# 基于智能卡的可追踪撤销匿名凭证方案

莫晓翰 赖俊祚 吴 驰 孙 萌
（暨南大学网络空间安全学院 广州 510632）

**摘 要** 匿名凭证是一种有效解决隐私安全问题的方案，由发证机构为用户的属性进行签名，用户在提供凭证时不泄露个人身份信息，并选择性地揭露相关属性。基本的匿名凭证方案包含凭证的颁发、展示以及验证。验证者仅检验用户提供的属性是否满足访问策略以及凭证是否正确有效。若用户的凭证意外丢失或遭到窃取，获得此凭证的第三方在了解相关信息的情况下能够使用凭证通过验证者的检验。因此，Hesse和Singh提出了基于智能卡的匿名凭证方案，引入一张嵌有用户头像图片的智能卡，通过卡上的人脸图片与用户进行绑定。若第三方获得用户凭证，由于卡上的人脸图片与其不匹配，第三方无法使用该凭证通过验证者检验。然而，针对凭证匿名性带来的恶意用户追责问题，例如追踪和撤销功能，该方案并没有实现，存在一定的安全隐患。因此，本文提出了基于智能卡的可追踪撤销匿名凭证方案，同时实现了追踪和撤销功能。若用户违反协议，相关权威机构可以追踪到该匿名用户并进行撤销。通过安全性、功能、计算开销分析和性能评估，本文所提方案被证实是安全且高效的。

**关键词** 隐私保护；匿名凭证；基于智能卡；可追踪性；撤销
**中图法分类号** TP309 **DOI号** 10.11897/SP.J.1016.2026.00918

# Card-Based Anonymous Credential Scheme Simultaneously Achieves Revocation and Traceability

MO Xiao-Han LAI Jun-Zuo WU Chi SUN Meng
（College of Cyber Security, Jinan University, Guangzhou 510632）

**Abstract** Anonymous credentials are an effective solution to privacy and security issues, where an issuer signs a user's attributes to create an attribute-based anonymous credential. Users provide credentials without revealing personally identifiable information and selectively disclose relevant attributes. The core objective of anonymous credential is to protect the privacy of the user while ensuring the validity of the authentication. Anonymity is one of its key characteristics. Anonymity means that the user does not reveal his/her identity when presenting the credentials to the service provider, but only proves the validity of the credentials through zero-knowledge proofs. A zero-knowledge proof is a cryptographic protocol in which one party (the prover) can demonstrate to another (the verifier) that they possess certain knowledge, without disclosing any part of that knowledge during the interactive process. Consequently, the service provider becomes convinced that the credential is valid and was issued by a legitimate issuer, but learns nothing about the user's identity beyond what is explicitly disclosed. Selective disclosure complements this by giving users fine-grained control over their data. It refers to the user's ability to provide only a subset of the attributes embedded within their credential, specifically those required by the service provider's policy, rather than being forced to present all attributes in their entirety. A

收稿日期：2024-04-11；在线发布日期：2025-11-12。本课题得到国家自然科学基金青年科学基金项目（A类）（No. 62525206）、国家自然科学基金面上项目（No. 62472198）、广东省基础与应用基础研究基金（No. 2023B1515040020）资助。**莫晓翰**，硕士，主要研究领域为密码学与信息安全。E-mail：xiaohanmoz@outlook.com。**赖俊祚**（通信作者），博士，教授，主要研究领域为密码学与信息安全。E-mail：laijunzuo@gmail.com。**吴 驰**，硕士，主要研究领域为密码学与信息安全。**孙 萌**，博士研究生，主要研究领域为密码学与信息安全。

basic anonymous credential scheme involves the issuance, presentation, and verification of credentials. The verifier only checks whether the attributes provided by the user satisfy the access policy and whether the user's credential is valid. If the user's credential is accidentally lost or stolen, a third party who obtains the credential will be able to use it to pass the verifier's verification with the knowledge of the relevant information. To counter this threat, Hesse and Singh proposed a card-based anonymous credential scheme, which introduces a smart card embedded with a picture of the user, and binds the user to the card through the picture on the card. In their proposed system, the user must physically present his/her smart card to service provider in person. During the verification process, the service provider not only verifies the validity of the user's digital credential but also performs a crucial visual check: confirming whether the picture on the smart card matches the physical appearance of the user. This simple yet effective measure provides a strong layer of security. If a third party obtains user credentials, the third party is unable to use the credentials to pass the verifier's verification due to the picture on the card failing to match him. However, the scheme does not address the problem of malicious users' accountability due to the anonymity of credentials, such as tracing and revocation functionalities, and this poses certain security risks. Therefore, this paper proposes a card-based anonymous credential scheme that simultaneously achieves revocation and traceability. If a user violates the protocol, the relevant authority can trace the user and revoke it. The proposed scheme is proven to be secure and efficient through security analysis, functionality comparison, computational cost analysis and performance evaluation.

**Keywords** privacy-preservation; anonymous credentials; card-based; traceability; revocation

## 1 引 言

匿名凭证是一种在不泄露用户个人身份和其他无关信息的情况下允许用户证明自己拥有某些特定属性的数字凭证。其设计的核心目标是保护用户的隐私，同时确保身份认证的可靠性。匿名凭证通常由发证机构颁发，使用私钥对用户的属性进行数字签名，从而生成基于属性的匿名凭证。匿名性指的是用户向服务提供商出示凭证的时候不会透露自己的身份，并能向其证明凭证的有效性。通常，凭证支持用户进行选择性揭露[1]。选择性揭露指的是用户可以在出示凭证时只提供服务提供商需要的属性，而不是出示凭证上所有的属性。

当前，匿名凭证主要是多次使用凭证，即在满足不可链接性的同时允许凭证的多次使用，在匿名订阅[2]、电子票据[3]、在线服务的访问控制[4]等方面具有广泛的应用场景。研究者们使用CL签名[5]、PS签名[6]、BBS签名[7-8]、可净化签名(Sanitizable Signatures, SS)[9]、等价类上的结构保持签名(Structure-Preserving Signatures on Equivalence Classes, SPS-EQ)[10]等签名算法构造匿名凭证方案。

近年来，除了传统的单设备匿名凭证方案，还出现了多设备的匿名凭证方案。多设备场景一般包含一张智能卡和一个外部设备。构建多设备的匿名凭证的原因包含两个，一个是设备和智能卡之间资源的不对称性，例如为了让智能卡的计算负载不受属性数量的影响；另一个是利用智能卡中存在的安全元件来防止凭证克隆或盗窃。传统的基于属性的匿名凭证方案中，用户向服务提供商展示凭证只会公开访问策略需要的属性集合，而不会透露其他有用的身份信息，这是凭证的匿名性决定的。但其中暗含着一个问题，即服务提供商如何确认该用户就是该凭证的合法拥有者，确认该凭证就是颁发给该用户的。传统的匿名凭证方案仅能让验证者确认该用户给出的凭证是合法的。当该用户的凭证意外丢失或遭到窃取，获取此凭证的第三方在了解相关属性及其他秘密的情况下可以使用凭证通过服务提供商的检验，即使该凭证并不是颁发给他的。因此，针对此问题，Hesse和Singh提出了基于智能卡的匿名凭证(card-based Anonymous Credentials, cbAC)[11]。该方案引入一张嵌有用户头像图片的智能卡，通过卡上的人脸图片与用户进行绑定。若第三方获得用户凭证，由于卡上的人脸图片与其不匹配，第三方无

法使用该凭证通过验证者检验。智能卡的计算能力较弱，需要手机等计算能力较强的设备协助计算。用户在获取、展示凭证时，都需要在线下进行。发证机构和服务提供商需要①验证用户与智能卡的共同证明，以及②比对用户本人与智能卡上的照片，在二者都通过的情况下证明用户身份。

然而，匿名性也会导致一些滥用或者恶意的行为，例如，如果有恶意用户非法窃取了合法用户的凭证和相应秘密，便可以对用户的凭证进行非法使用；或者，即使是合法用户，也可能在使用凭证的过程中违反相应协议，比如继续使用过期的凭证。由于用户使用凭证是匿名的，监管部门无法找到相应的用户。因此，应该平衡匿名和追责，即需要监管部门能追踪到违规匿名用户的真实身份，并对其进行撤销。在此基础上，当用户向服务提供商申请服务时，不仅要给出服务提供商需要的属性证明，还需要证明自身是经过监管部门认证的合法者。目前，主要通过用户信息加密[12]、追踪密钥配对[13]等方法进行匿名用户的追踪，通过白名单[14]、黑名单[15]和累加器技术[16]完成匿名凭证系统的撤销功能。

但是，基于智能卡的匿名凭证的方案未考虑追踪与撤销功能，无法解决追踪具有不当或者违法行为的匿名用户、并对其进行撤销的问题，存在一定的安全隐患。

因此，针对上述问题，本文构造了基于智能卡的可追踪撤销匿名凭证系统，主要贡献如下：针对基于智能卡的匿名凭证，实现追踪、撤销功能并完善注册功能，利用BBS+签名、伪随机函数、ElGamal加密、累加器等技术构造方案。发证机构与服务提供商仅支持已注册且未被撤销的合法用户，并需要用户在线下进行交互。在保证发证和验证的效率下做到毫秒级的追踪与撤销，并通过安全性、功能、计算开销分析和性能评估证明本方案是安全且高效的。

本文在第2节中简要介绍一些相关工作；第3节介绍涉及的预备知识；第4节给出方案的基本概念；第5节对方案进行详细介绍；第6节对方案进行实现与比较；最后第7节进行总结。

## 2 相关工作

### 2.1 多设备的匿名凭证

在基本的匿名凭证中，用户的数据通常存储在一个设备，如电脑中，然后使用设备与发证机构和验证者进行交互完成发证和验证的步骤。而在多个设备的场景中，除了上述的便携设备外，通常还包含了一张智能卡。这种智能卡与基于属性的匿名凭证结合的方案需要智能卡和设备的共同使用，而不是在智能卡或者设备上独立运行整个协议，以便智能卡和设备可以联合向发证机构和验证者提供身份证明。

在移动设备领域，如手机，设计匿名凭证方案需要考虑更多的问题，如受限设备获取凭证的问题以及凭证的防共享问题。基于此，Hanzlik和Slamanig[17]采用智能卡（SIM卡）作为核心设备来存储秘密数据，并与辅助设备（如手机）协作完成凭证的获取和展示，提出核心/辅助设备匿名凭证（Core/Helper Anonymous Credentials，CHAC）。该方案的优势在于，它使得核心设备的计算负担不再随凭证上属性数量的增加而增加，解决了多设备场景中的计算效率问题。然而，该方案使用的具有灵活公钥的签名、等价类签名、可聚合的基于属性的等价类签名等原语较为复杂。

