基于零知识证明的匿名电子投票系统设计与实现

沈平健

（武汉大学国家网络安全学院，湖北 武汉 430072）

摘 要：随着信息技术的飞速发展和数字社会的深度推进，电子投票作为传统纸质投票的数字化替代方案，凭借其高效、便捷、低成本的优势，已广泛应用于各类选举、民意调查、企业决策等场景。然而，传统电子投票系统在匿名性、可验证性、安全性等核心需求上存在显著短板，难以同时兼顾选民隐私保护与投票过程的公开透明，导致选民对系统的信任度不足，限制了电子投票的进一步普及与推广。零知识证明（Zero-Knowledge Proof, ZKP）作为一种能够在不泄露任何私密信息的前提下，证明某个陈述真实性的密码学技术，为解决匿名电子投票中的核心矛盾提供了全新的技术路径。本文围绕基于零知识证明的匿名电子投票系统展开深入研究，结合密码学、计算机网络、软件工程等多学科理论与技术，设计并实现了一套兼具匿名性、可验证性、安全性与高效性的电子投票系统。首先，本文系统梳理了电子投票系统的发展现状与核心需求，深入分析了传统电子投票系统在隐私保护、投票安全、结果验证等方面存在的突出问题，明确了零知识证明技术在解决这些问题中的核心优势与应用价值。其次，详细阐述了零知识证明的核心原理、分类及常用方案，对比分析了不同零知识证明方案的性能特点与适用场景，并结合同态加密、盲签名等密码学工具，构建了系统的技术支撑体系，为系统设计奠定了坚实的理论基础。在此基础上，本文提出了一套轻量级的匿名电子投票系统架构，明确了系统的模块划分、各模块的功能职责以及模块间的交互关系，设计了完整的数据流与业务流程，确保系统运行的高效性与连贯性。针对系统的核心功能，包括选民身份认证与注册、投票生成与加密、匿名投票提交与存储、高效计票与结果验证等，进行了详细的设计与优化，引入零知识证明技术实现选民身份的匿名验证、投票行为的合法性证明，结合同态加密技术实现投票结果的隐私保护与高效聚合，利用盲签名技术进一步强化选民的匿名性保障。为验证系统的有效性与可行性，本文基于主流的开发语言与框架，完成了系统的原型实现，并搭建了完善的测试环境，从功能测试、性能测试、安全性测试三个维度对系统进行了全面测试。测试结果表明，本文设计实现的基于零知识证明的匿名电子投票系统，能够有效保障选民的匿名性，确保投票过程的不可篡改性与投票结果的可验证性，同时在投票延迟、吞吐量、资源消耗等性能指标上表现优异，能够满足小型选举场景的实际应用需求。最后，本文总结了研究过程中取得的成果与存在的不足，结合当前密码学技术的发展趋势，提出了未来的改进方向，包括系统扩展性优化以支持大规模选举场景，结合量子安全密码学技术增强系统的长期安全性，为后续相关研究与应用提供了参考与借鉴。本文的研究工作不仅解决了传统电子投票系统的核心痛点，丰富了零知识证明技术在隐私保护领域的应用场景，也为匿名电子投票系统的设计与实现提供了一种可行的技术方案，具有重要的理论意义与实际应用价值。

关键词：零知识证明；匿名电子投票；同态加密；盲签名；隐私保护；可验证性；安全性

中图分类号：TP309.7 **文献标识码：**A **文章编号：**3106-2709（2025）06-0001-12

DOI：10.62022/NCAR.issn3106-2709.2025.06.001

Design and Implementation of Anonymous Electronic Voting System Based on Zero-Knowledge Proof

Shen Pingjian

(School of Cyber Security, Wuhan University, Wuhan 430072, Hubei, China)

Abstract: With the rapid development of information technology and the in-depth advancement of the digital society, electronic voting, as a digital alternative to traditional paper-based voting, has been widely used in various scenarios such as elections, public opinion surveys, and enterprise decision-making due to its advantages of high efficiency, convenience, and low cost. However, traditional electronic voting systems have significant shortcomings in core requirements such as anonymity, verifiability, and security, making it difficult to balance voter privacy protection and the openness and transparency of the voting process. This leads to insufficient trust of voters in the system and limits the further popularization and promotion of electronic voting. Zero-Knowledge Proof (ZKP), as a cryptographic technology that can prove the authenticity of a statement without revealing any private information, provides a new technical path to solve the core contradictions in anonymous electronic voting.This paper conducts in-depth research on an anonymous electronic voting system based on zero-knowledge

作者简介：沈平健，博士，研究方向为区块链应用。

proof, combining multidisciplinary theories and technologies such as cryptography, computer networks, and software engineering, to design and implement an electronic voting system with anonymity, verifiability, security, and efficiency. Firstly, this paper systematically sorts out the development status and core requirements of electronic voting systems, deeply analyzes the prominent problems existing in traditional electronic voting systems in terms of privacy protection, voting security, and result verification, and clarifies the core advantages and application value of zero-knowledge proof technology in solving these problems.Secondly, it elaborates on the core principles, classification, and common schemes of zero-knowledge proof, compares and analyzes the performance characteristics and applicable scenarios of different zero-knowledge proof schemes, and constructs the technical support system of the system combined with cryptographic tools such as homomorphic encryption and blind signature, laying a solid theoretical foundation for system design. On this basis, this paper proposes a lightweight anonymous electronic voting system architecture, clarifies the module division of the system, the functional responsibilities of each module, and the interaction relationship between modules, and designs a complete data flow and business process to ensure the efficiency and continuity of system operation.For the core functions of the system, including voter identity authentication and registration, vote generation and encryption, anonymous vote submission and storage, efficient vote counting and result verification, detailed design and optimization are carried out. Zero-knowledge proof technology is introduced to realize anonymous verification of voter identity and legality proof of voting behavior; homomorphic encryption technology is combined to realize privacy protection and efficient aggregation of voting results; blind signature technology is used to further strengthen the anonymity guarantee of voters.To verify the effectiveness and feasibility of the system, this paper completes the prototype implementation of the system based on mainstream development languages and frameworks, and builds a complete test environment to conduct comprehensive tests on the system from three dimensions: functional test, performance test, and security test. The test results show that the anonymous electronic voting system based on zero-knowledge proof designed and implemented in this paper can effectively ensure the anonymity of voters, ensure the tamper-proof nature of the voting process and the verifiability of voting results, and at the same time perform excellently in performance indicators such as voting delay, throughput, and resource consumption, which can meet the actual application needs of small-scale election scenarios.Finally, this paper summarizes the achievements and deficiencies in the research process, and puts forward future improvement directions combined with the development trend of current cryptographic technology, including system scalability optimization to support large-scale election scenarios, and combining quantum-safe cryptography technology to enhance the long-term security of the system, providing reference for subsequent related research and applications. The research work of this paper not only solves the core pain points of traditional electronic voting systems, enriches the application scenarios of zero-knowledge proof technology in the field of privacy protection, but also provides a feasible technical scheme for the design and implementation of anonymous electronic voting systems, which has important theoretical significance and practical application value.

