Zero-Knowledge Proof and Group Signature Scheme Based on Supersingular Isogeny (Post-print)

Authors: Zhao Xingbo, Li Mengdong, Wang Ying, Zhu Yilin

Date: 2022-05-10T11:22:58+00:00

Abstract

Bullens et al. left an open problem in CSI-Fish, namely designing an identification protocol that allows the system challenge space to be #1;, rather than a small set #1;. This paper proposes a zero-knowledge proof scheme based on supersingular isogenies. The scheme treats the challenge C as an isogeny, thereby solving this problem and achieving a smaller soundness error as well as shorter public key length. The scheme can also be transformed into a non-interactive zero-knowledge proof via the Fiat-Shamir transform, consequently enabling the realization of supersingular isogeny-based signature schemes and group signature schemes in the quantum random oracle model. Moreover, this paper analyzes the security and correctness of the scheme.

Full Text

Zero-Knowledge Proof and Group Signature Scheme Based on Supersingular Isogeny

Zhao Xingbo, Li Mengdong†, Wang Ying, Zhu Yilin
(Dept. of Cryptology Science & Technology, Beijing Electronic Science & Technology Institute, Beijing 100070, China)

Abstract: Bullens et al. left an open problem in CSI-FiSh to devise an identification protocol that allows the challenge set to be the entire class group rather than a small subset. This paper proposes a zero-knowledge proof scheme based on supersingular isogeny that addresses this problem by treating the challenge C as an isogeny itself, thereby achieving a smaller soundness error and reduced public key length. The scheme can be transformed into a non-interactive zero-knowledge proof via the Fiat-Shamir transform, enabling the construction of supersingular isogeny-based signature and group signature schemes under the

quantum random oracle model. This paper analyzes the security and correctness of these proposed schemes.

Key words: zero-knowledge proof; supersingular; isogeny; group signature

0 Introduction

Isogeny-based cryptography represents a promising and valuable candidate for post-quantum cryptography. An isogeny is a morphism between elliptic curves that preserves the base point and constitutes a group homomorphism [1]. While early isogeny-based cryptographic systems primarily studied ordinary curves [2,3], the existence of subexponential-time quantum algorithms for the ordinary curve isogeny problem led to a shift toward supersingular curves, for which Biasse et al. [4] established that quantum algorithms require exponential time. Consequently, most contemporary isogeny-based schemes operate on supersingular elliptic curves.

Current constructions of isogeny-based signatures rely fundamentally on two isogeny problems: the Computational Supersingular Isogeny (CSSI) problem [5] and the Group Action Inverse Problem (GAIP) [6]. Most isogeny-based signatures combine these problems with the Fiat-Shamir transform [7,8]. Signature schemes based on CSSI [9,10] produce signatures of at least 12KB even in their most optimized variants [10]. In contrast, De Feo and Galbraith proposed SeaSign [11], which leverages GAIP and employs the Fiat-Shamir-with-aborts technique to achieve remarkably compact signatures under 1KB at the 128-bit security level. More recently, Beullens et al. [12] improved upon SeaSign by computing the ideal class group, yielding the first practical isogeny-based signature scheme, CSI-FiSh. This scheme enables uniform sampling from the ideal class group with canonical representation, requiring only 390 milliseconds for signing or verification while producing 263-byte signatures. Thus, CSI-FiSh represents a highly practical isogeny-based signature scheme.

Through analysis of CSI-FiSh and other supersingular isogeny-based signature schemes, this paper proposes a zero-knowledge proof system that improves upon the proof system in CSI-FiSh. Our scheme resolves the open problem posed in CSI-FiSh by expanding the challenge space from a small set to the order N of the ideal class group in CSIDH-512. Compared to CSI-FiSh, our scheme achieves a smaller soundness error and shorter public key length, requiring only a single elliptic curve as the public key. Building upon this proof system, we construct both a supersingular isogeny-based signature scheme and a group signature scheme, providing security proofs for the signature scheme.

