Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Government of India

IEEE COMPUTER SOCIETY Bangalore Chapter
IAS IEEE INDUSTRY APPLICATIONS SOCIETY Linking Research to Practice Bangalore Chapter

5th INTERNATIONAL CONFERENCE ON

PUBLIC KEY INFRASTRUCTURE AND ITS APPLICATIONS (PKIA 2024)

SEPTEMBER 5-6th, 2024

Efficiency of Zero-Knowledge Proofs: A Through Review and Analysis

Chitranjan Prasad Sah, Gurwinder Singh, Manjot Kaur
Department of Computer Science and Engineering,
Chandigarh University, Punjab, India

सी डैक CDAC

https://pkiindia.in Social Media /pkiindia

IEEE BANGALORE SECTION

CONTENTS

ABSTRACT

- Zero Knowledge Proofs (ZKPs) are cryptographic security techniques that allow secure data exchange without revealing secret information.
- This research study investigates and analyzes efficiency factors, robustness features, applicability, and uses, along with challenges for the implementation of these techniques.
- ZKPs Types: interactive, non-interactive, and succinct non-interactive arguments of knowledge (SNARKs).
- Libra stands out for its outstanding efficiency, requiring a one-time trusted setup depending on the input size among different prominent models of ZKPs.
- The study explores various challenges in ZKPs to enhance their robustness.
- To solve problems like the trusted setup dilemma and quantum computing attacks, the research suggests making progress by integrating different models, improving efficiency, looking into new mathematical problems etc.
- The results highlight the need to overcome constraints and improve ZKPs security and effectiveness in practical setups to enhance their efficiency.

INTRODUCTION

- ZKPs are a special kind of security technique in which two parties try to convince each other's claims while protecting the privacy of underlying data [1, 2].
- These parties (Prover and Verifier) communicate in a non-interactive manner, which guarantees an extremely safe way to verify claims without disclosing private information.
- Cryptography classifies Zero Knowledge Proofs as non-black box approaches due to their sophisticated and advanced nature
- ZKPs protocols can be used in voting, auctions, and blockchains, digital signatures, verifiable encryption, blind signatures, cryptocurrencies, proof-of-identity etc.
- Zero Knowledge Proofs stand as a beacon of security, offering a robust solution to the challenges posed by the ever-expanding data-sharing networks.
- Secure communication without unnecessary information disclosure, ZKPs pave the way for a future where privacy and integrity are paramount in the digital realm.
- This review study explores various challenges associated with ZKPs, aiming to enhance their robustness and suitability for the various applications

FUNDAMENTALS OF ZERO KNOWLEDGE PROOFS

- ZKPs help us secure digital communication by allowing a prover to authenticate a claim to a verifier without disclosing additional information that is presented in the question itself.
- These proofs are based on three main features known as completeness, soundness, and zero-knowledge:
- Completeness: If the statement is true, an honest prover can convince an honest verifier of its validity.
- Soundness: If the statement is false, no cheating prover can convince an honest verifier that it is true, except with a small probability.
- Zero-knowledge: The verifier learns nothing beyond the truth of the statement.
- This study investigates and discusses protocols such as the Schnorr ZKPs Protocol for the discrete logarithm problem [44], Fiat-Shamir Heuristic, Bulletproofs, ZKBoo, zk-SNARKs, and ZKIP.
- We can achieve a high level of security by using interactive ZKPs, but multiple communication rounds are required.
- NIZKPs address communication overhead and offer efficient proofs.
- SNARKs is a subclass of NIZKPs that takes efficiency to the next level, achieving impressive succinctness and scalability.