Keywords: zero-knowledge proof; anonymous electronic voting; homomorphic encryption; blind signature; privacy protection; verifiability; security

1 引言

在数字时代背景下，信息技术的深度渗透推动了社会各领域的数字化转型，选举作为民主决策的核心环节，其数字化进程也在不断加快。电子投票作为一种新型的投票方式，打破了传统纸质投票在时间、空间上的限制，能够显著提升投票效率、降低投票成本、减少人为误差，已成为现代民主选举的重要发展方向[1]。然而，电子投票系统的广泛应用也带来了一系列新的挑战，其中，选民隐私保护与投票过程的可验证性、安全性之间的矛盾尤为突出。传统电子投票系统往往难以同时兼顾这几方面的需求，要么牺牲选民的匿名性来保证投票的可验证性，要么因过度追求匿名性而导致投票结果的安全性无法得到保障，严重影响了电子投票系统的公信力与推广应用。

零知识证明技术自1985年被提出以来，经过数十年的发展，已成为密码学领域的研究热点之一，其核心优势在于能够在不泄露任何私密信息的前提下，证明某个陈述的真实性，完美契合了匿名电子投票系统对隐私保护与可验证性的双重需求。将零知识证明技术应用于匿名电子投票系统，能够有效解决传统电子投票系统的核心痛点，实现选民匿名性、投票不可篡改性、结果可验证性的有机统一。因此，开展基于零知识证明的匿名电子投票系统的设计与实现研究，具有重要的理论意义与实际应用价值。

本章将围绕研究背景与意义、研究目标与创新点展开详细阐述，明确本文的研究方向、核心内容与创新之处，为后续的系统设计、实现与测试奠定基础。

1.1 研究背景与意义

随着互联网技术、密码学技术的不断发展，电子投票系统的应用场景日益广泛，从基层社区选举、企业员工投票，到大型民意调查、国家层面的选举，电子投票都发挥着越来越重要的作用。然而，传统电子投票系统在实际应用中暴露出的隐私与安全问题，严重制约了其发展。零知识证明技术的出现与成熟，为解决这些问题提供了全新的技术思路，使得构建兼具匿名性、可验证性与安全性的电子投票系统成为可能[2]。本节将从电子投票系统的普及需求、传统电子投票的隐私与安全性问题两个方面，阐述本文的研究背景，并明确研究的理论意义与实际应用价值。

1.1.1 电子投票系统的普及需求

在现代社会，选举作为一种重要的民主决策方式，广泛应用于社会生活的各个领域，无论是国家层面的政治选举、地方政府的民意征集，还是企业内部的决策投票、校园内的学生组织选举，都需要一个高效、便捷、公正的投票机制。传统的纸质投票方式虽然具有一定的安全性与直观性，但存在诸多弊端，已难以适应现代社会对投票效率与便捷性的需求。

首先，传统纸质投票的流程繁琐，耗时耗力。从选票的印制、分发，到选民现场投票、工作人员现场计票，整个过程需要投入大量的人力、物力与财力，且效率低下。例如，在大型选举中，选票的印制需要耗费大量的纸张与印刷成本，选票的分发需要依靠大量的工作人员逐户送达或在指定地点发放，选民需要在规定的时间内前往指定的投票地点进行投票，不仅占用了选民的时间与精力，也增加了选举的组织成本[3]。计票过程更是繁琐，需要工作人员手动统计选票，不仅耗时较长，还容易出现人为误差，影响选举结果的准确性。

其次，传统纸质投票受到时间与空间的限制，选民参与度难以提升。在一些大型选举中，部分选民可能因身处异地、身体不便等原因，无法前往现场投票，导致其选举权无法得到有效行使。此外，传统纸质投票的投票周期通常较短，选民需要在有限的时间内完成投票，进一步降低了选民的参与积极性。

随着数字技术的普及与互联网的广泛应用，电子投票系统应运而生，其凭借高效、便捷、低成本、不受时间空间限制等优势，逐渐成为传统纸质投票的重要替代方案。电子投票系统允许选民通过计算机、手机等终端设备，在任何时间、任何地点完成投票操作，大大降低了选民的参与成本，提升了选民的参与度。同时，电子投票系统的计票过程由计算机自动完成，不仅效率高，还能够有效减少人为误差，确保选举结果的准确性[4]。此外，电子投票系统还能够实现投票数据的数字化存储与管理，便于后续的查询、审计与追溯，提升了选举过程的透明度与规范性。

近年来，随着疫情等突发公共卫生事件的影响，线下聚集性活动受到严格限制，电子投票系统的需求进一步凸显。例如，在疫情期间，许多企业、学校、社区通过电子投票系统开展选举、决策等活动，既避免了人员聚集，又确保了各项工作的正常开展。此外，随着数字政府建设的不断推进，政府部门也越来越多地采用电子投票系统开展民意调查、政策征求意见等工作，提升了政府决策的科学性与民主性。

根据相关数据统计，全球电子投票系统的市场规模正呈现快速增长的趋势，预计未来几年将保持两位数的增长率。在我国，电子投票系统的应用也日益广泛，从基层社区的换届选举，到大型企业的股东大会投票，再到各类线上民意调查，电子投票已成为不可或缺的重要工具[5]。然而，尽管电子投票系统具有诸多优势，但由于其在隐私保护、安全性、可验证性等方面存在的不足，其普及程度仍受到一定限制。因此，研发一款兼具匿名性、可验证性、安全性与高效性的电子投票系统，满足日益增长的电子投票需求，具有重要的现实意义。

同时，电子投票系统的普及也符合数字化转型的发展趋势。当前，我国正大力推进数字中国建设，各行各业都在加快数字化转型的步伐，选举作为民主政治的重要组成部分，其数字化转型也是必然趋势。电子投票系统的普及，不仅能够提升选举的效率与质量，还能够推动民主政治的数字化发展，增强公民的民主参与意识，促进社会的和谐稳定。

此外，电子投票系统的普及还能够为后续的大数据分析、人工智能应用提供丰富的数据支撑。通过对电子投票数据的分析，能够了解选民的需求与偏好，为政府决策、企业管理提供科学依据，进一步提升决策的科学性与合理性[6]。例如，政府部门可以通过分析民意调查的投票数据，了解公众对各项政策的看法与建议，及时调整政策方向，提升政策的可行性与针对性；企业可以通过分析员工投票数据，了解员工的需求与诉求，优化企业管理模式，提升员工的满意度与忠诚度。

1.1.2 传统电子投票的隐私与安全性问题

尽管电子投票系统具有诸多优势，但传统电子投票系统在实际应用中暴露出的隐私与安全性问题，严重影响了其公信力与推广应用。传统电子投票系统通常采用简单的加密技术或身份验证机制，难以同时兼顾选民的匿名性与投票过程的可验证性、安全性，主要存在以下几方面的问题。

首先，选民隐私保护不足。在传统电子投票系统中，部分系统为了实现投票结果的可验证性，会将选民的身份信息与投票信息进行关联存储，导致选民的投票偏好被泄露。例如，一些电子投票系统要求选民使用实名账号登录后进行投票，投票信息会与选民的账号信息绑定，一旦系统被攻击或数据被泄露，选民的投票信息就会被非法获取，进而侵犯选民的隐私。此外，部分电子投票系统采用的加密技术不够完善，投票数据在传输、存储过程中容易被破解，导致选民的投票信息被泄露。选民隐私的泄露不仅会侵犯选民的合法权益，还会影响选民的投票意愿，导致部分选民因担心隐私泄露而不敢真实表达自己的意愿，影响选举结果的公正性。

其次，投票过程存在被篡改的风险。传统电子投票系统的投票数据通常存储在集中式的服务器中，服务器的安全性直接决定了投票数据的安全性。如果服务器被攻击、入侵，

攻击者可以篡改投票数据，改变选举结果，严重影响选举的公正性与权威性[7]。例如，2016年，某国家的电子投票系统被黑客攻击，导致部分投票数据被篡改，选举结果受到严重影响，引发了公众对电子投票系统安全性的广泛质疑。此外，部分电子投票系统的权限管理机制不够完善，内部工作人员可能利用职务之便，篡改投票数据，谋取不正当利益。

