A Modified Schnorr Sigma Protocol and Its Application to Isogeny-Based Identification

Mahdi Mahdavi[1], Zaira Pindado[2], Amineh Sakhaie[3], and Helena Rifà-Pous[1]
[1] Universitat Oberta de Catalunya (UOC), [2] Barcelona Supercomputing Center (BSC), [3] University of Lisbon
e-mail: {m_mahdavi | hrifa}@uoc.edu zaira.pindado@bsc.es
fc65105@alunos.ciencias.ulisboa.pt

***Abstract*—Quantum computing threatens classical cryptographic protocols like the Schnorr identification scheme, which relies on the Discrete Logarithm Problem (DLP), vulnerable to quantum attacks. In this paper, we propose a modification to the classical Schnorr protocol by redefining the prover response as $r = cu \pm x$ mod q instead of $r = u + cx$ mod q. While this adjustment preserves the arithmetic simplicity of the original protocol, it introduces subtle but significant changes to the protocol's security and verifiability. We analyze its soundness, zero-knowledge properties, extractor functionality, and practical viability, and explore its adaptation into a secure digital signature system under standard cryptographic assumptions. To underscore the practical significance of our approach, we implement the modified protocol within an isogeny-based framework, demonstrating its capacity to enhance an existing identification scheme with respect to both security and efficiency. Our findings illustrate that revisiting classical protocols through judicious modifications can yield more robust, quantum-resistant solutions for applications like blockchain.**

Keywords-Schnorr Protocol; Zero-knowledge proofs; Discrete Logarithm Problem; Isogeny-based cryptography; Post-Quantum Cryptography.

I. Introduction

Identification protocols are fundamental cryptographic primitives that enable a prover to convince a verifier of their identity by demonstrating knowledge of a secret without disclosing it. These protocols are the foundation for many cryptographic systems, such as authentication frameworks, zero-knowledge proofs, and digital signature algorithms. One of the most celebrated and widely studied identification schemes is the Schnorr identification protocol [1], which offers a simple and elegant construction grounded in the hardness of the Discrete Logarithm Problem (DLP) [2].

The Schnorr protocol is a canonical Σ-protocol that defines the prover's response to the verifier's challenge c as $r = u + cx \bmod q$, where u is a random nonce used in the commitment, x is the prover's secret and c is the challenge. This formulation balances efficiency and security, and forms the basis for many digital signature schemes through the Fiat–Shamir transformation [3].

As a Σ-protocol, Schnorr satisfies three essential properties: completeness, which ensures that an honest prover always convinces the verifier; special soundness, which guarantees that if an adversary can produce two accepting transcripts with the same commitment but different challenges, then it is possible to efficiently extract the secret x, and Honest Verifier Zero-Knowledge (HVZK), meaning that a simulator, given access to the challenge, can generate transcripts that are computationally indistinguishable from real interactions, without knowing the prover's secret.

A. Related work

The Schnorr protocol has been extensively studied and extended in various directions. Fuchsbauer et al. [4] analyzed blind Schnorr signatures and signed ElGamal encryption techniques using the Algebraic Group Model (AGM), demonstrating robust security guarantees under normal assumptions without the use of heuristic arguments.

In the threshold setting, Bacho et al. [5] introduced HARTS, the first threshold Schnorr signature scheme that is simultaneously adaptively secure, robust under full asynchrony, and communication-efficient. HARTS supports high-threshold configurations—where the number of required signers can significantly exceed the corruption threshold—and outputs standard Schnorr signatures using only one asynchronous online round and subcubic communication.

Fukumitsu and Hasegawa [6] demonstrated that Schnorr signatures are secure in the multi-user setting under the AGM, assuming the hardness of the DLP. This multi-user resilience is essential for large-scale deployments, such as public key infrastructures.

In parallel, Fuchsbauer and Wolf [7] proposed a practical, concurrently secure blind signature protocol compatible with standard Schnorr signatures. Their technique ensures system compatibility while introducing predicate blind signatures, enabling signers to impose constraints on signed messages—a feature particularly valuable for privacy-preserving blockchain applications.

In post-quantum cryptography, Galbraith, Petit, and Silva [8] developed two digital signature systems based on the hardness of isogeny problems over supersingular elliptic curves, leveraging a novel identification technique to achieve quantum-resistant security. A key innovation in their work is a novel identification technique that builds upon a well-established computational problem but addresses limitations seen in prior methods. These systems can be converted into secure digital signatures using both classical and quantum-safe approaches, providing a realistic path to efficient post-quantum cryptography solutions. In a related advancement, Baghery et al. [9] adapted the Schnorr sigma protocol to the isogeny-based setting.

These developments illustrate the robustness of the Schnorr paradigm across diverse cryptographic settings. Building on this foundation, we introduce a novel algebraic modification to the protocol's response function to improve efficiency and resilience in isogeny-based, post-quantum identification schemes.

B. Our contribution

In this paper, we propose a novel variation of the Schnorr identification protocol in which the prover's response is computed as $r = cu \pm x \mod q$, fundamentally altering the interaction between the nonce, challenge, and secret. This structural change results in a new verification equation and requires a complete re-evaluation of the protocol's security properties. Unlike minor tweaks, our modification challenges the conventional structure and allows for new analytical insights.

