 $sk = \log_u v$。B 采用以下方式模拟 Issue 协议，即选取 $F_2 \in_R G_1$，选取 $c, \xi_{sk}, \xi_{mid} \in_R \mathbb{Z}_p$，计算 $R_1 = g_1^{\xi_{sk}} F_1^{-c}, R_2 = g_2^{\xi_{mid}} F_2^{-c}$，设置 $c = H_2(Fed_{pk} \| n_{\bar{I}} \| F_1 \| F_2 \| R_1 \| R_2)$。

情况 2：若满足 $i \neq i^*$，B 以诚实方式与 $\bar{I}$ 执行 Issue 协议。

无论属于哪种情况，当 Issue 协议结束后，B 均需执行以下操作。

① 对于 $j' = 1, \cdots, J_1 + J_2 + \cdots + J_n$，设置 $CL_{U_i}[Ctr_{U_i}, j'] \leftarrow 1$。

② 对于 $j' = 1, \cdots, J_1$，设置 $OL_{U_i}[Ctr_{U_i}, j'] \leftarrow ob_1$。对于 $j' = J_1 + 1, \cdots, J_2$，设置 $OL_{U_i}[Ctr_{U_i}, j'] \leftarrow ob_2$。以此类推，直至对于 $j' = J_1 + \cdots + J_{n-1} + 1, \cdots, J_n$，设置 $OL_{U_i}[Ctr_{U_i}, j'] \leftarrow ob_n$。

③ 设置 $Ctr_{U_i} \leftarrow Ctr_{U_i} + 1$。

④ 若 $i = i^*$，则设置 $Reg \leftarrow Reg \cup \{(U_i, *, *, F_1, F_2, cre, c = 0)\}$，其中，符号“*”表示未知元素。否则，设置 $Reg \leftarrow Reg \cup \{(U_i, sk, mid, F_1, F_2, cre, c = 0)\}$。

Redeem 询问：当接收到 Adv 提出的询问 $(U_i, \alpha, \beta, \bar{V})$，$B$ 首先根据 U_i 在列表 Reg 的对应表目中的标识位检查 U_i 是否尚未被攻破且满足 $CL_{U_i}[\alpha, \beta] = 1$，若是，$B$ 分以下 2 种情况进行处理。

情况 1：若满足 $i = i^*$，则 B 采用模拟方式产生知识签名 π。

情况 2：若 $i \neq i^*$，则 B 以诚实方式产生知识签名 π。

无论属于哪种情况，当 Redeem 协议结束后，B 均需设置 $CL_{U_i}[\alpha, \beta] = 0$。

Corrupt 询问：当 Adv 请求攻破用户 U_i，若 $i = i^*$，则 B 运行失败；否则，B 采用不可伪造性实验（模式 1）中的方式模拟当前询问。

在挑战阶段，当 Adv 输出 $(U_0, U_1, \alpha_0, \beta_0, \alpha_1, \beta_1, \bar{V})$，$B$ 检查是否同时满足以下条件：① U_0、U_1 均未被攻破；② $CL_{U_0}[\alpha_0, \beta_0] = CL_{U_1}[\alpha_1, \beta_1] = 1$；③ $OL_{U_0}[\alpha_0, \beta_0] = OL_{U_1}[\alpha_1, \beta_1]$；④ $U_{i^*} \in \{U_0, U_1\}$。若不满足，则 B 运行失败。否则，B 选取 $c \in_R \{0,1\}$，使 $U_c = U_{i^*}$，并且执行以下步骤。

① B 以 U_c 的身份与 $\bar{V}$ 执行 Redeem 协议，并且在该协议中向 $\bar{V}$ 兑换第 α_0 张 MC 中的第 β_0 张息票。在该协议中，B 选取 $r \in_R \mathbb{Z}_p$，设置 $B = w^r, K = z^r$，且采用当前实验 Redeem 询问中的技术模拟产生知识签名 π。

② B 以 U_{1-c} 的身份与 $\bar{V}$ 执行 Redeem 协议，并且在该协议中向 $\bar{V}$ 兑换第 α_1 张 MC 中的第 β_1 张息票。在该协议中，B 以诚实方式产生知识签名 π。

