Provably Secure Short Signature Scheme from Isogeny between Elliptic Curves

Kunal Dey[1] and Sumit Kumar Debnath[2,*]

[1]Department of Mathematics, National Institute of Technology Jamshedpur,
Jamshedpur-831014, India; kunaldey3@gmail.com
[2]Department of Mathematics, National Institute of Technology Jamshedpur,
Jamshedpur-831014, India; sdebnath.math@nitjsr.ac.in

Abstract

Digital signature is one of the most important public key cryptographic primitive for message authentication. In a digital signature scheme, receiver of a message-signature pair gets assurance about the fact that the message belongs to the sender and neither receiver nor any third party can manipulate the message. In the current state of art, most of the existing digital signatures' security relies on classical cryptographic assumption based hard problems, such as discrete log, integer factorization, etc. However, rapid development of quantum computing creates a security threat to these classical digital signature schemes. It indicates the recruitment of an alternative solution which can prevent quantum attacks. We focus on this concern by implementing a post-quantum secure isogeny based digital signature scheme without making use of SIDH and CSIDH. Our scheme achieves *uf-cma* security under a hard problem in isogeny. The proposed signature scheme incurs 256 byte public key size and 128 byte signature size to achieve 128-bit security level (NIST-1 level of security). In particular, the size of signature of our design is smaller than all other IBC based signature schemes at the 128-bit security level.

Keywords: isogeny based cryptography; post-quantum cryptography; elliptic curve cryptography; digital signature; Weil pairing.

1 Introduction

Digital Signature is widely used important cryptographic mechanism which is applied to authenticate a message. It typically consists of three algorithms. First one is for generating public key-secret key pair of the user. While, the second one is the signing algorithm and the third one is the verification algorithm. The following properties should be required to design a valid digital signature:

(i) **Authentication -** It certifies that message has been formed by a valid sender.

(ii) **Integrity -** This property makes sure that the message has not been altered during transition.

[*] Corresponding author

(iii) **Non-repudiation -** It ensures that the signer or source cannot deny the generation of the signature on a message.

In most cryptographic protocol suites, there is a standard element like Digital signatures. It is applicable in several practical real life scenarios, such as electronic mail, digital contracts, electronic cash, electronic voting, sharing medical record, transmission of government/public sectors' secure data, etc. Some of them are discussed below.

Secure communication: Digital signature enables secure communication via email, sms, etc.

Healthcare: Administrative body uses digital signature in treatment to share patients medical record, digital prescription, hospital's private data, etc., in an efficient and secure way.

Cryptocurrencies: In order to authenticate the holder of a bitcoin and manage transaction data, digital signature is employed.

The notion of digital signature was first introduced by Diffie and Hellman [13] in 1976. Later, Rivest et al. [25] established well known RSA digital signature which is used in many software marketing packages. In the following, several classical digital signatures were developed, such as ElGamal signature [16], Merkle Signature [22], etc. Security of these classical signatures depends on hard problems of number-theory, such as "discrete logarithm problem", "integer factorization problem". However, the continuous growth of quantum technology makes a security threat to these problems. This is because, one may solve these problems in polynomial time by running Shor's algorithm [27] with the help of efficient quantum computers. Thereby, classical digital signatures' security is will be at risk, once there will be availability of quantum computers at large scale. As a consequence, it becomes essential to find some alternative that can prevent future quantum attacks. Post-quantum digital signature is an ideal choice to resolve this issue. In the current state of art, there exists several post-quantum digital signature schemes [4, 11, 12, 14, 15, 17, 19, 29, 30]. Among these, the isogeny based constructions attained tremendous attention in the recent research community due to the following salient features of isogeny based cryptography (IBC): smaller public key sizes and low communication cost. Security of IBC relies on some hard problems related to the isogeny between two elliptic curves which are either ordinary elliptic curves or supersingular elliptic curves. The concept of IBC was introduced by Couveignes [9].

