

# 零信任与零知识融合的匿名身份认证

路直<sup>1)</sup> 沈任飞<sup>1)</sup> 聂何望<sup>1),3)</sup> 骆婷<sup>1)</sup> 路松峰<sup>1),2)</sup>

<sup>1)</sup>(华中科技大学网络空间安全学院 武汉 430074)

<sup>2)</sup>(深圳华中科技大学研究院 广东 深圳 518052)

<sup>3)</sup>(广西师范大学计算机科学与工程学院/软件学院/人工智能学院 广西 桂林 541004)

**摘要** 在零信任安全架构中,身份认证必须遵循“持续验证”的原则,即每一次访问请求均需独立完成身份验证,并通常结合多因素认证以增强安全性。然而,传统的多因素认证模式要求认证方频繁暴露敏感身份信息,如身份证号和生物特征,不仅增加了隐私泄露的风险,也为关联攻击提供了条件。为解决这一问题,本文提出一种融合零知识证明与零信任架构的匿名身份认证协议,创新性地引入“认证方与验证方互不信任”的安全模型:验证方不信任认证方,要求其证明身份的有效性;认证方亦不信任验证方,拒绝以明文方式泄露身份,仅通过密文零知识证明完成认证。本文针对身份证号与面部特征两个常见身份因子,分别构造满足 Sigma 协议结构的专用零知识证明过程,并通过密钥动态更新机制实现每轮匿名凭证的独立性,从而在保障认证完整性的同时,提供跨轮次不可关联性,防止身份溯源与隐私泄露。理论分析与实验结果表明,该协议在计算与通信成本方面具备良好的可扩展性。尤其在面向高维面部特征的认证任务中,本文设计的结构化零知识协议大幅提升了认证效率。与采用通用零知识框架的面部特征方法相比,本文方案在向量维度为 1000,密钥参数为 2048 位的典型配置下,将证明生成与验证时间分别从数十秒与百秒级降至毫秒级,通信成本从百兆字节级压缩至小于 0.5 MB,分别降低约 98%与 99.75%,大幅增强了协议在真实系统中的可部署性。本协议的完整认证过程延迟控制在 500 ms 以内,通信开销小于 0.5 MB,能够广泛适用于面向高频认证与隐私保护要求较高的零信任场景,特别是基于生物特征识别的身份认证系统中。

**关键词** 零信任; 零知识证明; 身份认证; 匿名凭证; 隐私计算

中图分类号 TP309 DOI号 10.11897/SP.J.1016.2026.00661

## Anonymous Authentication Through the Fusion of Zero Trust and Zero Knowledge

LU Zhi<sup>1)</sup> SHEN Ren-Fei<sup>1)</sup> NIE He-Wang<sup>1),3)</sup> LUO Ting<sup>1)</sup> LU Song-Feng<sup>1),2)</sup>

<sup>1)</sup>(School of Cyber Science and Engineering, Huazhong University of Science and Technology, Wuhan 430074)

<sup>2)</sup>(Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen, Guangdong 518052)

<sup>3)</sup>(School of Computer Science and Engineering/School of Software/School of Artificial Intelligence, Guangxi Normal University, Guilin, Guangxi 541004)

**Abstract** Identity authentication is foundational to ensuring that only legitimately authorized users or devices can access protected resources. As cloud, IoT, and edge computing blur traditional perimeters and enlarge the attack surface, static username-password schemes fail to satisfy modern security

收稿日期: 2025-05-23; 在线发布日期: 2025-11-05。本课题得到2023年湖北省重大研究计划(2023BAA027)、2023年度长沙市揭榜挂帅重大科技项目(kq2503009)、深圳市科技计划国际合作研究项目(GJHZ20240218114659027)、湖北省重点研发计划项目(2024BAB049)、中央高校基本科研业务费专项资金(YCJJ20252331,YCJJ20252336)资助。路直, 博士研究生, 中国计算机学会(CCF)学生会员, 主要研究领域为密码学、零知识证明、匿名凭证、工业互联网安全。E-mail: luzhizz@foxmail.com。沈任飞, 博士研究生, 主要研究领域为应用密码学和分布式系统安全。聂何望, 博士, 副教授, 主要研究领域为人工智能安全领域。骆婷, 博士, 讲师, 中国计算机学会(CCF)会员, 主要研究领域为应用密码学。E-mail: luoting@hust.edu.cn。路松峰(通信作者), 博士, 教授, 主要研究领域为网络安全、人工智能安全、工业互联网安全。E-mail: lusongfeng@hust.edu.cn。

requirements: they lack dynamic behavioral assessment and remain vulnerable to phishing, man-in-the-middle attacks, and credential reuse. Zero-trust architectures respond by enforcing “never trust, always verify,” re-evaluating identity and authorization at each request. In practice, zero trust is frequently paired with multi-factor authentication (MFA), which raises assurance by combining heterogeneous factors such as passwords, biometrics, digital certificates, or device identifiers. However, this combination introduces two persistent challenges. First, MFA compels frequent disclosure of highly sensitive attributes—e.g., national ID numbers and biometric features—to verifiers that may be partially trusted, creating significant privacy risks. Second, continuous verification generates high-frequency authentication events which, if linkable across sessions or services, enable correlation attacks, user profiling, replay, and timing analysis. This paper proposes an anonymous, cross-round unlinkable MFA protocol that integrates zero-knowledge proofs (ZKPs) into the zero-trust setting while explicitly modeling mutual distrust: not only does the verifier refuse to accept unsubstantiated claims, but the prover also refuses to disclose plaintext attributes. Instead, the prover completes authentication via cryptographically protected, non-interactive ZK proofs over committed or encrypted values. This bilateral stance aligns with privacy regulations and user expectations while preserving the operational goals of zero trust. We design two dedicated, well-structured Sigma-protocol instantiations (made non-interactive via Fiat-Shamir) for two common identity factors. For national ID numbers, we extend the Schnorr protocol with a per-round secret-key update mechanism that derives a fresh public key in each session. The resulting public keys are unlinkable across rounds, achieving cross-session anonymity while attesting format validity, registry membership, and non-revocation without revealing the identifier. For facial features, we introduce a zero-knowledge construction for cosine-similarity matching: by committing to auxiliary variables and mapping vector similarity to a structured constraint system, the prover demonstrates that an encrypted high-dimensional feature vector lies within a specified threshold of an enrolled template, without disclosing either the vector or the threshold. Because similarity is expressed as constraints over committed vectors, the approach naturally generalizes to other biometrics that admit vectorization and fuzzy matching. Our protocol unifies anonymity, validity, and unlinkability, while avoiding the circuit-conversion burden and heavy cryptography typical of general-purpose ZKP frameworks. Under 2048-bit parameters, the national-ID factor achieves sub-0.1 ms computational latency with communication below 512 bytes per round. For facial authentication with 1000-dimensional vectors, the structured proofs dramatically improve efficiency relative to general-purpose ZK approaches: proof generation is reduced from over 30 seconds to milliseconds, verification from over 100 seconds to milliseconds, and communication from over 100 MB to under 0.5 MB—corresponding to approximately 98% savings in computation and 99.75% savings in bandwidth. These results indicate strong scalability for high-frequency authentication in zero-trust deployments, including resource-constrained devices and high-concurrency settings. By embedding non-interactive, factor-specific ZK proofs within a mutual-distrust model, the proposed protocol reconciles continuous verification with stringent privacy protection. It enables practical, cross-round unlinkable MFA without exposing national IDs or biometric templates, thereby reducing correlation risk and enhancing deployability in privacy-sensitive zero-trust systems.

**Key words** zero trust; zero-knowledge proof; anonymous authentication; anonymous credentials; privacy computing

# 1 引言

在信息安全和网络安全体系中，身份认证始终处于关键地位，其核心目标是确保仅有具备合法权限的用户或设备能够访问受保护的资源<sup>[1]</sup>。随着云计算、物联网与边缘计算的普及，网络边界逐渐模糊，攻击面显著扩大，传统基于用户名与密码的身份验证模式已难以满足现代系统对安全性的要求。此类模式不仅缺乏对用户行为的动态识别能力，也易受到钓鱼攻击、中间人攻击及凭据重用等安全威胁。

为适应复杂化的威胁模型，零信任架构逐步成为现代网络安全体系的重要支撑方向。该架构以“永不信任，持续验证”为基本原则<sup>[2]</sup>，主张在每一次请求发生时均重新评估主体身份与权限。这种理念已被广泛采纳于政府、工业、金融等关键行业的系统安全设计中。

为进一步增强认证的强度，零信任架构常与因素认证机制协同部署。多因素认证通常要求认证方提供两种或以上不同类型的身份要素(如密码、生物特征、数字证书或设备标识)，以降低单一认证因子被攻击所带来的风险。尽管该方式可有效提升安全性，但也随之引入了两项重大挑战：

(1) 多因素认证暴露了更多个人隐私信息：认证方需频繁提交如身份证号、指纹、面部特征等高敏感度数据，若验证方不受信或传输过程存在泄露风险，将严重侵犯用户隐私<sup>[3]</sup>。

(2) 持续验证导致高频率认证请求，从而产生身份关联性问题：在零信任环境中，认证行为不再是单点触发，而是贯穿整个访问周期。若验证过程中身份凭证或交互过程具有关联性，攻击者即可通过请求之间的链接特征进行用户画像，甚至完成重放攻击、时序分析等隐私威胁。

随着网络安全法和隐私法规日益完善，人民群众对个人隐私也变得更加重视，使得认证方不希望泄露过多的个人隐私，尤其是在使用生物特征数据时。因此，如何在保护隐私的前提下完成频繁的多因素认证，成为零信任架构下身份认证系统面临的重要问题。

一个直接的解决方案是利用通用零知识证明(Zero Knowledge Proof, ZKP)框架来实现隐私保护的多因素认证<sup>[4]</sup>。零知识证明允许认证方在不泄露任何身份明文的前提下，向验证方证明其满足某种

认证条件。Groth16<sup>[5]</sup>、Bulletproofs<sup>[6]</sup>、SNIP<sup>[7]</sup>等通用ZKP构造，能够表达任意可计算的陈述，理论上适用于复杂的身份认证约束。然而，通用ZKP方案在实际部署中面临较大挑战。一方面，其构造复杂，需将认证逻辑转换为约束系统或算术电路，实施门槛高、维护成本大；另一方面，其生成和验证证明的时间复杂度较高，不适用于高频、低延迟的认证场景。特别是在需要面向资源受限设备或高并发访问的系统中，效率瓶颈更加突出。

为应对上述问题，本文提出一种面向零信任架构、融合零知识证明机制的跨轮次不可关联的匿名多因素身份认证协议。所谓“跨轮次”，是指认证过程中用户可能在多个不同时间点、会话或系统交互中多次发起认证请求。本协议首次系统引入“认证方与验证方互不信任”的安全模型——在验证方不信任认证方的基础上，进一步考虑认证方对验证方的不信任。认证方不再明文传输身份要素，而是通过密文化的、非交互式的零知识方式完成身份合法性验证，确保认证过程在隐私感知、安全性与效率之间实现动态平衡。

针对身份证号与面部识别两类常见身份因子，本文分别构建了两类专用、结构良好的Sigma协议<sup>[8]</sup>实例化零知识证明协议：对于身份证号验证，本文在Schnorr协议<sup>[9]</sup>的基础上引入私钥更新机制，使得每轮认证生成独立的公钥，公钥不可被链接，从而实现跨轮次匿名性；对于面部特征认证，本文首次提出一种将余弦相似度计算零知识化的方案，通过构造可验证的辅助变量承诺结构，将向量相似性映射为结构良好的约束系统，从而在不暴露原始面部向量的前提下完成生物特征匹配的认证过程。除了面部识别，其他常见的生物因子如声纹、指纹等，也同样可以通过向量化建模并采用模糊匹配机制进行身份验证。因此，本文提出的基于余弦相似度的零知识认证方案具有一定的通用性，适用于多种生物特征的认证场景。本文的主要贡献如下：

(1) 提出互不信任模型的认证架构扩展。在“验证方不信任认证方”的零信任架构基础上，进一步提出“认证方不信任验证方”的隐私增强模型，通过密文化身份证明实现双向不信任条件下的安全认证交互。

(2) 构建两类针对性强的高效零知识协议。分别针对身份证号和面部识别因子，设计结构良好的Sigma协议实例，实现认证过程中数据的匿名性、

合法性与不可链接性统一，特别是面部识别零知识化方案为领域首创。

(3) 显著优化认证系统的效率与可部署性。相较于通用零知识证明方法，本文方案避免了电路转换与高阶加密运算的复杂性。在 2048 位下实现跨轮次不可关联的匿名凭证机制时，身份证号认证的计算延迟可控制 0.1 ms 以内，通信开销小于 512 字节；与采用通用 ZKP 架构(如 SNIP)的面部特征认证方法相比，本文方案在向量维度为 1000 的典型场景下，将证明生成与验证时间分别从超过 30 s 和 100 s 降至毫秒级，将通信成本从超过 100 MB 降至 0.5 MB 以下，在计算和通信开销上分别减少约 98% 和 99.75%。整体方案具备良好的效率表现与实际部署可行性。

