Enhancing the Flexibility and Automation of Post-Quantu Anonymous Credentials: A Comparative Analysis of Zero-Knowledge Virtual Machines and SNARK Circuit Compilers

A Thesis Submitted to the Department of Computer Science and Communications Engineering, the Graduate School of Fundamental Science and Engineering of Waseda University in Partial Fulfillment of the Requirements for the Degree of Master of Engineering

Takumi Otsuka

The Department of Computer Science and Communications Engineering, the Graduate School of Fundamental Science and Engineering of Waseda University

5124FG15-6

Submission Date : , 2026

Research Guidance: : Research on Cryptographic Protocols

Advisor: : Prof. Kazue Sako

Abstract

The advent of quantum computing demands a rapid transition to post-quantum cryptographic solutions. In digital identity, SNARK-friendly schemes like Loquat[1] underpin post-quantum anonymous credential systems such as BDEC[2]. However, BDEC's reliance on static, custom zkSNARK[3] circuits for credential verification leads to critical inflexibility, rendering it impractical for dynamic attribute management. Zero-Knowledge Virtual Machines[4] (zkVMs) promise a solution, offering to prove arbitrary programs and transform complex circuits into high-level code updates. This research will investigate the specific zero-knowledge properties of different zkVMs through comparative analysis of zkVMs and alternative SNARK circuit compilers[5], implementing and benchmarking the BDEC verifier within both approaches. This quantitative and qualitative analysis will determine which approach offers a more viable and agile foundation for the next generation of digital identity systems, specifically addressing the trade-offs between flexibility, performance with concrete metrics such as prover time, verification time, and memory usage.

Contents

List of Figures

List of Tables

1 Introduction

2 Background

Notation

Let $\lambda \in \mathbb{N}$ be the security parameter, $\mathsf{negl}(\lambda)$ denote a negligible function, and PPT stand for probabilistic polynomial-time algorithms.
We use pp to denote public parameters, and sk, pk for secret and public keys, respectively. The symbol crs represents a common reference string typically used in zero-knowledge proof systems, and pk, vk refer to the proving and verifying keys of zkSNARKs. The public input to a zkSNARK is denoted x, the private witness as ω, and the proof as π. For digital signatures, m is the message, and σ is its signature. The relation or circuit verified by zkSNARKs is expressed as $C(x, \omega)$.
Regarding anonymous credentials, $\mathcal{A}$ denotes the universal set of attributes, with attr and $\mathsf{subattr}$ as subsets of $\mathcal{A}$. A credential is represented by cred, and a shown credential by show. The logical statement or predicate proved on attributes is stmt, and auxiliary descriptions by aux.
For the Loquat post-quantum signature scheme, $\mathsf{L\text{-}pp}$ denotes its specific public parameters, and H the collision-resistant hash functions it uses. We denote $R1CS$ as the Rank-1 Constraint System representation of arithmetic circuits. The prime field used for the Legendre PRF is $\mathbb{F}_p$, and $\mathcal{L}(\cdot)$ the Legendre symbol pseudorandom function.

2.1 Cryptographic Primitives

2.1.1 zkSNARKs

A zk-SNARK (more commonly referred to as Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) [**?**, **?**, **?**] is a cryptographic proof system that enables a *prover* to convince a *verifier* that they know a secret witness ω satisfying a publicly-known statement $C(x, \omega) = \mathsf{true}$, without revealing ω, in a succinct and non-interactive format. Concretely, a zk-SNARK consists of the following algorithms,

1. $\mathsf{Setup}(1^\lambda) \ \rightarrow \ (\mathsf{pk}, \mathsf{vk})$,
2. $\mathsf{Prove}(\mathsf{pk}, x, \omega) \ \rightarrow \ \pi$,
3. $\mathsf{Verify}(\mathsf{vk}, x, \pi) \ \in \ \{0, 1\}$,

where λ is the security parameter, x is the public input and ω the private witness.