在常见的匿名凭证系统中，验证者仅验证用户提供的属性是否满足对应的访问策略。如果用户凭证意外丢失或遭到窃取，当拾取人或者偷窃者得到用户的信息及属性情况，便可非法使用该凭证。即，验证者无法确认凭证使用者和凭证拥有者是否是同一个人。基于此场景，Hesse和Singh考虑用户手机和一张嵌有用户头像照片的智能卡，使用BBS+签名构造匿名凭证方案。用户需要通过线下去找发证机构和验证者进行凭证的获取和展示。该方案提出了BBS+的联合知识证明，令手机和智能卡能够共同向发证机构和验证者提供身份证明。同时智能卡不仅和手机通信，还会与发证机构和验证者交互，取消了智能卡与手机的绑定。并通过智能卡上的用户照片确保凭证拥有人和凭证使用人一致性。

### 2.2 用户追踪与凭证撤销

#### 2.2.1 用户追踪

在匿名凭证系统中，为了实现可追踪性，通常会有一个追踪机构能够使用追踪密钥将凭证与其所有者关联，从而达到追踪用户的目的。主要有用户信息加密、追踪密钥配对等方法。

Blömer和Bobolz[12]让追踪机构生成自己的公私钥对，在凭证展示阶段，用户使用追踪机构的公钥加密个人信息生成假名，追踪机构使用私钥对假名进行解密获取真实信息从而找到用户。Li等人[18]的方案也是使用类似的方法。

Hébant和Pointcheval[13]的方案中，用户需要向追踪机构提供追踪密钥。在凭证展示阶段，用户随机化自己的公钥和凭证，追踪机构可以使用对应追踪密钥通过双线性映射的配对算法完成用户追踪。

2.2.2　凭证撤销

凭证撤销机制是确保系统在面对不再有效的凭证时，能够及时更新状态的一种方法。通常，方案中包含一个撤销机构对凭证进行撤销，撤销机制是通过白名单、黑名单、累加器等技术实现的。

白名单是指有效的用户列表，如果提供凭证的用户不在白名单中则视为无效的用户；反之，黑名单是指无效的用户列表，如果提供凭证的用户不在黑名单中才是合法有效的用户。

累加器用于累加一组元素，并给出每个元素在累加器中的相关证明。通用累加器可以证明某个元素不在累加器中，动态累加器则能够动态地添加或移除元素。匿名凭证系统通常采用动态累加器来处理凭证撤销问题。Nguyen[16]提出了一个基于双线性映射的动态累加器，之后的累加器方案大多基于此进行改进，如Au等人[19]和Vitto等人[20]添加了累加器的通用性，构造出动态且通用的累加器。

### 2.3　匿名身份认证

作为隐私保护的关键技术，匿名身份认证使用户在访问在线服务时，既能证明自己拥有相应权限或符合特定要求，又能确保其真实身份得到完全隐藏。其广泛应用于匿名投票、医疗数据共享和隐私保护访问控制等各类隐私敏感场景。本文提及的匿名凭证就是其中一种相关工具。除此之外，还有属性基签名（Attribute-based Signatures，ABS）、环签名（Ring Signatures）等相关技术。

ABS是一种允许签名者基于其属性生成签名的密码学方案[21-22]，签名仅揭示“签名者满足某些属性”而不暴露具体身份，因此，用户可以基于其属性生成签名，验证者仅能确认用户满足某些属性条件而无法获知其真实身份。其广泛应用于匿名投票、隐私敏感数据访问等需要细粒度隐私保护的场景。近年来，ABS与格结合，构造基于格的高效ABS[23-24]，用于抵抗量子计算攻击。同时，还有可追溯与可审计的ABS[25-27]，用于追踪恶意用户并进行惩罚。

环签名是一种匿名签名技术，允许签名者从一组可能的参与者（称为“环”）中生成签名而不暴露具体身份[28]，因此，用户可以在不暴露真实身份的情况下向验证者证明自己属于某个合法群体。其广泛应用于隐私加密货币、敏感数据泄露认证等场景。近年来，学者们研究可追踪的环签名约束权力[29]，研究门限环签名以防止密钥中心化风险[30]，研究后量子安全的环签名[31-32]等。

## 3　预备知识

### 3.1　双线性群

给定阶为$p$的乘法循环群$\mathbb{G}_1$，$\mathbb{G}_2$和$\mathbb{G}_T$，其中$p$为素数，$g_1$和$g_2$分别为$\mathbb{G}_1$和$\mathbb{G}_2$的生成元。一个高效的可计算的双线性映射$e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$满足以下性质[33]：

（1）双线性：对于$\forall g_1\in\mathbb{G}_1,\forall g_2\in\mathbb{G}_2$，

$[\forall a,b]\in\mathbb{Z}_p$有$e\left(g_1^a,g_2^b\right)=e(g_1,g_2)^{ab}$。

（2）非退化性：对于$\forall g_1\in\mathbb{G}_1,\forall g_2\in\mathbb{G}_2$有$e(g_1,g_2)\neq 1_{\mathbb{G}_T}$。

（3）可计算性：对于$\forall g_1\in\mathbb{G}_1,\forall g_2\in\mathbb{G}_2$，存在计算$e(g_1,g_2)$的有效算法。

同时，Galbraith等人[34]定义了三类双线性映射：

第一类：$\mathbb{G}_1=\mathbb{G}_2$。

第二类：$\mathbb{G}_1\neq\mathbb{G}_2$，但存在一个可有效计算同态$\phi:\mathbb{G}_2\to\mathbb{G}_1$能将$\mathbb{G}_2$映射到$\mathbb{G}_1$。

第三类：$\mathbb{G}_1\neq\mathbb{G}_2$，并且在计算上无法找到一个从$\mathbb{G}_1$到$\mathbb{G}_2$或者从$\mathbb{G}_2$到$\mathbb{G}_1$的有效同态映射。

在本文中，只考虑第三类双线性映射。

### 3.2　BBS+签名

BBS+签名由Au等人[35]于2006年提出，由以下四个高效的算法构成：

（1）初始化（*Setup*）：输入安全参数$1^\lambda$以及消息向量大小$l$，输出公共参数$pp$。

（2）密钥生成（*KeyGen*）：输入公共参数$pp$，输出公钥$pk$以及私钥$sk$。

（3）签名（*Sign*）：输入公共参数$pp$、消息向量$\vec{M}$以及私钥$sk$，输出BBS+签名$\sigma$。

（4）验证（*Verify*）：输入公共参数$pp$、消息向量$\vec{M}$、BBS+签名$\sigma$以及公钥$pk$，如果BBS+签名有效，则输出1，否则输出0。

### 3.3　ElGamal加密

ElGamal加密由ElGamal于1985年提出[36]，包含以下三个高效的算法：

（1）密钥生成（*KeyGen*）：输入安全参数$1^\lambda$，输出公私钥对$(pk,sk)$。

（2）加密（*Enc*）：输入明文消息$m$以及公钥$pk$，输出密文$C$。

（3）解密（*Dec*）：输入密文$C$以及私钥$sk$，输出明文消息$m$。

### 3.4 伪随机函数

Goldreich等人[37]于1986年提出了伪随机函数（Pseudo-Random Function，PRF）的经典构造。它由以下两个高效的算法组成：

（1）密钥生成（*KGen*）：输入安全参数$1^\lambda$，输出密钥$rk$。

（2）计算随机值（*Eval*）：输入密钥$rk$和种子*string*，输出随机值$\gamma$。

### 3.5 累加器

本文使用Au等人的累加器[19]，它由以下高效的算法组成：

（1）初始化（*Gen*）：输入安全参数$1^\lambda$和最大可累加元素数量$n$，生成双线性映射群$BG=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g_0,\hat{g}_0)$，其中生成元$g_0\in\mathbb{G}_1$，$\hat{g}_0\in\mathbb{G}_2$。选择随机数$\alpha\leftarrow\mathbb{Z}_p^*$作为私钥$sk$，令公钥$pk=\left(BG,g_i=\left(g_1^{\alpha^i}\right)_{i\in[n]},\hat{g}_i=\left(g_2^{\alpha^i}\right)_{i\in[n]}\right)$。

（2）计算累加值（*Eval*）：输入一组元素$X=\{x_1,x_2,\cdots,x_n\}\in\mathbb{Z}_p^*$、私钥$sk$和公钥$pk$，计算$\pi(X)=\prod_{i\in[n]}(x_i+\alpha)=\sum_{i=0}^{n}u_i\cdot\alpha^i$，输出累加器值$\Pi_X=g_0^{\pi(X)}=\prod_{i=0}^{n}g_i^{u_i}$。

（3）更新累加器（*Update*）：输入累加器值$\Pi_X$、元素$y'$、私钥$sk$和公钥$pk$，添加$y'$则输出$\Pi'_X=\Pi_X^{y'+\alpha}$；删除$y'$则计算$\Pi'_X=\Pi_X^{\frac{1}{y'+\alpha}}$。

（4）生成证据（*WitCreate*）：输入累加器值$\Pi_X$、元素$y\in X$、私钥$sk$和公钥$pk$，计算$g(X)=\prod_{i=1,x_i\neq y}^{n}(x_i+\alpha)=\sum_{i=0}^{n-1}u_i\cdot\alpha^i$，输出证据$\omega_y=\prod_{i=0}^{n-1}\hat{g}_i^{u_i}$。

（5）验证证据（*WitVerify*）：输入累加器值$\Pi_X$、证据$\omega_y$、元素$y$和公钥$pk$，如果$e(\Pi_X,\hat{g}_0)=e\left(g_0^y g_0^\alpha,\omega_y\right)$成立则输出1，否则输出0。

（6）更新证据（*WitUpdate*）：输入证据$\omega_y$、元素$y'$、私钥$sk$和公钥$pk$，添加$y'$则输出$\omega'_y=\omega_y^{y'+\alpha}$；删除$y'$则输出$\omega'_y=\omega_y^{\frac{1}{y'+\alpha}}$。

### 3.6 零知识证明

零知识证明（Zero-Knowledge Proof，ZKP）由Goldwasser等人提出[38]，并由Feige等人[39]正式化。零知识证明让证明者能够说服验证者相信声明是真的，而不会透露其他额外信息。它满足[40]：

（1）完备性：如果证明者的声明是真的，那么一定可以被验证者接受。

（2）合理性：如果证明者的声明是假的，任何一个作弊的证明者都不可能使诚实的验证者通过验证。

（3）零知识性：协议结束后，验证者只知道证明者的声明是真的；除此之外，验证者无法获取任何有用的知识。

本文使用Camenisch和Stadler[41]引入的符号进行简易说明并进行离散对数之间的知识证明：$PoK\{(w):(x,w)\in R\}$，其中$x$是声明（公开值），$w$表示证据（私有值），使得$(x,w)$满足关系$R$。