Our main contributions can be summarised as follows.

1) Formal definition and analysis of the modified protocol, reversing the typical dependency between the challenge and the secret. We also prove the security proofs that guarantee the protocol maintains completeness, special soundness, and honest-verifier zero-knowledge.
2) We analyze how the modified response can be adapted for use in non-interactive settings via the Fiat–Shamir heuristic, preserving signature viability.
3) We propose a new post-quantum id protocol based on isogenies using the modified Schnorr protocol.
4) An examination of the proposed Sigma protocol's application within isogeny-based cryptographic systems. Building upon and extending prior work [9], we identify significant advantages, most notably the elimination of the requirement for witnesses at critical proof stages. This refinement enhances protocol resilience by preventing leakage of errors related to the protocol, or witness during execution.

In addition, our modified Schnorr protocol enables the use of the MPC-in-the-Head technique and its advantages, which we leave as an avenue for future work.

This paper is structured as follows. In Section II, we provide the necessary background on Σ-protocols, digital signature schemes, and isogeny-based identification systems. Section III introduces our modified Schnorr protocol in detail, including the new response format and its implications on completeness, special soundness, and honest-verifier zero-knowledge. We also show how our construction leads to a secure digital signature scheme under the Discrete Logarithm Problem and supports non-interactive instantiations via the Fiat–Shamir transform. In Section IV, we extend the modified protocol to an isogeny-based setting, presenting a novel identification scheme that improve upon previous work by eliminating the need for witnesses during critical stages and enhancing resilience against execution errors. Finally, Section V concludes with a summary of our findings and outlines potential directions for future research in post-quantum cryptography.

II. PRELIMINARIES

A. Notation

Let $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ denote the set of integers modulo q, being q a positive prime integer and $\mathbb{Z}_q^*$ its multiplicative set. Let $\mathbb{G}$ be a group of order q with generator $g \in \mathbb{G}$.

Let $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ denote the ring of integers modulo N, where N is a composite integer with a known prime factorization $N = \prod_{i=1}^{m} q_i^{r_i}$, such that $q_1 < q_2 < \cdots < q_m$ are distinct prime numbers and each $r_i \in \mathbb{N}$.

For any set S, the notation $a \xleftarrow{\$} S$ indicates that the element a is sampled uniformly at random from S. A function $\mu(X)$ from the natural numbers to the non-negative real numbers is *negligible* if for every positive polynomial p there is a constant C such that for all integers $x > C$, we have $\mu(x) < \frac{1}{p(x)}$ [9]. We denote by λ the security parameter.

Discrete Logarithm Problem (DLP). *Given a group $\mathbb{G}$, a generator $g \in \mathbb{G}$ and some element $h = g^x \in \mathbb{G}$, recovering x is called the Discrete Logarithm Problem.*

B. Sigma protocols

Let $V = V(\lambda)$ and $W = W(\lambda)$ be two sets defined with respect to a security parameter λ. Let $\mathrm{R} \subseteq V \times W$ be a **relation** on $V \times W$ that defines a **language** $\mathrm{L} = \{v \in V : \exists w \in W, \mathrm{R}(v; w) = 1\}$. An element $w \in W$ such that $\mathrm{R}(v; w) = 1$ for some $v \in \mathrm{L}$ is called a **witness** for v.

A sigma-protocol (Σ-protocol) for the relation R is a three-round interactive protocol between two Probabilistic Polynomial-Time (PPT) algorithms: a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. The prover holds a witness w for $v \in \mathbf{L}$, and the verifier knows v. The protocol proceeds as follows: $\mathcal{P}$ sends a *commitment* a, $\mathcal{V}$ answers with a *challenge* c, and $\mathcal{P}$ sends a *response* r. The verifier accepts or rejects the proof based on the triple (a, c, r), which is called a transcript of the Σ-protocol.

A Σ-protocol satisfies three properties: completeness, special soundness, and honest verifier zero-knowledge (HVZK).

Completeness. *A Σ-protocol Π with parties $(\mathcal{P}, \mathcal{V})$ is complete for* R*, if for all $(v; w) \in \mathrm{R}$, the honest $\mathcal{V}$ always accepts the honest proof of $\mathcal{P}$.*

Special Soundness. *A Σ-protocol Π has a* special soundness *for* R *if there exists a PPT extractor $\mathcal{E}$ such that, for any $v \in \mathrm{L}$, given two valid transcripts (a, c, r) and (a, c', r') with the same commitment a but different challenges $c \neq c'$, the extractor $\mathcal{E}(a, c, r, c', r')$ outputs a valid witness w such that $(v; w) \in \mathrm{R}$.*

Honest-Verifier Zero-Knowledge (HVZK). *A Σ-protocol Π satisfies* HVZK *for* R *if there exists a PPT simulator* Sim *such that, for all $(v; w) \in \mathrm{R}$, the transcript (a, c, r) generated by $\mathsf{Sim}(v)$ is computationally indistinguishable from a real transcript produced by an honest execution between the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ on input $(v; w)$.*

