计算机系统网络和电信 2025 (1) 7
ISSN: 2661-3719(Print); 2661-3727(Online)

基于零知识证明的数字可信身份验证技术研究

李春勇
上海亘岩网络科技有限公司　上海　200000

摘　要：随着信息安全需求的不断增加，传统的身份验证方式面临着较大的安全隐患和隐私泄露问题。基于零知识证明的数字可信身份验证技术被提出作为一种解决方案，本研究旨在探讨这种新兴技术的理论框架、实现方法及其在实际应用中的性能表现，通过构建一个基于零知识证明的身份验证模型，本文设计并实施了模拟仿真实验，考察了验证时间、通信开销和抗攻击能力等关键指标。实验结果表明，随着用户数量的增加，验证时间和通信开销呈现线性增长，而系统在防范中间人攻击和重放攻击时表现优异，防御成功率高达 95% 以上。

关键词：零知识证明；数字身份验证；信息安全；隐私保护

1. 引言

随着数字化技术的快速发展，数字身份认证作为信息安全中的重要组成部分，已成为各类在线交易、智能设备交互、金融应用等领域的关键技术之一。传统的身份验证方式，如基于密码的验证，存在着被窃取、篡改等安全隐患，尤其在面对复杂的网络攻击时其脆弱性愈加突出。为了有效解决这些问题，基于零知识证明（Zero-Knowledge Proof, ZKP）的数字可信身份验证技术应运而生，成为保障隐私和身份安全的重要手段。零知识证明是一种能够在不透露任何其他信息的情况下证明某一断言真实性的密码学方法，在数字身份验证中，零知识证明技术不仅能验证用户身份的真实性，还能在保证隐私性的同时防止身份信息泄露，极大地提高了系统的安全性和用户的隐私保护。

2. 零知识证明技术原理

2.1 零知识证明的基本原理

零知识证明是一种交互式证明协议，旨在证明某个陈述的真实性，同时不向验证者泄露任何关于陈述本身的信息。根据其基本原理，零知识证明必须满足三个重要属性：完备性、可靠性和零知识性。

1. 完备性（Completeness）：如果陈述为真，诚实的证明者能够使验证者信服。

2. 可靠性（Soundness）：如果陈述为假，骗子证明者不能成功地说服验证者。

3. 零知识性（Zero-Knowledge）：证明过程中，验证者不能获得任何关于陈述本身的额外信息，除了其真实性。

在数字身份验证中，零知识证明技术应用于以下情境：验证者希望确认证明者的身份，而证明者只需提供一个证明，表明自己具有某些信息或属性，而无需透露具体的身份信息，通过零知识证明，证明者不仅能够验证自己的身份，还能确保在整个过程中其私密信息不被泄露。

2.2 零知识证明协议与算法

零知识证明协议通常由一系列的交互步骤组成，核心思想是通过多轮交互，证明者能够使验证者确信某个声明为真。最常见的零知识证明协议包括交互式零知识证明和非交互式零知识证明。其中交互式零知识证明依赖于证明者和验证者之间的多次信息交换，而非交互式零知识证明则通过单次消息传递来完成证明过程。

在数字身份验证的场景中，基于零知识证明的验证协议一般包括以下几个步骤：

1. 初始化阶段：证明者和验证者通过某种协议建立一个信任关系，定义验证的目标。

2. 挑战阶段：验证者向证明者发送一个随机生成的挑战，这通常是通过某种函数（如哈希函数）来生成的。

3. 响应阶段：证明者根据其掌握的私密信息，对挑战进行响应，证明自己具备验证所需的身份信息或属性。

4. 验证阶段：验证者使用预定义的规则，验证响应的有效性，从而确认证明者身份的真实性。

常见的零知识证明算法包括 zk-SNARKs（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）和 zk-STARKs（Zero-Knowledge Scalable Transparent Argument

of Knowledge ）。具体到身份验证，zk-SNARKs 通过确保较短的证明和验证时间，适用于资源受限的设备，而 zk-STARKs 则在透明性和抗量子攻击方面表现突出。

3. 基于零知识证明的数字身份验证模型

3.1 模型设计与构建

在基于零知识证明的数字身份验证系统中，模型设计的核心目标是确保在不泄露任何私密信息的前提下，能够准确、有效地验证用户身份，本文提出了一种以零知识证明为核心的数字身份验证框架，包含验证用户身份、信息交互、隐私保护等几个关键模块。

身份信息模型：用户身份由一组私密信息（如密码、私钥或生物特征）表示。零知识证明模型通过证明者（用户）和验证者（系统）之间的交互，确保只有正确的证明者能够通过身份验证，假设证明者持有某个秘密信息 SS，需要通过零知识证明证明 S 的真实性，而不暴露 S 本身。

身份验证协议：根据零知识证明协议，设计了一个多轮交互的验证过程。在每轮交互中，证明者根据其秘密信息 S 和随机生成的挑战 C，生成相应的响应 RR。验证者根据挑战 C 和响应 R 判断验证是否成功。