In the last few decades, several works [2, 12, 23, 26] have been done in the context of IBC. However, there are only few constructions of IBC based digital signatures. Galbraith et al. [18] came up a signature scheme based on quaternios of l-isogeny problem. In the following, the signature SeaSign was proposed by Feo et al. [11]. They employed CSIDH [8] as the cryptographic building block. Beullens et al. [5] developed CSI-FIsh with the help of CSIDH [8]. Recently, Feo et al. [12] presented a digital signature scheme SQISign by using quaternions and isogeny.

1.1 Our contribution

The well known classical digital signatures, like RSA, ElGamal and elliptic curve digital signature algorithm (ECDSA) would suffer security flaws if sufficiently large quantum computers are invented. This is due to the existence of Shor's algorithm. As a consequence, there would be a security threat in the technologies which employ these classical digital signatures as the underlying fundamental blocks. It indicates the necessity of quantum computer immune digital signatures, which belongs to post-quantum cryptography (PQC). IBC is one of the main contestant of PQC. It is very attractive due to smaller public key sizes and low communication cost.

In the literature, there are only a few isogeny based digital signatures [5, 11, 12, 18]. Thus developing secure and more efficient isogeny based digital signature is an interesting direction of research. In our work, we focus to design and analysis of a new signature scheme using IBC. We are motivated by techniques of [3, 6] for the construction of our scheme. The proposed signature does not make use of SIDH [20] and CSIDH [8]. We prove that our scheme attains *uf-cma* security under the hardness expectation that computation of the image of a given point under an unrevealed isogeny is a hard problem. In order to reach 128-bit security level (NIST-1 level of security), sizes of the public key and signature of our scheme turn out be 256 byte and 128 byte respectively. Particularly, signature size of our construction is smaller than that of all other IBC based signature schemes at the 128-bit security level. It is practically feasible to apply the proposed signature in several real life scenarios as mentioned above since it produces a short signature with feasible size public key.

2 Preliminaries

2.1 Notations

$\mathbb{F}_q$ denotes a finite field of characteristic p for some prime p and $\overline{\mathbb{F}}_q$ represnts the extension filed of the filed $\mathbb{F}_q$. $\#X$ stands for the cardinality of X.

Definition 2.1. Bilinear pairing [1, 21]: *Let G_1 and G_2 be two additive groups of exponent n with identity 0 and G_3 be a cyclic group of order n with identity 1. A bilinear map $e : G_1 \times G_2 \longrightarrow G_3$ should attains the following properties:*
a) For all $X, X' \in G_1$ and $Y, Y' \in G_2$, $e(X + X', Y) = e(X, Y)e(X', Y)$ and $e(X, Y + Y') = e(X, Y)e(X, Y')$.
b) For all $X \in G_1$ with $X \neq 0$, there exist $Y \in G_2$ such that $e(X, Y) \neq 1$.
c) e can be efficiently computed.

Definition 2.2. Divisor of a rational function [1, 21]: *Let f be a rational function. Then divisor of f is denoted by $div(f)$ and defined as $div(f) =< f >= \sum_{P \in C} ord_P(f)(P)$, where $ord_P(f)$ is the number of zeroes or poles at P.*

2.2 Elliptic curve and isogeny [10]

An elliptic curve over $\mathbb{F}_p$ is a sooth projective curve of genus 1 with atleast one $\mathbb{F}_p$- rational point. The short Weierstrass form of an elliptic curve $E/\mathbb{F}_p$ is defined as $y^2 = x^3 + cx + d$ with $c, d \in \mathbb{F}_p$, $4c^3 + 27d^2 \neq 0$ and $p \neq 2, 3$, where $\theta = (0 : 1 : 0)$ is the point at infinity. The collection of all $\mathbb{F}_p$-rational points on an elliptic curve forms a group which is known as elliptic curve group and it is denoted by $E(\mathbb{F}_p)$. Hasse's theorem ensures that $\#E(\mathbb{F}_p) = p + 1 - a$ with $|a| \leq 2\sqrt{p}$. The n-th torsion group for an elliptic curve $E/\mathbb{F}_p$ is denoted by $E[n]$ and defined as the collection of all points P in $E(\overline{\mathbb{F}}_p)$ such that order of P divides n.