## 4 方案基本概念

在本节中，我们将介绍方案模型、方案概述、算法组成和安全模型。

### 4.1 方案模型

我们的匿名凭证的系统模型包含以下4个实体：

（1）发卡机构：实现用户注册、用户追踪和撤销功能。首先，用户注册时需要去线下发卡机构，发卡机构会为用户颁发嵌有其头像图片的智能卡；然后，当用户违反协议时，发卡机构能找到该匿名用户的身份；最后，发卡机构能撤销用户。

（2）发证机构：实现凭证颁发功能。用户获取凭证需要携带智能卡去线下发证机构，发证机构接收请求后为用户颁发凭证。

（3）用户：用户包含手机和智能卡两个部分，二者共同组成用户。

①智能卡：存有用户无法得知的秘密。发证机构和服务提供商需要检测秘密。同时，智能卡嵌有用户头像图片，确保智能卡参与了凭证方案。

②手机：作为一种计算能力较强的便携式设备，主要帮助用户进行计算和存储凭证。

（4）服务提供商：作为验证者，为用户提供对应的服务。在验证阶段，用户需要携带智能卡去线下与服务提供商进行交互。服务提供商检测用户提供的属性是否通过其设置的访问策略。本系统的访问

策略是指用户出示的属性是否满足对应许可以及是否拥有对应的凭证。

### 4.2　方案概述

下面简要介绍本文方案的流程，如图1所示。

（1）系统初始化：系统生成对应双线性映射群及其余公共参数。

（2）密钥生成：发证机构生成密钥对。发卡机构生成密钥对。

（3）用户注册：用户在线下找发卡机构，发卡机构为用户颁发嵌有其头像图片的智能卡并进行注册。智能卡含有秘密的唯一身份标识符*uid*。发卡机构为用户生成唯一身份标识符*id*并保存。

（4）凭证颁发：用户携带智能卡去线下找发证机构。智能卡生成*uid*的承诺和相关证明。用户可以选择隐藏部分属性，并使用手机生成隐藏属性的承诺和相关证明。发证机构查看智能卡上的头像图片与用户是否一致，并检验身份和两个证明的正确性。验证通过后，发证机构生成凭证*cred*。用户将凭证存放到手机中。

（5）凭证展示及验证：用户携带智能卡去线下找服务提供商。智能卡生成*uid*的承诺和相关证明。用户根据服务提供商设置的访问策略隐藏无关属性，使用手机生成隐藏属性的承诺和相关证明，并对*id*进行加密生成密文$C_{id}$和相关证明，同时生成身份的相关证明。服务提供商查看智能卡上的头像图片与用户是否一致，并检验所有证明和凭证的正确有效性。验证通过后，服务提供商向用户提供服务。

（6）用户追踪：若用户违反协议，发卡机构可以解密*id*密文$C_{id}$得到原始用户*id*。

（7）撤销：若发卡机构想要撤销用户，将*id*删除。

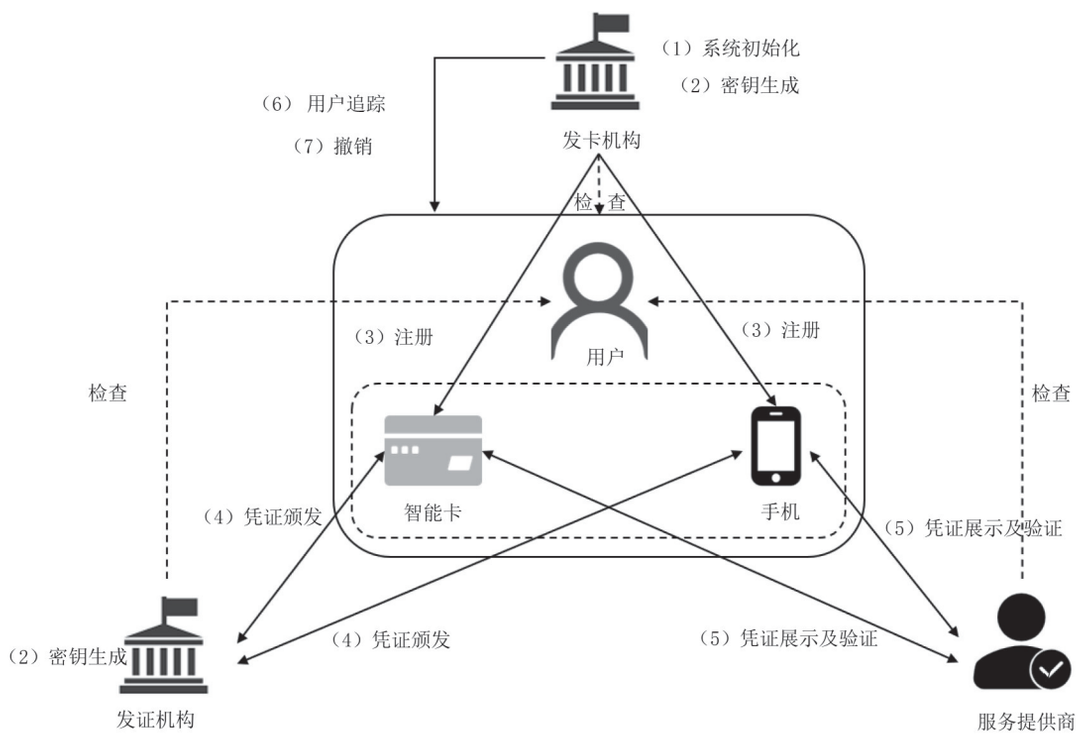


图1　方案流程

### 4.3　算法组成

我们的系统包含以下算法，除了*Setup*外的所有算法默认输入公共参数*pp*：

• $Setup(1^{\lambda}, l)\rightarrow pp$：该算法输入安全参数$1^{\lambda}$和属性数量$l$，输出公共参数*pp*。

• $IKGen(1^{\lambda})\rightarrow(isk, ipk)$：该算法输入安全参数$1^{\lambda}$，输出发证机构的私钥*isk*和公钥*ipk*。

• $CIKGen(1^{\lambda}, t)\rightarrow(rpk, rsk, epk, esk)$：该算法输入安全参数$1^{\lambda}$和累加器可以累加的最大元素数量$t$，输出累加器公钥*rpk*、累加器私钥*rsk*、加密公钥*epk*和加密私钥*esk*。

• $Register(1^{\lambda}, acc_{id}, ID)\rightarrow(K, uid, Q, id, acc'_{id}, \omega_{id}, ID')$：该算法输入安全参数$1^{\lambda}$、当前累加器值$acc_{id}$和当前累加的身份集合*ID*，输出伪随机函数密钥*K*、智能卡*uid*、*uid*相关*Q*、用户身份*id*、更新后的累加器值$acc'_{id}$、对应证据$\omega_{id}$和更新后的累加身份集

合$ID'$。

• $CObtain(K,uid)\leftrightarrow POBtain(K,Q,Attr)\leftrightarrow Issue(Attr_{D_o},id,\omega_{id},rpk,acc_{id},isk)\rightarrow cred$：这是智能卡、手机和发证机构之间交互协议。$CObtain$输入伪随机函数密钥$K$和智能卡$uid$。$POBtain$输入伪随机函数密钥$K$、$uid$相关$Q$和属性集合$Attr$。$Issue$输入揭露的属性集合$Attr_{D_o}$、用户身份$id$、对应证据$\omega_{id}$、发卡机构的累加器公钥$rpk$、当前累加器值$acc_{id}$和发证机构私钥$isk$。协议输出凭证$cred$。

• $CShow(K,uid)\leftrightarrow PShow(K,Q,Attr,id,\omega_{id},rpk,epk)\leftrightarrow Verify(Attr_{D_s},C_{id},(A',\bar{A},d),ipk,rpk,epk,acc_{id})\rightarrow 0/1$：这是智能卡、手机和服务提供商之间的交互协议。$CShow$输入伪随机函数密钥$K$和智能卡$uid$。$PShow$输入伪随机函数密钥$K$、$uid$相关$Q$、属性集合$Attr$、用户身份$id$、对应证据$\omega_{id}$、发卡机构累加器公钥$rpk$和加密公钥$epk$。$Verify$输入揭露的属性集合$Attr_{D_s}$、$id$密文$C_{id}$、随机化凭证$(A',\bar{A},d)$、发证机构公钥$ipk$、发卡机构的累加器公钥$rpk$、加密公钥$epk$和当前累加器值$acc_{id}$。如果验证通过，输出1，否则输出0。

• $Trace(C_{id},epk,esk)\rightarrow id$：该算法输入追踪用户身份密文$C_{id}$、发卡机构加密公钥$epk$和加密私钥$esk$，输出追踪用户身份$id$。

• $Revoke(rpk,rsk,id,acc_{id},ID)\rightarrow(acc'_{id},ID')$：该算法输入发卡机构的累加器公钥$rpk$、累加器私钥$rsk$、待撤销的用户身份$id$、当前累加器值$acc_{id}$和当前累加的身份集合$ID$，输出更新后的累加器值$acc'_{id}$和更新后的累加身份集合$ID'$。

### 4.4 安全模型

我们的安全模型实现了匿名性和不可伪造性。其中，匿名性要求敌手获得同用户使用相同凭证生成的两个凭证证明时，无法有效区分它们，并且敌手也不能将同一凭证的多次使用展示链接起来。不可伪造性是指敌手无法伪造一个用户没有接收过的凭证，但是该凭证能通过验证。

下面，我们将给出一些集合定义。集合$HU$记录诚实用户，集合$CU$记录腐化的用户，集合$UID$记录智能卡$uid$，集合$QID$记录$uid$相关$Q$，集合$PID$记录用户$id$，集合$W$记录$id$对应证据，集合$CRED$记录颁发的凭证$cred$，集合$ATTR$记录对应的属性集合$Attr$。敌手$\mathcal{A}$可以访问下列预言机。

• $\mathcal{O}HU(i)$：输入身份标识符$i$，若$i\in HU\cup CU$，则输出$\perp$。否则，将诚实用户$i$添加到$HU$。

• $\mathcal{O}CU(i)$：输入身份标识符$i$，若$i\in HU$，则将$i$从$HU$中移除并添加到$CU$。否则，将腐化用户$i$添加到$CU$。

• $ApplyReg(i)$：输入身份标识符$i$，若$i\notin HU\cup CU$，则输出$\perp$。否则，调用算法$Register$为用户$i$进行注册，设置$PID[i]=id_i$，$W[i]=\omega id_i$，$UID[i]=uid_i$，$Q[i]=Q_i$。