身份验证的过程可描述为如下数学模型：

$$\text{Verification}(S,C) = \text{Check}(f(S,C),R) \quad (1)$$

f(S,C) 是验证过程中的挑战响应函数，R 是证明者的响应，验证者通过对 f(S,C) 和 R 的计算来判断身份验证是否通过。

3.2 零知识证明在数字身份验证中的应用框架

本研究提出的数字身份验证模型基于零知识证明的协议，构建了一个分层的应用框架，以适应不同的身份验证需求。框架主要由以下几个模块组成：

1. 身份信息存储模块：系统将用户身份的敏感信息（如加密后的密码、指纹等）以安全的方式存储在可信环境中，只有授权的验证者能够访问。

2. 零知识证明生成模块：当用户请求身份验证时，零知识证明生成模块根据用户的密钥和身份信息生成相应的零知识证明。证明者通过使用私密信息和公开的挑战 CC，生成响应 RR。

3. 身份验证模块：身份验证模块通过与用户的交互，使用零知识证明协议核实用户身份的真实性。在验证过程中，验证者根据预定义的规则判断验证是否通过。

4. 安全与隐私保护模块：系统通过加密技术和隐私保护机制，确保用户身份信息在验证过程中的安全性，在不泄露任何敏感信息的情况下，验证者能够确定用户身份的有效性。

5. 零知识证明在数字身份验证中的应用框架的核心目标是平衡验证的效率与隐私保护，以适应现代互联网环境中对安全性与效率的双重需求。

3.3 身份信息隐私保护机制

在数字身份验证过程中，隐私保护是一个至关重要的考虑因素。传统的身份验证方式可能会导致用户信息泄露，增加了被攻击和滥用的风险。基于零知识证明的身份验证技术通过以下几个方面有效地保障用户隐私：

1. 信息不可见性：在验证过程中，验证者只能通过零知识证明验证用户的身份，而无法获得用户的任何敏感信息（如密码或个人数据）。验证者仅知晓用户身份的真实性，而不知晓用户的私密信息。

2. 匿名性：零知识证明可以实现身份验证过程中的匿名性，确保在不泄露用户真实身份的情况下验证其身份，通过使用加密和零知识证明算法，用户可以在不同的场景中进行匿名认证，保护其隐私。

3. 抗追踪性：通过零知识证明技术，用户可以在不同的身份验证过程中使用不同的证明信息，从而有效避免了身份信息的追踪和滥用。

4. 在实现这些隐私保护机制时，本文基于以下数学公式进行建模，描述零知识证明与隐私保护的关系：

设用户的身份信息为 II，证明者持有的秘密信息为 SS，零知识证明过程中的挑战为 CC，响应为 RR。验证者的身份验证过程可以表示为：

$$\text{Verification}(C,R) \Rightarrow \text{Valid}(S) \text{ where } \rightarrow \text{Valid}(S) \text{ implies the correctness of the secret information.} \quad (2)$$

在保护用户隐私时，验证者仅通过验证 C 和 R，而不访问具体的私密信息 S：

$$\text{Privacy Protection}(S,C,R) \Rightarrow \text{Exposure}(S) \text{ where } \rightarrow \text{Exposure}(S) \text{ ensures that S remains hidden.} \quad (3)$$

4. 模拟仿真实验设计与分析

4.1 实验场景与实验平台

为了评估基于零知识证明的数字可信身份验证技术的性能，本研究设计了一系列模拟实验。实验场景模拟了现代互联网环境下，多个用户通过零知识证明协议与系统进行身份验证的过程。实验平台基于 Python 编程语言开发，利用

相关零知识证明算法库（如 zk–SNARKs）进行实现，并在虚拟化环境中进行多次实验验证。

1. 实验场景设计：本实验设计了两个主要场景：一是低延迟、高频率的身份验证场景，二是高负载、低频次的身份验证场景。实验中设置多个用户通过零知识证明协议依次向系统发起身份验证请求，模拟了各种实际情况。

2. 实验平台配置: 本实验在以下硬件和软件平台上进行:

硬件配置：Intel i7 8 核处理器，16GB 内存，500GB SSD 存储

软件配置：Python 3.9，zk–SNARKs 库，Ubuntu 20.04 操作系统，虚拟机配置

4.2 实验步骤与零知识证明协议的实现

实验的步骤包括以下几个主要环节：

1. 身份信息准备：生成每个用户的密钥对，包括公钥和私钥。密钥对的生成使用了加密算法（如 RSA、ECC）与零知识证明算法相结合。

2. 零知识证明协议实现：基于用户的私密信息和系统设定的挑战函数，利用零知识证明协议（例如 zk–SNARKs）来完成身份验证过程。在每个验证请求中，系统会发起一个随机挑战，并要求用户基于其私密信息生成响应。

