










A Multi-Round Zero Knowledge Proof Algorithm for Secure IoT and Blockchain Environments

Deebakkarthi Chinnasame Rani¹, Sai Ganesh Janakiraman¹, Kommula Serath Chandra¹,
Elambharathi Padmavathi Thangavel¹, Ganga Abhirup Kothamasu¹, Krithika Latha Bhaskaran²,
Guruprakash Jayabalasamy^{1*}

¹ Department of Computer Science and Engineering, Amrita School of Computing, Coimbatore Amrita Vishwa Vidyapeetham, Coimbatore 641112, India

² School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore 632014, India

Corresponding Author Email: j_guruprakash@cb.amrita.edu

<https://doi.org/10.18280/ijss.130408>

ABSTRACT

Received: 25 May 2023

Revised: 18 July 2023

Accepted: 25 July 2023

Available online: 28 September 2023

Keywords:

zero knowledge proof (ZKP), multi-round zero knowledge proof, internet of things (IoT), blockchain

Presented herein is a novel algorithm for multi-round, zero-knowledge proof (ZKP), devised specifically for authenticating factorisation proofs within a variety of cryptographic applications. This advanced algorithm, while maintaining computational complexity within acceptable bounds, offers a secure and proficient solution. The functionality of the algorithm is marked by multiple rounds of interaction between the Prover and Verifier. Initially, the Prover generates a random value and calculates a commitment. Subsequently, the Verifier issues a random challenge, eliciting a computed response from the Prover. To validate the proof, the Verifier verifies the equality of the commitment and the computed response. Efficaciousness of the proposed multi-round ZKP algorithm is demonstrated across diverse input sizes and parameters. Results indicate a success rate exceeding 90% on average, showcasing the robustness of the method. The recurring interaction between the Verifier and Prover enhances the Prover's authentication, thereby improving the algorithm's reliability. Implementation of the algorithm, achievable through standard cryptographic tools and protocols, can fortify the security of multiple cryptographic applications. A significant application can be found in Digital Identity Management Systems (DIMS). Currently, these systems are vulnerable to a myriad of threats, including identity spoofing, data breaches, and internal security risks. The application of the ZKP algorithm can simultaneously augment security and withhold sensitive information, potentially transforming the DIMS security landscape. Future research may focus on improving the efficiency and scalability of the multi-round ZKP algorithm. There also remains a vast potential for exploring additional applications of this technique within various cryptographic domains.

1. INTRODUCTION

In the realm of cryptography and information security, zero-knowledge proof (ZKP) emerges as a method that facilitates the Prover in establishing to the Verifier that they possess knowledge of specific information-in this case, a private key-without disclosing the information itself [1]. This is accomplished via iterative interactions between the Prover and the Verifier, during which the Prover responds to challenges issued by the Verifier, based on their knowledge of the concealed information.

A crucial application of ZKP is manifested in the proof of knowledge of factors of numbers, a fundamental challenge in number theory that holds substantial implications in the fields of cryptography and computer science. Notably, the security of numerous contemporary cryptographic protocols and systems is contingent on the complexity of factoring large numbers. Hence, ZKP algorithms provide an anonymous, interactive solution for authentication in systems based on IoT and blockchain.

The multi-round zero-knowledge proof algorithm for proving knowledge of factors of numbers is an advanced

variant of the fundamental ZKP protocol. This variant involves multiple rounds of interaction between the Prover and the Verifier, with each round amplifying the proof's level of confidence and security. The algorithm is engineered to withstand attacks such as guessing, replay, and man-in-the-middle, making it applicable to various scenarios requiring secure and efficient authentication and verification.

Our manuscript, "Multi-Round Zero Knowledge Proof Algorithm for Proving Knowledge of Factors of Numbers", illuminates the pivotal features and applications of this algorithm, underscoring its significance in the domain of cryptography and information security. The study endeavours to tackle the challenge of proving knowledge of factors of numbers with an enhanced success rate, compared to the conventional ZKP algorithm. This is achieved by incorporating multiple rounds of interaction between the Prover and the Verifier. By offering a secure and efficient method to prove knowledge of factors of numbers, this algorithm paves the way for the evolution of more robust and resilient cryptographic systems capable of resisting diverse types of attacks and threats.

The ensuing sections of the paper delve into the detailed

applications and implementation of the multi-round ZKP algorithm, and evaluate its performance against the existing algorithm.