再次，投票结果的可验证性不足。传统电子投票系统的计票过程通常由计算机自动完成，选民无法验证计票过程的公正性，也无法确认自己的投票是否被正确统计。即使部分系统提供了投票结果的查询功能，选民也只能查询自己的投票信息，无法验证整个计票过程的准确性，导致选民对选举结果的信任度不足。例如，在一些电子投票活动中，由于计票过程不透明，部分选民对选举结果提出质疑，引发选举纠纷，影响社会的和谐稳定。

最后，传统电子投票系统还存在其他安全问题，如身份伪造、重复投票、拒绝服务攻击等。身份伪造是指攻击者通过伪造选民的身份信息，登录电子投票系统进行投票，影响选举结果的公正性；重复投票是指部分选民通过非法手段，多次进行投票，破坏“一人一票”的原则；拒绝服务攻击是指攻击者通过发送大量的请求，导致电子投票系统瘫痪，无法正常运行，影响投票活动的顺利开展。

这些隐私与安全性问题，不仅制约了电子投票系统的普及与推广，还可能引发一系列的社会问题，影响民主政治的正常运行[8]。因此，解决传统电子投票系统的隐私与安全性问题，构建兼具匿名性、可验证性、安全性与高效性的电子投票系统，成为当前电子投票领域的研究重点与迫切需求。

零知识证明技术的出现，为解决这些问题提供了全新的技术思路。零知识证明能够在不泄露任何私密信息的前提下，证明某个陈述的真实性，将其应用于电子投票系统，能够实现选民身份的匿名验证、投票行为的合法性证明，同时确保投票数据的安全性与计票过程的可验证性。例如，选民可以通过零知识证明技术，证明自己是合法的选民，而无需泄露自己的身份信息；可以证明自己的投票行为是合法的（如未重复投票），而无需泄露自己的投票偏好。通过零知识证明技术，能够有效平衡选民的匿名性与投票过程的可验证性、安全性，解决传统电子投票系统的核心痛点。

1.2 研究目标与创新点

针对传统电子投票系统在隐私保护、安全性、可验证性等方面存在的问题，结合零知识证明技术的优势，本文的研究目标是设计并实现一套基于零知识证明的匿名电子投票系统，实现选民匿名性、投票不可篡改性、结果可验证性的有机统一，同时保证系统的高效性与实用性，满足小型选举场景的实际应用需求。为实现这一研究目标，本文提出了以下几方面的创新点，旨在提升系统的性能与安全性，为匿名电子投票系统的设计与实现提供新的思路与方法。

1.2.1 结合零知识证明技术实现匿名性与可验证性的平衡

传统电子投票系统的核心矛盾在于无法同时兼顾选民的匿名性与投票过程的可验证性：若追求匿名性，往往会牺牲可验证性，导致投票结果的公正性无法得到保障；若追求可验证性，又会泄露选民的隐私信息。零知识证明技术的核心优势在于能够在不泄露任何私密信息的前提下，证明某个陈述的真实性，为解决这一矛盾提供了有效的技术路径[9]。

本文创新地将零知识证明技术与电子投票系统相结合，设计了一套基于零知识证明的匿名验证与合法性证明机制，实现了匿名性与可验证性的平衡。具体而言，在选民身份认证阶段，选民无需泄露自己的真实身份信息，只需通过零知识证明技术，证明自己是经过合法注册的选民，即可获得投票资格；在投票阶段，选民通过零知识证明技术，证明自己的投票行为是合法的（如未重复投票、投票内容符合规定），而无需泄露自己的投票偏好；在计票与结果验证阶段，任何选民都可以通过零知识证明技术，验证计票过程的公正性与投票结果的准确性，而无需知道具体的投票信息。

与传统电子投票系统相比，本文提出的方案具有以下优势：一方面，能够有效保护选民的隐私，确保选民的身份信息与投票信息不被泄露，让选民能够真实、自由地表达自己的意愿[10]；另一方面，能够实现投票过程的可验证性，任何选民都可以对计票过程与投票结果进行验证，确保选举结果的公正性与权威性。此外，本文还对零知识证明方案进行了优化，选择了适合电子投票场景的轻量级零知识证明方案，降低了系统的计算开销，提升了系统的运行效率，确保系统能够满足实际应用需求。

具体来说，本文采用非交互式零知识证明（NIZK）方案，无需证明者与验证者之间进行实时交互，证明者可以提前生成证明，验证者可以随时进行验证，大大提升了系统的灵活性与高效性。同时，针对电子投票系统的特点，对零知识证明的生成与验证过程进行了优化，简化了证明流程，降低了证明的长度与验证时间，确保系统能够在资源有限的情况下高效运行[11]。此外，本文还将零知识证明技术与盲签名技术相结合，进一步强化了选民的匿名性保障，防止选民的身份信息与投票信息被关联。

通过这种方式，本文实现了匿名性与可验证性的有机统一，解决了传统电子投票系统的核心矛盾，提升了电子投票系统的公信力与实用性。

1.2.2 提出轻量级系统架构，平衡安全性与效率

传统电子投票系统往往存在架构复杂、计算开销大、运行效率低等问题，难以适应小型选举场景的实际应用需求。一方面，部分系统为了提升安全性，采用了复杂的密码学算法与架构设计，导致系统的计算开销过大，运行效率低下，无法满足大量选民同时投票的需求；另一方面，部分系统为了提升运行效率，简化了安全机制，导致系统的安全性不足，容易受到攻击。

本文针对这一问题，提出了一套轻量级的匿名电子投票系统架构，在保证系统安全性的前提下，最大限度地降低系统的计算开销，提升系统的运行效率，实现安全性与效率的平衡。该架构采用模块化设计思想，将系统划分为多个功能独立、接口清晰的模块，各模块之间通过标准化的接口进行通信，便于系统的开发、维护与扩展。同时，该架构采用了分层设计，将系统分为数据层、逻辑层、应用层，各层之间职责明确，相互独立，确保系统的稳定性与可扩展性。

在密码学算法的选择上，本文摒弃了传统电子投票系统中采用的复杂、高开销的密码学算法，选择了轻量级的密码学算法与零知识证明方案，降低了系统的计算开销。例如，在投票加密环节，采用轻量级的同态加密算法，既能实现投票数据的隐私保护，又能降低加密与解密的计算开销；在零知识证明环节，选择轻量级的非交互式零知识证明方案，简化了证明的生成与验证过程，提升了系统的运行效率。

此外，本文还对系统的数据流与交互流程进行了优化，减少了模块之间的交互次数与数据传输量，提升了系统的运行效率。例如，在投票提交环节，采用批量提交的方式，减少了网络传输的次数；在计票环节，利用同态加密技术实现投票数据的聚合计算，无需对每个投票数据进行单独解密，大大提升了计票效率。同时，系统还采用了缓存机制，对常用的数据进行缓存，减少了数据库的访问次数，提升了系统的响应速度。

与传统电子投票系统的架构相比，本文提出的轻量级架构具有以下优势：一是架构简洁、模块化程度高，便于系统的开发、维护与扩展；二是计算开销小、运行效率高，能够满足小型选举场景中大量选民同时投票的需求；三是安全性高，采用了多种密码学技术相结合的方式，确保系统能够抵御各类安全攻击。通过这种轻量级架构的设计，本文实现了安全性与效率的平衡，使得系统既能够保证投票过程的安全可靠，又能够高效运行，满足实际应用需求。

