MECOMARE, 12 (2) (2023) pp. 53-58

Published by: TRIGIN Publisher

International Journal of Mechanical Computational and Manufacturing Research

Journal homepage: www.trigin.pelnus.ac.id

zk-SNARKs as a cryptographic solution for data privacy and security in the digital era

Imam Santoso[1], Yuli Christyono[2]

[1,2] Department Electrical Engineering, Diponegoro University, Semarang, Indonesia

ARTICLE INFO

Article history:

Received Aug 25, 2023
Revised Aug 28, 2023
Accepted Aug 31, 2023

Keywords:

Cryptography;
Data Privacy;
Digital Security;
zk-SNARKs.

ABSTRACT

This research brings the concept of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) in the context of data security and privacy in the digital world. zk-SNARKs is a cryptographic technology that allows individuals to prove a statement or knowledge without having to reveal the actual details of the information. We illustrate this concept through a simple example of proving age over 18 without revealing the actual date of birth. This research highlights the importance of maintaining data privacy in various technological applications, including the use of zk-SNARKs in blockchain to maintain transaction privacy and personal data protection in increasingly sophisticated applications. However, the implementation of zk-SNARKs requires deep mathematical understanding and strong data security concerns. With great potential to support data privacy and security in the evolving digital era, zk-SNARKs is a highly relevant tool in addressing privacy-related challenges in the digital world. The conclusion of this research is that zk-SNARKs is an important tool in maintaining data privacy and security in the digital age. With its ability to allow individuals to prove knowledge or assertions without revealing actual details of information, this technology has wide applications in various sectors, including finance, data management, and data privacy protection. However, it should be emphasized that the implementation of zk-SNARKs requires extra care in securing the system and ensuring that the technology is used properly to maintain high data privacy and security. With further development and understanding in this technology, zk-SNARKs can be an integral component in building a safer and more private digital world.

Corresponding Author:

Imam Santoso,
Department of Electrical Engineering,
Diponegoro University,
Jl. Prof. Sudarto No.13, Tembalang, Semarang, Jawa Tengah,50275, Indonesia.
Email: imamstso@elektro.undip.ac.id

1. INTRODUCTION

In the advancing digital age, challenges related to data privacy and security have become a major concern (Bonfield et al., 2020; Gui et al., 2020; Hoy & Chambers, 2020; Woods et al., 2020). Loss of personal data privacy has become one of the critical issues facing users and organizations around the world (Atlam & Wills, 2020; Dhagarra et al., 2020). In an effort to safeguard personal data and respond to the growing demands for privacy, cryptographic technologies are constantly evolving (Aldawood & Skinner, 2019; Barth et al., 2019; Muhammad Wali et al., 2023). One of the latest innovations that plays a vital role in maintaining data privacy is zk-SNARKs (Zero-Knowledge

Succinct Non-Interactive Argument of Knowledge). This technology presents a robust solution to harmonize data security with privacy which is highly required in various technological applications (Banerjee et al., 2020; Ozdemir & Boneh, 2022; Qi et al., 2023).

This research aims to introduce zk-SNARKs as a vital tool in maintaining data privacy and security in the digital era. We will explain the concept of zk-SNARKs, illustrate its use through a simple example, and outline its important implications in various sectors, including blockchain, finance, and data management. In addition, we will highlight the challenges and considerations associated with implementing zk-SNARKs, including deep mathematical understanding and attention to data security (ElSheikh & Youssef, 2022; Kosba et al., 2020; Pinto, 2020; Satybaldy & Nowostawski, 2020).

The ever-evolving digital age has brought great benefits in various aspects of our lives (Anani et al., 2021; Herden et al., 2021). However, with technological advancements come great challenges, especially regarding data privacy. The personal data we share online can often be used to monitor, identify or even exploit us. This is why maintaining data privacy has become a major focus for individuals, organizations, and regulators. One solution that has long been used to protect data is cryptography. Cryptography involves using mathematical techniques to encrypt data so that only authorized parties can read or access it (Namasudra, 2022). However, cryptography alone is not always enough to maintain data privacy. In many cases, we need to verify information or facts without revealing the actual data. This is where zk-SNARKs enters the game.

zk-SNARKs stands for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge. zk-SNARKs are cryptographic tools that allow two parties to verify the truth of a statement or knowledge without having to reveal the actual data to each other. In other words, zk-SNARKs allows someone to prove that they have knowledge of something without revealing what they know. This makes zk-SNARKs a very powerful tool in maintaining the privacy of personal data (Nitulescu, 2020; Ozdemir & Boneh, 2022; Pinto, 2020).