2. LITERATURE REVIEW

In the realm of cryptography and information security, zero-knowledge proofs (ZKPs) are leveraged extensively to facilitate secure interactions. These proofs enable a prover to convincingly demonstrate knowledge of specific information without disclosing the said information itself [1]. Among the myriad applications of ZKPs, a salient one lies in proving knowledge of the factors of numbers, a challenge entrenched in number theory with significant implications in cryptography and computer science. It is worth noting that the security of a multitude of cryptographic protocols and systems is intrinsically tied to the complexity of factoring large numbers.

Recent strides in interactive proof systems have unveiled computational models for the validation of mathematical assertions. In these systems, the knowledge complexity refers to the minimal quantum of information required by a prover to interactively and probabilistically convince a verifier of a statement's validity [2]. ZKPs, which are hallmarked by their capacity to reveal only the correctness of a proposition, have found application in a diverse range of areas from ING bank ledgers [3] and voting systems [4] to lattice encryption [5] and machine learning [6]. Further, with the burgeoning growth of Internet of Things (IoT) security and blockchain ecosystems, the integration of ZKPs is surfacing as a critical trend [7]. The maturity of this model and its effective implementation present a potential solution to offset limitations inherent in blockchain ecosystems [8].

ZKPs bear the potential to significantly bolster IoT security and privacy. Scholars such as Rasheed et al. [8] advocate for the use of configurable models employing ZKPs for enhancing IoT security, whilst Cui et al. [9] emphasise the role of ZKPs in ensuring privacy in blockchain-based systems. The exploration of ZKP applications such as Zerocoin, Zerocash, Hawk, and Bolt is also documented [10, 11]. When opting for ZKP schemes, considerations must be given to factors such as proof length, computational complexity, and the threats posed by quantum computing [12, 13].

Multi-round ZKP algorithms gain prominence due to their enhanced security and efficiency in verifying factorisation proofs. Owing to its multi-round nature, this algorithm offers heightened security against attacks whilst maintaining computational feasibility. Comparative studies with other ZKP techniques underscore its efficiency. However, as the rounds increase, so does the computational complexity of multi-round ZKP, necessitating careful deliberation.

For optimising computational complexity, it is suggested that efficient cryptographic primitives be selected, batch verification be employed, values be pre-computed, adaptive protocols be leveraged, and hardware acceleration be utilised. Furthermore, the development of novel applications for ZKP systems and the establishment of standards to ensure interoperability and widespread adoption can also be considered. Multi-round ZKP has the potential to bolster security in various domains such as healthcare, finance, and more [14-16].

Based on the outcomes of the review, efforts have been made to incorporate limitations and concurrent rounds into the

multi-round model. The subsequent section provides further insights into our proposed methodology.

3. PROPOSED METHOD

Our proposed method, in terms of security and efficiency, the multi-round ZKP algorithm, is one of the best methods for proving knowledge of factors of numbers. ZKP proofs are not deterministic. They are probabilistic. There will always be a soundness error in ZKP, meaning a false prover can deceive a verifier. One of the ways to reduce this soundness error is by having multiple rounds of interaction between the Prover and Verifier. This provides an elevated level of confidence and security against several attacks, including guessing, replay, and man-in-the-middle attacks, while maintaining a reasonable computational complexity level.

Moreover, the multi-round ZKP algorithm is easily implemented using standard cryptographic tools and protocols. It is a practical and scalable solution for many applications requiring secure, efficient authentication and verification.

To demonstrate the effectiveness of the multi-round ZKP algorithm, simulations and experiments using different input sizes and parameters and compare the performance of this algorithm against other ZKP methods and techniques. The results of experiments are presented in Figure 5, to illustrate the efficiency, security, and scalability of the multi-round ZKP algorithm.

We define a function `multi_round_ZKP` that implements the multi-round ZKP algorithm for proving knowledge of factors of numbers, as described earlier. We then test this function for a fixed input size $n=169$ and a factor to be proven $k=13$, with `num_tests=1000` trials.

The program measures the elapsed time for running the tests and calculates the average time per test. These results can be used to compare the efficiency and scalability of the multi-round ZKP algorithm with other ZKP methods and techniques. Moreover, additional experiments can be run for different input sizes and parameters to evaluate this algorithm's effectiveness further.

