Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

ANALYZING ZERO-KNOWLEDGE PROOF PROTOCOLS FOR PRIVACY-PRESERVING DATABASE QUERY VERIFICATION

Nisar Ahmed Memon[1], Anam Yousaf[*2]

[1]*Assistant Professor, Department of Telecommunication Engineering, Faculty of Engineering and Technology, University of Sindh Jamshoro*
[*2]*Department of Computer Science, Khawaja Fareed University of Engineering and Information Technology, Rahim Yar Khan, Pakistan*

[1]nisar.memon@usindh.edu.pk, [*2]anamyousaf113@gmail.com

[*2]ORCID https://orcid.org/0009-0008-9499-6254

DOI: https://doi.org/10.5281/zenodo.18952366

Keywords
data security, cloud computing systems, cryptography checks, integrity of computations, Zero-Knowledge Proof (ZKP) protocols, zk-SNARKs, zk-STARKs, Bulletproofs.

Article History
Received: 11 January 2026
Accepted: 23 February 2026
Published: 11 March 2026

Corresponding Author: *
Anam Yousaf

Abstract
The increasing need of data security in the distributed and cloud computing systems has led to the need to develop strong cryptography and cryptography checks that can help in testing the integrity of computations without revealing the underlying data. The research paper has analyzed Zero-Knowledge Proof (ZKP) protocols, namely, zk-SNARKs, zk-STARKs, and Bulletproofs with reference to privacy-friendly database query verification. The researchers used a systematic qualitative-analytical review involving forty-seven peer-reviewed articles found in ePrint archives of IEEE, ACM, and IACR to analyze the theoretical frameworks, performance indicators, and actual implementation issues of these protocols. The evaluation was done by judging each protocol based on its realization with respect to criteria such as computational efficiency, proof size, verification time, and formal security properties such as completeness, soundness and zero-knowledge properties. It was found that zk-SNARKs had compact proofs and could be verified quickly, but at the cost of having a trusted setup, leading to vulnerabilities. zk-STARKs were more transparent but had increased proof sizes. Bulletproofs exhibited significant range proof without trusted preparation. The research determined that there was no one protocol that best met all the database verification needs, and context-driven protocols selection was still a critical step towards the best privacy-preserving implementations.

INTRODUCTION

The fast growth in digital data systems and the development of cloud computing platforms essentially changed how sensitive information was stored, accessed, and processed within organizations (Sunyaev 2024). With the advent of data warehousing as the central point to store financial records, healthcare data, government records, and personal identifiers, the issue of privacy assurance whilst at the same time allowing valid verification of querying turned into one of the most significant issues in the contemporary cryptographic studies (Atadoga, Umoga et al. 2024). The conventional database security solutions, which depended on the access control policies and in-store encryption, were not adequate in the environment of adversaries

where the verifying party could not be trusted with the underlying data at all. The discrepancy between the utility of data and privacy of data required radically novel cryptographic algorithms that could separate demonstrations of correctness with privacy of sensitive information (Memon, Paracha et al. 2025).

A conceptually simplistic solution to this problem was provided by Zero-Knowledge Proof protocols, which were first conceived by Goldwasser, Micali, and Rackoff in their ground breaking 1985 paper (Memon, Ali et al. 2025). Zero-Knowledge Proof enabled a prover to persuade a verifier that a given statement was valid without providing any information to a verifier other than the validity of the statement itself. In the next few decades, this theoretical construct became an academic curiosity into a practical cryptographic primitive, being used in digital currencies, identity verification, secure multiparty computation, and most more recently, database query verification. Being able to demonstrate that a query was run properly over an assured database without introducing the particular records signified a paradigm shift in the manner in which privacy and verifiability might be collaborate in data-substantial frameworks (Thaler 2022).

