计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202111235
60(6): 1417−1430, 2023

格上可追溯的匿名单点登录方案

汤永利　李　英　赵宗渠　李星宇　王瀚博
（河南理工大学软件学院　河南焦作　454003）
（yltang@hpu.edu.cn）

Traceable Anonymous Single Sign on Scheme on Lattice

Tang Yongli, Li Ying, Zhao Zongqu, Li Xingyu, and Wang Hanbo
（*School of Software*, *Henan Polytechnic University*, *Jiaozuo*, *Henan* 454003）

Abstract　The single sign on (SSO) scheme can avoid the waste of resources and information leakage caused by the redundancy of authentication module, and the anonymous single sign on can realize anonymous authentication and authorization under the condition of protecting personal privacy. However, the existing anonymous single sign on schemes do not consider the accountability of fraud caused by the anonymity of users. For this problem, a traceable anonymous single sign on scheme on lattice is proposed. The proposed scheme uses the identity-based cryptosystem on lattice to alleviate the problem of public key certificate management, and realizes the anonymous authentication of the user through the authorized authentication tag and pseudonym. Then, the strong designated verifier technology is used to realize the directional verification of user service requests. And the trusted organization is introduced to recover the user's identity and pursue responsibility through the public key. The proposed scheme is proved to have unlinkability, unforgeability and traceability under the security model. The security and performance analysis results show that under PARMS II and PARMS III, our scheme can generate the access service tickets for 4 service requests by running for about 75 ms and 108 ms respectively. And it can reach the quantum security strength of 230 b and 292 b.

Key words　single sign on; traceability; anonymous authentication; inhomogeneous small integer solution; identity-based cryptosystem

摘　要　单点登录（single sign on, SSO）方案能够避免认证模块冗余带来的资源浪费、信息泄露问题，而具有匿名性的单点登录能够在保护个人隐私的情况下实现匿名认证与授权，但现有的匿名单点登录方案未考虑因用户匿名而出现的欺诈行为追责问题. 针对此问题，首先提出一个格上可追溯的匿名单点登录方案. 所提方案采用格上基于身份的密码体制缓解公钥证书管理问题，通过授权认证标签和假名实现对用户的匿名认证；然后使用强指定验证者技术实现用户服务请求的定向验证；同时引入受信任机构，通过公钥恢复出用户身份并进行追责；最后在安全模型下证明方案具有不可链接性、不可伪造性与可追溯性. 安全性与性能分析结果表明方案在 PARMS II 和 PARMS III 这 2 组参数下，分别运行大约 75 ms 和 108 ms 便可为用户生成可供 4 次服务请求的访问服务票据，并可达到 230 b 和 292 b 的量子安全强度.

关键词　单点登录；可追溯性；匿名认证；非齐次小整数解；基于身份的密码体制

收稿日期：2021-12-15；**修回日期**：2022-08-17

基金项目：国家自然科学基金项目（61802117）；河南理工大学青年骨干教师资助计划项目（2018XQG-10）；河南省高校科技创新团队支持计划项目（20IRTSTHN013）

This work was supported by the National Natural Science Foundation of China (61802117), the Youth Backbone Teacher Support Program of Henan Polytechnic University (2018XQG-10), and the Support Plan Program of Scientific and Technological Innovation Team in University of Henan Province (20IRTSTHN013).

通信作者：赵宗渠（zhaozong_qu@hpu.edu.cn）

中图法分类号 TP309

身份认证协议使用户能够高效、方便地访问远程资源. 但传统的身份认证协议仅向用户提供来自单一身份验证服务器的访问服务提供商，如果用户试图通过使用这些认证协议来访问多个独立的服务提供商，则需在不同系统中进行注册，保存大量的账号和口令. 这种基于用户名和认证信息的独立身份管理系统使所有参与的服务端和用户端都需要功能类似的认证模块，导致系统资源的浪费，同时增加用户认证信息被泄露的风险.

单点登录(single sign on, SSO)方案是允许用户使用一个主凭证来访问多个在线账户方案的总称，它结合认证与授权，一般应用在多个应用的系统中. 用户只需要登录 1 次，在进行身份认证后就可以访问相互信任的应用系统，解决了独立身份管理系统的弊端.

2004 年，Wu 等人[1]首次提出多应用系统下的单点登录方案. 2006 年，Mangipudi 等人[2]提出匿名单点登录(anonymous single sign on, ASSO)方案，解决了用户访问服务过程中的拒绝服务(DoS)攻击. 2012 年，Chang 等人[3]提出可以解决假冒攻击的 ASSO 方案. 2013 年，Wang 等人[4]指出 Chang 等人[3]的方案不能有效保护用户证书，进而基于 RSA 签名构造了 ASSO 方案. 2017 年，Wen 等人[5]提出了一个基于拉格朗日插值多项式的 ASSO 方案，它的匿名仅提供给用户而不提供给服务器，易受用户和服务器假冒攻击，且用户的服务请求由系统的所有验证者来验证，而不是由指定的验证者来验证，这可能对用户和验证者都造成潜在隐私泄露风险. 同年，Gope 等人[6]针对移动云计算服务，在限制用户访问服务次数的前提下，提出一个满足用户与服务提供商间双向匿名认证的方案，解决了用户单点登录时的隐私泄露问题.

为解决用户访问服务时的限制问题，2018 年，Lee[7]构造的基于切比雪夫混沌映射的高效 ASSO 方案，该方案在多个服务提供商串通时，不能实现用户对服务提供商的匿名. Jegadeesan 等人[8]基于 ECDLP 困难问题提出新的解决方案，通过可信第三方为用户分发一个随机值来生成私钥，实现分布式移动计算环境中用户对服务提供商的匿名认证. 2019 年，Jia 等人[9]针对移动边缘计算提出基于身份的匿名认证方案，利用 k-改进的双线性逆 Diffie-Hellman(k-modified bilinear inverse Diffie–Hellman, k-mBIDH)困难问题，在可信第三方不参与的情况下，通过服务器对用户登录消息的解密，实现用户的匿名单点登录.

现存的 ASSO 方案[8-13]可以实现用户匿名访问服务，但此时用户的完全匿名性，导致用户可以随意进行恶意操作，从事非法活动而不被问责. 对于这种情况，应该有监督机构揭示出用户的身份，必要时对用户追责，追溯出用户所有的服务请求. 2018 年，Han 等人[14]引入指定验证者签名[15-18]技术，提出一个只能由指定服务提供商验证的 ASSO 方案，实现服务不可链接性. 并在此基础上构造出新的 ASSO 方案[19]，该方案在指定的服务提供商不可用时，中央验证者可以授权新的服务商代表原始服务商对用户进行认证，同时也可以揭示用户身份并追溯用户的服务请求，实现问责性. 2021 年，Zhang 等人[20]构造出轻量级的 ASSO 方案，采用 PS 签名[21]构造匿名凭证，利用非交互零知识证明技术对用户信息进行选择性披露，在保护用户隐私的情况下实现用户的匿名单点登录；在解密机构的协助下，对行为不端的用户进行问责. 该方案有效降低通信开销，但匿名凭证与非交互零知识证明的生成，导致其计算效率较低.

文献 [8−14,19−20] 的 ASSO 方案都是基于大整数分解和离散对数等数论难题设计的，随着量子计算领域的研究不断取得突破，解决这些数论难题成为可能[22]. 目前国际后量子密码研究中，格密码体制因其安全性高、运算速度快等特点受到了广泛关注，已知格上的最短向量问题(shortest vector problem, SVP)和最近向量问题(closest vector problem, CVP)等难题在量子计算机下还未存在概率多项式时间高效求解算法[23].

为解决匿名单点登录过程中用户不诚信行为的问题，本文采用格上基于身份的密码体制，提出了一个格上可追溯的匿名单点登录方案. 主要贡献有 4 点：

1)构建格上基于身份的可追溯的 ASSO 方案. 利用格上基于身份的密码体制缓解现有单点登录方案中公钥证书管理问题，采用指定验证者签名技术[24]实现用户服务请求的定向验证. 方案的不可链接性、不可伪造性与可追溯性都可规约至非齐次小整数解(inhomogeneous small integer solution, ISIS)问题上. 在 NIST 后量子密码标准化进程的不断推进下，本方案可以有效抵抗量子攻击[23,25-26].

2)采用授权认证标签和假名技术[27]实现用户匿名性. 为保护用户隐私，利用假名$(\boldsymbol{p}_v, \boldsymbol{q}_v)$进行用户身份认证与服务请求. 由于假名是一次性的，因此所提方案可以有效抵抗假冒攻击与重放攻击. 同时在假

名泄露的情况下，敌手也无法从多个已泄露的假名中揭露出任何有关用户身份的信息，有效解决跨多个验证器验证过程中的用户信息泄露问题.

3）对行为不端用户进行问责. 用户的匿名性可能会导致用户进行恶意的服务请求，必要时可信机构可以根据用户的服务票据T_u，恢复出用户身份$ID_u=\dfrac{c_2-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{c}_1}{\left\lfloor\frac{q}{2}\right\rfloor}$，取消用户的匿名，追溯出用户的服务请求.

4）在达到 112 b, 230 b, 292 b 的量子安全级别下进行方案效率分析. 实验结果表明，与现有的单点登录方案[4,7,19]相比，本方案生成的密钥尺寸更小，在降低通信开销的同时有效提高计算效率，具有更强的安全性.

1 预备知识

设n为安全参数，素数$q\in\mathbb{Z}$为模，大写黑体字母（如$\boldsymbol{A}$）为矩阵，$\boldsymbol{A}^{\mathrm{T}}$为$\boldsymbol{A}$的转置，小写黑体字母（如$\boldsymbol{a}$）为列向量，以及$\|\boldsymbol{a}\|=\sqrt{a_1^2+a_2^2+\cdots+a_n^2}$是向量$\boldsymbol{a}=(a_1,a_2,\cdots,a_n)\in\mathbb{R}^n$的欧几里得范数，$a\xleftarrow{\mathrm{R}}\chi$表示$a$是从集合$\chi$中均匀随机选取的. $poly(n)$为 n 的多项式函数，$\log n$是 n 的对数关系函数.

1.1 格的相关定义

矩阵$\boldsymbol{B}=(\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m)\in\mathbb{Z}^{n\times m}$，$\boldsymbol{b}_1,\boldsymbol{b}_2,\cdots,\boldsymbol{b}_m\in\mathbb{Z}^n$为$m$个线性无关的向量. 由$\boldsymbol{B}$生成的格定义为$\Lambda=\left\{\sum_{i=1}^{m}x_i\boldsymbol{b}_i:x_i\in\mathbb{Z}\right\}$，$n$和$m$是整数，且分别是格$\Lambda$的维数和秩，$\boldsymbol{B}$是$\Lambda$的基.

定义 1. ISIS 问题. 设$\boldsymbol{A}\in\mathbb{Z}_q^{n\times m}$，实数$\beta>0$. $\mathrm{ISIS}_{q,n,m,\beta}$问题的目标是给定任意向量$\boldsymbol{y}\in\mathbb{Z}^n$，找到一个非零向量$\boldsymbol{x}\in\mathbb{Z}^m$，使$\boldsymbol{A}\boldsymbol{x}=\boldsymbol{y}(\bmod q)$和$\|\boldsymbol{x}\|\leqslant\beta$成立. 当$\boldsymbol{y}=(0)^n$时，可转化为$\mathrm{SIS}_{q,n,m,\beta}$（small integer solution）问题，其目标是找到一个非零向量$\boldsymbol{x}\in\mathbb{Z}^m$，使$\boldsymbol{A}\boldsymbol{x}=\boldsymbol{0}(\bmod q)$和$\|\boldsymbol{x}\|\leqslant\beta$成立.

定义 2. 最短独立向量问题（shortest independent vector problem, SIVP）. 设矩阵$\boldsymbol{B}\in\mathbb{Z}^{n\times m}$是格$\Lambda\in\mathbb{Z}^n$的基. 格$\Lambda$的最短独立向量问题是找一个$n$个线性无关的格向量集合$C=\{\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n\}\subset\Lambda$，使得$\|\boldsymbol{c}_i\|=\lambda_i(\Lambda)$. SIVP_γ的目标是获得一个集合$C=\{\boldsymbol{c}_1,\boldsymbol{c}_2,\cdots,\boldsymbol{c}_n\}\subset\Lambda$，使得$\|C\|\leqslant\gamma\cdot\lambda_n(\Lambda)$，其中$\lambda_n(\Lambda)$为$\Lambda$的第$n$个连续最小值.