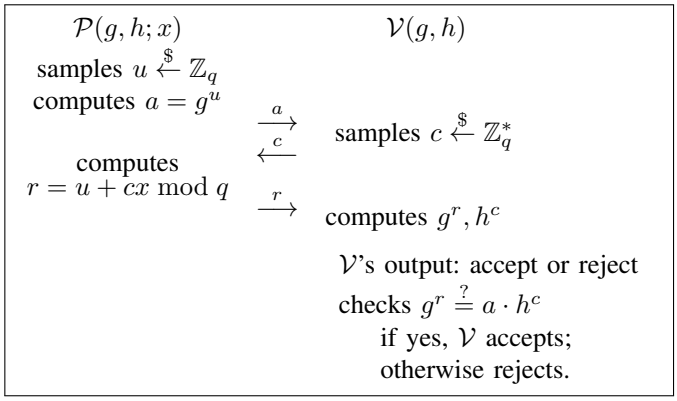

Figure 1. Protocol 1- Schnorr Protocol for relation $\mathrm{R_{ID}}$.

1) Schnorr Identification Protocol: The Schnorr protocol instantiates a Σ-protocol for the relation $\mathrm{R_{ID}} = \{(g, h; x) \mid h = g^x\}$ with $\mathbb{G}$ a multiplicative group of order q and generator g. Let $x \in \mathbb{Z}_q$ be the secret key (witness) and $h = g^x \in \mathbb{G}$ be the public key. Protocol 1 (see Figure 1) describes the steps of the Schnorr protocol.

The Schnorr protocol satisfies the key properties of a Σ-protocol:

- **Completeness:** If the prover is honest and knows x, then

$$g^r = g^{u+cx} = g^u \cdot (g^x)^c = a \cdot h^c$$

  and the verifier accepts.
- **Special Soundness:** Given two accepting transcripts (a, c, r) and (a, c', r') with $c \neq c'$, we show how the verifier can extract x.First, we have $g^r = a \cdot h^c$ and $g^{r'} = a \cdot h^{c'}$. Then, by operating these two expressions, $g^r g^{-r'} = h^{c-c'}$ we get that the discrete logarithm of h is equal to $(r - r')(c - c')^{-1} \mod q$.
- **HVZK:** There exists a simulator S that, chooses random values $c \xleftarrow{\$} \mathbb{Z}_q^*$ and $r \xleftarrow{\$} \mathbb{Z}_n$, computes:

$$a = g^r \cdot h^{-c}$$

  and outputs a transcript (a, c, r) that is indistinguishable from a real one.

C. Isogeny-Based ID Protocol Using Structured Public Keys

An identification (ID) protocol allows a prover to demonstrate the knowledge of a secret key corresponding to a public key, often formalized as a Σ-protocol over a hard relation. In isogeny-based cryptography, the underlying hardness assumption is the difficulty of computing isogenies between supersingular elliptic curves, a post-quantum hard problem.

Commutative Supersingular Isogeny Diffie–Hellman (CSIDH) [10] was proposed to enhance the efficiency of isogeny-based cryptography by using supersingular elliptic curves over the prime field $\mathbb{F}_p$. The CSI-FiSh signature scheme [11] was developed within the CSIDH framework to provide efficient isogeny-based signatures. It began with a binary challenge space and was later optimized with larger public keys and an improved identification protocol, achieving subsecond signing times.

In [9], the authors propose an efficient isogeny-based identification protocol that extends CSI-FiSh [11], which was previously enhanced in [12] and [13] to support a larger challenge space through the use of structured public keys. This enhancement significantly reduces the soundness error and communication overhead. The protocol is built on Hard Homogeneous Spaces and introduces exceptional and superexceptional sets to ensure extractability and security. A non-interactive signature version is derived via the Fiat–Shamir transform, achieving strong unforgeability in the quantum random oracle model. Additionally, they present trustless key generation techniques using zero-knowledge proofs of well-formedness, making the scheme both efficient and suitable for postquantum cryptographic applications.

Let E_0 be a fixed supersingular elliptic curve over $\mathbb{F}_p$, and let $\mathrm{Cl}(\mathcal{O})$ be the class group of its endomorphism ring $\mathcal{O}$. This group acts freely and transitively on the isogeny class of E_0, defining a Hard Homogeneous Space (HHS). The secret key is an element $x \in \mathbb{Z}_N$, and the public key is $E_1 = [x]E_0$, where $[x]$ denotes the group action via an ideal class.

Classical isogeny-based ID protocols, such as those underlying CSI-FiSh [11], suffer from efficiency issues due to binary challenge spaces. To reduce the soundness error ϵ, they must be repeated λ times, where $\epsilon = 2^{-\lambda}$. The new protocol extends the challenge space to k elements, reducing the soundness error per round to $1/k$, or $1/(2k-1)$ when symmetry (through twisting) is used.

The security of our protocol is based on a hardness assumption: the $(c_0, \ldots, c_{k-1})$-*Vectorization Problem with Auxiliary Inputs*. Detailed definitions and explanations of this issue are presented in [9], which, it should be noted, draws inspiration from papers [14] and [15]. Given a starting curve E_0 and a sequence of images $\{E_i = [c_i x]E_0\}$, where $c_0 = 0$, $c_1 = 1$ and all pairwise differences $c_i - c_j$ (for $i \neq j$) are invertible modulo N. the problem is to recover the secret scalar x, under the assumption that each $c_i \in \mathbb{Z}_N$ and all pairwise differences $c_i - c_j$ are invertible modulo N. This assumption generalizes the discrete logarithm problem with auxiliary inputs to the setting of isogenies and hard homogeneous spaces.