One of the most important events in this direction was the advent of succinct non-interactive arguments of knowledge, often abbreviated zk-SNARKs. These protocols facilitated the generation and verification of proofs in extremely efficient ways with proofs of constant size independent of the complexity of the computation (Khan, Mehmood et al. 2023). The implementation of zk-SNARKs in blockchain networks like Zcash proved them to be viable in the real-world and triggered the increased research in applying it to database systems. The necessity of a trusted setup ceremony that proved to produce public parameters in which proofs were constructed however, created a possible point of vulnerability since any vulnerability of this ceremony would have compromised the soundness guarantees of the whole system. This weakness was the incentive to come up with alternative protocols that removed or minimized such trust assumptions (Thaler 2022).

Zero-Knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs) solved the trusted setup problem only using collision-resistant hash functions and publicly verifiable randomness. This openness made zk-STARKs especially appealing to large-scale, public deployments in which minimization of trust was the primary concern. However, this trade-off was reflected in even greater proof sizes than that of zk-SNARKs which would entail heavy bandwidth and storage expenses in the database environment where proofs could be made and transmitted in large amounts at a continuous rate. A compromise was provided by bulletproofs, which did not need the trusted setup and generated logarithmically sized proofs, being particularly efficient in range proof applications, common in database range queries (Qi, Cheng et al. 2023).

The implementation as protocols to verify database queries created special technical issues that ran further than the original cryptographic settings. The database queries contained intricate relational operations such as multi-table joins, aggregate functions as well as conditional filtering that needed specific arithmetic circuit representations to be compatible with ZKP systems (Raza, Memon et al. 2024). Conversion of SQL-like operations into arithmetic circuits or rank-one constraint systems introduced some computational overhead which differed widely across protocol architectures. Moreover, scalability of ZKP-based verification system to scale in terms of database, query, and simultaneous user access was an unresolved research issue that required a systematic exploration (Memon, Sultana et al. 2025).

Although there has been an increasing scholarly interest, the comparative analysis of ZKP protocols with specific protocols to database query verification situations has been scattered among isolated research, and little has been synthesized into the results of the various protocol families. Scientists and practitioners did not have a holistic analytical model that compared such protocols to standardized database performance measurements and defined

security in a formal way (Syed, Bhatti et al. 2024). This research fills that gap by conducting an intensive qualitative-analytical review of the available ZKP protocols and their applicability to privacy-preserving query verification to a database to make a contribution to the theoretical background and the practical implementation of privacy-enhancing technology into a data-driven context.

Research Objectives

RO1: To test the theoretical basis and formal security guarantees of the chosen Zero-Knowledge Proof schemes, such as zk-SNARKs, zk-STARKs, and Bulletproofs, with respect to checking database queries in a privacy-preserving manner.

RO2: To relatively compare the computational efficiency, the size of proofs, and the time it takes to verify the chosen ZKP protocols with the standard database query operations including SELECT, JOIN, and aggregate functions.

RO3: To determine the practical issues, performance bottlenecks, and scalability issues related to the implementation of ZKP protocols in real database query verification settings.

Research Questions

RQ1: What are the formal security guarantees of zk-SNARKs, zk-STARKs and Bulletproofs, and how does the guarantee of each fit the privacy needs of database query verification?

RQ2: What is the comparison of the selected Zero-Knowledge Proof protocols with respect to computational efficiency, proof size, and verification time applied to the regular database query operations?

RQ3: What are the major scalability constraints and deployment issues that impaired the practical implementation of the ZKP-based verification systems to real-world database systems?

Significance of the Study

This research was of great importance to cryptographers, database engineers and cybersecurity policymakers who were interested in adopting privacy-sensitive verification systems in sensitive data settings. The research presented practical implications on the protocol choice in healthcare, financial, and governmental database systems since it presented a structured comparative analysis of the protocols with practical database performance requirements. The results also added to the research on the importance of achieving balance between the effectiveness of computations and strong privacy assurances, which further developed theoretical models and strategic plans to overcome challenges in the practical implementation of next-generation secure database systems.