Theorem 2.3. *[28] For an elliptic curve $E/\mathbb{F}_q$ with char($\mathbb{F}_q$)=p,*

$$E[i^e] \simeq \begin{cases} \mathbb{Z}/i^e\mathbb{Z} \oplus \mathbb{Z}/i^e\mathbb{Z}, & \text{if } i \neq p \\ \mathbb{Z}/i^e\mathbb{Z} \text{ or } 0, & \text{if } i = p \end{cases}$$

for each prime i and $e \in \mathbb{Z}$.

One may conclude that $E[p]$ is either isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or 0. If $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$, E is called an ordinary elliptic curve and otherwise, E is called supersingular.

A morphism is a rational map which is defined everywhere. It is either surjective or constant on projective curves. Isogeny $\phi : E \rightarrow E'$ is a surjective morphism inducing a group homomorphism from $E(\overline{\mathbb{F}}_p)$ to $E'(\overline{\mathbb{F}}_p)$ for two elliptic curves E and E'. In particular, an isogeny $\phi : E \rightarrow E'$ can be written as $\phi(x, y) = \left(\frac{\alpha(x)}{\beta(x)}, \frac{r(x)}{s(x)}y\right)$, where $\alpha(x), \beta(x), r(x), s(x) \in \mathbb{F}_p[x]$, $\alpha(x)$ is perpendicular to $\beta(x)$ and $r(x)$ is perpendicular to $s(x)$ in $\mathbb{F}_p[x]$. Degree of ϕ is the maximum of $deg(p(x))$ and $deg(q(x))$. If $\left(\frac{\alpha(x)}{\beta(x)}\right)' \neq 0$, ϕ is called a separable isogeny; otherwise, ϕ is inseparable. Two elliptic curves E and E' are called isomorphic if there exists isogenies $\phi_1 : E \rightarrow E'$ and $\phi_2 : E' \rightarrow E$ such that their compositions are identity.

An endomorphism is a morphism on E that fixes a distinguished point. The collection of all endomorphisms of E, along with the zero map, forms a ring, namely endomorphism ring of E ($End(E)$) under the binary compositions "pointwise addition" and "mapping composition". The endomorphism defined over $\mathbb{F}_p$ is called $\mathbb{F}_p$- rational endomorphsm and the set of such endomorphisms is denoted by $End_p(E)$. For any natural number m, multiplication by m map of an elliptic curve E is denoted by $[m] : E \longrightarrow E$. It is an example of isogeny with kernel $E[m]$. Given an n-degree isogeny $\phi : E \rightarrow E'$ over $\mathbb{F}_p$ there must exists an isogeny $\hat{\phi} : E' \rightarrow E$ with $\phi\hat{\phi} = \hat{\phi}\phi = [n]$. $\hat{\phi}$ is known as the dual isogeny [24] of ϕ and it is unique.

2.3 Hardness assumption

We prove that our proposed signature scheme is secure under the following hardness assumption which we call hidden isogeny (HI) problem in this literature.

Definition 2.4. ***(Hidden Isogeny (HI) Problem** [23]) Given elliptic curves E, E' and a point P on E, it is hard to find the image of P under an unrevealed isogeny $\phi : E \rightarrow E'$.*