1.1 Supersingular Elliptic Curves and Isogenies

An isogeny $\varphi : E \to E_1$ between elliptic curves is a morphism that is also a group homomorphism. Tate [13] established that two elliptic curves E, E_1 over a finite field are isogenous if and only if $\#E(\mathbb{F}_q) = \#E_1(\mathbb{F}_q)$. The endomorphism

set $\mathrm{End}(E)$, equipped with point addition and function composition, forms a ring structure [14]. In $\mathbb{F}_p$, the Frobenius endomorphism π satisfies the characteristic equation $\pi^2 - t\pi + q = 0$, where t is the Frobenius trace. A curve E is supersingular if and only if $t = 0$.

The $\mathbb{F}_p$-rational endomorphism ring $\mathrm{End}_p(E)$ always contains the subring $\mathbb{Z}[\pi]$. Let $\mathcal{O}$ be an order in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-p})$. The ideal class group $\mathrm{cl}(\mathcal{O})$ acts freely and transitively on the set of supersingular elliptic curves E defined over $\mathbb{F}_p$ with $\mathrm{End}_p(E) \cong \mathcal{O}$. For any ideal $\mathfrak{a} \in \mathrm{cl}(\mathcal{O})$, there exists a Frobenius map such that $\mathfrak{a} \star E$ represents this action [15]. Recently, this action $\star$ has been used to design several cryptographic primitives—CSIDH and its derived signature schemes SeaSign and CSI-FiSh—whose security relies on the Group Action Inverse Problem, defined as follows:

Problem 1 (Group Action Inverse Problem: GAIP). Given two curves E, E' with $\mathrm{End}_p(E) \cong \mathrm{End}_p(E') \cong \mathcal{O}$, find an ideal $\mathfrak{a} \subset \mathcal{O}$ such that $E' = \mathfrak{a} \star E$.

1.2 CSI-FiSh

Beullens et al. proposed an efficient signature scheme based on the hardness of CSIDH-512. For the prime p selected in CSIDH for the CSIDH-512 parameter set, Beullens et al. determined that the relevant class group of the endomorphism ring is cyclic, generated by g with order $N = 3371407185159360429529586774429358488931599414504681995853008278745587322049091 74$. For any ideal $\mathfrak{a} \in \mathrm{cl}(\mathcal{O})$, one can write $\mathfrak{a} = g^a$ where $a \in \mathbb{Z}_N$. As long as the CSIDH-512 parameter set is used, anyone can uniformly sample class group elements and obtain a canonical representation. For a supersingular elliptic curve E_0 isogenous to E, we simplify the notation $\mathfrak{a} \star E_0$ to $[a]E_0$.

1.3 Zero-Knowledge Proof

A zero-knowledge proof (ZKP) is a two-party protocol between a prover and a verifier where the prover demonstrates knowledge of secret information without revealing anything beyond the validity of the statement itself. For a language $L \subseteq \{0,1\}^*$ where each string x is accompanied by a witness w such that $(x, w) \in R$, we define a Σ-protocol following [16]:

Definition 1. A Σ-protocol for a relation R with challenge set C is a three-move protocol between prover P and probabilistic polynomial-time (PPT) verifier V with the following properties:

- **Three-move form:** The protocol proceeds as: (1) Prover P computes commitment t and sends it to verifier V; (2) Verifier V selects challenge $c \in C$ and sends it to P; (3) Prover sends response r to verifier, who finally accepts or rejects based on the transcript (t, c, r).
- **Completeness:** For honest prover P and verifier V, when $(x, w) \in R$, the verifier accepts with probability at least $1 - \alpha$.

- **Special Soundness:** There exists a PPT knowledge extractor K that, given two accepting transcripts (t, c, r) and (t, c', r') with $c \neq c'$, outputs w' such that $(x, w') \in R$. The soundness error is $\delta = 1/|C|$.
- **Honest-Verifier Zero Knowledge (HVZK):** There exists a PPT simulator that, on input $x \in L$ and $c \in C$, produces transcripts indistinguishable from real protocol executions [16].

A 3-round special-sound HVZK proof protocol can be converted to a non-interactive zero-knowledge proof via the Fiat-Shamir transform.