## 2 相关工作

身份认证作为网络安全的第一道防线，其核心目标是在开放网络环境中确保访问主体的真实性和合法性。近年来，传统身份认证技术逐步向智能化、去中心化方向演进。传统方法主要包括基于密码的认证、多因素认证(MFA)和生物特征识别。其中，多因素认证通过结合“所知”(密码)、“所有”(硬件令牌)和“所是”(生物特征)提升安全性，但存在用户体验复杂、硬件依赖性强等问题<sup>[10]</sup>。FIDO 联盟提出的无密码认证标准(如 WebAuthn)通过生物特征与本地设备绑定的方式显著简化了认证流程，已在谷歌、微软等平台部署<sup>[11]</sup>。生物识别技术(如指纹、虹膜)虽具有唯一性，但面临数据泄露风险高、跨平台兼容性不足的挑战<sup>[12]</sup>。近期研究开始探索行为生物特征(如击键动力学、步态识别)的持续认证模式，通过机器学习动态验证用户身份<sup>[13]</sup>。

去中心化身份(DID)技术通过区块链实现用户自主控制身份数据，有效规避中心化存储的单个故障风险。W3C 提出的 Verifiable Credentials 标准已在跨境数字身份框架中成功应用，实现了数据主权与隐私保护的协同<sup>[14]</sup>。在跨链互操作性方面，Polkadot 的 Substrate 框架通过中继链技术实现了异构区块链间的身份凭证传递，为多链生态身份管理提供了新范式<sup>[15]</sup>。此外，量子计算的发展对现有 DID 加密体系构成威胁，基于格密码学的抗量子 DID 方案开始受到关注<sup>[16]</sup>。

零知识证明(ZKP)技术通过“证明而不泄露”的特性，为隐私保护型身份认证提供了创新路径。

交互式零知识证明(如 Zcash 采用的 zk-SNARKs)和非交互式版本分别在加密货币交易<sup>[15]</sup>和分布式身份认证<sup>[17]</sup>中展现出独特优势。在医疗领域，基于 ZKP 的联邦学习框架允许医院共享疾病预测模型的同时保护患者隐私<sup>[18]</sup>。值得注意的是，后量子零知识证明协议(如基于哈希的 STARKs)的研究正在加速，以应对量子计算机的潜在威胁<sup>[19]</sup>。袁琪等人<sup>[20]</sup>结合 CP-ABE 与 Schnorr 协议<sup>[9]</sup>设计了医疗身份认证方案；张杨等人<sup>[21]</sup>构建了区块链与 ZK-SNARK 融合的认证机制；麻付强等人<sup>[22]</sup>开发了基于秘密共享的多实体联合认证算法。在物联网场景，轻量级 ZKP 协议使资源受限设备也能实现隐私认证<sup>[23]</sup>。Falic 在 FPGA 硬件上利用多标量乘法加速 zk-STARK 使得吞吐加速 1.62 以及 8.5 倍的能量节省<sup>[24]</sup>。

系统架构层面，SS-DID 框架通过多层分片区块链技术实现了跨链身份的可验证性<sup>[25]</sup>。uPort 系统已在医疗数据共享场景验证了属性证明的可行性<sup>[26]</sup>。欧盟的 eIDAS 2.0 规范引入基于 DID 的数字钱包，支持 GDPR 合规的跨境身份验证<sup>[27]</sup>。在性能优化方面，基于 GPU 集群的并行化证明生成方案将 zk-SNARKs 效率提升 76%<sup>[28]</sup>，而 PlonkUP 协议通过多项式承诺技术进一步降低证明体积<sup>[29]</sup>。AI 驱动的动态认证开始兴起，通过强化学习实时调整认证策略，在金融反欺诈场景取得显著效果<sup>[30]</sup>。

我们主要对比了两种方案。首先，Schnorr 协议<sup>[9]</sup>是一种经典的零知识证明协议，广泛应用于证明离散对数关系。由于其简洁性和高效性，它常被用作构建更复杂协议的基础。在我们的对比实验中，Schnorr 协议用于实现基础的身份验证型证明。其次，Amrita 等人<sup>[31]</sup>在安全顶级会议 CCS 上利用了基于秘密共享的非交互式零知识证明(SNIP)<sup>[7]</sup>的方法。虽然 SNIP 能较灵活地支持多项式形式的计算验证，但在实现余弦相似度这一涉及浮点/高维运算的函数时，其开销显著上升。主要原因在于：余弦相似度的近似建模导致电路复杂度大；SNIP 使用秘密共享模拟计算，通信开销较高；证明不具备压缩性，导致在高维输入或多轮验证场景下开销累积严重。因此，其在实际匿名认证场景中的适用性受到一定限制。

## 3 预备知识

我们设黑体  $\mathbf{x}$  为  $\ell$  维度的向量，白体  $x$  为标量。

$\mathbb{N}$  表示正整数数域,  $\mathbb{N}_t$  表示模数为  $t$  的正整数数域。 $\mathbb{N}_t$  是明文域, 密文域  $\mathbb{N}_p$ , 其中  $p$  是一个大素数, 且  $p \gg t$ 。对于明文域的标量而言, 其共占  $\log_2 t$  比特, 密文域标量则为  $\log_2 p$  比特, 后文省略其为  $\log t$  或  $\log p$ 。

### 3.1 身份认证

身份认证是信息安全中的基础机制, 用于验证用户或设备的身份。其主要目的是确保系统只允许经过认证的用户或设备访问受保护的资源。传统的身份认证方式通常依赖于用户名和密码的组合, 因此, 现代身份认证方法逐渐采用更加安全的技术, 如多因素认证、生物识别技术以及公钥基础设施等。但仍存在密码泄露、社会工程攻击、权限滥用和用户隐私泄露等问题, 用户提供的因素越多, 隐私泄露越严重。

### 3.2 零信任架构

零信任架构(Zero Trust Architecture, ZTA)是一种现代网络安全模型, 其核心原则是“永不信任, 总是验证”。与传统的“边界防护”模式不同, 零信任架构假设所有设备、用户和网络请求随时都可能受到攻击, 因此每一次的访问请求都必须经过严格的验证。其核心思想是“验证即授权”, 即不论请求来源是否处于企业的内部网络, 所有访问都必须进行持续的身份验证、授权和监控。在零信任架构中, 验证方不信任认证方。因此, 所有请求都必须经过严格的验证才能被允许访问。

### 3.3 零知识证明

零知识证明(Zero Knowledge Proof, ZKP)<sup>[32]</sup>是一种密码学协议, 允许认证方  $P$  向验证方  $V$  证明某个命题  $S$  是正确的, 而无需透露除命题正确性之外的任何信息。零知识证明基于“认证方不信任验证方”的概念。在这一过程中, 认证方通过零知识协议向验证方证明自己的身份或特定属性, 但并不向验证方透露任何具体的个人信息或凭证。通过这种方式, 认证方能够向验证方证明自己具备某种属性或符合某个标准, 同时确保隐私不被泄露。概念如下:

(1) 命题  $S$  是需要被证明的某个陈述或断言, 通常表示为某种数学或逻辑形式。

(2) 实例  $x$  是命题  $S$  的一个具体表现或具体化的输入。它是一个可以验证命题是否成立的具体数据。

(3) 证明材料  $w$  是认证方在证明过程中使用的私密信息。

验证方  $V$  通过随机选择挑战, 迫使认证方  $P$  给出证明材料的有效响应, 而不暴露额外信息。交互记录  $T$  是验证方与认证方  $P$  之间交换的所有信息的集合。它记录了所有的挑战和响应。验证方  $V$  根据交互记录  $T$  来判断命题是否成立。协议需要满足 3 项安全属性:

(1) 完整性(Completeness): 如果命题  $S(x)$  为真, 诚实的认证方  $P$  能够在多次交互后使验证方  $V$  相信命题成立。

(2) 健全性(Soundness): 如果命题  $S(x)$  为假, 任何不诚实的认证方  $P$  都无法使验证方  $V$  相信命题成立。

(3) 零知识性(Zero-Knowledge): 验证方只能获得有关命题正确性的信息, 而无法从交互记录  $T$  中获得任何其他额外信息。

### 3.4 承诺

在密码学中, 承诺方案<sup>[33]</sup>用于认证方能够先固定某个秘密值(称为“承诺”), 之后在适当的时候揭示该值。承诺需同时满足以下两个核心安全性质:

(1) 隐藏性: 隐藏性要求承诺值不会泄露关于原始消息的信息。数学上来说, 承诺值  $\text{Com}(m)$  在计算上应该是不可区分的其中  $m$  是消息。对于任意两个不同的消息  $m_0, m_1$ , 它们的承诺值  $\text{Com}(m_0)$  和  $\text{Com}(m_1)$  应该不可区分。

(2) 绑定性: 绑定性要求认证方承诺了一个值之后不能改变它。这确保了认证方在提交承诺后无法作弊, 更改原本承诺的消息。数学上, 绑定性意味着对于一个有效的承诺值, 攻击者不能找到两个不同的消息和随机数对  $(m) \neq (m')$ , 使得  $\text{Com}(m) = \text{Com}(m')$  碰撞的概率是可忽略的。

本文中, 我们采用离散对数问题构建承诺, 与 Schnorr 协议<sup>[9]</sup>一致。设定一个大素数  $p$  和其生成元  $g$ 。假设承诺消息为  $m$ , 属于明文域  $\mathbb{N}_t$ 。承诺值为  $\text{Com}(m) = g^m \bmod p$ , 属于密文域  $\mathbb{N}_p$ 。该承诺是加法同态, 例如, 给定  $\text{Com}(m_1) = g^{m_1}, \text{Com}(m_2) = g^{m_2}$ , 则  $\text{Com}(m_1)\text{Com}(m_2) = \text{Com}(m_1 + m_2)$ 。

### 3.5 Sigma 协议

Sigma 协议是一类零知识证明协议的抽象模型<sup>[8]</sup>, 主要用于证明某些命题的正确性而无需透露除命题是否成立之外的任何信息。其安全属性与零知识证明基本相同, 不同点是其需要满足特殊健全性(Special Soundness)。条件是: 如果验证方收到两个不同的响应  $s_1$  和  $s_2$ , 并且这两个响应对应于相同

的承诺和不同的挑战值  $d_1$  和  $d_2$ ，那么可以推导出认证方的证明材料  $w$ 。Sigma 协议主要包括以下三个步骤：

(1) 承诺：认证方通过向验证方发送一个初步的承诺值来启动证明过程。在这一阶段，认证方通常会选择一个随机值(盲化因子)，以确保承诺过程中的不可预测性。承诺值的生成方式应符合隐藏性和绑定性属性。

(2) 挑战：验证方在接收到承诺值后，会向认证方发送一个随机生成的挑战值。此步骤可以通过 Fiat-Shamir<sup>[34]</sup>变换将交互式证明转换为无交互式证明。

(3) 响应：认证方根据挑战和承诺值生成响应，并将其返回给验证方。响应的正确性取决于认证方是否知道某个秘密信息，而这个秘密信息正是认证方在承诺阶段所承诺的内容。

### 3.6 安全需求

在传统的零信任架构中，重点通常是验证方对认证方的“不信任”，并要求认证方持续向验证方披露多种敏感身份信息。基于这一框架，本研究进一步拓展了安全性要求，提出认证方同样不信任验证方。以下是认证方在这一新架构下所需满足的主要安全需求：

(1) 跨轮次匿名性：任何验证方或认证方都无法区分两个诚实认证方的认证记录，也无法将认证记录与认证方端的注册或身份信息相关联，如身份证号与面部信息。

(2) 认证完整性：确保认证过程中的所有交互信息在传输过程中未被篡改，保证验证的健全性和准确性。

(3) 抗重放攻击：防止攻击者截获并重放合法认证请求，以冒充认证方进行恶意操作。

(4) 抗中间人攻击：确保认证过程中所有信息的传输不被第三方篡改或拦截，防止中间人插入篡改认证数据。

(5) 防身份盗用：确保认证方的身份信息不被盗用，避免恶意用户冒充合法认证方进行身份欺诈。

## 4 方 案

目标是在零信任身份认证系统中，结合零知识证明协议，保护用户的隐私。系统组成如下：

(1) 签发机构：签发机构为认证方颁发数字证书或加密凭证。此处，身份证号和面部信息被作为

认证信息，签发机构可以是公安等权威机构。

(2) 认证方：认证方是需要验证其身份或属性的实体。认证方提供其身份的零知识化多因素认证证明，向验证方证明其身份的真实性。

(3) 验证方：验证方是认证方所需访问的对象，它负责验证访问请求的合法性，并根据身份提供相应的服务。零信任架构要求验证方对每个访问请求进行持续验证。验证方通过零知识证明协议验证认证方的身份。

