高效的强隐私保护和可转让的属性票据方案

封化民[1,2]，史瑞[1,2]，袁峰[3]，李艳俊[4]，杨旸[5]

（1. 北京邮电大学网络空间安全学院，北京 100876；2. 北京电子科技学院信息安全研究所，北京 100070；
3. 中国航天科工集团第二研究院 706 所，北京 100854；4. 中国电子科技集团第十五研究所，北京 100846；
5. 福州大学数学与计算机科学学院，福建 福州 350108）

摘 要：为了解决电子票据中面临的效率低、灵活性差和隐私保护不全面的问题，提出了高效的强隐私保护且可转让的属性票据方案。首先，结合属性证书和集合承诺构建了基于属性泄露的票据购买算法；其次，利用等价类上的结构保持签名和动态可延展签名降低了票据购买的计算复杂度，实现了常数复杂度的票据转让和票据验证；再次，为了杜绝恶意的验票方根据卖方身份猜测用户信息的可能，在票据验证中同时实现了用户和卖方的匿名性；最后，给出了方案的安全性定义，并将其安全性规约到普通密码学假设或已证明安全的密码学原语的安全性上。对比和实验结果表明了所提方案的灵活性和高效性。

关键词：属性票据；隐私保护；匿名证书；结构保持签名

中图分类号：TP309.2

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022053

Efficient strong privacy protection and transferable attribute-based ticket scheme

FENG Huamin[1,2], SHI Rui[1,2], YUAN Feng[3], LI Yanjun[4], YANG Yang[5]

1. School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
2. Institute of Information Security, Beijing Electronic Science and Technology Institute, Beijing 100070, China
3. Institute 706, Second Academy of CASIC, Beijing 100854, China
4. The 15th Research Institute of CETC, Beijing 100846, China
5. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China

Abstract: To solve the problems of efficiency, flexibility, and privacy protection faced by electronic tickets, an efficient and transferable attribute-based ticket scheme with strong privacy protection was proposed. Firstly, a ticket issuing algorithm based on attribute disclosure was constructed by combining attribute-based credentials and set commitment. Secondly, the structure-preserving signature on equivalence class and dynamic malleable signature were used to reduce the computational complexity of the ticket issuance, and the ticket transfer and ticket verification with constant complexity were realized. In addition, to prevent the possibility of malicious verifiers guessing user information according to the seller's identity, the scheme not only realized the anonymity of the user, but also realized the anonymity of the seller in the ticket verification for the first time. Finally, the security definition of the scheme was given, and its security was reduced to either well-known complexity cryptography assumptions or the security of proven cryptography primitives. Comparison and experimental results demonstrate that the proposed scheme is flexible and efficient.

Keywords: attribute-based ticket, privacy protection, anonymous credential, structure-preserving signature

---

收稿日期：2021−11−22；**修回日期**：2022−02−22

通信作者：史瑞，shir@bupt.edu.cn

基金项目：国家重点研发计划基金资助项目（No.2018YFB0803600）；北京电子科技学院一流学科建设基金资助项目（No.3201024）

Foundation Items: The National Key Research and Development Program of China (No.2018YFB0803600), First Class Discipline Building Project of Beijing Electronic Science and Technology Institute (No.3201024)

0 引言

随着手机、平板电脑、可穿戴设备等移动终端和互联网技术的快速发展，电子票据正迅速普及并为人们的生活带来了极大的便利。目前，电子票据已成为交通、娱乐等行业的许多公司登记、处理和销售票据的一种趋势。此外，在云环境下，电子票据还可以作为访问在线服务的一种凭证。例如，Han等[1]利用电子票据构造了一个在线的匿名单登录系统。相比于传统的纸质票据，电子票据可存储在移动设备上，不需要消耗纸质，减少了资源浪费，有助于实现碳达峰和碳中和；电子票据可在线购买和验证，减少了复杂的线下交易，提升了用户体验。

与匿名的纸质票据相比，电子票据的主要安全隐患是用户隐私信息的泄露。在电子票据系统中，用户数据（如姓名、住址、身份证号码、电话和其他属性信息等）可能会被收集和滥用。此外，传统的电子票据[2-8]模型都假设卖方的身份是公开的，但这也可能泄露用户的很多信息，例如，美国电子驾照签发者的身份中可能包含用户的邮政编码，进而可以推测出用户的家庭住址。因此，为了更全面地保护用户隐私，杜绝恶意的验票方根据卖方身份推测用户信息的可能，有必要隐藏卖方的身份。2021年8月，我国颁布了《中华人民共和国个人信息保护法》，使保护用户信息权益变得更加重要。为了保护用户隐私，国内外学者使用假名[9]、盲签名[10]、群签名[11]、随机化签名[12-14]和匿名证书[2,8]等技术设计了很多电子票据方案，但是已有方案都仅提供了用户的匿名性，却不支持卖方的匿名性。

属性票据作为电子票据的一种特殊类型，可提供基于属性泄露的票据购买方式，这种方式在保证认证性的同时实现了个人信息的最小化泄露。例如，学生购买优惠票时只需泄露学生属性，而姓名、学号和所在学院等信息都应保密；残疾人购买优惠票时只需泄露残疾属性，而不需要泄露更多的患病细节和其他个人信息；军人在购买优惠票时只需泄露军人属性，而具体的服役单位、军衔和职务等信息都应保密。属性票据提高了电子票据使用的灵活性，是电子票据方案应该具备的一个重要功能。Han等[2]第一次提出了支持属性策略的电子票据方案，但是其方案使用了复杂的零知识证明（ZKP, zero knowledge proof），使票据购买算法的计算消耗随着用户属性数量的增加线性增长。

非实名纸质票据的另一重要特点是可转让性，如电影票、景区门票、排队票等；用户可以方便地将票据赠送给其他用户（如朋友、家人等）。目前，已有的可转让电子票据方案[5-6]都使用签名链的方式构造票据转让算法，使票据转让和票据验证算法的计算消耗都随着票据转让次数的增加呈线性增长。

为了解决电子票据方案存在的上述问题，本文提出了一个高效的强隐私保护且支持属性策略和票据转让功能的电子票据方案，主要贡献如下。

1) 强隐私保护。该方案既能保护用户的匿名性，也在票据验证中保护了卖方的匿名性。这使恶意的验票方无法从票据验证中获得用户和卖方的任何信息，这种强隐私保护特征弥补了已有电子票据方案在用户隐私保护方面的不足。

2) 可转让的属性票据。该方案支持基于属性泄露的售票策略，用户可以通过泄露个人部分属性从卖方匿名地购买任何符合售票策略的票据。该方案支持灵活的票据转让功能，用户可以将票据转让给任何已注册的用户，卖方也可在发布票据时禁止票据转让。

3) 高效的算法。与文献[2]方案相比，该方案将票据购买算法的计算复杂度从$O(n)$降低到$O(n-k)$。与文献[5-6]方案相比，该方案将票据转让和票据验证算法的计算复杂度从$O(t)$降低到$O(1)$。其中，n、k、t分别为用户属性数量、泄露属性数量和票据转让次数。

4) 高效的双花检测和追踪。对于可转让电子票据，双花者可能是票据转让链中的任何用户，该方案结合“施诺尔（Schnorr）技巧”[15]和公钥加密技术实现了票据转让链中所有双花用户的身份追踪。

本文使用MIRACL（multiprecision integer and rational arithmetic C/C++ library）实现了该方案，并与已有的属性票据[2]和可转让票据[5]方案进行了效率对比；实验结果表明，所提方案在功能和效率上都优于已有方案。

Quercia等[16]利用Chaum[10]盲签名提出了一种用于移动交易的电子票据方案。Rupp等[17]基于Chaum[10]盲签名和Boneh等[18]短签名方案衍生出来一种保护隐私的预支付方案。Milutinovic等[19]基于Abe等[20]的盲签名、Pedersen[21]的秘密共享和Camenisch等[12]的匿名证书提出了一种保护用户隐私的电子票据方案。这些方案都可以保护用户隐私，但与本文方案不同，它们不支持属性票据，不能保护卖方隐私，不支持高效的票据转让，且出现

重复消费后无法对恶意用户进行身份追踪。

Nakanishi 等[22]基于 Camenisch 群签名提出了一种电子优惠券方案。Vives-Guasch 等[23]利用 Boneh 群签名提出了一种自动收费系统。Heydt-Benjamin 等[3]使用匿名证书、电子现金和代理重新加密技术实现了公共交通电子票据系统的安全性和隐私性。Arfaoui 等[7]将 Bonyeh-Boyen 签名[24]与 Camenisch 等[12]的匿名证书方案相结合，提出了一种保护隐私的近场通信移动票据系统。Vives-Guasch 等[25]使用轻量级加密技术和具有近场通信能力的移动电话提出了一个电子票据系统。这些方案可以实现用户和票据的匿名性，但与本文方案不同，它们不支持属性票据，不能保护卖方隐私，也不支持高效的票据转让。

Han 等[2]基于 Bonyeh-Boyen 签名[24]的范围证明提出了一个基于属性证书的隐私保护电子票据方案。Han 的方案支持属性策略和双花用户的身份追踪，但是与本文方案不同，它不能保护卖方隐私，也不支持高效的票据转让，且其票据购买算法的计算消耗和通信消耗都随用户属性数量的增大呈线性增加。

Vives-Guasch 等[5]使用群签名构造了匿名和可转让的电子票据方案；Payeras-Capella 等[6]测试了文献[5]方案的性能。文献[5]方案实现了可转让的匿名票据，但是与本文方案不同，它们不支持属性票据，不能保护卖方隐私，且其票据转让和验证算法的计算消耗随着票据转让次数的增加呈线性增加。

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，$\mathbb{G}_1\neq\mathbb{G}_2$，$\mathbb{G}_1$ 与 $\mathbb{G}_2$ 之间不存在同态映射，双线性映射 $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$ 满足以下 3 个条件。① 双线性：任意 $g\in\mathbb{G}_2,\tilde{g}\in\mathbb{G}_2,a,b\in\mathbb{Z}_p^*$，有 $e(g^a,\tilde{g}^b)=e(g,\tilde{g})^{ab}$；② 非退化性：对于 $g\neq 1_{\mathbb{G}_1},\tilde{g}\neq 1_{\mathbb{G}_2}$，有 $e(g,\tilde{g})\neq 1_{\mathbb{G}_T}$；③可计算性：任意 $g\in\mathbb{G}_2,\tilde{g}\in\mathbb{G}_2$，存在高效算法计算 $e(g,\tilde{g})$。

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）[26]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[26]的。

1.3　离散对数假设

离散对数假设是指给定二元组 $g,g^x\in\mathbb{G}$，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　集合承诺

集合承诺（SC, set commitment）[27-28]由初始化、计算承诺、打开承诺、打开子集、验证子集算法组成。在标准模型下，集合承诺满足正确性、绑定性、隐藏性和被打开子集的不可伪造性。

1.5　等价类上的结构保持签名

等价类上的结构保持签名（SPS-EQ, structure-preserving signature on equivalence class）[27]由初始化、密钥生成、签名、修改签名和验签算法组成。在一般群模型下，SPS-EQ 签名满足正确性、不可伪造性和签名适应性，且其明文空间是类隐藏的。