3. 实验过程执行：模拟多个用户同时向系统发起身份验证请求。每次验证过程中，用户通过零知识证明生成验证响应，系统根据相应的验证规则进行身份验证。

4. 数据收集与分析：在每次验证完成后，收集包括验证时间、通信开销、抗攻击能力等指标，并对这些数据进行分析。

5. 实验结果与指标评估

5.1 验证时间

验证时间是指从用户发起身份验证请求到系统完成验证所需的总时间，该指标直接影响用户体验，尤其在高频率身份验证场景中，验证时间的长短至关重要。实验中，验证时间在不同用户数量和不同挑战难度下有所变化。

表 1 验证时间

用户数	平均验证时间 (ms)	最大验证时间 (ms)	最小验证时间 (ms)
10	120	150	100
50	145	180	120
100	180	220	150
200	250	290	210
500	420	460	380

从数据可以看出，随着用户数量的增加，验证时间呈现出线性增长的趋势，由于每增加一个用户，系统需要进行更多的验证交互，随着优化算法（如并行处理）的引入，验证时间的增长可能会得到一定的缓解，通过分析最大和最小验证时间差异，表明不同用户的身份验证请求差异较大，某些高负载情况下会导致验证时间显著增加。

5.2 通信开销

通信开销指的是在每次身份验证过程中，证明者与验证者之间交换的数据量，直接影响网络资源的消耗和系统的响应速度。

表 2 通信开销

用户数	平均通信开销 (KB)	最大通信开销 (KB)	最小通信开销 (KB)
10	18	22	15
50	25	30	20
100	35	40	30
200	55	60	50
500	85	90	80

实验结果表明，随着用户数量的增加，通信开销显著增加，由于身份验证过程中零知识证明协议需要传输多个数据包，且随着验证请求的增加，数据量也相应增加。从数据中可以看出，通信开销与用户数量呈现正相关关系，较高的通信开销可能导致系统在高负载环境下的响应性能降低，减少通信开销，优化数据交换协议是提升系统效率的关键。

5.3 抗攻击能力

抗攻击能力是评估数字身份验证系统在面对各种攻击时，系统能够保持身份验证准确性的能力。此项实验重点评估了基于零知识证明的身份验证系统在面对中间人攻击、重放攻击等网络攻击时的表现。

表 3 抗攻击能力

攻击类型	攻击成功率 (%)	防御成功率 (%)
中间人攻击	5	95
重放攻击	3	97
拒绝服务攻击	10	90
强制破解	15	85

在面对不同类型的攻击时，零知识证明身份验证系统表现出了较强的抗攻击能力，尤其在中间人攻击和重放攻击方面，其防御成功率都达到 95% 以上。在面对拒绝服务攻击和强制破解时，系统的防御能力稍显不足，攻击成功率相对较高。这表明在提高系统防御能力时，需要在计算复杂性和攻击防御之间找到平衡。

6. 结论

本研究探讨了基于零知识证明的数字可信身份验证技术，提出了一种新的身份验证模型，并通过实验验证了其在实际应用中的可行性与性能，通过零知识证明技术，用户能够在保证隐私性的前提下，安全地验证自己的身份，有效避免了传统身份验证方法中的信息泄露和安全隐患。

实验结果表明，随着用户数量的增加，验证时间和通信开销呈线性增长，零知识证明技术依然能够在合理的范围内保证系统的高效性。尤其在面对中间人攻击和重放攻击时，系统表现出了较强的抗攻击能力，防御成功率达到 95% 以上，面对拒绝服务攻击和强制破解时，系统的防御能力有所下降，这表明在未来的研究中，优化抗攻击策略是提升系统安全性的关键方向。

基于零知识证明的数字身份验证技术为信息安全领域提供了新的解决思路，其在保护用户隐私和提高身份验证效率方面具有显著优势。未来的研究可在降低通信开销、提升系统抗攻击能力、优化验证效率等方面进一步加强，以推动其在更广泛的应用场景中的落地与推广。

参考文献：

[1] 张杨 , 莫秀良 . 基于区块链和零知识证明的身份认证机制 [J]. 天津理工大学学报 , 2024(3).

[2] 王天明 . 金融交易服务中基于零知识证明的区块链隐私保护机制研究 [D]. 中央财经大学 ,2022.

[3] 高创创 , 刘晓飞 . 一种基于零知识证明的安全身份验证方法 .CN202211363644.8[2025-01-19].

[4] 邓春华 . 基于零知识证明技术的 Range Proof 技术及其应用研究 [D]. 西南交通大学 ,2020.

[5] 焦志伟 , 吴正豪 , 徐亦佳 , 等 . 基于隐私保护的分布式数字身份认证技术研究及实践探索 [J]. 信息通信技术与政策 , 2024, 50(1):59-66.

作者简介：

李春勇 (1977.04—) , 女 , 汉族 , 河南汝南人 , 本科学历 , 任职于上海亘岩网络科技有限公司，研究方向：数字可信技术研发与应用。