系统的零知识化多因素身份认证流程如图 1 所示。每个认证方  $P_i$  首先需要向身份签发机构注册，获得个人唯一的身份证号  $i$ ，并登记个人面部识别信息  $f_i$ 。签发机构与认证方利用这些个人隐私信息，采用 Schnorr 算法生成公私钥，以及签名  $\sigma_i^{(id)}, \sigma_i^{(f)}$ ，其中签发机构将公钥公开。当认证方  $P_i$  需要向某服务商或机构  $V$  发起访问时，首先需要进行身份验证。匿名身份验证过程中所发送的匿名凭证包括身份  $i$  和面部信息  $f_i$ 。认证方首先生成对应的承诺和盲化因子，并附带签名发送给验证方。验证方随机生成挑战并发送给认证方，认证方根据挑战生成相应响应并返回给验证方。验证方验证响应，如果与挑战、承诺和签名一致，则验证通过。

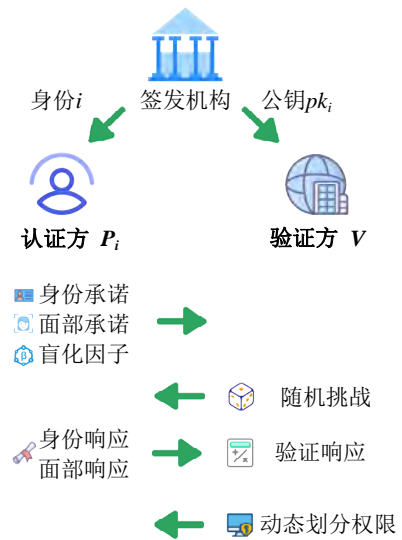


图 1 零知识化多因素身份认证流程

本工作选取身份证号与面部信息作为认证示例，旨在覆盖两类典型的匿名身份验证机制：基于精确匹配的验证(如身份证号)与基于模糊匹配的验证(如面部信息)。前者验证逻辑简洁，后者则需处理数据不确定性，验证相对复杂。二者结合有助于全面展示零知识证明在多样化身份认证场景中

的适用性, 为相关研究提供方法论与实验支持。前者适用于政务服务、医疗咨询或匿名投票、举报等场景, 后者则契合在零信任环境下的门禁控制、远程考勤与自动身份识别等应用需求。

#### 4.1 跨轮次不可关联的匿名身份验证

为了防止攻击者盗用或滥用身份信息, 每个认证方都有一个唯一标识的身份证号  $i$ , 并且该身份信息在签发机构(如公安机关)处进行了登记。匿名身份认证协议如图 2 所示。该协议可以视为 Schnorr 协议的变种, 是 Sigma 协议的一种实现。

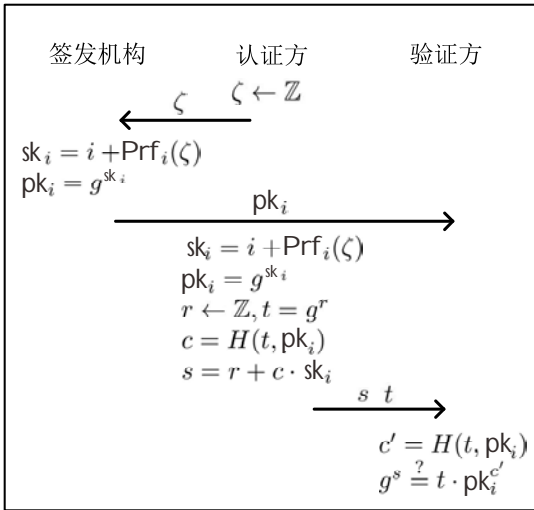


图 2 协议 1-跨轮次不可关联的匿名身份验证

在此协议中, 签发机构知道认证方的真实身份证号  $i$ 。协议分为三个主要阶段:

(1) 密钥生成: 若认证方  $P_i$  多次向同一验证方提交身份认证请求, 且公钥未发生变化, 验证方便能轻易地将多次认证请求关联, 从而泄露身份信息。为避免此类情况, 每次认证方向验证方证明身份时, 都需生成一个随机数  $\zeta$ , 私钥设置为  $sk_i = i + \text{Prf}_i(\zeta)$ 。其中  $\text{Prf}_i$  是属于认证方  $i$  的伪随机函数。随后, 签发机构设置公钥  $pk_i = g^{sk_i}$ , 并将其发送给验证方  $V$ 。

(2) 签名过程: 认证方将身份证号  $i$  编码为私钥  $sk_i = i + \text{Prf}_i(\zeta)$ , 并计算公钥  $pk_i = g^{sk_i}$ 。然后生成一个随机数  $r$ , 用于生成承诺  $t = g^r$ 。接下来, 认证方利用 Fiat-Shamir 变换, 将  $t, pk_i$  作为哈希函数的输入, 计算出挑战值  $c$ :

$$c = H(t, pk_i) \quad (1)$$

随后, 根据挑战、随机数、私钥计算出响应  $s$ :

$$s = r + c \cdot sk_i \quad (2)$$

认证方  $P_i$  将身份认证信息  $\sigma_i^{(id)} = (t, s)$  发送给

验证方。

(3) 验证过程: 验证方接收到身份认证信息  $\sigma_i^{(id)}$  后, 用相同的哈希函数计算挑战值  $c' = H(t, pk_i)$ , 并验证以下等式是否成立:

$$g^{s'} = t \cdot pk_i^{c'}$$

如果等式成立, 则身份认证信息有效, 验证方可以确信签名者知道私钥  $sk_i$ , 且未泄露任何私钥信息。如果等式不成立, 则签名无效。

至此, 跨轮次不可关联的匿名身份验证过程完成。该方案的安全性分析见第 5 节, 效率分析见第 6 节。

#### 4.2 跨轮次不可关联的匿名面部识别

认证方  $P_i$  首先需要在签发机构登记其面部信息  $f^*$ 。每次认证方向验证方  $V$  提交面部识别请求时, 需确保其面部信息  $f$  已在签发机构登记。然而, 每次验证时, 认证方提供的面部信息  $f$  与系统录入的  $f^*$  不完全相同。一种常见的模糊匹配方法是计算两者的余弦相似度  $\cos(f, f^*)$ , 如式(3)所示:

$$\cos(f, f^*) = \frac{\sum f_j \cdot f_j^*}{\|f\|_2 \cdot \|f^*\|_2} = \frac{\langle f, f^* \rangle}{\sqrt{\langle f, f \rangle} \cdot \sqrt{\langle f^*, f^* \rangle}} \quad (3)$$

若  $\cos(f, f^*) > a$ , 则验证通过, 其中  $a$  为设定的阈值。然而, 如果签发机构将  $f^*$  直接发送给验证方  $V$ , 则会导致隐私泄露。因此, 采用与第 4.1 节类似的方法, 在  $f^*$  上添加一个干扰项  $\text{Prf}_i(\zeta)$ , 既能保护  $f^*$  的隐私, 又能确保跨轮次验证不会被关联。我们设定公钥为  $pk_i = f^* \cdot \text{Prf}_i(\zeta)$ , 私钥为  $sk_i = f \cdot \text{Prf}_i(\zeta)$ , 从而确保:  $\cos(f, f^*) = \cos(pk_i, sk_i)$ 。

面部识别的零知识化验证较为复杂, 因为离散对数问题具有同态加法性质, 但不具备同态乘法性质。这意味着, 尽管  $g^f \cdot g^{f^*} = g^{f+f^*}$ , 但  $g^{f \cdot f^*}$  并不等于  $g^f \cdot g^{f^*}$  相乘或者做次方运算。因此, 从直观上看, 无法基于离散对数问题将余弦相似度的零知识化。

证明  $\cos(f, f^*) > a$  是否成立, 可以转化为证明式(4)是否成立, 其中  $d \geq B$  是一个随机数,  $b = a^2 pk_i, pk_i$  为已知常量,  $\alpha \leq B$  是一个随机数,  $B = (1 - a^2) pk_i, pk_i \log_2 2p$  是一个已知常量。式(4)的推导过程的求法见附录一。

$$d(pk_i, sk_i^2 - bsk_i, sk_i) + \alpha \leq (d+1)B \quad (4)$$

现在, 我们需要解决离散对数不具备乘法同态的问题。在零知识化上述关系时, 需要将其转换为承诺形式。 $sk_i$  的承诺是  $C = g^{sk_i}$ 。我们需要证明  $pk_i, sk_i^2$  的承诺,  $bsk_i, sk_i$  的承诺中使用的  $sk_i$  与

$C$  中的  $sk_i$  是同一个, 从而完成结构良好性证明。

首先, 随机生成  $C$  的盲化因子  $T = g^\alpha$ , 其中  $\alpha$  是一个随机向量。假设挑战为  $d$ , 则关于  $sk_i$  的响应为

$$s_x = d \cdot sk_i + \alpha.$$

为了用  $s_x$  构造出  $\langle pk_i, sk_i \rangle^2$  和  $b\langle sk_i, sk_i \rangle$ , 我们构造式(5)和(6)两个等式:

$$b\langle s_x, s_x \rangle = bd^2\langle sk_i, sk_i \rangle + 2bd\langle sk_i, \alpha \rangle + b\langle \alpha, \alpha \rangle \quad (5)$$

$$\begin{aligned} \langle s_x, pk_i \rangle^2 &= d^2\langle pk_i, sk_i \rangle^2 + 2d\langle pk_i, sk_i \rangle \\ &\quad \langle pk_i, \alpha \rangle + \langle pk_i, \alpha \rangle^2 \end{aligned} \quad (6)$$

根据  $sk_i, pk_i, \alpha$  的信息, 生成式(7)中的辅助变量:

$$\begin{aligned} x_1 &= 2\langle sk_i, \alpha \rangle, x_2 = \langle \alpha, \alpha \rangle \\ x_3 &= b\langle sk_i, sk_i \rangle, x_4 = \langle pk_i, sk_i \rangle^2 \\ x_5 &= \langle pk_i, \alpha \rangle^2, x_6 = 2\langle pk_i, sk_i \rangle \cdot \langle pk_i, \alpha \rangle \end{aligned} \quad (7)$$

然后, 生成这些辅助变量  $x_j$  的承诺  $c_j = g^{x_j}$  以及盲化因子  $t_j = g^{\alpha_j}$ , 其中  $\alpha_j$  是随机生成的,  $j \in [1, 6]$ 。

接下来, 利用 Fiat-Shamir 变换将交互式证明转换为非交互式证明, 生成挑战  $d = H(C, T, pk_i)$ , 并生成响应:

$$s_x = d \cdot sk_i + \alpha, \quad s_{x_j} = d \cdot x_j + \alpha_j, j \in [1, 6].$$

认证方将  $(\{s_{x_j}, c_j, t_j\}_j, s_x, C, T)$  发送给验证方。

验证方可以将对等式(5)和(6)的验证转换为对式(8)和(9)的验证:

$$g^{s_{x_j}} = t_j c_j^d, j \in [1, 6], \quad g^{s_x} = T \cdot C^d \quad (8)$$

$$g^{b\langle s_x, s_x \rangle} = c_3^{bd^2} c_1^{bd} c_2^b, g^{\langle s_x, pk_i \rangle^2} = c_4^{d^2} c_6^d c_5 \quad (9)$$

至此, 我们证明了  $\langle pk_i, sk_i \rangle^2$  和  $b\langle sk_i, sk_i \rangle$  的承诺中使用的  $sk_i$  与  $C$  中使用的是同一个  $sk_i$ , 从而完成了结构良好性证明。

现在, 我们需要解决如何零知识化区间证明, 即如何证明  $x < y$ 。一种直观的方式是使用目前已有的通用区间证明架构 Bulletproofs<sup>[6]</sup>。然而, 根据式(7)中的变量, 我们可以将式(4)的区间证明转换为证明  $d(x_4 - x_3) + \alpha \leq (d+1)B$ 。而  $d(x_4 - x_3) + \alpha$  则可以转换为  $s_{x_4} - s_{x_3}$ , 只需要设  $\alpha = \alpha_4 - \alpha_3$ , 并满足  $\alpha \leq B$ 。如此, 我们完成了结构良好性证明的同时, 也可以在  $O(1)$  的时间内完成区间证明。

至此, 我们完成了跨轮次不可关联的匿名面部识别验证的设计思路阐述。该零知识证明协议可见于图3。协议由三个主要阶段组成:

