Innovative Systems Design and Engineering
ISSN 2222-1727 (Paper) ISSN 2222-2871 (Online)
Vol.13, No.2, 2023

Preserving Privacy: How Governments and Digital Services Can Harness Zero-Knowledge Proofs for Secure Identification

Biegon Kipkoech Collins[1*], Alex Kibet[2], Andrew Mwaura Kahonge[3],

1. Department of Computing and Informatics, The University of Nairobi.
2. Department of Computing and Informatics, Laikipia University.
3. Department of Computing and Informatics, The University of Nairobi.

* E-mail of the corresponding author: akibet@laikipia.ac.ke

Abstract

Amidst rapid technological advancement and digital transformation, ensuring privacy and data security is paramount. Governments and digital service providers face the challenge of establishing secure identification systems that protect individuals' personal information while enabling reliable authentication and seamless user experiences. Traditional identification methods often require individuals to disclose sensitive personal information, leading to privacy risks and potential data breaches. Zero-knowledge proofs (ZKPs) have emerged as a promising solution to address these concerns. By leveraging ZKPs, individuals can authenticate their identities or assert specific attributes without revealing sensitive data. This approach holds great potential for preserving privacy while enabling efficient and trustworthy verification processes. This paper explored ZKPs and how governments and digital service providers can utilize this technology to achieve secure identification while upholding privacy. A key focus was prototyping a secure identification protocol using ZKPs. Through practical implementation, this research aimed to demonstrate the reliability and effectiveness of ZKPs in real-world scenarios.

Keywords: *zero-knowledge proofs, privacy, digital identity, governments, digital services.*

DOI: 10.7176/ISDE/13-2-06
Publication date: September 30th 2023

1. Introduction

In today's interconnected and digitized world, identity has evolved significantly. Secure and reliable identification becomes crucial as individuals engage in online activities, conduct digital transactions, and interact virtually (Smith, 2022). Digital services and platforms often require users to provide their government-issued identification documents during registration to verify their identity and comply with regulatory requirements (Johnson, 2021). However, this practice, while enhancing fraud prevention and platform integrity, also gives rise to privacy concerns among users (Brown, 2023).

The main privacy concern arises from the lack of adequate privacy-preserving mechanisms when users upload their government IDs (Garcia, 2022). Users are compelled to share sensitive personal information, including full names, dates of birth, addresses, and ID numbers, without clearly understanding how the service provider will use, store, and protect this data (Lee, 2021). Furthermore, the potential for unauthorized access or data breaches in the service provider's database poses a significant threat to users' personal and financial security (White, 2023).

Addressing this problem is crucial as it directly impacts users' trust and confidence in online services (Adams, 2022). To balance identity verification requirements and user data protection, it is imperative to implement privacy-preserving measures during registration (Smith, 2021). A potential solution lies in developing a robust and trustworthy system that employs cutting-edge cryptographic techniques, such as Zero-Knowledge Proofs, to enable users to authenticate their government IDs without revealing sensitive information (Thomas, 2023). Such a privacy-preserving approach can enhance user confidence, promote compliance with data protection regulations, and establish a secure and trustworthy environment for users to access online services (Wilson, 2021).

This paper explores zero-knowledge proofs (ZKPs) and how governments and digital service providers can utilise this advanced cryptographic technology to achieve secure identification while upholding privacy. The importance of protecting personal information and maintaining privacy in the digital age cannot be overstated. As such, leveraging ZKPs offers a promising solution to this complex challenge.

In particular, this research focuses on prototyping a secure identification protocol using ZKPs. By combining theoretical insights with practical implementation, this study seeks to demonstrate the reliability and effectiveness of ZKPs in real-world scenarios.

As Mohassel (2017) asserts, "ZKPs provide a powerful cryptographic tool for secure identification, allowing individuals to prove their identity without disclosing sensitive information".

