Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 46 No. 5
May 2025

Comparative Study of Zero-Knowledge Proof Systems: Applications and Future Challenges

Madhuri S. Arade [1], Dr.Nitin N. Pise [2]

[1] PhD Scholar, Department of Computer Engg & Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

[2] Professor, Department of Computer Engg & Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India

Email Id: [1] arademadhuri15@gmail.com, [2] nitin.pise@mitwpu.edu.in

Abstract

In today's world, information security has become crucial and essential for all applications. Beyond securing data, maintaining information privacy is equally important. Zero-knowledge proof (ZKP) is a key cryptographic protocol that allows a prover to demonstrate the validity of information to a verifier without revealing the actual data. This paper explores various types of zero-knowledge proofs, including interactive and non-interactive approaches, along with different variations of non-interactive ZKPs. It provides a comparative analysis of these ZKP methods, identifying their challenges and potential future directions. Zero-knowledge proofs have a wide range of applications, including blockchain, cryptographic systems, and authentication mechanisms. While ZKP offers several advantages, it also encounters challenges such as scalability, post-quantum security, reducing proof size, and optimizing verification time, which are key areas for future enhancement.

Keywords: Zero Knowledge proof(zkp), zk-snark, zk-stark, types of zkp.

1. Introduction

The advancement of computers, the internet, and the web has become an essential part of modern society, significantly impacting daily life. Computers have streamlined tasks and automated numerous functions, enhancing efficiency across various domains. However, like any technological advancement, these innovations come with challenges—particularly security threats in digital information.

To address concerns related to security and privacy, various cryptographic protocols have been developed to safeguard against cyber threats. Cryptography enables the protection of information through encryption techniques, utilizing either symmetric or asymmetric keys.

- Symmetric Key Cryptography - uses a single secret key to encrypt and decrypt data, ensuring secure communication between parties.
- Asymmetric Key Cryptography - employs a pair of public and private keys, enhancing security by enabling encrypted communication without sharing a single secret key.

One of the most notable cryptographic protocols is Zero-Knowledge Proof (ZKP), introduced in the ref paper [1]-[4] in the 1980s, ZKP allows a prover to demonstrate the validity of a statement to a verifier without revealing any underlying details. This means that the verifier can confirm the truthfulness of the statement without gaining access to the actual information.

2. Fundamentals of zero knowledge proof

Essential properties of ZKP [1] are as follows.

Completeness

If the statement is true and both the prover and verifier follow the protocol correctly, the verifier will be convinced of the statement’s validity with overwhelming probability.

Soundness

A dishonest prover cannot convince an honest verifier of a false statement except with negligible probability. This ensures that proving false claims is computationally infeasible.

Zero-Knowledge

The proof reveals no information beyond the validity of the statement itself. The verifier learns nothing about the underlying data or secret used in the proof. Figure. 1 represents the block diagram of zero knowledge system.

Figure 1: Zero knowledge proof Block diagram

Consider a real-world scenario in a pharmaceutical supply chain, where the manufacturer acts as the prover, and the distributor is the verifier given in figure 2. When the distributor wants to purchase drugs and needs to confirm their authenticity, Zero-Knowledge Proofs (ZKPs) can be used for verification.

In this case, the manufacturer needs to share only essential information, such as the drug name, intended use, manufacturing date, expiry date, and price, while keeping sensitive details, like the manufacturing process and proprietary formula confidential. This is where ZKPs come into play.

The manufacturer (prover) generates a polynomial equation with arithmetic circuits, which generates the basis of the proof. This proof is then sent to the distributor (verifier). The verifier can then query the proof to ensure its correctness without learning any hidden details.

Through this process, the manufacturer successfully proves the authenticity of the drugs without revealing confidential information, ensuring both trust and data privacy in the supply chain.