1.6　动态可延展签名

动态可延展签名（DMS, dynamically malleable signatures）[29]由初始化、密钥生成、签名、验证延展密钥、延展签名和验签算法组成。在一般群模型下，DMS 签名具有正确性、不可伪造性和完美的派生隐私性。

2　方案和安全模型

2.1　方案模型

如图 1 所示，可转让的属性票据方案包括证书中心（CA，certificate authority）、用户（U，user）、卖方（S，seller）和验票方（V，verifier）四类实体。CA 执行系统初始化（步骤 1)），产生售票策略集合，并向 U 和 S 签发证书（步骤 2)和步骤 3))；S 是票据卖方，它从 CA 获取公钥证书（步骤 2))，并根据 CA 公布的售票策略向 U 销售票据（步骤 4))；U 是拥有多个属性的用户，它从 CA 获取属性证书（步骤 3))，并根据售票策略匿名的从 S 购买票据（步骤 4))；V 是验票方，它负责验证票据的合法性（步骤 6))，并检查票据是否是重复消费，若是重复消费则追踪用户的公钥（步骤 7))。U 可以将票据转让给其他可信用户（步骤 5))，任何拥有票据（从 S 购买或由其他用户转让）的已注册用户都可以向 V 匿名地消费票据（步骤 6))。

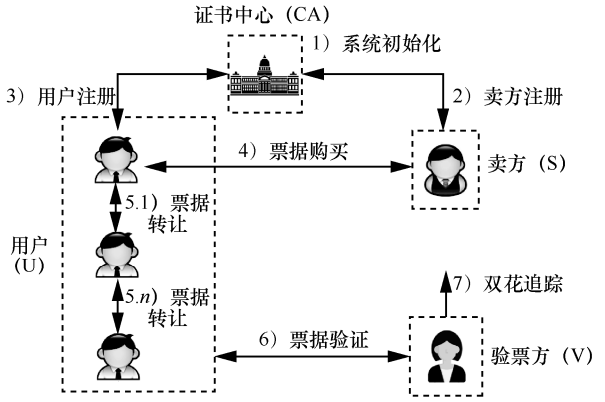

图 1 可转让属性票据的方案模型

表 1 定义了常用的符号。一个可转让的属性票据方案包括 7 个算法，具体介绍如下。

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
$1_{\mathbb{G}_1}, 1_{\mathbb{G}_2}$	$\mathbb{G}_1, \mathbb{G}_2$ 的单位元
CA,S,U,V	证书中心，卖方，用户，验票方
msk,pp	CA 的主密钥，系统参数
$\mathbb{S}, \mathbb{A}, \mathbb{D}$	售票策略集合，用户属性集合，泄露属性集合
(usk, upk)	用户公私钥对
(ssk, spk)	卖方公私钥对
$\text{cred}_\text{u}, \text{cred}_\text{s}$	用户证书，卖方证书
tkt, tid	票据，票据标识
f, tk	票据转让标识，转让密钥
$H(\{0,1\}^*) \to \mathbb{Z}_p$	哈希函数
ds	追踪双花信息
$\perp$	失败标识符

1) 系统初始化：$\text{Setup}(1^\lambda) \to (\text{pp},\text{msk},\mathbb{S})$。CA 执行系统初始化算法，输入安全参数 λ，输出系统参数 pp、主私钥 msk 和售票策略集合 $\mathbb{S}$。

2) 卖方注册：$\text{SReg}(\text{S}(\text{ssk},\text{spk},\text{pp}) \leftrightarrow \text{CA}(\text{msk},\text{pp})) \to \text{cred}_\text{s}$。S 与 CA 交互执行卖方注册算法。S 产生卖方私钥 ssk 和公钥 spk，S 输入 ssk、spk 和 pp；CA 输入 msk 和 pp。若算法执行成功，S 获得公钥证书 cred_s，否则返回 $\perp$。

3) 用户注册：$\text{UReg}(\text{U}(\text{usk},\text{upk},\mathbb{A},\text{pp}) \leftrightarrow \text{CA}(\text{msk},\text{pp})) \to \text{cred}_\text{u}$。U 与 CA 交互执行用户注册算法。U 产生用户私钥 usk 和公钥 upk，输入 usk、upk、pp 和用户属性集合 $\mathbb{A} = (a_i)_{i=1}^n$；CA 输入 msk 和 pp。若算法执行成功，U 获得属性证书 cred_u，否则返回 $\perp$。

4) 票据购买：$\text{Issue}(\text{U}(\text{usk},\text{cred}_\text{u},\mathbb{A},\mathbb{D},\text{pp}) \leftrightarrow \text{S}(\text{ssk},\text{cred}_\text{s},\text{pp})) \to (\text{tkt}, f, \text{tk})$。U 与 S 交互执行票据购买算法。为了证明 U 符合售票策略集合 $\mathbb{S}$ 中的一条策略，U 需要泄露属性集合 $\mathbb{D} \subseteq \mathbb{A}$。S 设置票据转让标识 f，若 $f=1$ 则允许 U 转让票据，否则禁止转让。若算法执行成功，U 获得票据 tkt、票据转让标识 f 和转让密钥 tk，否则返回 $\perp$。

5) 票据转让：$\text{Transfer}(\text{U}(\text{ssk},\text{tkt},\text{tk},f,\text{pp}) \leftrightarrow \text{U}'(\text{ssk}',\text{pp})) \to (\text{tkt}', f, \text{tk}')$。U 与用户 U′ 交互执行票据转让算法。U 输入 ssk、tkt、f、tk 和 pp，U′ 输入私钥 ssk′ 和 pp。若算法执行成功，U′ 获得票据 tkt′、转让标识 f 和转让密钥 tk′，否则返回 $\perp$。

6) 票据验证：$\text{Show}(\text{U}(\text{ssk},\text{cred}_\text{u},\text{tkt},\text{pp}) \leftrightarrow \text{V}(\text{pp})) \to (b,\text{tid},\text{ds})$。U 与 V 交互执行票据验证算法。若票据验证成功，V 输出 $b=1$、票据标识 tid 和追踪双花信息 ds，否则输出 $b=0$。

7) 双花追踪：$\text{DsTrace}(\text{tid},\text{ds},\text{tid}',\text{ds}') \to (\text{upk},\text{upk}')$。V 输入 2 个票据验证算法的输出 (tid,ds) 和 (tid′,ds′)，若 $\text{tid}=\text{tid}'$，则检测到重复消费，V 执行双花追踪算法，输出重复消费者的公钥。

2.2 威胁模型

CA 在系统中是完全可信的实体。S 是诚实且好奇的，它诚实地按照 CA 发布的售票策略集合为用户售票，但好奇用户的真实身份和属性信息。U 是恶意的，它可能伪造票据或重复消费票据，但在票据转让协议中，票据转让用户 U 和接受转让用户 U′ 之间是互信的。V 是诚实且好奇的，它诚实地验证票据，检测重复消费并追踪恶意用户公钥，但它好奇用户和卖方的真实身份。

2.3 安全模型

电子票据方案应满足以下安全要求：用户证书和票据的不可伪造性、诚实用户的不可链接性和验票算法中卖方身份的不可链接性。为了准确地定义上述安全需求，本文使用基于游戏[12-15,27,29]的方法定义了电子票据方案的安全模型。

全局变量：使用集合 HU、CU、USK、UPK 分

别记录诚实用户编号、恶意用户编号、用户私钥和用户公钥；使用集合 HS、CS、SSK、SPK 分别记录诚实卖方编号、恶意卖方编号、卖方私钥和卖方公钥；使用列表 $\mathrm{LU}=(\mathrm{UI},\mathrm{UC},\mathrm{UA})$ 记录注册用户编号、用户证书和属性集合；使用列表 $\mathrm{LS}=(\mathrm{SI},\mathrm{SC})$ 记录注册卖方编号和卖方证书；使用列表 $\mathrm{LT}=(\mathrm{TI},\mathrm{TKT},\mathrm{TK},\mathrm{TF})$ 记录用户编号、票据、票据转让密钥和转让标识。

预言机：下面给出安全定义中使用的预言机。

$O_{\mathrm{HS}}(j)$：输入卖方编号 j。若 $j\in\mathrm{CS}$ 或 $j\in\mathrm{HS}$，则返回 $\perp$，否则产生诚实卖方 j 的密钥对 $(\mathrm{SSK}[j],\mathrm{SPK}[j])$，将 j 添加到 HS，返回 $\mathrm{SPK}[j]$。

$O_{\mathrm{SR}}(j)$：输入卖方编号 j。若 $j\notin\mathrm{HS}$，则返回 $\perp$，否则执行卖方注册算法 $\mathrm{cred}_{\mathrm{s}}\leftarrow\mathrm{SReg}(\mathrm{S}(\mathrm{SSK}[j],\mathrm{SPK}[j],\mathrm{pp})\leftrightarrow\mathrm{CA}(\mathrm{msk},\mathrm{pp}))$，将 $(j,\mathrm{cred}_{\mathrm{s}})$ 添加到 LS。

$O_{\mathrm{CS}}(j)$：输入卖方编号 j。若 $j\notin\mathrm{HS}$，则返回 $\perp$，否则将 j 从 HS 删除并添加到 CS，返回 $\mathrm{SSK}[j]$ 和 $(\mathrm{SI}[k],\mathrm{SC}[k])$，其中 $\mathrm{SI}[k]=j$。

$O_{\mathrm{HU}}(i)$：输入用户编号 i。若 $i\in\mathrm{CU}$ 或 $i\in\mathrm{HU}$，则返回 $\perp$，否则产生诚实用户 i 的密钥 $(\mathrm{USK}[i],\mathrm{UPK}[i])$，将 i 添加到 HU，返回 $\mathrm{UPK}[i]$。

$O_{\mathrm{UR}}(i,\mathbb{A})$：输入用户编号 i 和属性集合 $\mathbb{A}$。若 $i\notin\mathrm{HU}$，则返回 $\perp$，否则执行用户注册算法 $\mathrm{cred}_{\mathrm{u}}\leftarrow\mathrm{UReg}(\mathrm{U}(\mathrm{USK}[i],\mathrm{UPK}[i],\mathbb{A},\mathrm{pp})\leftrightarrow\mathrm{CA}(\mathrm{msk},\mathrm{pp}))$，将 $(i,\mathrm{cred}_{\mathrm{u}},\mathbb{A})$ 添加到 LU。

$O_{\mathrm{CU}}(i)$：输入用户编号 i。若 $i\notin\mathrm{HU}$，则返回 $\perp$，否则将 i 从 HU 删除并添加到 CU，返回 $\mathrm{USK}[i]$ 和 $(\mathrm{UI}[k],\mathrm{UC}[k],\mathrm{UA}[k])$，其中 $\mathrm{UI}[k]=i$。