公钥签发: 认证者  $P_i$  每次进行面部识别时, 从正整数空间生成一个新的随机数  $\zeta$ , 用以加密面部

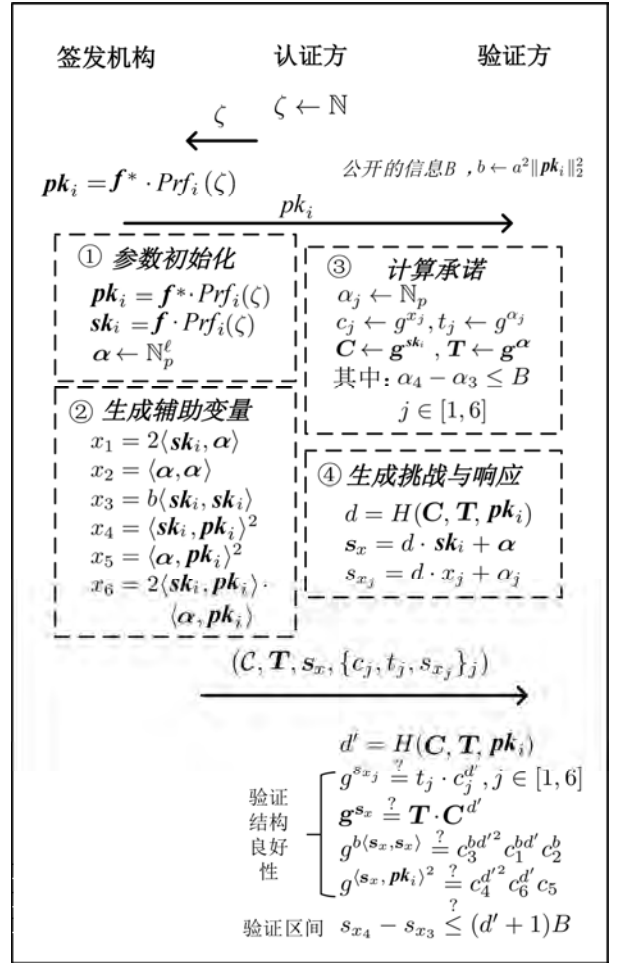


图3 协议2-跨轮次不可关联的匿名面部识别验证

信息  $f$  和签发机构登记的  $f^*$ 。公钥设定为  $pk_i = f^* \cdot \text{Prf}_i(\zeta)$ , 并将其发送给验证方  $V$ 。其中  $\text{Prf}_i$  是一个属于认证者  $P_i$  的伪随机函数。

证明过程: 认证者同样设置公钥为  $pk_i = f^* \cdot \text{Prf}_i(\zeta)$ , 私钥为  $sk_i = f \cdot \text{Prf}_i(\zeta)$ 。随机生成  $\alpha_j$ ,  $j \in [1, 6]$ , 其中  $\alpha_4 - \alpha_3 \leq B$ ,  $B$  是一个公开的常数。生成辅助变量  $x_1 = 2\langle sk_i, \alpha \rangle, x_2 = \langle \alpha, \alpha \rangle, x_3 = b\langle sk_i, sk_i \rangle, x_4 = \langle pk_i, sk_i \rangle^2, x_5 = \langle pk_i, \alpha \rangle^2, x_6 = 2\langle pk_i, sk_i \rangle \cdot \langle pk_i, \alpha \rangle$ 。再生成对应的承诺  $C = g^{sk_i}, c_j = g^{x_j}$  和盲化因子  $T = g^\alpha, t_j = g^{\alpha_j}, j \in [1, 6]$ 。利用哈希函数生成挑战  $d = H(C, T, pk_i)$ , 并计算出响应  $s_x = d \cdot sk_i + \alpha, s_{x_j} = d \cdot x_j + \alpha_j, j \in [1, 6]$ 。认证方将  $\sigma_i^{(f)} = (\{s_{x_j}, c_j, t_j\}_j, s_x, C, T)$  发送给验证方。

验证过程: 验证方根据认证方发送的信息, 生成一个挑战  $d' = H(C, T, pk_i)$ 。然后对每一个承诺  $\{c_j\}_j, C$  进行结构良好性验证, 即验证  $g^{s_{x_j}} = t_j c_j^{d'}$ ,  $g^{s_x} = T \cdot C^{d'}$  是否相等。然后再验证  $g^{b\langle s_x, s_x \rangle} = c_3^{bd^2} c_1^{bd} c_2^b$ ,  $g^{\langle s_x, pk_i \rangle^2} = c_4^{d^2} c_6^d c_5$ , 即验证等式(5)和(6)是否成立。如果成立, 则完成了对余弦相似度计算与承诺  $C$  的

结构良好性证明, 即证明计算余弦相似度时所用的  $f$  与承诺  $C$  中的  $f$  是同一个  $f$ 。最后再验证  $s_{x_4} - s_{x_3} \leq (d' + 1)B$  是否成立, 如果成立则表明面部识别验证通过。如果上述验证有任意一个不通过, 则验证失败。

至此, 我们完成了跨轮次不可关联的匿名面部识别验证。其相关的安全性分析见第 5 节, 效率分析见第 6 节。

## 5 安全性分析

### 5.1 安全需求与零知识证明协议的关系

为了确保系统满足五项核心安全需求, 我们将它们规约到零知识证明的三个基本属性。

(1) 跨轮次匿名性: ZKP 的零知识性属性保证了认证方仅凭证明自己知道某个秘密(如私钥), 而不泄露任何关于身份的信息。我们设第  $\tau$  轮次的参数如下: 随机生成  $\zeta^\tau$ , 再计算出  $sk_i^\tau = i + \text{Prf}_i(\zeta^\tau)$ ,  $sk_i^\tau = f \cdot \text{Prf}_i(\zeta^\tau)$  和  $pk_i^\tau = g^{sk_i^\tau}$ ,  $pk_i^\tau = f^* \cdot \text{Prf}_i(\zeta^\tau)$ 。那么对于第  $\tau$  轮次和第  $\kappa$  轮次而言,  $\zeta^\tau$ 、 $\zeta^\kappa$  均是随机生成的,  $\zeta^\tau$ 、 $\zeta^\kappa$  是不可区分。因此  $\text{Prf}_i(\zeta^\tau)$ 、 $\text{Prf}_i(\zeta^\kappa)$  是不可区分的。所以  $sk_i^\tau$ 、 $sk_i^\kappa$ 、 $pk_i^\tau$ 、 $pk_i^\kappa$  与  $sk_i^\kappa$ 、 $sk_i^\tau$ 、 $pk_i^\kappa$ 、 $pk_i^\tau$  是不可区分的, 这使得每次认证都是独立的, 因此不可能将不同轮次的认证信息关联起来。

(2) 认证完整性: ZKP 的完整性属性保证了, 如果认证方确实知道私钥, 验证方总是能够验证认证请求的合法性。认证方通过私钥和公钥生成承诺、挑战和响应, 验证方通过验证这些响应来确保认证方的合法身份。这保证了完整性, 即只有真实的认证方才能通过验证。

(3) 抗重放攻击: 随机挑战-响应机制, 确保每次认证过程都是唯一的。每次认证使用新的随机数  $\zeta$  生成新的私钥和公钥, 挑战值也是每次随机生成的。因此, 即使攻击者捕获了某次认证的信息, 也无法在未来重放这些信息, 因为每次认证时所用的公钥和私钥都会发生变化, 导致重放攻击无效。

(4) 抗中间人攻击: 在 ZKP 中, 认证方的私钥和其他敏感信息从未直接传输给验证方。通过挑战-响应机制, 认证方依赖自己的私钥生成响应并进行验证, 而中间人无法伪造有效的响应。即使中间人截获了认证信息, 也无法篡改或伪造认证方的身份验证, 因为响应值始终依赖于认证方的私钥和随机生成的挑战。因此, ZKP 有效防止了中间人攻击。

(5) 防止身份盗用: 在我们的协议中, 身份信息的公钥和私钥通过 ZKP 的健全性保证只有掌握私钥的认证方才能生成有效的认证信息。每次认证时, 认证方需要生成新的私钥, 公钥则是由签发机关发放, 并基于私钥生成有效的响应。攻击者获取了签发机关的公钥, 也无法伪造有效的认证请求, 因为只有真正掌握私钥的人才能通过验证。因此, ZKP 的健全性以及签发机构有效防止了身份盗用。

### 5.2 协议1的安全性证明

**定理 1.** 协议 1 是一个 Sigma 协议形式的零知识证明协议, 满足完整性、特殊健全性和零知识性证明。

**完整性:** 根据零知识证明的完整性定义, 若认证方  $P_i$  确实知道私钥  $sk_i$ , 则验证方应能够通过提供的身份认证信息验证认证方的身份, 而不会发生验证失败的情况。

假设认证方  $P_i$  确实知道私钥  $sk_i$ 。认证方选择一个随机数  $r$  并生成承诺  $t = g^r$ 。然后, 认证方计算挑战  $c = H(t, pk_i)$ , 并根据这个挑战计算响应  $s = r + c \cdot sk_i$ 。

验证方收到认证信息  $\sigma_i^{(id)}$  后, 首先计算挑战  $c' = H(t, pk_i)$ , 然后验证等式:

$$g^s = t \cdot pk_i^{c'}$$

由于  $\sigma_i^{(id)}$  中的  $t, pk_i$  与认证方计算挑战  $c = H(t, pk_i)$  中的  $t, pk_i$  是相同的, 因此  $c' = c$ 。代入响应  $s = r + c \cdot sk_i$ , 得到:

$$g^{r+c \cdot sk_i} = g^r \cdot (g^{sk_i})^c$$

由于  $pk_i = g^{sk_i}$ , 我们可以将其代入上式:

$$g^r \cdot pk_i^c = g^r \cdot (g^{sk_i})^c$$

这正是验证方所要验证的等式。因此, 等式成立。验证方能够通过计算给定的身份认证信息  $\sigma_i^{(id)}$  来确认认证方确实知道私钥  $sk_i$ , 并且知道身份证号  $i$ , 因此, 协议满足完整性。

**特殊健全性:** 我们需要证明, 如果验证方接收到两个不同的响应  $s_1$  和  $s_2$ , 并且它们对应于相同的承诺  $t$ 、公钥  $pk_i$  和不同的挑战值  $c_1$  和  $c_2$ , 那么我们能够推导出认证方所知道的私钥  $sk_i$ 。此处挑战值  $c_1$  和  $c_2$  若是认证方随机选取的, 若利用 Fiat-Shamir 变换将交互式证明转换为非交互式证明, 则哈希函数中需要再增加上一个计数器 counter, 来生成两个不同的挑战值  $c_1$  和  $c_2$ , 如  $H(t, pk_i, counter)$ 。

假设验证方收到上述信息,根据协议过程,认证方计算响应  $s_1$  和  $s_2$  时,分别根据挑战值  $c_1$  和  $c_2$  计算的响应公式为

$$s_1 = r + c_1 \cdot sk_i, s_2 = r + c_2 \cdot sk_i。$$

因此,有

$$s_1 - s_2 = (c_1 - c_2) \cdot sk_i。$$

我们可以得到私钥  $sk_i$  的表达式:

$$sk_i = \frac{s_1 - s_2}{c_1 - c_2}。$$

从上述推导可以看出,如果验证方能够获得两个不同的响应  $s_1$  和  $s_2$ ,并且分别对应不同的挑战值  $c_1$  和  $c_2$ ,验证方能够计算出私钥  $sk_i$ 。

虽然验证方仍然不能获得认证方的核心隐私信息-身份证号  $i$ ,但是协议 1 已符合特殊健全性的定义。

零知识性:在本协议中,零知识性确保了认证方通过认证信息  $\sigma_i^{(id)} = (t, s)$  证明自己知道私钥  $sk_i$ ,从而证明自己是在签发机构登记过身份证号  $i$ ,而验证方无法从认证过程中获取任何关于私钥  $sk_i$  的信息,更无法获得任何关于身份证号  $i$  的信息。

为了证明协议符合零知识性,我们将展示一个模拟者,模拟者能够通过随意选择挑战和响应来模拟认证过程,而不需要知道私钥  $sk_i$ 。即验证方无法从协议中获取任何额外的信息,无法从交互中推导出私钥  $sk_i$ ,也无法获得与秘密相关的其他信息。