引理 1. 给定正整数n，多项式界定的$m\approx ploy(n)$，$\beta\approx ploy(n)$，素数$q\geqslant\beta\cdot w\sqrt{(n\log n)}$. 在平均情况下找到$\mathrm{SIS}_{q,n,m,\beta}$和$\mathrm{ISIS}_{q,n,m,\beta}$问题的解，与在任意$n$维格上，在最糟糕的情况下求解$\mathrm{SIVP}_\gamma$问题一样困难，其中$\gamma=\beta\cdot\tilde{O}(\sqrt{n})$[28].

1.2 离散高斯分布

对于任意$\sigma>0$，以$\boldsymbol{c}\in\mathbb{R}^m$为中心、$\sigma$为标准差的格$\Lambda$上离散高斯分布定义为$D_{\Lambda,\sigma,\boldsymbol{c}}(\boldsymbol{x})=\dfrac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\Lambda)}$，其中，$\boldsymbol{x}\in\Lambda$，$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})=\exp\left(-\dfrac{\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{\sigma^2}\right)$，$\rho_{\sigma,\boldsymbol{c}}(\Lambda)=\sum_{\boldsymbol{x}\in\Lambda}\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})$. $\boldsymbol{c}$为零向量时，可以忽略不写.

引理 2. 高斯分布具有 2 个性质. 给定标准差σ和正整数m，则：

1）$Pr[\boldsymbol{x}\leftarrow D_\sigma^m:\|\boldsymbol{x}\|>2\sigma\sqrt{m}]<2^{-m}$；

2）$Pr[\boldsymbol{x}\leftarrow D_\sigma^1:\|\boldsymbol{x}\|>\omega(\sigma\sqrt{\log m})]=2^{-w\log m}$.

2 方案模型

2.1 方案流程

系统初始化时，各参与方必须从被称为“私钥生成器（private key generator, PKG）”的可信第三方获得基于身份的公私钥. 整个方案流程如图 1 所示，用户（user, U）加入系统时，需要把自己的公钥和身份发送给中央验证者（central verifier, CV），以便去匿名化. 用户为获得 1 个票据，给票据发行者（issuer, I）发送自己的服务请求，票据发行者为用户生成相应的票据. 随后用户给指定服务提供商发送相应的认证标签，服务提供商也称票据验证者（verifier, V），当票据验证者认证标签通过后，就可授权用户去访问服务. 当用户出现不诚信行为时，中央验证者可以通过票据对用户进行去匿名化，追溯出用户的整个服务请求. 在具体方案中，用户、中央验证者、票据发行者、票据验证者分别被实例化为 *u*, *cv*, *iss*, *v*.

2.2 形式化定义

可追溯的匿名单点登录方案由 6 个多项式时间算法组成.

1）$Keygen(1^n)$：输入安全参数n，输出系统的公共参数$Param$以及系统主密钥$\boldsymbol{msk}$.

2）$ExtractKey(Param, ID_j, \boldsymbol{msk})$：输入系统的公共参数$Param$，身份$ID_j$以及系统的主密钥$\boldsymbol{msk}$，输出私钥$\boldsymbol{sk}_j$和公钥$\boldsymbol{pk}_j$.

3）$User\text{-}Registration(Input_u(Param, ID_u, \boldsymbol{pk}_u, \boldsymbol{pk}_{cv})\leftrightarrow Input_{cv}(Param, \boldsymbol{sk}_{cv}))$：输入公共参数$Param$，用户身份$ID_u$以及公钥$\boldsymbol{pk}_u$，中央验证者公私钥$(\boldsymbol{pk}_{cv}, \boldsymbol{sk}_{cv})$，最终中央验证者在本地列表里存储$(ID_u, \boldsymbol{pk}_u)$. “$\leftrightarrow$”表示该算法需要在用户和中央验证者的交互下才可以有正确输出.

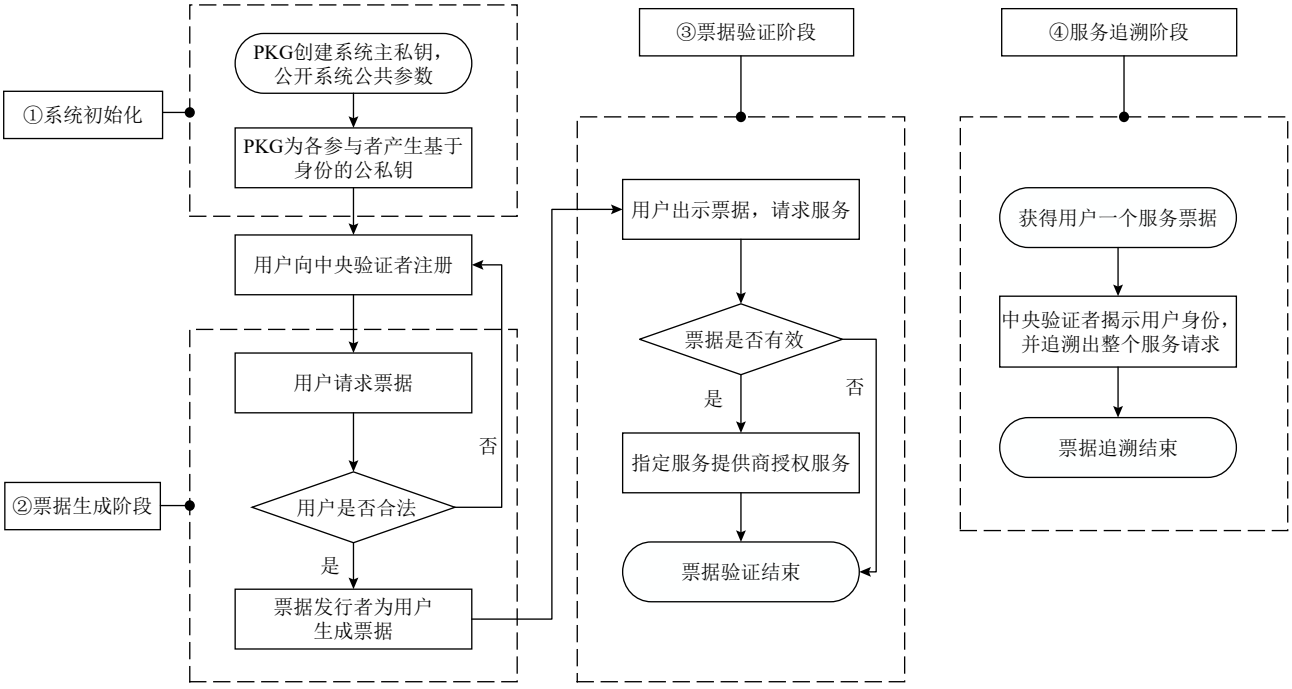

Fig. 1 Flow chart of the supervised ASSO scheme on lattice

图 1 格上可追溯的 ASSO 方案流程图

4) $Ticket\text{-}Issuing(Input_u(Param, J_u, \boldsymbol{sk}_u) \leftrightarrow Input_{iss}(\boldsymbol{sk}_{iss}, Param, \boldsymbol{pk}_u))$: 输入系统的公共参数$Param$, 票据发行者的私钥$\boldsymbol{sk}_{iss}$, 用户想要访问的服务请求$J_u$以及公私钥$(\boldsymbol{pk}_u, \boldsymbol{sk}_u)$, 输出用户服务请求$J_u$对应的票据$T_u$.

5) $Ticket\text{-}Validating(Input_u(Param, Tag_v, \boldsymbol{sk}_u) \leftrightarrow Input_v(Param, \boldsymbol{sk}_v, \boldsymbol{pk}_v, \boldsymbol{pk}_u, \boldsymbol{pk}_{iss}))$: 输入系统的公共参数$Param$, 指定票据验证者的公私钥$(\boldsymbol{pk}_v, \boldsymbol{sk}_v)$, 用户的认证标签$Tag_v$以及公私钥$(\boldsymbol{pk}_u, \boldsymbol{sk}_u)$, 票据发行者的公钥$\boldsymbol{pk}_{iss}$. 如果$Tag_v$通过验证, 返回“Valid”, 否则返回“Invalid”.

6) $Ticket\text{-}Trace(Input_u(T_u) \leftrightarrow Input_{cv}(Param, \boldsymbol{sk}_{cv}))$: 输入系统的公共参数$Param$和用户票据$T_u$, 中央验证者的私钥$\boldsymbol{sk}_{cv}$. 如果追溯成功, 则输出用户的身份$ID_u$以及其服务请求$J_u$, 否则返回“⊥”.

2.3 安全模型

一个具有可追溯性的匿名单点登录方案需要满足用户服务的不可链接性、票据的不可伪造性和服务票据的可追溯性[19].

定义 3. 不可链接性. 要求即使某些票据验证者与用户串通时也不能对其他用户的整个服务信息进行剖析, 有效保护用户服务请求的隐私. 如果对于任意概率多项式时间(probabilistic polynomial time, PPT)算法敌手$\mathcal{A}$, $\mathcal{A}$最多进行σ_1次票据发行询问、σ_2次票据验证询问、σ_3次票据追溯询问, 以可忽略的优势 $Adv_{\mathcal{A}} = \left| Pr[b' = b] - \frac{1}{2} \right| \leqslant \varepsilon(\ell)$赢得游戏挑战时, 则称格上可追溯的匿名单点登录方案是$(\sigma_1, \sigma_2, \sigma_3, \varepsilon(\ell))$用户服务请求安全的(具体见 4.2 节).

定义 4. 不可伪造性. 要求即便指定票据验证者、中央验证者与用户串通, 它们也不能伪造一个有效的票据. 如果对于任意 PPT 敌手$\mathcal{A}$, $\mathcal{A}$最多进行p次票据发行询问时, 对于所有$ID_v \in J_u$, 以可忽略的优势$Adv_{\mathcal{A}} = Pr[Ticket\text{-}Validating(Input_u \leftrightarrow Input_v) \rightarrow (\perp, (1, Tag_{v^*}))] \leqslant \varepsilon(\ell)$赢得游戏挑战时, 称格上可追溯的匿名单点登录方案是$(p, \varepsilon(\ell))$票据发行安全的(具体见 4.3 节).

定义 5. 可追溯性要求. 即便某些用户串通, 它们也无法生成属于串通组某一成员的票据, 使得票据追溯算法无法捕捉到该票据. 本文假设票据发行者是诚实的. 如果任意 PPT 敌手$\mathcal{A}$在最多进行k次票据发行询问时, 以可忽略的优势$Adv_{\mathcal{A}} = Pr[u^* \neq \overline{u} \in QK_u | Ticket\text{-}Trace(Input_u \leftrightarrow Input_{cv}) \rightarrow (\overline{u}, J_{\overline{u}})] \leqslant \varepsilon(\ell)$赢得所构造的游戏挑战时, 则称格上可追溯的匿名单点登录方案是$(k, \varepsilon(\ell))$可追溯的(具体见 4.4 节).

3 格上可追溯的匿名单点登录方案

本文使用方阵$\boldsymbol{A} \xleftarrow{R} \mathbb{Z}_q^{m \times m}$, 有助于在矩阵本身与行/列向量间执行运算, 从而保持矩阵乘法的平稳运行. 方案包括 6 个阶段.

3.1 系统建立阶段

运行$Keygen(1^n)$算法, 以安全参数n作为算法输入,

最终输出 PKG 的主密钥$\boldsymbol{msk}$和系统的公共参数 $Param$. PKG 执行运算 1)~4)：

1)选择 1 个安全参数 n, $\beta = ploy(n)$, 素数模 $q \geqslant \beta\sqrt{\omega(n\log n)}$, 整数 $m \geqslant 2n\log q$, 高斯参数 σ 和矩阵 $\boldsymbol{A} \xleftarrow{R} \mathbb{Z}_q^{m\times m}$, $\boldsymbol{A}$ 的秩为 $n(m \geqslant n)$.

2)选取 $\boldsymbol{x} \xleftarrow{R} D_\sigma^m$, 以压倒性的概率输出 $\|\boldsymbol{x}\| \leqslant 2\sigma\sqrt{m} \leqslant \dfrac{\beta}{2}$, 并计算 $\boldsymbol{mpk} = \boldsymbol{Ax}$, 则主密钥 $\boldsymbol{msk} = \boldsymbol{x}$, $\boldsymbol{mpk}$ 是主公钥.

3)选择 5 个加密安全的 Hash 函数：$h: \{0,1\}^* \to \{r: \{-1,0,1\}^m, \|r\|_1 \leqslant \eta\}$, η 是 r 的汉明值；$H_1: \{0,1\}^* \to \mathbb{Z}_2^{m\times m}$, $\mathbb{Z}_2^{m\times m}$ 是一个对角线上为 $\{0,1\}$、其他为 0 的方阵；$H_2: \{0,1\}^* \to \mathbb{Z}$; $H_3: \{0,1\}^* \to \{0,1\}^\tau$, $\tau < m$; $H: \{0,1\}^* \to B_k^m$, B_k^m 是长度为 m 且“1”的个数为 k 的二进制向量集.

