Improved Digital Signatures Based on Elliptic Curve Endomorphism Rings

Xiu Xu[3,4,5⋆], Chris Leonardi[1], Anzo Teh[1], David Jao[1,2], Kunpeng Wang[3,4,5], Wei Yu[3,4,5], Reza Azarderakhsh[6]

[1] Department of Combinatorics and Optimization, University of Waterloo
[2] evolutionQ, Inc., Waterloo, Ontario, Canada
[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[4] Data Assurance and Communications Security Research Center, Beijing, China
[5] School of Cyber Security, University of Chinese Academy of Sciences
[6] Florida Atlantic University

Abstract. In AsiaCrypt 2017, Galbraith-Petit-Silva proposed a digital signature scheme based on the problem of computing the endomorphism ring of a supersingular elliptic curve. This problem is more standard than that of the De Feo-Jao-Plût SIDH scheme, since it lacks the auxiliary points which lead to the adaptive active attack of Galbraith-Petit-Shani-Ti. The GPS signature scheme applies the Fiat-Shamir or Unruh transformation to the raw identification protocol obtained from the endomorphism ring problem, and makes use of the Kohel-Lauter-Petit-Tignol quaternion isogeny path algorithm to find a new ideal. However, the GPS signature scheme is not very practical. In this paper, we take a first step towards quantifying the efficiency of the GPS signature scheme. We propose some improvements in the underlying algorithms for the GPS scheme, along with a new method which trades off key size for signature size to decrease the signature size from around 11 kilobytes to 1 kilobyte at the 128-bit security level by using multi-bit challenges. We also provide a concrete implementation of the GPS signature scheme using Sage and CoCalc.

Keywords: post-quantum, digital signature, supersingular isogeny, endomorphism ring

1 Introduction

Supersingular isogeny cryptosystems have emerged as a promising post-quantum system with the introduction of the Supersingular Isogeny Diffie-Hellman scheme of Jao and De Feo [12]. Although SIDH is believed to resist attacks from quantum computers, it relies on a variation of the standard isogeny-finding hard problem of Charles et al. [3] which involves sending auxiliary point information that enables an adaptive active attack [9], which can recover a static secret key

⋆ Corresponding author email: xuxiu2017@gmail.com

bit by bit over many protocol runs. By contrast, the problem of computing the endomorphism ring of a supersingular curve is known to be equivalent to the standard isogeny-finding problem on supersingular isogeny graphs [7].

In the realm of digital signatures, a signature scheme based on the SIDH problem can be obtained by applying the either Fiat-Shamir or Unruh transformation to the zero-knowledge proof of identity proposed in [8]. Such a scheme was proposed by Galbraith et al. [10] and Yoo et al. [20] independently. In addition, [10] also proposes a second signature scheme which requires only the hardness of computing endomoprhism rings of a supersingular elliptic curve, which we call the GPS scheme after the authors of [10]. Although [10] provides concrete parameter sizes and key lengths for the 128-bit security level, as well as asymptotic runtime estimates, no concrete implementation results are reported, and we are not aware of any available published implementation of the GPS scheme for real parameter sets of cryptographic size.

Our Contributions.

1. We provide the first published description of a concrete implementation of the GPS scheme in Sage, albeit for parameter sizes which fall short of cryptographic size. Our efforts indicate that the main bottleneck in GPS is likely to be the process of translation from the new ideal generated by the Kohel et al. algorithm [14] to a new isogeny, which involves constructing torsion points over large extension fields at a relatively great cost.
2. We propose a new strategy for computing the aforementioned new isogeny by taking advantage of the fact that all supersingular curves can be defined over $\mathbb{F}_{p^2}$, in order to renormalize the codomain of each component isogeny in the chain, which helps control the growth of the extension field degree. Our new isogeny chain is structured as follows:

$$E_0/\mathbb{F}_{p^2} \xrightarrow[\langle P_1 \rangle]{\phi_1} E_1'/\mathbb{F}_{p^{d_1}} \xrightarrow{f_1} E_1/\mathbb{F}_{p^2} \xrightarrow[\langle f_1 \cdot \phi_1(P_1) \rangle]{\phi_2} E_2'/\mathbb{F}_{p^{d_2}} \xrightarrow{f_2} E_2/\mathbb{F}_{p^2} \to \dots$$

3. We propose an optimization of GPS using multi-bit challenges at the expense of large public keys, based on a new assumption involving the forking lemma. This answers an open problem that was posed in [6] concerning how to obtain a similar tradeoff between public key size and signature size as in SeaSign for the SIDH setting. Our variant is secure under the random oracle model, and reduces GPS signature sizes to 1 kilobyte, close to that of SeaSign. The time cost is reduced as well, since we run $\lambda / \log s$ parallel computations instead of λ, where $\log s$ is the challenge size in bits and λ is the security parameter. Our construction uses a modified quaternion isogeny path algorithm whose starting point can be any maximal order (not only the special order $\mathcal{O}_0$), which is of independent interest.
4. We also consider some improvements in the algorithms for translating between isogeny and ideal, including point halving, fast discrete logarithm and Minkowski basis computation.

