基于带智能卡的移动终端实现的隐私保护的属性票据方案

史瑞[1,2]，封化民[1,2]，谢惠琴[2]，史国振[2]，刘飚[2]，杨旸[3]

（1. 北京邮电大学网络空间安全学院，北京 100876；2. 北京电子科技学院，北京 100070；
3. 福州大学数学与计算机科学学院，福建 福州 350108）

摘 要：为了解决现有电子票据系统难以在资源受限设备中部署，以及无法防止票据在未授权设备之间共享的问题，提出了基于带智能卡的移动终端实现的隐私保护的属性票据方案。其中，智能卡为安全可信但资源受限的核心设备，负责存储密钥信息并处理轻量级的运算；智能终端为功能强大的辅助设备，负责处理与密钥无关但耗时的运算。首先，结合伪随机函数、匿名的临时身份方案、带随机化标签的可聚合签名和 Pointcheval-Sanders 签名，构造了一个可在带智能卡的移动终端部署的支持属性策略的电子票据方案；其次，给出了电子票据的安全模型并证明了所提方案满足不可链接性和不可伪造性；最后，在个人计算机、国产智能卡（爱信诺 ACH512）和智能手机（华为荣耀 9i）上实现了所提方案，对比和实验结果表明了所提方案的高效性。

关键词：电子票据；隐私保护；智能卡；智能手机；数字签名

中图分类号：TP309.2

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022156

Privacy-preserving attribute ticket scheme based on mobile terminal with smart card

SHI Rui[1,2], FENG Huamin[1,2], XIE Huiqin[2], SHI Guozhen[2], LIU Biao[2], YANG Yang[3]

1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Beijing Electronic Science and Technology Institute, Beijing 100070, China
3. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China

Abstract: To solve the problem that the existing electronic ticket systems are challenging to deploy in resource-constrained devices and cannot prevent the sharing of tickets among unauthorized devices, a privacy-preserving attribute ticket scheme based on mobile terminal with a smart card was proposed. The smart card was a secure and constrained-yet-trusted core device that holds secret information and performs lightweight operations. The mobile terminal was a powerful helper device that handles key-independent and time-consuming operations. Firstly, the efficient attribute-based ticket scheme deployed on the mobile terminal with a smart card was constructed by combining a pseudorandom function, anonymous ephemeral identities scheme, aggregatable signatures with randomizable tags, and Pointcheval-Sanders signatures. Secondly, the security model of the electronic tickets system was presented, and the proposed scheme was proved to be unlinkable and unforgeable. Finally, the proposed scheme was implemented on a personal computer, a smart card (Aisinochip ACH512), and a smart phone (Huawei Honor 9i), and the comparison and experimental results show that it is efficient.

Keywords: electronic ticket, privacy-preserving, smart card, smart phone, digital signature

收稿日期：2022−05−06；**修回日期：**2022−08−03

通信作者：王勇，yongwang@cqupt.edu.cn

基金项目：国家自然科学基金资助项目（No. 62101085）；重庆市教委科学技术研究基金资助项目（No. KJZD-K202000605）；重庆市研究生科研创新基金资助项目（No. CYS22473）

Foundation Items: The National Natural Science Foundation of China (No. 62101085), Science and Technology Research Program of Chongqing Municipal Education Commission (No.KJZD-K202000605), Chongqing Graduate Scientific Research Innovation Project (No.CYS22473)

0　引言

电子票据是用户属性信息、纸质票据和实体证件的电子化版本。随着智能移动终端（如智能手机、平板电脑）的普及和高速互联网络（如 5G、Wi-Fi）的应用，电子票据正逐步取代纸质票据和实体卡成为人们日常生活的必需品。例如，我国已经广泛使用电子医保卡代替实体医保卡就医，人们可在移动端完成挂号、取号和缴费等流程。在一些国家，航空、地铁和出入境票据的管理已全面电子化，人们可在手机上自助完成买票、检票和退票流程。此外，在购物、住宿、娱乐等领域，会员卡、年卡、优惠券和电影票等各种票据也已逐步电子化。

虽然关于电子票据的研究已有许多成果[1-17]，但是在移动应用场景中部署电子票据系统仍然面临着一些至今没有解决的问题。1) 无法将电子票据系统部署在资源受限的设备中（如智能卡）。智能卡设备由于功耗低、存储安全和携带方便等优点成为部署电子票据的最合适的平台。已有的属性票据方案[6,17]虽然可以在功能强大的设备（如个人计算机）中使用，但是这些方案使用了耗时的双线性映射运算，而目前标准的智能卡设备不支持这类运算，因此它们无法在轻量级设备中部署。2) 无法防止电子票据在未授权设备（用户）之间共享。在交通、购物、娱乐等商业领域中部署电子票据系统所带来的一个重要问题是无法阻止未付费（未授权）设备（用户）访问服务。解决这个问题的最直接方法是将票据的秘密信息存储在安全硬件设备中（如具有安全存储和防复制功能的智能卡），使没有安全硬件的参与就无法完成票据购买和消费协议。这不仅可以解决恶意用户不受限制地共享票据的问题，而且为诚实用户增加了额外的安全防护。

智能卡设备虽然有很多优点，但是其没有完整的电源和通信装置，因此需要借助外部辅助设备，通过接触或非接触方式才能完成读写和运算操作。因此，不依赖辅助设备而单独在智能卡上实现用户端的电子票据协议是不可能的。移动终端（如智能手机）由于部署面广、使用频率高、外部接口丰富、计算和通信效率高等优点是目前作为辅助设备的最优选择。这种以智能卡作为核心设备，移动终端作为辅助设备的模式已得到广泛应用。例如，在与银行的认证协议中，用户的硬件部分由 U 盾（智能卡）和智能手机（移动终端）组成，其中，U 盾是可信的并负责存储用户私钥和执行数字签名，智能手机负责执行账号管理和网络通信；银行在线转账的安全性由 U 盾保障而不依赖于智能手机，即使智能手机是恶意的也无法通过获取 U 盾中用户私钥的方式伪造转账。为了解决电子票据系统面临的上述问题，本文提出了一个基于带智能卡的移动终端（如带 U 盾的智能手机）部署的属性票据方案。

在本文的系统架构中，用户的硬件部分由一张资源受限但安全可信的智能卡和一部功能强大的移动终端组成。其核心思想是将智能卡作为用户的核心设备，存储用户的所有秘密信息，并执行与密钥有关但轻量化的运算；将移动终端作为用户的辅助设备，执行与密钥无关但耗时的运算；每个用户的智能卡唯一，而移动终端可以随时替换，且没有智能卡的参与移动终端无法完成任何协议。

本文给出了基于带智能卡的移动终端实现的属性票据方案的系统模型和安全模型，并结合伪随机函数、匿名的临时身份方案、带随机化标签的可聚合签名和 Pointcheval-Sanders（PS）签名提出了一个高效的构造实例，证明了所提方案满足不可伪造性和不可链接性的安全需求。

在所提方案的用户运算中，除了用户的注册验证和票据验证操作需要移动终端参与外，剩余的用户注册请求、票据购买请求和票据消费请求都可由智能卡单独完成，且移动终端参与的操作不需要任何用户秘密信息的参与。此外，用户的私钥和票据秘密信息不出卡，用户的身份、公钥、属性和证书等公开信息也可存储在智能卡中。因此，即使移动终端是恶意的，也无法在没有智能卡的参与下完成电子票据的任何协议。

所提方案支持基于属性泄露的购票策略，可在最小化信息泄露的原则下完成票据购买，最大程度地保护了用户隐私。例如，学生购买优惠票据时只需泄露“学生”属性，而学号、学院、住址、电话等敏感信息都应保密。与最新的属性票据方案[6,17]使用耗时的零知识证明和基于属性的随机化签名实现支持属性泄露策略的票据购买协议不同，所提方案使用一种聚合的方法构造用户属性证书，显著降低了票据购买算法的计算复杂度。

在票据购买协议中，智能卡发送完票据购买请求后，可能由于意外或恶意的行为导致其在没有收到卖方返回的票据验证信息的情况下被强制断电，

如智能卡从移动终端上被突然拔出或移动终端突然掉电。在这种情况下，即使智能卡重新上电，由于不能实时保存协议执行的上下文信息，将会导致用户购票失败。为了解决这个问题，在所提方案中使用带密钥的伪随机函数产生票据购买请求和卖方票据验证都需要的上下文信息。这意味着用户可以在智能卡上电后重新恢复上下文再验证票据的正确性。

通过与最新的属性票据方案[6,17]在个人计算机（华为 Matebook）上的实验对比，所提方案实现了最优的效率。通过在国产智能卡（爱信诺 ACH512）和智能手机（华为荣耀 9i）上的实验显示，所提方案完成一次票据购买算法需要在智能卡上消耗约 369 ms，在移动终端上消耗约 196 ms；完成一次票据消费算法只需要在智能卡上消耗约 197 ms。

Mut-Puigserver 等[1]按照功能需求（有效期、灵活性等）和安全需求（不可链接性、不可伪造性、传递性、不可双花等）将电子票据方案分为可传递票据[2-3]、不可传递票据[4]、一次性票据[2-5]和可多次使用的票据[1,4]。此外，Han 等[6]还提出了支持属性策略的电子票据。本文的研究内容是不可传递、一次性和支持属性策略的电子票据方案。

Fan 等[7]、Song 等[8]、Quercia 等[9]、Rupp 等[10]，以及 Milutinovice 等[4]分别利用不同的盲签名[11]提出了保护用户隐私的电子票据方案，但是他们的方案都不支持票据的不可传递性。Nakanishi 等[12]和 Vives-Guasch 等[13]分别使用不同的群签名[14]提出了电子票据方案，虽然他们的方案支持不可链接性和不可传递性，但是不支持属性策略。Heydt-Benjamin 等[3]和 Arfaoui 等[15]分别利用匿名证书[16]提出了电子票据方案，但是他们的方案不支持属性策略，也没有正式的安全证明。Han 等[6]使用随机化签名和零知识证明提出了首个支持属性策略的电子票据方案，但是该方案使用了大量的双线性对运算实现票据购买和票据消费算法，因此无法应用在智能卡设备中使用。封化民等[17]使用结构保持签名和可延展签名等提出了一个可转让的强隐私保护的属性票据方案，该方案首次在票据验证协议中同时实现了用户和卖方的匿名性，但是票据购买算法仍然需要 4 个双线性映射运算，因此无法在智能卡设备中部署。

Mostowski 等[18]在智能卡上实现了 U-prove 匿名证书方案；Camenisch 等[19]提出了一个适用于智能卡实现的带密钥验证的匿名证书方案；Verheul 等[20]提出了一个在智能卡上实现的可自盲化的匿名证书方案。这些不同类型的证书方案虽然可在智能卡上部署，但是它们都不是属性票据方案。Hanzlik 等[21]提出了一种在核心辅助环境下部署的匿名证书方案，该方案中用户由核心设备（如智能卡）和辅助设备（如智能手机组成）组成，为在移动环境下部署匿名证书提供了一种新的方法。

1 预备知识

1.1 双线性对

设 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ 是阶为素数 p 的循环群，g 和 $\tilde{g}$ 分别是 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 的生成元。TYPE-3 型双线性[22]映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 满足双线性、非退化性和可计算性，且 $\mathbb{G}_1$ 和 $\mathbb{G}_2$ 之间不存在同态映射。

1.2 零知识的知识签名

对于任意的多项式时间非确定性（NP, non-deterministic polynomial）关系 R，NP 语言 $L_R=\{y:\exists x,(x,y)\in R\}$ 的零知识的知识签名（ZKSoK, zero knowledge signature of knowledge）[23]定义为 $\pi=\mathrm{ZKSoK}\{x\mid(x,y)\in R\}(m)$。如果知识签名满足正确性、可模拟性和可提取性，则知识签名是模拟提取安全的。