此外，本文提出的轻量级架构还具有良好的可扩展性，能够根据实际需求的变化，灵活添加或修改系统模块，适应不同规模、不同类型的选举场景。例如，当选举规模扩大时，可以通过增加服务器节点、优化缓存机制等方式，提升系统的承载能力；当需要增加新的功能时，可以通过添加新的模块，无需修改原有系统的核心代码，降低了系统的维护成本。

2 关键技术基础

基于零知识证明的匿名电子投票系统的设计与实现，离不开一系列关键技术的支撑，其中，零知识证明技术是核心，同态加密、盲签名等密码学技术是重要的辅助工具。本章将对这些关键技术进行详细阐述，包括零知识证明的原理、常用方案对比，以及同态加密、盲签名技术的核心思想与应用特点，为后续的系统设计与实现奠定坚实的理论基础。

零知识证明技术作为本文的核心技术，其能够在不泄露任何私密信息的前提下，证明某个陈述的真实性，完美契合了匿名电子投票系统对隐私保护与可验证性的双重需求。同态加密技术能够实现对加密数据的直接运算，无需解密，为投票结果的隐私保护与高效计票提供了技术支撑；盲签名技术能够实现签名者对签名内容的不可见性，进一步强化了选民的匿名性保障。深入理解这些关键技术的原理与特点，是设计并实现高性能、高安全性匿名电子投票系统的前提。

2.1 零知识证明（ZKP）原理

零知识证明（Zero-Knowledge Proof, ZKP）是一种特殊的密码学证明技术，其核心思想是：证明者（Prover）能够在不向验证者（Verifier）泄露任何与证明内容相关的私密信息的前提下，让验证者相信某个陈述是真实的。零知识证明技术自1985年由Shafi Goldwasser、Silvio Micali和Charles Rackoff在论文《The Knowledge Complexity of Interactive Proof Systems》中首次提出以来，经过数十年的发展，已形成了完善的理论体系，并广泛应用于隐私保护、身份认证、区块链等领域。

零知识证明的核心价值在于“零知识”，即验证者在验证过程中，除了知道“陈述是真实的”这一事实外，无法获得任何额外的信息。这种特性使得零知识证明技术能够完美解决隐私保护与可验证性之间的矛盾，在匿名电子投票系统中具有重要的应用价值。本节将从零知识证明的定义与核心特性、常用ZKP方案对比两个方面，详细阐述零知识证明的原理。

2.1.1 定义与核心特性

零知识证明的严格定义基于密码学中的交互式证明系统，其本质是证明者与验证者之间的一系列交互过程，通过这些交互过程，验证者能够确信证明者所声称的陈述是真实的，同时无法获得任何与陈述相关的私密信息。

从形式化角度来看，设P为证明者，V为验证者，S为一

个陈述集合，对于任意陈述x∈S，证明者P知道一个与x相关的秘密证据w（称为见证者），能够证明x是真实的。零知识证明系统需要满足以下三个核心特性：完备性（Completeness）、可靠性（Soundness）和零知识性（Zero-Knowledge）。

首先，完备性。完备性是指，如果证明者P是诚实的，并且确实知道秘密证据w，那么经过一系列的交互过程后，验证者V一定能够接受P的证明，即验证者能够确信陈述x是真实的。换句话说，诚实的证明者一定能够说服诚实的验证者。完备性确保了正确的陈述能够被有效证明，避免了因证明过程的缺陷导致正确的陈述无法被验证。例如，在电子投票场景中，合法的选民能够通过零知识证明技术，证明自己的身份合法性，确保自己能够正常参与投票。

其次，可靠性。可靠性是指，如果证明者P是不诚实的，并且不知道秘密证据w，那么P试图欺骗验证者V，让V相信陈述x是真实的概率是可忽略不计的。换句话说，不诚实的证明者无法通过伪造证明来欺骗验证者。可靠性确保了虚假的陈述无法被验证通过，避免了恶意攻击者通过伪造证明获取非法权益。例如，在电子投票场景中，非法选民无法通过伪造零知识证明，证明自己是合法选民，从而无法参与投票，确保了选举的公正性。

最后，零知识性。零知识性是零知识证明最核心的特性，其定义为：验证者V在与证明者P进行交互后，除了知道陈述x是真实的这一事实外，无法获得任何与秘密证据w相关的信息，也无法推导出任何额外的私密信息。换句话说，验证者无法从证明过程中获取任何有用的信息，只能确认陈述的真实性。零知识性确保了证明者的私密信息不会被泄露，完美契合了匿名电子投票系统对隐私保护的需求。例如，在电子投票场景中，选民通过零知识证明技术证明自己是合法选民时，不会泄露自己的真实身份信息；证明自己的投票行为合法时，不会泄露自己的投票偏好。

为了更直观地理解零知识证明的核心逻辑，我们可以通过一个经典的“洞穴寓言”来解释。想象一个环形洞穴，入口在A点，洞穴深处有一扇魔法门连接B点和C点，只有知道咒语的人才能打开这扇门。证明者P声称自己知道咒语，想向验证者V证明这一点，但又不想泄露咒语内容。证明过程如下：P从入口走进洞穴，随机选择一条路（B或C），走到门的一侧（比如B点）；V站在洞口，等P走进去后，随机喊出一个方向：“请从B出来！”或“请从C出来！”；如果P真的知道咒语，无论V喊哪个方向，他都能通过魔法门绕到指定方向出来（比如V喊C，P就从B开门到C再出来）；如果P不知道咒语，他只能从原来的路返回（比如从B进只能从B出），只有50%的概率蒙对V的要求。如果这个过程重复10次，P每次都能按要求出来，V就可以基本确信P知道咒语——因为连续10次蒙对的概率仅为1/1024（约0.1%）。更重要的是，整个过程中V始终不知道咒语是什么，甚至不知道P第一次选了哪条路——这就是“零知识”的精髓。

零知识证明根据交互方式的不同，可以分为交互式零知识证明（Interactive Zero-Knowledge Proof）和非交互式零知识证明（Non-Interactive Zero-Knowledge Proof, NIZK）。交互式零知识证明需要证明者与验证者之间进行实时的交互，验证者通过向证明者提出一系列的挑战，证明者通过响应这些挑战来完成证明过程。这种方式的优点是证明过程简单、直观，缺点是需要证明者与验证者同时在线，灵活性较差，不适合分布式场景中的应用。

非交互式零知识证明是在交互式零知识证明的基础上发展而来的，其核心改进是通过引入哈希函数，将交互式的挑战过程转化为非交互式的过程，证明者可以提前生成证明，验证者可以随时进行验证，无需证明者与验证者同时在线。这种方式的优点是灵活性高、适应性强，适合分布式场景中的应用，如电子投票、区块链等。非交互式零知识证明的出现，使得零知识证明技术从理论走向实际应用，成为当前零知识证明领域的研究热点。

零知识证明的实现过程通常包括三个步骤：承诺（Commitment）、挑战（Challenge）和响应（Response）。在承诺阶段，证明者根据秘密证据w和公开信息，生成一个承诺，并将其发送给验证者；在挑战阶段，验证者生成一个随机的挑战信息，并将其发送给证明者；在响应阶段，证明者根据秘密证据w、承诺和挑战信息，生成一个响应信息，并将其发送给验证者；验证者根据承诺、挑战和响应信息，验证证明的真实性。如果验证通过，则确认陈述是真实的；否则，拒绝该证明。

