基于零知识证明的轨道交通闸机身份认证协议设计

吴森林
通号通信信息集团有限公司　北京　100070

摘　要：随着轨道交通的快速发展，闸机身份认证的安全性与效率愈发关键。传统认证方式存在信息泄露风险高、隐私保护不足等问题，难以满足现代轨道交通智能化、安全化运营需求。零知识证明技术凭借无需泄露敏感信息即可完成验证的特性，为轨道交通闸机身份认证提供了创新解决方案。本文深入分析当前轨道交通闸机身份认证的现状与面临的挑战，阐述零知识证明的原理及在身份认证中的优势，从协议设计目标、参与方及交互流程、核心算法设计、安全性与性能分析等方面详细探讨基于零知识证明的轨道交通闸机身份认证协议设计，并对协议实施过程中面临的技术实现、系统兼容、用户接受度等挑战提出应对策略，旨在提升轨道交通闸机身份认证的安全性与隐私保护水平，推动轨道交通智能化发展。

关键词：零知识证明；轨道交通闸机；身份认证协议；隐私保护；智能交通

1 引言

轨道交通作为城市公共交通的重要组成部分，具有大运量、高效率、低碳环保等优势，在缓解城市交通拥堵、促进城市发展中发挥着关键作用。随着城市化进程的加速和轨道交通网络的不断扩张，越来越多的乘客选择轨道交通出行，这对轨道交通运营的安全性和便捷性提出了更高要求。闸机作为乘客进出轨道交通站点的关键设备，其身份认证系统的安全性直接关系到乘客的人身财产安全和轨道交通的正常运营秩序。传统的轨道交通闸机身份认证方式，如基于磁卡、二维码的认证，主要依赖于明文信息的传输与验证，存在信息易被窃取、篡改，用户隐私难以保障等问题。零知识证明技术作为一种新型密码学技术，能够在不泄露任何有用信息的前提下，实现对用户身份的有效验证，为解决轨道交通闸机身份认证中的安全与隐私问题提供了新的思路。研究基于零知识证明的轨道交通闸机身份认证协议设计，对提升轨道交通运营安全水平、增强乘客出行体验具有重要的现实意义。

2 轨道交通闸机身份认证现状与面临的挑战

2.1 轨道交通闸机身份认证现状

在当前的社会背景下，我国轨道交通系统在身份认证方面已经发展出多种方式，以适应不同场景和用户需求。首先，基于磁卡的认证方式是较为传统的一种，乘客通过在闸机刷卡来完成身份验证和进出站的操作。这种方式的优点在于技术成熟，实施成本相对较低，因此在轨道交通系统中得到了广泛应用。然而，磁卡认证方式也存在一定的安全隐患，磁卡容易被复制和伪造，一旦卡片丢失，就存在被盗刷的风险，给乘客的财产安全和信息安全带来威胁。其次，基于二维码的认证方式是随着移动互联网的发展而兴起的一种新型认证方式。乘客通过手机APP生成二维码，闸机通过扫描二维码来完成身份认证。这种方式的优点在于使用便捷，乘客无需携带实体卡片，只需一部手机即可完成进出站操作。然而，二维码在传输过程中可能被截获和篡改，存在信息泄露的隐患，给乘客的信息安全带来风险。再次，基于生物特征的认证方式，如指纹识别、人脸识别等，是近年来兴起的一种高科技认证方式。这种方式的优点在于具有较高的安全性和便捷性，乘客无需携带任何实体卡片或手机，只需通过生物特征识别即可完成进出站操作。然而，生物特征采集设备成本较高，且识别准确率受环境因素影响较大，如光线、角度等，给乘客的使用体验带来一定的影响。

总体而言，现有的轨道交通闸机身份认证方式在安全性、隐私保护和用户体验方面存在一定的局限性，难以满足日益增长的轨道交通运营需求。随着科技的不断发展和用户需求的不断提升，轨道交通闸机身份认证方式需要不断创新和改进，以提高安全性和便捷性，为乘客提供更好的出行体验。

2.2 面临的挑战

在安全性方面，传统的认证方式依赖于明文信息传输和存储，一旦信息泄露，将导致乘客身份信息被盗用、账户资金损失等风险。例如，基于磁卡的认证系统，若磁卡信息被非法读取和复制，攻击者可使用复制卡非法进出站，给轨道交通运营带来安全隐患。基于二维码的认证方式，二维码在传输过程中可能被黑客截获并伪造，造成认证失效，给乘客的出行带来不便。