2.4 Weil pairing [1, 6, 7]

Let E be an elliptic curve over some finite field $\mathbb{F}_q$ and n be an integer such that $gcd(n, q) = 1$ and $n|\#E(\mathbb{F}_q)$. The smallest $k \in \mathbb{Z}^+$ with $n|q^k - 1$ is called the embedding degree. Consider a set $\mu_n = \{y \in \overline{\mathbb{F}}_p^* : y^n = 1\}$. The field $\mathbb{F}_q(\mu_n)$ represents finite extension $\mathbb{F}_{q^k}$ of $\mathbb{F}_q$ and $E(\mathbb{F}_{q^k})[n]$ is the set of points in $E(\mathbb{F}_{q^k})$ whose orders divide n. Let, $X, Y \in E(\mathbb{F}_{q^k})[n]$ and f_X, f_Y be rational functions on E such that $div(f_X) = n(X) - n(\theta)$, $div(f_Y) = n(Y) - n(\theta)$. Then Weil pairing $e_n : E(\mathbb{F}_{q^k})[n] \times E(\mathbb{F}_{q^k})[n] \longmapsto \mu_n$ is defined as $e_n(X, Y) = \frac{f_X(Y+Z)}{f_X(Z)} / \frac{f_Y(X-Z)}{f_Y(-Z)}$, where $Z \notin \{\theta, X, -Y, X - Y\}$ is a point in $E(\mathbb{F}_{q^k})[n]$.

Theorem 2.5. *Weil pairing satisfies the following properties:*

(i) $e_n(X,Y)^n = 1$.

(ii) *For all* $X, Y, Z \in E(\mathbb{F}_{q^k})[n]$, $e_n(X+Y,Z) = e_n(X,Z)e_n(Y,Z)$ *and* $e_n(Z,X+Y) = e_n(Z,X)e_n(Z,Y)$.

(iii) $e_n(X,X) = 1$, *for all* $X \in E(\mathbb{F}_{q^k})[n]$.

(iv) $e_n(X,Y) = e_n(Y,X)^{-1}$, $X, Y \in E(\mathbb{F}_{q^k})[n]$.

(v) $e_n(X,Y) = 1$ *for all* Y *if and only if* $X = \theta$.

(vi) $e_n(X,Y) = 1$ *for all* X *if and only if* $Y = \theta$.

Let $\phi : E \to E'$ be an isogeny and $\hat{\phi} : E' \to E$ be its dual isogeny. Then following [3], one may write $e_n(\phi(X),Y) = e_n(X,\hat{\phi}(Y))$, for all $X \in E(\mathbb{F}_{q^k})[n]$ and $Y \in E'(\mathbb{F}_{q^k})[n]$.

2.5 Digital signature scheme

A digital signature scheme involves three algorithms – Setup, $\mathsf{Signature}$ and $\mathsf{Verification}$ which are given below.

$(\mathsf{pk},\mathsf{sk}) \leftarrow \mathsf{Setup}(1^\lambda)$: On input security parameter λ, a signer generates public key-signing key pair $(\mathsf{pk}, \mathsf{sk})$.

$(\sigma) \leftarrow \mathsf{Signature}(m,\mathsf{sk})$: Given a message m and the signing key sk, the signer runs this algorithm to generate a signature σ on m.

$(1 \text{ or } 0) \leftarrow \mathsf{Verification}(m,\sigma,\mathsf{pk})$: Given (m,σ) and pk, a verifier exicutes this algorithm and check the validity of the pair (m,σ). He then outputs 1 if the pair is a valid one, otherwise outputs 0.

2.6 Unforgeability under chosen-message attack (*uf-cma*) [11]

It is a game between a probabilistic polynomial time (PPT) adversary $(\mathcal{A})$ and a challenger $(\mathcal{C})$ for a signature scheme $sig = (\mathsf{Setup},\mathsf{Signature},\mathsf{Verification})$ follows from Section 2.5. The experiment $Ex^{uf\text{-}cma}_{sig(1^\lambda)}$ is structured as follows:

Setup: Utilizing this algorithm $\mathcal{C}$ generates public key-signing key pair $(\mathsf{pk},\mathsf{sk})$ and forwards pk to $\mathcal{A}$.

Sign-query: In this phase, $\mathcal{A}$ makes query to $\mathcal{C}$ for signature of a message m. In the following, C runs the algorithm $\mathsf{Signature}$ and returns a valid signature σ to $\mathcal{A}$.