The zk-SNARK system should satisfy the following properties:

Completeness. If $C(x, \omega) = \mathsf{true}$, then for an honest *prover*

$$\Pr\left[\mathsf{Verify}(\mathsf{vk}, x, \pi) = 1 \;\middle|\; \pi \leftarrow \mathsf{Prove}(\mathsf{pk}, x, \omega)\right] \geq 1 - \mathsf{negl}(\lambda).$$

Soundness. For any probabilistic polynomial-time adversary Adv,

$$\Pr\left[\mathsf{Verify}(\mathsf{vk}, x, \pi) = 1 \ \wedge \ \neg\exists\, \omega' \colon \ C(x, \omega') = \mathsf{true} \;\middle|\; \begin{array}{c} (\mathsf{pk}, \mathsf{vk}) \leftarrow \mathsf{Setup}(1^\lambda), \\ (x, \pi) \leftarrow \mathsf{Adv}(\mathsf{pk}) \end{array}\right] \leq \mathsf{negl}(\lambda).$$

Moreover, there exists an extractor $\mathcal{E}$ such that if Adv outputs an accepting proof (x, π) with non-negligible probability, then $\mathcal{E}(\mathsf{Adv}\text{'s state})$ outputs a valid ω' satisfying $C(x, \omega') = \mathsf{true}$.

Zero-Knowledge. There exists a simulator Sim that, given only the verification key vk and a public input x with $C(x, \cdot)$ satisfiable, produces a proof π^* such that the distribution

$$(x, \pi) = (x, \pi \leftarrow \mathsf{Prove}(\mathsf{pk}, x, \omega))$$

is computationally indistinguishable from $(x, \pi^*) = (x, \pi^* \leftarrow \mathsf{Sim}(\mathsf{vk}, x))$.

Succinctness. The size of the proof π is short, typically $O(\mathsf{polylog}(|C|))$ or otherwise "sub-linear" in the size of the circuit representing C; the *verifier*7s running time is similarly efficient (e.g., $O(|x| + \mathsf{polylog}(|C|))$).

2.1.2 Digital Signatures

A digital signature scheme is composed of the following tuple of PPT algorithms $\mathsf{Setup}(1^\lambda)$, $\mathsf{KeyGen}(\mathsf{pp})$, $\mathsf{Sign}(sk, m)$, and $\mathsf{Verify}(pk, m, \sigma)$.

Definition 2.1 (EUF-CMA Security)**.** A digital signature scheme Σ is existentially unforgeable under chosen-message attacks (EUF-CMA) if for all PPT adversaries $\mathcal{A}$ with access to a signing oracle $\mathcal{O}_{\mathsf{Sign}}$, the probability that $\mathcal{A}$ outputs a pair $(m^\star, \sigma^\star)$ such that $\mathsf{Verify}(\mathsf{pk}, m^\star, \sigma^\star) = 1$ and $m^\star$ was never queried to $\mathcal{O}_{\mathsf{Sign}}$ is negligible in λ.

In this work, we instantiate the above notion with the *Loquat* post-quantum signature scheme.

Definition 2.2 (Loquat: A SNARK-Friendly Post-Quantum Signature)**.** Loquat [**?**] is a digital signature scheme post-quantum secure under collision-resistant hashes and Legendre PRF, where

$$\begin{aligned}
(\mathsf{L\text{-}pp}) &\leftarrow \mathsf{L\text{-}Setup}(1^\lambda),\\
(sk, pk) &\leftarrow \mathsf{L\text{-}KeyGen}(\mathsf{L\text{-}pp}),\\
\sigma &\leftarrow \mathsf{L\text{-}Sign}(\mathsf{L\text{-}pp}, sk, m),\\
\{0,1\} &\leftarrow \mathsf{L\text{-}Verify}(pk, m, \sigma, \mathsf{L\text{-}pp}).
\end{aligned}$$

Security. Loquat is proven EUF-CMA secure in the random-oracle model under the hardness of breaking the underlying Legendre PRF and the collision resistance of H [**?**].
A crucial property for this work is that the Loquat verification algorithm admits an efficient rank-1 constraint system (R1CS) representation.