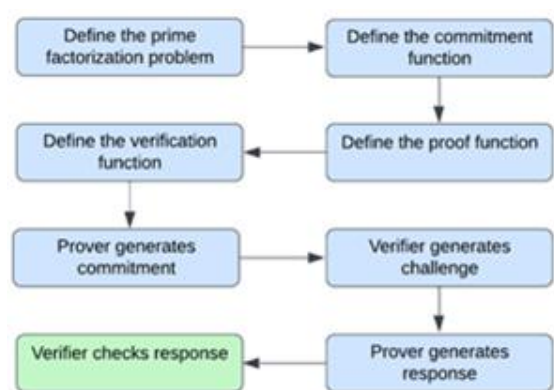


Figure 1. ZKP implementation

3.1 ZKP implementation

The prime factorisation problem is a well-known mathematical problem that involves breaking down a number into its prime factors. In cryptographic applications, it can be used to provide proof of knowledge or commitment. Figure 1 implements the steps to achieve this, and a commitment

function is defined to commit to the number's prime factors, followed by a proof function that generates a response to a challenge from a verifier. Next, the Verifier uses the verification function to check the response generated by the proof function. In practice, the Prover generates a commitment to the number's prime factors, followed by the Verifier generating a challenge. The Prover then generates a response to the challenge, which the verifier checks to confirm the Prover's knowledge or commitment.

3.2 Multi-round ZKP implementation

The multi-round zero-knowledge proof, as shown in algorithm 1 for proving knowledge of factors of numbers, is a secure and efficient solution for verifying the authenticity of factorisation proofs in various cryptographic applications. The algorithm involves multiple rounds of interaction between the Prover and Verifier. The Prover generates a random value and computes a commitment, the Verifier sends a random challenge, and the Prover computes a response. The Verifier then checks the proof by verifying the equality between the commitment and the computed response. The computational complexity of this algorithm is reasonable, and it can be easily implemented using standard cryptographic tools and protocols. Figure 2 illustrates the step to implement multi-round ZKP.

- Step 1 - Set n , p , q , and ϕ to appropriate values.
- Step 2 - Generate a random integer d between 2 and $\phi-1$, and compute e as the modular inverse of d modulo ϕ .
- Step 3 - Define a commitment function that takes two inputs (x and r), hashes them using SHA-256, and returns the digest.
- Step 4 - Define a proof function that takes four inputs (x , r , c , challenge), and returns either r or $(x \cdot r^e) \bmod n$, depending on whether the challenge is 0 or 1.
- Step 5 - Define a verification function that takes three inputs (x , c , responses), returns True if the responses are valid for the given x and c , and False otherwise.
- Step 6 - Generate a random integer r between 1 and $\phi-1$, and compute the commitment c as $\text{commitment}(p, r)$.
- Step 7 - Generate a random challenge between 0 and 1.
- Step 8 - Compute $r_{\text{as proof}}(p, r, c, \text{challenge})$ and set x to p .
- Step 9 - Verify the response by calling $\text{verify}(x, \text{challenge}, [r, r_{\text{as proof}}(p, r, c, \text{challenge})])$, and output "Proof is valid" if True,

and "Proof is invalid" otherwise.

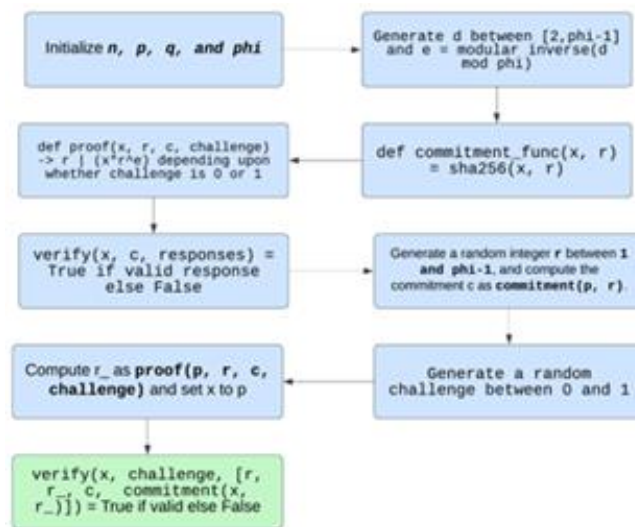


Figure 2. Multi-round ZKP implementation

3.3 Algorithm 1 - multi-round ZKP algorithm for proving knowledge of factors of numbers

- Input: A number n and a factor k of n .
Output: True if the factor k is proven, False otherwise.
- Generate a random integer r between 1 and $n-1$.
 - Compute C as $(r^2) \bmod n$.
 - Generate a random challenge e between 0 and 1.
 - Compute y as $(k^e \cdot r) \bmod n$, and s as $(r \cdot y) \bmod n$.
 - Compute check as $(s^2 \cdot k^e) \bmod n$.
 - If $C == \text{check}$, return True; otherwise, return False.