To better understand the concept of zk-SNARKs, we create an example of someone wanting to prove to another party that they are over 18 years old without revealing their actual date of birth. Using zk-SNARKs, they can do this by proving that they have knowledge of their age without having to reveal detailed information that could be used to identify them (Li et al., 2020; Panait & Olimid, 2021; Park et al., 2020).

One of the most prominent applications of zk-SNARKs is in blockchain technology. In blockchain, zk-SNARKs are used to maintain the privacy of transactions. A user can prove that they have enough balance to make a transaction without having to reveal the actual amount or details of the transaction. This helps in achieving the main goal of blockchain, which is transparency and security while maintaining user privacy (Guan et al., 2020; Hu et al., 2023; Pinto, 2020).

While zk-SNARKs offers many advantages in maintaining privacy and data security, its implementation is not an easy task. The use of this technology requires a deep mathematical understanding and strict attention to data security. Errors in the implementation of zk-SNARKs can result in vulnerabilities that can be exploited by malicious parties.

In a world that is increasingly dependent on digital technology, zk-SNARKs is a highly relevant tool in maintaining data privacy and security. With further understanding and development in this technology, zk-SNARKs can become one of the integral components in building a safer and more privacy-assured digital world. This research aims to explain the concept of zk-SNARKs, illustrate its use, and highlight the importance of attention to data security and privacy in the future use of this technology.

2. RESEARCH METHOD

The application of zk-SNARKs in simple use cases, such as confirming age without revealing the actual date of birth. Scenario, An individual wants to prove to the owner of a website that he is above 18 years of age without having to reveal his actual date of birth. Steps to implement zk-SNARKs:

1. Key Generation
   The individual first generates a pair of cryptographic keys, namely a public key and a private key. The public key will be used by the website owner to verify the proof, while the private key will be used by the individual to generate the proof.

2. Prove Age
   The individual wants to prove that he is above 18 years of age. He uses his private key to generate a mathematical proof (zk-SNARKs) stating that "I am above 18 years of age" without revealing his date of birth.
3. Verification
   The website owner receives the proof along with the individual's public key. He uses that public key to verify the proof. The verification process involves only mathematical calculations and does not require the disclosure of the actual date of birth.
4. Result
   If the verification result is positive, the website owner can be sure that the individual is above 18 years of age, but he does not know the actual date of birth. The individual still maintains his privacy.

In this example, zk-SNARKs is used to prove a statement (age over 18) without revealing the actual information (date of birth). This is one example of how zk-SNARKs can be used to maintain data privacy, while still allowing verification or confirmation of the truth of a statement.

The mathematical formulation for the application of zk-SNARKs in the mentioned use case (proving age above 18 years) can be represented as follows: G is a cyclic group with multiplication operation and large order n, g is the generator element of group G, pk is the public key provided by the website owner, sk is the individual's private key, A is the hash function that generates values in group G, m is the message containing the statement to be proved (e.g., "I am over 18 years old").

Then, the mathematical formulation for zk-SNARKs can be modeled as follows:
Proof Generation Process (Prover):

1. The individual selects a random value r from group G.
2. He calculates C=A(m).gr, which is the commitment to statement m and random value r.
3. The individual computes z=r-sk·C, which is a proof that he has knowledge of sk without expressing sk directly.

Verification Process (Verifier):

1. The website owner receives C and z along with pk.
2. He calculates C' =A(m)·gz
3. If C′=C, then the verification is successful, and the website owner can be sure that the individual is over 18 years old without knowing sk.

In this formulation, zk-SNARKs allows an individual to prove that he or she has knowledge of sk without revealing sk to other parties. The value of r is used as a random value that creates a commitment C that can only be generated by someone who has sk. The verification process involves only simple mathematical calculations and does not require actual disclosure of information.

Numerical example corresponding to the mentioned mathematical formulation of zk-SNARKs (proving age above 18 years) using integers as representation in group G.