1.3 平方离散对数假设

设 $\mathbb{G}$ 是阶为素数 p 的循环群，g' 是 $\mathbb{G}$ 的生成元。平方离散对数（SDL, square discrete logarithm）假设是指给定三元组 $(g',g'^{x},g'^{x^2})\in\mathbb{G}^3$，其中 $x\in\mathbb{Z}_p^*$，任意概率多项式时间（PPT, probabilistic polynomial time）敌手求解 x 的概率是可忽略的。

1.4 判定性平方 Diffie-Hellman 假设

设 $\mathbb{G}$ 是阶为素数 p 的循环群，g' 是 $\mathbb{G}$ 的生成元。判定性平方 Diffie-Hellman（DSqDH, decisional square diffie-hellman）假设[24]是指给定三元组 $(g',g'^{x},g'^{y})\in\mathbb{G}^3$，其中 $x,y\in\mathbb{Z}_p^*$，任意 PPT 敌手区分出下面 2 种情形的概率是可忽略的：$y=x^2$；y 从 $\mathbb{Z}_p^*$ 中随机选取。

1.5 伪随机函数

伪随机函数（PRF, pseudorandom function）由密钥生成和伪随机数生成 2 个算法组成。

1) 密钥生成：$\mathrm{PRF.KeyGen}(1^{\lambda})\to\mathrm{psk}$，产生一个密钥。

2) 伪随机数生成：对于一个有限的集合 $\mathbb{S}$ 和任

意字符串 $x \in \{0,1\}^*$，输出随机数 $y = \mathrm{PRF.Eval}_{\mathrm{psk}}(x)$，其中 $y \in \mathbb{S}$。

1.6　匿名的临时身份

匿名的临时身份（AET, anonymous ephemeral tag）方案[24]由初始化、标签生成、标签随机化、标签证明和标签验证算法组成。

1.7　带随机化标签的可聚合签名

带随机化标签的可聚合签名（ASRT, aggregatable signature with randomizable tag）[24]由初始化、密钥生成、签名、聚合并随机化签名和验签算法组成。在一般群模型下[25]，如果对每一个标签–索引对签名预言机只能被询问一次，那么带随机化标签的可聚合签名是不可伪造的。如果 DSqDH 问题是难解的，那么带随机化标签的可聚合签名是不可链接的。

1.8　Pointcheval-Sanders 签名

支持隐藏消息签发的 PS（Pointcheval-Sanders）签名[26]由初始化、密钥生成、签名协议和验签算法组成。在一般群模型下，PS 签名[26]在选择消息攻击模型下是不可伪造的。

2　系统模型和安全模型

2.1　系统架构

系统架构如图 1 所示。基于带智能卡的移动终端实现的隐私保护的属性票据方案由 4 类实体组成：证书中心（CA）、卖方（S）、用户（U）和验证方（V），用户的硬件部分由一张智能卡（如 U 盾）和一部移动终端设备（如智能手机）组成。智能卡存储用户的所有密钥信息并执行与密钥相关的运算，移动终端执行与密钥无关但耗时的运算。智能卡是安全可信的，敌手无法复制智能卡或从智能卡导出用户的秘密信息。移动终端是诚实但好奇的，一方面它诚实地与智能卡协作完成电子票据协议；另一方面它好奇用户的密钥和票据秘密信息。验证方维护一个只能添加的公开数据库用于存储已消费票据的标识。

方案的工作流程如下所述。

步骤 1　系统初始化。CA 执行系统初始化操作，产生系统公共参数、主公私钥对和一个票据策略集合。其中，系统公共参数、主公钥和票据策略集合公开，使其他参与实体可以获得。

步骤 2　卖方注册。2.1) S 产生卖方公私钥对，并向 CA 发起卖方注册请求；2.2) CA 验证 S 的请求后为 S 签发卖方证书；2.3) S 验证 CA 返回的卖方证书后将其保存在本地。

步骤 3　用户注册。3.1) U 的智能卡设备生成用户公私钥对（私钥不出卡），并通过移动终端设备的信道向 CA 发起注册请求；3.2) CA 验证 U 的注册请求后为 U 签发用户属性证书；3.3) U 的移动终端设备收到 CA 返回的用户证书后与智能卡设备协作验证其正确性后将其保存在本地。

步骤 4　票据购买和发布。4.1) 为了向 S 证明 U 已被 CA 认证且其泄露的属性集合符合票据策略集合中的一条属性策略，U 的智能卡设备计算一个属性泄露证明，并通过移动终端设备的信道向 S 发起票据购买请求；4.2) S 验证 U 的购买

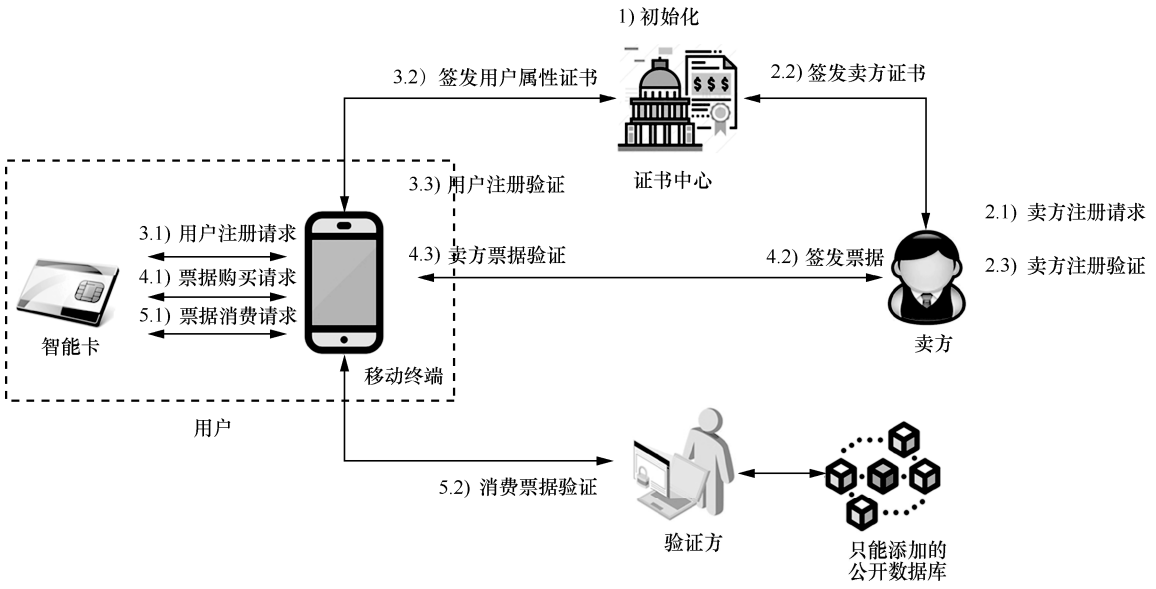

图 1　系统架构

请求后为U签发票据；4.3) U的移动终端设备收到票据并与智能卡设备协作验证其正确性后将其保存在本地。

步骤5 票据消费和验证。5.1) U的智能卡设备产生票据消费证明并通过移动终端设备向V发送票据消费请求；5.2) V收到消费请求后，首先检查票据是否双重消费，然后验证其合法性。

2.2 威胁模型

CA是诚实可信的。它诚实地产生安全的系统参数、主公私钥对和一个票据策略集合；它诚实地验证卖方和用户的身份和属性信息，并为合法卖方和用户签发证书。

S是诚实且好奇的。它诚实地验证用户的合法性以及用户泄露的属性子集与票据策略的一致性；它诚实地为合法用户签发票据，但好奇用户的真实身份和隐藏的属性信息。

U是恶意的。恶意的用户通过伪造用户的证书购买合法票据，或者直接伪造一个票据试图通过V的验证，或者双重消费一个合法票据。

V是诚实且好奇的。它诚实地维护公开数据库，检查票据消费请求是否是双重消费，验证票据消费请求是否合法，但好奇用户的真实身份信息。

2.3 形式化定义

安全的智能卡设备具有防复制和安全存储功能，可以有效地阻止移动终端读取用户密钥的行为，从硬件层面确保了好奇的移动终端无法获得智能卡中的密钥，也就不会影响用户侧的安全性，因此在本节中将用户的智能卡和移动终端设备统称为用户而不再加以区分。表1给出了所提方案常用的符号定义。隐私保护的属性票据方案由5个算法组成。

1) 系统初始化算法：$\text{Setup}(1^{\lambda},n)\rightarrow(\text{pp},\mathbb{P},\text{msk},\text{mpk})$。此算法由CA执行。CA输入一个安全参数$1^{\lambda}$和一个正整数$n$，输出系统参数pp、主私钥msk和主公钥mpk。

2) 卖方注册算法：$\text{SReg}(\text{S}(\text{pp})\leftrightarrow\text{CA}(\text{pp},\text{msk},\text{mpk}))\rightarrow((\text{ssk},\text{spk},\text{cred}_{\text{s}})/\perp)$。此算法由S和CA交互执行。S输入pp，CA输入pp、msk和mpk。若算法执行成功，S输出卖方私钥ssk、卖方公钥spk和卖方证书cred_{s}，否则算法输出$\perp$。

3) 用户注册算法：$\text{UReg}(\text{U}(\text{pp},\text{id},\{m_i\}_{i=1}^{n})\leftrightarrow\text{CA}(\text{pp},\text{msk},\text{mpk}))\rightarrow((\text{usk},\text{upk},\text{cred}_{\text{u}})/\perp)$。此算法由U和CA交互执行。U输入pp、用户身份id和用户属性集合$\{m_i\}_{i=1}^{n}$，CA输入pp、msk和mpk。若算法执行成功，U输出用户私钥usk、用户公钥upk和用户证书cred_{u}，否则算法输出$\perp$。

4) 票据购买和发布算法：$\langle\text{Obtain}(\text{usk},\text{upk},\{m_i\}_{i\in I},\text{cred}_{\text{u}})\leftrightarrow\text{Issue}(\text{ssk},\text{spk})\rangle\rightarrow((\text{tkt},\text{VP},\text{sn})/\perp)$。此算法由U和S交互执行。U输入usk、upk、需泄露的用户属性子集$\{m_i\}_{i\in I}$和cred_{u}，S输入ssk和spk。若算法执行成功，U输出S签发的票据tkt、票据有效期VP和票据唯一标识sn，否则算法输出$\perp$。

5) 票据消费和验证算法：$\langle\text{Show}(\text{tkt},\text{usk},\text{VP},\text{sn})\leftrightarrow\text{Verify}(\text{pp},\text{spk})\rangle\rightarrow(\text{tok},0/1)$。此算法由U和V交互执行。U输入tkt、usk、VP和sn，V输入pp和spk。U将票据tkt的消费请求tok发送V；如果tok不是双重消费且验证通过，V输出1，否则输出0。

表1 符号定义

符号	说明
λ	安全参数
$\varepsilon(\lambda)$	可忽略函数
$x\xleftarrow{R}\mathbb{Z}$	从集合$\mathbb{Z}$中随机选取元素x
CA, S, U, V	证书中心，卖方，用户，验证方
pp, msk, mpk	系统参数，主私钥，主公钥
$\mathbb{P}$	票据策略集合
n, m	用户属性的最大数量，泄露属性数量
$[1,n], I$	集合$\{1,\cdots,n\}$，用户的泄露子集索引
$\{m_i\}_{i=1}^{n},\{m_i\}_{i\in I}$	用户属性集合，泄露属性子集
usk, upk	用户公私钥对
ssk, spk	卖方公私钥对
cred_{u}, cred_{s}	用户证书，卖方证书
id, sn	用户身份标识，票据唯一标识
tkt,VP	一个票据，票据有效期
tok	一个票据的消费请求
$\text{Hash}(\{0,1\}^{*})\rightarrow\mathbb{Z}_p$	一个抗碰撞哈希函数
$\perp$	失败标识符