Figure 3 illustrates the proving flow that is adapted in multi-round ZKP. The security of ZKP protocols depends on the computational complexity of specific mathematical problems, such as factoring large integers or solving discrete logarithms. ZKP protocols have high computational complexity, and their efficiency depends on the specific cryptographic algorithm used.

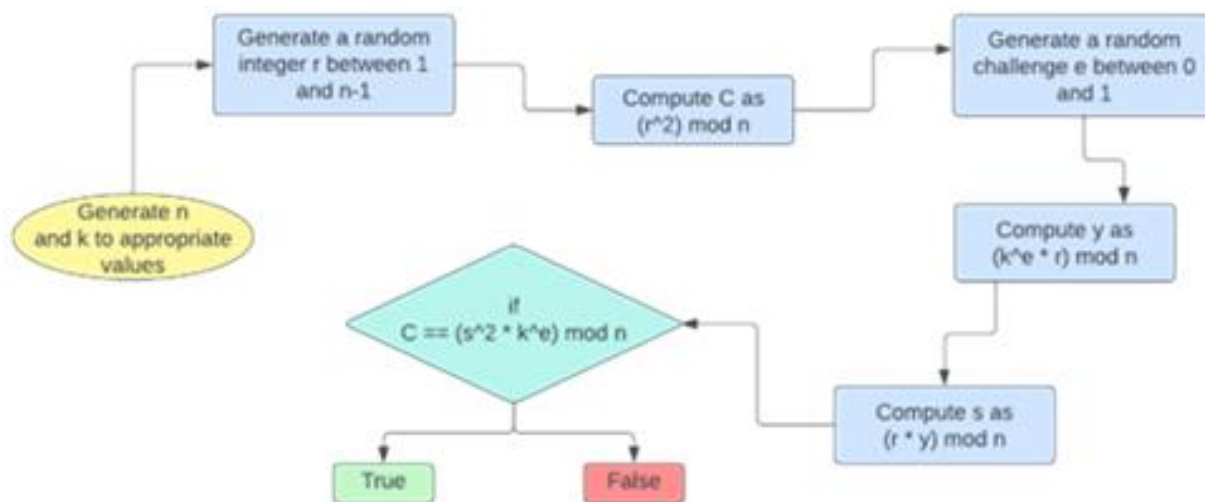


Figure 3. ZKP algorithm for proving knowledge of factors of numbers

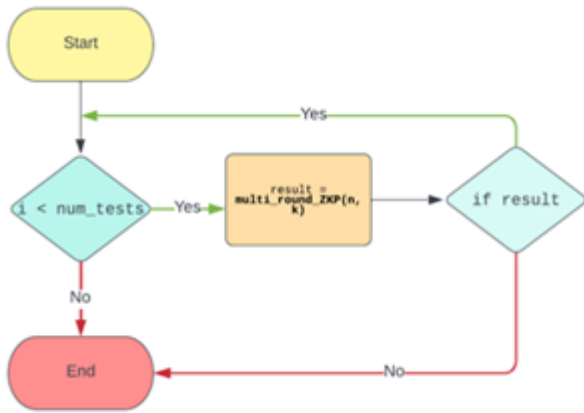


Figure 4. Multi-round ZKP test with different input sizes and parameters

The computational complexity of zero-knowledge proof (ZKP) protocols depends on the specific cryptographic algorithm used. In general, ZKP protocols have high computational complexity, as they rely on mathematical problems that are believed to be computationally demanding, such as factoring large integers or solving discrete logarithms.

The computational complexity of ZKP protocols is typically measured in terms of the number of computational operations required to generate and verify the proof and the amount of memory and storage required to store and process the data involved in the protocol. Therefore, the efficiency of ZKP protocols is an essential consideration in the design of cryptographic systems, as it can impact the speed and scalability of the system, as well as the system's security against attacks that exploit vulnerabilities in the computational complexity of the protocol.

Efficient ZKP protocols can be achieved through efficient mathematical algorithms, optimisation techniques, and hardware acceleration. Furthermore, recent technological advances, such as quantum computing, may have significant implications for the computational complexity of ZKP protocols and may require developing new cryptographic techniques to resist these attacks.