Definition 2. A canonical identification scheme $ID = (K, P, V, c)$ consists of: K is a PPT key generation algorithm outputting (pk, sk); P is a PPT algorithm that, on input sk, outputs a message m; $c \geq 1$ is the integer bit length of challenges; and V is a deterministic polynomial-time verification algorithm outputting 0 or 1 [17].

1.4 Signatures

A signature scheme $S = (\text{KeyGen}, \text{Sign}, \text{Verify})$ consists of three algorithms. **Definition 3 (EUF-CMA Security).** A signature scheme S is existentially unforgeable under chosen-message attacks (EUF-CMA) if for all PPT adversaries A, $\text{Adv}_{A,S}^{\text{EUF-CMA}}(1^\lambda) = \Pr[A \text{ wins}] = \text{negl}(\lambda)$.

Theorem 1 [10]. Let R with generation algorithm K be a hard relation, and let (P, V) be the prover and verifier in a Σ-protocol for R with c-bit challenges for some integer $c \geq 1$. If the Σ-protocol is complete, special-sound, and honest-verifier zero-knowledge, then the derived identification scheme is secure against passive attacks.

Theorem 2 [10]. Let ID be a canonical identification scheme secure against passive attacks. Let S be the signature scheme derived from ID via the Fiat-Shamir transform. Then S is existentially unforgeable under chosen-message attacks in the random oracle model.

1.5 Group Signatures

A group signature scheme comprises five polynomial-time algorithms:

- **GSetup:** Takes a security parameter and generates system public parameters and group public key.
- **GJoin:** An interactive protocol between user and group manager; if successful, the user becomes a valid group member and obtains a public/private key pair.
- **GSign:** For a given message m, the signature is jointly produced by the manager and group member.
- **GVerify:** Verifies signatures using the group public key and message m.
- **GTrace:** Enables the group manager to identify the actual signer of message m.

Security properties required for group signatures include: (1) correctness, (2) unforgeability, (3) anonymity, (4) traceability, and (5) collusion resistance.

2.1 Zero-Knowledge Proof Identification Protocol

For the CSIDH-512 parameter set, CSI-FiSh establishes that its ideal class group is cyclic with known order N and generator $\mathfrak{g}$. Using CSIDH-512, anyone can uniformly sample class group elements with unique representation. We describe our new supersingular isogeny-based identification protocol (Figure 1), which achieves a smaller soundness error and reduced public key length compared to CSI-FiSh.

Protocol Setup: Select a large prime $p = 4\prod_{i=1}^{l} \ell_i - 1$ where ℓ_i are small distinct odd primes. Given the set $\{\ell_i\}_{i=1}^{l}$, the ideal class group $\mathrm{cl}(\mathcal{O})$, and a supersingular elliptic curve E_0 over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$, the prover and verifier execute the following Σ-protocol (Figure 2) to prove knowledge of secret a:

- **Key Generation:** Select a random isogeny $[a] : E_0 \to E_1$. The public key is $pk = E_1$ and the secret key is $sk = a$.
- **Commitment:** Prover randomly selects $b \in_R \mathbb{Z}_N$, computes $E_b = [b]E_0$, and sends E_b to verifier.
- **Challenge:** Verifier checks $E_b \neq E_1$, then randomly selects challenge $c \in_R \mathbb{Z}_N$ and sends it to prover.
- **Response:** Prover computes $r = c + b - a \bmod N$ and sends r to verifier.
- **Verification:** Verifier checks whether $[r]E_0 = [c]E_1 + E_b$; if equal, accepts; otherwise rejects.

2.2 Security Analysis

Theorem 3. The isogeny-based identification protocol is a complete and secure Σ-protocol satisfying completeness, special soundness, and honest-verifier zero-knowledge.

Proof. **Completeness:** Assuming an honest prover who knows secret a, the verifier always accepts honestly generated proofs because $[r]E_0 = [c+b-a]E_0 = [c]E_1 + E_b$.

Special Soundness: Given two valid proofs with distinct challenges (t, c, r) and (t, c', r') where $c \neq c'$, we have $[r]E_0 = [c]E_1 + E_b$ and $[r']E_0 = [c']E_1 + E_b$. Subtracting yields $[r - r']E_0 = [c - c']E_1$, providing a solution to the GAIP problem. The cheating prover cannot succeed unless it correctly guesses challenge c. With challenge space $\mathbb{Z}_N$ containing N elements, the protocol achieves soundness error $1/N$.