模拟者生成随机数  $y$  来替换承诺  $t$ 。根据随机数  $y$  和公钥  $pk_i$  计算出挑战  $z = H(y, pk_i)$ 。然后模拟者计算  $v$  替换响应  $s$ :

$$v = \log_g(y \cdot pk_i^{H(y, pk_i)})。$$

模拟者向验证方发送模拟的证明信息  $\sigma_i^{(id)} = (y, v)$  来替代  $(t, s)$ 。验证方收到  $\sigma_i^{(id)}$  后,首先计算挑战  $z = H(y, pk_i)$ ,然后验证等式:

$$g^v = s \cdot pk_i^c。$$

由于  $\sigma_i^{(id)}$  中  $v = \log_g(y \cdot pk_i^{H(y, pk_i)})$ ,因此得到

$$g^{\log_g(y \cdot pk_i^{H(y, pk_i)})} = y \cdot pk_i^z。$$

由于  $z = H(y, pk_i)$ ,我们可以将其代入:

$$g^{\log_g(y \cdot pk_i^{H(y, pk_i)})} = y \cdot pk_i^{H(y, pk_i)}。$$

这正是验证方所要验证的等式。因此,等式成立。

至此,已经证明模拟者能够在不知晓私钥的情况下生成合法的认证信息,使得验证方无法从交互记录中分辨出模拟者和真实的认证方。因此协议保证了零知识性。

因此协议 1,是一个 Sigma 协议,进而是一个零知识证明协议。 证毕。

### 5.3 协议2的安全性证明

**定理 2.** 协议 2 是一个 Sigma 协议形式的零知识证明协议,满足完整性、特殊健全性和零知识性。证明。

完整性:认证方式与定理 1 相同。假设认证方  $P_1$  确实知道私钥  $sk_i$ 。认证方随机生成一个随机向量  $\alpha$  和 6 个随机标量  $\alpha_j$ ,其中  $j \in [1, 6]$ ,且满足  $\alpha_4 - \alpha_3 \leq B$ 。认证方利用  $\alpha$  和  $sk_i$  生成 6 个辅助变量  $x_j, j \in [1, 6]$ 。随后,为  $sk_i, x_j, \alpha, \alpha_j$  生成对应的承诺和盲化因子:

$$C = g^{sk_i}, T = g^\alpha, c_j = g^{x_j}, t_j = g^{\alpha_j}, j \in [1, 6]。$$

接下来,认证方计算挑战  $d = H(C, T, pk_i)$ ,并根据这个挑战计算响应:

$$s_x = d \cdot sk_i + \alpha, s_{x_j} = d \cdot x_j + \alpha_j, j \in [1, 6]。$$

认证方将  $\sigma_i^{(f)} = (\{s_{x_j}, c_j, t_j\}, s_x, C, T)$  发送给验证方。

验证方根据认证方发送  $\sigma_i^{(f)}$ ,生成一个挑战  $d' = H(C, T, pk_i)$ ,并验证下述等式是否成立:

$$\begin{aligned} g^{s_{x_j}} &= t_j c_j^{d'}, g^{s_x} = T \cdot C^{d'}, \\ g^{(bs_x, s_x)} &= c_3^{bd^2} c_1^{bd'} c_2^b, g^{(s_x, pk_i)^2} = c_4^{d^2} c_6^{d'} c_5, \\ s_{x_4} - s_{x_3} &\leq (d' + 1)B。 \end{aligned}$$

由于  $\sigma_i^{(f)}$  中的  $C, T$  与认证方计算挑战  $d' = H(C, T, pk_i)$  中的  $C, T$  是相同的,因此  $d' = d$ 。代入响应  $s_x = d \cdot sk_i + \alpha, s_{x_j} = d \cdot x_j + \alpha_j$ ,得到:

$$\begin{aligned} g^{s_x} &= g^{d \cdot sk_i + \alpha} = T \cdot C^d, \\ g^{s_{x_j}} &= g^{d \cdot x_j + \alpha_j} = t_j c_j^d。 \end{aligned}$$

因此,上述两个等式成立。因为公钥为  $pk_i = f^* \cdot Prf_i(\zeta)$ ,私钥为  $sk_i = f \cdot Prf_i(\zeta)$ ,将其带入到  $g^{(bs_x, s_x)}, g^{(s_x, pk_i)^2}$  相关的验证等式中,得到:

$$\begin{aligned} g^{(bs_x, s_x)} &= g^{bd^2 \langle sk_i, sk_i \rangle + 2bd \langle sk_i, \alpha \rangle + b \langle \alpha, \alpha \rangle} = g^{bd^2 x_3 + 2bdx_1 + bx_2} = \\ &= c_3^{bd^2} c_1^{bd} c_2^b, \\ g^{(s_x, pk_i)^2} &= g^{d^2 \langle pk_i, sk_i \rangle^2 + 2d \langle pk_i, sk_i \rangle \langle pk_i, \alpha \rangle + \langle pk_i, \alpha \rangle^2} = \\ &= g^{d^2 x_4 + dx_6 + x_5} = c_4^{d^2} c_6^d c_5。 \end{aligned}$$

这正是验证方所要验证的等式。

最后,验证方只需要判断  $s_{x_4} - s_{x_3} \leq (d' + 1)B$  是否成立。这一不等式成立等价于:认证方提供的面部信息  $f$  与其在签发机构登记的  $f^*$  计算余弦相似度值  $\cos(f, f^*)$ ,并确保其大于预设的阈值  $a$ 。

因此,验证方能够通过计算给定的身份认证信息  $\sigma_i^{(f)}$  来确认认证方确实知道私钥  $sk_i$ ,并且拥有正确的面部识别信息  $f$ 。因此,协议满足完整性。

特殊健全性:我们需要证明,如果验证方接收

到两组不同的响应  $s_x, \{s_{x_j}\}_j$  和  $s'_x, \{s'_{x_j}\}_j$ , 并且它们对应于相同的  $C, T, \{c_j, t_j\}_j$ 、公钥  $pk_i$ , 且具有不同的挑战值  $d_1$  和  $d_2$ , 那么我们能够推导出认证方所知道的私钥  $sk_i$ 。在这种情况下, 如果挑战值  $d_1$  和  $d_2$  若是认证方随机选取的, 则可直接使用。若通过 Fiat-Shamir 变换将交互式证明转换为非交互式证明, 则哈希函数中需要增加一个计数器 counter, 以生成两个不同的挑战值  $d_1$  和  $d_2$ , 如  $H(C, T, pk_i, counter)$ 。

假设验证方收到上述信息。根据协议过程, 认证方计算响应  $s_x, \{s_{x_j}\}_j$  和  $s'_x, \{s'_{x_j}\}_j$  时, 分别根据挑战值  $d_1$  和  $d_2$  计算的响应公式为:

$$s_x = d_1 \cdot sk_i + \alpha, \quad s_{x_j} = d_1 \cdot x_j + \alpha_j, j \in [1, 6],$$

$$s'_x = d_2 \cdot sk_i + \alpha, \quad s'_{x_j} = d_2 \cdot x_j + \alpha_j, j \in [1, 6].$$

由此得到:

$$s_x - s'_x = (d_1 - d_2)sk_i, \quad s_{x_j} - s'_{x_j} = (d_1 - d_2)x_j.$$

可以从中推导出私钥  $sk_i$  和辅助变量  $x_j$  的表达式:

$$sk_i = \frac{s_x - s'_x}{d_1 - d_2}, \quad x_j = \frac{s_{x_j} - s'_{x_j}}{d_1 - d_2}.$$

从上述推导可以看出, 如果验证方能够获得两组不同的响应  $s_x, \{s_{x_j}\}_j$  和  $s'_x, \{s'_{x_j}\}_j$ , 且它们分别对应于不同的挑战值  $d_1$  和  $d_2$ , 验证方就能够计算出私钥  $sk_i$  和辅助变量  $x_j$ 。

因此协议 2 符合特殊健全性的定义。

零知识性: 在本协议中, 零知识性确保了认证方通过认证信息  $\sigma_i^{(f)} = (\{s_{x_j}, c_j, t_j\}_j, s_x, C, T)$  证明自己知道私钥  $sk_i$ , 从而证明自己的面部信息  $f$  与在签发机构登记过的  $f^*$  是匹配的, 而验证方无法从认证过程中获取任何关于私钥  $sk_i$  的信息, 更无法获得任何关于面部信息  $f$  和  $f^*$  的信息。

为了证明协议符合零知识性, 我们将展示一个模拟者, 模拟者能够通过随意选择挑战和响应来模拟认证过程, 而不需要知道私钥  $sk_i$ 。

模拟者生成随机向量  $\vec{C}, \vec{T}$ , 来替换  $C, T$ , 这样挑战  $d = H(C, T, pk_i)$  就会被替换为  $\vec{d} = H(\vec{C}, \vec{T}, pk_i)$ 。接着, 模拟者计算出  $\vec{s}_x$  来替换  $s_x$ :

$$\vec{s}_x = \log_g(\vec{T} \cdot \vec{C}^{\vec{d}}).$$

然后, 利用  $s_x$ , 模拟者可以确定  $g^{b(\vec{s}_x, \vec{s}_x)}, g^{(\vec{s}_x, pk_i)^2}$  的值。接下来, 模拟者生成四个随机数  $\vec{c}_j, j \in \{1, 3, 4, 6\}$ , 并计算出  $\vec{c}_2, \vec{c}_5$  的值:

$$\vec{c}_2 = g^{(\vec{s}_x, \vec{s}_x)} / (\vec{c}_3^{\vec{d}^2} \cdot \vec{c}_1^{\vec{d}}),$$

$$\vec{c}_5 = g^{(\vec{s}_x, pk_i)^2} / (\vec{c}_4^{\vec{d}^2} \cdot \vec{c}_6^{\vec{d}}).$$

生成六个随机数  $\vec{s}_{x_j}, j \in [1, 6]$  其中  $\vec{s}_{x_4}, \vec{s}_{x_3}$  满足:

$$\vec{s}_{x_4} - \vec{s}_{x_3} \leq (\vec{d} + 1)B.$$

最后, 计算六个  $\vec{t}_j = g^{\vec{s}_{x_j}} / \vec{c}_j^{\vec{d}}, j \in [1, 6]$ 。模拟者将  $\sigma_i^{(f)} = (\{\vec{s}_{x_j}, \vec{c}_j, \vec{t}_j\}_j, \vec{s}_x, \vec{C}, \vec{T})$  发送给验证方。

验证方收到  $\sigma_i^{(f)}$  后, 首先计算出挑战  $\vec{d} = H(\vec{C}, \vec{T}, pk_i)$ , 然后验证下述等式是否成立:

$$g^{\vec{s}_{x_j}} = \vec{t}_j \vec{c}_j^{\vec{d}}, j \in [1, 6].$$

因为  $\vec{t}_j = g^{\vec{s}_{x_j}} / \vec{c}_j^{\vec{d}}, j \in [1, 6]$ , 所以上述等式显然成立。然后验证方再验证  $g^{\vec{s}_x} = \vec{T} \cdot \vec{C}^{\vec{d}}$  是否成立。由于  $\vec{s}_x = \log_g(\vec{T} \cdot \vec{C}^{\vec{d}})$ , 所以上述等式显然成立。接着, 验证方再验证以下等式是否成立:

$$g^{b(\vec{s}_x, \vec{s}_x)} = \vec{c}_3^{b\vec{d}^2} \cdot \vec{c}_1^{b\vec{d}} \cdot \vec{c}_2^b.$$

因为  $\vec{c}_2 = g^{(\vec{s}_x, \vec{s}_x)} / (\vec{c}_3^{\vec{d}^2} \cdot \vec{c}_1^{\vec{d}})$ , 所以上式成立。接下来验证方验证等式是否成立:

$$g^{(\vec{s}_x, pk_i)^2} = \vec{c}_4^{\vec{d}^2} \cdot \vec{c}_6^{\vec{d}} \cdot \vec{c}_5.$$

因为  $\vec{c}_5 = g^{(\vec{s}_x, pk_i)^2} / (\vec{c}_4^{\vec{d}^2} \cdot \vec{c}_6^{\vec{d}})$ , 所以上式成立。最后验证方验证  $\vec{s}_{x_4} - \vec{s}_{x_3} \leq (\vec{d} + 1)B$  是否成立, 而  $\vec{s}_{x_4} - \vec{s}_{x_3}$  在生成时就符合了上述约束。

至此, 已经证明模拟者能够在不知晓私钥的情况下生成合法的认证信息, 使得验证方无法从交互记录中分辨出模拟者和真实的认证方。因此协议保证了零知识性。

综上所述, 协议 2 满足完整性、特殊健全性和零知识性。因此协议 2, 是一个 Sigma 协议, 进而是一个零知识证明协议。证毕。

## 6 效率分析

协议 1 和协议 2 的计算复杂度和通信开销如表 1 所示, 详细分析请见下文。

表 1 协议 1 和协议 2 的计算和通信复杂度

复杂度	协议	签发机构	认证方	验证方
计算	1	$O(\log p)$	$O(2\log p)$	$O(2\log p)$
	2	$O(\ell)$	$O(2\ell \log p)$	$O(2\ell \log p)$
通信	1	$O(\log p)$	$O(2\ell \log p)$	\
	2	$O(\ell \log p)$	$O(3\ell \log p)$	\