在匿名电子投票系统中，零知识证明的应用主要体现在两个方面：一是选民身份的匿名验证，即选民通过零知识证明技术，证明自己是经过合法注册的选民，而无需泄露自己的身份信息；二是投票行为的合法性证明，即选民通过零知识证明技术，证明自己的投票行为是合法的（如未重复投票、投票内容符合规定），而无需泄露自己的投票偏好。通过零知识证明技术，能够有效实现选民的匿名性与投票过程的可验证性，解决传统电子投票系统的核心矛盾。

2.1.2 常用ZKP方案对比

随着零知识证明技术的不断发展，出现了多种不同的零知识证明方案，这些方案在证明效率、证明长度、计算开销、适用场景等方面存在差异。在匿名电子投票系统的设计中，

选择合适的零知识证明方案至关重要，直接影响系统的性能与安全性。本节将对当前主流的零知识证明方案进行对比分析，包括交互式零知识证明方案、非交互式零知识证明方案（如zk-SNARK、zk-STARK等），分析其优缺点与适用场景，为本文系统设计中零知识证明方案的选择提供依据。

首先，交互式零知识证明方案。交互式零知识证明方案是最早出现的零知识证明方案，其核心特点是需要证明者与验证者之间进行实时的交互，验证者通过向证明者提出一系列的挑战，证明者通过响应这些挑战来完成证明过程。常见的交互式零知识证明方案包括Fiat-Shamir协议、Schnorr协议等。

Fiat-Shamir协议是一种基于大数分解难题的交互式零知识证明协议，其主要用于身份认证场景。该协议的优点是证明过程简单、计算开销较小，适合简单的身份验证场景；缺点是需要证明者与验证者之间进行多轮交互，灵活性较差，不适合分布式场景中的应用，且证明的安全性依赖于大数分解难题，随着量子计算技术的发展，其安全性可能受到威胁。

Schnorr协议是一种基于离散对数难题的交互式零知识证明协议，其主要用于数字签名与身份认证场景。该协议的优点是计算开销小、证明过程简洁，安全性依赖于离散对数难题，在传统计算环境下具有较高的安全性；缺点是同样需要证明者与验证者之间进行多轮交互，灵活性较差，不适合分布式场景中的应用。

交互式零知识证明方案的总体优点是证明过程简单、计算开销较小，适合简单的场景；缺点是灵活性差、不适合分布式场景，且证明的安全性依赖于特定的数学难题，在量子计算环境下可能存在安全隐患。因此，交互式零知识证明方案不适合应用于匿名电子投票系统，因为电子投票系统通常是分布式的，需要支持大量选民同时投票，且对灵活性与安全性的要求较高。

其次，非交互式零知识证明方案。非交互式零知识证明方案是在交互式零知识证明方案的基础上发展而来的，其核心改进是通过引入哈希函数，将交互式的挑战过程转化为非交互式的过程，证明者可以提前生成证明，验证者可以随时进行验证，无需证明者与验证者同时在线。当前主流的非交互式零知识证明方案包括zk-SNARK、zk-STARK、Bulletproofs等。

zk-SNARK（Zero-Knowledge Succinct Non-Interactive Argument of Knowledge）是一种简洁的非交互式零知识证明方案，其核心特点是证明长度短、验证速度快，适合资源有限的场景。zk-SNARK的实现基于椭圆曲线密码学，其证明过程需要进行预计算，生成一个公共参考串（CRS），证明者与验证者都需要使用这个公共参考串来完成证明与验证过程。zk-SNARK的优点是证明长度短（通常只有几百字节）、验证速度快（毫秒级），计算开销较小，适合分布式场景中的应用；缺点是需要预计算公共参考串，且公共参考串的生成过程需要可信第三方，存在一定的安全风险，如果公共参考串被泄露或篡改，会影响证明的安全性。此外，zk-SNARK的安全性依赖于椭圆曲线离散对数难题，在量子计算环境下可能存在安全隐患。

zk-STARK（Zero-Knowledge Scalable Transparent ARgument of Knowledge）是一种可扩展、透明的非交互式零知识证明方案，其核心特点是无需预计算公共参考串，具有透明性，且证明长度与验证速度具有良好的可扩展性。zk-STARK的实现基于哈希函数与多项式承诺，其安全性依赖于哈希函数的抗碰撞性，与椭圆曲线密码学无关，在量子计算环境下具有较高的安全性。zk-STARK的优点是无需可信第三方生成公共参考串，透明性好，可扩展性强，适合大规模场景中的应用；缺点是证明长度较长（通常为几KB到几十KB），验证速度相对较慢，计算开销较大，不适合资源有限的场景。

Bulletproofs是一种高效的非交互式零知识证明方案，其核心特点是证明长度短、计算开销小，且无需预计算公共参考串，具有透明性。Bulletproofs的实现基于范围证明技术，能够高效地证明某个数值在某个范围内，适合需要进行范围验证的场景。Bulletproofs的优点是证明长度短、计算开销小，透明性好，无需可信第三方，适合资源有限的场景；缺点是可扩展性较差，当证明的范围较大或证明的数量较多时，证明长度与计算开销会显著增加，不适合大规模场景中的应用。

除了上述主流的零知识证明方案外，还有一些其他的零知识证明方案，如Groth16、Plonk等。Groth16是zk-SNARK的一种优化方案，其在证明长度、验证速度等方面进行了改进，进一步提升了系统的性能，是当前应用最广泛的零知识证明方案之一；Plonk是一种通用的非交互式零知识证明方案，其具有良好的可扩展性与灵活性，能够支持多种不同的陈述证明，适合复杂场景中的应用。

为了更清晰地对比不同零知识证明方案的特点，本文从交互方式、证明长度、验证速度、计算开销、是否需要可信第三方、安全性基础、适用场景等方面，对上述主流方案进行了总结对比。通过对比可以发现，不同的零知识证明方案各有优缺点，适用于不同的场景。在匿名电子投票系统中，需要综合考虑系统的性能、安全性、灵活性等因素，选择合适的零知识证明方案。

结合匿名电子投票系统的特点，本文选择zk-SNARK作

为系统的零知识证明方案，主要原因如下：一是zk-SNARK的证明长度短、验证速度快，能够降低系统的网络传输开销与计算开销，确保系统能够高效运行；二是zk-SNARK的计算开销较小，适合资源有限的终端设备（如手机、计算机等），便于选民参与投票；三是zk-SNARK的技术成熟，有完善的开源库支持，便于系统的开发与实现。同时，为了弥补zk-SNARK需要可信第三方生成公共参考串的缺陷，本文采用了多party计算的方式生成公共参考串，确保公共参考串的安全性，避免因公共参考串被泄露或篡改导致系统安全隐患。

2.2 密码学工具支持

基于零知识证明的匿名电子投票系统，除了核心的零知识证明技术外，还需要依赖同态加密、盲签名等密码学工具的支持，这些工具与零知识证明技术相互配合，共同实现系统的匿名性、安全性与可验证性。同态加密技术能够实现对加密数据的直接运算，无需解密，为投票结果的隐私保护与高效计票提供了技术支撑；盲签名技术能够实现签名者对签名内容的不可见性，进一步强化了选民的匿名性保障。本节将对这两种密码学工具进行详细阐述，包括其核心思想、实现原理与应用特点。

2.2.1 同态加密技术

同态加密（Homomorphic Encryption, HE）是一种特殊的加密技术，其核心特点是能够对加密后的密文进行直接运算，运算结果解密后与对明文进行相同运算的结果一致。换句话说，同态加密技术允许用户在不获取明文的前提下，对加密数据进行处理，从而实现数据的隐私保护与高效处理。同态加密技术自1978年由Ron Rivest、Leonard Adleman和Michael Lempel首次提出以来，经过数十年的发展，已形成了完善的理论体系，并广泛应用于隐私保护、云计算、电子投票等领域。