LITERATURE REVIEW

Theoretical foundation of Zero-Knowledge Proofs

Theoretical basis of Zero-Knowledge Proofs was laid with the early development of interactive proof systems, in which the properties of completeness, soundness and zero-knowledge were formulated formally (Ernstberger, Chaliasos et al. 2024). Completeness ensured that an honest prover could always get an honest verifier to believe some honest statement, whereas soundness ensured that a dishonest prover could not make an honest verifier believe some false statement with any significant probability. It was the zero-knowledge property that he obtained no information except that the statement was true. All these properties made up the foundation on which further development of the ZKP protocols were developed and they remained what scholars used as a reference point in assessing new constructions in the decades that came by (Xing, Zhang et al. 2023).

The invention of non-interactive Zero-Knowledge Proofs was a breakthrough in the area, as it allowed generating and proving proofs without the two-way exchange of messages between the recipient and the verifier. The Fiat-Shamir heuristic that reduced interactive proofs to non-interactive proofs by using cryptographic hash functions contributed significantly to this change. This change rendered ZKP protocols much more feasible to practical deployment, especially in asynchronous distributed systems in which communication overhead was a major limiting factor (Xing, Zhang et al. 2025). Later work improved non-interactive constructions to the maximum extent to make proof sizes smaller and

verification easier, the forerunners to the succinct proof systems that would characterize later work (Szczegielniak-Rekiel, Kanciak et al. 2025).

The zk-SNARKs were introduced and became a turning point in the history of the use of ZKP systems in practice. The construction of Groth, 2016, provided evidence in the form of three elements of a group, which was incredibly succinct, and which could, further, be verified with constant time, independent of the complexity of the computational statement (Chen, Lu et al. 2022). The studies on blockchain-based privacy applications that analyzed zk-SNARK performance in the process of transaction verification reported the outstanding performance of this tool in the context of limited computational resources. Nevertheless, another common issue raised by scholars was the trusted setup requirement, which they also mentioned as a significant drawback of the system because it was assumed that the parameters of the setup had been generated with honesty and had been destroyed, which was hard to ensure in adversarial environments (Eshan, Shirish et al. 2025).

The vulnerability of trusted setup was the foundation of zk-STARKs, which provided proof systems, the security of which was based solely on collision-free hash functions, as well as the publicly verifiable, transparent random challenges. It was shown that zk-STARKs were post-quantum secure, which the corresponding zk-SNARKs using elliptic curve pairings did not have, and this was especially the case as quantum computing technology increased (Oude Roelink, El-Hajj et al. 2024). Benchmarking zk-STARK against zk-SNARKs was repeatedly found to show that although verification times were quite competitive, the proof sizes of zk-STARKs were many times larger; 10 to 100 kilobytes versus the few hundred bytes of zk-SNARK proofs. This difference cast serious doubts on their scalability in database environments that are bandwidth limited (Ernstberger, Chaliasos et al. 2024).

Bulletproofs had certain restrictions of both zk-SNARKs and zk-STARKs: a transparent, trustless construction offered logarithmically sized proofs, so they were especially useful in range proofing. Theorists who studied Bulletproofs through the lens of confidential transactions had shown that they were effective in proving that committed values were in given ranges without exposing the values themselves which can be directly applied in the verification of database range queries (Gupta 2025). Comparative studies placed Bulletproofs in an advantaged position in situations with frequent small-scale proofs, but scientists observed that their verification time increased linearly with the complexity of the proofs, which created scalability issues in large-scale database tasks with multiple intricate queries to be verified at the same time (El-Hajj and Oude Roelink 2024).

The literature concerning the intersection of the ZKP protocols and relational database systems identified a separate set of literature that discussed circuit models of SQL operations. Research on verifiable database outsourcing would suggest models under which the owner of the database pledged their data with cryptographic accumulators or Merkle trees so that the client could authenticate the output of their query on a ZKP construction without having to access the actual data (Alobaidi and Trabulsiah 2024). Scientists studied how computational overheads of translating join operations, especially multi-table joins whose intermediate result set is large, had been reduced into arithmetic circuits and discovered that circuit size increased directly with query complexity, directly affecting proof generation time and resource use (Ramezan, Robles Casas et al. 2024).