$O_{\mathrm{Iss}}(i,j,I,f)$：输入用户编号 i、卖方编号 j、符合售票策略的属性集合索引 I 和票据转让标识 f。若 $i\notin\mathrm{HU}$ 或 $j\notin\mathrm{HS}$，则返回 $\perp$，否则执行票据购买算法 $(\mathrm{tkt},f,\mathrm{tk})\leftarrow\mathrm{Issue}(\mathrm{U}(\mathrm{USK}[i],\mathrm{UC}[k],\mathrm{UA}[k],\mathbb{D},\mathrm{pp})\leftrightarrow\mathrm{S}(\mathrm{SSK}[j],\mathrm{SC}[k'],\mathrm{pp}))$，其中 $\mathbb{D}=(a_i)_{i\in I}$，$\mathrm{UI}[k]=i,\mathrm{SI}[k']=j$，将 $(i,\mathrm{tkt},\mathrm{tk},f)$ 添加到 LT。

$O_{\mathrm{Iss.U}}(i,j,I,f)$：输入用户编号 i 和符合售票策略的属性集合索引 I。若 $i\notin\mathrm{HU}$，则返回 $\perp$，否则敌手 $\mathfrak{A}$ 模拟卖方 j 与诚实用户 i 交互执行票据购买协议 $(\mathrm{tkt},f,\mathrm{tk})\leftarrow\mathrm{Issue}(\mathrm{U}(\mathrm{USK}[i],\mathrm{UC}[k],\mathrm{UA}[k],\mathbb{D},\mathrm{pp})\leftrightarrow\mathfrak{A}(j,\bullet))$，其中 $\mathbb{D}=(a_i)_{i\in I},\mathrm{UI}[k]=i$，将 $(i,\mathrm{tkt},\mathrm{tk},f)$ 添加到 LT。

$O_{\mathrm{Iss.S}}(i,j,I,f)$：输入卖方编号 j 和符合售票策略的属性集合索引 I。若 $j\notin\mathrm{HS}$，则返回 $\perp$，否则敌手 $\mathfrak{A}$ 模拟用户 i 与诚实卖方 j 交互执行票据购买算法 $(\mathrm{tkt},f,\mathrm{tk})\leftarrow\mathrm{Issue}(\mathfrak{A}(i,\mathbb{D},\bullet))\leftrightarrow\mathrm{S}(\mathrm{SSK}[j],\mathrm{SC}[k'],\mathrm{pp}))$ 其中 $\mathbb{D}=(a_i)_{i\in I},\mathrm{SI}[k']=j$，将 $(i,\mathrm{tkt},\mathrm{tk},f)$ 添加到 LT。

$O_{\mathrm{Tra}}(i,i')$：输入用户编号 i 和 i'。若 $i\notin\mathrm{HU}$ 或 $i'\notin\mathrm{HU}$，则返回 $\perp$，否则执行票据转让算法 $(\mathrm{tkt}',f,\mathrm{tk}')\leftarrow\mathrm{Transfer}\ (\mathrm{U}(\mathrm{USK}[i],\mathrm{TKT}[k],\mathrm{TK}[k],\mathrm{TF}[k],\ \mathrm{pp})\leftrightarrow\mathrm{U}'\ (\mathrm{USK}[k'],\mathrm{pp}))$，其中 $\mathrm{TI}[k]=i,\mathrm{TI}[k']=i'$，将 $(i',\mathrm{tkt}',\mathrm{tk}',f)$ 添加到 LT。

$O_{\mathrm{Shw}}(i)$：输入用户编号 i。若 $i\notin\mathrm{HU}$，则返回 $\perp$，否则敌手 $\mathfrak{A}$ 模拟验票方与诚实用户 i 交互执行票据验证算法 $(b,\mathrm{tid},\mathrm{ds})\leftarrow\mathrm{Show}(\mathrm{U}(\mathrm{ssk},\mathrm{cred}_{\mathrm{u}},\mathrm{tkt},\mathrm{pp})\leftrightarrow\mathfrak{A}(\bullet))$，返回 $(b,\mathrm{tid},\mathrm{ds})$。

不可伪造性：不可伪造性保护诚实的卖方和验票方不受恶意用户的攻击。

定义 1　在 $\mathrm{Exp}^{\mathrm{unf}}(\mathfrak{A},\lambda)$（如图 2 所示）中，如果对于任意的 PPT 敌手 $\mathfrak{A}$，存在可忽略函数 $\varepsilon(\lambda)$，使

$$\left|\Pr\left[\mathrm{Exp}^{\mathrm{unf}}(\mathfrak{A},\lambda)=1\right]\right|\leqslant\varepsilon(\lambda)$$

则电子票据方案是不可伪造的。

$\mathrm{Exp}^{\mathrm{unf}}(\mathfrak{A},\lambda)$：
$O=\{O_{\mathrm{HS}},O_{\mathrm{SR}},O_{\mathrm{HU}},O_{\mathrm{UR}},O_{\mathrm{CU}},O_{\mathrm{Iss}},O_{\mathrm{Iss.S}},O_{\mathrm{Tra}},O_{\mathrm{Shw}}\}$
1. $(\mathrm{pp},\mathrm{msk},\mathbb{S})\leftarrow\mathrm{Setup}(1^{\lambda})$；
2. $(i^*,\mathrm{st})\leftarrow\mathfrak{A}^{O(\cdot)}$；
3. $(b,\bullet)\leftarrow\mathrm{Show}(\mathfrak{A}(i^*,\mathrm{st})\leftrightarrow\mathrm{V}(\mathrm{pp}))$；
4. if $(b=1\wedge i\notin\mathrm{HU})$，返回 1；else，返回 0。

图 2　不可伪造性实验

匿名性：匿名性保护诚实的用户不受恶意卖方和恶意验票方的攻击。

定义 2　在 $\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 和 $\mathrm{Exp}_2^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 中（如图 3 所示），如果对于任意的 PPT 敌手 $\mathfrak{A}$，存在可忽略函数 $\varepsilon(\lambda)$，使

$$\left|\Pr\left[\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)=1\right]\right|-\frac{1}{2}\leqslant\varepsilon(\lambda)$$

$$\left|\Pr\left[\mathrm{Exp}_2^{\mathrm{ano}}(\mathfrak{A},\lambda,b)=1\right]\right|-\frac{1}{2}\leqslant\varepsilon(\lambda)$$

则电子票据方案是匿名的。

$\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$：

$O_1=\{O_{\mathrm{HS}},O_{\mathrm{SR}},O_{\mathrm{CS}},O_{\mathrm{HU}},O_{\mathrm{UR}},O_{\mathrm{Iss}},O_{\mathrm{Iss.U}},O_{\mathrm{Tra}},O_{\mathrm{Shw}}\}$；

$O_2=\{O_{\mathrm{Iss}},O_{\mathrm{Tra}},O_{\mathrm{Shw}}\}$；

1. $(\mathrm{pp},\mathrm{msk},\mathbb{S})\leftarrow\mathrm{Setup}(1^\lambda)$；
2. $(j_0,j_1,\mathrm{st})\leftarrow\mathfrak{A}^{O_1(\cdot)}$；
3. if$(j_0\notin\mathrm{HS}\vee j_1\notin\mathrm{HS})$，返回 0；
4. $b^*\leftarrow\mathfrak{A}^{O_2(j_b,\cdot)}$；
5. if$(b=b^*)$，返回 1；else，返回 0；

$\mathrm{Exp}_2^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$：

$O_1=\{O_{\mathrm{HS}},O_{\mathrm{SR}},O_{\mathrm{CS}},O_{\mathrm{HU}},O_{\mathrm{UR}},O_{\mathrm{Iss}},O_{\mathrm{Iss.U}},O_{\mathrm{Shw}}\}$；

$O_2=\{O_{\mathrm{Iss.U}},O_{\mathrm{Shw}}\}$；

1. $(\mathrm{pp},\mathrm{msk},\mathbb{S})\leftarrow\mathrm{Setup}(1^\lambda)$；
2. $(i_0,i_1,I,\mathrm{st})\leftarrow\mathfrak{A}^{O_1(\cdot)}$；
3. if$(i_0\notin\mathrm{HU}\vee i_1\notin\mathrm{HU})$，返回 0；
4. $b^*\leftarrow\mathfrak{A}^{O_2(i_b,\cdot)}$；
5. if$(b=b^*)$，返回 1；else，返回 0。

图 3 匿名性实验

3 设计思想和方案构造

3.1 设计思想

本文方案的构造使用了集合承诺[27-28]、SPS-EQ 签名[27]、DMS 签名[29]和“Schnorr 技巧”[15]，主要面临的挑战是如何将它们结合，并构造出具有以下特点的电子票据方案。1) 在票据购买算法中，为了符合基于属性的售票策略，在用户注册时首先利用集合承诺将用户属性信息聚合为一个承诺，再使用 SPS-EQ 签名将属性承诺和用户公钥签名；在票据购买算法中，利用集合承诺打开子集算法和 SPS-EQ 修改签名算法，高效地实现了匿名的属性泄露证明。2) 在票据验证算法中，为了隐藏卖方公钥和证书，使用 SPS-EQ 签名签发卖方公钥证书；利用 SPS-EQ 签名可同时随机化消息和签名的特点，在票据验证时用户不需要获取卖方私钥就可以对卖方的公钥和证书随机化，用户仅增加了少量计算就隐藏了卖方的公钥和证书。3) 为了支持灵活的票据转让功能，使用 DMS 签名签发票据；在票据转让时，执行 DMS 签名的延展签名算法，实现了常数复杂度的票据转让和票据验证。4) 为了支持票据出现双花时的身份追踪，在票据验证算法中，首先使用公钥加密算法将用户公钥 upk 加密，再使用“Schnorr 技巧”将加密密钥 ek 隐藏起来。如果 V 检测到任何 2 个相同 tid 的票据，则立即识别到重复消费，并计算出所有双花用户的公钥。

3.2 方案构造

1) 系统初始化：$\mathrm{Setup}(1^\lambda)\rightarrow(\mathrm{pp},\mathrm{msk},\mathbb{S})$。如图 4 所示，CA 执行系统初始化算法。

证书中心：CA
① 生成售票策略集合 $\mathbb{S}$，产生双线性对参数 $\mathrm{pp}_{\mathrm{bp}}=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g,\tilde{g})$，选取 $w\xleftarrow{R}\mathbb{G}_1$；
② 选取 $q\xleftarrow{R}\mathbb{Z}_p$，计算集合承诺参数 $\mathrm{pp}_{\mathrm{sc}}=(g^{q^i},\tilde{g}^{q^i})_{i=1}^n$；
③选取 $\mathrm{msk}_{\mathrm{u}}=(x_0,x_1)\xleftarrow{R}\mathbb{Z}_p$，计算 $\mathrm{mpk}_{\mathrm{u}}=(\tilde{X}_0,\tilde{X}_1)=(\tilde{g}^{x_0},\tilde{g}^{x_1})$；
④ 选取 $\mathrm{msk}_{\mathrm{s}}=(x,y_0,\cdots,y_4)\xleftarrow{R}\mathbb{Z}_p$，计算 $\mathrm{mpk}_{\mathrm{s}}=(X,Y_0,\cdots,Y_4)=(g^x,g^{y_0},\cdots,g^{y_4})$；
⑤输出 $\mathrm{msk}=(q,\mathrm{msk}_{\mathrm{u}},\mathrm{msk}_{\mathrm{s}})$，$\mathrm{pp}=(\mathrm{pp}_{\mathrm{bp}},\mathrm{pp}_{\mathrm{sc}},\mathrm{mpk}_{\mathrm{u}},\mathrm{mpk}_{\mathrm{s}},w)$ 和 $\mathbb{S}$。