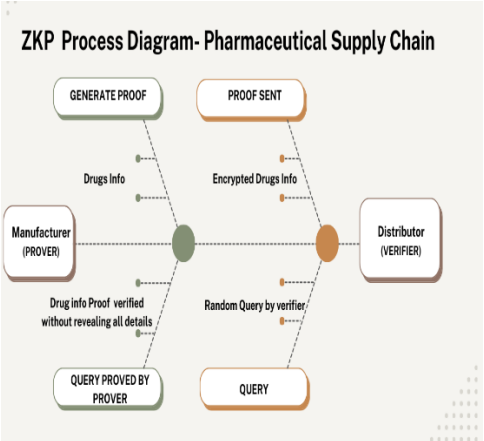

Figure 2: ZKP process of Pharmaceutical supply chain

3. Types of zero knowledge proof & Comparisons

The zero knowledge proof is majorly divided into two types.

- **Interactive ZKP[4] -**

Both the prover and verifier must be actively engaged during the process. To validate the proof, the verifier poses a series of random questions, which the prover answers in real time. If all responses align with the expected proof, the verification is considered successful. Since this process requires continuous interaction, both the prover and verifier must remain online.

Goldwasser et al. [4] demonstrate this concept using the graph isomorphism problem, where two graphs, G1 and G2, are isomorphic. The verifier randomly selects one of the graphs, and the prover correctly identifies it each time without revealing any information about the isomorphism itself.

- **Non Interactive ZKP[5] -**

In interactive ZKP, both the prover and verifier must be online throughout the process. This requirement is eliminated in non-interactive ZKP. In non-interactive ZKP[5], the prover generates the proof once, and the verifier can validate it independently without any further interaction with the prover.

Chen et al. [6] summarize the Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (ZK-SNARK) protocol, which is based on non-interactive ZKP. ZK-SNARKs require a trusted setup, including key generation for proof creation, where computational statements are transformed into algebraic statements using a quadratic arithmetic program. This paper designs ZK-SNARK protocols that allow participants to submit confidential bids, ensuring bid privacy while simultaneously proving the validity of their bids.

Ben-Sasson et al. [7] introduced zk-STARKs (Zero-Knowledge Scalable Transparent Arguments of Knowledge), a non-interactive zero-knowledge proof system. zk-STARKs offer key features such as scalability, transparency, and resistance to quantum attacks, making them a robust alternative to traditional ZKPs.

Scalability: The authors present a proof system where the size of the proof and the time required for verification grow sublinearly with the complexity of the computation. This efficiency makes zk-STARKs suitable for large-scale applications, such as blockchain

technologies, where verifying extensive computations is essential.

Transparency: zk-STARKs doesn't require trusted set up like zk-snark. This transparency is achieved through the use of publicly verifiable randomness, enhancing trust in the system by removing reliance on secret parameters.

Post-Quantum Security: The construction of zk-STARKs is based on collision-resistant hash functions, which are believed to be resistant to attacks by quantum computers. This design choice addresses the growing concern over the potential threats posed by quantum computing to classical cryptographic schemes. Zero-Knowledge Scalable Transparent Arguments of Knowledge (ZK-STARKs) play a crucial role in preserving privacy in blockchain applications and various cryptographic decentralized applications.

Bunz et al. [8] introduced Bulletproofs, a non-interactive zero-knowledge proof system utilizing the inner product argument technique. This approach recursively reduces large proofs into a series of smaller proofs, not using trusted setup while maintaining a compact proof size.

Gabizon et al. [9] proposed PLONK (Permutations over Lagrange-bases for Oecumenical Non-Interactive Arguments of Knowledge), which features a universal setup capable of supporting an unlimited number of circuits. PLONK generates proofs with a size independent of computational complexity, achieving efficiency through permutation-based operations over the Lagrange basis.

Groth et al. [10] developed Groth16, an optimized ZK-SNARK requiring only a small number of pairing product equations, leading to faster verification. Built on bilinear pairings and standard cryptographic assumptions, Groth16 enhances security and efficiency. It is widely used in privacy-focused blockchains like Zcash, enabling confidential transactions with minimal proof size and verification costs.

Alessandro Chiesa et al. [11] introduced Marlin, an improved ZK-SNARK variant incorporating a universal structured reference string (SRS), which enhances efficiency by removing the need for a new setup for each circuit. Marlin also employs holography to enable fast verification of encoded statements, making it suitable for large-scale computations.