• $\mathcal{O}ObIss(i,Attr_i)$：为诚实用户$i$创建凭证，即如果$i\notin HU$将输出$\perp$。否则，运行$(CObtain\leftrightarrow POBtain\leftrightarrow Issue)$交互协议生成凭证$cred_i$并更新$\omega id_i$。设置$W[i]=\omega id_i$，$ATTR[i]=Attr_i$，$CRED[i]=cred_i$。

• $\mathcal{O}Obtain(i,Attr_i)$：允许敌手$\mathcal{A}$模拟发证机构为诚实用户颁发凭证。输入用户索引$i$和属性集合$Attr_i$，如果$i\notin HU$，则输出$\perp$。否则，与敌手$\mathcal{A}$运行$(CObtain\leftrightarrow POBtain\leftrightarrow\mathcal{A}(\cdot))$交互协议生成凭证$cred_i$并更新$\omega id_i$。设置$W[i]=\omega id_i$，$ATTR[i]=Attr_i$，$CRED[i]=cred_i$。

• $\mathcal{O}Issue(i,Attr_i)$：允许敌手$\mathcal{A}$模拟用户$i$获取凭证，即如果$i\notin CU$则返回$\perp$。反之，运行$(Issue\leftrightarrow\mathcal{A}(\cdot))$交互协议生成凭证$cred_i$，设置$ATTR[i]=Attr_i$，$CRED[i]=cred_i$。

• $\mathcal{O}Show(i,Attr_i)$：输入用户索引$i$和属性集合$Attr_i$，如果$i\notin HU$或者$Attr_i\not\subseteq Attr[i]$，将输出$\perp$。否则，允许敌手模拟服务提供商对诚实用户$i$的凭证进行验证，运行$(CShow\leftrightarrow PShow\leftrightarrow\mathcal{A}(\cdot))$交互协议并返回相应凭证展示和零知识证明。

• $\mathcal{O}Revoke(i,id)$：输入用户索引$i$和身份$id$，若$i\notin HU\cup CU$或$id\notin PID$则输出$\perp$。否则，调用算法$Revoke$撤销$id$并删除$PID[i]$条目、$W[i]$条目、$UID[i]$条目和$Q[i]$条目。

• $\mathcal{O}Trace(C_{id})$：输入$id$密文$C_{id}$，调用算法$Trace$获取原始$id$。如果$id\notin PID$，则输出$\perp$。反之，输出原始$id$。

基于上述预言机和集合，具体的安全性定义和安全性游戏如下。

**定义1.(匿名性)** 对于一个基于智能卡的可追踪撤销匿名凭证方案Π，其匿名性通过以下敌手-挑战者游戏来定义。

如果对于任意概率多项式时间(Probabilistic Polynomial Time，PPT)敌手$\mathcal{A}$，他能够访问预言机$\mathcal{O}=(\mathcal{O}HU$、$\mathcal{O}CU$、$\mathcal{O}ApplyReg$、$\mathcal{O}Obtain$、$\mathcal{O}Show$、

$\mathcal{O}Revoke$、$\mathcal{O}Trace$)。其在匿名性游戏$Exp_{\Pi,\mathcal{A}}^{ano}(1^\lambda)$中的优势为$Adv_{\Pi,\mathcal{A}}^{ano}(1^\lambda)=\left|Pr\left[Exp_{\Pi,\mathcal{A}}^{ano-1}(1^\lambda)=1\right]-Pr\left[Exp_{\Pi,\mathcal{A}}^{ano-0}(1^\lambda)=1\right]\right|$。若对于所有$\lambda,l,t>0$,优势均可忽略,则称方案Π满足匿名性。匿名性实验$Exp_{\Pi,\mathcal{A}}^{ano-b}(1^\lambda)$的定义如下。

$$b\leftarrow\{0,1\},$$

$$(isk,ipk)\leftarrow IKGen(1^\lambda),$$

$$(rpk,rsk,epk,esk)\leftarrow CIKGen(1^\lambda,t),$$

$$(i_0,i_1,Attr^*,K^*)\leftarrow\mathcal{A}^{\mathcal{O}}(pp,isk,ipk,rpk,epk),$$

若$i_0,i_1\notin HU$或者$Attr^*\not\subseteq ATTR[i_0]\cap ATTR[i_1]$。则输出0;

$$b^*\leftarrow CShow(K^*,UID[i_b])\leftrightarrow PShow$$

$$(K^*,Q[i_b],Attr^*,PID[i_b],W[i_b],$$

$$rpk,epk)\leftrightarrow\mathcal{A}^{\mathcal{O}}(\cdot),\text{此时}\mathcal{O}\text{不包含}\mathcal{O}Trace$$

返回$b^*=b$。

**定义2.(不可伪造性)** 对于一个基于智能卡的可追踪撤销匿名凭证方案Π,其不可伪造性通过以下敌手-挑战者游戏来定义。

如果对于任意PPT敌手$\mathcal{A}$,他能够访问预言机$\mathcal{O}=(\mathcal{O}HU$、$\mathcal{O}CU$、$\mathcal{O}ApplyReg$、$\mathcal{O}ObIss$、$\mathcal{O}Issue$、$\mathcal{O}Show$、$\mathcal{O}Revoke$、$\mathcal{O}Trace)$。其在不可伪造性游戏$Exp_{\Pi,\mathcal{A}}^{forge}(1^\lambda)$中的优势为$Adv_{\Pi,\mathcal{A}}^{forge}(1^\lambda)=Pr\left[Exp_{\Pi,\mathcal{A}}^{forge}(1^\lambda)=1\right]$。若对于所有$\lambda,l,t>0$,优势均可忽略,则称方案Π满足不可伪造性。不可伪造性实验$Exp_{\Pi,\mathcal{A}}^{forge}(1^\lambda)$定义如下。

$$(isk,ipk)\leftarrow IKGen(1^\lambda)$$

$$(rpk,rsk,epk,esk)\leftarrow CIKGen(1^\lambda,t)$$

$$(Attr^*,C_{id}^*,A'^*,\bar{A}^*,d^*)\leftarrow\mathcal{A}^{\mathcal{O}}(ipk,rpk,epk)$$

如果$(1)\wedge((2)\vee(3))$成立,则返回1,否则返回0:

(1) $\mathcal{A}(\cdot)\leftrightarrow\mathcal{A}(\cdot)\leftrightarrow Verify\left(Attr^*,C_{id}^*,(A'^*,\bar{A}^*,d^*),\right.$

$\left.ipk,rpk,epk,acc_{id}\right)=1$;

(2) $\forall i\in CU,Attr^*\not\subseteq ATTR[i]$;

(3) $\forall i\in CU$, $\mathcal{O}Revoke(i,id)$被问询,其中$id=Trace(C_{id}^*,epk,esk)$

## 5　方案详细介绍

在本节中,我们将给出基于智能卡的可追踪撤销匿名凭证方案的详细介绍。我们将对方案进行高度概括:最初,发卡机构和发证机构会生成各自的密钥对。也就是说,发卡机构生成累加器密钥对和ElGamal的密钥对,发证机构生成BBS+的密钥对。

在获取凭证之前,用户需要去线下找发卡机构,发卡机构通过*Register*算法为用户注册,生成一张嵌有该用户头像图片的智能卡。智能卡含有秘密的唯一身份标识符*uid*。发卡机构为用户生成唯一身份标识符*id*并添加到累加器中,同时为用户返回相应的证据$\omega_{id}$和*uid*相关的*Q*。最后,发卡机构将$id-g_1^{id}$存储在记录中。

在*Issue*协议的凭证颁发过程中,用户需要携带智能卡去线下找发证机构。智能卡生成*uid*的承诺和相关零知识证明。用户可以选择向发证机构隐藏部分属性,使用手机生成隐藏属性的承诺和相关证明。用户将两个证明、身份*id*和证据$\omega_{id}$发送给发证机构。发证机构查看智能卡上的头像图片与用户是否一致,并检验两个证明以及$\omega_{id}$。如果检验均通过,发证机构会使用BBS+签署*uid*的承诺、隐藏属性的承诺、揭露的属性集合$Attr_{D_0}$以及*id*。最后,用户获得一个签名作为凭证。

用户收到凭证后,可以携带智能卡去线下找服务提供商,通过*CShow*、*PShow*和*Verify*协议与服务提供商进行身份验证。用户使用ElGamal加密*id*,并证明其持有有效凭证的所有权和未被撤销的*id*,且*id*被正确加密。同时,服务提供商查看智能卡上的头像图片与用户是否一致。

如果用户行为不当,发卡机构可以通过*Trace*算法揭示用户身份。发卡机构拥有ElGamal私钥,可以解密$C_{id}$获取$g_1^{id}$,从而检索对应的$id-g_1^{id}$。

如果用户因行为不当而需要被撤销,发卡机构可以通过*Revoke*算法从累加器中删除*id*。

### 5.1　方案构造

• $Setup(1^\lambda,l)\rightarrow pp$:输入安全参数$1^\lambda$和属性数量*l*,生成双线性映射群$BG=(p,\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_T,e,g_1,g_2)$,其中生成元$g_1\in\mathbb{G}_1,g_2\in\mathbb{G}_2$。从$\mathbb{G}_1$上随机选取$(l+3)$个元素$h_0,\cdots,h_{l+2}\leftarrow\mathbb{G}_1$,记$L=\{1,\cdots,l\}$。选取一个哈希函数$Hash:\{0,1\}^*\rightarrow\mathbb{Z}_p^*$。输出公共参数$pp=(BG,h_0,\cdots,h_l,L,Hash)$。

• $IKGen(1^\lambda)\rightarrow(isk,ipk)$:发证机构选取一个随机数$x\leftarrow\mathbb{Z}_p$,记私钥$isk=x$,计算公钥$ipk=w=g_2^x$。

• $CIKGen(1^\lambda,t)\rightarrow(rpk,rsk,epk,esk)$:输入安全参数$1^\lambda$和累加器可以累加的最大元素数量*t*,发卡机构

选取一个随机数$\alpha\leftarrow\mathbb{Z}_p^*$,记累加私钥$rsk=\alpha$,计算累加公钥$rpk=\left\{rpk_i,\ \widetilde{rpk}_i\right\}_{i\in[t]}=\left\{\left(g_1^{\alpha}\right)^i,\left(g_2^{\alpha}\right)^i\right\}_{i\in[t]}$。选取另一随机数$v\leftarrow\mathbb{Z}_p^*$,令加密私钥$esk=v$,计算加密公钥$epk=g_1^v$。