RESEARCH METHODOLOGY AND CONTRIBUTIONS

- Theoretical analysis has been used to conduct a literature review, gathering and comprehending existing zero-knowledge proof techniques, along with their associated security properties, protocols, and computational complexities across various problems and applications.
- We have used empirical and comparative studies for the performance analysis of ZKPs.
- Our research contribution are as following:
- We have proposed the use of ZKPs in conjunction with subset sum problem techniques to meet security requirements for various types of communications and transactions.
- we have analyzed the efficiency matrix of different IZKPs and NIZKPs in order to easily select efficient ZKPs techniques for use in our required application design.
- We have explored different kinds of applications of IZKPs and NIZKPs for use in different domains, identified significant challenges in ZKPs, and proposed potential future research directions in this field

EFFICIENCY METRICS AND ANALYSIS

- **The research focuses on conducting a detailed analysis of communication efficiency within cryptographic protocols, specifically examining the exchange of group (G) and $\mathbb{Z}_q$ items from a prover (P) to verifier (V) and vice-versa.**
- **The cost comparison given by Henry et al. [44] for discrete logarithm (DL) problem in G given as in Table1**
- **The research paper [33] includes Table 2, offering a comprehensive cost comparison between integer factorization and discrete logarithms.**

TABLE I. COST COMPARISONS OF OPERATIONS

Operation	Concrete cost	Asymptotic cost
$\text{ExpCost}_{\mathbb{G}}(\tau)$	$3\tau/2$	$\tau + \tau/\lg\tau$
$\text{ExpCost}_{\mathbb{G}}^{(m)}(\tau)$	$3m\tau/2$	$\tau + m\tau/\lg(m\tau)$
$\text{ExpCost}_{\mathbb{G}}((n,\tau))$	$\tau + n\tau/2$	$\tau + n\tau/\lg(n\tau)$
$\text{ExpCost}_{\mathbb{G}}^{(m)}((n,\tau))$	$m\tau + mn\tau/2$	$\tau \cdot \min\{m,n\} + mn\tau/\lg(mn\tau)$

TABLE II. EFFICIENCY COMPARISION OF INTEGER FACTORIZATION AND DISCRETE LOGARITHM PROBLEM

	Integer Factorization Problem		Discrete Logarithm Problem	
Operation	**Concrete Cost**	**Asymptotic Cost**	**Concrete Cost**	**Asymptotic Cost**
$\text{ExpCost}_{\mathbb{G}}(\tau)$	$(\lg\tau)^2$	$\tau^{1/4}$	$3\tau/2$	$\tau + \tau/\lg\tau$
$\text{ExpCost}_{\mathbb{G}}^{(m)}(\tau)$	$m(\lg\tau)^2$	$m\tau^{1/4}$	$3m\tau/2$	$\tau + m\tau/\lg(m\tau)$

EFFICIENCY METRICS AND ANALYSIS

TABLE III. YEARWISE EFFICIENCY MATRIX ANALYSIS OF ZKPS

Year	References	Types of ZKPs	Mathematical Problem/Features	Efficiency
1998	[36]	NIZKPs	Circuit Satisfiability	$O(kn\log(n/\varepsilon))$ *and* $O(n\lg(n/\varepsilon))$
2010	[11]	NIZKPs	Circuit Satisfiability	$\|C\| poly \log(k)$ bits
2014	[44]	IZKPs	Discrete Logarithm Problem	$O(\tau + \tau/\lg\tau)$
2016	[33]	IZKPs	Integer Factorization Problem	$O(\tau^{1/4})$
2018	[37]	ZKPs	Low Degree Polynomials	$O((\log N)/(\log\log N))$
2019	[38]	NIZKPs	general circuits by Giacomelli et al.	$O((\|F\|\lambda + \|x\|)\lambda)$
2019	[34]	IZKPs	Quadratic Residuosity Problem	$O((\lg\tau)^4)$
2021	[39]	ZKPs	Double Discrete Logarithm Problem	$O(1)$ time as well as space complexity
2021	[40]	NIZKPs	Lattice-based	k_2, $ploy_1$ and k_2, l_2
2022	[35]	IZKPs	General Number Field Sieve (Integer Factorization Problem)	$O(exp(1.923(\ln q)^{1/3}(\ln\ln q)^{2/3}))$

- From the discussion we find that ZKPs encompass diverse classes, including IZKPs, NIZKPs, and SNARKs.
- Using these cryptographic techniques, a prover and a verifier exchange a fact (an assertion) without disclosing any confidential information about the assertion.
- Each class offers unique advantages in terms of security, efficiency and usability.
- SNARKs are a specific class of NIZKPs that excels in proof size and verification time efficiency