Ames et al. [12] proposed Ligero, a zero-knowledge argument protocol for NP that achieves sublinear communication complexity without relying on a trusted setup. It follows a public-coin approach, allowing transformation into a non-interactive ZKP using the Fiat–Shamir heuristic in the random oracle model. Ligero exclusively relies on symmetric-key primitives for practical and efficient implementation.

Mary Maller et al. [13] designed Sonic, a zero-knowledge proof system with a universal and linear SRS, enabling constant-size proofs. Sonic enhances blockchain privacy and scalability by facilitating efficient transaction and smart contract verification without requiring a trusted setup.

Setty et al. [14] introduced Spartan, an advanced ZK-SNARK variant that eliminates the need for a trusted setup. Spartan achieves time-optimal proving, ensuring that prover work is proportional to computation size. It supports sublinear verification, enabling rapid validation without full proof recomputation. Additionally, it handles Rank-1 Constraint Systems (R1CS) and arbitrary arithmetic circuits, making it highly versatile. Spartan provides different proof constructions, including transparent zk-SNARKs and commit-and-prove proofs.

Kothapalli et al. [15] developed NOVA, a recursive ZKP system that aggregates multiple problem instances into a single proof, significantly reducing proof generation and verification complexity.

Chiesa et al. [16] introduced FRACTAL, a novel technique for constructing recursive proof systems that ensure both post-quantum security and transparency.

Liu et al. [17] designed Pianist, a system aimed at improving ZKP scalability and efficiency by distributing proof generation across multiple machines.

Tiancheng Xie et al. [18] proposed zkBridge, a major advancement in cross-chain interoperability. It offers a trustless and efficient mechanism for blockchain communication, leveraging succinct proofs and a modular architecture to enhance security and performance in existing cross-chain bridges.

Xie et al. [19] introduced Orion, a system designed to achieve linear prover time scaling with computation size. Similarly, Zhang et al. [20] contributed a solution maintaining strictly linear prover complexity in relation to circuit size.

Zero-Knowledge Proofs [21] further advance the field by integrating an interactive proof protocol with polynomial commitments, introducing a zero-knowledge argument scheme that optimizes prover complexity both theoretically and practically.

Table 1 provides a comparative analysis of various ZKP techniques.

Table 1: Comparison between Different ZKP

Paper & Authors	**Type of ZKP**	**Efficiency**	**Security Assumptions**	**Applications**
Goldreichet al[1]	General ZKP Composition	Addresses composition of ZKP systems	Standard cryptographic assumptions	Theoretical foundations
Goldwasser et al.[4]	Interactive ZKPs	Polynomial-time verifier efficiency	Knowledge complexity framework	Cryptographic protocols
Blum et al.[5]	Non-Interactive ZKPs (NIZK)	Improves efficiency over interactive ZKPs	Fiat-Shamir heuristic	Digital signatures, secure authentication
Chen et al[6]	zk-SNARKs Review	Comparative study of zk-SNARKs efficiency	Various cryptographic	Privacy in blockchain &cryptography
Ben-Sasson et al.[7]	Zk-STARK	Transparent, post-quantum secure	No trusted setup	Blockchain scalability
Bünz et al.[8]	Bulletproofs	Short proofs, no trusted setup	Discrete logarithm	Confidential transactions
Gabizon et al.[9]	PLONK	Universal & efficient	Trusted setup	General-purpose zk-SNARKs
Groth et al.[10]	Pairing-based NIZK	Reduced proof size	Bilinear pairing	Cryptographic protocols
Chiesa et al.[11]	Marlin	Universal & updatable SRS	Trusted setup	Scalable ZK proofs
Ames et al. [12]	Ligero	Lightweight, sublinear arguments	No trusted setup	Efficient proof systems
Maller et al. [13]	Sonic	Universal & updatable SRS	Trusted setup	Blockchain applications
Setty et al.[14]	Spartan	General-purpose zk-SNARKs	No trusted setup	Cryptographic proofs
Kothapalli et al.[15]	Nova	Recursive ZK arguments	Folding scheme-based security	Scalable recursive proofs
Chiesa et al.[16]	FRACTAL	Post-quantum recursive proofs	Holography-based security	Transparent, scalable ZKPs
Liu et al. [17]	Pianist	Scalable zkRollups	Fully distributed ZK proofs	Blockchain scalability
Tiancheng Xie et al.[18]	zkBridge	Trustless cross chain proofs	No trusted setup	Cross-chain interoperability