SNARK-friendliness. For the Loquat-128 parameter set instantiated with the Griffin hash function, the verification circuit can be represented using approximately 1.49×10^5 R1CS constraints [**?**]. This is significantly smaller than known SNARK encodings of lattice-based post-quantum signature schemes such as CRYSTALS-Dilithium at comparable security levels [**?**], and thus makes Loquat particularly suitable for use inside zkSNARK circuits.

2.2 Anonymous Credentials

Definition 2.3 (Anonymous Credential System)**.** An anonymous credential system over an attribute universe $\mathcal{A}$ is a tuple of PPT algorithms $\mathsf{AC.Setup}(1^\lambda)$, $\mathsf{AC.KeyGen}(\mathsf{pp})$, $\mathsf{AC.Issue}(isk, ipk, \mathsf{attr} \subseteq \mathcal{A}, aux)$, $\mathsf{AC.Show}(\mathsf{cred}, \mathsf{subattr} \subseteq \mathsf{attr}, \mathsf{stmt})$, and $\mathsf{AC.Verify}(\mathsf{pk_I}, \mathsf{show}, \pi, \mathsf{subattr}, \mathsf{stmt}, aux)$.

Definition 2.4 (BDEC: Post-Quantum Blockchain-based Digital Education Credential)**.** BDEC is a post-quantum anonymous credential system designed to securely and privately verify educational achievements on a blockchain. It builds upon generic anonymous credentials and ensures the following properties:

- **Unforgeability**: No adversary can forge valid credentials.
- **Anonymity**: Credentials hide the user's identity.
- **Unlinkability**: Different proofs by the same user cannot be linked.
- **Conditional Linkability**: Selective linking enables managing fragmented learning records.
- **Revocation**: Credentials can be revoked if compromised.

2.2.1 Static Circuit Limitation

BDEC fixes circuit size to maximum attributes $|A| \leq N$ (e.g., $N = 32$). Dynamic $|A|$ requires new $\mathsf{Setup}(N')$ per update, breaking efficiency.

2.3 Dynamic Approaches

2.3.1 Zero-Knowledge Virtual Machines

2.3.2 SNARK Circuit Compilers

3 Dynamism

Theorem 3.1 (Architectural Constraint Overhead for BDEC)**.**

Theorem 3.2.

Theorem 3.3.

4 Evaluation

5 Discussion

6 Conclusion

Acknowledgement

References

[1] X. Zhang, R. Steinfeld, M. F. Esgin, J. K. Liu, D. Liu, and S. Ruj, "Loquat: A SNARK-friendly post-quantum signature based on the legendre PRF with applications in ring and aggregate signatures," Cryptology ePrint Archive, Paper 2024/868, 2024. [Online]. Available: https://eprint.iacr.org/2024/868

[2] Z. Z. Li, X. Zhang, H. Cui, J. Zhao, and X. Chen, "Bdec: Enhancing learning credibility via post-quantum digital credentials," in *Provable and Practical Security: 18th International Conference, ProvSec 2024, Gold Coast, QLD, Australia, September 25–27, 2024, Proceedings, Part II*. Berlin, Heidelberg: Springer-Verlag, 2025, pp. 45–64. [Online]. Available: https://doi.org/10.1007/978-981-96-0957-4_3

[3] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from bitcoin," Cryptology ePrint Archive, Paper 2014/349, 2014. [Online]. Available: https://eprint.iacr.org/2014/349

[4] T. Dokchitser, and A. Bulkin, "Zero knowledge virtual machine step by step," Cryptology ePrint Archive, Paper 2023/1032, 2023. [Online]. Available: https://eprint.iacr.org/2023/1032

[5] R. Lavin, X. Liu, H. Mohanty, L. Norman, G. Zaarour, and B. Krishnamachari, "A survey on the applications of zero-knowledge proofs," 2024. [Online]. Available: https://arxiv.org/abs/2408.00243

A Proof of Theorem