2.4 安全性定义

为了在防止恶意用户伪造票据的同时保护诚实用户的隐私，属性票据方案应该同时满足不可伪造性和不可链接性。所提方案的安全性定义遵循文献[6,17]的工作，不同之处是为了使安全性的定义更准确地反映威胁模型，本文将不可伪造性分为证书的不可伪造性和票据的不可伪造性，将

不可链接性分为证书的不可链接性和票据的不可链接性。

首先，给出安全性定义需要调用的全局变量和预言机。定义 A 为 PPT 敌手，C 为挑战者。在实验中，C 向 A 模拟所有预言机，所有预言机都可以访问全局变量。

全局变量介绍如下。

1) HU：存储诚实用户身份的列表。

2) CU：存储恶意用户身份的列表。

3) HS：存储诚实卖方身份的列表。

4) CS：存储恶意卖方身份的列表。

5) SR：存储卖方私钥、公钥和证书的列表。

6) UR：存储用户身份、私钥、公钥、属性和证书的列表；

7) TKT：存储用户身份、卖方身份、票据、票据有效期和票据唯一标识的列表。

8) TOK：存储用户身份、卖方身份、票据和票据消费请求的列表。

预言机介绍如下。

1) $\mathrm{O}_{\mathrm{UReg}}(i,\{m_i\}_{i=1}^n)$：此预言机用于描述一个具有属性 $\{m_i\}_{i=1}^n$ 的诚实用户 i 和 CA 执行用户注册算法。如果 $i\in \mathrm{HU}\bigcup \mathrm{CU}$，则返回 $\perp$；否则，CA 和 i 执行算法 $\mathrm{UReg}(\mathrm{U}(\mathrm{pp},i,\{m_i\}_{i=1}^n)\leftrightarrow \mathrm{CA}(\mathrm{pp},\mathrm{msk},\mathrm{mpk}))\rightarrow((\mathrm{usk},\mathrm{upk},\mathrm{cred}_{\mathrm{u}})/\perp)$。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{HU}\leftarrow i$，$\mathrm{UR}[i]\leftarrow(i,\mathrm{usk},\mathrm{upk},\{m_i\}_{i=1}^n,\mathrm{cred}_{\mathrm{u}})$。

2) $\mathrm{O}_{\mathrm{UReg.CA}}(i,\{m_i\}_{i=1}^n)$：此预言机用于描述一个具有属性 $\{m_i\}_{i=1}^n$ 的恶意用户 i 和 CA 执行用户注册算法。如果 $i\in \mathrm{HU}\bigcup \mathrm{CU}$，则返回 $\perp$；否则，CA 和 A 执行算法 $\mathrm{UReg}(\mathrm{A}(\cdot)\leftrightarrow \mathrm{CA}(\mathrm{pp},\mathrm{msk},\mathrm{mpk}))\rightarrow((\mathrm{usk},\mathrm{upk},\mathrm{cred}_{\mathrm{u}})/\perp)$，其中用户 i 的运算部分由 A 执行。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{CU}\leftarrow i$，$\mathrm{UR}[i]\leftarrow(i,*,\mathrm{upk},\{m_i\}_{i=1}^n,\mathrm{cred}_{\mathrm{u}})$，其中 $*$ 为未知私钥。

3) $\mathrm{O}_{\mathrm{CU}}(i)$：此预言机用于描述 A 获得一个诚实用户 i 的秘密信息。如果 $i\notin \mathrm{HU}$，则返回 $\perp$；否则，查询 $\mathrm{UR}[i]$，从 HU 删除 i，添加 $\mathrm{CU}\leftarrow i$，返回 $(i,\mathrm{usk},\mathrm{upk},\{m_i\}_{i=1}^n,\mathrm{cred}_{\mathrm{u}})$。

4) $\mathrm{O}_{\mathrm{SReg}}(j)$：此预言机用于描述一个诚实卖方 j 和 CA 执行卖方注册算法。如果 $j\in \mathrm{HS}\bigcup \mathrm{CS}$，则返回 $\perp$；否则，CA 和 j 执行算法 $\mathrm{SReg}(\mathrm{S}(\mathrm{pp})\leftrightarrow \mathrm{CA}(\mathrm{pp},\mathrm{msk},\mathrm{mpk})\rightarrow((\mathrm{ssk},\mathrm{spk},\mathrm{cred}_{\mathrm{s}})/\perp)$。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{HS}\leftarrow j$，$\mathrm{SR}[j]\leftarrow(j,\mathrm{ssk},\mathrm{spk},\mathrm{cred}_{\mathrm{s}})$。

5) $\mathrm{O}_{\mathrm{SReg.CA}}(j)$：此预言机用于描述一个恶意卖方 j 和 CA 执行卖方注册算法。如果 $j\in \mathrm{HS}\bigcup \mathrm{CS}$，则返回 $\perp$；否则，CA 和 A 执行算法：$\mathrm{SReg}(\mathrm{A}(\cdot)\leftrightarrow \mathrm{CA}(\mathrm{pp},\mathrm{msk},\mathrm{mpk})\rightarrow((\mathrm{ssk},\mathrm{spk},\mathrm{cred}_{\mathrm{s}})/\perp)$，其中卖方 j 的运算部分由 A 执行。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{HS}\leftarrow j$，$\mathrm{SR}[j]\leftarrow(j,*,\mathrm{spk},\mathrm{cred}_{\mathrm{s}})$，其中 $*$ 为未知私钥。

6) $\mathrm{O}_{\mathrm{CS}}(j)$：此预言机用于描述 A 获得一个诚实卖方 j 的秘密信息。如果 $j\notin \mathrm{HS}$，则返回 $\perp$；否则，查询 $\mathrm{SR}[j]$，从 HS 删除 j，添加 $\mathrm{CS}\leftarrow j$，返回 $(j,\mathrm{ssk},\mathrm{spk},\mathrm{cred}_{\mathrm{s}})$。

7) $\mathrm{O}_{\mathrm{ObtIss}}(i,j,I)$：此预言机用于描述一个诚实用户 i 和一个诚实卖方 j 执行票据购买和发布算法。如果 $i\notin \mathrm{HU}, j\notin \mathrm{HS}, I\not\subset[1,n]$，则返回 $\perp$；否则，查询 $\mathrm{UR}[i]$ 和 $\mathrm{SR}[j]$，并执行算法 $\langle\mathrm{Obtain}(\mathrm{usk},\mathrm{upk},\{m_i\}_{i\in I},\mathrm{cred}_{\mathrm{u}})\leftrightarrow \mathrm{Issue}(\mathrm{ssk},\mathrm{spk})\rangle\rightarrow((\mathrm{tkt},\mathrm{VP},\mathrm{sn})/\perp)$。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{TKT}[i][j]\leftarrow(i,j,\mathrm{tkt},\mathrm{VP},\mathrm{sn})$。

8) $\mathrm{O}_{\mathrm{Obtain}}(i,j,I)$：此预言机用于描述一个诚实用户 i 和一个恶意卖方 j 执行票据购买和发布算法。如果 $i\notin \mathrm{HU}, j\notin \mathrm{CS}, I\not\subset[1,n]$，则返回 $\perp$；否则，查询 $\mathrm{UR}[i]$，并和 A 执行算法 $\langle\mathrm{Obtain}(\mathrm{usk},\mathrm{upk},\{m_i\}_{i\in I},\mathrm{cred}_{\mathrm{u}})\leftrightarrow \mathrm{A}(\cdot)\rangle\rightarrow((\mathrm{tkt},\mathrm{VP},\mathrm{sn})/\perp)$，其中卖方 j 的运算部分由 A 执行。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{TKT}[i][j]\leftarrow(i,j,\mathrm{tkt},\mathrm{VP},\mathrm{sn})$。

9) $\mathrm{O}_{\mathrm{Issue}}(i,j,I)$：此预言机用于描述一个恶意用户 i 和一个诚实卖方 j 执行票据购买和发布算法。如果 $i\notin \mathrm{CU}, j\notin \mathrm{HS}, I\not\subset[1,n]$，则返回 $\perp$；否则，查询 $\mathrm{SR}[j]$，并和 A 执行算法 $\langle\mathrm{A}(\cdot)\leftrightarrow \mathrm{Issue}(\mathrm{ssk},\mathrm{spk})\rangle\rightarrow((*,\mathrm{VP},*)/\perp)$。如果算法输出 $\perp$，则返回 $\perp$；否则，设置 $\mathrm{TKT}[i][j]\leftarrow(i,j,*,\mathrm{VP},*)$，其中 $*$ 为未知票据和未知票据标识。

10) $\mathrm{O}_{\mathrm{Show}}(i,j,k)$：此预言机用于描述一个诚实用户 i 和一个恶意验证方 k 执行票据消费和验证算法。如果 $i\notin \mathrm{HU}$，则返回 $\perp$；否则，查询 $\mathrm{UR}[i]$、$\mathrm{SR}[j]$ 和 $\mathrm{TKT}[i][j]$，并和 A 执行算法 $\langle\mathrm{Show}(\mathrm{tkt},\mathrm{usk},\mathrm{VP},\mathrm{sn})\leftrightarrow \mathrm{A}(\cdot)\rangle\rightarrow(\mathrm{tok},0/1)$，其中验证方的计算部分由 A 执行。如果算法输出 0，则返回 0；否则，设置 $\mathrm{TOK}[i][j]\leftarrow(i,j,\mathrm{tkt},\mathrm{tok})$，并返回 1。

11) $\mathrm{O}^{\mathrm{cred}}_{\mathrm{AnCh}_b}(i_0,i_1,I,j)$：此预言机用于在证书的不可链接性实验中描述一个诚实用户 i_b 执行票据购买算法。如果 $i_0\notin\mathrm{HU},i_1\notin\mathrm{HU},I\subset[1,n]$，则返回⊥；否则，查询 UR[i_b]和 SR[j]，并返回算法 $\mathrm{Obtain}(\mathrm{usk},\mathrm{upk},\{m_i\}_{i\in I},\mathrm{cred}_{\mathrm{u}})$ 的输出。

12) $\mathrm{O}^{\mathrm{tkt}}_{\mathrm{AnCh}_b}(i_0,i_1,j)$：此预言机用于在票据的不可链接性实验中描述一个诚实用户 i_b 执行票据消费算法。如果 $i_0\notin\mathrm{HU},i_1\notin\mathrm{HU}$，则返回⊥；否则，查询 UR[i_b]和 SR[j]，并返回算法 $\mathrm{Show}(\mathrm{tkt},\mathrm{usk},\mathrm{VP},\mathrm{sn})$ 的输出。

证书的不可伪造性确保恶意的用户无法通过伪造证书从卖方购买票据。在证书不可伪造性实验中，敌手模拟恶意用户的行为且允许敌手询问 CA 和诚实卖方的预言机。如果在实验结束时，敌手在票据购买算法中输出了一个未注册用户或已注册诚实用户的合法购买请求，则敌手赢得了实验。

定义 1 证书的不可伪造性。在 $\mathrm{EXP}^{\mathrm{unf-cred}}(\mathrm{A},\lambda,n)$ 中，如果对任意的 PPT 敌手 A，存在可忽略函数 $\varepsilon(\lambda)$，使 $\left|\Pr[\mathrm{EXP}^{\mathrm{unf-cred}}(\mathrm{A},\lambda,n)=1]\right|\leqslant\varepsilon(\lambda)$，则属性票据方案满足证书的不可伪造性。