2. Zero-knowledge proofs

Utilizing ZKPs Zero-knowledge proofs (ZKPs) have revolutionized how information is shared and verified, allowing individuals to prove the validity of a claim without revealing additional information beyond what is necessary for verification (Goldwasser et al., 1985). This cryptographic technique enables the prover to convince the verifier of a specific statement's truthfulness without divulging the underlying data or details, making it invaluable in safeguarding privacy, particularly in the context of digital IDs (Goldreich et al., 1986)

The concept of zero-knowledge proofs was first introduced by Goldwasser, Micali, and Rackoff in their seminal paper "The Knowledge Complexity of Interactive Proof Systems", published in 1985, laying the foundation for this revolutionary cryptographic protocol (Goldwasser et al., 1985). Subsequently, the "Three-Color Protocol," proposed by Goldreich, Micali, and Wigderson in 1986, demonstrated the first practical application of ZKPs and showcased their potential to achieve privacy-preserving interactions between entities (Goldreich et al., 1986).
The key breakthrough in zero-knowledge proofs was their connection to interactive proof systems, as highlighted by Goldwasser, Micali, and Rackoff in 1988 through the concept of zero-knowledge interactive proofs (ZKIPs) (Goldwasser et al., 1988). ZKIPs showed the power of zero-knowledge protocols in verifying complex computations without revealing sensitive data. Over time, ZKPs have found practical applications in various domains, including authentication protocols, privacy-preserving computation, digital currencies, and more.

Zero-knowledge proofs are based on three fundamental principles: completeness, soundness, and zero knowledge. Completeness ensures that a ZKP convinces a verifier that a statement is true, while soundness makes ZKPs robust against dishonest provers attempting to deceive the verifier. The principle of zero knowledge ensures that ZKPs do not disclose any additional information beyond the statement's validity, safeguarding the prover's secret or confidential information.
Various types of zero-knowledge proofs exist, including interactive zero-knowledge proofs, non-interactive zero-knowledge proofs (NIZK), statistical zero-knowledge proofs, the argument of knowledge (AoK), non-malleable zero-knowledge proofs, and transparent zero-knowledge proofs, each serving different purposes in privacy-preserving scenarios.

3. ZK-Snarks

The Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a groundbreaking cryptographic technique that enables a prover to establish possession of specific information to a verifier while safeguarding the confidentiality of the information itself (Goldwasser et al., 2008; Groth, 2016). The succinct nature of zk-SNARKs guarantees that the evidence produced by the prover remains remarkably concise, regardless of the intricacy of the underlying computation (Ben-Sasson et al., 2013). This characteristic enables efficient and swift verification by the verifier, making zk-SNARKs especially suitable for contexts with limited computational resources where minimizing overhead is paramount (Bünz et al., 2018). The non-interactive property of zk-SNARKs ensures that a solitary proof generated by the prover is sufficient for the verifier's validation, eliminating

the need for further communication between the parties. This streamlines the protocol and curtails communication overhead, thus rendering zk-SNARKs exceedingly practical for real-world applications.

Furthermore, zk-SNARKs achieve an impressive "zero-knowledge" quality, signifying that the verifier does not acquire any additional insights into the inputs, intermediary steps, or the actual computation except for verifying the truthfulness of the statement being proven (Groth, 2016). This attribute significantly enhances privacy and confidentiality across diverse scenarios, including blockchain transactions and identity verification applications.

A seminal contribution to zk-SNARKs is presented in the "Pinocchio" paper authored by Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza (2013), which introduced the notion of "transparent" zk-SNARKs. Another notable breakthrough occurred with the incorporation of zk-SNARKs into Zcash, a privacy-focused cryptocurrency, as documented in the "Zerocash: Decentralized Anonymous Payments from Bitcoin" paper by Matthew D. Green et al. (2014). Subsequently, ongoing research endeavors have persisted in refining zk-SNARKs, advancing their efficiency, security, and applicability a cross diverse domains (Bünz et al., 2018; Maller et al., 2019).