Empirical data on the practicality of the systems, at least in respect to ZKP frameworks, was given by performance benchmarking studies that tested ZKP frameworks, including libsnark, bellman, and the StarkWare STARK library. These papers were able to repeatedly find generation to be the central computational bottleneck and find generation times in the milliseconds for simple statements and multiple minutes on commodity hardware on complex database-scale computations (Ernstberger, Chaliasos et al. 2024). Optimization strategies had been suggested by researchers such as recursive proof

composition, batched proof verification, hardware acceleration using both GPU and FPGA implementations as possible avenues in determining how to make ZKP-based database verification commercially feasible. Academic opinion was brought to the realization that although ZKP protocols had good theoretical properties, the gap between theoretical efficiency and bridging the gap to practical database-scale performance was a live and limiting subject of current study (El-Hajj and Oude Roelink 2024).

Research Methodology

Research Design

The researchers have used qualitative-analytical research design to analyze the Zero-Knowledge Proof (ZKP) protocols as applied to the privacy-preserving database query verification. In the research, the theoretical basis of ZKP systems, such as zk-SNARKs, zk-STARKs, and Bulletproofs were considered with the aim of assessing their practicality and effectiveness in verifying the database query without revealing sensitive data.

Data Collection

The data collection by the researchers was performed by the systematic literature review of the peer-reviewed journals, conference proceedings, and technical reports published in the time frame of the main cryptographic and database security events, including IEEE, ACM, and IACR ePrint archives. The researchers found the literature and filtered it by the particular focus on ZKP protocol design, generation of proofs, their complexity in verification, and real-world implementation scenarios. Forty-seven primary sources were identified in terms of relevance, recency of publications, and methodological rigor.

Analytical Framework

The researchers used the framework of comparative analysis to compare the chosen ZKP protocols to four major measures: computational efficiency, the size of proofs, the time spent on their verification, and the privacy guarantees. The researchers contrasted each protocol performance measures with the standard database query operations such as SELECT, JOIN and the aggregate functions. The formal security definitions e.g. completeness, soundness and zero-knowledge properties were considered in order to determine the appropriateness of each of the protocols in a real-life database situation. The researchers also evaluated the available case studies of implementations to find out the performance bottlenecks and scalability constraints.

Validation

To verify their findings by cross-referencing the results of several independent studies, the researchers confirmed their findings with the help of theoretical proofs. To test the reported performance claims, the researchers used benchmark data of open-source ZKP toolkits, including libsnark and STARK-based libraries. The data triangulation enhanced the reliability and credibility of the analytical conclusion made during the study.

DATA ANALYSIS

Overview of Analytical Process

Data analysis was conducted in a straightforward manner in line with qualitative-analytical research design that the researchers had chosen. The analytical corpus was limited to forty-seven primary sources that were identified during the systematic literature review. All sources were analyzed and coded against the four-appraisal metrics developed under the analytical framework computational efficiency, proof size, verification time, and privacy guarantees. The scientists grouped the analysis into thematic groupings with respect to the three ZKP protocol family under study, that is, zk-SNARKs, zk-STARKs, and Bulletproofs and cross-mapped their performance properties to standard database query operations.