The protocol presented in [9] can be made non-interactive using the Fiat-Shamir transform in the Quantum Random Oracle Model (QROM). This structure enables a tradeoff: larger public keys allow shorter proofs and 14× faster executions than repeated binary-challenge protocols, without compromising post-quantum security or requiring trusted third parties.

D. Hard Homogeneous Space

A Hard Homogeneous Space (HHS), as formulated by Couveignes [12], comprises a finite abelian group $\mathbb{G}$ and a finite set $\mathcal{E}$, equipped with an efficient computable group action

$$\star : \mathbb{G} \times \mathcal{E} \to \mathcal{E}.$$

This action satisfies the following structural properties:

1) **Freeness and Transitivity:** The group action is *free*, which means that for any $E \in \mathcal{E}$ and $g \in \mathbb{G}$, if $g \star E = E$, then g is the identity in $\mathbb{G}$. It is also *transitive*, to ensure that for every pair $E_1, E_2 \in \mathcal{E}$, there exists a $g \in \mathbb{G}$ such that $g \star E_1 = E_2$.
2) **Efficient Operations:** The group operation in $\mathbb{G}$, membership and equality checks in both $\mathbb{G}$ and $\mathcal{E}$, and the group action $\star$ are all efficiently computable. Furthermore, each element in $\mathbb{G}$ has a unique representation that can be computed efficiently, and elements of $\mathbb{G}$ can be sampled uniformly at random.
3) **Hard Computational Problems:** Security in HHS-based cryptosystems relies on the intractability of two core problems:
   - *Vectorization Problem:* Given $E_1, E_2 \in \mathcal{E}$, compute $g \in \mathbb{G}$ such that $g \star E_1 = E_2$.
   - *Parallelization Problem:* Given $E_1, E_2, F_1 \in \mathcal{E}$ with $E_2 = g \star E_1$ for some unknown $g \in \mathbb{G}$, compute $F_2 = g \star F_1$.

In the common special case where $\mathbb{G}$ is a cyclic group of known order N with generator g, the action can be expressed using additive notation as $[a]E := g^a \star E$, where $a \in \mathbb{Z}_N$ and $E \in \mathcal{E}$. This representation satisfies the compositional property

$$[a][b]E = [a+b]E,$$

which is frequently exploited in isogeny-based protocols.

III. Modified Schnorr Protocol

In this section, regarded as the most significant portion of this work, we first present the new protocol based on Schnorr where the response form is specifically one of $r = cu + x$ or $r = cu - x$, previously agreed on between the prover and the verifier. We then proceed to investigate and prove its core properties.

A. Modified Schnorr Protocol

Let $\mathbb{G} = \langle g \rangle$ be a cyclic group of prime order q and g a generator. The following sigma protocol lets the prover convince a verifier about the prover's knowledge of their secret key is $x \in \mathbb{Z}_q$, such that the corresponding public key is $h = g^x \in \mathbb{G}$. More precisely, the sigma protocol is a proof system for the following relation:

$$\mathrm{R_{ID}} = \{(g, h; x) : h = g^x\}.$$

The protocol for relation $\mathrm{R_{ID}}$ is described in Protocol 2 (see Figure 2) in the following, where previously $r = cu + x$ or $r = cu - x$ has been chosen, but use both in the exposition:

The commitment and the challenge steps of our protocol are exactly as Schnorr's. We changed the response of the prover that now is $r = cu \pm x \mod q$, which is send r to V in the final step. In the verification phase, the verifier accepts if $g^r = a^c \cdot h$ in the case of $r = cu + x$, or if $g^r \cdot h = a^c$ in the case of $r = cu - x$.

In the following, we analyse that our modified protocol holds same properties as the original scheme that are the main properties of a sigma protocol.

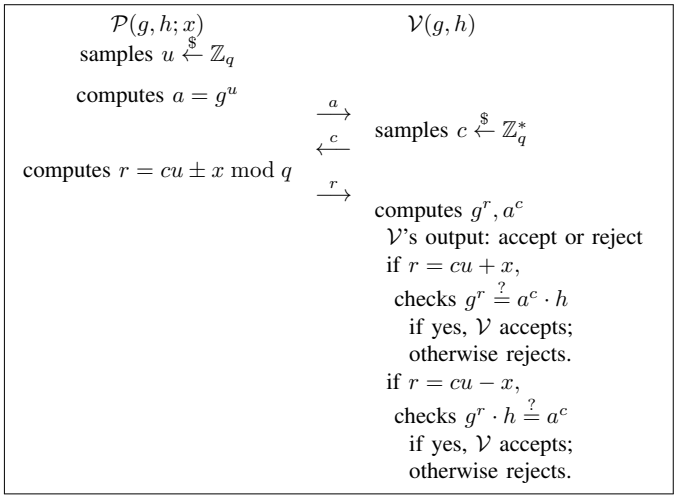

Figure 2. Protocol 2- Modified Schnorr Protocol for relation $\mathrm{R_{ID}}$.