在隐私保护方面，现有的认证方式往往需要收集大量用户个人信息，如身份证号、手机号等，这些信息在存储和传输过程中面临泄露风险，侵犯用户隐私。随着个人信息保护意识的不断提高，用户对隐私保护的需求也越来越强烈，因此，轨道交通闸机身份认证方式需要加强对用户个人信息的保护，以保障用户的隐私权益。

此外，随着轨道交通智能化发展，不同城市、不同线路之间的闸机系统需要实现互联互通，传统认证方式难以满足跨区域、跨系统认证的需求，增加了运营管理的复杂性。因此，轨道交通闸机身份认证方式需要不断创新和改进，以适应轨道交通智能化发展的需求，提高运营管理效率，为乘客提供更加便捷、安全的出行体验。

3 零知识证明原理及在身份认证中的优势

3.1 零知识证明原理

零知识证明是一种先进的密码学技术，其核心特点在于证明者能够在完全不向验证者泄露任何有用信息的前提下，成功使验证者确信某个特定论断的真实性。零知识证明系统通常由三个基本部分构成：证明者、验证者以及在某些特定场景下可能存在的可信第三方（尽管在某些情况下这一角色可以被省略）。证明者掌握着某个关键的秘密信息，通过与验证者进行一系列精心设计的交互过程，能够在不暴露该秘密信息的情况下，向验证者充分证明自己确实知晓该秘密信息。以经典的“洞穴问题”为例，假设一个洞穴拥有两个入口A和B，并且中间设有一道只能通过特定钥匙才能开启的门。证明者持有这把钥匙，而验证者希望确认证明者是否真的知道如何打开这扇门，但又不想让证明者透露任何关于钥匙的具体信息。于是，证明者进入洞穴后，验证者在洞穴外随机选择入口A或B，并要求证明者从所选入口出来。如果证明者每次都能按照验证者的要求，从指定的入口顺利走出，经过多次这样的验证过程后，验证者便可以确信证明者确实掌握了打开门的钥匙。而在此过程中，证明者自始至终都没有向验证者透露任何关于钥匙的具体信息。

3.2 在身份认证中的优势

将零知识证明技术应用于轨道交通闸机系统的身份认证，展现出诸多显著的优势。首先，该技术能够有效保护用户的隐私安全。在身份认证的过程中，用户无需向闸机系统提供任何敏感的个人信息，例如身份证号码、银行卡号码等，仅需通过零知识证明协议来证明自己的合法身份，从而大大降低了用户个人信息泄露的风险。其次，零知识证明协议基于高度复杂的密码学算法，具备极强的抗攻击能力，能够有效抵御诸如重放攻击、中间人攻击等常见的网络攻击手段，确保身份认证过程的高度安全性。此外，零知识证明技术还具有良好的通用性和强大的扩展性，便于与现有的轨道交通闸机系统进行无缝集成，支持跨区域、跨系统的身份认证需求，充分满足轨道交通行业智能化发展的迫切需求。

4 基于零知识证明的轨道交通闸机身份认证协议设计

4.1 协议设计目标

本协议的设计目标主要涵盖以下三个核心方面：首先，确保身份认证过程的安全性，通过采用先进的加密技术和多重验证机制，有效防止非法用户通过伪造身份信息的方式非法通过闸机，同时具备强大的防御能力，能够抵御包括但不限于网络钓鱼、数据篡改、暴力破解等各类网络攻击手段，保障系统的整体安全性和稳定性；其次，严格保护用户隐私，在身份认证的各个环节中，采取严格的数据加密和访问控制措施，确保用户的敏感信息如身份证号、银行卡信息等不会在认证过程中被泄露或被未经授权的第三方获取，从而维护用户的个人隐私权益；最后，显著提高认证效率，通过优化认证流程和引入高效的算法，确保乘客在通过闸机时能够享受到快速、便捷的认证服务，大幅减少因认证过程繁琐而导致的排队等待时间，提升乘客的整体出行体验。此外，本协议还应具备良好的兼容性，能够与现有的轨道交通闸机系统和票务管理系统实现无缝对接，无需进行大规模的系统改造即可顺利集成，从而便于在实际应用中进行推广和普及，确保协议的实用性和广泛适用性。

4.2 协议参与方及交互流程

协议参与方包括乘客（证明者）、闸机（验证者）和轨道交通运营中心服务器。交互流程如下：乘客靠近闸机时，闸机向乘客设备（如手机APP）发送认证请求；乘客设备接收到请求后，生成包含零知识证明信息的响应消息，并发送给闸机；闸机接收到响应消息后，对零知识证明信息进行初步验证，若验证通过，则将相关信息发送给轨道交通运营中心服务器；服务器对信息进行二次验证，验证通过后向闸机发送授权指令，闸机接收到授权指令后开启闸门，允许乘客通过。在整个交互过程中，乘客无需向闸机和服务器透露任何敏感身份信息，仅通过零知识证明完成身份认证。