Forgery: In this phase, $\mathcal{A}$ outputs a forge signature σ' for a message m' which has not been queried before in **Sign-query** phase. If The message-signature pair (m',σ') passes the $\mathsf{Verification}$ algorithm then $\mathcal{A}$ wins the game.

The probability of success of $\mathcal{A}$ is denoted by $Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^\lambda)}}$ and defined by $Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^\lambda)}} = \mathsf{Pr}[Ex^{uf\text{-}cma}_{sig(1^\lambda)} = 1] = \mathsf{Pr}[\mathcal{A} \text{ wins the game}]$.

Definition 2.6. *A signature scheme is said to have* uf-cma *security if* $Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^{\lambda})}}$ *is negligible for any probabilistic polynomial time adversary* $\mathcal{A}$ *who is allowed to make at most* t *(polynomial time)* ***Sign-query****.*

3 Proposed signature scheme

Parameters: Consider two primes p, q with $p = 12q - 1$ and a supersingular elliptic curve E over $\mathbb{F}_p$. Then $\#E(\mathbb{F}_p) = p + 1 = 12q$. Note that $Char(\mathbb{F}_{p^2}) = p$ with $q \nmid p$ and $k = 2$ is the smallest positive integer such that $q \mid p^k - 1$. As a consequence, 2 is the embedding degree. Indeed, $\mathbb{F}_p(\mu_q) = \mathbb{F}_{p^2}$, where $\mu_q = \{y \in \mathbb{F}^*_{p^2} : y^q = 1\}$ is a cyclic group of order q. Here $gcd(p, q) = 1$ and $q \mid \#E(\mathbb{F}_p)$. Thereby, the Weil pairing $e_q : E(\mathbb{F}_{p^2})[q] \times E(\mathbb{F}_{p^2})[q] \longmapsto \mu_q$, as discussed in Section 2.4, is well defined. Note that $E(\mathbb{F}_p)[q] \subset E(\mathbb{F}_{p^2})[q]$.

A high level overview: The proposed signature scheme is designed based on the concept of . It uses IBC in its construction to achieve post-quantum security. Our signature scheme involves three algorithm: Setup, Signature and Verification. During Setup, a signer generates his public key-signing key pair (pk, sk). In the following, the signer runs Signature to generate a signature σ on a message m. The algorithm Verification is run by a verifier to verify the validity of the pair (m, σ). Detail description of our scheme is provided below.

Protocol 1. *Proposed signature*

(pk, sk) $\leftarrow$ Setup(1^{λ}). *The signer randomly chooses a secret isogeny* ϕ *from* $End_p(E)$. *To generate public key, he performs the following operations:*

1. *selects a random element* $x \in E(\mathbb{F}_{p^2})[q] \setminus E(\mathbb{F}_p)[q]$,
2. *computes the dual isogeny* $\hat{\phi}$,
3. *determines* $\hat{\phi}(x)$,
4. *if* $\hat{\phi}(x) \in E(\mathbb{F}_{p^2})[q] \setminus E(\mathbb{F}_p)[q]$ *then sets the signing key* sk *as* ϕ *and public key* pk *as* $(x, \hat{\phi}(x))$*; otherwise, starts from step 1.*

$(\sigma) \leftarrow$ Signature(m, sk). *Given a message* $m \in 0, 1^*$, *the signer executes the following operations to generate a valid signature on* m *using* sk $= \phi$*:*

1. *randomly chooses* $k \in \mathbb{Z}^{\star}_q$ *and* $y \in E(\mathbb{F}_p)[q]$ *and determines* $e_q(y, x)^k = r \in \mu^*_q$,
2. *evaluates* $H(m, r) = v \in E(\mathbb{F}_p)[q]$, *where* $H : \{0, 1\}^* \times \mu_q \longmapsto E(\mathbb{F}_p)[q]$ *is a cryptographically secure collision resistant hash function,*
3. *Computes* $u = \phi(v) + [k]y \in E(\mathbb{F}_p)[q]$,
4. *outputs the signature as* $\sigma = (u, v)$.