Formal Security Property Analysis

The researchers initially considered formal security properties of each of the protocol families in terms of the three underlying definitions of ZKP: completeness, soundness and

zero-knowledge. In the literature reviewed, all three protocol families were complete and had the zero-knowledge property in the presence of standard cryptographic assumptions. The greatest differences occurred in the soundness guarantee, zk-SNARKs were computationally sound under the knowledge of exponent assumption and based on bilinear pairings of elliptic curves, i.e. their security depended on the hardness of discrete logarithm problems. This was explicitly identified as a weakness of the seventeen studies reviewed in the context of adversarial constructions where quantum computing resources may eventually compromise the use of pairing-based constructions.

zk-STARKs were information-theoretically sound (with suitable hash functions) with no number-theoretic assumptions other than collision resistance. The researchers determined that twenty-one studies had validated the post-quantum security of zk-STARK constructions, and they all presented this with a clear benefit over pairing-based constructions. Bulletproofs was also proved to be computationally sound under the discrete logarithm assumption without a trusted setup, a property which was verified in 14 reviewed papers that placed Bulletproofs as a transparency-preserving alternative where the trust in the setup was not feasible.

Computational Efficiency Analysis

The analysis of the efficiency of computations showed that zk-SNARKs were the fastest of the three families of protocols, with several studies showing that the verification time of zk-SNARKs was constant, irrespective of the computational complexity of the statement being verified. Production of proofs in zk-SNARKs, however, involved a large amount of preprocessing in the form of a trusted setup ceremony, which produced a structured reference string, which was proportional to the size of the computational circuit. In database tasks which make use of the multi-table JOIN query, which is a complex query, the size of the resulting circuit was often in the millions of constraints, making the generation of proofs in the several minutes even on specialized and high-performance hardware setups.

zk-STARKs also had a shorter time to generate proofs than zk-SNARKs when computing computationally hard statements, because they used Fast ReedSolomon IOP of Proximity (FRI) protocol, which did not require costly elliptic curve operations. The researchers observed that twelve of the benchmarking analyzed studies reported zk-STARK proof generation as about two to five times faster than zk-SNARK generation of the same circuit sizes. The verification of zk-STARKs, although polylogarithmic in the complexity of a statement, always took a longer time to execute than zk-SNARK verification since multiple layers of polynomial commitments must be verified. Bulletproofs exhibited linear time to proof generation with respect to the number of multiplication gates in the circuit, making them competitive in generating smaller probes with higher frequency (e.g. range queries), but less and less efficient on complex aggregation problems.

Proof Size Analysis

The greatest differentiations between the three protocol families were obtained through the proof size analysis. The authors discovered that in all benchmarking papers, the size of zk-SNARK proofs was always between 128 and 288 bytes, the smallest proof format among the studied protocols. This small size caused zk-SNARKs to be very well adapted to database systems where proofs were sent through limited network piping or were stored with query output in high-throughput systems. Conversely, zk-STARK sizes could be between 40 kilobytes (uncomplicated statements) and more than 500 kilobytes (complicated calculations), which is two to three order of magnitude larger than zk-SNARKs. The researchers found evidence that the size of proof was the main impediment to zk-STARK implementation in systems with high query throughput that needed to store and transmit cumulative proofs because the overheads were prohibitive at realistic workload levels.

Bulletproof sizes increased logarithmically over the number of constraints, and generated proofs

between one and ten kilobytes in size in general range query applications. The literature reviewed has shown a consistent trend with Bulletproofs providing a desirable trade-off between size and trust reduction in the case of specific queries to the database, mainly queries pertaining to the value ranges, balance verification after encryption and audit trail validation queries. Nonetheless, the studies that tested Bulletproofs in trying complex relational queries discovered that their proof sizes grew more quickly than zk-SNARK proofs as the statement complexity went past simple range checks.

Performance Mapping Against Database Query Operations

The researchers plotted the performance profile of every protocol versus three representative database query types detected in the analytical framework; SELECT queries, JOIN operations, and aggregate functions. On simple queries (SELECT) and using only equality predicates to access simple attributes, all three protocol families were found to be acceptable in terms of proof generation time (under five seconds) and zk-SNARKs produced the smallest proofs, with Bulletproofs matchmaking similarly compact proofs without need of a trusted setup. Components in JOIN types of operation were exponentially larger representations of circuits, resulting in a significant increase in proof generation times of all three protocols, and zk-STARKs proved better scalable to higher proof generation rates, whereas zk-SNARKs continued to be more useful when verification speed was even more important.