1) Completeness: Let us ensure that an honest prover always passes the verifier's check.

$$g^r = g^{cu+x} = g^{cu} \cdot (g^x) = (g^u)^c \cdot (g^x) = a^c \cdot h.$$

Hence $g^r = a^c \cdot h$, So, the verifier will accept. Thus, completeness holds. For the case $r = cu - x$, the completeness property is established as follows.

$$g^r \cdot h = g^{cu-x} \cdot (g^x) = g^{cu} = (g^u)^c = a^c.$$

2) Special Soundness: To prove *soundness*, we must demonstrate that if an adversary can produce valid responses to two distinct challenges $c \neq c'$ for the same commitment a, then the secret x can be extracted.

Assume the adversary outputs a valid transcript (a, c, r). By rewinding the adversary with the same commitment a but a different challenge c', we obtain a second valid transcript (a, c', r'). Therefore, we have two valid transcripts: (a, c, r), (a, c', r') with $c \neq c'$, and both satisfying the verification equations:

$$g^r = a^c \cdot h \quad \text{and} \quad g^{r'} = a^{c'} \cdot h.$$

We compute

$$(g^r)^{c'} (g^{r'})^{-c} = (a^c h)^{c'} (a^{c'} h)^{-c} = h^{c'-c}. \tag{1}$$

Thus, the secret, which is the Discrete Logarithm of h in the basis g, can be extracted by computing:

$$x = (rc' - r'c) \cdot (c' - c)^{-1} \mod q.$$

This confirms that knowledge of valid responses to two distinct challenges allows extraction of the secret witness x, thereby proving the soundness of the protocol.

Note that we used the verification of the case that the response is, $r = cu + x$, to prove the above equality. In the case where the response is $r = cu - x$, the same relation can be employed to extract x.

3) Honest-Verifier Zero-Knowledge (HVZK): To prove HVZK, we show that the simulator chooses a random challenge c and a random response r, can simulate a valid transcript without knowing the secret x. Given the public parameters g, h, the simulator begins by selecting a random challenge $c \in \mathbb{Z}_q^*$ and a random response $r \in \mathbb{Z}_q$. Then, it computes the commitment $a \in \mathbb{G}$ so that the final transcript (a, c, r) satisfies the verification equation of the verifier.

Specifically, the simulator sets $a = (g^r h^{-1})^{c^{-1}}$ if $r = cu + x$, or $a = (g^r h)^{c^{-1}}$ if $r = cu - x$. This ensures that the verification equation $g^r = a^c \cdot h$ is valid, even if the simulator does not know x. Since both c and r are chosen independently and uniformly at random, and the commitment a is derived deterministically, the simulator output is computationally indistinguishable from that of an honest execution. Consequently, the protocol maintains the HVZK property, assuming the hardness of the discrete logarithm problem and that c is invertible modulo q.

B. Non-Interactive Schnorr and Its Modified Variant

The Fiat–Shamir transformation [3] allows converting interactive identification protocols, such as Schnorr's [16], into non-interactive zero-knowledge proofs (NIZKs). This transformation replaces the verifier's random challenge with a deterministic output derived from a cryptographic hash function, typically modeled as a random oracle. It enables the prover to independently compute the proof without interaction, making it suitable for applications such as digital signatures and proof of key possession.

In both the classical and modified Schnorr protocols, the prover first computes a commitment $a = g^u$, where $u \in \mathbb{Z}_q$ is randomly chosen. The challenge is then generated as $c = \mathcal{H}(a, m)$, where m represents the public data (e.g., a message or context), and $\mathcal{H}$ is a cryptographic hash function. The prover computes the response r using either the classical form $r = u + cx \mod q$ or the modified form $r = cu \pm x \mod q$, depending on the protocol variant.

The final proof consists of the pair (a, r). The verifier reconstructs c from the hash and checks the validity of the proof by verifying the corresponding group equation. This non-interactive approach preserves zero-knowledge and soundness under the random oracle model.

IV. Isogeny-Based ID Protocol Using Modified Schnorr

The isogeny-based identification protocol presented in [9] extends the CSI-FiSh framework by introducing structured public keys, which significantly improve efficiency and reduce the soundness error rate. Although it operates within the Hard Homogeneous Space (HHS) formed by the class group acting on supersingular elliptic curves, the protocol maintains a classic Σ-protocol format with a commitment, challenge, and response reminiscent of the Schnorr identification scheme.

Our modified Isogeny-Based ID Schnorr variant offers a conceptual change by redefining the prover response as $r = cu \pm x \mod q$, in contrast to the traditional $r = u + cx \mod q$. The resulting protocol has completeness, special soundness, and HVZK, making it suitable for efficient Fiat-Shamir-based signature schemes.

A. An Efficient ID Protocol based on Modified Schnorr

Let p be a large prime such that the supersingular elliptic curves over $\mathbb{F}_p$ form a well-connected isogeny graph. Denote by $\mathcal{E}$ the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves, and let $\mathrm{Cl}(\mathcal{O}) \cong \mathbb{Z}_N$ denote the class group of maximal order $\mathcal{O}$ in a quaternion algebra acting on $\mathcal{E}$ via isogenies.