最终，Adv 输出对挑战比特 c 的猜测结果 b。若满足 $b = c$，则 B 判定 z 为群 G_1 上的随机元素，否则，B 判定 $z = u^{ab}$ 成立，从而攻破了群 G_1 上的 DDH 假设。

注意，Adv 同样无法在当前实验中借助 U_0, U_1 在兑换过程中产生的重复检测标签 S 对它们进行分辨。因为，根据文献[13]结论，在群 $\tilde{G}$ 上的 y-DDHI 假设下，元素 S 与 $\tilde{G}$ 上的随机元素是不可分辨的。

综上得出，在 $\tilde{G}$ 上的 y-DDHI 假设和 G_1 上的 DDH 假设下，Adv 仅能以可忽略的概率获胜。

3) 可声明性。B 执行可声明性实验的初始化操作，并且采用可声明性实验中定义的方式回答 Adv 提出的散列询问和 Redeem 询问。由于 Claim 算法中的验证操作是 V 在 Redeem 协议中执行的验证操作的子集，因此，Adv 将无法在该实验中获胜。

4) 不可分割性。B 执行不可分割性实验的初始化操作。此外，B 创建计数器 $CtrD_i, i = 1, \cdots, N$，该计数器的取值代表了第 i 张 MC 的剩余价值，其中 N 表示 Adv 提出的 Issue 询问次数上界。B 创建一维数组 $\overline{MC}$，其中，$\overline{MC}[i]$ 用于存储为 Adv 发布的第 i 张 MC。在实验中，B 为 Adv 提供以下的预言服务。

散列询问：描述过程同不可伪造性实验（模式 1）。

Issue 询问：假设 B 已经为 Adv 发布了 $i-1$ 张 MC。当 Adv 提出询问 $(J_1, \cdots, J_n)$，B 利用重绕技术提取出秘密知识 sk, mid_i，B 为 Adv 产生 $cre_i = (A_i, e_i, s_i)$。B 设置 $\overline{MC}[i] \leftarrow (sk, mid_i, J_1, \cdots, J_n, cre_i)$, $CtrD_i \leftarrow CtrD_i + (J_1 + \cdots + J_n), BL \leftarrow BL \cup \{sk\}$。

Semi-Issue 询问：假设 B 已经为 Adv 发布了 $i-1$ 张 MC。当 Adv 提出询问 $(J_1, \cdots, J_n)$，B 自行选取 $sk, mid_i \in_R \mathbb{Z}_p$，为 Adv 产生 $cre_i = (A_i, e_i, s_i)$。B 设置 $\overline{MC}[i] \leftarrow (sk, mid_i, J_1, \cdots, J_n, cre_i)$，$CtrD_i \leftarrow$

$CtrD_i + (J_1 + \cdots + J_n)$。

Redeem 询问：B 以 V 的身份与 Adv 执行 Redeem 协议，并且通过对 Adv 执行重绕而提取出秘密知识 $(sk, mid, J_1, \cdots, J_n, A, e, s)$。$B$ 根据 mid 在数组 $\overline{MC}$ 中进行查找而判定 Adv 使用的是哪张 MC。假设满足 $mid \in \overline{MC}[i]$。B 设置 $CtrD_i \leftarrow CtrD_i - 1$。

Semi-Redeem 询问：B 的模拟过程同不可伪造性实验（模式 1）。

最终，Adv 输出某张 MC^* 的序列号 mid^*，满足 $mid^* \in \overline{MC}[i^*]$，$B$ 根据计数器 $CtrD_{i^*}$ 的取值而判定 MC^* 的剩余价值是否大于零。若是，则 B 以 $\overline{MC}[i^*]$ 为输入执行 Redeem 协议。显然，该协议总是能执行成功。由于用户 $\overline{U}$ 因满足 $sk \in BL$ 而无法通过 Redeem 协议的验证过程，同时用户 $\overline{\overline{U}}$ 的 host 部分不掌握 TPM 私钥，因而无法实现对 MC^* 的分割使用，即 Adv 将无法在当前实验中获胜。