APPLICATIONS OF ZERO KNOWLEDGE PROOFS

- ZKPs can be used for various kind of cryptographic protocols design and implementation without compromising security in comparison to traditional technique for the same.
- The Research paper "QuickSilver: Efficient and Affordable Zero-Knowledge Proofs for Circuits and Polynomials over Any Field" [46] has been implemented the zero-knowledge (ZK) proof protocols that make computations using circuits or polynomials much faster and cheaper.
- ZKPs can be used for identification scheme such as access control and authentication security system design and implementation in different applications.
- The research papers [42, 45] discuss different types of applications of Zero-Knowledge Proofs (ZKPs), such as Anonymous Verifiable Voting, Exchanging Digital Assets, Remote Biometric Authentication, Secure Auction, Confidential Transactions (Privacy-Preserving Transactions), ZKP for Graph Three Colorability, ZKP for Feige-Fiat-Shamir Identification Scheme, and so on

CHALLENGES AND FUTURE RESEARCH DIRECTIONS

- In the research paper [42], the authors have identified significant challenges in zero-knowledge proofs (ZKPs) and propose potential research avenues on the following topics:
- Reducing Assumptions: Obtaining better efficiency without involving a reliable third party is a major difficulty in the context of zkSNARK
- Integration of Diverse Mechanisms: Different kinds of ZKPs models offer distinct advantages, and exploring the integration of strengths from various models into a unified system holds promise.
- Efficiency Optimization
- Strongly Linear Version of Proof: Enabled verifiers can implement linear queries on inputs by investigating a new ZKPs type and a strongly linear version of the proof
- Other Mathematical Problems: If we want to enhance ZKPs efficiency, then it is essential to explore mathematical problems beyond bilinear group calculations
- Cryptographic Tools: Integrating cryptographic tools such as signature and commitment methods with non-interactive ZKPs models can enhance efficiency
- Lattice-Based Cryptography: Public-key cryptographic algorithms in blockchain-based ZKPs models are vulnerable to quantum computing attacks

CONCLUSION

- This review study comprehensively investigates and analyzes efficiency factors, robustness features, applicability, and uses, along with challenges for the implementation of the ZKPs technique used in cryptography.
- The paper categorizes ZKPs as interactive, non-interactive, and SNARKs, each with distinct trade-offs.
- Efficiency metrics analyze models like zkSNARK, Ligero, Bulletproofs, Hyrax, Aurora, and Libra, highlighting Libra's standout efficiency with a one-time trusted setup.
- The review study investigates several ZKPs challenges that need to be addressed in order to make it more robust, including the trusted setup problem and quantum computing risks.
- Future research aims to enhance ZKP efficiency and security by integrating models, optimizing, exploring new problems, incorporating cryptographic tools, and exploring lattice-based cryptography.