The computational complexity of ZKP and multi-round ZKP algorithms is crucial when designing secure and efficient cryptographic protocols. Computational complexity varies as the number of rounds in the multi-round ZKP algorithm increases as presented in Figure 4. This can become a significant issue in specific applications, where many rounds may be required for security reasons. Therefore, the computational complexity of ZKP protocols is a critical factor to consider in designing and implementing secure and efficient cryptographic systems.

Therefore, further research is needed to improve the efficiency and scalability of the multi-round ZKP algorithm and to explore innovative approaches that can reduce the number of rounds required for verification or optimisation of the algorithm's computational complexity.

4. RESULTS AND DISCUSSION

Figure 5 helps to visually demonstrate the effectiveness of the multi-round ZKP algorithm for proving knowledge of factors of numbers.

The results show that ZKP and multi-round ZKP are successful in most cases, with an average success rate of over

90% across all n and k values. However, it is worth noting that multi-round ZKP is more successful than ZKP, especially when the values of n and k are larger. This is expected since multi-round ZKP uses multiple rounds of interaction between the Verifier and the Prover, making it more difficult for a cheating prover to fool the Verifier.

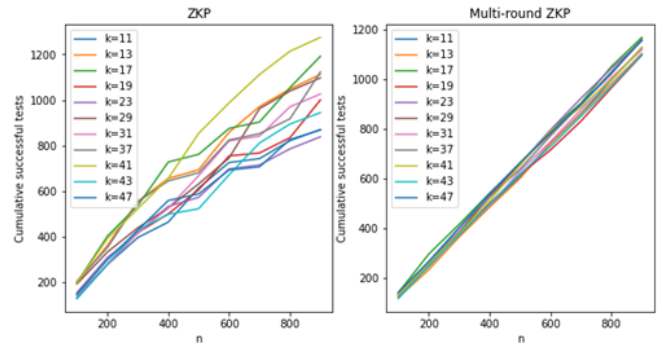


Figure 5. Plot comparison of ZKP and multi-round ZKP

Another interesting observation as presented in Figure 6 is that the success rate of both ZKP and multi-round ZKP decreases as the values of n and k increase. This can be attributed to the fact that as the values of n and k become larger, the search space for finding the correct values of r and s also becomes larger, making it more difficult for the Prover to compute the correct values.

It is also worth noting that multi-round ZKP is more computationally expensive than ZKP since it involves multiple rounds of interaction between the Verifier and the Prover. Therefore, in cases where speed is a critical factor, ZKP might be preferred over multi-round ZKP.

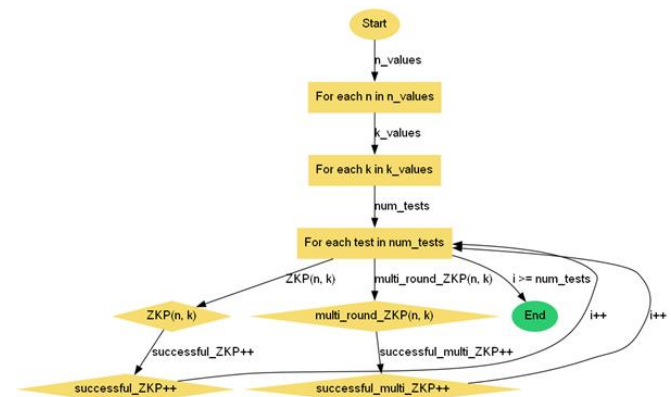


Figure 6. Comparison execution of ZKP and multi-round ZKP

In conclusion, both ZKP and multi-round ZKP effectively ensure the correctness of computation without revealing sensitive information. However, the choice between the two depends on the specific use case and the trade-off between security and computational efficiency.

The most significant benefit of using ZKP is privacy. In a world that is increasingly hostile towards a user's privacy, implementing ZKP is a step in the right direction. Though theoretically non-deterministic, the probability that a false prover can deceive the Verifier could be approximated to $1/n^m$, where m is the number of rounds performed. Even for the small input chosen here with ($n=169$) and 5 rounds, the probability would be 1 in 133 billion.

The ethos of blockchain is decentralisation and privacy. It was invented to break free from the shackles of a “Big Brother” - a centralised authoritarian figure. But there have been some impediments that compromise the user’s privacy. The widespread adoption of a robust, privacy-protection protocol like ZKP could vanquish all qualms. The applications are endless. ZKP could be used anywhere a data leak could happen.

The third party can access the user’s information even in traditional payment systems. Though their job was only to serve as a gateway, they harvested user data. This can be abolished if ZKP is implemented.