Paper & Authors	Type of ZKP	Efficiency	Security Assumptions	Applications
Xie et al.[19]	Orion	linear prover time	No trusted setup	Efficient proof gen.
Zhang et al. [20]	Interactive Proofs	Linear prover time	GKR protocol	Arithmetic circuit verification

4. Applications

- **ZKP in Blockchain & Cryptocurrency** – Enhances privacy, scalability, and trustless verification, with applications such as zk-Rollups and Bulletproofs.
- **ZKP in Secure Computing** – Plays a crucial role in cloud computing, AI, and secure multiparty computations, ensuring data confidentiality and integrity.
- **Cross-Chain & Scalability** – Solutions like zkBridge and Pianist enable efficient blockchain interoperability and scaling, enhancing decentralized ecosystems.

5. Challenges

After analyzing various zero-knowledge proof (ZKP) research efforts, the following challenges have been identified:

- **Scalability** – Needs significant improvements to handle larger computations efficiently.
- **Eliminating Trusted Setup** – ZKP protocols should move towards transparent and trustless setups to enhance security and decentralization.
- **Post-Quantum Security** – With the rise of quantum computing, ensuring resistance against quantum attacks remains a crucial challenge.
- **Optimizing Proof Efficiency** – Reducing proof size, prover time, and verification time is essential for making ZKPs more practical and scalable.

6. Future Directions

After reviewing research papers [1]-[21], several future research directions in zero-knowledge proofs (ZKPs) have been identified, as outlined in Table 2.

Table 2: Future research directions for zero knowledge proof

Research Direction	Potential Improvements
Scalability Improvements	- More efficient zk-SNARKs with sublinear prover time. - Optimization of proof verification on blockchain.
Decentralized & Transparent Proofs	- Expansion of transparent proof systems (STARKs, Bulletproofs). - Replacing traditional zk-SNARKs with universal or updatable SRS models.
Post-Quantum Cryptography	- Designing ZKPs that remain secure against quantum computers.
Efficient Proof Aggregation & Folding	- Improving recursive proof efficiency (e.g., Nova, FRACTAL). - Batch verification techniques to lower costs.

7. Conclusion

This paper explores the fundamentals of zero-knowledge proofs (ZKPs) and their key classifications, including interactive and non-interactive ZKPs. While interactive ZKPs require multiple rounds of communication between the prover and verifier, non-interactive ZKPs, such as ZK-SNARKs and ZK-STARKs, offer greater efficiency by eliminating the need for continuous interaction. Through a comprehensive comparison of various ZK-SNARK advancements, this survey highlights the significance of ZKPs in ensuring privacy, confidentiality, and security across multiple domains, including blockchain technology, cryptographic applications, and authentication systems.

Looking ahead, ZK-STARKs present a promising research direction, particularly in addressing challenges related to scalability and post-quantum security. As cryptographic advancements continue, the evolution of ZKP protocols will play a crucial role in building more secure, efficient, and privacy-preserving systems.

References

[1] Goldreich, O., Oren, Y. Definitions and properties of zero-knowledge proof systems. J. Cryptology 7, 1–32 (1994). https://doi.org/10.1007/BF00195207

[2] Goldreich, Oded, and Hugo Krawczyk. "On the composition of zero-knowledge proof systems."SIAM Journal on Computing 25.1 (1996): 169-192.

[3] Maurer, U. (2009). Unifying Zero-Knowledge Proofs of Knowledge. In: Preneel, B. (eds) Progress in Cryptology – AFRICACRYPT 2009. AFRICACRYPT 2009. Lecture Notes in Computer Science, vol 5580. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-02384-2_17

[4] Goldwasser, S., Micali, S., & Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186–208. doi:10.1137/0218012

[5] Manuel Blum, Paul Feldman, and Silvio Micali. 1988. Non-interactive zero-knowledge and its applications. In Proceedings of the twentieth annual ACM symposium on Theory of computing (STOC '88). Association for Computing Machinery, New York, NY, USA, 103–112. https://doi.org/10.1145/62212.62222

[6] Chen, Thomas & Lu, Hui & Kunpittaya, Teeramet & Luo, Alan. (2022). A Review of zk-SNARKs. 10.48550/arXiv.2202.06877.