Honest-Verifier Zero Knowledge: To simulate a proof, the simulator randomly samples $c, r \in_R \mathbb{Z}_N$ and computes $E_b = [r]E_0 - [c]E_1$, outputting transcript (E_b, c, r). By the decisional GAIP assumption, simulated proofs are indis-

tinguishable from real protocol executions where the challenge equals c, as both produce uniformly random r and E_b values as responses. Thus, the protocol is honest-verifier zero-knowledge.

2.3 Signature Scheme

Algorithms 1-3 describe our isogeny-based signature scheme, whose security relies on the GAIP hardness assumption. The scheme applies the Fiat-Shamir transform to the zero-knowledge proof protocol from Section 2.1, replacing challenge c with a hash of the ephemeral key E and message m, i.e., $c = H(E, m)$. Signature σ consists of (r, E), and the verifier computes $c = H(E, m)$. The detailed scheme follows:

Algorithm 1 KeyGen
Input: Initial curve E_0 and ideal class group order N
Output: Public/private key pair (pk, sk)
1. $sk \leftarrow a \in_R \mathbb{Z}_N$
2. $pk \leftarrow E_1 = [a]E_0$
3. return (pk, sk)

Algorithm 2 Sign
Input: Message m and private key sk
Output: Signature σ
1. $b \leftarrow_R \mathbb{Z}_N$
2. $E \leftarrow [b]E_0$
3. $c \leftarrow H(E, m)$
4. $r \leftarrow c + b - a \bmod N$
5. $\sigma \leftarrow (r, E)$
6. return σ

Algorithm 3 Verify
Input: Message m, public key pk, signature σ
Output: Valid or Invalid
1. Compute $c' \leftarrow H(E, m)$
2. if $[r]E_0 = [c']E_1 + E$ then
3. return Valid
4. else
5. return Invalid

2.4 Security Analysis

Theorem 4. In the random oracle model, the supersingular isogeny-based signature scheme is existentially unforgeable under chosen-message attacks (EUF-CMA).

Proof. As shown in Section 2.2, the identification scheme (Σ-protocol) is special-sound and honest-verifier zero-knowledge. By Theorem 1, this implies the identification scheme is secure against impersonation under passive attacks. Applying

Theorem 2, the resulting signature scheme is EUF-CMA secure in the random oracle model.

2.5 Comparative Analysis

The basic identification protocol in CSI-FiSh operates as follows: To prove knowledge of a group element $\mathfrak{a}$ such that $E_1 = \mathfrak{a} \star E_0$, the prover randomly selects $b \in_R \mathbb{Z}_N$, computes $E_b = [b]E_0$, and sends E_b to the verifier. The verifier randomly selects a bit $c \in \{0, 1\}$. If $c = 0$, the prover responds with $r = b$ and the verifier checks $[r]E_0 = E_b$; if $c = 1$, the prover responds with $r = b - a$ and the verifier checks whether E equals $[r]E_1$. This protocol' s challenge space is binary ($c \in \{0, 1\}$) with public key length of one curve.

To reduce soundness error, CSI-FiSh expanded the challenge space at the cost of increased public key size. Their approach selects a positive integer S where the secret key is an $(S-1)$-dimensional vector $(a_1, \ldots, a_{S-1})$ appearing in the public key list as $([a_1]E_0, \ldots, [a_{S-1}]E_0)$. The prover must prove knowledge of a secret $s \in \mathbb{Z}_N$ and that $[s]E_0$ appears among the listed curve pairs. The verifier samples challenges c from $\{-S+1, \ldots, S-1\}$, and the prover responds with $r = b - cs \bmod N$. CSI-FiSh achieves $1/(2S-1)$ soundness error with public key length $S-1$ curves.

Our scheme treats challenge c as an isogeny, enabling combination of ephemeral key b and challenge c into $[b+c]E_0$ without encountering the non-linear group action issues present in ring-based constructions. This allows c to be randomly selected from $\mathbb{Z}_N$, expanding the challenge space to the class group order N and achieving $1/N$ soundness error. The trade-off is requiring one additional isogeny computation $[c]E_1$, increasing computational overhead.