5. OPTIMISATION TECHNIQUES

To optimise the computational complexity of multi-round zero-knowledge proof (ZKP) protocols. Some of these techniques include:

Choosing efficient cryptographic primitives: The choice of cryptographic primitives, such as hash functions, elliptic curves, and symmetric key algorithms, can significantly impact the efficiency of ZKP protocols. By selecting efficient and secure primitives, it is possible to reduce the computational complexity of the protocol while maintaining an elevated level of security [17].

Batch verification: Batch verification is a technique where multiple proofs are verified simultaneously, reducing the computational complexity of the verification process. This technique is particularly useful in scenarios where multiple proofs must be verified simultaneously, such as in a blockchain-based system [18].

Precomputation: Precomputation involves pre-computing certain values used repeatedly in the protocol, such as the generator points or the hash functions. By pre-computing these values, it is possible to reduce the computational overhead of the protocol [19].

Adaptive ZKP protocols: Adaptive ZKP protocols are protocols where the Prover can adaptively choose the values used in the protocol based on the Verifier’s challenge. This allows the Prover to minimise the number of operations required, further reducing the computational complexity of the protocol [20].

Hardware acceleration: Hardware acceleration involves using specialised hardware, such as field-programmable gate arrays (FPGAs) or graphics processing units (GPUs), to accelerate the computations involved in the protocol. This can significantly reduce the computational complexity of the protocol while maintaining an elevated level of security [21].

Scaling ZKP systems: One of the main challenges with ZKP systems is their scalability. As the size of the problem increases, the time and computational resources required to generate a proof increase as well [22].

Developing new applications: ZKP systems have already found applications in various fields, such as blockchain, privacy-preserving data analysis, and authentication protocols. Future work can focus on developing new applications for ZKP systems in fields such as voting, healthcare, and finance [23].

Interoperability: Currently, multiple ZKP systems use different cryptographic primitives and are not interoperable with each other. Future work can focus on developing interoperable ZKP systems that can communicate with each other and be used in conjunction with other cryptographic protocols [24].

Standardisation: As ZKP systems become more widely adopted, there is a need for standardisation of protocols and primitives. Future work can focus on developing standards for ZKP systems to ensure interoperability and promote widespread adoption [25].

Optimising the computational complexity of ZKP protocols requires careful consideration of the specific cryptographic algorithm used and the specific application and hardware platform used. However, by selecting efficient primitives, using batch verification, pre-computing values, using adaptive protocols, and leveraging hardware acceleration, it is possible to improve the efficiency and scalability of ZKP protocols significantly.

6. APPLICATIONS OF MULTI-ROUND ZKP IN VARIOUS RESEARCH DOMAINS

Binu et al. [26] proposed a two-way secure ZKP authentication mechanism, Ravi Shanker Reddy and Beena [27] proposed a content-based health device registration on the blockchain, Jyothi and Supriya [28] showcased a blockchain-based KYC DApp, Babu and Supriya [29] proposed a rapid decision-making model at the edges to reduce and optimise cost. All the considered applications and similar application domains can be benefited by using the proposed multi-round ZKP method to strengthen security further.

7. CONCLUSIONS

In conclusion, the multi-round zero-knowledge proof (ZKP) algorithm designed to validate factorisation proofs for numbers emerges as a robust and efficient solution within diverse cryptographic contexts. This algorithm ensures heightened security against various attack vectors while maintaining a reasonable computational burden. The comparative analysis underscores the efficacy of the multi-round ZKP across distinct input sizes and parameters, underscoring its seamless integration into established cryptographic tools and protocols. Additionally, the transferability of the multi-round ZKP to diverse network models and architectures, beyond its current applications, presents an intriguing direction. Researchers can unlock new dimensions of its utility and robustness by adapting and fine-tuning the algorithm for various network topologies, such as peer-to-peer networks or distributed ledgers.

Moving forward, prospective research avenues could prioritise enhancing the efficiency and scalability of the multi-round ZKP algorithm. This might involve innovating novel approaches to streamline the verification process by minimising the requisite number of rounds or devising techniques to optimise the algorithm’s computational intricacies. Furthermore, the multi-round ZKP algorithm holds promise for novel applications in disparate cryptographic realms, such as blockchain, IoT, and cloud computing. Integrating Multi round ZKP into IoT communication protocols enhances data authenticity and safeguards against tampering, improving the overall security of IoT ecosystems. On the other hand, the algorithm contributes to the privacy and integrity of smart contracts. Its ability to validate complex computations without revealing sensitive data ensures the confidential execution of contract logic, addressing privacy concerns while maintaining trust and security within

blockchain transactions. Exploring these uncharted domains can unveil the full potential of this technique in fortifying the digital landscape.