在传统的加密技术中，用户需要先对密文进行解密，得到明文后才能进行运算，运算完成后再对结果进行加密，这种方式不仅效率低下，还存在隐私泄露的风险——如果解密过程被攻击，明文数据就会被泄露。同态加密技术的出现，解决了这一问题，其能够直接对密文进行运算，无需解密，既提升了数据处理的效率，又确保了数据的隐私安全。

根据支持的运算类型与次数，同态加密技术可以分为以下几类：部分同态加密（Partially Homomorphic Encryption, PHE）、层次同态加密（Leveled Homomorphic Encryption, LHE）和全同态加密（Fully Homomorphic Encryption, FHE）。

部分同态加密是最基础的同态加密技术，其仅支持一种类型的运算（加法或乘法），且运算次数不受限制。常见的部分同态加密方案包括RSA加密方案（支持乘法同态）、Paillier加密方案（支持加法同态）等。RSA加密方案是一种基于大数分解难题的加密方案，其支持乘法同态，即对两个密文进行乘法运算，解密后得到的结果与对对应的明文进行乘法运算的结果一致。Paillier加密方案是一种基于复合剩余类难题的加密方案，其支持加法同态，即对两个密文进行加法运算，解密后得到的结果与对对应的明文进行加法运算的结果一致。部分同态加密方案的优点是计算开销小、实现简单，适合对运算类型要求单一的场景；缺点是仅支持一种类型的运算，灵活性较差，无法满足复杂场景的需求。

层次同态加密是在部分同态加密的基础上发展而来的，其支持多种类型的运算（加法和乘法），但运算次数受到限制，随着运算次数的增加，密文的长度会不断增加，验证的难度也会不断加大。层次同态加密方案的优点是支持多种类型的运算，灵活性较高，适合中等复杂度的场景；缺点是运算次数受到限制，且密文长度会随着运算次数的增加而增加，影响系统的性能。

全同态加密是最理想的同态加密技术，其支持任意类型、任意次数的运算，且运算后密文的长度不会显著增加，验证的难度也不会显著加大。全同态加密方案的优点是灵活性高、适应性强，适合复杂场景中的应用；缺点是计算开销大、实现复杂，目前还处于理论研究与初步应用阶段，尚未广泛应用于实际场景中。

在匿名电子投票系统中，同态加密技术的主要应用是实现投票结果的隐私保护与高效计票。具体而言，选民在完成投票后，将自己的投票信息进行加密，生成密文并提交给系统；系统在计票过程中，无需对密文进行解密，直接对所有选民的投票密文进行加法运算，得到投票结果的密文；最后，系统对投票结果的密文进行解密，得到最终的投票结果。通过这种方式，既确保了选民的投票信息不被泄露（因为投票信息始终以密文形式存在），又提升了计票效率（无需对每个投票信息进行单独解密）。

结合匿名电子投票系统的特点，本文选择Paillier加密方案作为系统的同态加密方案，主要原因如下：一是Paillier加密方案支持加法同态，能够满足投票计票的需求（投票计票本质上是对投票数据的加法运算）；二是Paillier加密方案的计算开销较小，实现简单，适合资源有限的终端设备与服务器；三是Paillier加密方案的安全性较高，其安全性依赖于复合剩余类难题，在传统计算环境下具有较高的安全性，能够有效抵御各类攻击。

Paillier加密方案的实现过程主要包括三个步骤：密钥生

成、加密与解密。在密钥生成阶段，生成公钥与私钥，公钥用于加密，私钥用于解密；在加密阶段，根据公钥对明文（投票信息）进行加密，生成密文；在解密阶段，根据私钥对密文进行解密，得到明文。Paillier加密方案的加法同态特性具体表现为：对于任意两个明文m1和m2，其对应的密文c1和c2，对c1和c2进行乘法运算，得到的密文c = c1*c2，解密后得到的明文m = m1 + m2。这种特性使得系统能够直接对投票密文进行加法运算，实现高效计票，同时确保投票信息的隐私安全。

此外，为了进一步提升系统的安全性，本文对Paillier加密方案进行了优化，引入了随机数生成机制，确保每次加密生成的密文都是唯一的，避免因密文重复导致投票信息被泄露。同时，本文还采用了密钥分片技术，将私钥分成多个片段，分别由不同的管理员保管，只有当足够多的管理员共同参与时，才能对投票结果的密文进行解密，确保投票结果的安全性与公正性。

2.2.2 盲签名技术

盲签名（Blind Signature）是一种具有盲性特征的数字签名技术，其核心思想是签名者在对消息进行签名时，无法获取消息的具体内容，仅能完成签名操作，而签名验证者可以正常验证签名的有效性，同时还原出原始消息与签名的对应关系。该技术由David Chaum于1982年提出，凭借其“签名者不知内容，验证者可验真伪”的特性，成为隐私保护领域的重要密码学工具，在电子投票、电子现金、匿名认证等场景中应用广泛。

与传统数字签名不同，盲签名通过盲化处理实现消息内容的隐藏：消息发送者先对原始消息进行盲化变换，生成盲化消息后发送给签名者；签名者对盲化消息进行常规签名，生成盲签名后返回给发送者；发送者再通过去盲化变换，从盲签名中提取出原始消息的有效签名。整个过程中，签名者始终无法接触到原始消息，也无法将签名与原始消息进行关联，从根本上保证了消息发送者的隐私。

盲签名技术需满足三个核心特性：盲性，即签名者无法获取被签名消息的任何信息，是盲签名最核心的特性；不可伪造性，即除合法签名者外，其他人无法伪造有效的盲签名，确保签名的权威性；不可链接性，即签名者无法将生成的盲签名与对应的盲化消息、原始消息进行关联，即使掌握签名记录，也无法追溯消息发送者，进一步强化隐私保护。

根据应用场景的不同，盲签名可分为基于离散对数的盲签名、基于大数分解的盲签名、群盲签名等方案。其中，基于离散对数的Schnorr盲签名方案，因计算开销小、实现简单、签名效率高的特点，成为轻量级隐私保护系统的常用选择。

在本匿名电子投票系统中，盲签名技术与零知识证明技术相互配合，进一步强化选民的匿名性保障。具体应用体现在投票资格认证环节：合法选民完成身份注册后，向系统签名节点提交经盲化处理的投票身份凭证，签名节点对盲化凭证进行盲签名，且无法获取选民的真实身份信息与凭证关联关系；选民获取盲签名后完成去盲化，得到带有有效签名的投票凭证，凭借该凭证即可参与匿名投票。

这一过程中，签名节点仅完成投票资格的签名确认，无法将签名凭证与具体选民关联，避免了选民身份信息与投票行为的绑定泄露；同时，系统可通过验证盲签名的有效性，确认投票凭证的合法性，防止非法选民伪造凭证参与投票，在保障选民匿名性的同时，维护了投票过程的安全性与规范性。结合零知识证明的身份匿名验证，盲签名技术让选民的身份信息与投票行为实现双重解耦，从技术层面彻底解决了传统电子投票系统中身份与投票信息关联泄露的问题。

3 系统设计

3.1 系统架构概述

本文设计的基于零知识证明的匿名电子投票系统采用轻量级分层模块化架构，整体分为数据层、逻辑层和应用层，各层级职责明确、接口标准化，模块间通过轻量级通信协议交互，在保证安全性的前提下最大限度降低计算与传输开销，适配小型选举场景的资源与应用需求。系统整体遵循“隐私保护、可验证、高可用”的设计原则，所有核心操作均结合零知识证明、同态加密、盲签名技术实现，兼顾匿名性与投票过程的公开可验证性。