(1 *or* 0) $\leftarrow$ Verification(m, σ, pk). *The verifier checks the correctness of the message-signature pair* (m, σ) *as follows:*

1. *evaluates* $\overline{r} = e_q(u, x)e_q(v, -\hat{\phi}(x))$.
2. *if* $H(m, \overline{r}) = v$ *then the signature is valid and outputs 1, otherwise the signature is invalid and outputs 0.*

Correctness: In order to show the correctness of our scheme, it is sufficient to prove that $\overline{r} = r$.

$$\begin{aligned}\overline{r} &= e_q(u,x)e_q(v,-\hat{\phi}(x)) \\ &= e_q(\phi(v)+[k]y,x)e_q(v,-\hat{\phi}(x)) \\ &= e_q(\phi(v),x)e_q([k]y,x)e_q(v,-\hat{\phi}(x)) \\ &= e_q([k]y,x)e_q(\phi(v),x)e_q(\phi(v),-x) \\ &= e_q([k]y,x)e_q(\phi(v),\theta) \\ &= e_q([k]y,x) \\ &= e_q(y,x)^k \\ &= r\end{aligned}$$

Remark 3.1. *We know that $\gamma, \delta \in E(\mathbb{F}_{p^2})[q]$, $e_q(\gamma,\delta) = 1$ if and only if one of γ and δ is a multiple of other. In our scheme, the points v, u lie in $E(\mathbb{F}_p)[q]$ and x, $\hat{\phi}(x)$ lie in $E(\mathbb{F}_{p^2})[q] \setminus E(\mathbb{F}_p)[q]$. As a consequence, neither one of x, u can be written as a multiple of other nor one of $\hat{\phi}(x), v$ can be written as a multiple of other. Thus we can conclude that $e_q(u,x) \neq 1$ and $e_q(v,-\hat{\phi}(x)) \neq 1$.*

4 Security

This section discusses the security of our proposed scheme.

Theorem 4.1. *If finding the image of a given point under an unrevealed isogeny is hard i.e., if HI problem is hard then the proposed signature scheme is* uf-cma *secure.*

Proof. Let there be a adversary $\mathcal{A}$ with non-negligible success probability in the *uf-cma* game. Then we show that an oracle machine $OM^{\mathcal{A}}$ can be designed in sauch a way that it will break the computational problem of isogeny. Here we consider the hash function H as random oracle. We present a series of games Ga^0, Ga^1, Ga^2, where Ga^i slightly modifies Ga^{i-1} for $i = 1, 2$. Let the success probability of $\mathcal{A}$ in Ga^i is $\mathsf{Pr}[\mathsf{Ga}^i]$.

Ga^0: It is exactly same as $\mathsf{uf\text{-}cma}$ game for signature scheme. Here, $Adv_{\mathcal{A}}^{Ex_{sig(1^\lambda)}^{uf\text{-}cma}} = \mathsf{Pr}[Ex_{sig(1^\lambda)}^{uf\text{-}cma} = 1] = \mathsf{Pr}[\mathsf{Ga}^0]$.

Ga^1: This game is analogues to Ga^0 except that during the **Sign-query**, $OM^{\mathcal{A}}$ replaces the signature by randomly chosen u, v from $\mathcal{E}(\mathbb{F}_p)[q]$ and restores v in the place of the hash (H) query on (m, r) , where $r = e_q(u,x)e_q(v,-\hat{\phi}(x))$. If $|\mathsf{Pr}[\mathsf{Ga}^1] - \mathsf{Pr}[\mathsf{Ga}^0]|$ is non-negligible, then $\mathcal{A}$ will be able to distinguish the output distributions of random oracle H, which is impossible. Hence, $|\mathsf{Pr}[\mathsf{Ga}^1] - \mathsf{Pr}[\mathsf{Ga}^0]|$ is negligible, say $\epsilon_1(\lambda)$.