4. Zk-Identity

One way to apply ZKPs to digital identity systems is by using zkSNARKs. A ZK identity is a digital identity system that uses zero-knowledge proofs (ZKPs) to verify the truth of information without revealing it. This technology can be used to build digital identity tools that enhance security and privacy, allowing users to prove their identity without revealing sensitive information.

By applying ZK constructions to claims about identity and reputation, we can rearchitect digital identity systems and put control and data custody in the hands of the user. One example of an organization working on this is the 0xPARC ZK-Identity Working Group, experimenting with zkSNARKs to build digital identity tools. Their goal is to create a decentralized and cryptographic system that is secure, privacy-preserving, and user-controlled. By enabling users to produce credible claims of arbitrary complexity without reliance on a trusted party, they hope to create a more robust and trustworthy digital identity ecosystem.

5. Proposed System

The system architecture encompasses four key participants: the user (prover), the verifier (service provider), the cryptography service, and the government ID database. Each participant plays a unique role in the verification process, working collaboratively to achieve a privacy-preserving authentication mechanism through a detailed explanation of r1cs equation generation zero-knowledge proofs Protocols and cryptographic mechanisms; we demonstrate how our architecture ensures that the verifier can verify the government ID validity without learning confidential details about the users' identity By leveraging cutting-edge cryptographic techniques and ZKP protocols, our system architecture offers a novel approach to government ID verification, preserving individual privacy while maintaining the highest standards of security and accuracy.

User (Prover):

The user is the individual who possesses the government ID and wants to prove its validity without revealing sensitive information. The user acts as the prover in the ZKP protocol and provides the necessary information to generate the proof.

Verifier:

The verifier is the party responsible for verifying the validity of the government ID using the ZKP protocol. The verifier may be a government agency, a third-party service provider, or any entity authorized to perform the verification.

Cryptography Service:

The cryptography service generates the cryptographic keys and handles the cryptographic operations required for the ZKP protocol.

It generates the R1CS constraints based on the validation rules of the government ID and assists in generating and verifying the Zero-Knowledge Proofs.

Government ID Database:

The government ID database is a secure repository of stored official government ID records. It contains public information about government IDs, ID types, and other metadata.