5 协议实施面临的挑战及应对策略

5.1 技术实现挑战及应对

基于零知识证明的身份认证协议，其核心在于运用复杂的密码学算法和先进的通信技术，以确保身份认证的安全性和隐私性。然而，在实际的技术实施过程中，我们面临着一系列的技术难题。首先，零知识证明算法

本身的计算复杂度较高，这对乘客所使用的设备和轨道交通闸机的计算能力提出了较高的要求。在资源受限的移动设备上，如何高效地执行这些算法，成为了一个亟待解决的问题。其次，协议的通信流程设计需要兼顾信息传输的准确性和及时性，以确保乘客能够顺畅地通过闸机，而不造成拥堵。

为了应对这些挑战，我们可以采取一系列的技术措施。首先，可以通过硬件加速技术来提升算法的计算效率。例如，在轨道交通闸机中集成专用的密码芯片，利用硬件的高效处理能力来加速算法的执行。同时，可以优化通信协议，采用轻量级的通信框架，减少信息传输的量，从而提高通信的效率。此外，我们还可以加强与科研机构和技术企业的合作，共同研究和攻克技术难题，确保身份认证协议的稳定运行。

5.2 系统兼容挑战及应对

在现有的轨道交通系统中，闸机系统和票务管理系统的种类繁多，各个系统的架构和功能特点各不相同。因此，基于零知识证明的身份认证协议在实施过程中，需要解决与这些不同系统的兼容问题。为了实现系统之间的兼容，我们需要制定统一的接口标准和数据格式，以确保协议能够与现有的系统进行无缝对接。在协议的设计过程中，我们需要充分考虑现有系统的架构和功能特点，采用模块化的设计理念，以便于对现有的系统进行升级改造。同时，我们还需要建立兼容性测试平台，对协议与不同系统的兼容性进行全面和深入的测试，以便及时发现和解决兼容性问题。

5.3 用户接受度挑战及应对

零知识证明技术作为一种相对较新的技术，其复杂性和专业性可能会让普通用户感到难以理解，从而对其安全性和可靠性产生疑虑，这可能会影响用户的接受度。为了提高用户对零知识证明技术和基于此技术的身份认证协议的接受度，我们需要加强对这些技术的宣传和推广。通过通俗易懂的方式，向用户介绍零知识证明技术的原理和优势，以及本协议如何保护他们的隐私和安全，从而消除用户的疑虑。在协议的应用初期，我们可以提供便捷的用户支持服务，及时解决用户在使用过程中遇到的问题。此外，我们还可以通过提供优惠政策、奖励机制等方式，鼓励用户使用新的认证方式，提高用户的参与度。

6 结论

基于零知识证明的轨道交通闸机身份认证协议设计为解决传统认证方式存在的安全和隐私问题提供了有效途径。通过合理设计协议目标、参与方及交互流程、核心算法，并对协议的安全性和性能进行分析，该协议能够在保障用户隐私的前提下，实现高效、安全的身份认证。尽管在协议实施过程中面临技术实现、系统兼容、用户接受度等挑战，但通过采取相应的应对策略，可以逐步克服困难，推动协议的实际应用。未来，随着密码学技术的不断发展和轨道交通智能化水平的提升，基于零知识证明的身份认证技术将在轨道交通领域得到更广泛的应用，为轨道交通的安全、便捷运营提供有力保障。

参考文献

[1]王剑,杨国栋.轨道交通闸片材料铜粉与钨粉的磨损特性及应用研究[J].世界有色金属,2025,(05):19-21.

[2]宋周轩,易成.基于AnyLogic仿真的轨道交通客流组织优化[J].人民公交,2024,(24):170-172.DOI:10.16857/j.cnki.cn11-5903/u.2024.24.051.

[3]李阳,邓胜江,张兆龙.多制式轨道交通融合的检票闸机设计与应用[J].铁路计算机应用,2024,33(07):61-64.

[4]石琦,方勇,胡华,等.基于监控视频数据的城市轨道交通车站闸机设施处行人停滞行为谱特征研究[J].城市轨道交通研究,2024,27(03):150-154+159.DOI:10.16037/j.1007-869x.2024.03.027.

[5]才溢,周然,杜恬恬,等.轨道交通闸机通过能力差异性影响因素研究[J].交通工程,2024,24(02):1-7.DOI:10.13986/j.cnki.jote.2024.02.001.