尽管对委托运算协议[14,15]有利于减轻用户的运算负担，但是在现实应用中无法确保提供委托运算服务的服务器一定保持诚实。由于对 Φ 的调用发生在用户端 host 对证书 $cre = (A, e, s)$ 进行验证的环节，因此，需要对定理 1 证明过程中涉及“由归约算法 B 充当诚实用户且由攻击者 Adv 充当恶意参与方”的攻击场景进行重新讨论，即需要对不可伪造性实验（模式 2）和无关联性实验进行重新讨论。同时，在本节假设 Adv 总是与提供对运算服务的恶意服务器（记为 $\overline{S}$）进行合谋。

引理 1　在不可伪造性实验（模式 2）中，即使攻击者 Adv 与恶意服务器 $\overline{S}$ 进行合谋，也无助于它在该实验中获胜。

证明　除了定理 1 中描述的执行过程，当前实验还可以以下方式执行。B 设置列表 L_{cre}，用于保存以诚实方式产生的用户证书。在实验执行过程中，B 为 Adv 提供以下的预言服务。

Sign 询问：当接收到 Adv 提出的询问 $(F_1, F_2, J_1, \cdots, J_n)$，$B$ 借助 $O_{\text{BBS+}}(\gamma)$ 为 Adv 产生证书 $cre = (A, e, s)$。B 设置 $L_{cre} \leftarrow L_{cre} \cup \{(A, e, s)\}$。

AidedVerify 询问：当接收到 Adv 的询问 $(F_1, mid, J_1, \cdots, J_n, (A, e, s))$，$B$ 设置 $C_1 = A, C_2 = w_I h_0^e$，$C_3 = g_0 F_1 g_2^{mid} g_3^{J_1} \cdots g_{n+2}^{J_n} g_{n+3}^{s}, C_4 = h_0$，将对运算的任务 $\hat{e}(C_1, C_2), \hat{e}(C_3, C_4)$ 委托给 Adv，并获得委托运算结果 $\Phi(C_1, C_2)$、$\Phi(C_3, C_4)$。

最终，Adv 输出关于元组 $(sk^*, mid^*, J_1^*, \cdots, J_n^*)$ 的 BBS+签名 (A^*, e^*, s^*)，使 $(A^*, e^*, s^*) \notin L_{cre}$。$B$ 设置 $C_1^* = A^*, C_2^* = w_I h_0^{e^*}$，$C_3^* = g_0 g_1^{sk^*} g_2^{mid^*} g_3^{J_1^*} \cdots g_{n+2}^{J_n^*} g_{n+3}^{s^*}$，$C_4^* = h_0$，并验证是否满足 $\Phi(C_1^*, C_2^*) = \Phi(C_3^*, C_4^*)$。若满足，则可以归结为以下 2 种情况：①$(A^*, e^*, s^*)$ 为关于元组 $(sk^*, mid^*, J_1^*, \cdots, J_n^*)$ 的有效 BBS+签名，表明 B 借助该签名攻破了底层 BBS+方案的不可伪造性；②(A^*, e^*, s^*) 并非关于 $(sk^*, mid^*, J_1^*, \cdots, J_n^*)$ 的有效 BBS+签名，此时满足 $\hat{e}(C_1, C_2) \neq \hat{e}(C_3, C_4)$ 且 $\Phi(C_1, C_2) = \Phi(C_3, C_4)$。显然，$B$ 此时借助 Adv 攻破了底层协议 Φ 的完备性。

采用类似的技术，可以证明以下 3 个引理。

引理 2　在不可伪造性实验（模式 2）中，即使攻击者 Adv 与恶意服务器 $\overline{S}$ 进行合谋，也无法使诚实用户接受错误的委托运算结果。

引理 3　在无关联性实验中，即使攻击者 Adv 与恶意服务器 $\overline{S}$ 进行合谋，也无法使诚实用户在服务器辅助验证和标准验证 2 种模式下获得不一致的验证结果。

引理 4　在无关联性实验中，即使攻击者 Adv 与恶意服务器 $\overline{S}$ 进行合谋，也无法实现对诚实用户进行分辨。

定理 2　只要底层 BBS+签名方案在适应性选择消息攻击下满足存在的不可伪造性，同时底层对委托运算协议 Φ 满足完备性、可验证性和保密性，则在引入底层协议 Φ 后，本文 MCS 仍然是安全的。