The pair $(\mathbb{Z}_N, \mathcal{E})$ thus defines a *hard homogeneous space* [12] $(\mathcal{G}, \mathcal{X})$, equipped with a free and transitive action:

$$[a] \star E := \phi_a(E), \quad \text{for } a \in \mathbb{Z}_N,\ E \in \mathcal{E}.$$

Let $E_0 \in \mathcal{E}$ denote a publicly agreed base curve. We assume the existence of a publicly known *exceptional set* $C = \{c_0 = 0, c_1 = 1, \ldots, c_{k-1}\} \subset \mathbb{Z}_N$ such that every pairwise difference $c_i - c_j \in \mathbb{Z}_N^*$ is invertible. This assumption enables the construction of a sound Σ-protocol with extractability. Based on [9], we know that an Exceptional Set is defined as follows.

Definition. *Let $N \in \mathbb{Z}_{>0}$. A subset $C = \{c_0, c_1, \ldots, c_{k-1}\} \subset \mathbb{Z}_N$ is called an* exceptional set modulo N *if all pairwise differences are invertible, i.e., for all $i \neq j$, the element $c_i - c_j \in \mathbb{Z}_N^*$. This set guarantees that for any two distinct challenges $c, c' \in \mathbb{C}$, the value $c - c'$ is invertible modulo N, enabling efficient extraction in Σ-protocols.*

Remark. Given a target size k for an exceptional set and a modulus N, it is sufficient that the smallest prime factor q_1 of N satisfies $q_1 \geq k$. Under this condition, there exists an efficient algorithm, referred to as `XSGen`, capable of generating an exceptional set $C = \{c_0, c_1, \ldots, c_{k-1}\} \subseteq \mathbb{Z}_N$ of size k, in which all pairwise differences $c_i - c_j$ (for $i \neq j$) are invertible modulo N. If $q_1 < k$, one can still construct such a set by restricting the operation to a subgroup of $\mathbb{Z}_N$ in which smaller prime divisors are eliminated. This involves factoring out those small primes so that the minimal prime factor of the resulting subgroup is at least k. The only structural constraint imposed on N is that it must not be k-smooth, that is, N should not be composed entirely of prime factors less than k, which is typically a reasonable assumption for cryptographic applications involving large composite moduli [9].

B. Identification Protocol steps

In the first step for this protocol, we start with Key Generation. The prover samples $x \xleftarrow{\$} \mathbb{Z}_N$ as a secret key, and the public key is $E_x := [x] \star E_0$. The tuple $(E_0, E_x) \in \mathcal{E}^2$ is published, while x remains private to the prover. The identification protocol is a 3-move public-coin Σ-protocol defined by the protocol 3 (see Figure 3) as following steps. This Protocol ensures that the prover demonstrates knowledge of x consistent with the challenge and commitment.

Before detailing the protocol's primary characteristics, it is essential to first outline its underlying structure and associated benefits. Building on the proof techniques presented in [9], it can be readily shown that the set $\mathbf{A}$ in protocol 3 is well-defined and retains its essential properties. For any A_i, a corresponding proof, referred to as a pre-proof, must be

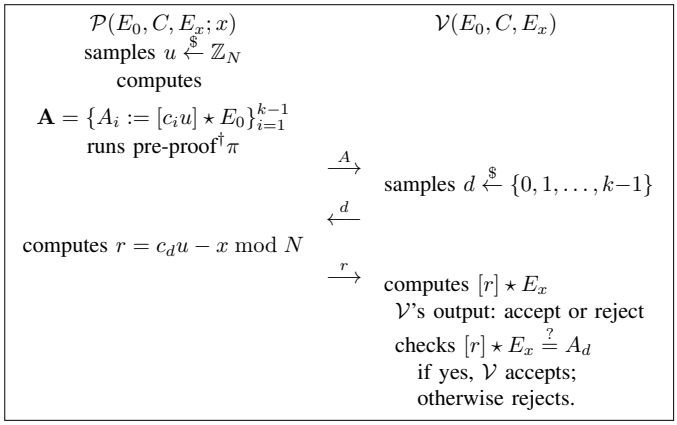

Figure 3. Protocol 3- Isogeny Schnorr Protocol for relation $\mathrm{R_{ID}}$.

provided. This pre-proof follows the same approach as the proof techniques in [9], concretely Theorems 5.1 and 5.2 in [9], as well as remark (IV-A).

It is important to note that the protocol presented in [9] operates under idealized assumptions—namely, that all components, including randomness and network integrity, function flawlessly. Under such conditions, any deviation—such as inaccurate randomness or communication failures— during pre-proof can compromise the witness and, consequently, the security of the main protocol by causing information leakage from x.