图 4 系统初始化

2) 卖方注册：$\mathrm{SReg}(\mathrm{S}(\mathrm{ssk},\mathrm{spk},\mathrm{pp})\leftrightarrow\mathrm{CA}(\mathrm{msk},\mathrm{pp}))\rightarrow\mathrm{cred}_{\mathrm{s}}$。如图 5 所示，S 与 CA 交互执行卖方注册算法。

3) 用户注册：$\mathrm{UReg}(\mathrm{U}(\mathrm{usk},\mathrm{upk},\mathbb{A},\mathrm{pp})\leftrightarrow\mathrm{CA}(\mathrm{msk},\mathrm{pp}))\rightarrow\mathrm{cred}_{\mathrm{u}}$。如图 6 所示，U 与 CA 交互执行用户注册算法。

4) 票据购买：$\mathrm{Issue}(\mathrm{U}(\mathrm{usk},\mathrm{cred}_{\mathrm{u}},\mathbb{A},\mathbb{D},\mathrm{pp})\leftrightarrow\mathrm{S}(\mathrm{ssk},\mathrm{cred}_{\mathrm{s}},\mathrm{pp}))\rightarrow(\mathrm{tkt},f,\mathrm{tk})$。如图 7 所示，U 与 S 交互执行票据购买算法。

5) 票据转让：$\mathrm{Transfer}(\mathrm{U}(\mathrm{ssk},\mathrm{tkt},\mathrm{tk},f,\mathrm{pp})\leftrightarrow\mathrm{U}'(\mathrm{ssk}',\mathrm{pp}))\rightarrow(\mathrm{tkt}',f,\mathrm{tk}')$。如图 8 所示，当 $f=1$ 时，转让用户 U 与接受用户 U′ 交互执行票据转让算法。

6) 票据验证：$\mathrm{Show}(\mathrm{U}(\mathrm{ssk},\mathrm{cred}_{\mathrm{u}},\mathrm{tkt},\mathrm{pp})\leftrightarrow\mathrm{V}(\mathrm{pp}))\rightarrow(b,\mathrm{tid},\mathrm{ds})$。如图 9 所示，U 与 V 交互执

卖方：S		证书中心：CA
选取私钥 $\mathrm{ssk}=(a,b_0,b_1,\cdots,b_4)\xleftarrow{R}\mathbb{Z}_p$，计算公钥 $\mathrm{spk}=(\tilde{A},\tilde{B}_0,\cdots,\tilde{B}_4)\leftarrow(\tilde{g}^a,\tilde{g}^{b_0},\cdots,\tilde{g}^{b_4})$；计算 $\pi_1=\mathrm{ZKSoK}\left\{(a,b_0,b_1,\cdots,b_4)\mid\tilde{A}=\tilde{g}^a\wedge\tilde{B}_i=\tilde{g}^{b_i},0\leqslant i\leqslant4\right\}$。	$\xrightarrow{\mathrm{spk},\pi_1}$	若 π_1 验证失败，返回 $\perp$；
若 $e(X,\tilde{A})\prod_{i=0}^{4}e(Y_i,\tilde{B}_i)\neq e(Y_{\mathrm{s}},\tilde{Z}_{\mathrm{s}})$ 或 $e(Y_{\mathrm{s}},\tilde{g})\neq e(g,\tilde{Y}_{\mathrm{s}})$，返回 $\perp$，否则存储证书 $\mathrm{cred}_{\mathrm{s}}$。	$\xleftarrow{\mathrm{cred}_{\mathrm{s}}}$	选取 $r_{\mathrm{s}}\xleftarrow{R}\mathbb{Z}_p$，计算 $\mathrm{cred}_{\mathrm{s}}=(Z_{\mathrm{s}},Y_{\mathrm{s}},\tilde{Y}_{\mathrm{s}})\leftarrow\left(\tilde{A}^x\prod_{i=0}^{4}\tilde{B}_i^{y_i}\right)^{r_{\mathrm{s}}},g^{r_{\mathrm{s}}^{-1}},\tilde{g}^{r_{\mathrm{s}}^{-1}})$。

图 5 卖方注册

用户：U		证书中心：CA
设置用户属性集合 $\mathbb{A}=\{a_i\}_{i=1}^{n},(a_i\in\mathbb{Z}_p)$ ； 选取私钥 $\mathrm{usk}\xleftarrow{R}\mathbb{Z}_p$ ，计算公钥 $\mathrm{upk}=g^{\mathrm{usk}}$； 计算 $\pi_2=\mathrm{ZKSoK}\{\mathrm{usk}\mid \mathrm{upk}=g^{\mathrm{usk}}\}$ ； 选取 $\rho\xleftarrow{R}\mathbb{Z}_p$ ，计算 $C_{\mathrm{u}}=F_{\mathbb{A}}(q)^{\rho},P=\tilde{g}^{\rho}$。	$\xrightarrow{\mathbb{A},\mathrm{upk},\pi_2,C_{\mathrm{u}},P}$	若π_2验证失败，返回⊥； 若 $e(C_{\mathrm{u}},\tilde{g})\neq e(F_{\mathbb{A}}(q),P)$ ，返回⊥； 选取 $r_{\mathrm{u}}\xleftarrow{R}\mathbb{Z}_p$ ，计算 $\sigma_{\mathrm{u}}=(Z_{\mathrm{u}},Y_{\mathrm{u}},\tilde{Y}_{\mathrm{u}})\leftarrow$ $((C_{\mathrm{u}}^{x_0}(\mathrm{upk})^{x_1})^{r_{\mathrm{u}}},g^{r_{\mathrm{u}}^{-1}},\tilde{g}^{r_{\mathrm{u}}^{-1}})$。
若 $e(C_{\mathrm{u}},\tilde{X}_0)e(\mathrm{upk},\tilde{X}_1)\neq e(Y_{\mathrm{u}},\tilde{Z}_{\mathrm{u}})$ 或 $e(Y_{\mathrm{u}},\tilde{g})\neq e(g,\tilde{Y}_{\mathrm{u}})$， 返回⊥，否则存储证书 $\mathrm{cred}_{\mathrm{u}}=(C_{\mathrm{u}},\mathrm{upk},\sigma_{\mathrm{u}})$。	$\xleftarrow{\sigma_{\mathrm{u}}}$	

图 6　用户注册

用户：U		卖方：S
若π_1'或$\mathrm{cred}_{\mathrm{s}}$验证失败，返回⊥；选择 $I\subseteq[1,n]$ ，设置泄露属性集合 $\mathbb{D}=\{a_i\}_{i\in I}$； 选取 $k,v\xleftarrow{R}\mathbb{Z}_p$，计算 $(C_{\mathrm{u}}',\mathrm{upk}')\leftarrow(C_{\mathrm{u}}^{v},(\mathrm{upk})^{v});\sigma_{\mathrm{u}}'=(Z_{\mathrm{u}}',Y_{\mathrm{u}}',\tilde{Y}_{\mathrm{u}}')\leftarrow(Z_{\mathrm{u}}^{kv},Y_{\mathrm{u}}^{k^{-1}},\tilde{Y}_{\mathrm{u}}^{k^{-1}})$; $\mathrm{cred}_{\mathrm{u}}'\leftarrow(C_{\mathrm{u}}',\mathrm{upk}',\sigma_{\mathrm{u}}');W=F_{\mathbb{A}\setminus\mathbb{D}}(q)^{\rho},W'=W^{v}$; 选取 $z,\mathrm{dsrnd},\mathrm{ek},\mathrm{tid}',r_0,\cdots,r_3\xleftarrow{R}\mathbb{Z}_p$ ，计算 $h'=g^{z},\alpha_0=h^{\mathrm{usk}}g^{r_0},\alpha_1=h^{\mathrm{dsrnd}}g^{r_1},\alpha_2=h^{\mathrm{ek}}g^{r_2}$, $\alpha_3=h^{\mathrm{tid}}g^{r_1},\beta_i=h'^{r_i},0\leqslant i\leqslant 3$, $\pi_3=\mathrm{ZKSoK}\left\{\begin{pmatrix}\mathrm{usk},z,\mathrm{dsid},\mathrm{ek},\\ \mathrm{tid}',r_0,\cdots,r_3,v\end{pmatrix}\middle\vert\begin{matrix}h'=g^{z}\wedge\alpha_0=h^{\mathrm{usk}}g^{r_0}\alpha_1=h^{\mathrm{dsrnd}}g^{r_1}\wedge\alpha_2=h^{\mathrm{ek}}g^{r_2}\wedge\\ \alpha_3=h^{\mathrm{tid}'}g^{r_3}\wedge\beta_i=h''^{r_i},0\leqslant i\leqslant 3\wedge\mathrm{upk}'=g^{\mathrm{usk}v}\end{matrix}\right\}$ 计算 $\mathrm{tid}=\mathrm{tid}'+\mathrm{tid}'',T_1=h,T_2=\alpha'\beta'^{-z^{-1}}$；若 $e(T_2,\tilde{g})\neq e(T_1,\tilde{A}\tilde{B}_0^{\mathrm{usk}}\tilde{B}_1^{\mathrm{dsrnd}}\tilde{B}_2^{\mathrm{ek}}\tilde{B}_3^{\mathrm{tid}}\tilde{B}_4^{\mathrm{VP}})$， 返回⊥；当$f$=1时，若 $e(h,\tilde{B}_0)\neq e(\mathrm{tk},\tilde{g})$ ，返回⊥；存储票据 $\mathrm{tkt}=(\mathrm{spk},\mathrm{cred}_{\mathrm{s}},T_1,T_2)$和tk。	$\xleftarrow{\mathrm{spk},\mathrm{cred}_{\mathrm{s}},\pi_1',\mathrm{h}}$	选取 $h\xleftarrow{R}\mathbb{G}_1$；计算 $\pi_1'=\mathrm{ZKSoK}\{(a,b_0,b_1,\cdots,b_4)\mid\tilde{A}=\tilde{g}^{a}\wedge\tilde{B}_i=\tilde{g}^{b_i},0\leqslant i\leqslant 4\}$
	$\xrightarrow{\mathrm{cred}_{\mathrm{u}}',W',\mathbb{D}}$ $h',(\alpha_i,\beta_i)_{i=0}^{3},\pi_3$	若π_3验证失败，返回⊥； 若 $e(C_{\mathrm{u}}',\tilde{X}_0)e(\mathrm{upk}',\tilde{X}_1)\neq e(Y_{\mathrm{u}}',\tilde{Z}_{\mathrm{u}}'),e(Y_{\mathrm{u}}',\tilde{g})\neq e(g,\tilde{Y}_{\mathrm{u}}')$ 返回⊥； 若 $e(W',\tilde{F}_{\mathbb{D}}(q))\neq e(C_{\mathrm{u}}',\tilde{g})$ ，返回⊥； 选取 $\mathrm{tid}''\xleftarrow{R}\mathbb{Z}_p^{*}$，设置票据有效期 $\mathrm{VP}\in\mathbb{Z}_p$，计 算 $(\alpha',\beta')\leftarrow\left(h^{a}\prod_{i=0}^{3}\alpha_i^{b_i}h^{\mathrm{tid}''b_3+\mathrm{VP}b_4},\prod_{i=0}^{3}\beta_i^{b_i}\right)$；
返回⊥；当f=1时，若 $e(h,\tilde{B}_0)\neq e(\mathrm{tk},\tilde{g})$ ，返回⊥；存储票据 $\mathrm{tkt}=(\mathrm{spk},\mathrm{cred}_{\mathrm{s}},T_1,T_2)$和tk。	$\xleftarrow{\mathrm{tid}'',\mathrm{VT},\alpha',\beta'}$ f,tk	设置票据转让标识$f\in\{0,1\}$，若f=1，令 $\mathrm{tk}=h^{b_0}$， 否则 $\mathrm{tk}=1_{\mathbb{G}_1}$。