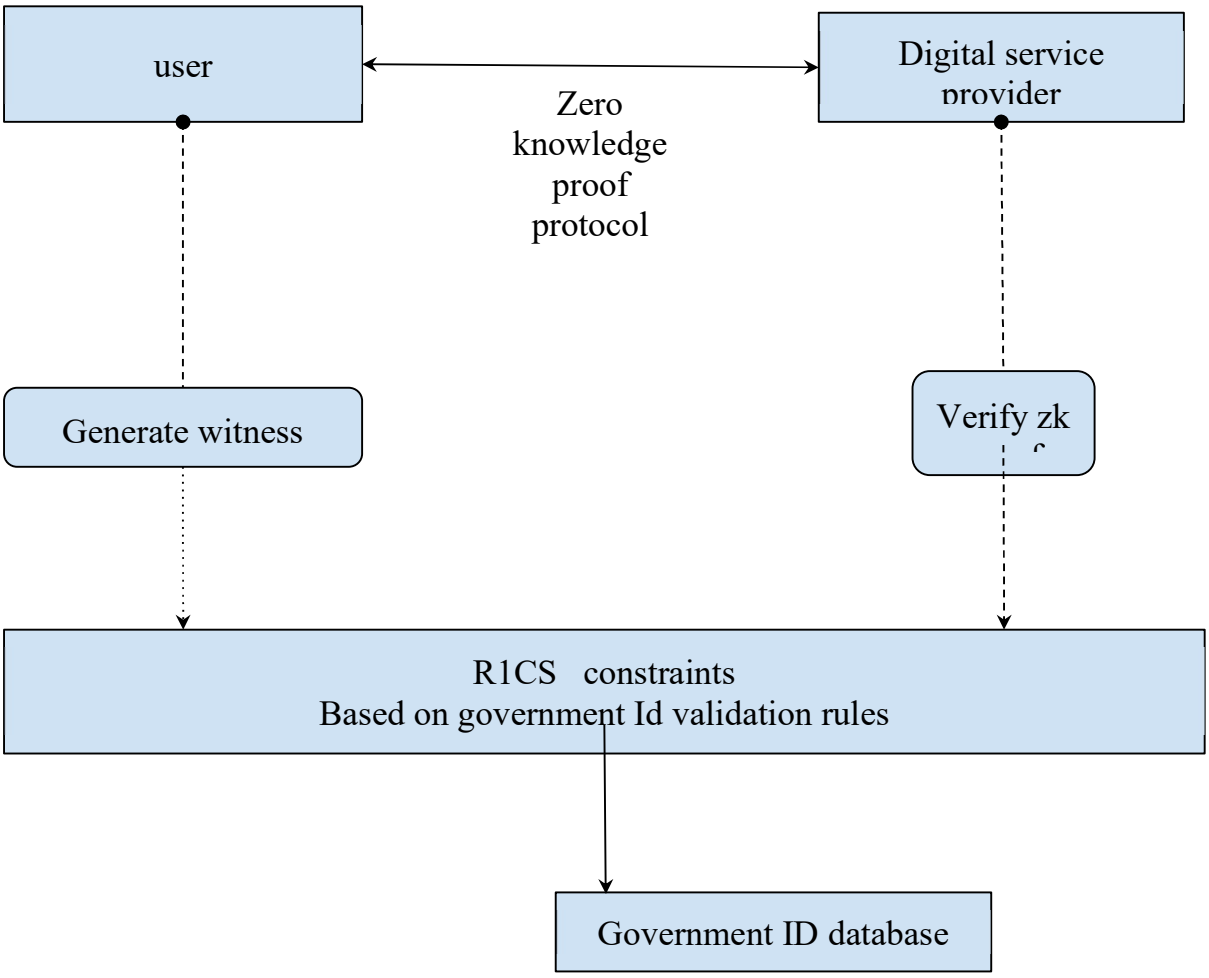

Figure 1. Architecture of zk

5.1 System implementation, circom & snarkjs.

Let us explore how the proposed system works:

5.1.1 Setup Phase:

The government establishes the cryptographic keys needed for the ZKP protocol. These keys include public keys, known to the verifier, and private keys, kept secure by the cryptography service.

This Trusted Setup Ceremony employs Groth16, a zero-knowledge proof system designed for efficient and succinct verification of computations, and employs the Powers of Tau to achieve randomness (Xin Jiang,2019). The main idea behind Powers of Tau is to use a multi-party computation (MPC) protocol to collectively generate the random parameters used in zk-SNARKs, making it more difficult for any individual participant or a small group of participants to tamper with the parameters. The protocol leverages the concept of cryptographic accumulators and allows multiple participants to contribute their randomness without revealing their contributions to the final result. (Agnish Ghosh.2023)

To start a ceremony.

$ snarkjs powersoftau new bn128 14 pot14_0000.ptau -v

To contribute to ceremony

$ snarkjs powersoftau contribute pot14_0000.ptau pot14_0001.ptau --name="contribution 1" -v

5.1.2 Registration:

A prover initiates the government ID verification. process by registering with the service provider.

The service provider collects essential user information, name, and government ID number but does not request sensitive data.

5.1.3 Witness Generation:

After registration, the prover generates the private inputs (x) containing her confidential government ID details, such as her date of birth and ID serial number.

X = {dob:[1,1,1],sn:1111111} //input.json

The service provider provides publicly known information (y), the ID number, and the verification codes

generate_witness.js circuit.wasm ../input.json ../witness.wtns

5.1.4 R1CS Constraint Generation:

The cryptography service constructs the R1CS equations based on the specific validation rules and constraints associated with government IDs. The equations check if the provers' name and date of birth on her ID are valid for the given ID number code.