证明　在不可伪造性实验（模式 2）和无关联性实验中，归约算法 B 以诚实用户身份与 Adv 和恶意服务器 $\overline{S}$ 的联合进行交互。尽管 B 在执行交互过程中需要将对运算的任务委托给 $\overline{S}$，但引理 1~引理 4 表明，委托运算过程并不会有助于 Adv 在这 2 个实验中获胜。综上得出，在引入底层对委托运算协议 Φ 后，本文 MCS 仍然是安全的。

7　本文系统的性能分析

表 2 为本文系统与已有系统的主要性质对比。在发布协议中，表 2 中的所有系统在本质上均要求用户与商家（或发布者）执行一次或多次盲签名协议。其中，文献[5,6]系统要求执行的盲签名轮次与 MC 的价值 k 呈线性关系，而其他系统仅需执行 1 次盲签名发布协议。在表 2 中，本文系统、文献[7]的方案 2 以及文献[9,12]系统均支持息票对象的概

表 2　本文系统与已有系统的主要性质比较

已有系统	发布协议复杂度	是否支持兑换不同类型服务	是否允许用户指定兑换次数	是否支持多商家环境	不可分割性质等级	不可分割性实现机制	匿名性等级
文献[3]	$O(1)$	否	否	否	弱	软件	强
文献[4]	$O(1)$	否	否	否	弱	软件	强
文献[5]	$O(k)$	否	是	否	强	软件	强
文献[6]	$O(k)$	否	是	是	强	软件	强
文献[7]方案 1	$O(1)$	否	是	否	强	软件	强
文献[7]方案 2	$O(1)$	是	是	否	强	软件	强
文献[8]方案 1	$O(1)$	否	是	否	强	软件	强
文献[8]方案 2	$O(1)$	否	是	否	强	软件	强
文献[9]	$O(1)$	是	是	是	弱	软件	弱
文献[12]	$O(1)$	是	是	否	—	—	强
本文	$O(1)$	是	是	是	最强	硬件	强

念，因而允许用户利用 1 张 *MC* 兑换多种类型的商品或服务，而其他的系统仅允许兑换一种类型的商品或服务。早期的系统[3,4]要求将 *MC* 的价值 k 作为系统的固定参数，因而影响了其实用性，此后的系统均支持用户与发布者（或商家）协商 k 的取值。需要指出的是，本文系统和文献[6,9]系统均考虑了多商家联合经营的模式，因此满足更好的客户友好性质。如前所述，文献[3~9]系统都是利用纯软件的方法来确保多重息票的不可分割性，本文系统则借助 TPM 芯片实现了最强的不可分割性。此外，文献[12]系统是目前唯一支持对多重息票进行分割使用的系统。在匿名性方面，文献[9]系统因构造过程使用了群签名技术而实现了最弱的匿名性。

表 3 和表 4 对本文系统与表 2 所列其他系统（文献[12]系统除外）进行了通信耗费和运算耗费的详细比较。所采用的具体方法如下。

1) 文献[3,5,6]系统都是在 RSA 群上构造的，本文选取了相同的安全参数[30]。文献[4]系统和本文系统都是在双线性群对 (G_1, G_2) 上构造的，本文同样选取了相同的参数。此外，文献[7~9]系统的构造过

表 3　本文系统与已有系统的通信耗费比较

方案	发布协议		兑换协议	
	用户	商家/发布者	用户	商家
文献[3]	26 528	2 528	1 343 424	0
文献[4]	651	491	3 790	0
文献[5]	166 400	129 088	25 888	2 528
文献[6]	161 408	137 088	32 864	2 528
文献[7]方案 1	13 750	982	14 510	0
文献[7]方案 2	15 190	982	8 413	0
文献[8]方案 1	1 793	822	16 683	0
文献[8]方案 2	17 418	7 003	174 109	5 464
文献[9]	18 848	3 072	29 794	160
本文	982	491	11 326	320