4)主密钥 $\boldsymbol{x}$ 保密, 公开 $Param = \{m, n, q, \boldsymbol{A}, \boldsymbol{mpk}, H_1, H_2, H_3, h, H\}$.

3.2 密钥提取阶段

密钥提取阶段用来产生各参与者基于身份的私钥, 此阶段使用安全通道进行信息发送. 该阶段以 PKG 的主密钥、参与者的身份以及公共参数作为输入, 输出参与者基于身份的私钥. 用户为了获得基于身份的公私钥, 给 PKG 发送它的身份. 为了使用户注册阶段和票据追溯阶段能够顺利恢复出用户身份, 设 $ID_u \in \{0,1\}^{64}$. PKG 选择 $\boldsymbol{r}_u \xleftarrow{R} D_\sigma^m$, 计算 $\boldsymbol{l}_u = \boldsymbol{A}\cdot\boldsymbol{r}_u$, $\boldsymbol{R}_u = H_1(ID_u, \boldsymbol{l}_u)$, $\boldsymbol{d}_u = \boldsymbol{r}_u + \boldsymbol{R}_u\cdot\boldsymbol{x} \bmod q$, 用安全信道将 $\langle \boldsymbol{l}_u, \boldsymbol{d}_u\rangle$ 发送给用户. 基于身份的私钥 $\boldsymbol{d}_u$ 如果满足 $\boldsymbol{A}\cdot\boldsymbol{d}_u = \boldsymbol{l}_u + \boldsymbol{R}_u\cdot\boldsymbol{mpk}$, 则是有效的, 此时用户的公钥为 $\boldsymbol{pk}_u = \boldsymbol{A}\cdot\boldsymbol{d}_u$. 使用相同的方法, 计算中央验证者基于身份的公私钥 $(\boldsymbol{d}_{cv}, \boldsymbol{pk}_{cv})$, 指定票据验证者基于身份的公私钥 $(\boldsymbol{d}_v, \boldsymbol{pk}_v)$.

票据发行者基于身份的公私钥生成方式略有不同, 票据发行者给 PKG 发送身份 ID_{iss}. 然后 PKG 选择 $\boldsymbol{r}_{iss} \xleftarrow{R} D_\sigma^m$, 计算 $\boldsymbol{l}_{iss} = \boldsymbol{r}_{iss}^{\mathrm{T}}\cdot\boldsymbol{A}$, $\boldsymbol{R}_{iss} = H_1(ID_{iss}, \boldsymbol{l}_{iss})$, $\boldsymbol{d}_{iss} = \boldsymbol{r}_{iss} + \boldsymbol{R}_{iss}\cdot\boldsymbol{x} \bmod q$, 最终给票据发行者返回 $\langle \boldsymbol{l}_{iss}, \boldsymbol{d}_{iss}\rangle$. 计算 $\boldsymbol{pk}_{iss} = \boldsymbol{d}_{iss}^{\mathrm{T}}\cdot\boldsymbol{A}$, 则票据发行者基于身份的私钥为 $\boldsymbol{d}_{iss}$, 公钥为 $\boldsymbol{pk}_{iss}$.

3.3 用户注册阶段

用户加入系统时, 需要向中央验证者注册, 以便中央验证者对用户去匿名化, 追溯出其服务请求. 每个用户加入系统时, 选取 $\boldsymbol{b} \xleftarrow{R} D_\sigma^m$, 计算 2 个密文 $\boldsymbol{c}_1 = \boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{b}$, $c_2 = \boldsymbol{pk}_{cv}^{\mathrm{T}}\cdot\boldsymbol{b} + ID_u\cdot\left\lfloor\dfrac{q}{2}\right\rfloor$, 然后发送 $((\boldsymbol{c}_1, c_2), \boldsymbol{l}_u)$ 给中央验证者, 中央验证者收到信息后, 计算 $ID_u = \dfrac{c_2 - \boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{c}_1}{\left\lfloor\dfrac{q}{2}\right\rfloor}$, 得用户的身份 ID_u, 通过验证 $\boldsymbol{pk}_u = \boldsymbol{l}_u + H_1(ID_u, \boldsymbol{l}_u)\cdot\boldsymbol{mpk}$ 是否成立, 保证用户身份的合法性, 如果成立, 则本地存储用户的 $(ID_u, \boldsymbol{pk}_u)$.

3.4 票据发行阶段

为获得 1 张票据, 用户选择它的服务信息 J_u, J_u 由用户想要访问的服务所对应验证者的身份 ID_v 组成, 即 $ID_v \in J_u$. 整个具体过程如图 2 所示, 对于每个 $ID_v \in J_u$, 用户使用其私钥 $\boldsymbol{d}_u$ 生成 1 个假名 $(\boldsymbol{p}_v, \boldsymbol{q}_v)$, 并发送给票据发行者. 票据发行者通过验证 $\boldsymbol{A}\cdot\boldsymbol{q}_v \stackrel{?}{=} \boldsymbol{p}_v\cdot H_2(f, \boldsymbol{p}_v) + \boldsymbol{pk}_u$ 来判断用户是否为 1 个合法用户, 若是合法用户, 票据发行者为用户生成认证标签 $Tag_v = ((f, \boldsymbol{p}_v, \boldsymbol{q}_v), (\boldsymbol{t}, \boldsymbol{r}, \boldsymbol{z}_u), (\boldsymbol{e}_1, e_2), Text, (s_v, \boldsymbol{c}_v, \boldsymbol{z}_v))$. $(\boldsymbol{e}_1, e_2)$ 是用中央验证者公钥 $\boldsymbol{pk}_{cv}$ 加密 ID_v 所生产的 2 个密文, 在票据追溯时, 完成用户服务请求的恢复. 签名 $(\boldsymbol{t}, \boldsymbol{r}, \boldsymbol{z}_u)$ 是用来验证 Tag_v 的有效性, 只有指定的验证者才可以验证. s_v 是认证标签 Tag_v 的序列号, $(s_v, \boldsymbol{c}_v, \boldsymbol{z}_v)$ 是票据发行者对 s_v 的签名, $Text$ 是时间戳, 用来防止票据的重放. 最终票据由这些单独的标签组成, 即 $T_u = \{(D_v, Tag_v) | ID_v \in J_u\} \cup \{(S, \boldsymbol{c}, \boldsymbol{z})\}$.

此阶段, 票据发行者使用它的私钥对每个认证标签和整个票据进行签名, 而认证标签和整个票据的完整性是使用它们各自内容的散列 $s_v = H_2(\boldsymbol{p}_v\|\boldsymbol{q}_v\|\boldsymbol{e}_1\|e_2\|\boldsymbol{t}\|\boldsymbol{r}\|\boldsymbol{z}_u\|Text)$ 和 $S = H_2(s_1\|\ s_2\|\cdots\|s_{|J_u|})$ 来保证的. 票据发行者将票据发送给用户, 用户通过验证散列值来验证每个认证标签和整个票据的完整性, 以及验证签名 $\boldsymbol{c}_v \stackrel{?}{=} H(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_v \bmod q, s_v)$ 和 $\boldsymbol{c} \stackrel{?}{=} H(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z} \bmod q, S)$ 来证明每个认证标签和整个票据来自票据发行者.

3.5 票据验证阶段

当验证 1 个票据时, 指定票据验证者初始化 1 个空表 T_v, 将身份 ID_v 发送给用户. 用户通过计算 $D_v = H_3(\boldsymbol{q}_u, ID_v)$, 找到对应的标签 Tag_v, 并将 Tag_v 发送给指定票据验证者. 如图 3 所示, 指定票据验证者通过判断 $(s_v, \boldsymbol{c}_v, \boldsymbol{z}_v)$ 是否属于 T_v, 来防止票据 2 次验证. 如果 Tag_v 是个新鲜的标签, 则将 $(s_v, \boldsymbol{c}_v, \boldsymbol{z}_v)$ 加入 T_v, 并通过检查 $\boldsymbol{A}\cdot\boldsymbol{q}_v \stackrel{?}{=} \boldsymbol{p}_v\cdot H_2(f, \boldsymbol{p}_v) + \boldsymbol{pk}_u$ 来验证用户是否为合法用户, 检查 $s_v \stackrel{?}{=} H_2(\boldsymbol{p}_v\|\boldsymbol{q}_v\|\boldsymbol{e}_1\|e_2\|\boldsymbol{t}\|\boldsymbol{r}\|\boldsymbol{z}_u\|Text)$, $\boldsymbol{r} \stackrel{?}{=} h(\boldsymbol{d}_v^{\mathrm{T}}\cdot(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_u - \boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^{\mathrm{T}})\cdot\boldsymbol{t} \bmod q, \boldsymbol{pk}_v)$, $\boldsymbol{c}_v \stackrel{?}{=} H(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_v \bmod q, s_v)$ 来验证标签的有效性. 若全部成立, 则通过验证.

3.6 票据追溯阶段

票据追溯阶段用来揭示用户的身份, 完成用户的去匿名化, 追溯出用户的整个服务请求 J_u, 实现监管性. 如图 4 所示, 针对用户的服务票据 T_u, 中央验证者初始化一个集合 $P_u = \{\}$. 当 $Tag_v \in T_u$ 时, 通过计算 $\boldsymbol{pk}_u = \boldsymbol{A}\cdot\boldsymbol{q}_v - \boldsymbol{p}_v\cdot H(f, \boldsymbol{p}_v)$, 再根据本地存储的 $(\boldsymbol{pk}_u, ID_u)$ 去匿名化, 最后, 计算 $ID_v = \dfrac{e_2 - \boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{e}_1}{\left\lfloor\dfrac{q}{2}\right\rfloor}$ 获得指定票据验证