$\mathrm{EXP}^{\mathrm{unf\text{-}cred}}(\mathrm{A},\lambda,n)$：

1) $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^{\lambda},n)$；

2) $\mathrm{O}=\{\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{UReg.CA}},\mathrm{O}_{\mathrm{CU}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Issue}}\}$；

3) $(i^*,j^*,\mathrm{st})\leftarrow\mathrm{A}(\cdot)^{\mathrm{O}}$；

3) $(\cdot,b)\leftarrow\langle\mathrm{A}(\mathrm{st},i^*)\leftrightarrow\mathrm{Issue}(j^*)\rangle$；

4) 如果 $b=\perp$ 或 $i^*\in\mathrm{CU}$ 或 $j^*\notin\mathrm{HS}$，返回 0；

5) 返回 1。

票据的不可伪造性确保了恶意用户无法通过伪造票据通过验证方的验证。在票据的不可伪造性实验中，敌手模拟恶意用户的行为且允许敌手询问 CA 和诚实卖方的预言机。如果在实验结束时，敌手在票据消费算法中输出了一个未注册用户或已注册诚实用户的合法的票据消费请求，则敌手赢得了实验。

定义 2 票据的不可伪造性。在 $\mathrm{EXP}^{\mathrm{unf-tkt}}(\mathrm{A},\lambda,n)$ 中，如果对任意的 PPT 敌手 A，存在可忽略函数 $\varepsilon(\lambda)$，使 $\left|\Pr[\mathrm{EXP}^{\mathrm{unf-tkt}}(\mathrm{A},\lambda,n)=1]\right|\leqslant\varepsilon(\lambda)$，则属性票据方案满足票据的不可伪造性。

$\mathrm{EXP}^{\mathrm{unf\text{-}tkt}}(\mathrm{A},\lambda,n)$：

1) $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^{\lambda},n)$；

2) $\mathrm{O}=\{\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{UReg.CA}},\mathrm{O}_{\mathrm{CU}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Issue}},\mathrm{O}_{\mathrm{Show}}\}$；

3) $(i^*,j^*,\mathrm{st})\leftarrow\mathrm{A}(\cdot)^{\mathrm{O}}$；

3) $(\cdot,b)\leftarrow\langle\mathrm{A}(\mathrm{st},i^*)\leftrightarrow\mathrm{Verify}(\mathrm{pp},j^*)\rangle$；

4) 如果 $b=0$ 或 $i^*\in\mathrm{CU}$ 或 $j^*\notin\mathrm{HS}$，返回 0；

5) 返回 1。

证书的不可链接性确保了好奇的卖方无法通过为用户签发票据获取用户的任何身份和隐藏的属性信息，具体指卖方无法将任意的 2 个票据购买请求链接。

定义 3 证书的不可链接性。在 $\mathrm{EXP}^{\mathrm{unl-cred}}_b(\mathrm{A},\lambda,n)$ 中，如果对任意的 PPT 敌手 A，存在可忽略函数 $\varepsilon(\lambda)$，使 $\left|\Pr[\mathrm{EXP}^{\mathrm{unl-cred}}_1(\mathrm{A},\lambda,n)=1]-\frac{1}{2}\right|\leqslant\varepsilon(\lambda)$，则属性票据方案满足证书的不可链接性。

$\mathrm{EXP}^{\mathrm{unl\text{-}cred}}_b(\mathrm{A},\lambda,n)$：

1) $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^{\lambda},n)$；

2) $\mathrm{O}=\{\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{SReg.CA}},\mathrm{O}_{\mathrm{CS}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Obtain}}\}$；

3) $(i_0,i_1,j^*,I^*,\mathrm{st})\leftarrow\mathrm{A}(\cdot)^{\mathrm{O}}$；

3) $b^*\leftarrow\mathrm{A}(\mathrm{st})^{\mathrm{O}^{\mathrm{cred}}_{\mathrm{AnCh}_b}(i_0,i_1,j^*,I^*)}$；

4) 如果 $b^*=b$，返回 1；

5) 返回 0。

票据的不可链接性确保了好奇的验证方（也同时是卖方）无法通过验证票据消费请求获取用户的任何身份信息，具体指验证方无法将任意的 2 个票据消费请求链接。

定义 4 票据的不可链接性。在 $\mathrm{EXP}^{\mathrm{unl-tkt}}_b(\mathrm{A},\lambda,n)$ 中，如果对任意的 PPT 敌手 A，存在可忽略函数 $\varepsilon(\lambda)$，使 $\left|\Pr[\mathrm{EXP}^{\mathrm{unl-tkt}}_1(\mathrm{A},\lambda,n)=1]-\frac{1}{2}\right|\leqslant\varepsilon(\lambda)$，则属性票据方案满足票据的不可链接性。

$\mathrm{EXP}^{\mathrm{unl\text{-}tkt}}_b(\mathrm{A},\lambda,n)$：

1) $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^{\lambda},n)$；

2) $\mathrm{O}=\{\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{SReg.CA}},\mathrm{O}_{\mathrm{CS}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Obtain}},\mathrm{O}_{\mathrm{Show}}\}$；

3) $(i_0,i_1,j^*,\mathrm{st})\leftarrow\mathrm{A}(\cdot)^{\mathrm{O}}$；

4) $b^*\leftarrow\mathrm{A}(\mathrm{st})^{\mathrm{O}^{\mathrm{tkt}}_{\mathrm{AnCh}_b}(i_0,i_1,j^*)}$；

5) 如果 $b^*=b$，返回 1；

6) 返回 0。

3 方案设计

3.1 设计思想

构造电子票据方案面临的主要挑战是在满足上文定义的系统模型和安全模型下将用户的所有运算轻量化，使其可在智能卡上高效实现。

为了在票据购买算法中实现高效的属性泄露证明，所提方案将匿名的临时身份作为用户公钥，使用户公钥成为一个可随机化的标签；在用户注册时，CA 对每个用户属性分别签发一个带随机化标签（用户公钥）的签名；在购买票据时，用户只需按照票据策略将需泄露的属性对应的多个签名聚合，然后将用户公钥和聚合后的签名随机化后发送给卖方。这种方法避免了将大量不需要泄露的属性隐藏在签名中，且聚合签名和用户公钥的随机化操作只需 $\mathbb{G}_1$ 上的幂运算，提高了票据购买的效率。

为了阻止双花消费，在票据购买时为每个票据产生唯一的标识；当消费票据时，验证方可根据票据唯一标识检查票据是否为双重消费。在票据购买和发布算法中，票据的唯一标识不能泄露给卖方（如果泄露将破坏票据的不可链接性），因此票据发布算法需支持隐私属性的票据签发。为此，所提方案使用支持高效协议的 PS 签名构造用户票据。在票据购买时，用户产生一个票据标识的承诺；在票据发布时，卖方在承诺上签名；在票据消费时，所提方案使用了文献[27]的方法，避免了用户执行耗时的双线性映射运算。此外，为了防止智能卡突然断电导致的购票失败，所提方案利用带密钥的伪随机函数生成票据购买算法的上下文信息，使智能卡重新上电后仍可验证卖方返回的票据。

3.2　方案构造

1) 系统初始化：$\text{Setup}(1^{\lambda},n)\to(\text{pp},\mathbb{P},\text{msk},\text{mpk})$。

CA 产生票据策略集合 $\mathbb{P}$，选取一个 TYPE-3 双线性对参数 $\text{pp}=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g,\tilde{g})$。CA 随机选取 $(x,y,z,\{a_i,b_i\}_{i=1}^n)\xleftarrow{R}\mathbb{Z}_p^*$，计算 $\tilde{X}=\tilde{g}^x,\tilde{Y}=\tilde{g}^y,\tilde{Z}=\tilde{g}^z,\{\tilde{A}_i=\tilde{g}^{a_i},\tilde{B}_i=\tilde{g}^{b_i}\}_{i=1}^n$；CA 随机选取 $(c,d_0,d_1,d_2,d_3)\xleftarrow{R}\mathbb{Z}_p^*$，计算 $(C,D_0,D_1,D_2,D_3)\leftarrow(g^c,g^{d_0},g^{d_1},g^{d_2},g^{d_3})$。最后，CA 设置 $\text{msk}=(x,y,z,\{a_i,b_i\}_{i=1}^n,c,d_0,d_1,d_2,d_3)$，$\text{mpk}=(\tilde{X},\tilde{Y},\tilde{Z},\{\tilde{A}_i,\tilde{B}_i\}_{i=1}^n,C,D_0,D_1,D_2,D_3)$。

2) 卖方注册：$\text{SReg}(\text{S}(\text{pp})\leftrightarrow\text{CA}(\text{pp},\text{msk},\text{mpk}))\to((\text{ssk},\text{spk},\text{cred}_\text{s})/\perp)$。

如图 2 所示，为了获得卖方证书，首先，S 产生 PS 签名私钥 ssk 和公钥 spk；然后，S 计算知识签名 π_1 证明其拥有 ssk 的知识；最后将注册请求信息 (spk,π_1) 发送 CA。CA 验证 S 的身份和 π_1 后，计算 PS 签名 cred_s，并返回 S。S 验证 cred_s 的正确性后，将 cred_s 作为证书保存。

3) 用户注册：$\text{UReg}(\text{U}(\text{pp},\text{id},\{m_i\}_{i=1}^n)\leftrightarrow\text{CA}(\text{pp},\text{msk},\text{mpk}))\to((\text{usk},\text{upk},\text{cred}_\text{u})/\perp)$

如图 3 所示，为了获得卖方证书，首先，智能卡产生伪随机函数的密钥 ρ 和私钥 μ，并设置用户密钥 $\text{usk}=(\rho,\mu)$；然后，智能卡计算与用户身份 id 绑定的随机元素 h，并计算公钥 upk；最后，智能卡计算知识签名 π_2 证明其拥有 μ 的知识，并将注册请求 $(\text{id},\text{upk},\pi_2,\{m_i\}_{i=1}^n)$ 发送给移动终端。移动终端收到智能卡的注册请求后转发给 CA。CA 验证 U 的身份、属性信息和 π_2 后，分别为每个属性−标签对 (m_i,upk) 计算 ASRT 签名 σ_i，并将 $\text{cred}_\text{u}=\{\sigma_i\}_{i=1}^n$ 返回 U。移动终端验证 cred_u 的正确性后，将其发送给智能卡。智能卡将 cred_u 作为证书保存。

4) 票据购买和签发：$\langle\text{Obtain}(\text{usk},\text{upk},\{m_i\}_{i\in I},\text{cred}_\text{u})\leftrightarrow\text{Issue}(\text{ssk},\text{spk})\rangle\to((\text{tkt},\text{VP},\text{sn})/\perp)$。

如图 4 所示，为了获得票据，首先，智能卡从移动终端收到一个 S 产生的挑战随机数 nounce；然后，智能卡将需泄露的属性集合对应的签名 $\{\sigma_i\}_{i\in I}$ 聚合为一个签名 σ，并将用户公钥和聚合签名随机化为 (upk',σ')；为了防止双重消费，智能卡