Our scheme' s public key length is one elliptic curve. Tables 1 and 2 compare our scheme with CSI-FiSh.

Table 1. Comparison of Identification Protocols

Scheme	Public Key Length	Challenge Space	Soundness Error	Isogeny Operations
CSI-FiSh Basic	1 curve	$\{0, 1\}$	$1/2$	1
CSI-FiSh Adapted	$S-1$ curves	$\{-S+1, S-1\}$	$1/(2S-1)$	1
Our Scheme	1 curve	$\mathbb{Z}_N$	$1/N$	2

Table 2. Comparison of Signature Schemes

Scheme	Public Key Length	Signature Size	Security Assumption
CSI-FiSh Signature	$S-1$ curves	263 bytes	GAIP
Our Signature Scheme	1 curve	$\approx$ 300 bytes	GAIP

3.1 Group Signature Scheme Based on Supersingular Isogeny

In group signatures, group members must generate a non-interactive zero-knowledge proof (NIZK) demonstrating possession of a valid key pair. The signature comprises a ciphertext and proof (with the message embedded in the proof). Verification simply checks proof validity. We present our group signature scheme, which follows the stateful list approach of [19] but replaces bilinear map-based authentication with our isogeny-based ZK protocol. The isogeny-based approach offers short keys and quantum resistance at the cost of increased computation.

Our scheme involves four entities: a public key list PKL, group manager GM, group members U_i, and a trusted timestamp authority. The public key list displays current member information $(ID_i, E_i, \text{startTime}, \text{endTime})$. GM handles member enrollment, signature tracing, and real-time list updates, broadcasting the latest PKL to all members. The timestamp authority provides timestamp services, while group members U_i generate group signatures.

Group Signature Generation: To sign message m, member U_i collaborates with GM. U_i randomly selects $b_i \in_R \mathbb{Z}_N$, computes $E_{b_i} = [b_i]E_0$, obtains current time $Time$, then computes $s_i = H_2(E_{b_i} \| E_i \| m \| Time)$ and $t_i = b_i + s_i \cdot x_i \bmod N$. U_i sends $(ID_i, E_i, E_{b_i}, s_i, t_i, Time)$ to GM.

Table 3. Public Key List PKL

Index	Group Member	Member Public Key
1	U_1	E_1
...	...	...

Note: GM maintains PKL in real-time, broadcasting updates upon member enrollment or revocation and sending PKL to members as certificates.

Upon receiving $(ID_i, E_i, E_{b_i}, s_i, t_i, Time)$, GM first verifies $Time$' s validity, then checks PKL for ID_i and validates $[t_i]E_0 = [s_i]E_i + E_{b_i}$. If valid, GM computes $E_{v_i} = [t_i]E_{GM}$ and stores $(ID_i, E_{v_i}, s_i, t_i)$ in a tracking list (Table 4).

Table 4. Tracking List L_{Track}

Index	Group Member	Tracing Information
1	U_1	$(ID_1, E_{v_1}, s_1, t_1)$
...	...	...

Verification: Upon receiving signature $\sigma' = (ID_i, E_{v_i}, s_i, t_i)$, the verifier checks $[t_i]E_{GM} = E_{v_i}$. If valid, σ' is accepted as a group signature for m; otherwise, it is rejected.

Tracing: When disputes arise, GM queries L_{Track} using E_{v_i} to identify the signer U_i and provide evidence of signature generation.

3.2 Correctness Analysis

Our scheme comprises five phases: system setup, member enrollment, signing, verification, and tracing.

1) System Setup: Select prime $p = 4\prod_{i=1}^{l} \ell_i - 1$ with small odd primes ℓ_i, ideal class group $\mathrm{cl}(\mathcal{O})$, and supersingular elliptic curve E_0 over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$. For GM: select $x \in_R \mathbb{Z}_N$ as private key, compute $E_{GM} = [x]E_0$. The group public key is $gpk = \{E_0, E_{GM}, p, N, H_1, H_2\}$.