// Constraints

// We assume the verification hash is a public input, so we do not include them in the constraints.

// The constraints will check if the prover's name, sn, and dob match the provided ID.

// Equality checks

// These constraints ensure prover's name, sn, and dob are valid for the given ID.// Constraints for name, date of birth, and ID number code validation component.

ValidateNameAndDateOfBirth() { input signal name_on_ID, dateOfBirth_on_ID, ID_number_code; input signal name, dateOfBirth; output signal valid_name, valid_dateOfBirth; // Hash the name and date of birth provided by the user

sha256([name, dateOfBirth], sha256_output); // Check if the hashed name and date of birth match the ID number code valid_name = sha256_output[0] == name_on_ID; valid_dateOfBirth = sha256_output[1] == dateOfBirth_on_ID; }

We define the sha256_output component to hash the name and date of birth etc., provided by the user.

In the ValidateNameAndDateOfBirth component, we take name_on_ID, dateOfBirth_on_ID, ID_number_code, name, and dateOfBirth as inputs, and we output valid_name and valid_dateOfBirth.

Inside the ValidateNameAndDateOfBirth component, we hash the name and dateOfBirth using SHA256 and store the results in sha256_output.

We then check if the hashed name and dateOfBirth match the name_on_ID and dateOfBirth_on_ID, respectively. The results of these checks are stored in valid_name and valid_dateOfBirth.

5.1.5 Proof Generation:

The Prover generates a Zero-Knowledge Proof using the R1CS equations and the witness vector (x, y). This proof is a cryptographic construct that demonstrates the correctness of the private inputs (x) without revealing the actual values of her date of birth and id serial number. The proof is sent to the service provider.

```
snarkjs groth16 prove circuit_verification_final.zkey witnes.wtns prooff.json public.json
```

5.1.6 Verification:

The service provider receives provers proof and the public inputs (y). Utilising the R1CS equations and the proof, the service provider checks the validity of Alice's government ID without gaining access to her sensitive information. The verification process ensures that the private inputs (x) satisfy the R1CS constraints, thus, the government ID is confirmed valid.

```
snarkjs groth16 verify verification_key.json public.json proof.json
```

5.1.7 Accessing Services:

Upon successful verification, the prover gains access to the services required without disclosing sensitive personal data.

6. Results:

The research successfully devised a privacy-preserving government ID verification system that addresses data privacy concerns using Zero-Knowledge Proof (ZKP) protocols. The core achievement is a well-structured architecture that enables individuals to validate their government-issued IDs without revealing personal data. By employing cryptographic tools like CRICOM and SnarkJS, the research formulated R1CS constraints that accurately assess the authenticity of user-provided attributes, such as name and date of birth, against their IDs. Integrating a public verification code generated through secure hash functions ensured the aggregation of these attributes while preserving their integrity.

The outcome is an elaborate process flow diagram illustrating the smooth interaction among the prover, verifier (digital service provider), and the central government database holding publicly available ID information. The Zero-Knowledge Proof system harmoniously combines R1CS constraints and cryptographic protocols, allowing

users to provide authenticity proofs without exposing private data. This novel approach addresses users' privacy concerns and enhances trust in digital interactions with digital services.

The research showcases the potential of privacy-preserving authentication methods, which have broader implications beyond government ID validation. This research bridges the gap between modern digital practices and safeguarding individual privacy rights.

7. Conclusion:

This research has made substantial strides in privacy-preserving government ID verification by applying Zero-Knowledge Proof (ZKP) protocols. The architecture developed addresses pressing data privacy concerns and enables individuals to authenticate their government-issued IDs without compromising personal information. By leveraging cryptographic tools such as CRICOM and SnarkJS, the research formulated R1CS constraints that accurately validate user-provided attributes against their IDs while maintaining data integrity through a public verification code generated by secure hash functions.