图 7　票据购买

用户：U		用户：U′
当f=1时，可执行票据转让；选取 $r\xleftarrow{R}\mathbb{Z}_p$ ， 计算 $\mathrm{tk}'=\mathrm{tk}^{r},T_1'=T_1^{r},T_2'=(T_2(\mathrm{tk})^{-\mathrm{usk}})^{r}$	$\xrightarrow{\mathrm{spk},\mathrm{cred}_{\mathrm{s}},T_1',T_2',\mathrm{tk}'}$ $\mathrm{dsrnd},\mathrm{ek},\mathrm{tid},\mathrm{VP}$	若 $e(T_1',\tilde{B}_0)\neq e(\mathrm{tk},\tilde{g})$，返回⊥；选取 $r'\xleftarrow{R}\mathbb{Z}_p^{*}$，计算 $T_1'\leftarrow T_1'^{r'},T_2'\leftarrow(T_2'(\mathrm{tk}')^{\mathrm{usk}'})^{r'},\mathrm{tk}'\leftarrow(\mathrm{tk}')^{r'}$； 若 $e(T_2',\tilde{g})\neq e(T_1',\tilde{A}\tilde{B}_0^{\mathrm{usk}'}\tilde{B}_1^{\mathrm{dsrnd}}\tilde{B}_2^{\mathrm{ek}}\tilde{B}_3^{\mathrm{tid}}\tilde{B}_4^{\mathrm{VP}})$，返回⊥； 存储票据 $\mathrm{tkt}'=(\mathrm{spk},\mathrm{cred}_{\mathrm{s}},T_1',T_2')$ 和tk′。

图 8　票据转让

用户：U		验票方：V
选取 $r_1,r_2,k_1,k_2,k_3,v_1,v_2\xleftarrow{R}\mathbb{Z}_p$ ，计算 $\mathrm{spk}'=(\tilde{A},\tilde{B}_0',\cdots,\tilde{B}_4')\leftarrow(\tilde{A}^{v_1},\tilde{B}_0^{v_1},\cdots,\tilde{B}_4^{v_1});\mathrm{cred}_{\mathrm{s}}'=(Z_{\mathrm{s}}',Y_{\mathrm{s}}',\tilde{Y}_{\mathrm{s}}')\leftarrow(Z_{\mathrm{s}}^{v_1k_1},Y_{\mathrm{s}}^{k_1^{-1}},\tilde{Y}_{\mathrm{s}}^{k_1^{-1}})$; $(C_{\mathrm{u}}',\mathrm{upk}')\leftarrow(C_{\mathrm{u}}^{v_2},(\mathrm{upk})^{v_2});\sigma_{\mathrm{u}}'=(Z_{\mathrm{u}}',Y_{\mathrm{u}}',\tilde{Y}_{\mathrm{u}}')\leftarrow(Z_{\mathrm{u}}^{k_2v_2},Y_{\mathrm{u}}^{k_2^{-1}},\tilde{Y}_{\mathrm{u}}^{k_2^{-1}})$; $\mathrm{cred}_{\mathrm{u}}'\leftarrow(C_{\mathrm{u}}',\mathrm{upk}',\sigma_{\mathrm{u}}');\ T_1'=T_1^{r_1},T_2'=T_2^{r_1v_1};\mathrm{ch}=H(\mathrm{spk}',\mathrm{cred}_{\mathrm{s}}',\mathrm{cred}_{\mathrm{u}}',T_1',T_2')$; $s=\mathrm{dsrnd}+\mathrm{ek}\cdot\mathrm{ch};(C_1,C_2)=(w^{k_3},g^{\mathrm{usk}}w^{\mathrm{ek}k_3})$; $\kappa=\tilde{A}'\tilde{B}_0'^{\mathrm{usk}}\tilde{B}_1'^{\mathrm{dsrnd}}\tilde{B}_2'^{\mathrm{ek}}\tilde{B}_3'^{\mathrm{tid}}\tilde{B}_4'^{\mathrm{VP}}\tilde{g}^{r_2},\nu=(T_1')^{r_2}$; $\pi_4=\mathrm{ZKSoK}\left\{\begin{pmatrix}\mathrm{usk},\mathrm{dsrnd},\\ \mathrm{ek},k_3,v_2,r_2\end{pmatrix}\middle\vert\begin{matrix}\kappa=\tilde{A}'\tilde{B}_0'^{\mathrm{usk}}\tilde{B}_1'^{\mathrm{dsrnd}}\tilde{B}_2'^{\mathrm{ek}}\tilde{B}_3'^{\mathrm{tid}}\tilde{B}_4'^{\mathrm{VP}}\tilde{g}^{r_2}\wedge\nu=(T_1')^{r_2}\wedge s=\\ \mathrm{dsrnd}+\mathrm{ek}\cdot\mathrm{ch}\wedge(C_1,C_2)=(w^{k_3},g^{\mathrm{usk}}w^{\mathrm{ek}k_3})\wedge\mathrm{upk}'=g^{\mathrm{usk}v_2}\end{matrix}\right\}$	$\xrightarrow{\mathrm{spk}',\mathrm{cred}_{\mathrm{s}}',\mathrm{cred}_{u}',T_1',T_2'}$ $\mathrm{tid},\mathrm{VP},\mathrm{ch},s,\tilde{C}_1,\tilde{C}_2,\pi_4$	若 $e(X,\tilde{A}')\prod_{i=0}^{4}e(Y_i,\tilde{B}_i)\neq e(Y_{\mathrm{s}},\tilde{Z}_{\mathrm{s}})$ 或 $e(Y_{\mathrm{s}}',\tilde{g})\neq e(g,\tilde{Y}_{\mathrm{s}}')$，返回$b$=0； 若$e(C_{\mathrm{u}}',\tilde{X}_0)e(\mathrm{upk}',\tilde{X}_1)\neq e(Y_{\mathrm{u}}',\tilde{Z}_{\mathrm{u}}')$或 $e(Y_{\mathrm{u}}',\tilde{g})\neq e(g,\tilde{Y}_{\mathrm{u}}')$ ，返回b=0； 若 $e(T_1',\kappa)\neq e(T_2'\nu,\tilde{g})$，返回$b$=0； 若 π_4验证失败，返回b=0；存储 ds=(ch,s,C_1,C_2)和tid，返回b=1。

图 9　票据验证

行票据验证算法。

7) 双花追踪：$\mathrm{DsTrace}(\mathrm{tid},\mathrm{ds},\mathrm{tid}',\mathrm{ds}')\to(\mathrm{upk},\mathrm{upk}')$。若 $\mathrm{tid}=\mathrm{tid}'$，则 V 检测到重复消费。此时，V 计算 $\mathrm{ek}=\dfrac{s-s'}{\mathrm{ch}'-\mathrm{ch}}$，输出 $\mathrm{upk}=C_2C_1^{-\mathrm{ek}}$，$\mathrm{upk}'=C_2'C_1'^{-\mathrm{ek}}$。

4 安全性分析

4.1 不可伪造性

定理 1 已知 $\pi_1,\pi_1',\pi_2,\pi_3,\pi_4$ 是知识签名，如果 SPS-EQ 签名和 DMS 签名在选择消息攻击模型下是不可伪造的，集合承诺的被打开子集是不可伪造的，且离散对数问题在 $\mathbb{G}_1$ 上是难解的，那么电子票据方案是不可伪造的。

证明 在不可伪造性实验 $\mathrm{Exp}^{\mathrm{unf}}(\mathfrak{A},\lambda)$ 中，证明区分了 4 种类型的敌手。

类型 1。伪造了证书 $\mathrm{cred}_{\mathrm{u}}^*=(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$，其中 $\forall i\in\mathrm{HU}\cup\mathrm{CU},\mathrm{UC}[i]\neq\mathrm{cred}_{\mathrm{u}}^*$。此时，$\mathfrak{A}$ 伪造了一个 SPS-EQ 签名的消息签名对 $(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$。

类型 2。对于证书 $\mathrm{cred}_{\mathrm{u}}^*=(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$，其中 $\exists i\in\mathrm{CU},\mathrm{UC}[i]=\mathrm{cred}_{\mathrm{u}}^*$，伪造了泄露属性子集 $\mathbb{D}^*\notin\mathrm{UA}[i]$。此时，$\mathfrak{A}$ 伪造了一个集合承诺的打开子集证明。

类型 3。伪造了证书 $\mathrm{cred}_{\mathrm{u}}^*=(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$，其中 $\exists i\in\mathrm{HU},\mathrm{UC}[i]=\mathrm{cred}_{\mathrm{u}}^*$。此时，$\mathfrak{A}$ 计算出 $\mathbb{G}_1$ 上的离散对数。

类型 4。伪造了票据 (T_1^*,T_2^*)，其中 $\exists i\in\mathrm{HU}\cup\mathrm{CU},\mathrm{TK}[i]=(\mathrm{spk},\mathrm{cred}_{\mathrm{s}},T_1^*,T_2^*)$。此时，$\mathfrak{A}$ 伪造了一个 DMS 签名 (T_1^*,T_2^*)。证毕。

引理 1 如果存在类型 1 的敌手 $\mathfrak{A}$ 以概率 ε 赢得不可伪造性游戏，那么存在挑战者 $\mathfrak{C}$ 以相同的概率伪造了 SPS-EQ 签名。

证明 $\mathfrak{C}$ 执行 SPS-EQ 签名的不可伪造性游戏，获得参数 $\mathrm{pp}'=(\mathrm{pp}_{\mathrm{bp}},\mathrm{mpk}_{\mathrm{u}})$；$\mathfrak{C}$ 使用 pp' 作为参数产生系统剩余参数 $(\mathrm{pp}_{\mathrm{sc}},\mathrm{mpk}_{\mathrm{s}},w)$ 和 $\mathrm{msk}=(q,\mathrm{msk}_{\mathrm{s}})$。$\mathfrak{C}$ 将参数 $\mathrm{pp}=(\mathrm{pp}',\mathrm{pp}_{\mathrm{sc}},\mathrm{mpk}_{\mathrm{s}},w)$ 发送给 $\mathfrak{A}$。$\mathfrak{C}$ 能够不限次数地访问 SPS-EQ 签名预言机 $O_{\mathrm{Sign}}(\cdot)$，并向 $\mathfrak{A}$ 模拟预言机 $O_{\mathrm{HS}},O_{\mathrm{SR}},O_{\mathrm{HU}},O_{\mathrm{CU}},O_{\mathrm{Iss}},O_{\mathrm{Iss.S}},O_{\mathrm{Tra}},O_{\mathrm{Shw}}$。因为 $\mathfrak{C}$ 拥有所有用户、卖方和部分 CA 的私钥，所以这些预言机的执行与真实的游戏是一致的。