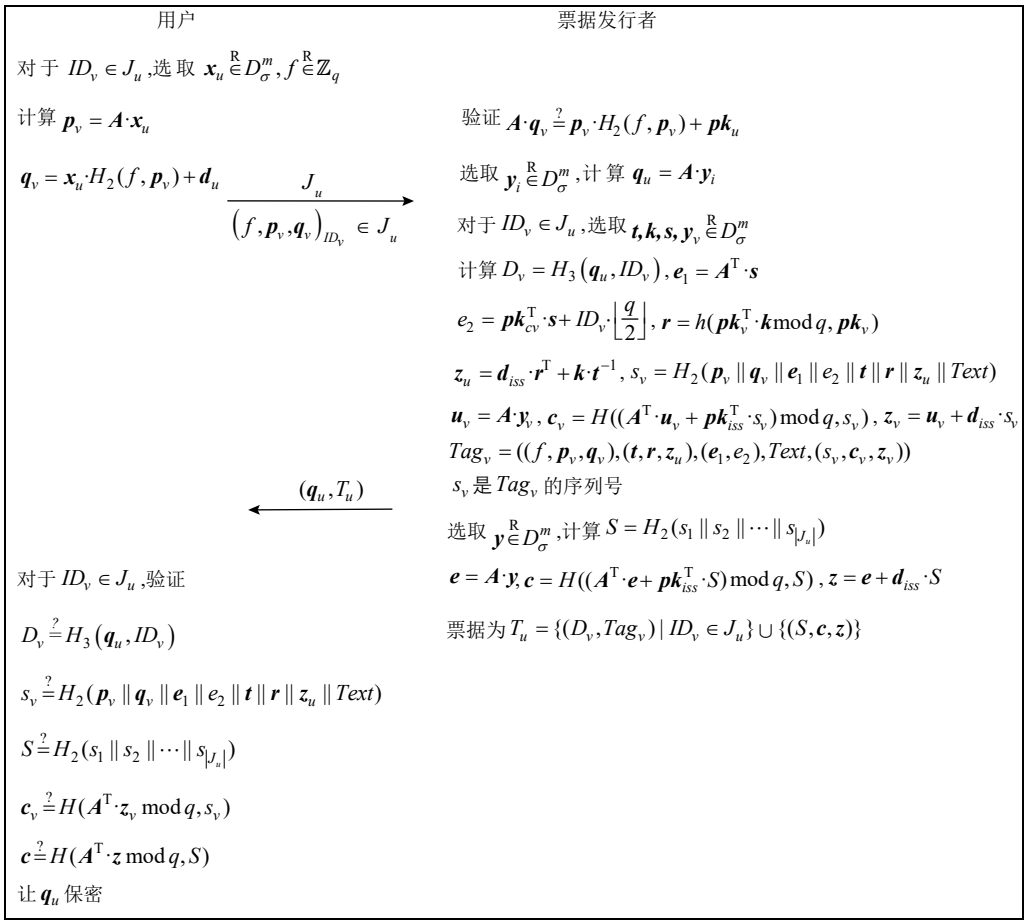

Fig. 2 Ticket-Issuing phase

图 2 票据发行阶段

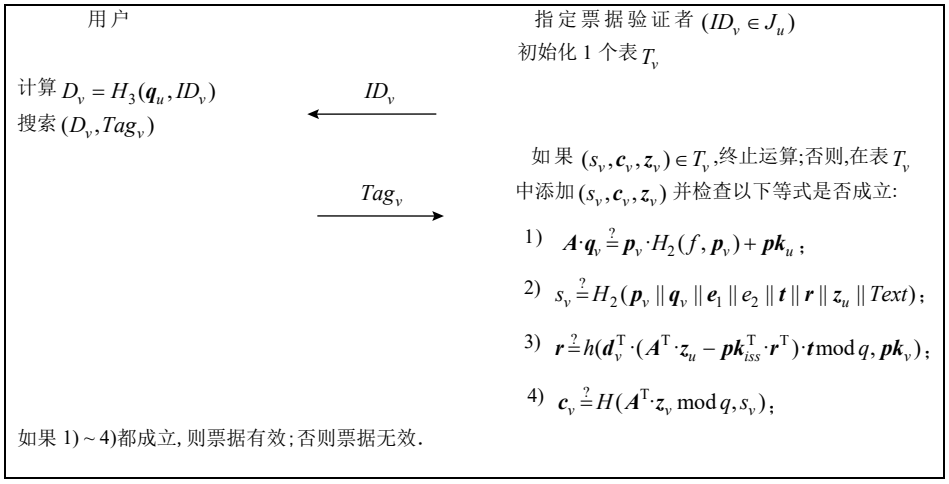

Fig. 3 Ticket-Validating phase

图 3 票据验证阶段

者的身份, 通过判断$ID_v \in J_u$的所有恒等式来判断用户的服务请求. 此时, 如果已知单个标签, 在用户不合作的情况下, 整个票证信息T_u也可以直接从票据发行者处获得.

4 正确性与安全性证明

本文构造的格上可追溯的匿名单点登录方案具有不可链接性、不可伪造性和可追溯性, 并给出正确

给定 1 个票据 T_u，中央验证者执行以下运算:

1) 让 $P_u=\{\}$，对于 $Tag_v\in T_u$:

① 计算 $\boldsymbol{pk}_u=\boldsymbol{A}\cdot\boldsymbol{q}_v-\boldsymbol{p}_v\cdot H(f,\boldsymbol{p}_v)$，$ID_v=\dfrac{e_2-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{e}_1}{\left\lfloor\frac{q}{2}\right\rfloor}$，并验证:

② $s_v\overset{?}{=}H_2(\boldsymbol{p}_v\|\boldsymbol{q}_v\|\boldsymbol{e}_1\|e_2\|\boldsymbol{t}\|\boldsymbol{r}\|\boldsymbol{z}_u\|Text)$，$\boldsymbol{c}_v\overset{?}{=}H(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_v \bmod q,s_v)$;

③ 如果①②都成立，则 $P_u=P_u\cup\{ID_v\}$；否则，终止运算.

④ 对 $\boldsymbol{pk}_u$ 所对应的所有标签进行①～③的验证.

2) $S\overset{?}{=}H_2(s_1\|s_2\|\cdots\|s_{|J_u|})$，$\boldsymbol{c}\overset{?}{=}H(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}\bmod q,S)$;

如果 1) 2)都成立,则中央验证者可以通过用户公钥 $\boldsymbol{pk}_u$ 来确定用户的服务信息是 $J_u=P_u$,实现票据追溯；否则，票据追溯失败.

Fig. 4 Ticket-Trace phase

图 4 票据追溯阶段

性与安全性证明.

4.1 正确性

所构造的格上可追溯的匿名单点登录方案,在用户密钥提取算法ExtractKey中,$\boldsymbol{l}_u=\boldsymbol{A}\cdot\boldsymbol{r}_u$, $\boldsymbol{d}_u=\boldsymbol{r}_u+\boldsymbol{R}_u\cdot\boldsymbol{x} \bmod q$,由此可得式(1)成立,用户的公私钥可以正确生成.

$$\boldsymbol{A}\cdot\boldsymbol{d}_u=\boldsymbol{A}\cdot\boldsymbol{r}_u+\boldsymbol{R}_u\cdot\boldsymbol{A}\cdot\boldsymbol{x}=\boldsymbol{l}_u+\boldsymbol{R}_u\cdot\boldsymbol{mpk}. \tag{1}$$

用户注册算法User - Registration中,$\boldsymbol{c}_1$和c_2是使用中央验证者公钥对用户身份加密所产生的密文,在式(2)中,通过使用中央验证者的私钥$\boldsymbol{d}_{cv}$,可以正确解密以恢复用户身份ID_u.

$$\frac{c_2-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{c}_1}{\left\lfloor\frac{q}{2}\right\rfloor}=\frac{\boldsymbol{pk}_{cv}^{\mathrm{T}}\cdot\boldsymbol{b}+ID_u\cdot\left\lfloor\frac{q}{2}\right\rfloor-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{b}}{\left\lfloor\frac{q}{2}\right\rfloor}=ID_u. \tag{2}$$

对于采用假名技术[27]所生成的正确假名$(\boldsymbol{p}_v,\boldsymbol{q}_v)$,根据$\boldsymbol{pk}_u=\boldsymbol{A}\cdot\boldsymbol{d}_u$可知式(3)一定成立,可顺利完成票据发行算法Ticket - Issuing中的用户匿名认证. 同时$(s_v,\boldsymbol{c}_v,z_v)$和$(S,\boldsymbol{c},z)$分别是票据发行者对$s_v$和$S$的签名,式(4)(5)是对这 2 个签名的验证过程,由 $z_v=\boldsymbol{u}_v+\boldsymbol{d}_{iss}\cdot s_v$, $z=\boldsymbol{e}+\boldsymbol{d}_{iss}\cdot S$可得式(4)(5)成立.

$$\boldsymbol{A}\cdot\boldsymbol{q}_v=\boldsymbol{A}\cdot\boldsymbol{x}_u\cdot H_2(f,\boldsymbol{p}_v)+\boldsymbol{A}\cdot\boldsymbol{d}_u=\boldsymbol{p}_v\cdot H_2(f,\boldsymbol{p}_v)+\boldsymbol{pk}_u, \tag{3}$$

$$\begin{aligned}H(\boldsymbol{A}^{\mathrm{T}}\cdot z_v\bmod q,s_v)=&H((\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{u}_v+\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{d}_{iss}s_v)\bmod q,s_v)=\\&H((\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{u}_v+\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot s_v)\bmod q,s_v),\end{aligned} \tag{4}$$

$$\begin{aligned}H(\boldsymbol{A}^{\mathrm{T}}\cdot z\bmod q,S)=&H((\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{e}+\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{d}_{iss}\cdot S)\bmod q,S)=\\&H((\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{e}+\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot S)\bmod q,S).\end{aligned} \tag{5}$$

票据验证算法Ticket - Validating中,通过对采用指定验证者签名方案[24]所生成的票据信息进行式(6)的验证,完成票据的有效性验证. 已知$\boldsymbol{z}_u=\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^{\mathrm{T}}+\boldsymbol{k}\cdot\boldsymbol{t}^{-1}$,则式(6)恒成立.

$$\begin{aligned}&h(\boldsymbol{d}_v^{\mathrm{T}}\cdot(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_u-\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^{\mathrm{T}})\cdot\boldsymbol{t}\bmod q,\boldsymbol{pk}_v)=\\&h(\boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{A}^{\mathrm{T}}(\boldsymbol{z}_u-\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^{\mathrm{T}})\cdot\boldsymbol{t}\bmod q,\boldsymbol{pk}_v)=\\&h(\boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{k}\cdot\boldsymbol{t}^{-1}\cdot\boldsymbol{t}\bmod q,\boldsymbol{pk}_v)=\\&h(\boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{k}\bmod q,\boldsymbol{pk}_v)=\\&h(\boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{k}\bmod q,\boldsymbol{pk}_v)=\boldsymbol{r}.\end{aligned} \tag{6}$$

通过式(7)(8),可以分别完成票据追溯算法Ticket - Trace中的用户身份去匿名化和访问服务追溯. 由式(3)成立可知式(7)恒成立. 式(8)是中央验证者CV利用其私钥$\boldsymbol{d}_{cv}$对密文$(\boldsymbol{e}_1,e_2)$进行解密.

$$\begin{aligned}\boldsymbol{A}\cdot\boldsymbol{q}_v-\boldsymbol{p}_v\cdot H_2(f,\boldsymbol{p}_v)=&\boldsymbol{A}\cdot\boldsymbol{x}_u\cdot H_2(f,\boldsymbol{p}_v)+\boldsymbol{A}\cdot\boldsymbol{d}_u-\\&\boldsymbol{p}_v\cdot H_2(f,\boldsymbol{p}_v)=\boldsymbol{pk}_u,\end{aligned} \tag{7}$$

$$\frac{e_2-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{e}_1}{\left\lfloor\frac{q}{2}\right\rfloor}=\frac{\boldsymbol{pk}_{cv}^{\mathrm{T}}\cdot\boldsymbol{b}+ID_v\cdot\left\lfloor\frac{q}{2}\right\rfloor-\boldsymbol{d}_{cv}^{\mathrm{T}}\cdot\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{b}}{\left\lfloor\frac{q}{2}\right\rfloor}=ID_v. \tag{8}$$

在 PKG 的协助下,正确生成各参与方的公私钥,式(1)～(8)成立,用户服务票据能正确生成,并通过指定票据验证者验证,最终中央验证者也可以在必要情况下正确追溯出用户的服务信息. 因此,所提方案满足正确性.

4.2 不可链接性证明

定理 1. 若存在敌手$\mathcal{A}$在至多进行σ_1次票据发行询问、σ_2次票据验证询问、σ_3次票据追溯询问后,以$(\sigma_1,\sigma_2,\sigma_3,\varepsilon'(\ell))$的优势打破本方案的选择性不可链接性,则可以构造一个以$\mathcal{A}$为子程序的算法$\mathcal{B}$,以不可忽略的优势$Adv_{\mathcal{B}}^{\mathrm{ISIS}_{q,n,m,\beta}}=\left|\frac{1}{2}Pr[b'=b|b=0]+\frac{1}{2}Pr[b'=b|b=1]-\frac{1}{2}\right|\geqslant\frac{\varepsilon'(\ell)}{2}$解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题.

证明. 给定一个元组$(\boldsymbol{r}_w^*,\boldsymbol{t}^*,\boldsymbol{k})$,挑战者$C$抛掷一个值为{0, 1}的硬币,得到 1 个比特位$b\in\{0,1\}$. 如果$b=0$, C给$\mathcal{B}$发送$\boldsymbol{g}=\boldsymbol{d}_{iss}\cdot\boldsymbol{r}_w^{*\mathrm{T}}+\boldsymbol{k}\cdot\boldsymbol{t}^{*-1}$;否则发送$\boldsymbol{g}\overset{\mathrm{R}}{\in}\mathbb{Z}_q^m$. 最终$\mathcal{B}$将输出它对$b$的猜测$b'$.

1)初始化. $\mathcal{A}$提交 2 个验证者v_0^*和v_1^*, $\mathcal{B}$抛掷一个

值为{0, 1}的硬币, 得到 1 个比特位$w \in \{0,1\}$. $\mathcal{B}$选取$\boldsymbol{k}, \boldsymbol{r}' \overset{R}{\in} D_\sigma^m$, 并计算$\boldsymbol{r}_w^* = h(\boldsymbol{pk}_v^{\mathrm{T}} \cdot \boldsymbol{k} \bmod q, \boldsymbol{pk}_v)$和$\boldsymbol{r}_{1-w}^* = \boldsymbol{r}'$.

2)系统设置. $\mathcal{B}$选择$\boldsymbol{A} \overset{R}{\in} \mathbb{Z}_q^{m\times m}$, $\boldsymbol{x} \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{mpk} = \boldsymbol{A} \cdot \boldsymbol{x}$, $h: \{0,1\}^* \to \{r: \{-1,0,1\}^m, \|r\|_1 \leqslant \eta\}$, η是r的汉明值; $H_1: \{0,1\}^* \to \mathbb{Z}_2^{m\times m}$, $\mathbb{Z}_2^{m\times m}$是一个对角线上为{0, 1}且其他为 0 的方阵; $H_2: \{0,1\}^* \to \mathbb{Z}$; $H_3: \{0,1\}^* \to \{0,1\}^\tau$, $\tau < m$; $H: \{0,1\}^* \to B_k^m$, B_k^m是长度为 m 且“1”的个数为 k 的二进制向量集, $\mathcal{B}$给$\mathcal{A}$发送公共参数$Param = \{m, n, q, \boldsymbol{A}, \boldsymbol{mpk}, H_1, H_2, H_3, h, H\}$.