### 6.1 协议1的效率分析

从图 2 可知, 协议 1 过程涉及三方参与者。各参与方的时间复杂度与通信开销进行如下分析:

签发机构需为每一个认证方计算私钥和公钥。私钥生成过程为  $sk_i = i + \text{Prf}_i(\zeta)$ , 其中  $\text{Prf}_i$  表示伪随机函数。这该计算涉及一次伪随机函数生成与一次标量加法, 计算复杂度为  $O(1)$ 。随后, 签发机构

计算公钥  $pk_i = g^{sk_i} \bmod p$ , 该步骤为这涉及一次模  $p$  次标量的指数幂运算, 其计算复杂度为  $O(\log p)$ , 其中  $p$  是大素数的大小。因此, 签发机构整体的计算复杂度为  $O(\log p) + O(1) = O(\log p)$ 。签发机构发送公钥  $pk_i$  给验证方。由于  $pk_i \in \mathbb{N}_p$ , 即其位长为  $\log p$ , 因此通信开销为  $k_i$  的通信开销是  $O(\log p)$ 。

认证方在每轮认证中需完成一共执行了七项操作。首先, 生成一个随机标量  $\zeta$ , 计算时间复杂度为  $O(1)$ ; 然后计算私钥  $sk_i = i + \text{Prf}_i(\zeta)$ , 同样, 时间复杂为  $O(1)$ ; 接着计算公钥  $pk_i = g^{sk_i} \bmod p$ , 需耗费  $O(\log p)$ ; 采样随机数  $r$  的复杂度为  $O(1)$ ; 计算承诺复杂度为  $O(\log p)$ ; 随后计算挑战  $c = H(t, pk_i)$ , 哈希函数复杂度为  $O(1)$ ; 响应计算为  $s = r + c \cdot sk_i$ , 时间复杂度仍为  $O(1)$ 。故认证方总体的时间复杂度为  $O(2\log p)$ 。在通信方面, 认证方向验证方发送承诺  $t$  与响应  $s$ 。这两个标量均为密文域  $\mathbb{N}_p$  中的元素, 因此通信开销是  $O(2\log p)$ 。

验证方执行两个主要任务: 首先重新计算挑战  $c' = H(t, pk_i)$ , 其计算复杂为  $O(1)$ ; 其次验证  $g^s$  与  $t \cdot pk_i^c$  是否相等, 该过程需执行两次指数运算, 分别计算  $g^s$ ,  $pk_i^c$ , 复杂度为  $O(2\log p)$ 。此外还需一次乘法与一次等值比较, 均为  $O(1)$ 。因此, 验证方总体计算复杂度为  $O(2\log p)$ 。

## 6.2 协议2的效率分析

从图 3 可知, 协议 2 同样涉及三个参与方。各参与方的时间复杂度与通信开销进行如下分析:

签发机构需为每一个认证方计算公钥。公钥生成过程为  $pk_i = f^* \cdot \text{Prf}_i(\zeta)$ , 时间复杂度为  $O(\ell)$ , 其中  $\ell$  是向量  $f^*$  的维度。因此, 签发机构整体的计算复杂度为  $O(\ell)$ 。在通信方面, 签发机构需将生成的公钥  $pk_i$  发送给验证方。由于  $pk_i \in \mathbb{N}_p^\ell$ , 每一维度的位长为  $\log p$ , 共  $\ell$  维度, 因此通信开销为  $O(\ell \log p)$ 。

认证方在每轮认证中需完成多项操作。首先, 生成随机标量  $\zeta$ , 计算复杂度为  $O(1)$ ; 然后根据该随机数重新生成私钥  $sk_i = f \cdot \text{Prf}_i(\zeta)$ , 和公钥  $pk_i = f^* \cdot \text{Prf}_i(\zeta)$ , 时间复杂度均为  $O(\ell)$ ; 之后认证方生成随机向量  $a$ , 其时间复杂度  $O(\ell)$ 。然后认证方需要生成六个辅助变量  $x_j$ , 这些辅助变量均用到了向量的内积。对  $\ell$  维度的向量进行内积的时间复杂度  $O(2\ell)$ , 共需要进行五次内积运算, 和 6 次标量乘法, 因此时间复杂度共计  $O(10\ell)$ ; 随后生成 6 个随机标量  $\alpha_j$ , 并计算承诺  $C = g^{sk_i}$ ,  $c_j = g^{x_j}$  和盲

化因子  $T = g^a$ ,  $t_j = g^{\alpha_j}$ ,  $j \in [1, 6]$ , 共计 12 次标量模运算, 和两次  $\ell$  维度向量模运算, 共  $O((2\ell + 12)\log p)$ 。又因为面部信息的维度  $\ell \gg 12$ , 因此约等于  $O(2\ell \log p)$ 。随后计算挑战  $d = H(C, T, pk_i)$ , 复杂度为  $O(1)$ ; 响应计算分为一个向量响应  $s_x = d \cdot sk_i + a$ , 时间复杂度为  $O(2\ell)$ , 6 个标量响应  $s_{x_j} = d \cdot x_j + \alpha_j$ ,  $j \in [1, 6]$ , 时间复杂度为  $O(2)$ 。而  $p$  是一个大素数, 因此认证方总体的时间复杂度约等于  $O(2\ell \log p)$ 。在通信方面, 认证方向验证方发送  $\sigma_i^{(r)} = (\{s_{x_j}, c_j, t_j\}_j, s_x, C, T)$ , 共 18 个密文域  $\mathbb{N}_p$  的标量和 3 个密文域  $\mathbb{N}_p^\ell$  的向量, 因此通信开销是  $O((13 + 3\ell)\log p) \approx O(3\ell \log p)$ 。

验证方首先重新计算挑战  $d'$ , 其计算复杂为  $O(1)$ ; 其次验证  $g^{s_{x_j}}$  与  $t_j \cdot c_j^{d'}$  是否相等,  $j \in [1, 6]$ , 该过程需共需要执行 18 次指数运算, 复杂度为  $O(18\log p)$ 。此外还需一次乘法与一次等值比较, 均为  $O(1)$ 。然后验证  $g^{s_x}$  与  $T \cdot C^{d'}$  是否相等, 复杂度为  $O(2\ell + 2\ell \log p)$ 。接下来, 计算出  $g^{bs_x \cdot s_x}$ ,  $c_3^{bd^2}$ ,  $c_1^{bd}$ ,  $c_2^{b^2}$ ,  $g^{s_x \cdot pk_i^2}$ ,  $c_4^{d^2}$ ,  $c_6^{d^2}$ , 共 7 次指数运算, 复杂度为  $O(7\log p)$ 。因此, 验证方总体计算复杂度为  $O(25\log p + 2\ell + 2\ell \log p)$ 。而  $p$  是一个大素数,  $\log p$ ,  $\ell$  通常取值在 128 ~ 512, 因此约等于  $O(2\ell \log p)$ 。

## 7 实验验证

### 7.1 实验环境

我们的实验运行在一台台式电脑上, 搭载了 Intel(R) Core(TM) i7-9700 CPU@3.00 GHz 处理器, 机带 RAM 为 32 GB。代码则是通过 Rust1.84 编写。对于离散对数中的大素数  $p$  我们则使用了 RFC 2412 和 RFC 3526 定义的安全大素数, 为了测试不同素数对效率的影响, 我们分别采用了 768 bits、1024 bits、1536 bits、2048 bits、3072 bits、4096 bits、6144 bits、8192 bits 的大素数  $p$ , 对应于 RFC 2412 定义的组编号 1、2, RFC 3526 定义的组编号 5、14、15、16、17、18。哈希函数则选用了 SHA256, 伪随机数发生器  $\text{Prf}_i$  则选用 HMAC-SHA256, 即一个标准的基于 SHA-256 的消息鉴别码。

对于协议 2 所涉及到的面部识别, 本质上是对向量的余弦相似度计算。比如 Facenet 这种通用面部识别系统, 会采集到 128、256、512 个特征向量。因此我们设  $\ell \in [10^2, 10^4]$ , 覆盖各种情况的面部识别参数。下述实验结果取的是 5 次实验的平均数。

### 7.2 各参数对协议效率的影响

为验证协议 1 计算复杂度分析的准确性，我们在不同输入规模（对应大素数  $p$  的位长）下对签发机构、认证方与验证方的运行时间进行了实测，结果如图 4 所示。实验表明，随着输入规模的增加，三类参与方的运行时间均呈现对数增长趋势，整体曲线形态与理论预测的复杂度  $O(\log p)$ 、 $O(2\log p)$ 、 $O(2\log p)$  高度一致。尤其是认证方与验证方，其运行时间几乎重合，反映出两者在协议中均需执行两次模幂运算，具有相近的计算成本；而签发机构的运行时间略低，仅需一次模幂计算，与其理论模型完全吻合。该结果充分验证了协议 1 复杂度分析的正确性与现实适应性。

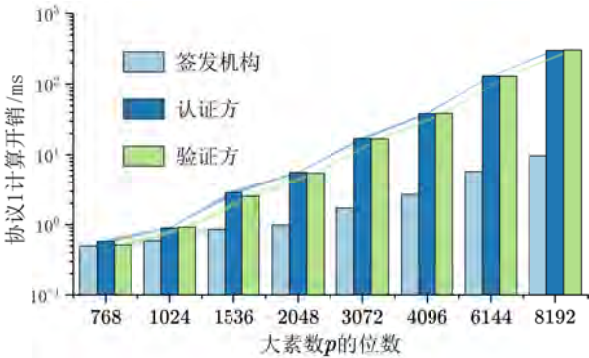


图 4 协议 1 采用不同参数  $p$  的时间开销

在通信方面，协议中所有传输数据均为有限域  $N_p$  中的标量，每个标量在理论上需占用  $\log_2 p$  比特。在实验中，通信开销按字节(Bytes)进行统计，因此每个标量在实际传输中占用  $\log_2 p / 8$  字节。图 5 展示了各方在不同安全参数下的通信数据量，反映了实际网络环境中协议通信负载的变化趋势。实验结果表明，签发机构与认证方的通信开销均随输入规模线性增长，分别对应发送一个和两个标量的信息量，符合理论分析中通信复杂度为  $(\log p)$ 、 $O(2\log p)$  的预期。验证方作为接收端，其通信成本反映了前两者发送数据之和。整体来看，协议 1 在确保安全性与匿名性的前提下，实现了通信负载的有效控制，具备良好的可扩展性。

图 6 展示了协议 2 在不同安全参数（即大素数  $p$  位长）下的平均运行时间。实验结果表明，签发机构的计算开销随参数变化保持稳定，验证了理论中其复杂度为  $O(\ell)$  且与  $p$  无关的预期，该稳定性也表明运行时间的微弱波动主要源于系统环境扰动。相比之下，认证方与验证方的运行时间随  $p$  的位长增

长呈对数趋势，二者曲线高度重合，验证了理论中  $O(2\ell \log p)$  的复杂度分析，其中  $O(\log p)$  为主要影响因素之一。

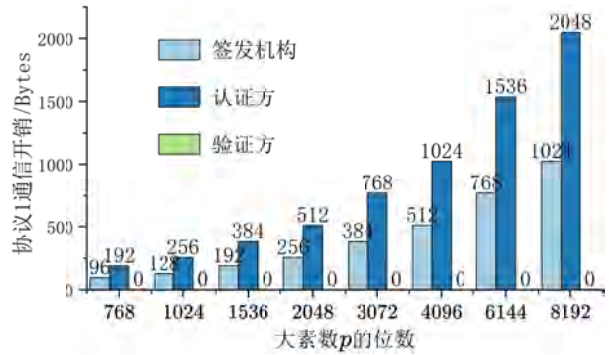


图 5 协议 1 采用不同参数  $p$  的通信开销

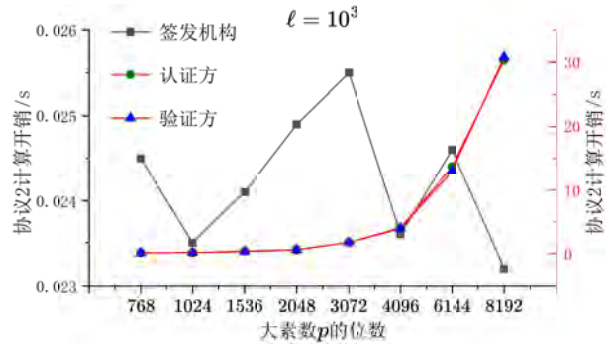


图 6 协议 2 采用不同参数  $p$  的时间开销

图 7 给出了协议 2 中认证方与验证方的通信开销。与协议 1 类似，协议 2 中所有通信数据也属于  $N_p$  域，其位长为  $\log_2 p$  bits，故通信数据大小理论上与  $\log_2 p$  成正比。实验表明，随着大素数  $p$  的位数增加，通信开销线性增长。尤其是认证方的通信量明显高于验证方，约为其三倍，反映出协议中大量承诺、盲化因子与响应向量均由认证方生成与发送。这一增长趋势与理论中的通信复杂度  $O(\ell \log p)$ 、 $O(3\ell \log p)$  相吻合，进一步验证了协议设计在维持匿名性与不可关联性的同时，对通信资源提出的合理要求。