$O_{\mathrm{UR}}(i,\mathbb{A})$。对于用户注册预言机，$\mathfrak{C}$ 计算属性集合 $\mathbb{A}$ 的承诺 C_{u}，将 $(C_{\mathrm{u}},\mathrm{UPK}[i])$ 发送给 $O_{\mathrm{Sign}}(\cdot)$，获得签名 σ_{u}；$\mathfrak{C}$ 将 $(i,\mathrm{cred}_{\mathrm{u}},\mathbb{A})$ 添加到 LU。

如果敌手以 ε 的概率伪造了证书 $\mathrm{cred}_{\mathrm{u}}^*=(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$，并在票据购买算法中通过构造知识签名 π_3 通过了 S 的验证，或在票据验证算法中通过构造知识签名 π_4 通过了 V 的验证。因为 π_3,π_4 是知识签名，所以 $\mathfrak{C}$ 可执行知识提取器获取证据 (usk,v)，其中 $\mathrm{upk}^*=\mathrm{upk}^v$。因为此处考虑类型 1 的伪造，所以对 $\forall i\in\mathrm{HU}\cup\mathrm{CU},\mathrm{UC}[i]\neq((C_{\mathrm{u}}^*)^{v^{-1}},\ (\mathrm{upk}^*)^{v^{-1}},\bullet)$，$\mathfrak{C}$ 没有询问过等价类 $(C_{\mathrm{u}}^*,\mathrm{upk}^*)$ 的签名。因为 $\mathfrak{C}$ 的模拟不会中断，所以 $\mathfrak{C}$ 以 ε 的概率伪造了 SPS-EQ 签名的消息签名对 $(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$。证毕。

引理 2 如果存在类型 2 的敌手 $\mathfrak{A}$ 以概率 ε 赢得不可伪造性游戏，那么存在挑战者 $\mathfrak{C}$ 以相同的概率伪造了集合承诺的打开子集证明。

证明 $\mathfrak{C}$ 执行集合承诺的不可伪造性游戏，获得参数 $\mathrm{pp}'=(\mathrm{pp}_{\mathrm{sc}},g,\tilde{g})$；$\mathfrak{C}$ 使用 pp' 作为参数产生系统剩余参数 $(\mathbb{G}_T,e,\mathrm{mpk}_{\mathrm{u}},\mathrm{mpk}_{\mathrm{s}},w)$ 和 $\mathrm{msk}=(\mathrm{msk}_{\mathrm{u}},\mathrm{msk}_{\mathrm{s}})$。$\mathfrak{C}$ 将参数 pp 发送给 $\mathfrak{A}$。因为任何参与实体根据集合承诺的参数都可计算承诺，所以所有预言机的执行都与真实的游戏是一致的。

如果在票据购买算法中，敌手输出了一个有效的证明 $(\mathrm{cred}_{\mathrm{u}}^*,W^*,\mathbb{D}^*,\pi_3,\cdots)$，并通过了 $\mathfrak{C}$ 的验证。因为 π_3 是知识签名，所以 $\mathfrak{C}$ 可执行知识提取器获取证据 (usk,v)，其中 $\mathrm{upk}^*=\mathrm{upk}^v$。此处考虑类型 2 的伪造，对 $\exists i\in\mathrm{CU},\mathrm{UC}[i]=((C_{\mathrm{u}}^*)^{v^{-1}},(\mathrm{upk}^*)^{v^{-1}},\bullet)$，且属性子集 $\mathbb{D}^*\notin\mathrm{UA}[i]$。因此，$\mathfrak{C}$ 伪造了属性集合 $\mathrm{UA}[i]$ 承诺 C_{u}^* 的泄露子集 $\mathbb{D}^*$ 和隐藏子集承诺 W'^*，且打开集合承诺的证据为 v。证毕。

引理 3 如果存在类型 3 的敌手 $\mathfrak{A}$ 以概率 ε 赢得不可伪造性游戏，那么存在挑战者 $\mathfrak{C}$ 以 $\dfrac{\varepsilon}{m}$ 的概率计算出 $\mathbb{G}_1$ 上的离散对数，其中 m 为诚实卖方的数量。

证明 设 $(\mathbb{G}_1,g,g^x)$ 是一个离散对数挑战，$\mathfrak{C}$ 使用 $(\mathbb{G}_1,g)$ 作为参数产生剩余参数，并将参数 pp 发送给 $\mathfrak{A}$。在不可伪造性游戏中，$\mathfrak{C}$ 猜测诚实用户 $i^*\in\mathrm{HU}$，游戏结束时如果敌手伪造了 i^* 的证书，$\mathfrak{C}$ 可通过知识提取器获得 x。$\mathfrak{C}$ 向 $\mathfrak{A}$ 模拟预言机。

$O_{\mathrm{HS}},O_{\mathrm{SR}},O_{\mathrm{Iss.S}},O_{\mathrm{Tra}}$。因为 $\mathfrak{C}$ 知道卖方和 CA 的私钥，所以这些预言机的执行与真实的游戏一致。

$O_{\mathrm{HU}}(i)$。如果 $i\neq i^*$，预言机的执行与真实的游

戏是一致的；如果 $i=i^*$，$\mathfrak{C}$ 设置 $\mathrm{UPK}[i]=g^x$。

$O_{\mathrm{CU}}(i)$。如果 $i\neq i^*$，预言机的执行与真实的游戏是一致的；如果 $i=i^*$，返回 $\perp$。

$O_{\mathrm{UR}}(i,\mathbb{A}),O_{\mathrm{Iss}}(i,j,I,f),O_{\mathrm{Shw}}(i)$。如果 $i\neq i^*$，那么这些预言机的执行与真实的游戏是一致的；如果 $i=i^*$，$\mathfrak{C}$ 模拟知识签名 π_2,π_3 和 π_4。

因为此处考虑类型 3 的伪造，如果敌手以 ε 的概率伪造了诚实用户 i 的证书 $\mathrm{cred}_{\mathrm{u}}^*=(C_{\mathrm{u}}^*,\mathrm{upk}^*,\sigma_{\mathrm{u}}^*)$，并在票据购买算法中通过构造知识签名 π_3 通过了 S 的验证，或在票据验证算法中通过构造知识签名 π_4 通过了 V 的验证。如果 $i\neq i^*$，游戏中断；否则，因为 π_3,π_4 是知识签名，$\mathfrak{C}$ 可执行知识提取器获取证据 (usk,v)，其中 $\mathrm{usk}=x$。因为游戏中断的概率为 $m-\dfrac{1}{m}$，所以 $\mathfrak{C}$ 以 $\dfrac{\varepsilon}{m}$ 的概率计算出离散对数。证毕。

引理 4　如果存在类型 4 的敌手 $\mathfrak{A}$ 以概率 ε 赢得不可伪造性游戏，那么存在挑战者 $\mathfrak{C}$ 以 $\dfrac{\varepsilon}{m}$ 的概率伪造了 DMS 签名，其中 m 为诚实卖方的数量。

证明　$\mathfrak{C}$ 执行 DMS 签名的不可伪造性游戏，获得参数 $(\mathrm{pp}_{\mathrm{bp}},\mathrm{spk}^*)$。$\mathfrak{C}$ 使用 $\mathrm{pp}_{\mathrm{bp}}$ 作为参数产生系统剩余参数，并将参数 pp 发送给 $\mathfrak{A}$。在 DMS 签名的不可伪造性游戏中，$\mathfrak{C}$ 能够不限次数地访问 DMS 签名预言机 $O_{\mathrm{Sign}}(\cdot)$。在电子票据的不可伪造性游戏中，$\mathfrak{C}$ 猜测诚实卖方 $j^*\in\mathrm{HS}$，如果游戏结束时敌手伪造了卖方 j^* 签发的票据，$\mathfrak{C}$ 就获得了一个伪造的 DMS 签名。$\mathfrak{C}$ 向 $\mathfrak{A}$ 模拟预言机。

$O_{\mathrm{HU}},O_{\mathrm{UR}},O_{\mathrm{CU}},O_{\mathrm{Tra}},O_{\mathrm{Shw}}$。因为 $\mathfrak{C}$ 知道 CA 和用户的私钥，所以这些预言机的执行与真实的游戏一致。

$O_{\mathrm{HS}}(j)$。如果 $j\neq j^*$，预言机的执行与真实的游戏是一致的；如果 $j=j^*$，令 $\mathrm{SPK}[j]=\mathrm{spk}^*$。

$O_{\mathrm{SR}}(j)$。如果 $j\neq j^*$，预言机的执行与真实的游戏是一致的；如果 $j=j^*$，$\mathfrak{C}$ 模拟知识签名 π_2。

$O_{\mathrm{Iss}}(i,j,I,f),O_{\mathrm{Iss.S}}(i,j,I,f)$。如果 $j\neq j^*$，预言机的执行与真实的游戏是一致的；如果 $j=j^*$，$\mathfrak{C}$ 模拟知识签名 π_2；收到用户的购票申请后，$\mathfrak{C}$ 通过知识提取器从知识签名 π_3 中提取 $(z,\mathrm{usk},\mathrm{dsrnd},\mathrm{ek},\mathrm{tid}',r_0,\cdots,r_3)$；$\mathfrak{C}$ 随机选取 tid''，计算 $\mathrm{tid}=\mathrm{tid}'+\mathrm{tid}''$，设置票据有效期 $\mathrm{VP}\in\mathbb{Z}_p$，将 $(\mathrm{usk},\mathrm{dsrnd},\mathrm{ek},\mathrm{tid},\mathrm{VP})$ 和 $(r_0,\cdots,r_3)$ 分别发送 DMS 签名预言机 $O_{\mathrm{Sign}}(\cdot)$，并获得签名 (h,δ_1) 和 $(1_{\mathbb{G}_1},\delta_2)$；然后 $\mathfrak{C}$ 计算 $(\alpha',\beta')\leftarrow(\delta_1 g^{\sum_{i=0}^{3}r_i},\delta_1^z)$。

最后，敌手以 ε 的概率伪造了诚实卖方 j 签发的票据 (T_1^*,T_2^*)，并在票据验证算法中通过构造知识签名 π_4 通过了 V 的验证。如果 $j\neq j^*$，游戏中断；如果 $j=j^*$，因为 π_4 是知识签名，$\mathfrak{C}$ 可执行知识提取器获取证据 $(\mathrm{usk}^*,\mathrm{dsrnd}^*,\mathrm{ek}^*)$。因为此处考虑类型 4 的伪造，对 $\forall i\in\mathrm{HU}\cup\mathrm{CU},\mathrm{TK}[i]\neq(T_1^*,T_2^*)$，$\mathfrak{C}$ 没有询问过 $(\mathrm{usk}^*,\mathrm{dsrnd}^*,\mathrm{ek}^*,\mathrm{tid}^*,\mathrm{VP}^*)$ 的 DMS 签名，其中 tid^* 和 VP^* 是敌手在票据验证时泄露的。因为 $\mathfrak{C}$ 中断的概率为 $m-\dfrac{1}{m}$，所以 $\mathfrak{C}$ 以 $\dfrac{\varepsilon}{m}$ 的概率伪造了消息 $(\mathrm{usk}^*,\mathrm{dsrnd}^*,\mathrm{ek}^*,\mathrm{tid}^*,\mathrm{VP}^*)$ 的 DMS 签名 (T_1^*,T_2^*)。证毕。