• $Register(1^{\lambda},acc_{id},ID)\rightarrow(K,uid,Q,id,acc'_{id},\omega_{id},ID')$:

(1) 发卡机构生成智能卡时随机选取智能卡$uid\leftarrow\mathbb{Z}_p$,$uid$仅由智能卡一直持有,不会离开智能卡。计算$Q=h_1^{uid}$。

(2) 发卡机构选取伪随机函数$PRF$的密钥$K$,智能卡记录该密钥$K$。

(3) 发卡机构为用户选取唯一身份$id\leftarrow\mathbb{Z}_p^*$,添加到累加器中$ID'=ID\cup id$,更新累加器值$acc'_{id}=acc_{id}^{(id+\alpha)}$。计算$id$对应证据$\omega_{id}=(g_2^{\prod_{i=1}^{k}(id_i+\alpha)})^{\frac{1}{id+\alpha}}$,其中$k=|ID'|$。同时,在存储库$DB$中存储条目$id-g_1^{id}$。

发卡机构完成注册后,将智能卡交给用户,并将密钥$K$、$uid$相关$Q$、用户身份$id$、对应证据$\omega_{id}$发送给用户。用户验证等式$e(acc'_{id},g_2)=e(g_1^{id}\cdot rpk_1,\omega_{id})$是否成立。若等式成立,用户存储上述信息到手机中。

• $CObtain(K,uid)\leftrightarrow PObtain(K,Q,Attr)\leftrightarrow Issue(Attr_{D_O},id,\omega_{id},rpk,\ acc_{id},isk)\rightarrow cred$:用户携带手机和智能卡去线下找发证机构。

(1) 智能卡选取随机种子$n_{CO}\leftarrow\{0,1\}^{\lambda}$,计算$r=PRF.Eval(K,n_{CO})$和承诺$B_O=h_1^{uid}h_0^r$。此外,计算零知识证明$\pi_1=PoK\{(uid,r):h_1^{uid}h_0^r=B_O\}$。将随机种子$n_{CO}$、承诺$B_O$和证明$\pi_1$发送给发证机构。发证机构将$n_{CO}$发送给手机。

(2) 手机计算$r=PRF.Eval(K,n_{CO})$,验证等式$Qh_0^r=B_O$是否成立。

(3) 用户更新证据$\omega_{id}$,选择需要隐藏的属性,其索引集合记为$H_O$。揭露的属性集合记为$Attr_{D_O}$,对应索引集合$I_O=L/H_O$。选取随机数$s'\leftarrow\mathbb{Z}_p$,计算承诺$C=h_0^{s'}\cdot\prod_{i\in H_O}h_{i+1}^{attr_i}$。此外,手机运行零知识证明协议$PoK\left\{\left(s',\{attr_i\}_{i\in H_O}\right):h_0^{s'}\prod_{i\in H_O}h_{i+1}^{attr_i}=C\right\}$计算证明$\pi_2$。将承诺$C$、隐藏属性索引集合$H_O$、揭露的属性集合$Attr_{D_O}$、证明$\pi_2$、用户身份$id$和对应证据$\omega_{id}$发送给发证机构。

(4) 发证机构检验等式$e(acc_{id},g_2)=e(g_1^{id}\cdot rpk_1,\omega_{id})$是否成立并验证$\pi_1$和$\pi_2$。

(5) 验证均通过后,发证机构随机选取$e\leftarrow\mathbb{Z}_p^*\backslash\{x\}$和$s\leftarrow\mathbb{Z}_p$,记$I_O=L/H_O$,计算$A=\left(g_1h_0^sB_OC\cdot h_{l+2}^{id}\prod_{i\in I_O}h_{i+1}^{attr_i}\right)^{1/(e+x)}$。将签名$\sigma_{prep}=(A,e,s)$返回给用户。

(6) 用户接收预签名后,手机构造凭证$cred=(A,e,s_f=s+s'+r)$,验证等式$e(A,wg_2^e)=e\left(g_1h_0^sQh_{l+2}^{id}\prod_{i=1}^{l}h_{i+1}^{attr_i},g_2\right)$是否成立。若等式成立,手机存储凭证。

• $CShow(K,uid)\leftrightarrow PShow(K,Q,Attr,id,\omega_{id},rpk,epk)\leftrightarrow Verify(Attr_{D_S},C_{id},(A',\bar{A},d),ipk,rpk,epk,\ acc_{id})\rightarrow 0/1$:用户携带手机和智能卡去线下找服务提供商。

(1) 手机选取随机种子$n_H\leftarrow\{0,1\}^{\lambda}$发送给服务提供商,服务提供商发送给智能卡。

(2) 智能卡选取随机种子$n_{CS}\leftarrow\{0,1\}^{\lambda}$,计算$r=PRF.Eval(K,n_{CS}\|n_H)$和承诺$B_S=h_0^r\cdot h_1^{uid}$。此外,计算零知识证明$\pi_3=PoK\{(uid,r):h_1^{uid}h_0^r=B_S\}$。将随机种子$n_{CS}$、承诺$B_S$和证明$\pi_3$发送给服务提供商。服务提供商将$n_{CS}$发送给手机。

(3) 手机计算$r=PRF.Eval(K,n_{CS}\|n_H)$,验证等式$Qh_0^r=B_S$是否成立。

(4) 手机随机选取$r_{enc}\leftarrow\mathbb{Z}_p^*$,计算$C_1=g_1^{r_{enc}}$,$C_2=g_1^{id}\cdot epk^{r_{enc}}$。$id$密文$C_{id}=(C_1,C_2)$。

(5) 用户更新证据$\omega_{id}$,选择访问策略需要提供的属性集合$Attr_{D_S}$,其索引集合记为$I_S$。隐藏的属性索引集合$H_S=L/I_S$。选取随机数$r_1\leftarrow\mathbb{Z}_p^*$,$r_2\leftarrow\mathbb{Z}_p$,$r_3=1/r_1$,计算$s_r=s_f-r_2r_3-r$。计算$b=g_1h_0^{s_f}Qh_{l+2}^{id}\prod_{i=1}^{l}h_{i+1}^{attr_i}$,$A'=A^{r_1}$,$\bar{A}=A'^{-e}b^{r_1}$,$d=b^{r_1}h_0^{-r_2}$。

(6) 手机运行零知识证明协议计算证明$\pi_4=PoK\{(\{attr_i\}_{i\in H_S},id,r_{enc},\omega_{id},e,s_r,r_2,r_3):C_1=g_1^{r_{enc}}\wedge C_2=g_1^{id}\cdot epk^{r_{enc}}\wedge e(acc_{id},g_2)=e(g_1^{id}\cdot rpk_1,\omega_{id})\wedge A'^{-e}h_0^{r_2}=\bar{A}/d\wedge d^{-r_3}h_0^{s_r}h_{l+2}^{id}\prod_{i\in H_S}h_{i+1}^{attr_i}=g_1^{-1}B^{-1}\prod_{i\in I_S}h_{i+1}^{-attr_i}\}$。将隐藏属性索引集合$H_S$、揭露的属性集合$Attr_{D_S}$、证明$\pi_4$、$id$密文$C_{id}$以及随机化凭证$(A',\bar{A},d)$发送给服务提供商。

(7) 服务提供商验证$\pi_3$和$\pi_4$,并检验凭证的合

法性$e(A',w)=e(\bar{A},g_2)$。

以下为$\pi_4$的具体实现，$\tilde{u},\tilde{v},\tilde{h}\leftarrow\mathbb{G}_2$为公共参数。

- 手机随机选取$\beta,\gamma,r_\beta,r_\gamma,r_{\delta_1},r_{\delta_2},r_e,r_{s_r},r_{r_2},r_{r_3},r_{elg},r_{id}\leftarrow\mathbb{Z}_p$和$r_1,\cdots,r_h\leftarrow\mathbb{Z}_p$，其中$h=|H_S|$。计算$R_1=A'^{r_r}$，$R_2=h_0^{r_{r_2}}$，$R_3=d^{r_{r_3}}$，$R_4=h_0^{r_{s_r}}$，$R_5=g_1^{r_{elg}}$，$R_6=g_1^{r_{id}}$，$R_7=epk^{r_{elg}}$，$T_1=\tilde{u}^{\beta}$，$T_2=\tilde{v}^{\gamma}$，$T_3=\omega_{id}\tilde{h}^{\beta+\gamma}$，$\delta_1=id\cdot\beta$，$\delta_2=id\cdot\gamma$，$R_8=\tilde{u}^{r_\beta}$，$R_9=\tilde{v}^{r_\gamma}$，$R_{10}=e(g_1,T_3)^{r_{id}}e(rpk_1,\tilde{h})^{-r_\beta-r_\gamma}\cdot e(g_1,\tilde{h})^{-r_{\delta_1}-r_{\delta_2}}$，$R_{11}=T_1^{r_{id}}\tilde{u}^{-\delta_1}$，$R_{12}=T_2^{r_{id}}\cdot\tilde{v}^{-\delta_2}$，$\{R_{attr_i}=h_{j+1}^{r_i}\}_{i\in[h],j=H_{S_i}}$，$R_{id}=h_{l+2}^{r_{id}}$。将$(T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5,R_6,R_7,R_8,R_9,R_{10},R_{11},R_{12},R_{id},\{R_{attr_i}\}_{i\in[h]})$发送给服务提供商。

- 服务提供商随机选取$c\leftarrow\mathbb{Z}_p$作为挑战发送给手机。

- 手机计算$s_e=r_e+c\cdot e$，$s_{r_2}=r_{r_2}+c\cdot r_2$，$s_{r_3}=r_{r_3}+c\cdot r_3$，$s_{s_r}=r_{s_r}+c\cdot s_r$，$s_{elg}=r_{elg}+c\cdot r_{enc}$，$s_{id}=r_{id}+c\cdot id$，$\{s_i=r_i+c\cdot attr_j\}_{i\in[h],j=H_{S_i}}$，$s_\beta=r_\beta+c\cdot\beta$，$s_\gamma=r_\gamma+c\cdot\gamma$，$s_{\delta_1}=r_{\delta_1}+c\cdot\delta_1$，$s_{\delta_2}=r_{\delta_2}+c\cdot\delta_2$。将$(s_e,s_{r_2},s_{r_3},s_{s_r},s_{elg},s_{id},s_\beta,s_\gamma,s_{\delta_1},s_{\delta_2},\{s_i\}_{i\in[h]})$发送给服务提供商。