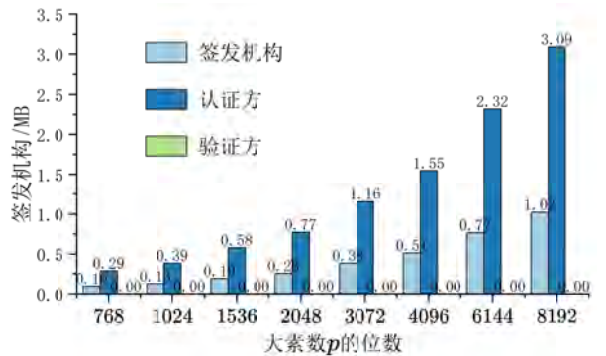


图 7 协议 2 采用不同参数  $p$  的通信开销

图 8 展示了在不同安全参数  $p$  下，向量维度  $\ell$  对协议 2 运行时间和通信开销的影响。实验结果表明，随着  $\ell$  增加，签发机构、认证方和验证方的计算时间，且不同  $p$  下的增长趋势保持一致。这与协议在理论上计算为  $O(\ell)$ 、 $O(2\ell\log p)$  和  $O(2\ell\log p)$  的分

析一致，说明时间开销  $\ell$  而言是线性的。在通信开销方面，签发机构与认证方的通信开销随着  $\ell$  的增长呈线性增长，且不同  $p$  下的增长趋势保持一致，符合理论中  $O(\ell\log p)$ 、 $O(2\ell\log p)$ 。该结果验证了协议 2 在高维特征场景下的良好可扩展性。

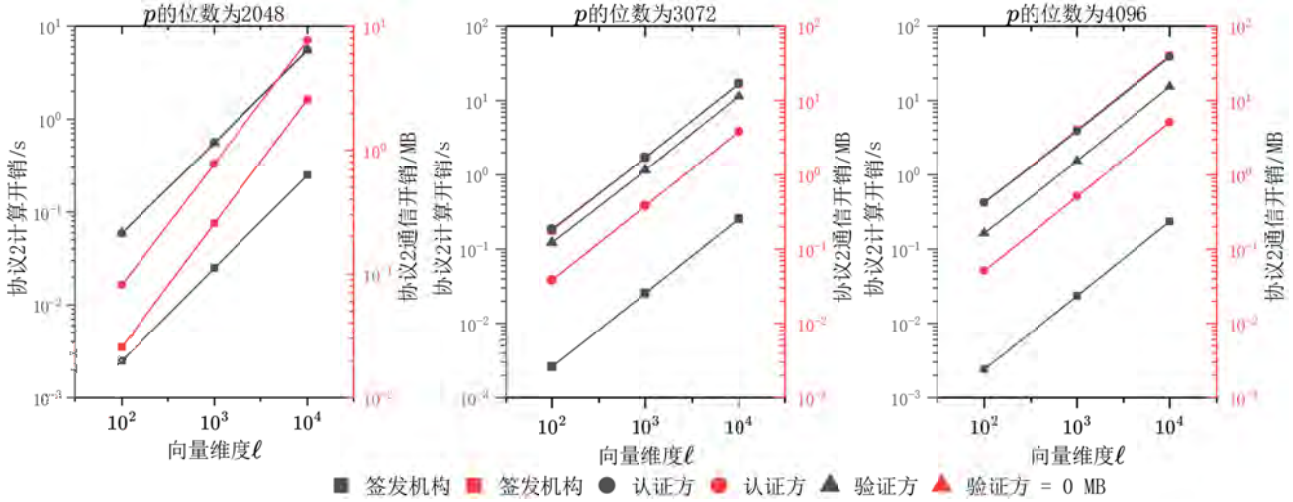


图 8 向量维度对协议 2 的计算和通信开销的影响

### 7.3 零知识化和不可链接的匿名化带来的开销

#### 7.3.1 协议 1 的不可链接的匿名化带来的额外开销

协议 1 所做的证明是跨轮次不可关联的匿名身份验证，其与目前主流的 Schnorr 协议的区别在于其匿名身份是跨轮次不可关联的。在协议 1 中，签发机构与认证方多执行了 1 个操作，即更新私钥  $sk_i = i + \text{Prf}_i(\zeta)$ ，以及认证方多生成了一个随机数  $\zeta$ 。这仅涉及一次标量加法、一次伪随机函数计算、一次随机数生成。而这些操作都是  $O(1)$  的，与幂运算的  $O(p)$  相比是可忽略不计的。因此，从理论角度来讲，协议 1 与 Schnorr 的理论时间复杂度是一致的，实验结果如图 9 所示，实验与理论相一致。

在通信方面，两个协议则是一致的，发送的数据种类、数据大小与数据量完全一致。图 10 展示了实验结果，因此实验和理论相一致。

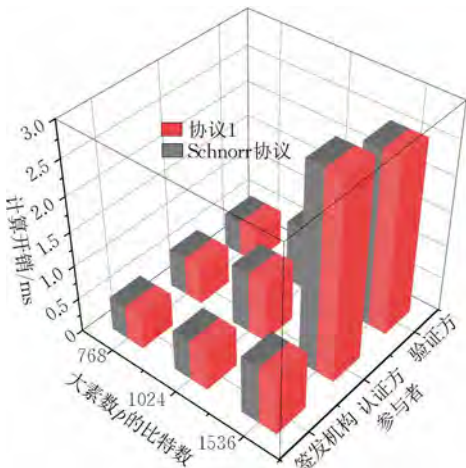


图 9 协议 1 与 Schnorr 协议在不同  $p$  下的计算开销

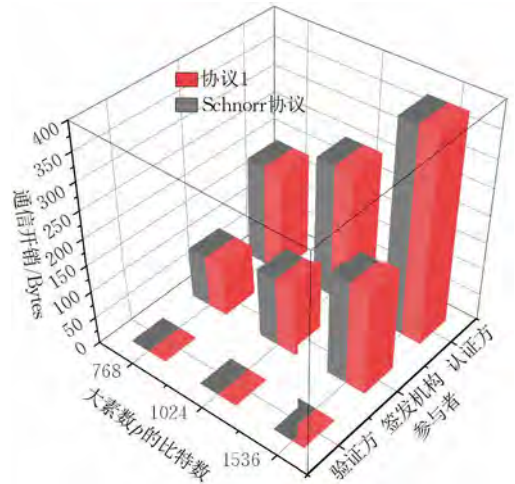


图 10 协议 1 与 Schnorr 协议在不同  $p$  下的通信开销

#### 7.3.2 协议 2 的零知识化带来的额外开销

在未进行零知识化的场景中，面部识别的本质是计算两个向量间的余弦相似度。该过程涉及三个向量内积操作，计算复杂度为  $O(3\ell)$ ，外加一次标量乘法、除法、开方及大小比较，均为常数时间操作，整体复杂度可近似为  $O(3\ell)$ 。此过程完全由验证方执行，认证方与签发机构无需参与任何计算。在通信方面，未零知识化方案中，签发机构需

发送注册的面部向量，认证方发送其当前面部向量。由于每个向量维度为  $\ell$ ，每个元素属于明文域  $\mathbb{N}_t$ ，故通信开销为  $O(\ell \log t)$ 。对于面部向量，其值通常在区间  $[0,1]$  内，实际以 32 位浮点数 (float32) 进行编码，因此可设明文上界为  $t = 2^{32}$ 。相比之下，协议 2 中所有操作均在密文域  $\mathbb{N}_p$  上进行，且满足  $p \gg t$ ，故理论上传输相同维度数据所需位数之差为  $O(3\ell \log p - \ell \log t) \approx O(3\ell \log p)$ 。

从理论分析可知，明文余弦相似度的计算与协议 2 所引入的零知识化处理相比，其计算和通信开销可以忽略不计。由于两者在运行时间上的主要差异仅与维度  $\ell$  相关，表 2 展示了二者在实验条件下的开销对比。结果表明，协议 2 的主要开销来源于匿名性与零知识安全性机制的引入。然而，该协议在实际运行中的时间与空间开销均处于可接受范围内。特别地，在实际面部识别应用中，向量维度通常不超过 512，实测表明各参与方计算延迟均小于 500 ms，具备良好的实用性。相比之下，采用通用零知识证明框架 SNIP 的方法<sup>[28]</sup>在进行同规模向量的余弦相似度证明时，其计算与通信开销均难以满足实际部署需求。在向量维度为 1000 的情况下，生成一次完整的零知识证明耗时超过 32 s，验证方完成验证则需 100 s 以上，认证过程的延迟极高。同时，该方案在通信方面的负担更加严重：认证方生成的证明体积已超过 100 MB，若向量维度进一步提升，通信量甚至可能超过 1 GB。

表 2 计算余弦相似度与协议 2( $p=2048$ )的开销对比

协议	参与方	$\ell = 100$	$\ell = 1000$	$\ell = 10000$
明文	验证方	0.03 ms	0.11 ms	2.84 ms
	签发机构	2.5 ms	24 ms	248 ms
Amrita <sup>[32]</sup>	认证方	3.75 s	32.67 s	331.2 s
	验证方	11.4 s	105.3 s	417.6 s
协议 2	签发机构	2.5 ms	24 ms	248 ms
	认证方	58 ms	550 ms	5553 ms
	验证方	59 ms	549 ms	5448 ms
明文	签发机构	0.0004 MB	0.004 MB	0.04 MB
	认证方	0.0004 MB	0.004 MB	0.04 MB
Amrita <sup>[32]</sup>	签发机构	0.02 MB	0.25 MB	2.56 MB
	认证方	32 MB	>100 MB	>1 GB
协议 2	签发机构	0.02 MB	0.25 MB	2.56 MB
	认证方	0.08 MB	0.77 MB	7.68 MB

相较之下，本文提出的专用零知识协议显著优化了余弦相似度计算在零知识化条件下的性能。实验数据显示，本方案在认证时间与通信开销方面分别降低了约 98%与 99.75%，在保证安全性与零知识性的前提下，极大提升了实际系统的可用性与可部署性。

## 8 结论

本文提出了一种适用于零信任架构下的、多因素、匿名身份认证协议，旨在实现身份认证过程中的隐私保护与高效性兼顾。通过引入“认证方与验证方互不信任”的新型身份认证模型，认证方在不泄露任何身份明文信息的前提下，使用结构化的 Sigma 协议实现密文化认证，从而有效抵御隐私泄露与关联攻击。在协议设计上，针对两类典型身份因子——身份证号与面部特征，本文分别构造了具有跨轮次不可关联性的精准匹配和模糊匹配专用零知识认证。对于身份证号认证，本文在 Schnorr 协议基础上引入动态密钥更新机制，使得每轮认证均使用独立公钥，保证认证结果无法被链接；对于面部识别认证，本文首次在 Sigma 协议框架下构造了基于余弦相似度验证的零知识证明协议，使验证方无需接触原始面部向量即可完成有效身份确认，从而实现生物特征认证的隐私保护与可验证性统一。同时，克服通用零知识证明方案在复杂和高维向量计算场景下效率低下的问题。在典型配置(向量维度为 1000，密钥长度 2048 位)下，相较于基于 SNIP 等通用 ZKP 框架的方法，本文协议在认证延迟与通信开销上分别降低约 98%和 99.75%，证明生成与验证时间控制在毫秒级，通信量小于 0.5 MB，大幅提升了系统的可部署性与响应能力。

本研究作为零信任环境下可信身份认证基础设施建设的重要组成部分，为多因素认证提供了一种高效、可验证、具匿名性的新范式。未来工作将进一步探索去中心化信任管理、自适应证明生成策略以及抗量子安全扩展等方向，以增强本方案在开放网络与未来安全体系中的通用性与长期适用性。

致谢 2023 年湖北省重大研究计划(2023BAA027)、2023 年度长沙市揭榜挂帅重大科技项目(kq2503009)、深圳市科技计划国际合作研究项目(GJHZ20240218-

114659027)、湖北省重点研发计划项目(2024BAB049)、中央高校基本科研业务费专项资金(YCJJ20252331, YCJJ2025-2336)资助。