2) Member Enrollment: To join, member U_i selects $a_i \in_R \mathbb{Z}_N$, computes $E_i = [a_i]E_0$, and sends ID_i to GM. GM verifies $[a_i]E_0 = E_i$, computes $h_i = H_1(ID_i)$ and $x_i = h_i + x \bmod N$, then sends (x_i, E_i) to U_i. U_i verifies $[x_i]E_0 = [h_i]E_{GM} + E_i$, setting $pk_i = E_i$ and $sk_i = a_i$.

3) Group Signing: To sign message m, U_i selects $b_i \in_R \mathbb{Z}_N$, computes $E_{b_i} = [b_i]E_0$, $s_i = H_2(E_{b_i} \| E_i \| m \| Time)$, and $t_i = b_i + s_i \cdot x_i \bmod N$, then sends $(ID_i, E_i, E_{b_i}, s_i, t_i, Time)$ to GM. GM verifies $Time$' s validity, checks PKL for ID_i, and validates $[t_i]E_0 = [s_i]E_i + E_{b_i}$. If valid, GM computes $E_{v_i} = [t_i]E_{GM}$ and stores $(ID_i, E_{v_i}, s_i, t_i)$.

4) Verification Correctness: To verify $\sigma' = (ID_i, E_{v_i}, s_i, t_i)$, check:

$$[t_i]E_{GM} = [t_i]([x]E_0) = [t_i \cdot x]E_0 = [s_i \cdot x_i \cdot x + b_i \cdot x]E_0 = [s_i]E_i + E_{b_i} = E_{v_i}$$

This demonstrates GM' s participation in signature generation.

5) Tracing Correctness: GM searches L_{Track} for $(ID_i, E_{v_i}, s_i, t_i)$ to identify the signer.

3.3 Security Analysis

Theorem 5 (Anonymity). For any PPT adversary A, our scheme is anonymous in the random oracle model.

Proof. We define a game between challenger C and adversary A:

Game G_0: C generates system parameters, selects $b \in \{0,1\}$, and provides A with oracle access. A outputs a guess b'. The advantage is $\mathrm{Adv}_A^{\mathrm{anon}} = |\Pr[b' = b] - 1/2|$.

Game G_1: Identical to G_0 except C uses U_0' s private key for signing when $b = 0$ and U_1' s private key when $b = 1$. By the decisional CSIDH assumption, signatures generated under either key are indistinguishable, making A' s advantage negligible. Therefore, our group signature scheme satisfies anonymity in the random oracle model.

Theorem 6 (Unforgeability). If GAIP is hard, our supersingular isogeny-based group signature is unforgeable in the random oracle model.

Proof. Assume adversary A forges a signature with non-negligible probability ϵ. We construct a challenger C that solves GAIP. C sets up the system, maintains hash lists L_1, L_2, and responds to A' s queries. When A produces a forged signature $\sigma^* = (ID_i^*, E_{v_i}^*, s_i^*, t_i^*)$ for message m^*, C extracts the underlying isogeny relationship. If A never queried ID_i^*' s private key nor requested a signature on m^*, then with probability ϵ, C can compute an ideal $\mathfrak{e}$ satisfying $E_{v_i}^* = \mathfrak{e} \star E_0$, solving GAIP. Thus, unforgeability reduces to GAIP hardness.

Theorem 7 (Collusion Resistance). For any PPT adversary A, our scheme is collusion-resistant in the random oracle model.

Proof. Collusion resistance ensures that even cooperating members cannot produce untraceable signatures. In our enrollment algorithm, GM stores member identities in PKL and verifies legitimacy before assisting in signature generation. Based on GAIP hardness, GM cannot learn members' private keys, and members cannot derive each other' s keys. All private keys remain confidential and independent, preventing collusion.

Theorem 8 (Traceability). For any PPT adversary A, our scheme is traceable in the random oracle model.

Proof. Traceability requires GM to identify signers by opening signatures. Our signatures are jointly produced by GM and members. During signing, GM verifies U_i' s identity against PKL and stores $(ID_i, E_{v_i}, s_i, t_i)$ in L_{Track}. Thus, GM can trace any signature by querying L_{Track}. Even if A compromises members and obtains GM' s public key, without GM' s private key x, A cannot forge untraceable signatures since valid signatures require GM' s participation and L_{Track} records all signing events.