Initial Setup:

1. n=23 (Order of the integer group)
2. g=5 (Integer group generator)
3. k=7 (Individual private key)
4. pk=115 (Website owner's public key)
5. m=18 (Statement to be proved: "I am over 18 years old")

Proof Generation Process (Prover):

1. The individual chooses a random value r=9 from group G.
2. He calculates C=(m+sk·r) mod n=(18+7·9) mod 23=18, which is the commitment to statement m and random value r.
3. The individual computes z=(r-sk·C)mod n=(9-7·18)mod 23=16, which is a proof that he has knowledge of sk without expressing sk directly.

Verification Process (Verifier):

1. The website owner accepts C=18 and z=16 along with pk=115.
2. He calculates $C' = (m + pk \cdot z) \bmod n = (18 + 115 \cdot 16) \bmod 23 = 18$.
3. Since $C' = C$, the verification is successful, and the website owner can be sure that the individual is over 18 years old without knowing sk.

3. RESULTS AND DISCUSSIONS

In the described example, the individual managed to prove to the website owner that he/she was over 18 years old without having to disclose the date of birth or any other personal information. The proof generation process of zk-SNARKs results in C=18 and z=16, while the verification process performed by the website owner results in $C'=18$. Since $C'=C$, the verification is successful, and the website owner can be sure that the individual meets the required age requirement (over 18 years old) without knowing their confidential information (sk value).

Discussion

Privacy Preserved

In this example, the privacy of the individual is preserved as they only need to reveal the values of C and z to the website owner, which contain no personal information that can be used to identify them or reveal their actual date of birth. This is one of the main advantages of zk-SNARKs in maintaining data privacy.

Verified Verification

The verification process conducted by the website owner successfully checks zk-SNARKs' proofs correctly. If the age above 18 declaration is not met, the verification will not be successful, so the website owner will only grant access to eligible individuals.

Conformance to Mathematical Formulation

The example conforms to the mathematical formulation of zk-SNARKs mentioned earlier. The mathematical computation process described in this example follows the exact steps used in zk-SNARKs to prove knowledge of sk without revealing the actual sk.

More Complex Applications

In actual use, zk-SNARKs can be used in a variety of more complex use cases, such as in blockchains to protect the privacy of transactions, secure personal data, and more. It is one of the essential tools in maintaining data privacy in the digital world.

4. CONCLUSION

This research highlights the importance of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) technology in maintaining data privacy and security in the digital world. With zk-SNARKs, individuals can prove an assertion or knowledge without having to reveal actual details, as illustrated in the simple use case of confirming age over 18. Data privacy is at the core of the use of this technology, and it is relevant in a variety of contexts, including in blockchain to maintain transaction privacy and personal data protection in increasingly sophisticated applications. However, it is important to remember that the use of zk-SNARKs requires deep mathematical understanding and careful implementation to ensure adequate security. Furthermore, this technology has great potential in supporting data privacy and security in the future, especially in the face of challenges related to privacy and confidentiality in an ever-evolving digital world. For future research, it is recommended to focus on three main aspects. First, the development of more efficient and user-friendly methods to implement zk-SNARKs, so that this technology can be adopted more widely without requiring a very deep understanding of mathematics. Second, further exploration in the application of zk-SNARKs in various industries, including in the context of the Internet of Things (IoT), digital health, and cybersecurity. Finally, research should keep abreast of legal and regulatory developments related to data privacy to ensure that the use of zk-SNARKs is aligned with the

applicable legal framework and relevant ethical guidelines, thus maintaining the balance between technological innovation and privacy protection required in this increasingly complex digital age.

REFERENCES

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Anani, G. E., Lamptey, H. K., & Frempong, C. O. (2021). Redefining Literacy in a Digital Age: The Role of Instructors in Promoting Digital Literacy. *Journal of English Language Teaching and Applied Linguistics*, *3*(8), 20–25.

Atlam, H. F., & Wills, G. B. (2020). IoT security, privacy, safety and ethics. *Digital Twin Technologies and Smart Cities*, 123–149.

Banerjee, A., Clear, M., & Tewari, H. (2020). Demystifying the Role of zk-SNARKs in Zcash. *2020 IEEE Conference on Application, Information and Network Security (AINS)*, 12–19.

Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55–69.

Bonfield, C. A., Salter, M., Longmuir, A., Benson, M., & Adachi, C. (2020). Transformation or evolution?: Education 4.0, teaching and learning in the digital age. *Higher Education Pedagogies*, *5*(1), 223–246.