### 参 考 文 献

- [1] Stallings W. Network Security Essentials: Applications and Standards. 5th ed. Boston, USA: Pearson Education, 2017
- [2] Rose S, Borchert O, Mitchell S, Connelly S. Zero Trust Architecture. Gaithersburg, USA: National Institute of Standards and Technology, 2020
- [3] Bonneau J, Herley C, Van Oorschot P C, Stajano F. The quest to replace passwords: A framework for comparative evaluation of Web authentication schemes//Proceedings of the IEEE Symposium on Security and Privacy. Oakland, USA, 2012: 553-567
- [4] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 1985, 18(1): 186-208
- [5] Groth J. On the size of pairing-based non-interactive arguments//Proceedings of the Advances in Cryptology – EUROCRYPT 2016. Vienna, Austria, 2016: 305-326
- [6] Bünz B, Bootle J, Boneh D, et al. Bulletproofs: Short proofs for confidential transactions and more//Proceedings of the 2018 IEEE Symposium on Security and Privacy (SP). San Francisco, USA, 2018, 315-334
- [7] Corrigan-Gibbs H, Boneh D. Prio: Private, robust, and scalable computation of aggregate statistics//Proceedings of the 14th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA, 2017: 259-282
- [8] Camenisch J, Stadler H U. Efficient group signature schemes for large groups//Proceedings of the Advances in Cryptology-CRYPTO'97, 17th Annual International Cryptology Conference. Santa Barbara, USA, 1997: 410-424
- [9] Schnorr C P. Efficient signature generation by smart cards. Journal of Cryptology, 1991, 4(3): 161-174
- [10] Joshua R, Trevor S, Ken R, et al. A Tale of two studies: The best and worst of yubikey usability//Proceedings of the 2018 IEEE Symposium on Security and Privacy. San Francisco. USA, 2018: 872-888
- [11] Tarun K, Kent S. A security and usability analysis of local attacks against FIDO2//Proceedings of the Network and Distributed System Security Symposium (NDSS). San Diego, USA, 2024: 1-15
- [12] Aditi R, Nasir D, Arun R. MasterPrint: Exploring the vulnerability of partial fingerprint-Based authentication systems. IEEE Transactions on Information Forensics and Security, 2017, 12(9): 2013-2025
- [13] Mohammed A, Ahmed A, Daehun N, David M. Sensor-Based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. IEEE Internet of Things Journal, 2021, 8(1): 65-84
- [14] W3C. Verifiable Credentials Data Model v2.0. W3C Recommendation, 2025
- [15] Wood G. Polkadot: Vision for a heterogeneous multi-chain framework. White Paper, 2023
- [16] Zhou Y, Liu S, Yang Y, et al. Lattice-Based dynamic decentralized anonymous credential scheme supporting batch verification. Computer Standards & Interfaces, 2026, 95:104039
- [17] Bithin A, Pawel S, Tien T, et al. Decentralized identity authentication with auditability and privacy. Algorithms, 2023, 16(1): 4
- [18] Lorenzo P, Luigi M, Federico D, et al. A zero-knowledge proof federated learning on DLT for healthcare data. Journal of Parallel and Distributed Computing, 2025, 196: 104992
- [19] Bootle J, Chiesa A, Sotiraki K. Lattice-Based succinct arguments for NP with polylogarithmic-Time verification// Proceedings of the Advances in Cryptology-CRYPTO 2023. Santa Barbara, USA, 2023: 227-251
- [20] Yuan Q, Liu M L, Shao Y, et al. Identity authentication scheme for medical system based on CP-ABE and Schnorr zero-knowledge proof. Journal of Qiqihar University (Natural Science Edition), 2024, 40(5): 16-23(in Chinese)  
(袁琪, 刘美玲, 邵月等. 基于CP-ABE与Schnorr零知识证明的医疗系统身份认证方案. 齐齐哈尔大学学报(自然科学版), 2024, 40(5): 16-23)
- [21] Zhang Y, Mo X L. Identity authentication mechanism based on blockchain and zero-knowledge proof. Journal of Tianjin University of Technology, 2024, 40(6): 110-116(in Chinese)  
(张杨, 莫秀良. 基于区块链和零知识证明的身份认证机制. 天津理工大学学报, 2024, 40(6): 110-116)
- [22] Ma F Q, Xu Z, Song G X. Zero-knowledge based multi-entity joint identity authentication algorithm. Computer Technology and Development, 2023, 33(11): 113-118(in Chinese)  
(麻付强, 徐峥, 宋桂香. 基于零知识的多实体联合身份认证算法. 计算机技术与发展, 2023, 33(11): 113-118)
- [23] Wang Z, Huang J, Miao K, et al. Lightweight zero-knowledge authentication scheme for IoT embedded devices. Computer Networks, 2023, 236: 110021
- [24] Yang Y, Lu Z, Zeng J, et al. Falic: An FPGA-Based multi-scalar multiplication accelerator for zero-knowledge proof. IEEE Transactions on Computers, 2024, 73(12): 2791-2804
- [25] Liu Y Z, et al. SS-DID: A secure and scalable Web3 decentralized identity. IEEE Internet of Things Journal, 2024, 11(15): 25694-25705
- [26] Naik N, Paul J. uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain//Proceedings of the IEEE

- International Symposium on Systems Engineering. Vienna, Austria, 2020: 1-6
- [27] European Parliament and Council. Regulation (EU) 2024/1183 amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union, 2024. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj>
- [28] Ethereum Foundation. Zero-knowledge rollups. Ethereum.org Documentation, 2024. <https://ethereum.org/en/developers/docs/scaling/zk-rollups/>
- [29] Luke P, Joshua F, Hector M, Jose L. PlonkUP: Reconciling PlonK with plookup. Cryptology ePrint Archive, Report 2023/5678, 2023
- [30] Claudy P, Samuel P. RLAAuth: A risk-based authentication system using reinforcement learning. IEEE Access, 2023, 11: 61129-61143
- [31] Amrita R, Chuan G, Somesh J, Laurens V. EIFFeL: Ensuring integrity for federated learning//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York, USA, 2535-2549
- [32] Li W, Zhang Z, Zhou Z, et al. An overview on succinct non-interactive zero-knowledge proofs. Journal of Cryptologic Research. 2022, 9(3): 379-447. DOI:10.13868/j.cnki.jcr.000525 (in Chinese)  
(李威翰, 张宗洋, 周子博等. 简洁非交互零知识证明综述. 密码学报, 2022, 9(3): 379-447. DOI:10.13868/j.cnki.jcr.000525)
- [33] Torben P. Non-interactive and information-theoretic secure verifiable secret sharing//Proceedings of the Advances in Cryptology-CRYPTO. Santa Barbara, USA, 1991: 129-140
- [34] Amos F, Adi S. How to prove yourself: Practical solutions to identification and signature problems//Proceedings of the Advances in CRYPTO. Santa Barbara, USA, 1986: 186-194

### 附录 1. 式(4)的推导过程

我们要证明  $\cos(f, f^*) > a$  等价于式(4)是否成立:

证明.

$$\because d(\langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle) + \alpha \leq (d+1)B$$

$$\therefore d(\langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle) \leq (d+1)B - \alpha$$

$$\because \alpha \leq B$$

$$\therefore d(\langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle) \leq (d+1)B - \alpha \leq d \cdot B$$

$$\because d \geq B > 0$$

$$\therefore \langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle \leq B$$

$\because$  所有的操作是在正整数域  $\mathbb{N}_p$  上进行的

$$\therefore 0 < \langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle \leq B$$

$$\because \langle \mathbf{pk}_i, \mathbf{sk}_i \rangle = \cos(\mathbf{pk}_i, \mathbf{sk}_i) \cdot \|\mathbf{pk}_i\|_2 \cdot \|\mathbf{sk}_i\|_2,$$

$$\langle \mathbf{sk}_i, \mathbf{sk}_i \rangle = \|\mathbf{sk}_i\|_2^2$$

$$\therefore 0 < (\cos(\mathbf{pk}_i, \mathbf{sk}_i) \cdot \|\mathbf{pk}_i\|_2 \cdot \|\mathbf{sk}_i\|_2)^2 - b \|\mathbf{sk}_i\|_2^2 \leq B$$

$$\because b = a^2 \langle \mathbf{pk}_i, \mathbf{pk}_i \rangle$$

$$\therefore 0 < \cos(\mathbf{pk}_i, \mathbf{sk}_i)^2 - a^2 \leq \frac{B}{\|\mathbf{pk}_i\|_2^2 \|\mathbf{sk}_i\|_2^2}$$

$$\because \forall j(\mathbf{sk}_i)_j \in [0, 1], j \leq \log_2 p$$

$$\therefore \|\mathbf{sk}_i\|_2^2 \leq \log_2 2p$$

$$\because B = (1 - a^2) \langle \mathbf{pk}_i, \mathbf{pk}_i \rangle \log_2 2p,$$

$$\therefore \frac{B}{\|\mathbf{pk}_i\|_2^2 \|\mathbf{sk}_i\|_2^2} = \frac{(1 - a^2) \langle \mathbf{pk}_i, \mathbf{pk}_i \rangle \log_2 2p}{\|\mathbf{pk}_i\|_2^2 \|\mathbf{sk}_i\|_2^2} =$$

$$\frac{(1 - a^2) \log_2 2p}{\|\mathbf{sk}_i\|_2^2} \geq (1 - a^2)$$

$$\therefore 0 < \cos(\mathbf{pk}_i, \mathbf{sk}_i)^2 - a^2 \leq 1 - a^2$$

$$\therefore a^2 < \cos(\mathbf{pk}_i, \mathbf{sk}_i)^2 \leq 1$$

$$\therefore a < \cos(\mathbf{pk}_i, \mathbf{sk}_i)$$

$$\because \mathbf{pk}_i = f^* \cdot \text{Prf}_i(\zeta), \mathbf{sk}_i = f \cdot \text{Prf}_i(\zeta)$$

$$\therefore \cos(\mathbf{pk}_i, \mathbf{sk}_i) = \cos(f, f^*)$$

$$\therefore a < \cos(\mathbf{pk}_i, \mathbf{sk}_i) = \cos(f, f^*)$$

至此证明了

$$d(\langle \mathbf{pk}_i, \mathbf{sk}_i \rangle^2 - b \langle \mathbf{sk}_i, \mathbf{sk}_i \rangle) + \alpha \leq (d+1)B$$

等价于  $a < \cos(f, f^*)$

证毕.



**LU Zhi**, Ph.D. candidate. His research interests include cryptography, zero-knowledge proof, anonymous credentials and Industrial Internet of Things security.

**NIE He-Wang**, Ph.D., associate professor. His main research field is artificial intelligence security.

**LUO Ting**, Ph.D., lecturer. Her main research area is applied cryptography.

**LU Song-Feng**, Ph.D., professor. His research interests include network security, artificial intelligence security, and industrial Internet security.

**SHEN Ren-Fei**, Ph.D. candidate. His research interests focus on applied cryptography and distributed system security.

## Background

This research addresses a critical challenge in the domain of privacy-preserving identity authentication, with a focus on developing anonymous and unlinkable multi-factor authentication protocols suitable for deployment in zero-trust network environments. As modern systems increasingly adopt zero-trust architecture (ZTA), authentication mechanisms must not only enforce continuous verification, but also preserve user privacy across repeated access attempts. In such settings, identity verification often relies on sensitive factors such as government-issued IDs and biometric data. However, conventional methods typically require the prover to disclose these attributes in plaintext, leading to privacy risks and vulnerability to cross-session correlation attacks.

While generic zero-knowledge proof (ZKP) frameworks—such as zk-SNARKs, Bulletproofs, and STARKs—offer strong cryptographic guarantees, their high computational complexity often makes them impractical for real-time, high-frequency authentication. Similarly, although anonymous credential systems and privacy-preserving biometric schemes have made progress, few existing solutions achieve a strong balance between efficiency, anonymity, and unlinkability under a multi-factor and zero-trust model.

To bridge this gap, this paper proposes a lightweight authentication protocol that instantiates Sigma-protocol-based

zero-knowledge proofs for two common identity factors: national ID numbers and facial features. A key contribution is the introduction of a mutual distrust model, where not only does the verifier distrust the prover, but the prover also refuses to disclose raw identity information to an untrusted verifier. Instead, each authentication is performed through a randomized, encrypted proof that ensures session-level unlinkability while maintaining correctness and security.

This research is supported by The 2023 Changsha City Major Science and Technology Project of “Challenge and Response” (Project Number: kq2503009). The project targets the development of secure and trustworthy open industrial numerical control (CNC) systems, and this paper addresses one of its key technical challenges: achieving efficient and privacy-preserving identity authentication between heterogeneous devices under a zero-trust architecture. The goal is to enable secure inter-device communication without reliance on pre-established trust or centralized credentials, ensuring both robustness and scalability in complex industrial control environments.

The solutions presented in this paper build directly on these foundations and contribute a deployable, high-efficiency protocol component to the broader zero-trust identity infrastructure envisioned in the national project.