THANK YOU

REFERENCES

- [1] J. Kilian, S. Micali, and R. Ostrovsky, “Minimum resource zero-knowledge proofs,” In Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science, IEEE, New York, PP. 474-479, 1989.
- [2] O. Goldreich and Y. Oren, “Definitions and properties of zero-knowledge proof systems,” Tech. Rep. TR-610, Haifa, Israel, 1990.
- [3] A. J. Menezes, S. A. Vanstone, and P. C. Van Oorschot, Handbook of Applied Cryptography. Boca Raton, CRC Press, Inc., FL, USA, 1996.
- [4] J. Groth, R. Ostrovsky, and A. Sahai, “Perfect non-interactive zero knowledge for NP,” UCLA, Department of Computer Science, Los Angeles, USA, August 2005.
- [5] J. Groth and A. Sahai, “Efficient non-interactive proof systems for bilinear groups,” SIAM Journal on Computing 41(5), pp. 1193-1232, 2012.
- [6] J. Katz, V. Koilesnikov and X. Wang, “Improved Non-Interactive Zero Knowledge with Applications to Post-Quantum Signatures,” University of Maryland and Georgia Tech, March 2019.
- [7] D. C. Sánchez, “Zero-Knowledge Proof-of-Identity,” Cryptography and Security, February 12, 2020.
- [8] E. Morais, T. Koens, C. Wijk, and A. Koren, “A survey on zero knowledge range proofs and applications,” Springer Nature journal Switzerland AG, SN Applied Sciences, July 2019.
- [9] S. Goldwasser, S.Micali, and C. Rackoff, “The knowledge complexity of interactive proof systems,” SIAM Journal on Computing, vol. 18, no. 1, pp. 186–208, 1989.
- [10] M. Blum, P. Feldman, and S. Micali, “Non-interactive zero knowledge and its applications,” in Proceedings of the 20th Annual ACM symposium on Theory of computing (STOC ’88), pp. 103–112, ACM, 1988.
- [11] J. Groth, "Short Non-interactive Zero-Knowledge Proofs," Advances in Cryptology - ASIACRYPT 2010, M. Abe, Ed., Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 341-358, 2010.
- [12] I. Damgård, "Commitment Schemes and Zero-Knowledge Protocols," in Lectures on Data Security, I. B. Damgård, Ed., EEF School 1998, Lecture Notes in Computer Science, vol. 1561, Springer, Berlin, Heidelberg, 1999.
- [13] I. Damgard, "On the existence of bit commitment schemes and zero-knowledge proofs," in Advances in Cryptology - CRYPTO '89, pp. 17-29, 1989.
- [14] K. Balasubramanian and K. Mala, “Zero Knowledge Proofs,” Advances in information security, privacy, and ethics book series, Jan. 2018.
- [15] U. Feige, A. Fiat, and A. Shamir, “Zero-knowledge proofs of identity,” Journal of Cryptology, vol. 1, no. 2, pp. 77–94, Jun. 1988.
- [16] H. Wu and F. Wang, "A Survey of Noninteractive Zero Knowledge Proof … m and its Applications," … Sc … W … ournal, vol. 2014, article ID 560484, May 4, 2014.

REFERENCES

- [17] M. Blum, A. de Santis, S.Micali, and G. Persiano, “Noninteractive zero-knowledge,” SIAM Journal on Computing, vol. 20, no. 6, pp. 1084–1118, 1991.
- [18] M. Chen, A. Chiesa, N. Spooner, "On Succinct Non-Interactive Arguments in Relativized Worlds," in Advances in Cryptology – EUROCRYPT 2022, Springer International Publishing, pp. 336-366, 2022.
- [19] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, “From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again,” Proceedings of the 3rd Innovations in Theoretical Computer Science Conference on - ITCS ’12, 2012.
- [20] M. Blum, P. Feldman, and S. Micali, “Non-Interactive Zero-Knowledge and Its Applications (Extended Abstract),” Symposium on the Theory of Computing, pp. 103–112, Jan. 1988.
- [21] A. D. Dwivedi, R. Singh, U. Ghosh, R. R. Mukkamala, A. Tolba, and O. Said, “Privacy preserving authentication system based on non-interactive zero knowledge proof suitable for Internet of Things,” Journal of Ambient Intelligence and Humanized Computing, Sep. 2021.
- [22] N. Bitansky, A. Chiesa, Y. Ishai, R. Ostrovsky, and O. Paneth, “Succinct Non-Interactive Arguments via Linear Interactive Proofs,” Journal of Cryptology, vol. 35, no. 3, May 2022.
- [23] J. N. Bos and M. J. Coster, "Addition chain heuristics," Proceedings of CRYPTO 1989, vol. 435, LNCS, pp. 400–407, Santa Barbara, CA, USA, August1989.
- [24] P. Erd¨os, “Remarks on number theory III: On addition chains,” Acta Arithmetica, pp. 77–81, 1960–1961.
- [25] A. Brauer, "On addition chains," Bulletin of the American Mathematical Society, vol. 45, no. 10, pp. 736-739, October 1939.
- [26] D. J. Bernstein, "Pippenger's exponentiation algorithm," to be incorporated into the author's High-speed cryptography book, January 2002.
- [27] C. H. Lim, "Efficient multi-exponentiation and application to batch verification of digital signatures," Technical Report, Sejong University, Seoul, South Korea, August 2000.
- [28] E. F. Brickell, D. M. Gordon, K. S. McCurley, and D. B. Wilson, "Fast exponentiation with precomputation (extended abstract)," in Proceedings of EUROCRYPT1992, vol. 658, LNCS, pp. 200–207, Balatonf¨ured, Hungary, May 1992.
- [29] C. H. Lim and P. J. Lee, "More flexible exponentiation with precomputation," in *Proceedings of CRYPTO1994*, vol. 839, LNCS, pp. 95–107, Santa Barbara, CA, USA, August 1994.
- [30] D. M’Ra¨ıhi and D. Naccache, "Batch exponentiation: A fast DLP-based signature generation strategy," in Proceedings of CCS1996, pp. 58–61, New Delhi, India, March 1996.
- [31] A. C.-C. Yao, "On the evaluation of powers," SIAM Journal on Computing (SICOMP), [illegible], no. 1, pp. 100–103, M[illegible] 19[illegible]