REFERENCES

- [1] Morais, E., Koens, T., van Wijk, C., Koren, A. (2019). A survey on zero knowledge range proofs and applications. *SN Applied Sciences*, 1: 946. <https://doi.org/10.1007/s42452-019-0989-z>
- [2] Goldwasser, S., Micali, S., Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *Proceedings of the Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing - STOC '85*, New York, New York, USA. [c/10.1145/22145.22178](https://doi.org/10.1145/22145.22178)
- [3] Yang, Y., Guan, Z., Wan, Z., Weng, J., Pang, H.H., Deng, R.H. (2021). PriScore: Blockchain-based self-tallying election system supporting score voting. *IEEE Transactions on Information Forensics and Security*, 16: 4705-4720. <https://doi.org/10.1109/tifs.2021.3108494>
- [4] Benhamouda, F., Camenisch, J., Krenn, S., Lyubashevsky, V., Neven, G. (2014). Algebraic Attack against Variants of McEliece with Goppa Polynomial of a Special Form. In: Sarkar, P., Iwata, T. (eds) *Advances in Cryptology – ASIACRYPT 2014*. ASIACRYPT 2014. *Lecture Notes in Computer Science*, vol 8873. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-45611-8_2
- [5] Zhang, J., Fang, Z., Zhang, Y., Song, D. (2020). Zero knowledge proofs for decision tree predictions and accuracy. In *Proceedings of the Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*; ACM: New York, NY, USA. <https://doi.org/10.1145/3372297.3417278>
- [6] Polychronaki, M., Kogias, D.G., Patrikakis, C.Z. (2022). Identity Management in Internet of Things with Blockchain. In: De, D., Bhattacharyya, S., Rodrigues, J.J.P.C. (eds) *Blockchain based Internet of Things*. *Lecture Notes on Data Engineering and Communications Technologies*, vol 112. Springer, Singapore. https://doi.org/10.1007/978-981-16-9260-4_9
- [7] Hu, Q. (2022). Enhancing account privacy in blockchain-based IoT access control via zero knowledge proof. *IEEE Network*, pp. 1-7. <https://doi.org/10.1109/MNET.126.2200334>
- [8] Rasheed, A., Hashemi, R.R., Bagabas, A., Young, J., Badri, C., Patel, K. (2019). Configurable anonymous authentication schemes for the internet of things (IoT). In *Proceedings of the 2019 IEEE International Conference on RFID* (RFID). <https://doi.org/10.1109/RFID.2019.8719256>
- [9] Cui, P., Guin, U., Skjellum, A., Umphress, D. (2019). Blockchain in IoT: Current trends, challenges, and future roadmap. *Journal of Hardware and Systems Security*, 3: 338-364. <https://doi.org/10.1007/s41635-019-00079-5>
- [10] Sun, X., Yu, F.R., Zhang, P., Sun, Z., Xie, W., Peng, X. (2021). A survey on zero-knowledge proof in blockchain. *IEEE Network*, 35(4): 198-205. <https://doi.org/10.1109/mnet.011.2000473>
- [11] Gong, Y., Jin, Y., Li, Y., Liu, Z., Zhu, Z. (2022). Analysis and comparison of the main zero-knowledge proof scheme. In *Proceedings of the 2022 International Conference on Big Data, Information and Computer Network* (BDICN), Sanya, China. <https://doi.org/10.1109/BDICN55575.2022.00074>
- [12] Harikrishnan, M., Lakshmy, K.V. (2019). Secure digital service payments using zero knowledge proof in distributed network. In *Proceedings of the 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India. <https://doi.org/10.1109/ICACCS.2019.8728462>
- [13] Haralambiev, K. (2012). *Efficient cryptographic primitives for non-interactive zero-knowledge proofs and applications*. Proquest, Umi Dissertation Publishing.
- [14] Feng, T., Yang, P., Liu, C., Fang, J., Ma, R. (2022). Blockchain data privacy protection and sharing scheme based on zero-knowledge proof. *Wireless Communications and Mobile Computing*, 2022: 1040662. <https://doi.org/10.1155/2022/1040662>
- [15] Dwork, C., Naor, M., Sahai, A. (2004). Concurrent zero knowledge. *Journal of the ACM*, 51(6): 851-898, <https://doi.org/10.1145/1039488.1039489>
- [16] Pass, R. (2004). *Alternative variants of zero-knowledge proofs*. Licentiate Thesis, Stockholm, Sweden. <https://www.cs.cornell.edu/~rafael/papers/raf-lic.pdf>.
- [17] Haralambiev, K. (2012). *Efficient Cryptographic Primitives for Non-Interactive Zero-Knowledge Proofs and Applications*. Proquest, Umi Dissertation Publishing.
- [18] Xiong, H., Jin, C., Alazab, M., Yeh, K.H., Wang, H., Gadekallu, T.R., Wang, W., Su, C. (2022). On the design of blockchain-based ECDSA with fault-tolerant batch verification protocol for blockchain-enabled IoMT. *IEEE Journal of Biomedical and Health Informatics*, 26: 1977-1986. <https://doi.org/10.1109/jbhi.2021.3112693>
- [19] Figueiredo, L.S., Livshits, B., Molnar, D., Veanes, M. (2016). Prepose: Privacy, security, and reliability for gesture-based programming. In *Proceedings of the 2016 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA. <https://doi.org/10.1109/SP.2016.16>
- [20] Kalmykov, I.A., Olenev, A.A., Kalmykova, N.I., Dukhovnyj, D.V. (2022). Using adaptive zero-knowledge authentication protocol in VANET automotive network. *Information (Basel)*, 14(1): 27. <https://doi.org/10.3390/info14010027>
- [21] Zhang, Y., Wang, S., Zhang, X., Dong, J., Mao, X., Long, F., Wang, C., Zhou, D., Gao, M., Sun, G. (2021). PipeZK: Accelerating zero-knowledge proof with a pipelined architecture. In *Proceedings of the 2021 ACM/IEEE 48th Annual International Symposium on Computer Architecture (ISCA)*, Valencia, Spain. <https://doi.org/10.1109/ISCA52012.2021.00040>
- [22] Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M. (2017). Scalable zero knowledge via cycles of elliptic curves. *Algorithmica*, 79(4): 1102-1160. <http://doi.org/10.1007/s00453-016-0221-0>
- [23] Steffen, S., Bichsel, B., Baumgartner, R., Vechev, M. (2022). ZeeStar: Private smart contracts by homomorphic encryption and zero-knowledge proofs. *2022 IEEE Symposium on Security and Privacy (SP)*. <http://doi.org/10.1109/sp46214.2022.9833732>
- [24] Banerjee, A., Dutta, B., Mandal, T., Chakraborty, R., Mondal, R. (2022). *Blockchain in IoT and beyond: Case studies on interoperability and privacy*. Blockchain based Internet of Things, Singapore: Springer Singapore, 113-138. http://doi.org/10.1007/978-981-16-9260-4_5
- [25] Wu, H., Zheng, W., Chiesa, A., Popa, R.A., Stoica, I.