3)注册询问. A 可以进行①~④注册询问.

①用户注册询问. 初始化一个列表RQ_u, 用来存储用户注册信息. $\mathcal{A}$提交一个用户的身份ID_u, 并发送给$\mathcal{B}$, $\mathcal{B}$选择$\boldsymbol{r}_u \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{l}_u = \boldsymbol{A} \cdot \boldsymbol{r}_u$, $\boldsymbol{R}_u = H_1(ID_u, \boldsymbol{l}_u)$, $\boldsymbol{d}_u = \boldsymbol{r}_u + \boldsymbol{R}_u \cdot \boldsymbol{x} \bmod q$, $\boldsymbol{pk}_u = \boldsymbol{A} \cdot \boldsymbol{d}_u$, $\mathcal{B}$给$\mathcal{A}$发送$(ID_u, \boldsymbol{pk}_u)$, 并添加到$RQ_u$. $\mathcal{A}$可以做出多次询问.

②票据发行者注册询问. $\mathcal{B}$选择$\boldsymbol{r}_{iss} \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{l}_{iss} = \boldsymbol{r}_{iss}^{\mathrm{T}} \cdot \boldsymbol{A}$, $\boldsymbol{R}_{iss} = H_1(ID_{iss}, \boldsymbol{l}_{iss})$, $\boldsymbol{d}_{iss} = \boldsymbol{r}_{iss} + \boldsymbol{R}_{iss} \cdot \boldsymbol{x} \bmod q$与$\boldsymbol{pk}_{iss} = \boldsymbol{d}_{iss}^{\mathrm{T}} \cdot \boldsymbol{A}$, $\mathcal{B}$给$\mathcal{A}$发送$(ID_{iss}, \boldsymbol{pk}_{iss})$.

③票据验证者注册询问. 设$Corruptu_v$是被$\mathcal{A}$损坏的验证者身份组成的集合, $\mathcal{A}$提交一个验证者身份$ID_v \notin \{ID_{v_0^*}, ID_{v_1^*}\}$, 当$ID_v \in Corruptu_v$时, $\mathcal{A}$给$\mathcal{B}$发送$(ID_v, \boldsymbol{pk}_v)$; 当$ID_v \notin Corruptu_v$时, $\mathcal{B}$选择$\boldsymbol{r}_v \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{l}_v = \boldsymbol{A} \cdot \boldsymbol{r}_v, \boldsymbol{R}_v = H_1(ID_v, \boldsymbol{l}_v), \boldsymbol{d}_v = \boldsymbol{r}_v + \boldsymbol{R}_v \cdot \boldsymbol{x} \bmod q, \boldsymbol{pk}_v = \boldsymbol{A} \cdot \boldsymbol{d}_v$, $\mathcal{B}$将$\boldsymbol{pk}_v$发送给$\mathcal{A}$. $\mathcal{A}$可以做出多次询问.

④中央验证者注册询问. $\mathcal{B}$选择$\boldsymbol{r}_{cv} \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{l}_{cv} = \boldsymbol{A} \cdot \boldsymbol{r}_{cv}$, $\boldsymbol{R}_{cv} = H_1(ID_{cv}, \boldsymbol{l}_{cv})$, $\boldsymbol{d}_{cv} = \boldsymbol{r}_{cv} + \boldsymbol{R}_{cv} \cdot \boldsymbol{x} \bmod q$和$\boldsymbol{pk}_{cv} = \boldsymbol{A} \cdot \boldsymbol{d}_{cv}$, $\mathcal{B}$给$\mathcal{A}$发送$(ID_{cv}, \boldsymbol{pk}_{cv})$.

4)票据发行询问. $\mathcal{A}$提交身份$ID_u \in RQ_u$, 服务信息J_u, 假名$PS_u = \{(\boldsymbol{p}_v, \boldsymbol{q}_v) | ID_v \in J_u\}$, 如果等式$\boldsymbol{A} \cdot \boldsymbol{q}_v = \boldsymbol{p}_v \cdot H_2(f, \boldsymbol{p}_v) + \boldsymbol{pk}_u$不成立, 则$\mathcal{B}$中止运行. 否则, $\mathcal{B}$执行运算: $\mathcal{B}$选择$\boldsymbol{y}_i \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{q}_u = \boldsymbol{A} \cdot \boldsymbol{y}_i$, 若$ID_v \in J_u$, $\mathcal{B}$选择$\boldsymbol{t}, \boldsymbol{k}, \boldsymbol{s}, \boldsymbol{y}_v \overset{R}{\in} D_\sigma^m$, 计算$D_v = H_3(\boldsymbol{q}_u, ID_v)$, $\boldsymbol{e}_1 = \boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{s}$, $e_2 = \boldsymbol{pk}_{cv}^{\mathrm{T}} \cdot \boldsymbol{s} + ID_v \cdot \left\lfloor \frac{q}{2} \right\rfloor$, $\boldsymbol{r} = h(\boldsymbol{pk}_v^{\mathrm{T}} \cdot \boldsymbol{k} \bmod q, \boldsymbol{pk}_v)$, $\boldsymbol{z}_u = \boldsymbol{d}_{iss} \cdot \boldsymbol{r}^{\mathrm{T}} + \boldsymbol{k} \cdot \boldsymbol{t}^{-1}$, $s_v = H_2(\boldsymbol{p}_v \| \boldsymbol{q}_v \| \boldsymbol{e}_1 \| e_2 \| \boldsymbol{t} \| \boldsymbol{r} \| \boldsymbol{z}_u \| Text)$, $\boldsymbol{u}_v = \boldsymbol{A} \cdot \boldsymbol{y}_v$, $\boldsymbol{c}_v = H((\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{u}_v + \boldsymbol{pk}_{iss}^{\mathrm{T}} \cdot s_v) \bmod q, s_v)$, $\boldsymbol{z}_v = \boldsymbol{u}_v + \boldsymbol{d}_{iss} \cdot s_v$, $Tag_v = ((f, \boldsymbol{p}_v, \boldsymbol{q}_v), (\boldsymbol{t}, \boldsymbol{r}, \boldsymbol{z}_u), (\boldsymbol{e}_1, e_2), Text, (s_v, \boldsymbol{c}_v, \boldsymbol{z}_v))$, $S = H_2(s_1 \| s_2 \| \cdots \| s_{|J_u|})$, $\mathcal{B}$选择$\boldsymbol{y} \overset{R}{\in} D_\sigma^m$, 计算$\boldsymbol{e} = \boldsymbol{A} \cdot \boldsymbol{y}$, $\boldsymbol{c} = H((\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{e} + \boldsymbol{pk}_{iss}^{\mathrm{T}} \cdot S) \bmod q, S)$, $\boldsymbol{z} = \boldsymbol{e} + \boldsymbol{d}_{iss} \cdot S$, 票据$T_u = \{(D_v, Tag_v) | ID_v \in J_u\} \cup \{(S, \boldsymbol{c}, \boldsymbol{z})\}$, $\mathcal{B}$给$\mathcal{A}$返回$(\boldsymbol{q}_u, T_u, Text)$. 设$QI$为$\mathcal{A}$查询的票证信息集合, 初始为空, $\mathcal{B}$向QI添加$\{PS_u, J_u, T_u, \boldsymbol{y}_i\} \cup \{\boldsymbol{k} | ID_v \in J_u\}$.

5)票据验证询问. $\mathcal{B}$初始化一个表T_v, $\mathcal{A}$提交一个Tag_v. 如果$Tag_v \in T_v$, $\mathcal{B}$运行中止; 否则, $\mathcal{B}$将Tag_v添加到T_v中, 执行以下操作, 如果$Tag_v \notin QI$, $\mathcal{B}$运行中止, 否则$\mathcal{B}$检查$D_v \overset{?}{=} H_3(\boldsymbol{q}_u, ID_v)$, $\boldsymbol{r} \overset{?}{=} h(\boldsymbol{d}_v^{\mathrm{T}} \cdot (\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{z}_u - \boldsymbol{pk}_{iss}^{\mathrm{T}} \cdot \boldsymbol{r}^{\mathrm{T}}) \cdot \boldsymbol{t} \bmod q, \boldsymbol{pk}_v)$, $s_v \overset{?}{=} H_2(\boldsymbol{p}_v \| \boldsymbol{q}_v \| \boldsymbol{e}_1 \| e_2 \| \boldsymbol{t} \| \boldsymbol{r} \| \boldsymbol{z}_u \| Text)$, $\boldsymbol{c}_v \overset{?}{=} H(\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{z}_v \bmod q, s_v)$, 如果以上等式成立, 则$\mathcal{B}$将$ID_v$返回给$\mathcal{A}$, 否则返回“⊥”表示失败. 设$QV$为由$\mathcal{A}$查询票据验证的列表, 初始为空, $\mathcal{B}$在QV中加入Tag_v.

6)票据追溯询问. $\mathcal{A}$提交一个票据T_u, $\mathcal{B}$执行 4 个操作.

设$P_u = \{\}$, 对于每个$Tag_v \in T_u$: 计算$\boldsymbol{pk}_u = \boldsymbol{A} \cdot \boldsymbol{q}_v - \boldsymbol{p}_v \cdot H(f, \boldsymbol{p}_v)$, $ID_v = \dfrac{e_2 - \boldsymbol{d}_{cv}^{\mathrm{T}} \cdot \boldsymbol{e}_1}{\left\lfloor \frac{q}{2} \right\rfloor}$, 根据$ID_v$检查$s_v \overset{?}{=} H_2(\boldsymbol{p}_v \| \boldsymbol{q}_v \| \boldsymbol{e}_1 \| e_2 \| \boldsymbol{t} \| \boldsymbol{r} \| \boldsymbol{z}_u \| Text)$, $\boldsymbol{c}_v \overset{?}{=} H(\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{z}_v \bmod q, s_v)$, 如果满足等式, 则$P_u = P_u \cup \{ID_v\}$, 否则终止; 若不终止, 则检查$S \overset{?}{=} H_2(s_1 \| s_2 \| \cdots \| s_{|J_u|})$, $\boldsymbol{c} \overset{?}{=} H(\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{z} \bmod q, S)$. 如果以上等式成立, 中央验证者可以根据用户的公钥$\boldsymbol{pk}_u$来确定用户的服务信息$J_u = P_u$, 否则追溯失败. 设QT为由$\mathcal{A}$查询的票据跟踪信息组成的列表, 初始为空. $\mathcal{B}$在QT中加入T_u.

挑战. $\mathcal{B}$选取$\boldsymbol{e}, \boldsymbol{y}_1, \boldsymbol{y}_2, \boldsymbol{y}_3 \overset{R}{\in} D_\sigma^m$, $f \overset{R}{\in} \mathbb{Z}_p$, 计算$\boldsymbol{p}_u^* = \boldsymbol{A} \cdot \boldsymbol{e}$, $\boldsymbol{q}_u^* = \boldsymbol{e} \cdot H_2(f, \boldsymbol{p}_u^*) + \boldsymbol{d}_u$, $\boldsymbol{b}_u^* = \boldsymbol{A} \cdot \boldsymbol{y}_1$, $D_v^* = H_3(\boldsymbol{b}_u^*, ID_v)$, $\boldsymbol{r}^* = \boldsymbol{r}_w^*$, $\boldsymbol{z}_u^* = \boldsymbol{g}$, $s_v^* = H_2(\boldsymbol{p}_u^* \| \boldsymbol{q}_u^* \| \boldsymbol{e}_1^* \| e_2^* \| \boldsymbol{t}^* \| \boldsymbol{r}^* \| \boldsymbol{z}^* \| Text)$, $\boldsymbol{u}_v^* = \boldsymbol{A} \cdot \boldsymbol{y}_2$, $\boldsymbol{c}_v^* = H((\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{u}_v^* + \boldsymbol{pk}_{iss}^{\mathrm{T}} \cdot s_u^*) \bmod q, s_u^*)$, $\boldsymbol{z}_v^* = \boldsymbol{u}_v^* + \boldsymbol{d}_{iss} \cdot s_u^*$, $Tag_u^* = ((f, \boldsymbol{p}_u^*, \boldsymbol{q}_u^*), (\boldsymbol{e}_1^*, e_2^*), (\boldsymbol{t}^*, \boldsymbol{r}^*, \boldsymbol{z}_u^*), Text, (s_v^*, \boldsymbol{c}_v^*, \boldsymbol{z}_v^*))$, $S^* = H_2(s_v^*)$以及$\boldsymbol{u}^* = \boldsymbol{A} \cdot \boldsymbol{y}_3$, $\boldsymbol{c}^* = H((\boldsymbol{A}^{\mathrm{T}} \cdot \boldsymbol{u}^* + \boldsymbol{pk}_{iss}^{\mathrm{T}} \cdot S^*) \bmod q, S^*)$, $\boldsymbol{z}^* = \boldsymbol{u}^* + \boldsymbol{d}_{iss} \cdot S^*$, $T_u^* = (D_v^*, Tag_u^*) \cup \{S^*, \boldsymbol{c}^*, \boldsymbol{z}^*\}$, $\mathcal{B}$给$\mathcal{A}$发送T_u^*.