表 4　　本文系统与已有系统的运算耗费比较

方案	发布协议		兑换协议	
	用户	商家/发布者	用户	商家
文献[3]	$30Exp(G_1)$	$30Exp(G_1)$	$1\,010Exp(G_1)$	$500Exp(G_1)$
文献[4]	$P+22Exp(G_1)$	$3Exp(G_1)$	$2P+48Exp(G_1)$	$4P+34Exp(G_1)$
文献[5]	$1\,520Exp(G_1)$	$1\,520Exp(G_1)$	$130Exp(G_1)$	$120Exp(G_1)$
文献[6]	$1\,040Exp(G_1)$	$550Exp(G_1)$	$160Exp(G_1)$	$140Exp(G_1)$
文献[7]方案 1	$2P+96Exp(G_1)$	$50Exp(G_1)$	$6P+19Exp(G_1)$	$4P+21Exp(G_1)$
文献[7]方案 2	$2P+96Exp(G_1)$	$48Exp(G_1)$	$2P+42Exp(G_1)$	$2P+31Exp(G_1)$
文献[8]方案 1	$16P+5Exp(G_1)$	$13Exp(G_1)$	$63Exp(G_1)$	$16P+36Exp(G_1)$
文献[8]方案 2	$16P+127Exp(G_1)$	$144Exp(G_1)$	$956Exp(G_1)$	$17P+847Exp(G_1)$
文献[9]	—	$10Exp(G_1)$	$2P+34Exp(G_1)$	$2P+48Exp(G_1)$
本文	$2Exp(G_1)$ * $53Exp(G_1)$ **	$4Exp(G_1)$	$2Exp(G_1)$ * $51Exp(G_1)$ **	$2P+33Exp(G_1)$

程同时使用了 RSA 群与双线性群对 (G_1,G_2)。在比较中，本文用符号 $|G_1|$、$|G_T|$ 分别表示群 G_1 和目标群 G_T 上的元素长度，$|\mathbb{Z}_p|$ 表示有限域 $\mathbb{Z}_p$ 上的元素长度，$|\mathbb{Z}_n|$ 表示 RSA 群上的元素长度。根据文献[24]的结论，当在 MNT 曲线上实现群对 (G_1,G_2) 且以 80 bit 安全性为目标时，满足 $|G_1|=171$ bit, $|G_T|=1\,026$ bit, $|\mathbb{Z}_p|=160$ bit,$|\mathbb{Z}_n|=1\,024$ bit。

2) 在运算耗费的分析中，本文并未对多指数运算与单指数运算进行区分，因为在对指数运算过程进行优化的情况下，这 2 种运算的耗费是接近的[24]。用符号 P 表示执行 1 次对运算的耗费，用 $Exp(G_1)$、$Exp(G_2)$、$Exp(G_T)$ 和 $Exp(\mathbb{Z}_n)$ 分别表示在群 G_1、G_2、G_T 和 $\mathbb{Z}_n$ 上执行 1 次指数运算的耗费。可以做出如下的估算，即 $Exp(\mathbb{Z}_n)\approx Exp(G_T)=10Exp(G_1)$ [24]。此外，本文认为 $Exp(G_2)\approx Exp(G_T)$。在文献[7]系统中，用户和商家需要执行群 G_1 上指数长度为 30 bit 的小指数运算。根据“指数长度为 x bit 特的指数运算相当于$1.5x$ 次乘法”的结论[31]得出，1 次群 G_1 上的标准指数运算相当于 5 次此类的小指数运算。最终，本文将 G_1、G_2、G_T 和 $\mathbb{Z}_n$ 上的指数运算以及小指数运算都估算为 G_1 上的指数运算。

3) 在本文系统中，特定参数 n 表示 MC 支持兑换的服务类型种类，J_i 表示第 i 类对象的数量。为了便于比较，本文假设用户在所有系统中仅申请一种类型的服务，于是 $n=1$。同时，假设每张 MC 的价值均为 50。不失一般性，对于本文系统，假设满足 $J_1=50$。此外，在本文系统的息票兑换协议中，底层的区间证明协议要求在以 $\upsilon(\upsilon>2)$ 为底数的编码系统中对未使用过的息票序号 $j\in[1,J_1]$ 进行分解。在文献[7]系统中，同样要求在 $u(u>2)$ 进制下对 MC 的已兑换次数进行分解。此处选取 $\upsilon=u=4$。

4) 在本文系统的息票发布协议中，用户需要调用底层的对委托运算协议实现对 BBS+方案签名的服务器辅助验证。为此，本文使用了文献[15]中的 PVPV（public variable point and public variable point）类型协议。用户每次调用该协议的运算耗费约为 $Exp(G_1)+Exp(G_2)+Exp(G_T)$。