Ga^2: It is identical to Ga^1 excepting $OM^{\mathcal{A}}$ replaces a random element from $E(\mathbb{F}_p)[q]$ in the place of the hash (H) query on (m^*, r^*). Using the similar concept as mentioned in Ga^1, we may write $|\mathsf{Pr}[\mathsf{Ga}^2] - \mathsf{Pr}[\mathsf{Ga}^1]|$ is negligible, say $\epsilon_2(\lambda)$.

Now we have, $|\mathsf{Pr}[\mathsf{Ga}^2] - Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^\lambda)}}| {=} |\mathsf{Pr}[\mathsf{Ga}^2] - \mathsf{Pr}[\mathsf{Ga}^0]| \leq |\mathsf{Pr}[\mathsf{Ga}^2] - \mathsf{Pr}[\mathsf{Ga}^1]| {+} |\mathsf{Pr}[\mathsf{Ga}^1] - \mathsf{Pr}[\mathsf{Ga}^0]| {=} \epsilon_1(\lambda) + \epsilon_2(\lambda) {=} \epsilon(\lambda)(\text{say})$.

Hence, $\mathcal{A}$'s success probability $\mathsf{Pr}[\mathsf{Ga}^2]$ in Ga^2 is same as $Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^\lambda)}}$, which is assumed to be non-negligible. Therefore, the oracle machine $OM^{\mathcal{A}}$ can generate two valid transcripts (r, v_1, u_1), (r, v_2, u_2) with the help of where $\mathcal{A}$ and controlling the outputs of the random oracle H, where $u_1 = \phi(v_1) + [k]y$, $u_2 = \phi(v_2) + [k]y$, $v_1 = \rho \in E(\mathbb{F}_p)[q]$ and $v_2 = \theta$. Then we have the following:

$$u_1 - u_2 = \phi(v_1 - v_2) = \phi(\rho - \theta) = \phi(\rho).$$

Hence, $OM^{\mathcal{A}}$ extracts the value of $\phi(\rho)$ without knowing the isogeny ϕ, which is a contradiction since the HI problem is hard. As a consequence, $\mathsf{Pr}[\mathsf{Ga}^2]$ is negligible which implies $Adv_{\mathcal{A}}^{Ex^{uf\text{-}cma}_{sig(1^\lambda)}}$ is negligible. Thus, our scheme has achived *uf-cma* security. □

5 Efficiency

We talk about the computation and communication cost of our scheme in this segment. To archive λ bit of security, we take $p \approx 2^{2\lambda}$.

Computation cost: In Setup, after choosing secret isogeny ϕ from $End_p(E)$, we compute its dual isogeny and find image of a random element $x \in \mathcal{E}(\mathbb{F}_{p^2})[q] \setminus \mathcal{E}(\mathbb{F}_p)[q]$ under ϕ. To sign a message, we need to compute one Weil pairing, one exponentiation, one hash evaluation and image of a point on $E(\mathbb{F}_p)$ under an isogeny ϕ. During $\mathsf{Verification}$, two Weil pairing and one hash function evaluation are required.

Communication cost: The public key consists of two points in $\mathcal{E}(\mathbb{F}_{p^2})$ and the signature consists of two points in $\mathcal{E}(\mathbb{F}_p)$. Thus the public key size and the signature size are $8\lceil\log_2(p)\rceil$ and $4\lceil\log_2(p)\rceil$ respectively. A comparative summary of our proposed signature with the existing IBC based signature schemes is presented in table 1 for 128-bit security level, where B stands for byte. Note that the signature size of our scheme is optimal.

Table 1 Comparison of communication costs to archive 128-bits security level.