[7] Ben-Sasson, Eli et al. “Scalable, transparent, and post-quantum secure computational integrity.” IACR Cryptol. ePrint Arch. 2018 (2018): 46.

[8] B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille and G. Maxwell, "Bulletproofs: Short Proofs for Confidential Transactions and More," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 315-334, doi: 10.1109/SP.2018.00020.

[9] Gabizon, Ariel et al. “PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge.” IACR Cryptol. ePrint Arch. 2019 (2019): 953.

[10] Groth, J. (2016). On the Size of Pairing-Based Non-interactive Arguments. In: Fischlin, M., Coron, JS. (eds) Advances in Cryptology – EUROCRYPT 2016. EUROCRYPT 2016. Lecture Notes in Computer Science(), vol 9666. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-49896-5_11

[11] Alessandro Chiesa, Yuncong Hu, Mary Maller, Pratyush Mishra, Noah Vesely, and Nicholas Ward. 2020. Marlin: Preprocessing zkSNARKs with Universal and Updatable SRS. In Advances in Cryptology – EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part I. Springer-Verlag, Berlin, Heidelberg, 738–768. https://doi.org/10.1007/978-3-030-45721-1_26

[12] Ames, Scott & Hazay, Carmit & Ishai, Yuval & Venkitasubramaniam, Muthuramakrishnan. (2017). Ligero: Lightweight Sublinear Arguments Without a Trusted Setup. 2087-2104. 10.1145/3133956.3134104

[13] Mary Maller, Sean Bowe, Markulf Kohlweiss, and Sarah Meiklejohn. 2019. Sonic: Zero-Knowledge SNARKs from Linear-Size Universal and Updatable Structured Reference Strings. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 2111–2128. https://doi.org/10.1145/3319535.3339817

[14] Setty, Srinath T. V. “Spartan: Efficient and general-purpose zkSNARKs without trusted setup.” IACR Cryptol. ePrint Arch. 2019 (2020): 550.

[15] Kothapalli, A., Setty, S., Tzialla, I. (2022). Nova: Recursive Zero-Knowledge Arguments from Folding Schemes. In: Dodis, Y., Shrimpton, T. (eds) Advances in Cryptology – CRYPTO 2022. CRYPTO 2022. Lecture Notes in Computer Science, vol 13510. Springer, Cham. https://doi.org/10.1007/978-3-031-15985-5_13

[16] Chiesa, A., Ojha, D., Spooner, N. (2020). Fractal: Post-quantum and Transparent Recursive Proofs from Holography. In: Canteaut, A., Ishai, Y. (eds) Advances in Cryptology – EUROCRYPT 2020. EUROCRYPT 2020. Lecture Notes in Computer Science(), vol 12105. Springer, Cham. https://doi.org/10.1007/978-3-030-45721-1_27

[17] Liu, Tianyi & Xie, Tiancheng & Zhang, Jiaheng & Song, Dawn & Zhang, Yupeng. (2024). Pianist: Scalable zkRollups via Fully Distributed Zero-Knowledge Proofs. 1777-1793. 10.1109/SP54263.2024.00035.

[18] Tiancheng Xie, Jiaheng Zhang, Zerui Cheng, Fan Zhang, Yupeng Zhang, Yongzheng Jia, Dan Boneh, and Dawn Song. 2022. ZkBridge: Trustless Cross-chain Bridges Made Practical. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22).

Association for Computing Machinery, New York, NY, USA, 3003–3017. https://doi.org/10.1145/3548606.3560652

[19] Xie, Tiancheng & Zhang, Yupeng & Song, Dawn. (2022). Orion: Zero Knowledge Proof with Linear Prover Time. 10.1007/978-3-031-15985-5_11.

[20] Zhang, Jiaheng et al. “Doubly Efficient Interactive Proofs for General Arithmetic Circuits with Linear Prover Time.” Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (2021): n. pag.

[21] Zero Knowledge Proofs: Challenges, Applications, and Real-world Deployment NIST Workshop on Privacy Enhancing Cryptography September 26th, 2024