3.4 Performance Analysis

We compare our group signature scheme with [19], which uses bilinear maps for member authentication while ours employs isogeny-based ZK authentication. Both schemes share advantages: (1) constant signature length independent of group size, suitable for large groups; (2) dynamic member management via PKL enabling efficient enrollment/revocation by modifying end times.

Key differences: (1) Our scheme relies on GAIP, preventing revoked members from deriving others' keys; (2) Members generate their own private keys, resisting framing attacks by GM; (3) Our scheme leverages supersingular isogeny properties—short keys and quantum resistance—but requires more computation time.

4 Conclusion

Building upon Bullens et al.' s CSI-FiSh, we propose a novel zero-knowledge proof scheme that, with a single public key, expands the challenge space to the class group order N, achieving stronger soundness. Through the Fiat-Shamir transform, we obtain supersingular isogeny-based signature and group signature schemes secure in the quantum random oracle model, with provable security for our signature scheme.

References

[1] Silverman J H. The arithmetic of elliptic curves [M]. Springer Science & Business Media, 2009.
[2] Rostovtsev A, Stolbunov A. Public-key cryptosystem based on isogenies [J]. Cryptology ePrint Archive, 2006/145.
[3] Childs A, Jao D, Soukharev V. Constructing elliptic curve isogenies in quantum subexponential time [J]. Journal of Mathematical Cryptology, 2014, 8 (1): 1-29.
[4] Biasse J F, Jao D, Sankar A. A quantum algorithm for computing isogenies between supersingular elliptic curves [C]// International Conference on Cryptology in India. Springer, Cham, 2014: 428-442.
[5] Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies [C]// International Workshop on Post-Quantum Cryptography. Springer, Berlin, Heidelberg, 2011: 19-34.
[6] Castryck W, Lange T, Martindale C, et al. CSIDH: an efficient post-quantum commutative group action [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018: 395-427.
[7] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems [C]// Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1986: 186-194.
[8] Abdalla M, An J H, Bellare M, et al. From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security [C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2002: 418-433.
[9] Yoo Y, Azarderakhsh R, Jalali A, et al. A post-quantum digital signature scheme based on supersingular isogenies [C]// International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017: 163-181.
[10] Galbraith S D, Petit C, Silva J. Identification protocols and signature schemes based on supersingular isogeny problems [C]// International confer-

ence on theory and application of cryptology and information security. Springer, Cham, 2017: 3-33.
[11] De Feo L, Galbraith S D. SeaSign: Compact isogeny signatures from class group actions [C]// Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2019: 110-139.
[12] Beullens W, Kleinjung T, Vercauteren F. CSI-FiSh: Efficient isogeny based signatures through class group computations [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2019: 227-247.
[13] Galbraith S D. Mathematics of public key cryptography [M]. Cambridge University Press, 2012.
[14] DeFeo L. Mathematics of isogeny based cryptography [J]. arXiv preprint arXiv: 1711.04062, 2017, 12.
[15] Cozzo D, Smart N P. Sashimi: Cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol [C]// International Conference on Post-Quantum Cryptography. Springer, Cham, 2020: 169-186.
[16] Benhamouda F, Camenisch J, Krenn S, et al. Better zero-knowledge proofs for lattice encryption and their application to group signatures [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2014: 115-134.
[17] Bellare M, Poettering B, Stebila D. From identification to signatures, tightly: a framework and generic transforms [C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2016: 435-464.
[18] EI Kaafarani A, Katsumata S, Pintore F. Lossy CSI-FiSh: Efficient signature scheme with tight reduction to decisional CSIDH-512 [C]// IACR International Conference on Public-Key Cryptography. Springer, Cham, 2020: 157-186.
[19] Yu Xuan, Hou Shuhui. Efficient and Secure Group Signature Scheme [J]. Communications Technology, 2018, 51 (2): 413-418.

Note: Figure translations are in progress. See original paper for figures.