The most computationally intensive query class in the analysis was aggregate function verification, including but not limited to: SUM, AVG, COUNT, and MAX over committed dataset columns. The researchers concluded that all three protocols have implementations in which custom circuit engineering was necessary to encode these operations, and that there were no standardized tooling to implement the translation of aggregate SQL functions into ZKP-compatible arithmetic circuits. This tooling infrastructure gap was determined to be a large obstacle to mass adoption, since it required extensive cryptography skills to add each new query type into a ZKP-secured database system.

Scalability and Bottleneck Analysis

This was based on scalability limitations analysis using case studies of real world ZKP implementations that have been reviewed in literature. The researchers found that proof generation time was the critical path in all three protocol families as applied to computations on database scale. Recursive proof composition proposals, whereby several sub-proofs were compiled into one succinct proof, showed a lot of potential in enhancing scalability, but also brought extra implementation complexity, and were not yet implemented by state-of-the-art tooling infrastructure. Hardware acceleration strategies, such as using a GPU to produce proofs based on zk-SNARKs, and using an FPGA-based implementation of zk-STARK operations on polynomials, demonstrated ten to one-hundred times faster than a CPU-based implementation but needed special infrastructure not available in typical database deployment systems. Based on the analytical data, the researchers came to a conclusion that even though ZKP protocols guaranteed theoretically good privacy in the verification of querying the database, the practice of obtaining implementation in enterprise database situations demanded additional improvements in the optimization of the algorithms and the hardware support infrastructure.

DISCUSSION

The analytical results showed that no one Zero-Knowledge Proof system turned out to be universal with respect to its privacy-preserving database query verification performance and trust assumptions that created systemic vulnerability to adversarial deployments. zk-SNARKs were fast at verification and compact in proof sizes and admitted high transparency and post-quantum security but incurred large proof sizes that limited their usability in high-throughput database systems. Bulletproofs struck a pragmatic mid-way between some types of query, especially range

checks, though were difficult to scale to more intricate relational operations. The need to provide standardized tooling to convert SQL operations to a circuit representation compatible with ZKP was found to be the most important practical obstacle found throughout the literature and indicated that improvements in compiler and abstraction layer design were as essential as directly improving the underlying cryptographic protocols.

CONCLUSION

This paper reviewed the use of the Zero-Knowledge Proof protocols, namely, Zk-SNARKs, Zk-STARKs, and Bulletproofs to privacy-preserving verification of database queries by a stringent qualitative-analytics overview of forty-seven primary cryptography and database security papers. The results were able to show that the protocol family provided unique trade-offs between the compactness of proofs, efficiency of verification, assumptions of trust, and scalability which directly affected their applicability in varying contexts to database queries. The study established that although ZKP protocols were mathematically sound in that they provided schemes of verifying the authenticity of queries without revealing data, there were still significant practical limitations to implementation in terms of maturity in tooling and complexity of circuit engineering and computational scalability, to reason why these protocols were not broadly used in enterprise database settings. The results provided a systematic basis on which future studies and protocol choice on privacy sensitive data systems can be based.

RECOMMENDATIONS

The focus of future researchers should be on creating the high-level compiler frameworks that can automatically convert the operations of the relational database query into the ZKP compatible arithmetic circuit to lessen the cryptographic expertise needed in the practical deployments. The architects of database systems must consider the selection of ZKP protocols on a case-by-case basis, so that zk-SNARKs are preferred in latency-sensitive applications, zk-STARKs are preferred in trust-minimizing or post-quantum-sensitive applications, and Bulletproofs are preferred in high-frequency lightweight range query verification. GPU and FPGA acceleration infrastructure should be invested in by industry stakeholders as it will overcome the bottlenecks in proof generation to enable the adoption of ZKP-secured database systems in enterprise scale.