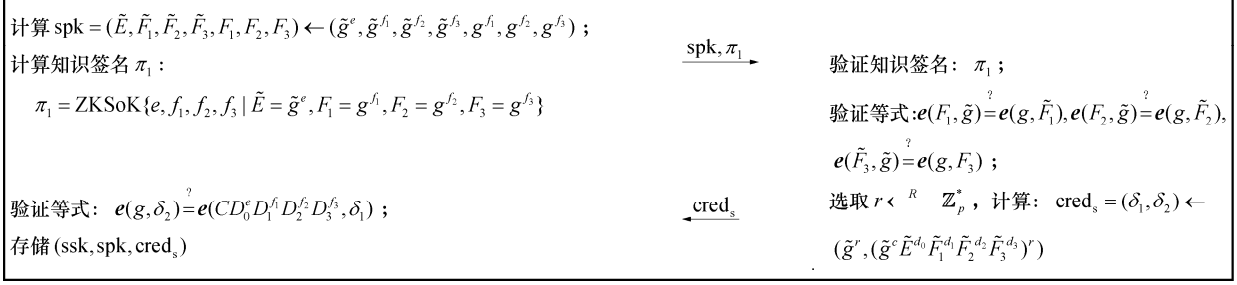

图 2　卖方注册算法

$\mathrm{UReg}(\mathrm{U}(\mathrm{pp},\mathrm{id},\{m_i\}_{i=1}^n)\leftrightarrow \mathrm{CA}(\mathrm{pp},\mathrm{msk},\mathrm{mpk}))\rightarrow(\mathrm{usk},\mathrm{upk},\mathrm{cred}_\mathrm{u})$

用户：U				可信中心：CA
智能卡		移动终端		
执行 $\rho\leftarrow \mathrm{PRF.KeyGen}(1^\lambda)$；				
计算 $h=\mathrm{Hash}(\mathrm{id})$；				
选取 $\mu\xleftarrow{R}\mathbb{Z}_p^*$，计算：				
$\mathrm{upk}=(u_1,u_2,u_3)\leftarrow(h,h^\mu,h^{\mu^2})$；				
设置 $\mathrm{usk}=(\rho,\mu)$，计算知识签名 π_2：	$\xrightarrow[\mathrm{upk},\pi_2]{\mathrm{id},\{m_i\}_{i=1}^n}$	将智能卡的注册请求发送给CA	$\xrightarrow[\mathrm{upk},\pi_2]{\mathrm{id},\{m_i\}_{i=1}^n}$	验证知识签名：π_2；
$\pi_2=\mathrm{ZKSoK}\{\mu\mid u_2=u_1^\mu,u_3=u_2^\mu\}$				对所有的 $i\in[1,n]$，
		对所有的 $i\in[1,n]$，验证等式：	$\xleftarrow{\{\sigma_i\}_{i=1}^n}$	计算：$\sigma_i=u_1^{x+\alpha_i+m_ib_i}u_2^yu_3^z$
存储 $(\mathrm{usk},\mathrm{upk},\mathrm{cred}_\mathrm{u}=\{\sigma_i\}_{i=1}^n)$	$\xleftarrow{\{\sigma_i\}_{i=1}^n}$	$e(\sigma_i,\tilde{g})\overset{?}{=}e(u_1,\tilde{X}\tilde{A}_i\tilde{B}_i^{m_i})e(u_2,\tilde{Y})e(u_3,\tilde{Z})$		

图 3　用户注册算法

$\langle\mathrm{Obtain}(\mathrm{usk},\mathrm{upk},\{m_i\}_{i\in I},\mathrm{cred}_\mathrm{u})\leftrightarrow\mathrm{Issue}(\mathrm{ssk},\mathrm{spk})\rangle\rightarrow(\mathrm{tkt},\mathrm{VP},\mathrm{sn})$

用户：U				卖方：S
智能卡		移动终端		
	$\xleftarrow{\mathrm{nounce}}$	将随机数发送给智能卡	$\xleftarrow{\mathrm{nounce}}$	选取随机数 $\mathrm{nounce}\xleftarrow{R}\mathbb{Z}_p^*$
选取 $r\xleftarrow{R}\mathbb{Z}_p^*$，计算：				
$\mathrm{upk}'=\mathrm{upk}^r\leftarrow(u_1^r,u_2^r,u_3^r)$；				
计算：$\sigma=\prod_{i\in I}\sigma_i,\sigma'=\sigma^r$；				
计算承诺：				
$(\mathrm{sn},t)=\mathrm{PRF}_\rho(\mathrm{id}\Vert\mathrm{nounce})$，$T=g^tF_1^\mu F_2^{\mathrm{sn}}$；				验证 π_3；
计算知识签名 π_3：				定义 $m=\lvert I\rvert$，验证等式：
$\pi_3=\mathrm{ZKSoK}\left\{\mu,t,\mathrm{sn}\;\middle\vert\;\begin{matrix}u_2'=u_1'^\mu,u_3'=u_2'^\mu,\\T=g^tF_1^\mu F_2^{sn}\end{matrix}\right\}(\mathrm{nounce})$	$\xrightarrow[\{m_i\}_{i\in I},\pi_3]{\mathrm{upk}',\sigma',T}$	将智能卡的票据购买请求发送给S	$\xrightarrow[\{m_i\}_{i\in I},\pi_3]{\mathrm{upk}',\sigma'}$	$e(\sigma',\tilde{g})\overset{?}{=}e(u_1',\tilde{X}^m\prod_{i\in I}(\tilde{A}_i\tilde{B}_i^{m_i}))\cdot e(u_2,\tilde{Y}^m)e(u_3,\tilde{Z}^m)$；
				选取 $k_1\xleftarrow{R}\mathbb{Z}_p^*$，设置票据有效期 $\mathrm{VP}\in\mathbb{Z}_p$；
计算：$T_1=\alpha,T_2=\beta\alpha^{-t}$；	$\xleftarrow{\alpha,\beta,\mathrm{VP}}$	返回票据信息	$\xleftarrow{\alpha,\beta,\mathrm{VP}}$	计算：$(\alpha,\beta)\leftarrow(g^{k_1},(Tg^eF_3^{\mathrm{VP}})^{k_1})$
计算：$\tilde{T}=\tilde{E}\tilde{F}_1^\mu\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}}$	$\xleftarrow{T_1,T_2,\tilde{T}}$	验证等式：		
存储 $\mathrm{tkt}=(T_1,T_2)$，VP 和 sn		$e(T_2,\tilde{g})\overset{?}{=}e(T_1,\tilde{T})$；		

图 4　票据购买和发布算法

使用伪随机函数生成票据唯一标识 sn 和加密密钥 t，并使用 ElGamal[28]算法将 μ 和 sn 的承诺加密为 T；最后，智能卡计算知识签名 π_3 证明其拥有秘密信息 (μ,t,sn)，并将票据购买请求 $(\mathrm{upk}',\sigma',T,\{m_i\}_{i\in I},\pi_3)$ 发送给移动终端。移动终端收到智能卡的票据购买请求后转发给 S。S 首先验证 π_3、upk' 和 σ' 后，然后设置票据有效期 VP，最后计算 PS 签名 (α,β)，并将票据验证信息 $(\alpha,\beta,\mathrm{VP})$ 返回用户。移动终端收到票据验证信息后将其转发给智能卡，智能卡使用密钥 t 解密后获得票据 (T_1,T_2)；为了不泄露票据秘密信息的同时验证票据的正确性，智能卡计算 $\tilde{T}$，并将 (T_1,T_2,T) 发送移动终端；移动终端验证通过后，智能卡设置票据 $\mathrm{tkt}=(T_1,T_2)$，并将 $(\mathrm{tkt},\mathrm{VP},\mathrm{sn})$ 保存。

如图 4 所示，在票据购买算法中，用户使用临时产生的加密密钥 t 和票据唯一标识 sn 参与计算票据购买请求，同时 t 和 sn 作为协议的上下文信息也用于验证卖方签发的票据。如果用户发送完票据购买请求后设备意外断电，用户（智能卡）可使用伪随机函数重新恢复 t 和 sn，从而继续完成票据验证而不需要重新发起购票请求。

下面，证明移动终端验证的正确性。因为

$T=g^{t}F_1^{\mu}F_2^{\mathrm{sn}},\alpha=g^{k_1},\beta=(Tg^{e}F_3^{\mathrm{VP}})^{k_1}$，有 $\beta=(g^{t}F_1^{\mu}\cdot F_2^{\mathrm{sn}}g^{e}F_3^{\mathrm{VP}})^{k_1}$，所以 $T_1=\alpha=g^{k_1},T_2=\beta\alpha^{-t}=(g^{t}F_1^{\mu}\cdot F_2^{\mathrm{sn}}g^{e}F_3^{\mathrm{VP}})^{k_1}g^{-tk_1}=(g^{e}F_1^{\mu}F_2^{\mathrm{sn}}F_3^{\mathrm{VP}})^{k_1}$。又因为 $\tilde{T}=\tilde{E}\tilde{F}_1^{\mu}\cdot\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}}$，所以 $\boldsymbol{e}(T_2,\tilde{g})=\boldsymbol{e}((g^{e}F_1^{\mu}F_2^{\mathrm{sn}}F_3^{\mathrm{VP}})^{k_1},\tilde{g})=\boldsymbol{e}(g^{k_1},\tilde{g}^{e}\tilde{F}_1^{\mu}\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}})=\boldsymbol{e}(T_1,\tilde{T})$。

5) 票据消费和验证：$\langle\mathrm{Show}(\mathrm{tkt},\mathrm{usk},\mathrm{VP},\mathrm{sn})\leftrightarrow\mathrm{Verify}(\mathrm{pp},\mathrm{spk})\rangle\rightarrow(\mathrm{tok},0/1)$。

如图 5 所示，为了消费票据，首先，智能卡将票据 tkt 随机化为 tkt′；然后，为了在泄露票据唯一标识 sn 和票据有效期 VP 的同时证明 tkt′ 的正确性，智能卡计算 κ 和 ν；最后，智能卡计算知识签名 π_4 证明其拥有用户密钥的知识，并将票据消费请求 $\mathrm{tok}=(\mathrm{tkt}',\kappa,\nu,\pi_4,\mathrm{sn},\mathrm{VP})$ 发送 V。V 收到票据消费请求后，首先验证其有效期和是否为双重消费，然后验证 π_4 和 tkt′ 的正确性，若验证通过，V 输出 1，否则输出 0。

下面，证明验证等式的正确性。因为 $T_2'=(T_1')^{e+\mu f_1+\mathrm{sn}f_2+\mathrm{VP}f_3},\kappa=g^{k_2}T_1'^{\mu},\nu=\tilde{F}_1^{k_2}$，所以 $\boldsymbol{e}(\kappa,\tilde{F}_1)\cdot\boldsymbol{e}(T_1',\tilde{E}\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}})=\boldsymbol{e}(g^{k_2}T_1'^{\mu},\tilde{F}_1)\boldsymbol{e}(T_1',\tilde{E}\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}})=\boldsymbol{e}(T_1',\tilde{F}_1^{\mu})\cdot\boldsymbol{e}(T_1',\tilde{E}\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}})\boldsymbol{e}(g,\tilde{F}_1^{k_2})=\boldsymbol{e}(T_1',\tilde{F}_1^{\mu}\tilde{E}\tilde{F}_2^{\mathrm{sn}}\tilde{F}_3^{\mathrm{VP}})\boldsymbol{e}(g,\nu)=\boldsymbol{e}(T_2',\tilde{g})\boldsymbol{e}(g,\nu)$。

4　安全性分析

4.1　证书的不可伪造性

定理 1　如果 SDL 问题在 $\mathbb{G}_1$ 上是难解的且 ASRT 签名是不可伪造的，那么所提方案满足证书的不可伪造性。

证明　如果敌手赢得了证书的不可伪造性实验 $\mathrm{EXP}^{\mathrm{unf-cred}}(\mathrm{A},\lambda,n)$，敌手或者伪造了一个未注册用户或者伪造了一个已注册诚实用户的票据购买请求。