4.2　匿名性

定理 2　已知 π_1',π_3,π_4 是知识签名，如果 SPS-EQ 签名满足签名适应性和明文空间的类隐藏性，DMS 签名具有完美的派生隐私性，那么电子票据方案满足匿名性。

证明　在匿名性实验 $\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 中，敌手 $\mathfrak{A}$ 模拟恶意的验票方，试图在票据验证算法中区分卖方身份。在匿名性实验 $\mathrm{Exp}_2^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 中，敌手 $\mathfrak{A}$ 模拟恶意的卖方，试图在票据购买或票据验证算法中区分用户身份。

引理 5　在实验 $\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 中，如果 SPS-EQ 签名满足签名适应性和明文空间的类隐藏性，那么电子票据方案满足匿名性。

证明　挑战者 $\mathfrak{C}$ 执行 $(\mathrm{pp},\mathrm{msk},\mathbb{S})\leftarrow\mathrm{Setup}(1^\lambda)$ 产生 CA 私钥和系统参数，并将 $(\mathrm{pp},\mathbb{S})$ 发送给 $\mathfrak{A}$。在匿名性游戏中，$\mathfrak{C}$ 猜测 $\mathfrak{A}$ 要区分的诚实卖方 $j^*\in\mathrm{HS}$。通过定义不可区分的游戏序列的方式可以证明，在最后的游戏中 $\mathfrak{A}$ 成功的概率是可忽略的。

Game_0。与 $\mathrm{Exp}_1^{\mathrm{ano}}(\mathfrak{A},\lambda,b)$ 相同。

Game_1。在预言机 O_{Iss}、$O_{\mathrm{Iss.U}}$、O_{Shw} 中，如果 $j=j^*$，使用 SPS-EQ 的签名算法代替修改签名算法，其他操作与 Game_0 相同。因为 $\mathfrak{C}$ 知道 CA 的私钥，所以上述代替可以实现。因为 SPS-EQ 签名满足签名适应性和明文空间的类隐藏性，因此 $\left|\Pr[\mathrm{Game}_0=1]\right|=\left|\Pr[\mathrm{Game}_1]=1\right|$。

表 2 功能比较

方案	匿名性	属性票据（证书）	属性泄露	卖方匿名性	可转让票据	票据转让	双花检测	双花追踪	形式化证明
文献[22]	√	×	—	×	×	—	√	×	×
文献[3]	√	×	—	×	×	—	√	√	×
文献[25]	√	×	—	×	×	—	√	√	×
文献[12]	√	√	ZKP	—	—	—	—	—	√
文献[13]	√	√	ZKP	—	—	—	—	—	√
文献[14]	√	√	ZKP	—	—	—	—	—	√
文献[2]	√	√	ZKP	×	×	—	√	√	√
文献[5-6]	√	×	—	×	√	签名链	√	√	√
本文方案	√	√	SPS-EQ	√	√	DMS	√	√	√

Game_2。在预言机 O_{Iss}、$O_{\text{Iss.U}}$、O_{Shw} 中，如果 $j=j^*$，使用 DMS 的签名算法代替延展签名算法，其他操作与 Game_1 相同。因为 $\mathfrak{C}$ 知道 S 的私钥，所以上述代替可以实现。因为 DMS 签名具有完美的派生隐私性，所以 $\left|\Pr\left[\text{Game}_1\right]=1\right|=\left|\Pr\left[\text{Game}_2\right]=1\right|$。

Game_3。在预言机 O_{Iss}、$O_{\text{Iss.U}}$、O_{Shw} 中，如果 $j=j^*$，模拟知识签名 π_1',π_3,π_4，其他操作与 Game_2 相同。因为知识签名的模拟是完美的，因此 $\left|\Pr\left[\text{Game}_2\right]=1\right|=\left|\Pr\left[\text{Game}_3\right]=1\right|$。

Game_4。m 是诚实卖方的数量，在游戏的第一阶段，敌手 $\mathfrak{A}$ 输出 2 个卖方 j_0 和 j_1。在第二阶段，$\mathfrak{C}$ 随机选择 $b\in\{0,1\}$，如果 $j_b\neq j^*$ 则返回 $\perp$，否则 $\mathfrak{A}$ 猜测票据卖方 j_b，其他的操作与 Game_3 相同。因为 Game_4 返回失败的概率为 $m-\dfrac{1}{m}$，所以 $\left|\Pr\left[\text{Game}_4\right]=1\right|=\dfrac{\left|\Pr\left[\text{Game}_3\right]=1\right|}{m}$。当 $j_b=j^*$ 时，因为知识签名的模拟是完美的，SPS-EQ 签名满足签名适应性和明文空间的类隐藏性，且 DMS 签名具有完美的派生隐私性，所以 $\left|\Pr\left[\text{Game}_4\right]=1\right|\leqslant\varepsilon$。

5 效率分析

5.1 理论分析

表 2 将本文方案与最近提出的电子票据方案和属性证书方案在功能上进行了比较，其中√表示支持，×表示不支持，—表示不涉及此项。文献[19]方案实现了匿名性和双花检测，但是不支持属性票据和可转让票据，不能实现卖方的匿名性和双花追踪。文献[3,21]方案实现了匿名性、双花追踪和双花检测，但是不支持属性票据、可转让票据和双花追踪。文献[12-14]方案支持匿名性和属性证书，但是其属性泄露证明使用了 ZKP。文献[2]方案支持匿名性、属性票据、双花追踪和双花检测，并给出了正式的安全证明，但是其不支持票据转让，属性泄露证明使用了 ZKP 实现。文献[5-6]方案支持可转让票据、双花检测和双花追踪，但是其不支持属性票据和卖方的匿名性，并且该方案使用签名链实现票据转让，导致票据转让和票据验证算法的计算复杂度随着转让次数的增加线性增长。本文方案不仅支持匿名性、属性票据、可转让、双花检测和双花追踪等功能，而且使用 SPS-EQ 签名实现了高效的属性泄露证明和卖方的匿名性，使用 DMS 签名实现了常数复杂度的票据转让和票据验证。

表 3 将本文方案与文献[2]方案在效率上进行了比较，其中 n 和 k 分别为用户属性数量和泄露属性数量。本文方案将票据购买算法中用户的计算复杂度从 $O(n)$ 降低到 $O(n-k)$，将卖方的计算复杂度从 $O(n)$ 降低到 $O(k)$。

表 3 与文献[2]方案的效率比较

算法	执行实体	本文方案	文献[2]方案
系统初始化	CA	$O(n)$	$O(n)$
卖方注册	S	$O(1)$	$O(1)$
	CA	$O(1)$	$O(1)$
用户注册	U	$O(n)$	$O(n)$
	CA	$O(n)$	$O(n)$
票据购买	U	$O(n-k)$	$O(n)$
	S	$O(k)$	$O(n)$
票据验证	U	$O(1)$	$O(1)$
	V	$O(1)$	$O(1)$
双花追踪	V	$O(1)$	$O(1)$

表 4 将本文方案与文献[5-6]方案在票据转让和票据验证算法的效率上进行了比较，其中 t 为票据转让次数。本文方案将票据转让算法中用户 U′ 的计算复杂度从 $O(t)$ 降低到 $O(1)$，将票据验证算法中验票方的计算复杂度从 $O(t)$ 降低到 $O(1)$，实现了常数复杂度的票据转让和票据验证。

表 4　　与文献[5-6]方案的效率比较

算法	执行实体	本文方案	文献[5-6]方案
票据转让	U	$O(1)$	$O(1)$
	U′	$O(1)$	$O(t)$
票据验证	U	$O(1)$	$O(1)$
	V	$O(1)$	$O(t)$

5.2　实验分析

使用基于数论的密码库 MIRACL 和 Type-3 双线性对实现了本文方案。其中椭圆曲线使用 AES-100 比特安全级别的 Barreto-Naehrig 曲线（BN-256）。实验平台为 HUAWEI MateBook，CPU 为 AMD Ryzen-5 4600H，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++。

图 10 将本文方案与文献[2]方案中的算法运行时间进行了对比，其中测试时设置用户属性数量 $n=10$，泄露属性数量 $k=3$。1-CA 表示系统初始化算法；2-S 表示卖方注册算法的卖方计算部分，2-CA 表示卖方注册算法的 CA 计算部分；3-U 表示用户注册算法的用户计算部分，3-CA 表示用户注册算法的 CA 计算部分；4-U 表示票据购买算法的用户计算部分，4-S 表示票据购买算法的卖方计算部分；5-U 表示票据验证算法的用户计算部分，5-V 表示票据验证算法的验票方计算部分。由图 10 可知，本文方案各个算法的运行时间仅分别为文献[2]方案的 4%、10%、45.6%、4%、16.6%、5.8%、4.3%、3.7%和 16.4%。

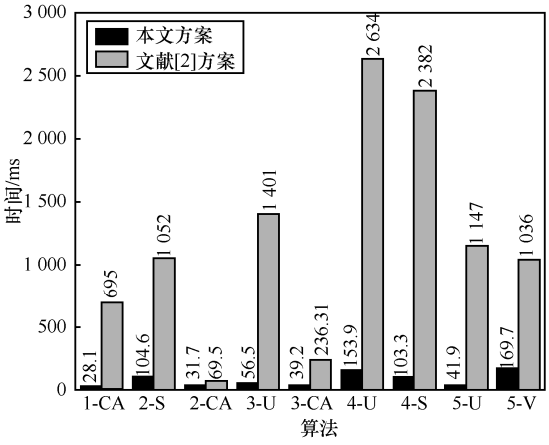

图 10　运行时间比较

图 11 是随着用户属性数量的增多，本文方案和文献[2]方案中的票据购买算法运行时间对比，其中在测试时设置泄露属性数量 $k=5$，用户属性数量 $n=\{20,40,60,80,100\}$。其中图 11(a)为票据购买算法用户计算部分的比较，图 11(b)为票据购买算法卖方计算部分的比较。由图 11(a)可知，本文方案和文献[2]方案的用户计算时间都随用户属性数量的增加线性增长，但是本文方案的时间消耗仅约为文献[2]方案的 6%。由图 11(b)可知，文献[2]方案的卖方计算时间随用户属性数量的增加线性增长，但是本文方案的计算时间（约为 107 ms）与属性数量无关，且本文方案的时间消耗仅约为文献[2]方案的 4%。