On the other hand, generating all $E_i = [c_i x]E_0$ in [9] requires invoking the aforementioned theorems and consistently relying on the witness x during the pre-proof construction. However, in the modified isogeny-based Schnorr protocol, this reliance is mitigated by replacing x with u, thereby reducing direct dependence on the witness. In contrast, our modified Schnorr protocol exhibits greater resilience, enabling corrective measures to be taken without undermining its core functionality. More specifically, in the modified isogeny-based Schnorr protocol, it is sufficient to halt execution, select a new value u, and restart the pre-proof and protocol—without affecting the witness. This property significantly enhances the protocol's reliability under failure scenarios or adversarial conditions.

1) Completeness: We know that if the prover follows the protocol honestly, the verifier accepts with probability 1. For our modified Schnorr protocol, given $A_d = [c_d u] \star E_0$, $E_x = [x] \star E_0$, and $r = c_d u - x$, we compute:

$$[r] \star E_x = [c_d u - x] \star [x]E_0 = [c_d u] \star E_0 = A_d.$$

Therefore, the verifier check passes.

2) Special Soundness: We demonstrate that given two valid transcripts for the same commitment and distinct challenges, the prover's secret x can be recovered efficiently. Given two accepting transcripts (A, d, r) and (A, d', r') with $d \neq d'$ and a known set $C = \{c_0 = 0, c_1 = 1, c_2, \cdots, c_{k-1}\}$, we have:

$$[r]\star E_x = A_d = [c_d u]\star E_0 \quad \text{and} \quad [r']\star E_x = A_{d'} = [c_{d'} u]\star E_0$$

note that we can extract c_d and $c_{d'}$ by having d, d' and set C. From the verification equation, one can conclude that $[r]E_x = A_d$ and $[r']E_x = A_{d'}$, and from the pre-proof (or trusted) commitment we know that $A_i = [c_i u]E_0$ for $i = 1, \cdots, k-1$. These imply that we have $[r][x]E_0 = [c_d u]E_0$ and $[r'][x]E_0 = [c_{d'} u]E_0$, so:

$$[r + x]E_0 = [c_d u]E_0 \quad \text{and} \quad [r' + x]E_0 = [c_{d'} u]E_0$$

These imply that:

$$[c_{d'}(r+x)]E_0 = [c_{d'} c_d u]E_0 \quad \text{and} \quad [c_d(r'+x)]E_0 = [c_d c_{d'} u]E_0$$

Since the right part of relations are the same we have:

$$[c_{d'}(r + x)]E_0 = [c_d(r' + x)]E_0$$

It implies that

$$c_{d'} r + c_{d'} x = c_d r' + c_d x \;\Rightarrow$$

$$c_{d'} r - c_d r' = c_d x - c_{d'} x = (c_d - c_{d'})x.$$

Since $d \neq d'$ so $c_d \neq c_{d'}$. Therefore, we can divide both sides to $c_d - c_{d'} \in \mathbb{Z}_N^*$ and then we compute:

$$x = \frac{c_{d'} r - c_d r'}{c_d - c_{d'}} \mod N.$$

This proves extractability and thus special soundness.

3) Honest-Verifier Zero-Knowledge (HVZK): To prove HVZK, we construct a simulator that produces a valid-looking transcript (A, c, r) without knowing the secret key $x \in \mathbb{Z}_N$. Consider that the simulator has a sequence of images $\{E_i = [c_i x]E_0\}$ according to $(c_0, \ldots, c_{k-1})$-Vectorization Problem with Auxiliary Inputs. The simulator selects $u \in \mathbb{Z}_N$ and samples a challenge $d \in \{0, \ldots, k-1\}$, both uniformly at random and set $E_x = [c_d x]E_0 = E_d$. Given random u and sequence $\{E_i = [c_i x]E_0\}$, the simulator calculates $A = \{A_i := [c_i u] \star E_i = [c_i u + c_i x] \star E_0\}_{i=1}^{k-1}$ and sets the response as $r = c_d u$. The resulting transcript (A, d, r) satisfies the verifier check by construction $[r] \star E_x = A_d$ and is identical to a real transcript, thus establishing the HVZK property.

Remark. In [9], the pre-proof phase involves verifying the public set $E_i = [c_i x]E_0$, directly involving the secret x. In contrast, our protocol verifies $E_i = [c_i u]E_0$, where u is a random value unrelated to the secret.

If, during the pre-proof phase in [9], the randomness used in the commitment has insufficient entropy, the verifier could potentially recover the secret x from the response. In our protocol, even if such a weakness occurs, only the random value u could be exposed, without compromising x. In that case, the prover can simply discard u and any related computations, select a fresh random value, and rerun the pre-proof securely.

V. Conclusion and future work

We have introduced a modified version of the Schnorr Sigma protocol, redefining the prover's response to reduce its dependency on the secret witness x. This seemingly minor algebraic change leads to meaningful improvements in both the structural and practical aspects of the protocol. Through a formal analysis, we have demonstrated that the modified scheme retains its fundamental security properties—including soundness and zero-knowledge—while offering enhanced robustness and flexibility.

Applying this construction in the isogeny-based setting, we addressed key limitations of an existing identification protocol, particularly those arising from its idealized assumptions and its heavy reliance on the witness during pre-proof generation. By shifting this dependency from x to a fresh random value u, our approach enables safer recovery from randomness failures or communication errors, without compromising the security of the secret key. This resilience to faults and adversarial interruptions marks a significant improvement in the protocol's practicality and reliability for real-world deployment. Moreover, our modification opens the door to applying the MPC-in-the-Head technique, offering potential advantages in efficiency and security. We leave the exploration and formal development of this direction to future work.