引理 1　如果敌手 A 在证书的不可伪造性实验中以不可忽略的概率 $\varepsilon(\lambda)$ 伪造了一个诚实用户的购买请求，那么存在挑战者 C 以 $\frac{\varepsilon(\lambda)}{q}$ 的概率求解 SDL 问题，其中 q 为诚实用户数量。

证明　假设 $(g,g^{\mu^*},g^{\mu^{*2}})\in\mathbb{G}_1^3$ 是一个 SDL 挑战，C 使用 $(g,\mathbb{G}_1)$ 作为参数，执行 $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^{\lambda},n)$ 产生剩余参数，并将 $(\mathrm{pp},\mathbb{P},\mathrm{mpk})$ 发送 A。C 猜测一个诚实用户 $i^*\in\mathrm{HU}$，使得实验结束时，A 伪造了 i^* 的一个票据购买请求。

C 可向 A 模拟如下预言机。

1) $\mathrm{O}_{\mathrm{UReg}}(i,\{m_i\}_{i=1}^{n})$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，C 随机选择 $\tau\in\mathbb{Z}_p^*$，设置 $h_{i^*}=\mathrm{HASH}(i^*)=g^{\tau}$，计算 $\mathrm{upk}_{i^*}=(g^{\tau},g^{\tau\mu^*},g^{\tau\mu^{*2}})$，并通过模拟知识签名 π_2 完成用户注册。

2) $\mathrm{O}_{\mathrm{CU}}(i)$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，返回 $\perp$。

3) $\mathrm{O}_{\mathrm{ObtIss}}(i,j,I)$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，C 随机选择 $(t,\mathrm{sn})\in\mathbb{Z}_p^*$，计算 $T=g^{t}(g^{\mu^*})^{f_1}g^{\mathrm{sn}f_2}$，并通过模拟知识签名 π_3 完成票据购买。

4) $\mathrm{O}_{\mathrm{UReg.CA}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{Issue}}$：因为 C 拥有 CA 和 S 的密钥，所以可以完美地模拟这些预言机。

如果 A 在票据购买算法中伪造了诚实用户 i^* 的票据购买请求（概率为 $\frac{1}{q}$），因为知识签名 π_3 是模拟提取安全的，那么 C 可提取 i^* 的密钥 μ^*，且成功的概率为 $\frac{\varepsilon(\lambda)}{q}$。证毕。

引理 2　如果敌手 A 在证书的不可伪造性实验中以不可忽略的概率 $\varepsilon(\lambda)$ 伪造了一个未注册用户的购买请求，那么存在挑战者 C 以相同的概率伪造

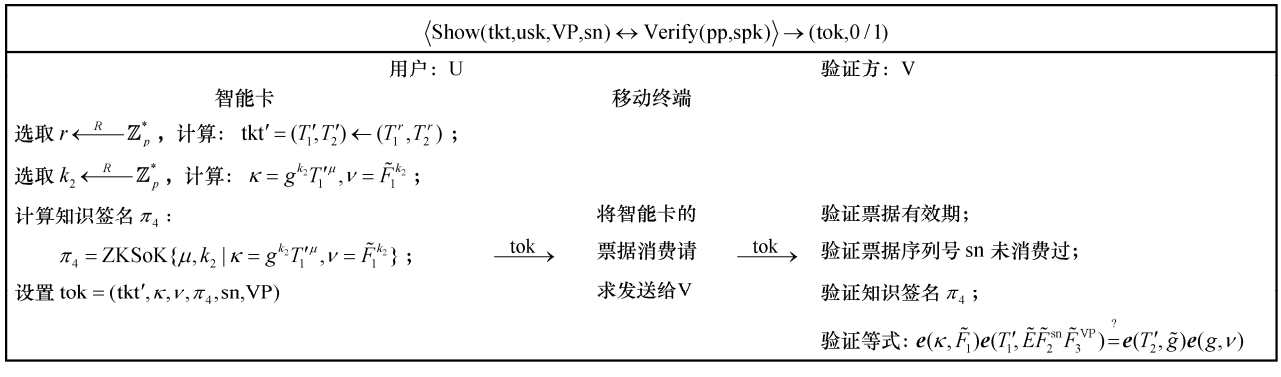

图 5　票据消费和验证算法

ASRT 签名。

证明 C 执行 ASRT 签名的不可伪造性实验，获得公共参数 pp 和签名公钥 $\mathrm{mpk}_{\mathrm{ASRT}}=(\tilde{X},\tilde{Y},\tilde{Z},\{\tilde{A}_i,\tilde{B}_i\}_{i=1}^n)$，且 C 可以不限次数的询问 ASRT 签名预言机 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{ASRT}}(\cdot)$。C 使用 pp 和 $\mathrm{mpk}_{\mathrm{ASRT}}$ 作为参数，执行 $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^\lambda,n)$ 产生剩余参数，并将 $(\mathrm{pp},\mathbb{P},\mathrm{mpk})$ 发送给 A。

C 可向 A 模拟如下预言机。

1) $\mathrm{O}_{\mathrm{UReg.CA}}(i,\{m_i\}_{i=1}^n)$：C 将 A 产生的用户公钥 upk_i 和属性信息 $\{m_i\}_{i=1}^n$ 发送 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{ASRT}}(\cdot)$，然后将输出的签名 $\{\sigma_i\}_{i=1}^n$ 返回 A。

2) $\mathrm{O}_{\mathrm{UReg}}(i,\{m_i\}_{i=1}^n)$：C 产生用户公私钥对 $(\mathrm{usk}_i,\mathrm{upk}_i)$，将用户公钥 upk_i 和属性信息 $\{m_i\}_{i=1}^n$ 发送 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{ASRT}}(\cdot)$，然后将输出的签名 $\{\sigma_i\}_{i=1}^n$ 保存在全局变量中。

3) $\mathrm{O}_{\mathrm{CU}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Issue}}$：因为 C 拥有诚实 U 和 S 的密钥，也拥有为 S 签发证书的主私钥，因此可以完美的模拟这些预言机。

如果实验结束时，A 在票据购买算法中以概率 $\varepsilon(\lambda)$ 伪造了未注册用户 i^* 的票据购买请求 $(\mathrm{upk}'_{i^*},\sigma'_{i^*},\{m_i\}_{i\in I},\pi_3)$，因为知识签名 π_3 是模拟提取安全的，所以 C 可提取 $i^*\notin\mathrm{HU}\bigcup\mathrm{CU}$ 的密钥 μ^*。因为 μ^* 是未注册用户的密钥，时延 C 可以以相同的概率输出一个标签–消息对 $(\mathrm{upk}'_{i^*},\{m_i\}_{i\in I})$ 的 ASRT 签名 σ'_{i^*}，其中 $(\mathrm{upk}'_{i^*},\{m_i\}_{i\in I})$ 未询问过预言机 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{ASRT}}(\cdot)$。证毕。

4.2 票据的不可伪造性

定理 2 如果 SDL 问题在 $\mathbb{G}_1$ 上是难解的且 PS 签名是不可伪造的，那么所提方案满足票据的不可伪造性。

证明 如果敌手赢得了票据的不可伪造性实验 $\mathrm{EXP}^{\mathrm{unf-tkt}}(\mathrm{A},\lambda,n)$，敌手或者伪造了一个未注册用户或者伪造了一个已注册诚实用户的票据消费请求。

引理 3 如果敌手 A 在票据的不可伪造性实验中以不可忽略的概率 $\varepsilon(\lambda)$ 伪造了一个诚实用户的购买请求，那么存在挑战者 C 以 $\dfrac{\varepsilon(\lambda)}{q}$ 的概率求解 SDL 问题，其中 q 为诚实用户数量。

证明 假设 $(g,g^{\mu^*},g^{\mu^{*2}})\in\mathbb{G}_1^3$ 是一个 SDL 挑战，C 使用 $(g,\mathbb{G}_1)$ 作为参数，执行 $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^\lambda,n)$ 产生剩余参数，并将 $(\mathrm{pp},\mathbb{P},\mathrm{mpk})$ 发送 A。C 猜测一个诚实用户 $i^*\in\mathrm{HU}$，使得实验结束时，A 伪造了 i^* 的一个票据购买请求。

C 可向 A 模拟如下预言机。

1) $\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{CU}},\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{UReg.CA}},\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{Issue}}$：C 的模拟与引理 1 一致。

2) $\mathrm{O}_{\mathrm{Show}}(i,j,k)$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，C 计算 $\kappa=g^{k_2}(g^{\mu^*})^{k_1r}$，并通过模拟知识签名 π_4 完成票据消费。

如果 A 在票据消费算法中伪造了诚实用户 i^* 的票据消费请求（概率为 $\dfrac{1}{q}$），因为知识签名 π_4 是模拟提取安全的，那么 C 可提取 i^* 的密钥 μ^*，且成功的概率为 $\dfrac{\varepsilon(\lambda)}{q}$。证毕。

引理 4 如果敌手 A 在票据的不可伪造性实验中以不可忽略的概率 $\varepsilon(\lambda)$ 伪造了一个未注册用户的消费请求，那么存在挑战者 C 以 $\dfrac{\varepsilon(\lambda)}{q}$ 的概率伪造 PS 签名，其中 q 为诚实卖方的数量。

证明 C 执行 PS 签名的不可伪造性实验，获得公共参数 pp 和签名公钥 $\mathrm{spk}_{\mathrm{ps}}=(\tilde{E},\tilde{F}_1,\tilde{F}_2,\tilde{F}_3,F_1,F_2,F_3)$，且 C 可以不限次数的询问 PS 签名预言机 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{PS}}(\cdot)$。C 使用 pp 作为参数，执行 $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})\leftarrow\mathrm{Setup}(1^\lambda,n)$ 产生剩余参数，并将 $(\mathrm{pp},\mathbb{P},\mathrm{mpk})$ 发送 A。

C 猜测 A 将伪造卖方 j^* 签发的票据，并向 A 模拟如下预言机。

1) $\mathrm{O}_{\mathrm{SReg}}(j)$：如果 $j\neq j^*$，C 的模拟与真实的执行一致；否则，C 设置 $\mathrm{spk}_{j^*}=\mathrm{spk}_{\mathrm{ps}}$，并通过模拟知识签名 π_1 完成卖方注册。

2) $\mathrm{O}_{\mathrm{Issue}}(i,j,I)$：如果 $j\neq j^*$，C 的模拟与真实的执行一致；否则，C 将 (T,VP) 发送 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{PS}}(\cdot)$，然后将输出的签名 (α,β) 和 VP 都返回 A。

3) $\mathrm{O}_{\mathrm{ObtIss}}(i,j,I)$：如果 $j\neq j^*$，C 的模拟与真实的执行一致；否则，C 随机选择 $(\mathrm{sn},\mathrm{VT})\in\mathbb{Z}_p^*$，将 $(\mu_i,\mathrm{sn},\mathrm{VP})$ 发送 $\mathrm{O}_{\mathrm{Sign}}^{\mathrm{PS}}(\cdot)$，然后将输出的签名 (T_1,T_2) 作为票据保存在全局变量。

4) $\mathrm{O}_{\mathrm{UReg}},\mathrm{O}_{\mathrm{UReg.CA}},\mathrm{O}_{\mathrm{CU}},\mathrm{O}_{\mathrm{Show}}$：因为 C 拥有用户、