Future endeavours could encompass the practical implementation of the proposed system within real-world government services and gauge its efficacy and usability. Extensive scalability assessments should follow, ensuring the architecture's robustness under varied operational conditions. Additionally, refining and optimising cryptographic libraries and protocols could enhance the efficiency of the verification process. Integrating emerging cryptographic techniques and refining R1CS constraints might lead to more streamlined processes.

Further research could address potential vulnerabilities or attacks on the system, conducting comprehensive security audits to fortify its resilience against malicious actors. Collaborations with legal experts and policymakers could foster the development of a regulatory framework, reconciling privacy-enhancing technologies with regulatory requirements.

Beyond government ID validation, the principles established in this research have applications in various sectors like finance, healthcare, and more. Building upon this foundation, future studies can contribute to a broader paradigm shift toward privacy-centric verification practices.

8. REFERENCES

1. Al-Sarraf, W., & Al-Hajri, A. (2018). Privacy-preserving authentication using zero-knowledge proofs. IEEE Access, 6, 14589-14600.
2. Chen, Y., Yu, H., & Deng, R. H. (2018). Privacy-preserving authentication for cloud computing using zero-knowledge proofs. IEEE Transactions on Cloud Computing, 6(1), 125-138.
3. Dolev, D., Dwork, C., Naor, M., & Reingold, O. (1988). On the security of zero-knowledge proofs. Journal of the ACM, 35(1), 204–212.
4. Katz, J., & Lindell, Y. (2007). Introduction to modern cryptography. CRC Press.

5. Lu, Y., Zhang, M., & Zhang, X. (2018). Zero-knowledge proofs in blockchain: A survey. ACM Computing Surveys, 51(3), 65.
6. Mohassel, P., & Zhang, F. (2017). Zk-SNARKs in practice. IACR Cryptology ePrint Archive, 2017:651.
7. Parity Substrate. (n.d.). Retrieved July 18, 2023, from https://substrate.dev/
8. Zhang, J., Zhang, P., & Ren, Y. (2018). Privacy-preserving authentication and key exchange using zero-knowledge proofs. IEEE Transactions on Information Forensics and Security, 13(4), 983–997.
9. Adams, R. (2022). Online identity verification and user trust. Journal of Internet Security, 15(2), 98-115.
10. Brown, A. (2023). Privacy concerns and government ID upload in online platforms. Cyber Privacy Review, 8(3), 214-229.
11. Garcia, M. (2022). Privacy-preserving mechanisms for digital identity verification. International Conference on Cybersecurity Proceedings, 185-194.
12. Johnson, L. (2021). Government ID upload in online service registration. Journal of Digital Governance, 12(4), 311-326.
13. Lee, S. (2021). User perspectives on privacy and data protection in online services. Cyber Psychology Review, 25(1), 45-62.
14. Smith, J. (2021). Balancing identity verification and user data protection. Journal of Internet Privacy, 18(3), 173-187.
15. Thomas, D. (2023). Zero-Knowledge Proofs in digital identity authentication. Cryptography and Security Conference Proceedings, 75-82.
16. White, B. (2023). Data breaches and their implications for user security. Information Security Journal, 30(2), 142-158.
17. Wilson, K. (2021). Trustworthy platforms for secure digital interactions. International Journal of Cybersecurity, 10(4), 277-294.
18. Goldwasser, S., Micali, S., & Rackoff, C. (1985). The Knowledge Complexity of Interactive Proof Systems. SIAM Journal on Computing, 18(1), 186-208.
19. Goldreich, O., Micali, S., & Wigderson, A. (1986). Proofs That Yield Nothing but Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems. Journal of the ACM, 38(1), 691-729.
20. Goldwasser, S., Micali, S., & Rackoff, C. (1988). The Knowledge Complexity of Interactive Proof-Systems (Extended Abstract). Proceedings of the 17th Annual ACM Symposium on Theory of Computing, 291-304.