- 服务提供商验证等式$A'^{-s_e}h_0^{s_{r_2}}=R_1R_2(\bar{A}/d)^c$，$d^{-s_{r_3}}h_0^{s_{s_r}}h_{l+2}^{s_{id}}\prod_{i\in[h],j=H_{S_i}}h_{j+1}^{s_i}=R_3R_4R_{id}\cdot(g_1^{-1}B^{-1}\prod_{i\in I_S}h_{i+1}^{-attr_i})^c\cdot\prod_{i\in[h]}R_{attr_i}$，$g_1^{s_{elg}}=R_5C_1^c$，$g_1^{s_{id}}\cdot epk^{s_{elg}}=R_6R_7\cdot C_2^c$，$\tilde{u}^{s_\beta}=T_1^c\cdot R_8$，$\tilde{v}^{s_\gamma}=T_2^c\cdot R_9$，$e(g_1,T_3)^{s_{id}}\cdot e(rpk_1,\tilde{h})^{-s_\beta-s_\gamma}\cdot e(g_1,\tilde{h})^{-s_{\delta_1}-s_{\delta_2}}=R_{10}\cdot(e(acc_{id},g_2)/e(rpk_1,T_3))^c$，$T_1^{s_{id}}\tilde{u}^{-s_{\delta_1}}=R_{11}$，$T_2^{s_{id}}\tilde{v}^{-s_{\delta_2}}=R_{12}$。

- $Trace(C_{id},epk,esk)\rightarrow id$：给定凭证展示时的$id$密文$C_{id}$及零知识证明$\pi_5=PoK\{(id,r_{enc}):C_1=g_1^{r_{enc}}\wedge C_2=g_1^{id}\cdot epk^{r_{enc}}\}$。发卡机构先检验$\pi_5$，检验通过后可以使用加密私钥$esk$进行解密获得$g_1^{id}=\frac{C_2}{C_1^{esk}}$。查找存储库$DB$中$g_1^{id}$对应条目的$id$即为待追踪的用户实际身份$id$。

- $Revoke(rpk,rsk,id,acc_{id},ID)\rightarrow(acc'_{id},ID')$：发卡机构从存储库$DB$中删除对应的条目$id-g_1^{id}$。将$id$从累加器中删除$ID'=ID\backslash id$，并更新累加器值$acc'_{id}=acc_{id}^{\frac{1}{id+\alpha}}$。

### 5.2　安全性证明

**定理1.（匿名性）**　基于智能卡的可追踪撤销匿名凭证方案满足匿名性，当且仅当$PoK$证明系统是零知识的。

证明．我们构建一个模拟器$\mathcal{S}$。它与敌手$\mathcal{A}$进行交互以执行基于智能卡的可追踪撤销匿名凭证方案。在此过程中，模拟器$\mathcal{S}$首先执行$Setup$算法生成公开参数$pp$，执行$IKGen$算法生成$(ipk,isk)$，执行$CIKGen$算法生成$(rpk,rsk,epk,esk)$。将$(pp,ipk,isk,rpk,epk)$发送给敌手$\mathcal{A}$。敌手$\mathcal{A}$可对如下预言机发起问询。

- $\mathcal{O}HU(i)$：如果$i$没被问询过，模拟器$\mathcal{S}$创建一个诚实用户$i$。
- $\mathcal{O}CU(i)$：如果$i$没被问询过，创建一个腐化用户$i$。
- $\mathcal{O}ApplyReg(i)$：模拟器$\mathcal{S}$像平常一样调用算法$Register$为用户$i$进行注册。
- $\mathcal{O}Obtain(i,Attr_i)$：如果$i\in HU$，模拟器$\mathcal{S}$与敌手$\mathcal{A}$运行$(CObtain\leftrightarrow PObtain\leftrightarrow issue)$交互协议，敌手$\mathcal{A}$使用$isk$进行交互，返回用户表示为$i$的凭证$CRED[i]$。
- $\mathcal{O}Show(i,Attr_i)$：如果$i\in HU$，像平常一样运行$(CShow\leftrightarrow PShow)$交互协议。
- $\mathcal{O}Revoke(i,id)$：模拟器$\mathcal{S}$使用$rsk$调用算法$Revoke$。
- $\mathcal{O}Trace(C_{id})$：模拟器$\mathcal{S}$使用$esk$调用算法$Trace$。

敌手$\mathcal{A}$根据上述预言机的问询输出用户$i_0,i_1$。若$i_0,i_1\in HU$，且$CRED[i_0],CRED[i_1]\neq\perp$，那么模拟器$\mathcal{S}$选取$i_b$，并将模拟得到的凭证展示$(C_{id},A',\bar{A},d)$作为应答反馈给敌手$\mathcal{A}$。敌手在无法问询$\mathcal{O}Trace$的情况下，输出$b^*$作为凭证展示来源的猜测。在零知识的$PoK$证明系统中，用户的$id$、$\omega_{id}$相关信息在凭证展示时是完全保密的。因此，敌手在无法执行追踪的情况下，其区分不同凭证展示的优势是可忽略的，从而保证了基于智能卡的可追踪撤销匿名凭证方案的匿名性。

证毕。

**定理2.（不可伪造性）**　基于智能卡的可追踪撤销匿名凭证方案满足不可伪造性，当且仅当BBS+签名是不可伪造的，并且累加器是抗碰撞的。

证明．我们构建一个模拟器$\mathcal{S}$。它与敌手$\mathcal{A}$进行交互以执行基于智能卡的可追踪撤销匿名凭证方

案。我们定义两种类型的敌手$\mathcal{A}$。

(1) 假设存在一个攻击基于智能卡的可追踪撤销匿名凭证方案的不可伪造性的第一类敌手$\mathcal{A}$,我们构建一个攻击BBS+签名不可伪造性的模拟器$\mathcal{S}$。实验开始时,模拟器$\mathcal{S}$执行$Setup$算法生成公共参数$pp$,执行$IKGen$算法生成$(ipk, isk)$,执行$CIKGen$算法生成$(rpk, rsk, epk, esk)$。将$(pp, ipk, rpk, epk)$发送给敌手$\mathcal{A}$。模拟器$\mathcal{S}$可以像之前一样回答对预言机的问询,除了$\mathcal{O}ObIss$和$\mathcal{O}Issue$。

• $\mathcal{O}HU(i)$:如果$i$没被问询过,模拟器$\mathcal{S}$创建一个诚实用户$i$。

• $\mathcal{O}CU(i)$:如果$i$没被问询过,创建一个腐化用户$i$。

• $\mathcal{O}ApplyReg(i)$:模拟器$\mathcal{S}$像平常一样调用算法$Register$为用户$i$进行注册。

• $\mathcal{O}ObIss(i, Attr_i)$:对$i \in HU$,模拟器$\mathcal{S}$检索并提交$(i, Attr_i, id_i, uid_i)$给签名预言机$\mathcal{O}Sign$,$\mathcal{O}Sign$返回凭证$cred_i$。

• $\mathcal{O}Issue(i, Attr_i)$:对$i \in CU$,模拟器$\mathcal{S}$从敌手$\mathcal{A}$的零知识证明中提取出$uid_i$。模拟器$\mathcal{S}$提交$(i, Attr_i, id_i, uid_i)$给签名预言机$\mathcal{O}Sign$,$\mathcal{O}Sign$返回凭证$cred_i$。

• $\mathcal{O}Show(i, Attr_i)$:模拟器$\mathcal{S}$像平常一样运行$(CShow \leftrightarrow PShow)$交互协议。

• $\mathcal{O}Revoke(i, id)$:模拟器$\mathcal{S}$使用$rsk$调用算法$Revoke$。

• $\mathcal{O}Trace(C_{id})$:模拟器$\mathcal{S}$使用$esk$调用算法$Trace$。

最后,模拟器$\mathcal{S}$提供策略,敌手$\mathcal{A}$向模拟器$\mathcal{S}$提交挑战内容$(C_{id}, A', \bar{A}, d)$和相关零知识证明,并与其运行$(CShow \leftrightarrow PShow \leftrightarrow Verify)$协议。若对某个腐化用户身份$id$满足$Trace(C_{id}, epk, esk) \rightarrow id_i$,且其所有被问询的属性集合均不满足策略,则表明$(A', \bar{A}, d)$构成了BBS+签名的有效伪造。

(2) 假设存在一个攻击基于智能卡的可追踪撤销匿名凭证方案的不可伪造性的第二类敌手$\mathcal{A}$,我们构建一个攻击累加器抗碰撞性的模拟器$\mathcal{S}$。模拟器$\mathcal{S}$初始化系统并像以前一样回答对预言机的问询。最后,敌手$\mathcal{A}$提交挑战$(C_{id}, A', \bar{A}, d)$及相关零知识证明给模拟器$\mathcal{S}$,其中$id_u$已被撤销。如果敌手$\mathcal{A}$和模拟器$\mathcal{S}$成功运行协议$(CShow \leftrightarrow PShow \leftrightarrow Verify)$,模拟器$\mathcal{S}$便可以从协议的零知识证明中提取出被撤销$id_u$的相关证据$\omega_{id_u}$,这攻破了累加器的抗碰撞性。

证毕。

## 6 实现与性能评价

为了更好地展示所提方案的性能,我们将与文献[17]和文献[11]所提方案,展开功能、理论计算开销和实际执行效率三方面的分析对比。

在功能方面,如表1所示,方案均支持多设备场景,并支持属性的选择性揭露。但是,文献[11]的方案是基础的基于智能卡的匿名凭证方案,没有考虑可追踪性与可撤销性。文献[17]的方案是基础的核心/辅助设备匿名凭证方案,同样没有考虑可追踪性与可撤销性。而本文方案很好地支持了表中的所有功能,更加完备,更加安全可靠。

**表1 不同匿名凭证方案的功能比较**

| 方案 | 多设备 | 选择性揭露 | 可追踪性 | 可撤销性 |
|---|---|---|---|---|
| 文献[17] | √ | √ | × | × |
| 文献[11] | √ | √ | × | × |
| 本文方案 | √ | √ | √ | √ |

在计算开销方面,如表2所示,$exp_{\mathbb{G}_1}$、$exp_{\mathbb{G}_2}$和$exp_{\mathbb{G}_T}$分别表示群$\mathbb{G}_1$、$\mathbb{G}_2$和$\mathbb{G}_T$上的指数运算次数,$pair$表示双线性映射的配对次数。$n$表示用户的属性数量,$d$表示用户揭露的属性数量,$t$表示允许注册的最大用户数量,$k$表示已注册的用户数量,"×"表示没有实现这个功能。需要特别说明的是,本文方案与文献[11]的方案均为基于智能卡的场景,文献[17]基于核心/辅助设备场景。因此,此处主要对本文方案与文献[11]的方案进行比较。