5) 在本文系统的 Issue 和 Redeem 协议中，发布者（或商家）还需要根据底层 DAA 方案的列表 BL 验证用户的 TPM 私钥是否因泄露而被废除，而参与比较的其他系统并未考虑这个问题。为了比较的公平，表 4 的运算耗费比较中并未统计执行此项检查的耗费。此外，用符号“*”和“**”对本文系统中 TPM 端和 host 端的运算耗费分别进行标记。

作为总结，本文系统实现了表 2 列举的所有重要性质。在通信耗费方面，本文系统仅次于最高效的文献[4]系统。在发布协议的运算耗费方面，本文系统接近于高效的文献[3,9]系统，且本文系统在兑换协议用户端的运算耗费方面是最高效的。

8 结束语

针对已有多重息票系统未能较好解决防止恶意用户对多重息票进行分割使用的现实问题，本文提出了基于 DAA 的轻量级多商家多重息票系统。相对于已有系统，本文系统不仅实现了支持兑换不同类型的服务、允许用户与发布者协商兑换次数和适合于多商家环境等实用性质，而且满足最强等级的不可分割性。此外，本文系统不要求用户执行任何的对运算，而且与 Pirker 等的移动支付框架相兼容。效率分析表明，本文系统在运算和通信耗费方面较已有系统具有明显优势。今后将进一步优化用户端（特别是 TPM）的运算效率，考虑所设计的系统与下一代 TPM 2.0 标准的兼容问题等。

参考文献：

[1] CHANG C C, SUN C Y. A secure and efficient authentication scheme for e-coupon systems[J]. Wireless Personal Communications, 2014, 77(4): 2981-2996.

[2] HSUEH S C, CHEN J M. Sharing secure m-coupons for peer-generated targeting via eWOM communications[J]. Electronic Commerce Research and Applications, 2010, 9(4): 283-293.

[3] CHEN L, ENZMANN M, SADEGHI A R, et al. A privacy-protecting coupon system[C]//The 9th International Conference on Financial Cryptography and Data Security. Roseau, 2005: 93-108.

[4] NGUYEN L. Privacy-protecting coupon system revisited[C]//The 10th International Conference on Financial Cryptography and Data Security. Anguilla, British West Indies, 2006: 266-280.

[5] CHEN L, ESCALANTE A, LÖHR H, et al. A privacy-protecting multi-coupon scheme with stronger protection against splitting[C]// The 11th International Conference on Financial Cryptography and Data Security. Scarborough, Trinidad and Tobago, 2008: 29-44.

[6] LÖHR H. Privacy-preserving protocols and applications for trusted platforms[D]. Bochum: Ruhr-Universit, 2012.

[7] 柳欣, 徐秋亮. 实用的强不可分割多重息票方案[J]. 计算机研究与发展, 2012,49(12): 2575-2590.
LIU X, XU Q L. Practical multi-coupon systems with strong unsplittability[J]. Journal of Computer Research and Development, 2012, 49(12): 2575-2590.

[8] 柳欣, 徐秋亮. 并发安全的紧凑多重息票方案[J].电子学报,2012, 40(5): 877-882.
LIU X, XU Q L. Compact multi-coupon systems with concurrent security[J]. Acta Electronica Sinica, 2012, 40(5):877-882.

[9] HINAREJOS M F, ISERN-DEYÀ A P, FERRER-GOMILA J L, et al. MC-2D: an efficient and scalable multicoupon scheme[J]. The Computer Journal, 2015, 58(4): 758-778.

[10] WANG W J, FENG D G, QIN Y, et al. ExBLACR: extending BLACR system[C]//The 19th Australasian Conference on Information Security and Privacy. Wollongong, NSW, Australia, 2014:397-412.

[11] XI L, FENG D G. FARB: fast anonymous reputation-based blacklisting without TTPs[C]//The 13th Workshop on Privacy in the Electronic Society. Scottsdale, Arizona, USA, 2014:139-148.

[12] CANARD S, GOUGET A, HUFSCHMITT E. A handy multi-coupon system[C]//The 4th International Conference Applied Cryptography and Network Security. Singapore, 2006: 66-81.