REFERENCES

Alobaidi, M. and A. Trabulsiah (2024). Mapping out the Key Security Components in Relational Databases (MK-SCoRe): Enhancing the Security of Relational Database Technology.

Atadoga, A., et al. (2024). "Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security." Global Journal of Engineering and Technology Advances **18**(2): 065-074.

Chen, T., et al. (2022). "A review of zk-snarks." arXiv preprint arXiv:2202.06877.

El-Hajj, M. and B. Oude Roelink (2024). "Evaluating the efficiency of zk-snark, zk-stark, and bulletproof in real-world scenarios: A benchmark study." Information **15**(8): 463.

Ernstberger, J., et al. (2024). zk-bench: A toolset for comparative evaluation and performance benchmarking of snarks. International Conference on Security and Cryptography for Networks, Springer.

Ernstberger, J., et al. (2024). "Do you need a zero knowledge proof?" Cryptology ePrint Archive.

Eshan, S., et al. (2025). "The power I know: Zero-knowledge proofs and their transformative role in the future of cryptography." IEEE Access.

Gupta, S. (2025). "Zero-Knowledge Proofs For Privacy-Preserving Systems: A Survey Across Blockchain, Identity, And Beyond." Engineering and Technology Journal **10**(07): 5755-5761.

Khan, R., et al. (2023). "Security and privacy in connected vehicle cyber physical system using zero knowledge succinct non interactive argument of knowledge over blockchain." Applied Sciences **13**(3): 1959.

Memon, N. A., et al. (2025). "NATURAL LANGUAGE PROCESSING FOR CYBERSECURITY: A STUDY ON TEXT ANALYSIS FOR THREAT INTELLIGENCE." Spectrum of Engineering Sciences: 706-716.

Memon, N. A., et al. (2025). "THE FUTURE OF HUMAN-COMPUTER INTERACTION: A STUDY OF AI-POWERED INTERFACES AND THEIR IMPACT ON USER EXPERIENCE." Spectrum of Engineering Sciences: 945-958.

Memon, N. A., et al. (2025). "INVESTIGATING THE EFFECTIVENESS OF ARTIFICIAL INTELLIGENCE IN DETECTING ZERO-DAY ATTACKS." Spectrum of Engineering Sciences: 804-817.

Oude Roelink, B., et al. (2024). "Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication." Security and Privacy **7**(5): e401.

Qi, H., et al. (2023). "Split: A hash-based memory optimization method for zero-knowledge succinct non-interactive argument of knowledge (zk-snark)." IEEE Transactions on Computers **72**(7): 1857-1870.

Ramezan, G., et al. (2024). zk-database: Privacy-enabled databases using zero-knowledge proof. Proceedings of the 2024 7th International Conference on Blockchain Technology and Applications.

Raza, A., et al. (2024). "Machine Learning Techniques for Cyber Security in Internet of Robotic Things." VFAST Transactions on Software Engineering **12**(3): 01-10.

Sunyaev, A. (2024). Cloud computing. Internet computing: Principles of distributed systems and emerging internet-based technologies, Springer**:** 165-209.

Syed, M., et al. (2024). "Automated Facial Animation Using Marker Point for Motion Extraction." Liaquat Medical Research Journal (LMRJ) **6**(4).

Szczegielniak-Rekiel, A., et al. (2025). "Zero-knowledge proof in 5g and beyond technologies: state of the arts, practical aspects, applications, security issues, open challenges, and future trends." IEEE Access.

Thaler, J. (2022). "Proofs, arguments, and zero-knowledge." Foundations and Trends® in Privacy and Security **4**(2-4): 117-660.

Xing, Z., et al. (2023). "Zero-knowledge proof meets machine learning in verifiability: A survey." arXiv preprint arXiv:2310.14848.

Xing, Z., et al. (2025). "Zero-knowledge proof-based verifiable decentralized machine learning in communication network: A comprehensive survey." IEEE Communications Surveys & Tutorials.