本文方案完善了用户注册的过程,发卡机构通过算法$CIKGen$生成对应的累加器密钥和加密密钥,计算开销与$t$有关。注册时,发卡机构通过算法$Register$生成智能卡和相关参数,并需要为用户生成身份$id$,其中,更新累加器值、生成对应证据$\omega_{id}$和验证$id$产生了额外开销。凭证获取算法$Obtain$包含$CObtain$、$PObtain$以及手机收到凭证后的验证,发证机构对用户$id$也需要进行签名,因此手机在验证凭证时额外增加了一个$\mathbb{G}_1$上的计算开销。同理,发证算法$Issue$也增加了一个$\mathbb{G}_1$上的计算开销,并且发证机构需要将$id$与证据$\omega_{id}$进行双线性映射的配对

计算，以验证用户是否完成注册。凭证展示算法*Show*包含*CShow*与*PShow*，增加了*id*相关签名、加密*id*及*id*与证据$\omega_{id}$的相关零知识证明协议的开销。同理，对于凭证验证算法*Verify*，也增加了类似计算开销。对于追踪算法*Trace*，本方案使用ElGamal的解密算法对*id*密文进行解密，需要验证该密文是否正确生成。在撤销*Revoke*阶段，发卡机构从存储库中删除*id*，并用一个$\mathbb{G}_1$上的指数运算完成累加器值更新。总的来说，本文方案为了实现追踪与撤销功能增加了额外的计算开销，在追踪和撤销阶段的开销较少，主要的额外开销在用户注册、凭证展示和凭证验证阶段，但仍是高效的且实际应用可接受的。由此可见，本文方案与现有方案相比更具可行性。

**表2　不同匿名凭证方案的计算开销比较**

| 算法 | 文献[17] | 文献[11] | 本文方案 |
|---|---|---|---|
| *IKeyGen* | $(2n)exp_{\mathbb{G}_2}$ | $1exp_{\mathbb{G}_2}$ | $1exp_{\mathbb{G}_2}$ |
| *CIKeyGen* | × | × | $(t+1)exp_{\mathbb{G}_1}+(t)exp_{\mathbb{G}_2}$ |
| *Register* | × | $1exp_{\mathbb{G}_1}$ | $3exp_{\mathbb{G}_1}+(k-1)exp_{\mathbb{G}_2}+2pair$ |
| *Obtain* | $2exp_{\mathbb{G}_1}+1exp_{\mathbb{G}_2}+(5n+2)pair$ | $(8+3n-2d)exp_{\mathbb{G}_1}+1exp_{\mathbb{G}_2}+2pair$ | $(9+3n-2d)exp_{\mathbb{G}_1}+1exp_{\mathbb{G}_2}+2pair$ |
| *Issue* | $(4n)exp_{\mathbb{G}_1}+(2n)exp_{\mathbb{G}_2}+5pair$ | $(8+n)exp_{\mathbb{G}_1}$ | $(9+n)exp_{\mathbb{G}_1}+2pair$ |
| *Show* | $10exp_{\mathbb{G}_1}+5exp_{\mathbb{G}_2}$ | $(15+2n-d)exp_{\mathbb{G}_1}$ | $(23+2n-d)exp_{\mathbb{G}_1}+10exp_{\mathbb{G}_2}+5exp_{\mathbb{G}_T}+3pair$ |
| *Verify* | $12pair$ | $(12+n)exp_{\mathbb{G}_1}+2pair$ | $(18+n)exp_{\mathbb{G}_1}+8exp_{\mathbb{G}_2}+5exp_{\mathbb{G}_T}+7pair$ |
| *Trace* | × | × | $6exp_{\mathbb{G}_1}$ |
| *Revoke* | × | × | $1exp_{\mathbb{G}_1}$ |

我们使用C++语言实现了文献[11]的方案、文献[18]的方案和本文方案并作了实验评估，同时也进行了对比分析。实验使用基于配对的密码库PBC（Pairing-based Cryptographic library）①。仿真平台的操作系统为Ubuntu 20.04，处理器为11th Gen Intel（R）Core（TM）i7-11390H @3.40 GHz 2.92 GHz，内存为8.00 GB RAM。在所有实验中，我们使用PBC库0.5.14版本，利用库中类型F的配对参数生成曲线，域和群的阶的位数为160比特。此处主要关注方案中用户注册、凭证颁发、凭证展示、凭证验证、用户追踪与撤销的时间状况，并给出相应的实验对比分析。

图2展示了用户注册时间与已注册用户数量有关。本文方案中，发卡机构在注册阶段为用户*id*生成对应证据，生成时间随着累加器中元素数量的增加而增加。因此，随着已注册用户数量的增加，累加器中存储的*id*数量相应增长，从而令用户注册时间增加。

图3说明了整个发证阶段的执行时间如何随属性数量的变化而变化，其中每多颁发10个属性，用户就多公开5个属性。整个发证阶段的时间成本随着属性数量的增加而增加。其中，本文方案的发证机构在发证阶段额外对用户*id*也进行了签名，并通过双线性映射的配对算法确认用户是否完成注册，时间成本略有增加。

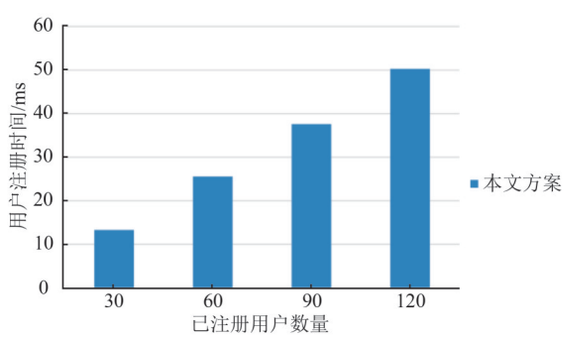


图2　注册阶段执行时间

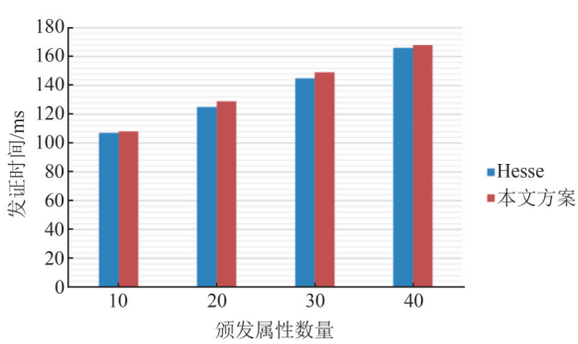


图3　发证阶段执行时间

图4展现了凭证上包含的不同数量的属性对展示阶段执行时间的影响，其中每多包含10个属性，用户就多公开5个属性。随着参数的增加，时间成本略有增加。本文方案与文献[11]的方案相

① https://crypto.stanford.edu/pbc

比，执行时间有所增加。这是因为本文方案需要加密$id$，并额外提供证据$\omega_{id}$及$id$密文$C_{id}$的相关零知识证明。这些增加的时间与属性无关，是可以接受的。

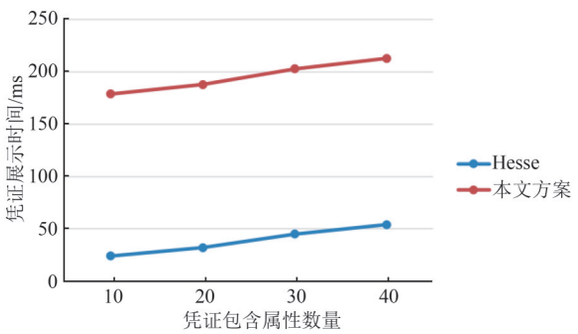


图4 展示阶段执行时间

图5描绘了凭证上包含的不同数量的属性对验证阶段执行时间的影响。与展示阶段类似，每多包含10个属性，用户就多公开5个属性，时间成本随着包含属性数量的增加而略有增加。由于本文方案在展示阶段额外对$id$进行加密，并额外提供了证据$\omega_{id}$及$id$密文$C_{id}$的相关零知识证明，因此，验证阶段要额外对这些零知识证明进行检验，从而增加了检验时间。这些增加的时间与属性无关，是可以接受的。

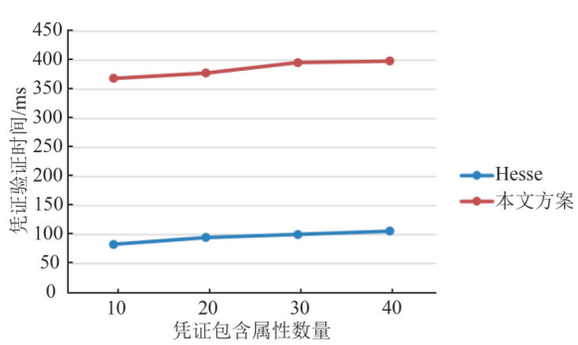


图5 验证阶段执行时间

在图6中，我们展示了不同的用户索引下标的追踪时间成本。追踪时间由用户的索引下标决定，与用户数量无关，随索引下标增加而略有增加。本文方案比文献[18]的方案稍快，均是毫秒级的快速追踪。表3给出了在不同数量的注册用户下撤销一个用户的执行时间，它们的时间接近，随着注册用户数量的增加而略有增加，与文献[18]的方案基本一致。

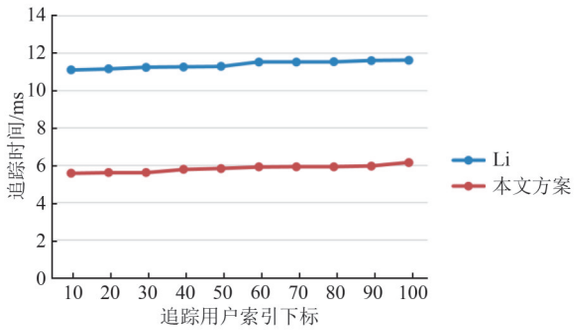


图6 追踪阶段执行时间

**表3 撤销阶段执行时间**

| 注册用户数量 | 撤销一个用户时间(ms) | |
|---|---|---|
| | 文献[18] | 本方案 |
| 30 | 1.09 | 1.10 |
| 60 | 1.10 | 1.11 |
| 90 | 1.11 | 1.11 |
| 120 | 1.13 | 1.12 |

## 7 总 结

本文设计了基于智能卡的可追踪撤销匿名凭证方案，在确保凭证使用者和凭证拥有者一致前提下，解决了用户追踪与撤销问题，扩展了匿名凭证的应用场景。本文提出的方案在保持高效发证和验证的同时，实现了追踪和撤销功能，并完善了注册机制，实现了毫秒级的追踪与撤销响应，使系统更加完备且安全可靠。通过与现有方案的功能、计算开销对比分析以及仿真实验评估对比，在额外花费少量的计算资源，达到用户追踪与撤销的安全需求是完全可行的。