CA 的私钥和 S 的公钥，因此可以完美地模拟这些预言机。

如果实验结束时，A 在票据消费算法中以概率 $\varepsilon(\lambda)$ 伪造了未注册用户 i^* 的关于卖方 j^*（概率为 $\frac{1}{q}$）的票据消费请求 $(\mathrm{tkt}'_{i^*},\kappa_{i^*},\nu_{i^*},\pi_4,\mathrm{sn}_{i^*},\mathrm{VP}_{i^*})$，因为知识签名 π_4 是模拟提取安全的，那么 C 可提取 $i^*\notin \mathrm{HU}\bigcup\mathrm{CU}$ 的密钥 μ^*。因为 μ^* 是未注册用户的密钥，所以 C 可以以相同的概率输出一个消息为 $(\mu^*,\mathrm{sn}_{i^*},\mathrm{VP}_{i^*})$ 的 PS 签名 tkt'_{i^*}，其中 $(\mu^*,\mathrm{sn}_{i^*},\mathrm{VP}_{i^*})$ 未询问过预言机 $\mathrm{O}^{\mathrm{PS}}_{\mathrm{Sign}}(\cdot)$。证毕。

4.3　证书的不可链接性

定理 3　如果 DsqDH 问题在 $\mathbb{G}_1$ 上是难解的，那么所提方案满足证书的不可链接性。

证明　如果敌手以不可忽略的概率 $\varepsilon(\lambda)$ 赢得证书的不可链接性实验 $\mathrm{EXP}_b^{\mathrm{unl-cred}}(\mathrm{A},\lambda,n)$，那么存在挑战者 C 以 $\frac{\varepsilon(\lambda)}{q}$ 的概率求解 $\mathbb{G}_1$ 上的 DsqDH 问题，其中 q 为诚实用户数量。

假设 $(g,g^{\mu},g^{\eta})\in\mathbb{G}_1^3$ 是一个 DsqDH 挑战。C 使用 $(g,\mathbb{G}_1)$ 作为参数产生剩余参数 $(\mathrm{pp},\mathbb{P},\mathrm{msk},\mathrm{mpk})$，并将 $(\mathrm{pp},\mathbb{P},\mathrm{mpk})$ 发送 A。C 猜测一个诚实用户 $i^*\in\mathrm{HU}$，使实验结束时 A 正与 i^* 交互。

在实验的第一阶段，C 向 A 模拟如下预言机。

1) $\mathrm{O}_{\mathrm{UReg}}(i,\{m_i\}_{i=1}^{n})$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，C 随机选择 $\tau\in\mathbb{Z}_p^*$，设置 $h_{i^*}=\mathrm{HASH}(i^*)=g^{\tau}$，计算 $\mathrm{upk}_{i^*}=(g^{\tau},g^{\tau\mu},g^{\tau\eta})$，并通过模拟知识签名 π_2 完成用户注册。

2) $\mathrm{O}_{\mathrm{ObtIss}},\mathrm{O}_{\mathrm{Obtain}}$：C 的模拟与引理 1 中的 $\mathrm{O}_{\mathrm{ObtIss}}(i,j,I)$ 一致。

3) $\mathrm{O}_{\mathrm{SReg}},\mathrm{O}_{\mathrm{SReg.CA}},\mathrm{O}_{\mathrm{CS}}$：因为 C 拥有 CA 和 S 的密钥，所以可以完美地模拟这些预言机。

在实验的某个阶段，A 输出 2 个诚实用户身份 i_0,i_1 和一个卖方身份 j。如果 $i_b\neq i^*$（概率为 $\frac{1}{q}$），那么 C 中止实验，否则继续模拟如下预言机。

4) $\mathrm{O}^{\mathrm{cred}}_{\mathrm{AnCh}_b}(i_0,i_1,I,j)$：C 随机选择 $(r,t,\mathrm{sn})\in\mathbb{Z}_p^*$，计算 $\mathrm{upk}'=\mathrm{upk}_{i^*}^{\,r}$ 和 $\sigma=\prod_{i\in I}\sigma_i,\sigma'=\sigma^r$，计算 $T=g^t(g^{\mu})^{f_1}g^{\mathrm{snf}_2}$，并模拟知识签名 π_3。

如果 $\eta=\mu^2$，C 的模拟是完美的；否则，$(\mathrm{upk}',\sigma',T)$ 都是随机元素，此时 A 无法以不可忽略的概率赢得实验。除非实验中止，A 的任何输出都可以被 C 用于解决 DsqDH 问题，因此 C 成功的概率为 $\frac{\varepsilon(\lambda)}{q}$。证毕。

4.4　票据的不可链接性

定理 4　如果 DsqDH 问题在 $\mathbb{G}_1$ 上是难解的，那么所提方案满足票据的不可链接性。

证明　如果敌手以不可忽略的概率 $\varepsilon(\lambda)$ 赢得票据的不可链接性实验 $\mathrm{EXP}_b^{\mathrm{unl-tkt}}(\mathrm{A},\lambda,n)$，那么存在挑战者 C 以 $\frac{\varepsilon(\lambda)}{q}$ 的概率求解 $\mathbb{G}_1$ 上的 DsqDH 问题，其中 q 为诚实用户数量。

实验设置与第一阶段预言机的模拟与定理 3 相同，除了下面的预言机。

1) $\mathrm{O}_{\mathrm{Show}}(i,j,k)$：如果 $i\neq i^*$，C 的模拟与真实的执行一致；否则，C 计算 $\kappa=g^{k_2}(g^{\mu})^{k_1r}$，并通过模拟知识签名 π_4 完成票据消费。

在实验的某个阶段，A 输出 2 个诚实用户身份 i_0,i_1 和一个卖方身份 j。如果 $i_b\neq i^*$（概率为 $\frac{1}{q}$），那么 C 中止实验，否则继续模拟如下预言机。

2) $\mathrm{O}^{\mathrm{tkt}}_{\mathrm{AnCh}_b}(i_0,i_1,j)$：C 计算 $T_1=(g^{\mu})^{k_1r}$，$T_2=(g^{\mu})^{e+\mu f_1+\mathrm{snf}_2+\mathrm{VPf}_3}=(g^{\eta})^{k_1rf_1}(g^{\mu})^{k_1r(e+\mathrm{snf}_2+\mathrm{VPf}_3)}$，计算计算 $\kappa=g^{k_2}(g^{\eta})^{k_1r}$，并模拟知识签名 π_4。如果 $\eta=\mu^2$，C 的所有模拟是完美的；否则，(T_1,T_2,κ,ν) 都是随机元素，此时 A 无法以不可忽略的概率赢得实验。除非实验中止，A 的任何输出都可以被 C 用于解决 DsqDH 问题，因此 C 成功的概率为 $\frac{\varepsilon(\lambda)}{q}$。证毕。

5　效率分析

5.1　理论分析

表 2 将所提方案与最新的电子票据方案在功能上进行了比较，其中√表示支持此项，×表示不支持此项。核心辅助设置指是否支持将用户的计算安全地分割为智能卡和移动终端实现；属性票据指是否支持属性泄露策略；不可转让指是否支持不可转让性；安全证明指是否有形式化的安全性证明；双花检测指是否能够检测双重消费；不可链接性和不可伪造性指是否支持此类安全需求。由表 2 可知，文献[4,7-10]方案不支持核

表 2 功能比较

方案	核心辅助设置	属性票据	不可转让	安全证明	双花检测	不可链接性	不可伪造性
文献[4,7-10]	×	×	×	√	√	√	√
文献[12-13]	×	×	√	√	√	√	√
文献[3,15]	×	×	√	×	√	√	√
文献[6]	×	√	√	√	√	√	√
文献[17]	×	√	×	√	√	√	√
所提方案	√	√	√	√	√	√	√

心辅助设置、属性票据和票据的不可转让性；文献[12-13]方案不支持核心辅助设置和属性票据；文献[3,15]方案不支持核心辅助设置和属性票据，也没有安全性证明；文献[6,17]方案和所提方案都支持属性票据、双花检测、不可链接性和不可伪造性，且都有形式化的安全证明，但是文献[6,17]方案都不支持核心辅助设置，且文献[17]方案不支持不可转让性。

表 3 将所提方案与最新的 2 个属性票据方案[6,17]在效率上进行了比较，其中 P_1,P_2,P_T,P_e 分别表示 $\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T$ 上的幂运算和双线性映射运算。相比文献[6,17]中的方案，所提方案显著降低了用户的运算量。在所提方案中，票据购买算法需用户执行 13 个 $\mathbb{G}_1$ 上的运算、3 个 $\mathbb{G}_2$ 上的运算和 2 个双线性映射运算；票据消费算法需用户执行 6 个 $\mathbb{G}_1$ 上的运算和 2 个 $\mathbb{G}_2$ 上的运算。所提方案中用户注册的计算量明显高于文献[17]方案，但是新用户仅需执行一次注册用户算法。

5.2 实验分析

为了准确地比较和评估所提方案的效率，使用 MIRACL、Barreto-Naehrig 曲线（BN-256）[29]和 SHA-256 实现了所提方案。

5.2.1 在个人计算机上的实现和对比

使用华为 MateBook 作为实验平台，CPU 为 AMD Ryzen-54 600 H，时钟频率为 3.0 GHz；操作系统为 64 位 Ubuntu Kylin 16.04，运行内存为 16 GB，实现语言为 C/C++，编译器为 GCC/G++。在 AES-100 比特安全级别和相同实验环境下，将所提方案与最新的属性票据方案[6,17]进行了性能比较。不同之处是文献[6]方案只能使用 TYPE-1 型双线性对实现，而所提方案和文献[17]方案使用了计算效率更高的 TYPE-3 型双线性对实现。

表 4 将所提方案与文献[6,17]方案在算法运行时间上进行了对比，其中测试时设置 $n=20$，$m=5$。所提方案各个算法的运行时间显著小于文献[6]方案。与文献[17]方案相比，所提方案的票据购买、票据发布、票据消费和票据验证算法的运行效率分别提高了约 200%、100%、700%、300%；所提方案的用户注册和证书发布算法的运行时间高于文献[17]，但是新用户只执行一次用户注册算法。

表 5 是随着用户属性数量的增多，用户注册算法的运行时间对比。3 种方案的运行时间都随着用户属性数量的增加而增长。所提方案的运行时间比

表 3 效率比较

算法	所提方案	文献[6]	文献[17]
用户注册	$4P_1+P_2+(2+2n)P_e$	$(n+6)P_1+(n+5)P_e$	$(3+n)P_1+P_2+5P_e$
证书发布	$(6+n)P_1$	$(n+3)P_1$	$(6+n)P_1+P_2+2P_e$
票据购买	$13P_1+3P_2+2P_e$	$(n+3m+38)P_1+(n+3m+22)P_e$	$(34+n-m)P_1+7P_2+4P_e$
票据发布	$4P_1+(m+3)P_2+4P_e$	$(3m+31)P_1+mP_T+(2m+17)P_e$	$28P_1+mP_2+7P_e$
票据消费	$6P_1+2P_2$	$24P_1+8P_e$	$17P_1+22P_2$
票据验证	$3P_1+4P_2+4P_e$	$19P_1+8P_e$	$9P_1+8P_2+16P_e$

文献[6]方案小，比文献[17]方案大，但是新用户只执行一次用户注册算法。

表 4　算法运行时间（单位：ms）对比

算法	所提方案	文献[6]	文献[17]
用户注册	743.4	5 273.9	71.3
证书发布	40.1	319.7	42.7
票据购买	30.7	12 215.2	95.7
票据发布	51	5 944.9	105.8
票据消费	4.8	1 905.6	41
票据验证	38.4	1 836.1	162.6

表 5　用户注册算法的运行时间（单位：ms）对比

用户属性数量/个	所提方案	文献[6]	文献[17]
10	375.3	3 169.9	63.8
20	743.4	5 273.9	71.3
30	1 127.9	7 377.9	78.9
40	1 493.3	9 481.9	86.4
50	1 858.6	11 585.9	93.9