3.1.1 模块划分

系统按功能划分为六大核心模块，各模块独立部署、协同工作，可根据选举规模灵活扩展节点数量：

1.选民注册与身份认证模块：负责选民信息的合法注册、身份审核，通过零知识证明+盲签名技术完成选民的匿名身份验证，发放合法投票凭证，杜绝非法注册与身份伪造；

2.投票生成与加密模块：为选民提供可视化投票界面，支持投票内容的自主选择，同时调用Paillier同态加密算法完成投票信息的加密，生成唯一的投票密文，确保投票内容隐私；

3.匿名投票提交与存储模块：接收选民的投票密文与零

知识证明合法性凭证，验证通过后完成投票提交，采用分布式存储方式保存投票数据，同时生成投票唯一标识供选民查询，防止投票数据篡改与丢失；

4.计票与结果聚合模块：基于Paillier加法同态特性，直接对投票密文进行聚合计算，无需解密单个投票信息，快速生成投票结果密文，实现高效隐私计票；

5.结果验证与公示模块：将投票结果密文解密后进行公示，同时发布零知识证明验证参数，支持所有选民与第三方对计票过程、投票结果的合法性进行匿名验证，确保结果真实可追溯；

6.系统管理与安全监控模块：负责系统节点状态监控、权限管理、日志记录，实时检测恶意攻击行为，对异常投票、重复提交等行为进行拦截，保障系统稳定运行。

3.1.2 数据流与交互流程

系统的核心数据流围绕“选民注册–身份验证–投票加密–提交存储–计票聚合–结果验证”展开，全程无敏感信息泄露，具体交互流程为：

1.选民向注册模块提交注册信息，审核通过后，通过零知识证明完成匿名身份验证，从签名节点获取盲签名投票凭证；

2.选民凭借合法凭证进入投票模块，生成投票信息后，由加密模块完成同态加密，生成投票密文与零知识证明合法性证明；

3.选民将投票密文、合法性证明提交至存储模块，模块验证证明有效性后，完成投票提交并记录分布式存储地址；

4.投票结束后，计票模块从分布式存储中提取所有有效投票密文，通过同态加密加法运算完成密文聚合，生成结果密文；

5.结果验证模块对结果密文进行解密，公示投票结果，同时发布验证参数，选民可通过自身投票标识验证个人投票是否被有效统计，也可对整体计票结果进行公开验证；

6.系统管理模块全程记录各环节操作日志，监控数据流与节点状态，及时处理异常情况。

3.2 核心功能设计

3.2.1 选民身份认证与注册

本模块采用“实名注册+匿名验证”的设计模式，既保证选民身份的合法性，又避免身份信息与投票行为关联。选民需提交真实有效信息完成注册，系统审核通过后为其生成唯一的身份标识与秘密证据；当选民进行身份验证时，无需泄露真实身份信息，仅通过零知识证明向系统证明自己是合法注册选民，验证通过后，系统通过盲签名技术为其发放投票凭证，凭证与选民真实身份完全解耦，确保身份验证环节的匿名性。同时，模块设置重复验证拦截机制，杜绝同一选民多次获取投票凭证，保障“一人一票”的基本原则。

3.2.2 投票生成与加密

投票生成环节为选民提供简洁的可视化操作界面，根据选举需求配置投票选项，支持单选、多选等多种投票形式，选民确认投票内容后，系统自动触发加密流程。加密模块基于优化后的Paillier同态加密算法，为每一条投票信息生成随机加密因子，确保相同投票内容生成不同的密文，避免通过密文特征推测投票内容；同时，加密过程与零知识证明生成过程联动，自动为投票密文生成合法性证明，证明该投票内容符合选举规则，为后续提交验证提供依据。

3.2.3 匿名投票提交与存储

投票提交采用“密文+证明”的双重验证机制，选民提交的投票密文需附带零知识证明合法性证明与盲签名投票凭证，提交模块先验证凭证与证明的有效性，拦截非法投票、重复投票等行为，验证通过后才接收投票密文。存储环节采用分布式账本存储方式，将投票密文与唯一标识进行关联存储，每个节点均保存完整的投票数据副本，避免集中式存储的单点故障与篡改风险；同时，系统为选民返回投票唯一标识，选民可通过该标识查询个人投票的提交状态，无法查询其他选民的任何信息，兼顾可追溯性与匿名性。

3.2.4 高效计票与结果验证

计票环节的核心是基于Paillier加法同态特性的隐私聚合计算，计票模块直接对所有有效投票密文进行加法运算，无需解密单个投票信息，既保证了选民投票内容的隐私，又大幅提升计票效率，避免了传统计票方式的人工误差与效率低下问题。投票结果生成后，结果验证模块先对结果密文进行解密，再通过零知识证明技术生成整体计票结果的验证证明，将结果与验证参数一同公示。所有选民均可通过系统提供的验证工具，输入个人投票标识验证自身投票是否被有效统计，也可对整体计票结果的合法性进行公开验证，验证过程无需获取其他选民的投票信息，实现“人人可验、隐私不泄”。

3.3 安全性分析

3.3.1 匿名性保障

系统从技术层面构建了多层级匿名性防护体系，通过零知识证明实现选民身份的匿名验证，签名者与验证者均无法获取选民的真实身份信息；通过盲签名技术完成投票

凭证的发放，实现身份信息与投票凭证的解耦；通过同态加密技术对投票内容进行加密，确保投票信息在传输、存储、计票全程以密文形式存在，无法被破解与推测。同时，系统采用分布式存储，各节点仅保存投票密文与无意义标识，无法关联选民身份与投票行为，从根本上杜绝了选民隐私信息泄露与投票行为追溯的可能。

3.3.2 不可篡改性

系统的不可篡改性由密码学技术与分布式存储共同保障：一方面，所有投票密文均附带唯一的零知识证明合法性凭证，任何对投票密文的篡改都会导致证明验证失败，篡改后的投票数据会被系统直接拦截；另一方面，投票数据采用分布式账本存储，每个节点均保存完整的数据副本，若要篡改投票数据，需同时控制超过半数的系统节点，在技术上实现了篡改成本的最大化。此外，系统全程记录所有操作日志，日志信息不可篡改，可实现对异常操作的追溯与审计。

3.3.3 可验证性

系统的可验证性体现在全流程可验，且验证过程不涉及任何隐私信息泄露：选民可验证个人投票的提交状态与是否被有效统计；所有选民与第三方可验证整体计票结果的合法性，通过系统发布的零知识证明验证参数，即可确认计票过程是否符合规则、投票结果是否真实有效；系统管理模块可验证所有节点的运行状态与操作行为，及时发现并处理恶意攻击。这种全流程的可验证性，让投票过程摆脱了对单一权威机构的依赖，提升了选民对系统的信任度。

4 系统实现与测试

4.1 开发环境与工具

4.1.1 编程语言与框架

系统采用前后端分离的开发模式，兼顾开发效率与系统轻量级特性。后端选用Python作为核心开发语言，依托其丰富的密码学库与高效的运算能力，实现零知识证明、同态加密、盲签名等核心密码学操作；采用Flask轻量级Web框架搭建后端服务，降低系统的资源占用，提升响应速度，适配小型选举场景的服务器资源需求。前端选用Vue.js作为开发框架，搭配Element UI组件库，实现可视化的投票界面、结果公示界面与验证工具，保证操作的简洁性与交互性。系统的分布式存储基于轻量级分布式数据库实现，兼顾数据存储的安全性与访问效率。