Dhagarra, D., Goswami, M., & Kumar, G. (2020). Impact of trust and privacy concerns on technology acceptance in healthcare: an Indian perspective. *International Journal of Medical Informatics*, *141*, 104164.

ElSheikh, M., & Youssef, A. M. (2022). Dispute-free scalable open vote network using zk-SNARKs. *ArXiv Preprint ArXiv:2203.03363*.

Guan, Z., Wan, Z., Yang, Y., Zhou, Y., & Huang, B. (2020). BlockMaze: An efficient privacy-preserving account-model blockchain based on zk-SNARKs. *IEEE Transactions on Dependable and Secure Computing*, *19*(3), 1446–1463.

Gui, G., Liu, M., Tang, F., Kato, N., & Adachi, F. (2020). 6G: Opening new horizons for integration of comfort, security, and intelligence. *IEEE Wireless Communications*, *27*(5), 126–132.

Herden, C. J., Alliu, E., Cakici, A., Cormier, T., Deguelle, C., Gambhir, S., Griffiths, C., Gupta, S., Kamani, S. R., & Kiratli, Y.-S. (2021). "Corporate Digital Responsibility" New corporate responsibilities in the digital age. *Sustainability Management Forum| NachhaltigkeitsManagementForum*, *29*(1), 13–29.

Hoy, R. F., & Chambers, D. C. (2020). Silica-related diseases in the modern world. *Allergy*, *75*(11), 2805–2817.

Hu, X., Zhou, W., Yin, J., Cheng, G., Yan, S., & Wu, H. (2023). Towards verifiable and privacy-preserving account model on a consortium blockchain based on zk-SNARKs. *Peer-to-Peer Networking and Applications*, 1–18.

Kosba, A., Papadopoulos, D., Papamanthou, C., & Song, D. (2020). {MIRAGE}: Succinct Arguments for Randomized Algorithms with Applications to Universal {zk-SNARKs}. *29th USENIX Security Symposium (USENIX Security 20)*, 2129–2146.

Li, X., Zheng, Y., Xia, K., Sun, T., & Beyler, J. (2020). Phantom: An efficient privacy protocol using zk-SNARKs based on smart contracts. *Cryptology EPrint Archive*.

Muhammad Wali, S. T., Efitra, S., Kom, M., Sudipa, I. G. I., Kom, S., Heryani, A., Sos, S., Hendriyani, C., Rakhmadi Rahman, S. T., & Kom, M. (2023). *Penerapan & Implementasi Big Data di Berbagai Sektor (Pembangunan Berkelanjutan Era Industri 4.0 dan Society 5.0)*. PT. Sonpedia Publishing Indonesia.

Namasudra, S. (2022). A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure. *Computers and Electrical Engineering*, *104*, 108426.

Nitulescu, A. (2020). *zk-SNARKs: a gentle introduction*. Technical report.

Ozdemir, A., & Boneh, D. (2022). Experimenting with Collaborative {zk-SNARKs}:{Zero-Knowledge} Proofs for Distributed Secrets. *31st USENIX Security Symposium (USENIX Security 22)*, 4291–4308.

Panait, A.-E., & Olimid, R. F. (2021). On using zk-SNARKs and zk-STARKs in blockchain-based identity management. *Innovative Security Solutions for Information Technology and Communications: 13th International Conference, SecITC 2020, Bucharest, Romania, November 19–20, 2020, Revised Selected Papers 13*, 130–145.

Park, J., Kim, H., Kim, G., & Ryou, J. (2020). Smart contract data feed framework for privacy-preserving oracle system on blockchain. *Computers*, *10*(1), 7.

Pinto, A. M. (2020). An introduction to the use of zk-SNARKs in blockchains. *Mathematical Research for Blockchain Economy: 1st International Conference MARBLE 2019, Santorini, Greece*, 233–249.

Qi, H., Cheng, Y., Xu, M., Yu, D., Wang, H., & Lyu, W. (2023). Split: A Hash-based Memory Optimization Method for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK). *IEEE Transactions on Computers*.

Satybaldy, A., & Nowostawski, M. (2020). Review of techniques for privacy-preserving blockchain systems.

Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, 1–9.

Woods, S. A., Ahmed, S., Nikolaou, I., Costa, A. C., & Anderson, N. R. (2020). Personnel selection in the digital age: A review of validity and applicant reactions, and future research challenges. *European Journal of Work and Organizational Psychology*, *29*(1), 64–77.