**致 谢** 本课题得到国家自然科学基金(No. 62525206、No. 62472198)、广东省基础与应用基础研究基金(No. 2023B1515040020)等提供相关支持。衷心感谢各位专家在审稿过程中提供的建议和帮助！

## 参 考 文 献

[1] Vullers P, Alpár G. Efficient selective disclosure on smart cards using idemix// Proceedings of the Third IFIP WG 11.6 Working Conference on Policies and Research in Identity Management. London, UK, 2013: 53-67

[2] Blanton M. Online subscriptions with anonymous access// Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. Tokyo, Japan, 2008: 217-227

[3] Milutinovic M, Decroix K, Naessens V, et al. Privacy-

preserving public transport ticketing system// Proceedings of the 29th Annual IFIP WG 11.3 Working Conference on Data and Applications Security and Privacy XXIX. Fairfax, USA, 2015: 135-150

[4] Rannenberg K, Camenisch J, Sabouri A. Attribute-based credentials for trust. Identity in the Information Society, Springer, 2015

[5] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps// Proceedings of the 24th Annual International Cryptology Conference. Santa Barbara, USA, 2004: 56-72

[6] Pointcheval D, Sanders O. Short randomizable signatures// Proceedings of the Cryptographers' Track at the RSA Conference 2016. San Francisco, USA, 2016: 111-126

[7] Boneh D, Boyen X. Short signatures without random oracles and the SDH assumption in bilinear groups. Journal of Cryptology, 2008, 21(2): 149-177

[8] Boneh D, Boyen X, Shacham H. Short group signatures// Proceedings of the 24th Annual International Cryptology Conference. Santa Barbara, USA, 2004: 41-55

[9] Canard S, Lescuyer R. Protecting privacy by sanitizing personal data: a new approach to anonymous credentials// Proceedings of the 8th ACM Symposium on Information, Computer and Communications Security. Hangzhou, China, 2013: 381-392

[10] Fuchsbauer G, Hanser C, Slamanig D. Practical round-optimal blind signatures in the standard model// Proceedings of the 35th Annual Cryptology Conference. Santa Barbara, USA, 2015: 233-253

[11] Hesse J, Singh N, Sorniotti A. How to bind anonymous credentials to humans// Proceedings of the 32nd USENIX Security Symposium. Anaheim, USA, 2023: 3047-3064

[12] Blömer J, Bobolz J. Delegatable attribute-based anonymous credentials from dynamically malleable signatures// Proceedings of the 16th International Conference on Applied Cryptography and Network Security. Leuven, Belgium, 2018: 221-239

[13] Hébant C, Pointcheval D. Traceable constant-size multi-authority credentials. Information and Computation, 2023, 293: 105060

[14] Liu Y, He D, Luo M, et al. ATRC: An anonymous traceable and revocable credential system using blockchain for VANETs. IEEE Transactions on Vehicular Technology, 2023, 73(2): 2482-2494

[15] Brickell E, Li J. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities// Proceedings of the 2007 ACM Workshop on Privacy in the Electronic Society. Alexandria, USA, 2007: 21-30

[16] Nguyen L. Accumulators from bilinear pairings and applications// Proceedings of the Cryptographers' Track at the RSA Conference 2005. San Francisco, USA, 2005: 275-292

[17] Hanzlik L, Slamanig D. With a little help from my friends: Constructing practical anonymous credentials// Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security. Virtual Event, Republic of Korea, 2021: 2004-2023

[18] Li P, Lai J, Yang Y, et al. Attribute-based anonymous credential: Delegation, traceability, and revocation. Computer Networks, 2023, 237: 110086

[19] Au M H, Tsang P P, Susilo W, et al. Dynamic universal accumulators for DDH groups and their application to attribute-based anonymous credential systems// Proceedings of the Cryptographers' Track at the RSA Conference 2009. San Francisco, USA, 2009: 295-308

[20] Vitto G, Biryukov A. Dynamic universal accumulator with batch update over bilinear groups//Proceedings of the Cryptographers' Track at the RSA Conference 2022. Virtual, 2022: 395-426

[21] Chen Y, Li J, Liu C, et al. Efficient attribute based server-aided verification signature. IEEE Transactions on Services Computing, 2021, 15(6): 3224-3232

[22] Li Ji-Guo, Zhu Liu-Fu, Shen Jian, et al. Attribute-Based Sanitizable Signature Scheme with Strong Designated Verifier. Chinese Journal of Computers, 2023, 46(09): 1806-1819 (in Chinese)
(李继国, 朱留富, 沈剑, 等. 具有强指定验证者的属性基可净化签名方案. 计算机学报, 2023, 46(09): 1806-1819)

[23] Luo F, Al-Kuwari S. Attribute-based signatures from lattices: Unbounded attributes and semi-adaptive security. Designs, Codes and Cryptography, 2022, 90(5): 1157-1177

[24] Kong Y, Jiang M, Ge H, et al. An Attribute-Based Signature Scheme with Flexible Access Control on Lattice// Proceedings of the 2nd International Conference on Computer, Vision and Intelligent Technology. Huaibei, China, 2024: 1-6

[25] Li Ji-Guo, Zhu Liu-Fu, Liu Cheng-Dong, et al. Provably Secure Traceable Attribute-Based Sanitizable Signature Scheme in the Standard Model. Journal of Computer Research and Development, 2021, 58(10): 2253-2264 (in Chinese)
(李继国, 朱留富, 刘成东, 等. 标准模型下证明安全的可追踪属性基净化签名方案. 计算机研究与发展, 2021, 58(10): 2253-2264)

[26] Kang Z, Li J, Shen J, et al. TFS-ABS: Traceable and forward-secure attribute-based signature scheme with constant-size. IEEE Transactions on Knowledge and Data Engineering, 2023, 35(9): 9514-9530

[27] Delerablée C, Gouriou L, Pointcheval D. Attribute-Based Signatures with Advanced Delegation, and Tracing// Proceedings of the Cryptographers' Track at the RSA Conference 2024. San Francisco, USA, 2024: 224-248

[28] Rivest R L, Shamir A, Tauman Y. How to leak a secret// Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia, 2001: 552-565

[29] Liang J, Huang Q, Huang J, et al. An identity-based traceable ring signatures based on lattice. Peer-to-Peer Networking and Applications, 2023, 16(2): 1270-1285

[30] Avitabile G, Botta V, Fiore D. Extendable threshold ring signatures with enhanced anonymity//Proceedings of the 26th IACR International Conference on Practice and Theory of

Public-Key Cryptography. Atlanta, USA, 2023: 281-311
[31] Buser M, Liu J K, Steinfeld R, et al. Post-quantum ID-based ring signatures from symmetric-key primitives// Proceedings of the 20th International Conference on Applied Cryptography and Network Security. Rome, Italy, 2022: 892-912
[32] Zhang X, Steinfeld R, Esgin M F, et al. Loquat: a SNARK-friendly post-quantum signature based on the legendre PRF with applications in ring and aggregate signatures// Proceedings of the 44th Annual International Cryptology Conference. Santa Barbara, USA, 2024: 3-38
[33] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps// Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland, 2003: 416-432
[34] Galbraith S D, Paterson K G, Smart N P. Pairings for cryptographers. Discrete Applied Mathematics, 2008, 156(16): 3113-3121
[35] Au M H, Susilo W, Mu Y. Constant-size dynamic k-TAA// Proceedings of the 5th International Conference on Security and Cryptography for Networks. Maiori, Italy, 2006: 111-125
[36] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469-472
[37] Goldreich O, Goldwasser S, Micali S. How to construct random functions. Journal of the ACM (JACM), 1986, 33(4): 792-807
[38] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof-systems// Proceedings of the 17th Annual ACM Symposium on Theory of Computing. Providence, USA, 1985: 291-304
[39] Fiege U, Fiat A, Shamir A. Zero knowledge proofs of identity// Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York, USA, 1987: 210-217
[40] Damgård I. Efficient concurrent zero-knowledge in the auxiliary string model// Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Bruges, Belgium, 2000: 418-430
[41] Camenisch J, Stadler M. Efficient group signature schemes for large groups// Proceedings of the 17th Annual International Cryptology Conference. Santa Barbara, USA, 1997: 410-424

**MO Xiao-Han**, M. S. His research interests include cryptography and information security.

**LAI Jun-Zuo**, Ph. D., professor. His research interests include cryptography and information security.

**WU Chi**, M. S. His research interests include cryptography and information security.

**SUN Meng**, Ph. D. candidate. Her research interests include cryptography and information security.

## Background

This research belongs to the field of privacy-preserving identity authentication, focusing on anonymous credentials.

Anonymous credentials are digital credentials that allow users to prove that they possess certain attributes without revealing their personal identity. The core objective of anonymous credential is to protect the privacy of the user while ensuring the ability of the authentication. Anonymous credentials are usually issued by an issuer that signs the user's attributes with a private key, resulting in an attribute-based anonymous credential. Anonymity means that the user does not reveal his/her identity when presenting the credentials to the service provider, but only proves the validity and legitimacy of the credentials through zero-knowledge proofs. Selective disclosure refers to the fact that the user can provide only the attributes required by the service provider when presenting the credentials, instead of presenting all the attributes on the credentials. A basic anonymous credential scheme involves the issuance, presentation, and verification of credentials.

Currently, anonymous credentials primarily focus on multi-use credentials, which allow multiple uses while satisfying unlinkability. They have a wide range of applications, such as anonymous subscriptions, electronic ticket, and access control for online services. Researchers have constructed anonymous credential schemes using signatures such as CL signatures, PS signatures, BBS signatures, sanitizable signature, and structure-preserving signatures on equivalence classes.

This paper is based on a multi-device setting. Existing multi-device anonymous credential schemes include the core/helper anonymous credential scheme proposed by Hanzilik et al., and the card-based anonymous credential scheme proposed by Hesse et al. Through Hesse's scheme, users can bind themselves to credentials. Even if third parties obtain the credentials, they cannot use them. However, this scheme does not support tracing and revocation functionalities, posing security risks.

Existing anonymous credential schemes supporting tracing

and revocation functionalities are all single-device schemes. None of these anonymous credentials support multi-device setting.

Therefore, in this paper, we designed an anonymous credential to address the aforementioned issues. The scheme employs an encryption scheme to enable user tracing and utilizes an accumulator to facilitate user revocation. It achieves millisecond-level tracing and revocation while ensuring efficient credential issuance, presentation, and verification, delivering enhanced security and reliability.

This work received support from several funding sources: the National Natural Science Foundation of China under Grant 62525206 and Grant 62472198, in part by Guangdong Basic and Applied Basic Research Foundation under Grant 2023B1515040020.