- (2018). DIZK: A distributed zero knowledge proof system. 27th USENIX Security Symposium (USENIX Security 18), pp. 675-692.
- [26] Binu, P.K., Induja, E., Earnest, M. (2018). Highly secured architectural model for web based applications using 2-way authentication technique. In Proceedings of the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Bangalore, India. <https://doi.org/10.1109/ICACCI.2018.8554377>
- [27] Ravi Shanker Reddy, T., Beena, B.M. (2023). AI Integrated Blockchain Technology for Secure Health Care—Consent-Based Secured Federated Transfer Learning for Predicting COVID-19 on Wearable Devices. In: Gupta, D., Khanna, A., Bhattacharyya, S., Hassanien, A.E., Anand, S., Jaiswal, A. (eds) International Conference on Innovative Computing and Communications. Lecture Notes in Networks and Systems, vol 473. Springer, Singapore. https://doi.org/10.1007/978-981-19-2821-5_30
- [28] Jyothi, C., Supriya, M. (2023). Decentralized Application (DApp) for Microfinance Using a Blockchain Network. In: Ranganathan, G., Bestak, R., Fernando, X. (eds) Pervasive Computing and Social Networking. Lecture Notes in Networks and Systems, vol 475. Springer, Singapore. https://doi.org/10.1007/978-981-19-2840-6_8
- [29] Babu, A.S., Supriya, M. (2022). Blockchain based fog computation model for military vehicular application. In Proceedings of the 2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT). https://doi.org/10.1007/978-981-19-2840-6_8