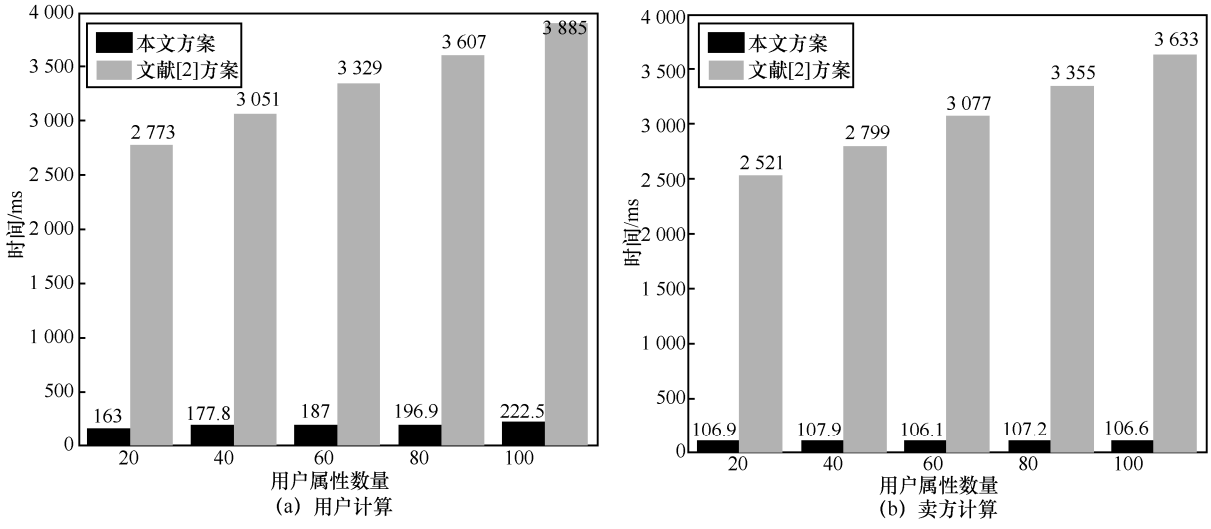

图 11　票据购买算法运行时间比较

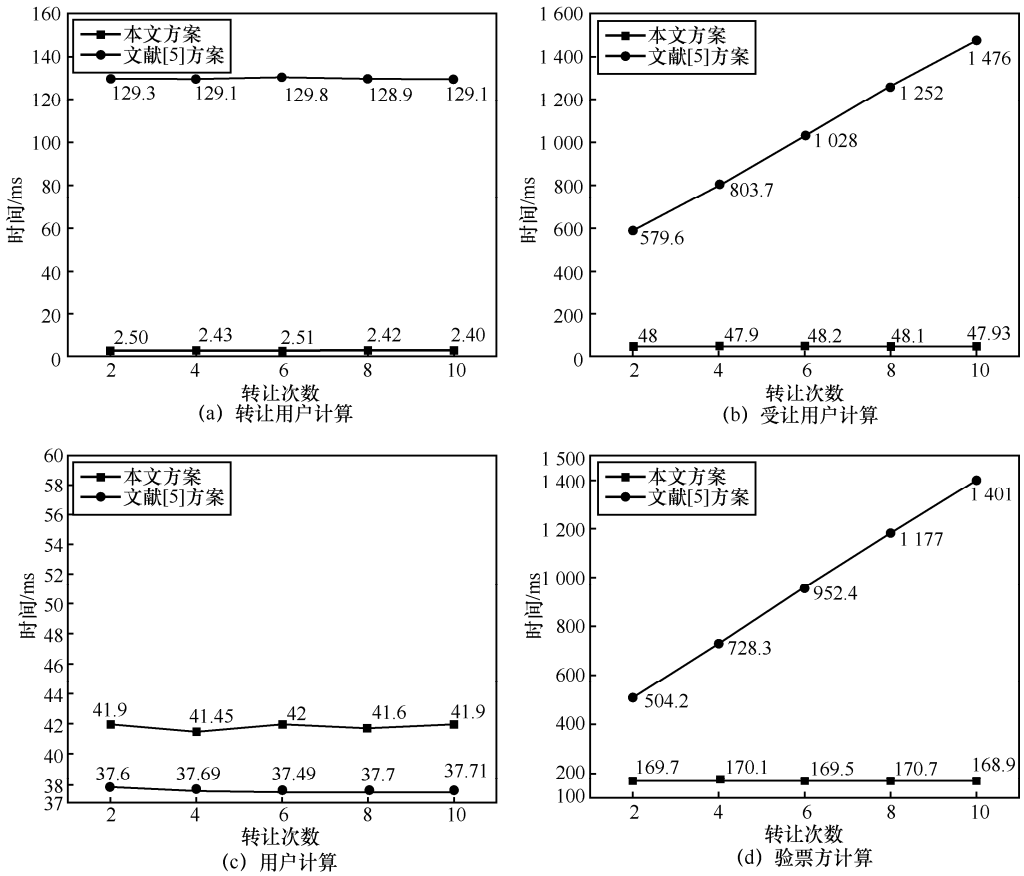

图 12 票据转让和验证算法中票据转让次数与运行时间关系

图 12 是随着票据转让次数的增加，本文方案和文献[5]方案中的票据转让和票据验证算法运行时间的对比，其中测试时设置用户属性数量 $n=10$，泄露属性数量 $k=3$，转让次数 $t=\{2,4,6,8,10\}$。其中图 12(a)为票据转让算法转让用户计算部分的比较，图 12(b)为票据转让算法受让用户计算部分的比较，图 12(c)为票据验证算法用户计算部分的比较，图 12(d)为票据验证算法验票方计算部分的比较。由图 12(a)可知，本文方案和文献[5]方案的票据转让算法的转让用户计算时间都与转让次数无关，其中本文方案和文献[5]方案耗时分别约 2.5 ms 和 129 ms，本文方案的时间消耗仅约为文献[5]方案的 2%。由图 12(b)可知，文献[5]方案的受让用户的计算时间随着转让次数的增加线性增长，但是本文方案的计算时间（约为 48 ms）与转让次数无关，且本文方案的时间消耗仅约为文献[5]方案的 9%。由图 12(c)可知，本文方案和文献[5]方案的票据验证算法的用户计算时间都与转让次数无关，其中本文方案和文献[5]方案耗时分别约 42 ms 和 37 ms，2 种方案的时间消耗基本相当。由图 12(d)可知，文献[5]方案的验证方计算时间随着转让次数的增加线性增长，但是本文方案的计算时间（约为 170 ms）与转让次数无关，且本文方案的时间消耗仅约为文献[5]方案的 34%。

以上分析和比较表明，本文方案与目前最新的电子票据方案相比，计算开销显著降低。

6 结束语

本文构造了高效的强隐私保护且支持属性策略和票据转让功能的电子票据方案。与目前的电子票据方案相比，本文方案不仅支持匿名性、属性票据、可转让、双花检测和双花追踪等功能，而且显著降低了票据购买算法的计算消耗，实现了常数复杂度的票据转让和验证算法，并以较少的计算代价实现了卖方的匿名性。

参考文献：

[1] HAN J G, CHEN L Q, SCHNEIDER S, et al. Anonymous single sign-on with proxy re-verification[J]. IEEE Transactions on Information Forensics and Security, 2020, 15: 223-236.

[2] 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.
[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] CHAUM D. Security without identification: transaction systems to make big brother obsolete[J]. Communications of the ACM, 1985, 28(10): 1030-1044.
[5] 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, 2014: 100-113.
[6] PAYERAS-CAPELLÀ M M, MUT-PUIGSERVER M, CASTELLÀ-ROCA J, et al. Design and performance evaluation of two approaches to obtain anonymity in transferable electronic ticketing schemes[J]. Mobile Networks and Applications, 2017, 22(6): 1137-1156.
[7] 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.
[8] CAMENISCH J, LYSYANSKAYA A. An efficient system for non-transferable anonymous credentials with optional anonymity revocation[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001: 93-118.
[9] LYSYANSKAYA A, RIVEST R L, SAHAI A, et al. Pseudonym systems[C]//International Workshop on Selected Areas in Cryptography. Berlin: Springer, 2000: 184-199.
[10] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Berlin: Springer, 1983: 199-203.
[11] CHAUM D, VAN HEYST E. Group signatures[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Berlin: Springer, 1991: 257-265.
[12] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]//Advances in Cryptology – CRYPTO 2004. Berlin: Springer, 2004: 56-72.
[13] AU M H, SUSILO W, MU Y. Constant-size dynamic k-TAA[C]// International Conference on Security and Cryptography for Networks. Berlin: Springer, 2006: 111-125.
[14] POINTCHEVAL D, SANDERS O. Short randomizable signatures[J]. IACR Cryptology ePrint Archive, 2015, 2015: 525.
[15] BOBOLZ J, EIDENS F, KRENN S, et al. Privacy-preserving incentive systems with highly efficient point-collection[C]//Proceedings of the 15th ACM Asia Conference on Computer and Communications Security. New York: ACM Press, 2020: 319-333.
[16] QUERCIA D, HAILES S. MOTET: mobile transactions using electronic tickets[C]//Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks. Piscataway: IEEE Press, 2005: 374-383.
[17] 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.
[18] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[C]//Advances in Cryptology — ASIACRYPT 2001. Springer: Berlin, 2001: 514-532.
[19] 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.
[20] ABE M, OKAMOTO T. Provably secure partially blind signatures[C]//Advances in Cryptology — CRYPTO 2000. Springer: Berlin, 2000: 271-286.
[21] PEDERSEN T P. Non-interactive and information-theoretic secure verifiable secret sharing[C]//Advances in Cryptology — CRYPTO'91. Springer: Berlin, 1992: 129-140.
[22] NAKANISHI T, HARUNA N, SUGIYAMA Y. Unlinkable electronic coupon protocol with anonymity control[C]//International Workshop on Information Security. Berlin: Springer, 1999: 37-46.
[23] 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. New York: ACM Press, 2010: 387-392.
[24] BONEH D, BOYEN X. Short signatures without random ora-cles[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Springer: Berlin, 2004: 56-73.
[25] VIVES-GUASCH A, PAYERAS-CAPELLÀ M M, MUT- PUIGSERVER M, et al. A secure E-ticketing scheme for mobile devices with near field communication (NFC) that includes exculpability and reusability[J]. IEICE Transactions on Information and Systems, 2012, 95(1): 78-93.
[26] CHASE M, LYSYANSKAYA A. On signatures of knowledge[C]// Annual International Cryptology Conference. Berlin: Springer, 2006: 78-96.
[27] FUCHSBAUER G, HANSER C, SLAMANIG D. Structure-preserving signatures on equivalence classes and constant-size anonymous credentials[J]. Journal of Cryptology, 2019, 32(2): 498-546.
[28] HANSER C, SLAMANIG D. Structure-preserving signatures on equivalence classes and their application to anonymous credentials[C]//International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2014: 491-511.
[29] BLÖMER J, BOBOLZ J. Delegatable attribute-based anonymous credentials from dynamically malleable signatures[C]// International Conference on Applied Cryptography and Network Security. Berlin: Springer, 2018: 221-239.

[作者简介]

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。

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。

袁峰（1982− ），男，北京人，博士，中国航天科工集团第二研究院 706 所研究员，主要研究方向为密码学和信息安全。

李艳俊（1979− ），女，山西晋城人，博士，中国电子科技集团第十五研究所研究员，主要研究方向为密码学和信息安全。

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。