Our work illustrates how carefully rethinking classical cryptographic constructions can lead to more robust solutions in post-quantum settings, such as isogeny-based cryptography, and opens the door to further exploration of protocol modifications that enhance security under realistic conditions.

Acknowledgments

This work was supported by the Spanish Ministry of Science and Innovation through the PID2021-125962OB-C31 "SECURING" project. Additional funding was provided by the ARTEMISA International Chair of Cybersecurity (C057/23) and the DANGER Strategic Project of Cybersecurity (C062/23), both funded by the Spanish National Institute of Cybersecurity through the European Union — NextGenerationEU and the Recovery, Transformation, and Resilience Plan. Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them. Zaira Pindado is supported by ERC grant (HomE, 101043467).

References

[1] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of Cryptology*, vol. 4, no. 3, pp. 161–174, 1991. DOI: 10.1007/BF00196725.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. DOI: 10.1109/TIT.1976.1055638.

[3] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Lecture Notes in Computer Science*, vol. 263, pp. 186–194, 1987. DOI: 10.1007/3-540-47721-7_12.

[4] G. Fuchsbauer, A. Plouviez, and Y. Seurin, "Blind schnorr signatures and signed elgamal encryption in the algebraic group model," *Lecture Notes in Computer Science*, vol. 12106, pp. 63–95, 2020. DOI: 10.1007/978-3-030-45724-2_3.

[5] R. Bacho, J. Loss, G. Stern, and B. Wagner, *Harts: High-threshold, adaptively secure, and robust threshold schnorr signatures*, To appear in: Advances in Cryptology – ASIACRYPT 2024, Lecture Notes in Computer Science, vol 15486, Springer, Singapore. Edited by KM. Chung and Y. Sasaki, 2025. [Online]. Available: https://doi.org/10.1007/978-981-96-0891-1_4.

[6] M. Fukumitsu and S. Hasegawa, "On multi-user security of schnorr signature in algebraic group model," *Proceedings of the Tenth International Symposium on Computing and Networking Workshops (CANDARW)*, pp. 295–301, 2022. DOI: 10.1109/CANDARW57323.2022.00014.

[7] G. Fuchsbauer and M. Wolf, "Concurrently secure blind schnorr signatures," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, 2024, pp. 124–160.

[8] S. D. Galbraith, C. Petit, and J. Silva, *Identification protocols and signature schemes based on supersingular isogeny problems*, Journal of Cryptology, Volume 33, Pages 130–175, Springer, https://doi.org/10.1007/s00145-019-09316-0, 2020. [Online]. Available: https://doi.org/10.1007/s00145-019-09316-0.

[9] K. Baghery, D. Cozzo, and R. Pedersen, "An isogeny-based id protocol using structured public keys," in *IMA international conference on cryptography and coding*, Springer, 2021, pp. 179–197. DOI: 10.1007/978-3-030-92641-0_9.

[10] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, "Csidh: An efficient post-quantum commutative group action," in *Advances in Cryptology – ASIACRYPT 2018*, ser. Lecture Notes in Computer Science, vol. 11274, Springer, 2018, pp. 395–427. DOI: 10.1007/978-3-030-03332-3_15.

[11] W. Beullens, T. Kleinjung, and F. Vercauteren, "CSI-FiSh: Efficient isogeny-based signatures through class group computations," in *Advances in Cryptology – ASIACRYPT 2019, Part I*, S. D. Galbraith and S. Moriai, Eds., ser. Lecture Notes in Computer Science, Presented at ASIACRYPT 2019, vol. 11921, Kobe, Japan: Springer, Heidelberg, Germany, Dec. 2019, pp. 227–247. DOI: 10.1007/978-3-030-34578-5_9.

[12] J.-M. Couveignes, *Hard homogeneous spaces*, Cryptology ePrint Archive, Report 2006/291, Preprint, Jul. 2006. [Online]. Available: https://eprint.iacr.org/2006/291.

[13] A. Rostovtsev and A. Stolbunov, "Public-key cryptosystem based on isogenies," *Cryptology ePrint Archive*, 2006.

[14] J. H. Cheon, "Discrete logarithm problems with auxiliary inputs," *Journal of Cryptology*, vol. 23, no. 3, pp. 457–476, Jul. 2010. DOI: 10.1007/s00145-009-9047-0.

[15] T. Kim, "Multiple discrete logarithm problems with auxiliary inputs," in *Advances in Cryptology – ASIACRYPT 2015, Part I*, T. Iwata and J. H. Cheon, Eds., ser. Lecture Notes in Computer Science, vol. 9452, Auckland, New Zealand: Springer, Nov. 2015, pp. 174–188. DOI: 10.1007/978-3-662-48797-6_8.

[16] F. Hao, *Schnorr non-interactive zero-knowledge proof*, RFC 8235, Internet Engineering Task Force (IETF), Informational, Sep. 2017. DOI: 10.17487/RFC8235. [Online]. Available: https://www.rfc-editor.org/info/rfc8235.