REFERENCES

- [32] N. Pippenger, "On the evaluation of powers and related problems (preliminary version)," in Proceedings of FOCS1976, pp. 258–263, Houston, TX, USA, October 1976.
- [33] C. P. Sah, K. Jha, and S. Nepal, “Zero-knowledge proofs technique using integer factorization for analyzing robustness in cryptography” In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 638-642, 2016.
- [34] C. P. Sah and P. R. Gupta "Comparative Analysis of Zero-Knowledge Proofs Technique using Quadratic Residuosity Problem," in 2019 6th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 632-636, March 2019.
- [35] C. P. Sah, “Robustness of zero-knowledge proofs using RSA problem,” in 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 40-44, March 2022.
- [36] J. Kilian and E. Petrank, "An Efficient Noninteractive Zero-Knowledge Proof System for NP with General Assumptions," Journal of Cryptology, vol. 11, no. 1, pp. 1-27, Jan. 1998.
- [37] J. Bootle and J. Groth, "Efficient Batch Zero-Knowledge Arguments for Low Degree Polynomials," in Proc. Public-Key Cryptography – PKC 2018, M. Abdalla and R. Dahab (eds), 2018.
- [38] M. Backes, L. Hanzlik, A. Herzberg, A. Kate, and I. Pryvalov, "Efficient Non-Interactive Zero-Knowledge Proofs in Cross-Domains Without Trusted Setup," in Proceedings/Book Title, pp. 286-313, Apr. 6, 2019.
- [39] B. Lian, G. Chen, and J. Li, "Efficient Zero-Knowledge Proofs of Knowledge of Double Discrete Logarithm," International Journal of Security and its Applications, vol. 9, pp. 191-208, Mar. 2015.
- [40] S. Xie, W. Yao, F. Wu, and Z. Zheng, "Noninteractive zero-knowledge proof scheme from RLWE-based key exchange," PLoS ONE, vol. 16, no. 8, p. e0256372, 2021.
- [41] K. Yang and X. Wang, "Non-interactive Zero-Knowledge Proofs to Multiple Verifiers," in S. Agrawal and D. Lin (Eds.), Advances in Cryptology – ASIACRYPT 2022 - 28th International Conference on the Theory and Application of Cryptology and Information Security, pp. 517-546, 2022.
- [42] X. Sun, F. R. Yu, P. Zhang, Z. Sun, W. Xie and X. Peng, "A Survey on Zero-Knowledge Proof in Blockchain," in IEEE Network, vol. 35, no. 4, pp. 198-205, July/August 2021.
- [43] M. Midha, A. K. Gupta, and P. Mathur, "Review on Zero-Knowledge Proof Method." In Proceedings of the Second International Conference on Information Management and Machine Intelligence: ICIMMI 2020, pp. 299-306, 2021.
- [44] R. Henry, “Efficient zero-knowledge proofs and applications,” Ph. D. thesis, University of Waterloo, Ontario, Canada, 2014.
- [45] L. Feng, and B. McMillin, “A survey on zero-knowledge proofs,” In Advances in Computers 2014 Jan 1, Vol. 94, pp. 25-69, Elsevier, 2014.
- [46] K. Yang, P. Sarkar, C. Weng, and X. Wang, "QuickSilver: Efficient and Affordable Zero [illegible]ledge Proofs for Circu[illegible]d P[illegible]ia[illegible]r Any Field," in Proceedings of the ACM Conference on Computer and Communications Secu[illegible]