表 6 是随着用户属性数量的增多，票据购买算法的运行时间对比。在文献[6,17]方案中，运行时间都随着用户属性数量的增加而增长。所提方案实现了常数复杂度的票据购买算法，与文献[17]方案相比，所提方案的票据购买算法的运行效率在用户属性数量为 10、20、30、40、50 时分别提高了约 180%、200%、230%、250%、280%。

表 6　票据购买算法的运行时间（单位：ms）对比

用户属性数量/个	所提方案	文献[6]	文献[17]
10	31.1	10111.2	88.2
20	30.8	12215.2	95.7
30	30.9	14319.2	103.3
40	31	16423.2	110.8
50	30.8	18527.2	118.4

表 7 是随着用户属性数量的增多，票据消费算法的运行时间对比。3 个方案都实现了常数复杂度的票据消费算法，所提方案的运行时间显著小于文献[6]方案。与文献[17]方案相比，所提方案的票据购买算法的运行效率提高了约 700%。

表 7　票据消费算法的运行时间（单位：ms）对比

用户属性数量/个	所提方案	文献[6]	文献[17]
10	4.9	1905.6	41.2
20	4.8	1905.6	41
30	4.9	1905.6	40.8
40	4.8	1905.6	40.9
50	4.9	1905.6	41

5.2.2　在智能卡和移动手机上的实现

为了评估所提方案在带智能卡的移动终端上的运行效率，本节使用智能手机作为用户的移动终端，使用个人计算机作为 CA、卖方和验证方的实现平台，并在国产智能卡上测试了所提方案。其中，智能卡为爱信诺 ACH512 智能卡芯片，运行内存为 128 KB，设置时钟频率为 40 MHz；智能手机为华为荣耀 9i，CPU 为 Hisilicon kirin 659 (ARMv8-A)，运行内存为 4 GB，主频为 2.36 GHz，操作系统为 Andriod 9.0；个人计算机为华为 Matebook。其中，测试时设置 $n=20$，$m=5$。

如图 6 所示，在所提方案中执行用户注册算法需在智能卡上消耗 116.7 ms，在移动终端上消耗 8 250 ms，在个人计算机（执行 CA 的运算）上消耗 40.1 ms。

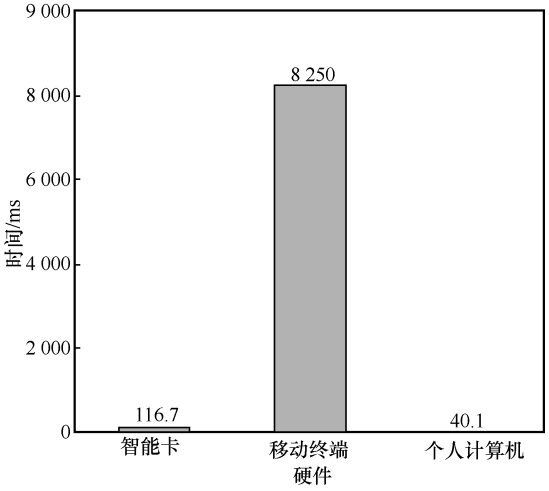

图 6　用户注册算法执行时间

如图 7 所示，在所提方案中执行票据购买和发布算法需在智能卡上消耗 368.5 ms，在移动终端上消耗 195 ms，在个人计算机（执行 S 的运算）上消耗 51 ms。

如图 8 所示，在所提方案中执行票据消费和验

证算法需在智能卡上消耗 196.6 ms，在个人计算机（执行 V 的运算）上消耗 38.4 ms，不需要移动终端参与任何运算。

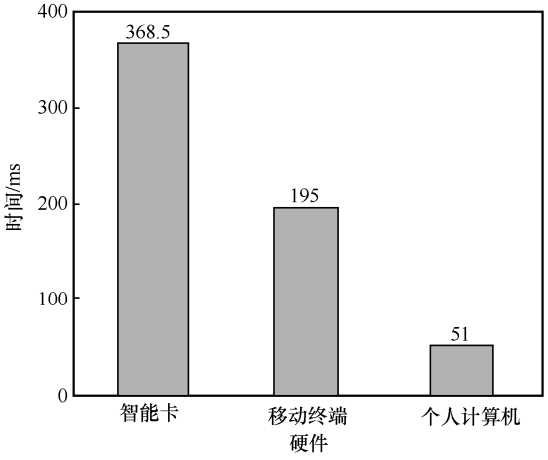

图 7　票据购买和发布算法执行时间

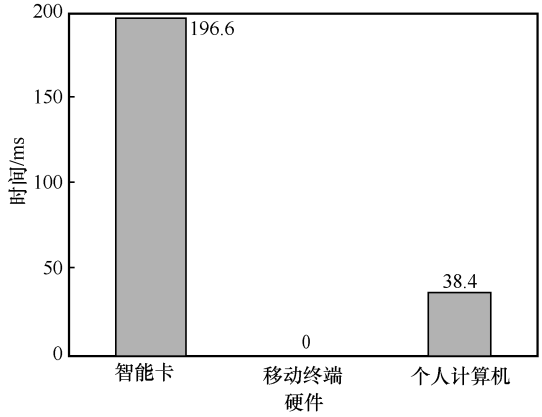

图 8　票据消费和验证算法执行时间

6　结束语

本文提出了一个适合在带智能卡的移动终端上部署的隐私保护的属性票据方案。所提方案满足不可链接性和不可伪造性的安全需求，并解决了现有电子票据系统难以在资源受限设备中部署，以及无法防止票据在未授权设备之间共享的问题。本文在个人计算机、智能卡和智能手机上测试了所提方案，测试结果证明了所提方案的高效性。

参考文献：

[1] MUT-PUIGSERVER M, PAYERAS-CAPELLÀ M M, FERRER-GOMILA J L, et al. A survey of electronic ticketing applied to transport[J]. Computers & Security, 2012, 31(8): 925-939.

[2] VIVES-GUASCH A, PAYERAS-CAPELLÀ M M, MUT-PUIGSERVER M, et al. Anonymous and transferable electronic ticketing scheme[C]// Data Privacy Management and Autonomous Spontaneous Security. Berlin: Springer, 2013: 100-113.

[3] HEYDT-BENJAMIN T S, CHAE H J, DEFEND B, et al. Privacy for public transportation[C]//International Workshop on Privacy Enhancing Technologies. Berlin: Springer, 2006: 1-19.

[4] MILUTINOVIC M, DECROIX K, NAESSENS V, et al. Privacy-preserving public transport ticketing system[C]//IFIP Annual Conference on Data and Applications Security and Privacy. Berlin: Springer, 2015: 135-150.

[5] PATEL B, CROWCROFT J. Ticket based service access for the mobile user[C]//Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking. New York: ACM Press, 1997: 223-233.

[6] HAN J G, CHEN L Q, SCHNEIDER S, et al. Privacy-preserving electronic ticket scheme with attribute-based credentials[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(4): 1836-1849.

[7] FAN C, LEI C L. Multi-recastable ticket schemes for electronic voting[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 1998, 81(5): 940-949.

[8] SONG R G, KORBA L. Pay-TV system with strong privacy and non-repudiation protection[J]. IEEE Transactions on Consumer Electronics, 2003, 49(2): 408-413.

[9] QUERCIA D, HAILES S. MOTET: mobile transactions using electronic tickets[C]//Proceedings of First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05). Piscataway: IEEE Press, 2005: 374-383.

[10] RUPP A, HINTERWÄLDER G, BALDIMTSI F, et al. P4R: privacy-preserving pre-payments with refunds for transportation systems[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2013: 205-212.

[11] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Berlin: Springer, 1983: 199-203.

[12] NAKANISHI T, HARUNA N, SUGIYAMA Y. Unlinkable electronic coupon protocol with anonymity control[C]//International Workshop on Information Security. Berlin: Springer, 1999: 37-46.

[13] VIVES-GUASCH A, CASTELLÀ-ROCA J, PAYERAS-CAPELLA M M, et al. An electronic and secure automatic fare collection system with revocable anonymity for users[C]//Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia. Piscataway: IEEE Press, 2010: 387-392.

[14] CHAUM D, HEYST E. Group signatures[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer, 1991: 257-265.

[15] ARFAOUI G, LALANDE J F, TRAORÉ J, et al. A practical set-membership proof for privacy-preserving NFC mobile ticketing[J]. Proceedings on Privacy Enhancing Technologies, 2015, 2015(2): 25-45.

[16] CHAUM D. Security without identification: transaction systems to

make big brother obsolete[J]. Communications of the ACM, 1985, 28(10): 1030-1044.

[17] 封化民, 史瑞, 袁峰, 等. 高效的强隐私保护和可转让的属性票据方案[J]. 通信学报, 2022, 43(3): 63-75.
FENG H M, SHI R, YUAN F, et al. Efficient strong privacy protection and transferable attribute-based ticket scheme[J]. Journal on Communications, 2022, 43(3): 63-75.

[18] MOSTOWSKI W, VULLERS P. Efficient U-prove implementation for anonymous credentials on smart cards[C]//International Conference on Security and Privacy in Communication Systems. Berlin: Springer, 2011: 243-260.

[19] CAMENISCH J, DRIJVERS M, DZURENDA P, et al. Fast keyed-verification anonymous credentials on standard smart cards[C]//IFIP International Conference on ICT Systems Security and Privacy Protection. Berlin: Springer, 2019: 286-298.

[20] VERHEUL E R. Self-blindable credential certificates from the Weil pairing[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 533-551.

[21] HANZLIK L, SLAMANIG D. With a little help from my friends: constructing practical anonymous credentials[C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2021: 2004-2023.

[22] GALBRAITH S D, PATERSON K G, SMART N P. Pairings for cryptographers[J]. Discrete Applied Mathematics, 2008, 156(16): 3113-3121.

[23] CHASE M, LYSYANSKAYA A. On signatures of knowledge[C]//Annual International Cryptology Conference. Berlin: Springer, 2006: 78-96.

[24] H'EBANT C, POINTCHEVAL D. Traceable constant-size multi-authority credentials[R]. Cryptology ePrint Archive, 2020.

[25] SHOUP V. Lower bounds for discrete logarithms and related problems[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1997: 256-266.

[26] POINTCHEVAL D, SANDERS O. Short randomizable signatures[C]//Cryptographers' Track at the RSA Conference. Berlin: Springer, 2016: 111-126.

[27] SONNINO A, AL-BASSAM M, BANO S, et al. Coconut: threshold issuance selective disclosure credentials with applications to distributed ledgers[J]. arXiv Preprint, arXiv:1802.07344, 2018.

[28] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[29] FAN J, VERCAUTEREN F, VERBAUWHEDE I. Faster FP-arithmetic for cryptographic pairings on Barreto-Naehrig curves[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009: 240-253.

[作者简介]

史瑞（1988− ），男，山东德州人，北京邮电大学博士生，北京电子科技学院工程师，主要研究方向为密码学和隐私保护。

封化民（1963− ），男，陕西富平人，博士，北京邮电大学教授，北京电子科技学院教授，主要研究方向为密码学和信息安全。

谢惠琴（1992− ），女，福建福安人，博士，北京电子科技学院讲师，主要研究方向为密码学、量子计算和量子密码。

史国振（1972− ），男，河南济源人，博士，北京电子科技学院教授，主要研究方向为网络与系统安全、嵌入式安全。

刘飚（1980−），男，湖南邵阳人，博士，北京电子科技学院讲师，主要研究方向为信息安全和机器学习。

杨旸（1984− ），女，湖北随州人，博士，福州大学教授，主要研究方向为密码学和隐私保护。