应答阶段. 和挑战阶段一样, 但有限制①~③: ①$(\boldsymbol{r}^*, \boldsymbol{t}^*, \boldsymbol{z}_u^*) \notin QV$; ②$(\boldsymbol{r}^*, \boldsymbol{t}^*, \boldsymbol{z}_u^*) \notin QT$; ③$\mathcal{A}$可以自适应做出最多$\sigma_1$次票据发行询问、$\sigma_2$次票据验证询问、$\sigma_3$次票据追溯询问.

输出. $\mathcal{A}$输出它对w的猜测w', 如果$w' = w$, 则$\mathcal{B}$输出$b' = 0$, 否则输出$b' = 1$.

如果$b = 0$, $\boldsymbol{g} = \boldsymbol{d}_{iss} \cdot \boldsymbol{r}_w^{*\mathrm{T}} + \boldsymbol{k} \cdot \boldsymbol{t}^{*-1}$, 则$T_u^*$是个有效的票据, 因此, $\mathcal{A}$以$\left| Pr[w' = w | b = 0] - \frac{1}{2} \right| \geqslant \varepsilon'(\ell)$的概率输出$w' = w$. 而当$w' = w$时, $\mathcal{B}$可以输出$b' = 0$, 即$\left| Pr[b' = b | b = 0] - \frac{1}{2} \right| \geqslant \varepsilon'(\ell)$.

如果$b = 1$, 则$\boldsymbol{g} \overset{R}{\in} \mathbb{Z}_q^m$, T_u^*中的元素是随机的, $Pr[w' \neq w | b = 1] = \frac{1}{2}$. 当$w' \neq w$时, $\mathcal{B}$可以输出$b' = 1$, 即$Pr[b' = b | b = 1] = \frac{1}{2}$. 因此$\mathcal{B}$解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题的优势: $Adv_{\mathcal{B}}^{\mathrm{ISIS}_{q,n,m,\beta}} = \left| \frac{1}{2} Pr[b' = b | b = 0] + \frac{1}{2} Pr[b' = b | b = 1] - \right.$

$\left|\frac{1}{2}\right| \geqslant \frac{\varepsilon'(\ell)}{2}$.

已知$\mathrm{ISIS}_{q,n,m,\beta}$在格上是个困难问题，求解非零短向量是困难的，$\mathcal{A}$无法以不可忽略的优势破坏不可链接性，本方案具有不可链接性.

证毕.

4.3 不可伪造性证明

定理 2. 如果存在一个敌手$\mathcal{A}$以$\varepsilon_1(\ell)$的优势打破方案的不可伪造性，则可以构造一个算法$\mathcal{B}$，它可以将$\mathcal{A}$作为一个子程序，以不可忽略的优势解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题.

证明. 设$\mathcal{A}$是攻击不可伪造性的PPT敌手，若$\mathcal{A}$采用文献[19, 29−30]中的谕言机问询模式，在至多进行$p(p<q)$次票据发行询问下，以$\varepsilon_1(\ell)$的优势伪造1个有效的用户服务票据，则算法$\mathcal{B}$可以以$\mathcal{A}$作为子程序，以$Adv_{\mathcal{B}}^{\mathrm{ISIS}_{q,n,m,\beta}} = Pr[Ticket\text{-}Validating(Input_u(\boldsymbol{sk}_{u^*}, Tag_{v^*}, Param) \leftrightarrow Input_v(\boldsymbol{sk}_{v^*}, \boldsymbol{pk}_{v^*}, \boldsymbol{pk}_{u^*}, Param)) \rightarrow (\perp, (1, Tag_{v^*}))] \geqslant \frac{q-p}{q}\varepsilon_1(\ell)$的优势解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题.

1)系统设置.$\mathcal{B}$选择$\boldsymbol{A} \xleftarrow{R} \mathbb{Z}_q^{m\times m}$，$\boldsymbol{x} \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{mpk} = \boldsymbol{A}\cdot\boldsymbol{x}$，$h: \{0,1\}^* \rightarrow \{r: \{-1,0,1\}^m, \|r\|_1 \leqslant \eta\}$，$\eta$是$r$的汉明值；$H_1: \{0,1\}^* \rightarrow \mathbb{Z}_2^{m\times m}$，$\mathbb{Z}_2^{m\times m}$是个对角线上为$\{0,1\}$而其他为0的方阵；$H_2: \{0,1\}^* \rightarrow \mathbb{Z}$；$H_3: \{0,1\}^* \rightarrow \{0,1\}^\tau$，$\tau < m$；$H: \{0,1\}^* \rightarrow B_k^m$，$B_k^m$是长度为$m$且“1”的个数为$k$的二进制向量集，$\mathcal{B}$给$\mathcal{A}$发送公共参数$Param = \{m, n, q, \boldsymbol{A}, MPK, H_1, H_2, H_3, h, H\}$.

2)注册询问. $\mathcal{A}$可以做出①~④注册询问.

①用户注册询问. 初始化一个列表RQ_u，用来存储用户注册信息. $\mathcal{A}$提交一个用户的身份ID_u，并发送给$\mathcal{B}$，$\mathcal{B}$选择$\boldsymbol{r}_u \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{l}_u = \boldsymbol{A}\cdot\boldsymbol{r}_u$，$\boldsymbol{R}_u = H_1(ID_u, \boldsymbol{l}_u)$，$\boldsymbol{d}_u = \boldsymbol{r}_u + \boldsymbol{R}_u\cdot\boldsymbol{x} \bmod q$，$\boldsymbol{pk}_u = \boldsymbol{A}\cdot\boldsymbol{d}_u$，$\mathcal{B}$给$\mathcal{A}$发送$(ID_u, \boldsymbol{pk}_u)$，并添加到$RQ_u$. $\mathcal{A}$可以做出多次询问.

②票据发行者注册询问. $\mathcal{B}$选择$\boldsymbol{r}_{iss} \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{l}_{iss} = \boldsymbol{r}_{iss}^{\mathrm{T}}\cdot\boldsymbol{A}$，$\boldsymbol{R}_{iss} = H_1(ID_{iss}, \boldsymbol{l}_{iss})$，$\boldsymbol{d}_{iss} = \boldsymbol{r}_{iss} + \boldsymbol{R}_{iss}\cdot\boldsymbol{x} \bmod q$与$\boldsymbol{pk}_{iss} = \boldsymbol{d}_{iss}^{\mathrm{T}}\cdot\boldsymbol{A}$，$\mathcal{B}$给$\mathcal{A}$发送$(ID_{iss}, \boldsymbol{pk}_{iss})$.

③票据验证者注册询问. $\mathcal{A}$选择一个身份ID_v发给$\mathcal{B}$，$\mathcal{B}$选择$\boldsymbol{r}_v \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{l}_v = \boldsymbol{A}\cdot\boldsymbol{r}_v$，$\boldsymbol{R}_v = H_1(ID_v, \boldsymbol{l}_v)$，$\boldsymbol{d}_v = \boldsymbol{r}_v + \boldsymbol{R}_v\cdot\boldsymbol{x} \bmod q$，$\boldsymbol{pk}_v = \boldsymbol{A}\cdot\boldsymbol{d}_v$，$\mathcal{B}$给$\mathcal{A}$发送$\boldsymbol{pk}_v$. $\mathcal{A}$可以做出多次询问.

④中心验证者注册询问. $\mathcal{A}$选择一个身份ID_{cv}发给$\mathcal{B}$，$\mathcal{B}$选择$\boldsymbol{r}_{cv} \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{l}_{cv} = \boldsymbol{A}\cdot\boldsymbol{r}_{cv}$，$\boldsymbol{R}_{cv} = H_1(ID_{cv}, \boldsymbol{l}_{cv})$，$\boldsymbol{d}_{cv} = \boldsymbol{r}_{cv} + \boldsymbol{R}_{cv}\cdot\boldsymbol{x} \bmod q$和$\boldsymbol{pk}_{cv} = \boldsymbol{A}\cdot\boldsymbol{d}_{cv}$，$\mathcal{B}$给$\mathcal{A}$发送$(ID_{cv}, \boldsymbol{pk}_{cv})$.

3)票据发行询问. $\mathcal{A}$提交一个身份$ID_u \in RQ_u$，一组服务信息J_u，假名$PS_u = \{(\boldsymbol{p}_v, \boldsymbol{q}_v) | ID_v \in J_u\}$，如果等式$\boldsymbol{A}\cdot\boldsymbol{q}_v = \boldsymbol{p}_v\cdot H_2(f, \boldsymbol{p}_v) + \boldsymbol{pk}_u$不成立，则$\mathcal{B}$中止运行；否则，$\mathcal{B}$使用4.2节中的方法产生一个票据$T_u = \{(D_v, Tag_v) | ID_v \in J_u\} \cup \{(S, \boldsymbol{c}, \boldsymbol{z})\}$，$\mathcal{B}$给$\mathcal{A}$返回$(\boldsymbol{q}_u, T_u)$. 设$QI$为$\mathcal{A}$查询的票证信息的集合，初始为空，$\mathcal{B}$向$QI$添加$(\boldsymbol{q}_u, T_u)$. $\mathcal{A}$至多进行$p(p<q)$次票据发行询问.

4)伪造阶段. $\mathcal{A}$输出一张票$T_u^* = \{(D_u^*, \boldsymbol{p}_u^*, \boldsymbol{q}_u^*, \boldsymbol{e}_1^*, e_2^*, \boldsymbol{t}^*, \boldsymbol{r}^*, \boldsymbol{z}_u^*, Text, s_v^*, \boldsymbol{c}_v^*, \boldsymbol{z}_v^*) | ID_{v^*} \in J_{u^*}\} \cup \{S^*, \boldsymbol{c}^*, \boldsymbol{z}^*\}$，且$T_u^* \notin QI$，若$\mathcal{A}$以不可忽略的优势$\varepsilon_1(\ell)$成功伪造1个票据$T_u^*$，那么$(\boldsymbol{t}^*, \boldsymbol{r}^*, \boldsymbol{z}_u^*)$满足$\boldsymbol{d}_v^{\mathrm{T}}\cdot(\boldsymbol{A}^{\mathrm{T}}\cdot\boldsymbol{z}_u^* - \boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^*)\cdot\boldsymbol{t}^* = (\boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{z}_u^* - \boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^*)\cdot\boldsymbol{t}^* \bmod q$，即$(\boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{z}_u^* - \boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^*)\cdot\boldsymbol{t}^*\cdot(\boldsymbol{t}^*)^{-1} - \boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{z}_u^* = -\boldsymbol{d}_v^{\mathrm{T}}\cdot\boldsymbol{pk}_{iss}^{\mathrm{T}}\cdot\boldsymbol{r}^* = -\boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^*$，记$W = -\boldsymbol{pk}_v^{\mathrm{T}}\cdot\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^*$，此时$\|\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^*\| \leqslant \beta$，则$\boldsymbol{d}_{iss}\cdot\boldsymbol{r}^*$是关于$\mathrm{ISIS}_{q,n,m,\beta}$的解. $\mathcal{B}$以优势$Adv_{\mathcal{B}}^{\mathrm{ISIS}_{q,n,m,\beta}} = Pr[Ticket\text{-}Validating(Input_u(\boldsymbol{sk}_{u^*}, Tag_{v^*}, Param) \leftrightarrow Input_{cv}(\boldsymbol{sk}_{v^*}, \boldsymbol{pk}_{v^*}, \boldsymbol{pk}_{u^*}, Param)) \rightarrow (\perp, (1, Tag_{v^*}))] \geqslant \frac{q-p}{q}\varepsilon_1(\ell)$解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题.