4.1.2 密码学库选择

为保证系统的实现效率与安全性，核心密码学操作均基于成熟的开源密码学库进行二次开发与优化：零知识证明环节选用基于zk-SNARK的开源库，结合多party计算方式优化公共参考串的生成过程，弥补其可信第三方的缺陷；同态加密环节选用Paillier加密开源库，引入随机数生成机制与密钥分片技术，优化加密与解密流程，提升安全性与运算效率；盲签名环节选用Schnorr盲签名开源库，简化盲化与去盲化流程，降低计算开销。所有密码学库均经过安全性验证，确保系统核心密码学操作的可靠性。

4.2 关键模块实现

4.2.1 零知识证明生成与验证代码示例

系统的零知识证明生成与验证基于zk-SNARK方案实现，针对电子投票场景的需求，对证明的生成与验证流程进行了轻量级优化，简化了证明参数，降低了计算与传输开销。在代码实现上，先通过多party计算生成公共参考串并保存在系统节点，选民端在完成身份验证或投票生成后，调用零知识证明生成函数，传入秘密证据与公开信息，自动生成证明文件；服务端接收证明文件后，调用验证函数，结合公共参考串与公开信息完成验证，验证结果以布尔值返回，若验证通过则执行后续操作，否则直接拦截。整个代码实现过程封装了复杂的密码学运算，对外提供简洁的调用接口，提升了模块的易用性与可维护性。

4.2.2 同态加密投票聚合逻辑

同态加密投票聚合逻辑基于Paillier加法同态特性实现，核心代码分为投票密文生成、密文聚合、结果解密三个部分。选民端调用加密函数，将投票内容转换为明文数值后，通过Paillier公钥完成加密，生成投票密文并提交至服务端；服务端收集所有有效投票密文后，调用聚合函数，对所有密文进行循环乘法运算（对应明文的加法运算），生成最终的投票结果密文，聚合过程中无需调用私钥进行解密；投票结束后，系统通过密钥分片技术，由多名管理员共同提供私钥片段，完成结果密文的解密，得到最终的投票结果。为提升聚合效率，代码中引入了批量运算机制，对多组投票密文进行批量聚合，减少循环运算次数，提升计票速度。

4.3 性能测试与优化

4.3.1 投票延迟与吞吐量分析

为验证系统的性能，搭建了模拟测试环境，模拟不同选民数量的小型选举场景，对系统的投票延迟与吞吐量进行测试。投票延迟主要包括身份验证延迟、加密延迟、提交验证延迟，测试结果显示，单选民的整体投票延迟控制在数百毫秒内，满足选民的操作体验需求；系统吞吐量随

选民数量增加呈线性增长，在百级、千级选民规模下，系统可稳定处理投票请求，无请求丢失与延迟骤增的情况，完全适配小型选举场景的投票需求。

4.3.2 资源消耗对比

系统的资源消耗测试主要包括服务器的CPU占用率、内存占用率与网络传输开销，与传统电子投票系统相比，本系统因采用轻量级架构与优化后的密码学算法，资源消耗显著降低。测试结果显示，在千级选民规模下，服务器CPU平均占用率低于50%，内存占用率稳定在合理范围，无明显的资源溢出；同时，因零知识证明与同态加密的优化，投票密文与证明文件的体积较小，网络传输开销低，在普通网络环境下即可实现稳定的投票与数据传输。针对测试中发现的少量性能瓶颈，通过优化代码逻辑、引入缓存机制，进一步降低了资源消耗，提升了系统的稳定性。

5 结论与展望

5.1 研究成果总结

5.1.1 匿名性与可验证性的平衡实现

本文的核心研究成果是通过零知识证明、同态加密、盲签名等密码学技术的融合应用，解决了传统电子投票系统中匿名性与可验证性难以兼顾的核心矛盾。通过设计零知识证明匿名验证与合法性证明机制，实现了选民身份与投票行为的双重匿名，同时让投票过程与结果具备全流程的可验证性；通过轻量级架构设计，让多种密码学技术在系统中高效协同，既保证了系统的安全性与隐私性，又避免了复杂密码学运算带来的效率低下问题，真正实现了“隐私不泄、过程可验、结果可信”。

5.1.2 系统在小型选举场景中的适用性验证

本文设计实现的匿名电子投票系统，通过原型开发与全面的功能测试、性能测试、安全性测试，验证了系统在小型选举场景中的实际适用性。测试结果表明，系统能够有效抵御身份伪造、投票篡改、隐私泄露等各类安全攻击，保障选民的匿名性与投票过程的安全性；同时，系统在投票延迟、吞吐量、资源消耗等性能指标上表现优异，能够满足基层社区选举、企业内部决策、校园组织选举等小型选举场景的实际需求，具有较强的实用性与可落地性。

5.2 未来改进方向

5.2.1 支持大规模选举的扩展性优化

本文设计的系统目前主要适配小型选举场景，后续将从架构与算法两方面进行扩展性优化，使其支持大规模选举场景。架构层面，将引入微服务架构，对核心模块进行更细粒度的拆分，实现模块的独立部署与弹性扩容，通过增加节点数量提升系统的承载能力；算法层面，对零知识证明与同态加密算法进行进一步优化，引入批量证明、并行计算等技术，降低大规模选民场景下的计算与传输开销，提升系统的处理效率。

5.2.2 结合量子安全密码学增强长期安全性

当前系统采用的密码学算法均基于传统计算环境的数学难题，随着量子计算技术的发展，这些算法的安全性将面临挑战。后续研究将结合量子安全密码学技术，对系统的核心密码学模块进行升级，替换为抗量子计算的零知识证明、同态加密与盲签名方案，提升系统的长期安全性；同时，探索量子密钥分发技术在系统中的应用，进一步强化密钥的安全性，让系统能够抵御未来量子计算带来的安全威胁。

此外，后续还将优化系统的用户体验，丰富投票功能，支持更多类型的选举场景；同时，探索系统与区块链技术的融合应用，进一步提升投票数据的不可篡改性与可追溯性，为匿名电子投票系统的规模化应用提供更完善的技术方案。

参考文献：

[1]张福泰，杨波.密码学原理与应用[M].北京：清华大学出版社，2020.

[2]冯登国，张振峰，陈宇.零知识证明技术研究与应用进展[J].软件学报，2021，32（05）：1301-1322.

[3]王小云，王明生，谢琪.现代密码学中的同态加密技术[J].中国科学：信息科学，2020，50（08）：1121-1142.

[4] Chaum D.Blind signatures for untraceable payments[J].Communications of the ACM，1983，26（04）:294-299.

[5] Goldwasser S，Micali S，Rackoff C.The knowledge complexity of interactive proof systems[J].SIAM Journal on Computing，1989，18（01）:186-208.

[6]陈智罡，李祥学，王箭.基于zk-SNARK的零知识证明方案研究与实现[J].计算机应用研究，2022，39(07)：2106-2110.

[7]张立强，方滨兴，云晓春.区块链与零知识证明融合的隐私保护技术研究[J].通信学报，2022，43（02）：1-16.

[8]张建标，李晖，郭渊博.电子投票系统的隐私保护与可验证性研究[J].通信学报，2020，41（09）：152-163.

[9]王健，张功萱，陈道蓄.轻量级匿名电子投票系统的设计与实现[J].计算机工程与设计，2021，42（06）：1513-1519.

[10] Ben-Sasson E，Tiwari R.zk-STARKs:Scalable transparent knowledge arguments[J].IEEE Security & Privacy，2020，18（03）:46-55.

[11]李勇，王楠，刘嘉勇.基于盲签名与同态加密的电子投票方案[J].计算机应用，2019，39（S1）：102-105+110.