[13] ISERNS-DEYÀ A P, HUGUET-ROTGER L, PAYERAS-CAPELLÀ M M, et al. On the practicability of using group signatures on mobile devices: implementation and performance analysis on the android platform[J]. International Journal of Information Security, 2014,(8): 1-11.

[14] CHOW S S M, AU M H, SUSILO W. Server-aided signatures verification secure against collusion attack[J]. Information Security Technical Report, 2013, 17(3): 46-57.

[15] CANARD S, DEVIGNE J, SANDERS O. Delegating a pairing can be both secure and efficient[C]//The 12th International Conference on Applied Cryptography and Network Security. Lausanne, Switzerland, 2014: 549-565.

[16] BRICKELL E, LI J T. A pairing-based DAA scheme further reducing TPM resources[C]//The 3rd International Conference on Trust and Trustworthy Computing. Berlin, Germany, 2010: 181-195.

[17] 杨波, 冯登国, 秦宇, 等. 基于可信移动平台的直接匿名证明方案研究[J]. 计算机研究与发展, 2014,51(7):1436-1445.
YANG B, FENG D G, QIN Y, et al. Research on direct anonymous attestation scheme on trusted mobile platform[J]. Journal of Computer Research and Development, 2014, 51(7): 1436-1445.

[18] CESENA E, LÖHR H, RAMUNNO G, et al. Anonymous authentication with TLS and DAA[C]//The 3rd International Conference on Trust and Trustworthy Computing. Berlin, Germany, 2010: 47-62.

[19] CHEN L. A DAA scheme requiring less TPM resources[C]//The 5th International Conference on Information Security and Cryptology. Beijing, China, 2010: 350-365.

[20] 张倩颖, 冯登国, 赵世军. 基于可信芯片的平台身份证明方案研究[J]. 通信学报,2014,35(8):95-106.
ZHANG Q Y, FENG D G, ZHAO S J. Research of platform identity attestation based on trusted chip[J]. Journal on Communications, 2014,35(8):95-106.

[21] BALDIMTSI F, LYSYANSKAYA A. Anonymous credentials light[C]//2013 ACM SIGSAC conference on Computer & Communications Security. Berlin, Germany, 2013:1087-1098.

[22] PIRKER M, SLAMANIG D. A framework for privacy-preserving mobile payment on security enhanced arm trustzone platforms[C]// Proceedings in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications. Liverpool, UK, 2012: 1155-1160.

[23] AU M H, SUSILO W, MU Y, et al. Constant-size dynamic k-times anonymous authentication[J]. IEEE Systems Journal, 2013, 7(2): 249-261.

[24] YANG Y, DING X, LU H, et al. Self-blindable credential: towards

lightweight anonymous entity authentication[EB/OL]. https://eprint.iacr.org/2013/207.pdf.

[25] PENG K, YI L. Studying a range proof technique-exception and optimization[C]//The 6th International Conference on Cryptology in Africa. Cairo, Egypt, 2013: 328-341.

[26] DODIS Y, YAMPOLSKIY A. A verifiable random function with short proofs and keys[C]//The 8th International Workshop on Theory and Practice in Public Key Cryptography. Les Diablerets, Switzerland, 2005: 416-431

[27] SCOTT M. Unbalancing pairing-based key exchange protocols[EB/OL]. https://eprint.iacr.org/2013/688.pdf.

[28] AU M H, SUSILO W, YIU S M. Event-oriented *k*-times revocable-iff-linked group signatures[C]//The 11th Australasian Conference on Information Security and Privacy. Melbourne, Australia, 2006: 223-234.

[29] PENG K. A general, flexible and efficient proof of inclusion and exclusion[C]//Cryptographers' Track at the RSA Conference 2011. San Francisco, CA, USA, 2011: 33-48.

[30] CAMENISCH J, LYSYANSKAYA A. A signature scheme with efficient protocols[C]//The 3rd International Conference on Security in Communication Networks. Amalfi, Italy, 2002: 268-289.

[31] 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.

作者简介：

柳欣（1978-），男，山东广饶人，博士，山东青年政治学院副教授，主要研究方向为密码学与信息安全。

徐秋亮（1960-），男，山东淄博人，山东大学教授、博士生导师，主要研究方向为密码学与信息安全。

张波（1981-），男，山东德州人，博士，济南大学讲师，主要研究方向为密码学与信息安全。