已知$\mathrm{ISIS}_{q,n,m,\beta}$是格上的一个困难问题，求解非零短向量的优势是可忽略的，$\mathcal{A}$无法以不可忽略的优势伪造认证标签，本方案具有不可伪造性.

证毕.

4.4 可追溯性证明

定理 3. 如果存在一个敌手$\mathcal{A}$以$\varepsilon(\ell)$的优势破坏方案的可追溯性，则可以构造一个算法$\mathcal{B}$，它可以将$\mathcal{A}$作为一个子程序，解决$\mathrm{ISIS}_{q,n,m,\beta}$或$\mathrm{SIS}_{q,n,m,\beta}$搜索问题.

证明. 设$\mathcal{A}$是攻击可追溯性的PPT敌手，若$\mathcal{A}$在至多进行$k(k<q)$次票据发行询问后，以$\varepsilon(\ell)$的优势伪造一个有效的用户服务票据且不被追溯，则算法$\mathcal{B}$可以以$\mathcal{A}$作为子程序，以$\frac{q-k}{2q}\varepsilon(\ell)$的优势解决$\mathrm{ISIS}_{q,n,m,\beta}$或以$\frac{\varepsilon(\ell)}{2}$的优势解决$\mathrm{SIS}_{q,n,m,\beta}$搜索问题.

系统设置和注册询问中的用户注册询问、票据发行者注册询问以及中央验证者注册询问过程和4.3节一致. 在票据验证者注册询问中，$\mathcal{A}$选择一个身份ID_v发给$\mathcal{B}$，$\mathcal{B}$和$\mathcal{A}$一起执行以下运算，选择$\boldsymbol{r}_v \xleftarrow{R} D_\sigma^m$，计算$\boldsymbol{l}_v = \boldsymbol{A}\cdot\boldsymbol{r}_v$，$\boldsymbol{R}_v = H_1(ID_v, \boldsymbol{l}_v)$，$\boldsymbol{d}_v = \boldsymbol{r}_v + \boldsymbol{R}_v\cdot\boldsymbol{x} \bmod q$，$\boldsymbol{pk}_v = \boldsymbol{A}\cdot\boldsymbol{d}_v$. $\mathcal{A}$可做出多次询问.

1)票据发行询问. $\mathcal{A}$提交一个身份$ID_u \in RQ_u$，一组服务信息J_u，假名$PS_u = \{(\boldsymbol{p}_v, \boldsymbol{q}_v) | ID_v \in J_u\}$，如果等式$\boldsymbol{A}\cdot\boldsymbol{q}_v = \boldsymbol{p}_v\cdot H_2(f, \boldsymbol{p}_v) + \boldsymbol{pk}_u$不成立，则$\mathcal{B}$中止运行；否则，$\mathcal{B}$使用4.2节中的方法产生一个票据$T_u = \{(D_v, Tag_v) | ID_v \in J_u\} \cup \{(S, \boldsymbol{c}, \boldsymbol{z})\}$，$\mathcal{B}$将$T_u$返回给$\mathcal{A}$. 设$QI$为$\mathcal{A}$查询的票证信息的集合，初始为空，$\mathcal{B}$在$QI$中添加$(\boldsymbol{q}_u, T_u)$；$\mathcal{A}$至多进行$k(k<q)$次票据发行查询.

2)伪造阶段. $\mathcal{A}$输出一张票据$T_u^* = \{(D_u^*, \boldsymbol{p}_v^*, \boldsymbol{q}_v^*, \boldsymbol{e}_1^*,$

$e_2^*, \boldsymbol{t}^*, \boldsymbol{r}^*, z_u^*, Text, s_v^*, \boldsymbol{c}_v^*, z_v^*)|ID_{v^*} \in J_{u^*}\} \cup \{S^*, \boldsymbol{c}^*, z^*\}$. 如果$T_u^*$包含了多个用户的公钥，则票据没有正确生成，$\mathcal{B}$中止运行. 如果$\mathcal{B}$未中止，则考虑2种方式：①伪造者输出了一个票据$T_u^*$，它至少包含1个新的假名$(\boldsymbol{p}_v', \boldsymbol{q}_v')$，同时$\mathcal{A}$查询过的任何票据中不包括假名$(\boldsymbol{p}_v', \boldsymbol{q}_v')$. ②伪造者输出一个票据$T_u^*$，里面含有被$\mathcal{A}$查询到的$T_u \in QI$中的假名，但是追溯该票据时，追溯到用户$u'$，此时$\mathcal{A}$并不知道用户$u'$的私钥$\boldsymbol{x}'$，令用户$u'$的私钥为$\boldsymbol{x}'$.

① 如果存在一个假名$(\boldsymbol{p}_v', \boldsymbol{q}_v') \in T_{u^*}$，$(\boldsymbol{p}_v', \boldsymbol{q}_v') \notin QI$，$Tag_v' = (\boldsymbol{p}_v', \boldsymbol{q}_v', \boldsymbol{e}_1', e_2', \boldsymbol{t}', \boldsymbol{r}', z_u', Test, s_v', \boldsymbol{c}_v', z_v')$，$\mathcal{A}$伪造一个对$s_v' = H_2(\boldsymbol{p}_v'\|\boldsymbol{q}_v'\|\boldsymbol{e}_1'\|e_2'\|\boldsymbol{t}'\|\boldsymbol{r}'\|z_u'\|Text)$的签名$(\boldsymbol{c}_v', z_v')$，因此$\mathcal{B}$可以使用4.3节中的方法去解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题.

②如果所有的$(\boldsymbol{p}_v', \boldsymbol{q}_v') \in T_{u^*}$，$(\boldsymbol{p}_v', \boldsymbol{q}_v') \in QI$. 最后票据追溯的时候，计算出$\boldsymbol{pk}_u = \boldsymbol{A} \cdot \boldsymbol{d}_u = \boldsymbol{l}_{u'} + \boldsymbol{R}_{u'} \cdot \boldsymbol{mpk} = \boldsymbol{A} \cdot \boldsymbol{d}_{u'}$，即$\boldsymbol{A}(\boldsymbol{d}_u - \boldsymbol{d}_{u'}) = \boldsymbol{0} \bmod q$. 由于$\boldsymbol{d}_u \neq \boldsymbol{d}_{u'}$，且$\|\boldsymbol{d}_u\|_\infty, \|\boldsymbol{d}_{u'}\|_\infty \leqslant \dfrac{\beta}{2}$，所以$\boldsymbol{d}_u - \boldsymbol{d}_{u'} \neq \boldsymbol{0} \bmod q$，$\boldsymbol{d}_u - \boldsymbol{d}_{u'}$是关于$\mathrm{SIS}_{q,n,m,\beta}$的解.

$\mathcal{A}$可采用①或②去破坏可追溯性，此时以$\dfrac{q-k}{2q}\varepsilon(\ell)$的优势解决$\mathrm{ISIS}_{q,n,m,\beta}$搜索问题或以$\dfrac{\varepsilon(\ell)}{2}$的优势解决$\mathrm{SIS}_{q,n,m,\beta}$搜索问题. 因此，$\mathcal{B}$的优势为$\varepsilon(\ell) = \max\left\{\dfrac{q-k}{2q}\varepsilon(\ell), \dfrac{\varepsilon(\ell)}{2}\right\}$.

已知$\mathrm{ISIS}_{q,n,m,\beta}$和$\mathrm{SIS}_{q,n,m,\beta}$在格上是个困难问题，求解非零短向量是困难的，$\mathcal{A}$无法以不可忽略的优势破坏可追溯性，故方案具有可追溯性.

证毕.

5 安全性能对比

本节对方案安全性进行分析，表1列出本文方案与文献[4,7,19]方案在匿名性、可追溯性、不可链接性、抗量子性以及各方案中票据发行算法的时间复杂度对比.

文献[4]引入带有随机数的单向散列函数来解决Hsu等人[31]方案中的假冒攻击，文献[4]方案中票据验证者可以通过使用扩展欧几里德算法，以高概率恢复出用户的认证凭证，并利用RSA签名方案和非交互零知识证明方案，实现用户的身份认证与票据的不可伪造性. 因此文献[4]方案不具备可追溯性和用户服务的不可链接性，不可以抵抗已知的量子算法攻击.

文献[7]中的方案利用切比雪夫混沌映射的半群性和交换性来隐藏用户的真实身份，但多个票据验证者串通起来时可以分析用户的服务请求，并且文献[7]方案在设计时未考虑因为欺诈行为的追溯问题[32]，其不具备匿名性、可追溯性、不可链接性，不可以抵抗已知的量子算法攻击.

文献[19]中的方案采用公钥证书技术，使中央验证者在追溯时获得用户公钥来揭示用户身份，并追溯出用户的所有访问服务，该方案实现了可追溯性与不可链接性. 该方案安全性是基于离散对数困难假设，不能抵抗已知的量子算法攻击.

本文方案中用户在请求票据时，通过为指定票据验证者生成假名来实现其匿名性，保证用户的匿名性与服务请求的不可链接性. 利用格上基于身份的密码体制来代替文献[19]中的公钥证书技术，简化了用户身份管理开销. 在追溯阶段，可信第三方通过计算出用户公钥来揭示用户身份，并追溯出整个服务请求. 同时票据发行阶段作为单点登录方案的重要一步，票据发行算法的时间复杂度大小关乎着方案的实际运行效率. 本方案的安全性基于ISIS困难假设，在参数$m = 512$ b，$q = 783361 \approx 2^{20}$($m$, q定义见1.1节)下即可达到与AES-128bit相当的安全量级. 根据NIST对称加密标准所提供的安全强度范围分类，在AES-128bit安全量级下进行对比方案参数的实例化，文献[4,7,19]中的参数分别设置为$m = 3\,200$ b(m为文献[4]中的模数)，$\kappa = 8$ b、$m = 3\,072$ b(κ为文献[7]中安全Hash函数的输出长度，m为文献[7]中的模数)和$m = 256$ b(m为文献[19]中群的阶数)[33]. 由表1可知，在所设参数下，所提方案与对比方案[4,7,19]的时间复杂度分别约为$O(2^{12.17})$,$O(2^{34.9})$,$O(2^{39.17})$,$O(2^{16})$. 可见，本方案在提供整体安全性的同时，具有较低时间复杂度.

Table 1 The Safety Performance Comparison of the Proposed Scheme and the Schemes of References [4,7,19]

表1 本文方案与文献[4,7,19]方案的安全性能对比

方案	困难问题	匿名性	可追溯性	不可链接性	抗量子性	时间复杂度
文献[4]方案	大整数分解	是	否	否	否	$O(\log^3 m)$
文献[7]方案	切比雪夫混沌映射的假设	否	否	否	否	$O(\kappa^2\log^2 m)$
文献[19]方案	离散对数	是	是	是	否	$O(\log^2 m)$
本文方案	ISIS	是	是	是	是	$O(m\log m)$

6 性能分析

6.1 抗量子安全强度分析

本文方案是基于格上困难问题构造的单点登录方案，结合格上 ISIS 困难问题求解以及未来数年中量子计算机的发展，为满足方案安全强度的要求，在表 2 中提供 3 组参数，并进一步使用格基约化算法 BKZ[34] 对本文方案进行量子安全强度测试，在这 3 组参数下，方案可分别达到 112 b, 230 b, 292 b 的安全度.

Table 2 Security Strength Under Different Parameter Settings

表 2 不同参数设置下的安全强度

参数设置	安全参数 n	维度 m	标准差 σ	模数 q	Hermit 因子	量子安全强度/b
PARMS Ⅰ	8	256	316 800	1 073 479 681	1.004 998	112
PARMS Ⅱ	8	512	316 800	1 073 479 681	1.002 707	230
PARMS Ⅲ	8	640	316 800	1 073 479 681	1.002 220	292

6.2 运算效率分析

在满足一定安全等级的情况下，将本文方案在 Windows10 系统、Intel® Core™ i5-7200U CPU @2.50 GHz 处理器和 8.00GB 运行内存下，利用 Sage 数学库，采用基于 SageMath 的 Python 进行方案实现与性能评估. 表 3 给出了本文方案在 PARMS Ⅰ, PARMS Ⅱ, PARMS Ⅲ这 3 组参数下的时间开销，所显示的时间是以 1 000 次运算的平均值统计. 下面主要分析 PARMS Ⅱ, PARMS Ⅲ参数下，即 m = 512 和 m = 640 这 2 种情况下各阶段的时间开销.