Schemes	Public key size	Signature size
Sea Sign(Rejection sampling)	64B	20144B
Sea Sign(Shorter signature)	4096KiB	978B
Sea Sign(Smaller public key)	32B	3136B
Chi-Fish	512B	956B
SQISign	64B	204B
Signature based on Endomorphism ring	96B	11264B
Our scheme	256B	128B

6 Conclusion

In this paper, we utilized the concepts of [3, 6] to design an isogeny based signature scheme that belongs to PQC. Our scheme depends on the fact that the computation of the image of a given point under an isogeny is believed to be a hard problem if the isogeny is kept secret. The proposed scheme attains *uf-cma* security in random oracle model. Our scheme incur optimal signature size in the context of post-quantum signatures. The public key size of our construction is comparable with the existing IBC based signatures. It would be an interesting direction of future work to reduce the public key size of our scheme.

7 Declarations

References

[1] Alex Edward Aftuck. The weil pairing on elliptic curves and its cryptographic applications. 2011.

[2] Reza Azarderakhsh, David Jao, Kassem Kalach, Brian Koziel, and Christopher Leonardi. Key compression for isogeny-based cryptosystems. In *Proceedings of the 3rd ACM International Workshop on ASIA Public-Key Cryptography*, pages 1–10, 2016.

[3] Mojtaba Bahramian and Elham Hajirezaei. An identity-based encryption scheme using isogeny of elliptic curves. *Facta Universitatis, Series: Mathematics and Informatics*, pages 1451–1460, 2021.

[4] Daniel J Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. Sphincs: practical stateless hash-based signatures. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 368–397. Springer, 2015.

[5] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. Csi-fish: Efficient isogeny based signatures through class group computations. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 227–247. Springer, 2019.

[6] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Annual international cryptology conference*, pages 213–229. Springer, 2001.

[7] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the weil pairing. In *International conference on the theory and application of cryptology and information security*, pages 514–532. Springer, 2001.

[8] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. Csidh: an efficient post-quantum commutative group action. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 395–427. Springer, 2018.

[9] Jean Marc Couveignes. Hard homogeneous spaces. *IACR Cryptol. ePrint Arch.*, 2006:291, 2006.

[10] Luca De Feo. Mathematics of isogeny based cryptography. *arXiv preprint arXiv:1711.04062*, 12, 2017.

[11] Luca De Feo and Steven D Galbraith. Seasign: Compact isogeny signatures from class group actions. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 759–789. Springer, 2019.

[12] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: compact post-quantum signatures from quaternions and isogenies. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 64–93. Springer, 2020.

[13] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[14] Jintai Ding and Dieter Schmidt. Rainbow, a new multivariable polynomial signature scheme. In *International Conference on Applied Cryptography and Network Security*, pages 164–175. Springer, 2005.

[15] Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. Crystals-dilithium: A lattice-based digital signature scheme. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 238–268, 2018.

[16] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.

[17] Philippe Gaborit and Marc Girault. Lightweight code-based identification and signature. In *2007 IEEE International Symposium on Information Theory*, pages 191–195. IEEE, 2007.

[18] Steven D Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 3–33. Springer, 2017.

[19] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman. Nss: An ntru lattice-based signature scheme. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 211–228. Springer, 2001.

[20] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[21] Alfred Menezes. An introduction to pairing-based cryptography. *Recent trends in cryptography*, 477:47–65, 2009.

[22] Ralph C Merkle. A certified digital signature. In *Conference on the Theory and Application of Cryptology*, pages 218–238. Springer, 1989.

[23] Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. Sigamal: A supersingular isogeny-based pke and its application to a prf. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 551–580. Springer, 2020.

[24] Michael Naehrig and Joost Renes. Dual isogenies and their application to public-key compression for isogeny-based cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 243–272. Springer, 2019.

[25] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[26] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptol. ePrint Arch.*, 2006:145, 2006.

[27] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[28] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra.* Cambridge university press, 2013.

[29] Christopher Wolf and Bart Preneel. Asymmetric cryptography: Hidden field equations. *IACR Cryptol. ePrint Arch.*, 2004:72, 2004.

[30] Dong Zheng, Xiangxue Li, and Kefei Chen. Code-based ring signature scheme. *IJ Network Security*, 5(2):154–157, 2007.