Table 3 Calculation Cost Analysis of Our Proposed Scheme

表 3 本文方案的计算开销分析 ms

阶段		PARMS Ⅰ	PARMS Ⅱ	PARMS Ⅲ
系统初始化		0.93	3.85	5.98
公私钥提取	产生票据发行者公私钥	5.93	21.62	34.08
	产生指定票据验证者公私钥	5.08	21.66	36.76
	产生中央验证者公私钥	5.52	20.88	36.69
	产生用户公私钥	5.72	20.39	33.70
用户注册		5.80	23.81	32.72
票据发行（用户进行 4 个服务请求）		27.71	74.89	108.34
票据验证		5.26	16.08	24.11
追溯		5.26	16.06	24.10

1)在实现整个匿名单点登录方案过程中，系统初始化、各参与方公私钥提取以及每个用户注册阶段只需进行 1 次操作. 在各参与者公私钥提取阶段，对于 PKG 生成的私钥，用户要通过验证等式来确保私钥是正确生成的，因此，此阶段在 m = 512 和 m = 640 时，分别需要大概 21 ms 和 36 ms.

2)当 m = 512 时，假如票据发行阶段用户一次性请求 4 个服务，整个过程大概需要 74.89 ms. 其中 7.4 ms 用来生成服务请求，48.55 ms 用来生成票据，2.57 ms 用来验证票据是否有效. 即使将 m 增加到 640，整个发行阶段也只需要 108.34 ms. 同时，用户可以预先计算它的票据请求，而且票据发行者可并行验证用户身份的合法性，从而将与票据发行者的交互时间缩短 14.78 ms(m = 512)或 22.46 ms(m = 640). 此外，发行者也可以预先计算一些值作为票据发行过程的一部分(例如$D_v, \boldsymbol{e}_1, e_2$等部分，参见图 2). 这样可将票据生成阶段减少 5.15 ms(m=512)或 6.64 ms(m = 640). 经算法优化后，整个过程大概需要 54.96 ms(m = 512)或 79.14 ms(m = 640).

3)在票据验证阶段，用户需要向指定票据验证者提交自己的认证标签以获得想要的服务. 此时，指定票据验证者需要验证指定验证者签名、单向 Hash 函数以及对认证标签与票据的签名，若全部验证通过，则授权用户访问服务，最终指定票据验证者验证单个标签，其过程只需要大约 16.08 ms 或 24.11 ms(m = 512 或 m = 640).

4)必要时，中央验证者才执行票据追溯算法. 此时中央验证者在进行简单的向量运算后，揭示用户的真实身份并追溯出用户的整个服务请求. 由于此阶段的主要运算过程与票据验证阶段相似，因此这 2 个阶段的计算开销大体相近.

6.3 存储与通信开销分析

为进一步评估方案效率，表 4 列出方案各阶段所产生的存储开销与通信开销. 系统初始化阶段与公私钥提取阶段会产生方案所需的公共参数与各参与方的公私钥，各参与方私钥作为要保密的信息，需要进行本地存储. 由表 4 可知，在给定的 3 组参数下，参与方的本地存储开销最大为 10.53KB.

用户注册阶段、票据验证阶段和票据发行阶段

Table 4 Analysis of Storage Cost and Communication Cost of Scheme

表 4 方案存储开销与通信开销分析 ms

阶段	存储开销与通信开销	PARMS Ⅰ	PARMS Ⅱ	PARMS Ⅲ
系统初始化	系统公开参数长度/KB	7.36	9.83	12.13
公私钥提取阶段	各参与方的公钥长度/KB	5.23	11.62	15.47
	各参与方的私钥长度/KB	4.61	8.22	10.53
用户注册阶段	用户通信开销/KB	9.81	19.03	23.64
票据发行阶段（用户进行 4 个服务请求	用户通信开销/KB	9.23	18.45	23.06
	票据发行者通信开销/KB	167.31	336.31	420.8
	票据大小/KB	162.7	327.09	409.28
票据验证阶段	票据验证者通信开销/B	16	18	18
	用户通信开销/KB	46.09	92.17	115.21

需要 2 个参与方进行协同交互.在用户注册阶段，用户需要传输对身份ID_u加密所产生的密文. 票据验证阶段，指定票据验证者和用户分别需要发送身份ID_v和票据标签Tag_v. 在票据发行阶段，用户给票据发行者发送一次性假名与服务请求，票据发行者再根据用户需求生成服务票据，此过程需要较大的通信开销. 在表 4 的 3 组参数下，方案各阶段的最大通信开销分别是 167.31 KB, 336.31 KB, 420.8 KB, 其中所生产的用户服务票据约占票据发行者通信开销的 97%.

7 结束语

本文基于 ISIS 困难假设，结合格上基于身份的密码体制与匿名认证技术，构造了一个可追溯的匿名单点登录方案，解决了同类方案中公钥证书管理问题以及因用户匿名访问服务而无法追责的问题. 根据方案在不同参数设置下的量子安全强度可知，其具备抗量子算法攻击的特点，同时在运行时间和通信开销上满足应用实施的需求. 当指定票据验证者发生单点故障时，考虑在票据发行阶段引入代理重加密技术，在不改变用户服务票据情况下，将用户重定向到代理票据验证者并继续访问服务，是未来的一个研究方向.

作者贡献声明：汤永利负责方案构造与证明、数据整理与实验分析；李英负责方案构造与证明，完成论文撰写与修改；赵宗渠负责方案构造与证明；李星宇负责数据整理与实验分析；王瀚博负责论文撰写与修改.

参 考 文 献

[1] Wu T S, Hsu C L. Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks[J]. Computers and Security, 2004, 23(2): 120−125

[2] Mangipudi K, Katti R. A secure identification and key agreement protocol with user anonymity[J]. Computers and Security, 2006, 25(6): 420−425

[3] Chang C C, Lee C Y. A secure single sign-on mechanism for distributed computer networks[J]. IEEE Transactions on Industrial Electronics, 2012, 59(1): 629−637

[4] Wang Guilin, Yu Jiangshan, Xie Qi. Security analysis of a single sign-on mechanism for distributed computer networks[J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 294−302

[5] Wen C K, Shih P W, Huang Y C, et al. An anonymous and authentication protocol for multi-server[J]. Information Technology and Control, 2017, 46(2): 235−245

[6] Gope P, Das A K. Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services[J]. IEEE Internet of Things Journal, 2017, 4(5): 1764−1772

[7] Lee T F. Provably secure anonymous single-sign-on authentication mechanisms using extended Chebyshev chaotic maps for distributed computer networks[J]. IEEE Systems Journal, 2018, 12(2): 1499−1505

[8] Jegadeesan S, Azees M, Kumar P M, et al. An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications[J]. Sustainable Cities and Society, 2019, 49: 101522−101528

[9] Jia Xiaoying, He Debiao, Kumar N, et al. A provably secure and efficient identity-based anonymous authentication scheme for mobile edge computing[J]. IEEE Systems Journal, 2019, 14(1): 560−571

[10] Elmufti K, Weerasinghe D, Rajarajan M, et al. Anonymous authentication for mobile single sign-on to protect user privacy[J]. International Journal of Mobile Communications, 2008, 6(6): 760−769

[11] Mahor V K, Padmavathi R, Chatterjee S, et al. A secure three factor-based fully anonymous user authentication protocol for multi-server

environment[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2020, 34(1): 45−60

[12] Kim H J, Lee I Y. A study on a secure single sign-on for user authentication information privacy in distributed computing environment[J]. International Journal of Communication Networks and Distributed Systems, 2017, 19(1): 28−45

[13] He Debiao, Zeadally S, Kumar N, et al. Efficient and anonymous mobile user authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(9): 2052−2064

[14] Han Jinguang, Chen Liqun, Schneider S, et al. Anonymous single-sign-on for n designated services with traceability[G] //LNCS 11098: Proc of the 23rd European Symp on Research in Computer Security. Cham, Switzerland: Springer, 2018: 470−490

[15] He Lei, Ma Jianfeng, Shen Limin, et al. Certificateless designated verifier proxy signature scheme for unmanned aerial vehicle networks[J]. Science China Information Sciences, 2021, 64(1): 1−15

[16] Yang Xiaodong, Chen Guilan, Li Ting, et al. Strong designated verifier signature scheme with undeniability and strong unforgeability in the standard model[J]. Applied Sciences, 2019, 9(10): 2062−2080

[17] Han Shu, Xie Mande, Yang Bailin, et al. A certificateless verifiable strong designated verifier signature scheme[J]. IEEE Access, 2019, 7: 126391−126408

[18] Chen Jing, Chen Jiong, He Kun, et al. SeCrowd: Efficient secure interactive crowdsourcing via permission-based signatures[J]. Future Generation Computer Systems, 2021, 115(6): 448−458

[19] Han Jinguang, Chen Liqun, Schneider S, et al. Anonymous single-sign-on with proxy re-verification[J]. IEEE Transactions on Information Forensics and Security, 2020, 15(1): 223−236

[20] Zhang Zhiyi, Król M, Sonnino A, et al. EL PASSO: Efficient and lightweight privacy-preserving single sign on[J]. Proceedings on Privacy Enhancing Technologies, 2021, 2021(2): 70−87

[21] Pointcheval D, Sanders O. Reassessing security of randomizable signatures[G] //LNCS 10808: Proc of Cryptographers'Track at the RSA Conf. Cham, Switzerland: Springer, 2018: 319−338

[22] Shor P W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Review, 1999, 41(2): 303−332

[23] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings[G] //LNCS 6110: Proc of the 29th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2010: 1−23

[24] Cai Jie, Jiang Han, Zhang Pingyuan, et al. ID-based strong designated verifier signature over R-SIS assumption[J]. Security and Communication Networks, 2019, 2019: 1−8

[25] Wang Qingxuan, Wang Ding, Cheng Chi, et al. Quantum2FA: Efficient quantum-resistant two-factor authentication scheme for mobile devices[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 99: 1−16

[26] Li Zengpeng, Wang Ding, Morais E. Quantum-safe round-optimal password authentication for mobile devices[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 19(3): 1885−1899

[27] Liu Hui, Sun Yining, Xu Yan, et al. A secure lattice-based anonymous authentication scheme for VANETs[J]. Journal of the Chinese Institute of Engineers, 2019, 42(1): 66−73

[28] Libert B, Ling San, Nguyen K, et al. Zero-knowledge arguments for lattice-based accumulators: Logarithmic-size ring signatures and group signatures without trapdoors[G] //LNCS 9666: Proc of the 35th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2016: 1−31

[29] Wang Ding, Wang Ping. Two birds with one stone: Two-factor authentication with security beyond conventional bound[J]. IEEE Transactions on Dependable and Secure Computing, 2016, 15(4): 708−722

[30] Qiu Shuming, Wang Ding, Xu Guoai, et al. Practical and provably secure three-factor authentication protocol based on extended chaotic-maps for mobile lightweight devices[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 19(2): 1338−1351

[31] Hsu C L, Chuang Y H. A novel user identification scheme with key distribution preserving user anonymity for distributed computer networks[J]. Information Sciences, 2009, 179(4): 422−429

[32] Hou Wanyu, Sun Yu, Li Dawei, et al. Anonymous authentication and key agreement protocol for 5G-V2V based on PUF[J]. Journal of Computer Research and Development, 2021, 58(10): 2265−2277 (in Chinese)
(侯琬钰, 孙钰, 李大伟, 等. 基于PUF的5G车联网V2V匿名认证与密钥协商协议[J]. 计算机研究与发展, 2021, 58(10): 2265−2277)

[33] Lenstra A K. Unbelievable security matching AES security using public key systems[G] //LNCS 2248: Proc of the 7th Int Conf on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2001: 67−86

[34] Schnorr C P, Euchner M. Lattice basis reduction: Improved practical algorithms and solving subset sum problems[J]. Mathematical Programming, 1994, 66(1): 181−199

Tang Yongli, born in 1972. PhD, professor. Senior member of CCF. His main research interests include information security, computer network, and cryptography.

汤永利, 1972 年生. 博士, 教授. CCF 高级会员. 主要研究方向为信息安全、计算机网络和密码学.

Li Ying, born in 1998. Master candidate. Her main research interests include information security and cryptography.

李　英, 1998 年生. 硕士研究生. 主要研究方向为信息安全和密码学.

Zhao Zongqu, born in 1974. PhD, lecturer. His main research interests include information security, cryptography, and malicious code analysis.

赵宗渠, 1974 年生. 博士, 讲师. 主要研究方向为信息安全、密码学和恶意代码分析.

Li Xingyu, born in 1998. Master candidate. His main research interests include information security and malicious code analysis.

李星宇, 1998年生. 硕士研究生. 主要研究方向为信息安全与恶意代码分析.

Wang Hanbo, born in 1997. Master candidate. His main research interests include information security and cryptography.

王瀚博, 1997年生. 硕士研究生. 主要研究方向为信息安全和密码学.