Related Work. Stolbunov [17] and Couveignes [5] presented initial versions of identification protocols and sketches of a signature scheme based on isogenies. They did not give a secure solution for how to represent the ideal $\mathfrak{b}_k\mathfrak{a}^{-1}$ in the case where the value of the challenge bit is $b_k = 1$, without leaking the private key. SeaSign [6] utilizes the idea of rejection sampling in exactly the way proposed by Lyubashevsky [15] to solve this problem. In addition, [6] sketches an approach to use multi-bit challenges, trading off challenge size for public key size. Large public keys can be easily stored in some settings, such as software signing and license checks, so this tradeoff is worthwhile in some cases.

Outline. The rest of this paper is organised as follows. Section 2 gives basic notation for isogenies and endomorphism rings, related assumptions, and the description of the identification scheme. Section 3 describes the new signature scheme we propose, with multiple challenge bits, and explains its efficiency and security. Section 4 describes our implementation of the original algorithms in the GPS signature scheme. Finally Section 5 presents our conclusions.

2 Preliminaries

2.1 Isogeny and Endomorphism Ring

An isogeny is a rational map from one curve E_0 to another curve E_1, mapping the infinite point of E_0 to the infinite point of E_1. An isogeny is group homomorphism, and (if separable) uniquely determined up to isomorphism by its kernel. An endomorphism is an isogeny from an elliptic curve to itself. The endomorphisms of an elliptic curve form a ring under pointwise addition and composition. For a non-constant separable isogeny, its degree is exactly the order of its kernel subgroup. Every isogeny $\phi\colon E_0 \to E_1$ has a dual isogeny $\hat{\phi}\colon E_1 \to E_0$ such that $\hat{\phi}\phi = [\deg \phi]$. From a computational point of view, the general method to compute an isogeny is to use Vélu's formulas [19].

Over a finite field, an ordinary elliptic curve E_0 is one whose endomorphism ring $\mathrm{End}(E_0)$ is isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\pi)$, and a supersingular elliptic curve is one whose endomorphism ring is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$ ramified at p and ∞. Such an algebra can be represented as $B_{p,\infty} = \mathbb{Q}\langle i, j\rangle$ with $i^2 = -1, j^2 = -p, k = ij = -ji$. Every supersingular elliptic curve is isomorphic to a curve defined over $\mathbb{F}_{p^2}$ for some p. Conjugation, reduced trace, reduced norm, and the bilinear form associated to the reduced norm are defined as follows:

1. $\alpha = a + bi + cj + dk \to \bar{\alpha} = a - bi - cj - dk$, where $a, b, c, d \in \mathbb{Q}$.
2. $\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2a$.
3. $\mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + pc^2 + pd^2$.
4. $\langle x, y\rangle = \mathrm{Nrd}(x + y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)$.

An ideal I in $B_{p,\infty}$ is a $\mathbb{Z}$-lattice of rank 4 and an order $\mathcal{O}$ is not only an ideal but also a ring. The left order of an ideal I is defined as $\mathcal{O}(I) = \{h \in B_{p,\infty} \mid$

$hI \subset I\}$, and I is called a left $\mathcal{O}$-ideal. If I is a left $\mathcal{O}$-ideal, then $I\bar{I} = N\mathcal{O}$ and $I = \mathcal{O}N + \mathcal{O}\alpha$ where N is the norm of the ideal and $N \mid \mathrm{Nrd}(\alpha)$. We say two left $\mathcal{O}$-ideals I_1 and I_2 are in the same equivalence class if $I_1 = I_2 q$ for some $q \in B_{p,\infty}^*$. Two orders $\mathcal{O}_1$ and $\mathcal{O}_2$ are of the same order type if $\alpha\mathcal{O}_1\alpha^{-1} = \mathcal{O}_2$ for $\alpha \in B_{p,\infty}^*$.

The Deuring correspondence states that there is a bijection from j-invariants of supersingular curves to maximal orders in the quaternion algebra $B_{p,\infty}$. For the supersingular curve $E_0 : y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$ where $p \equiv 3 \pmod 4$, the endomorphism ring of E_0 is isomorphic to the maximal order $\mathcal{O}_0 = \langle 1, i, \frac{1+k}{2}, \frac{i+j}{2} \rangle$, and there is an isomorphism of quaternion algebras $\theta\colon B_{p,\infty} \to \mathrm{End}(E_0) \otimes \mathbb{Q}$ sending $(1, i, j, k)$ to $(1, \phi, \pi, \pi\phi)$ where π is the Frobenius endomorphism mapping (x, y) to (x^p, y^p) and $\phi\colon (x, y) \to (-x, iy)$.

If we have an isogeny $\phi\colon E \to E'$ over $\mathbb{F}_{p^2}$ of degree n, then we can construct a left $\mathrm{End}(E)$-ideal $I = \mathrm{Hom}(E', E)\phi$ of norm n. Conversely, in order to construct an isogeny from a left $\mathrm{End}(E)$-ideal I, we define $E[I] = \bigcap_{\alpha \in I} \ker(\alpha)$. Then there is an associated isogeny $\phi_I\colon E \to E/E[I]$. If $(n, p) = 1$, then $E[I] = \{P \in E(\mathbb{F}_{p^2}) : \alpha(P) = \infty \text{ for all } \alpha \in I\}$.

2.2 Hard Problems

For more information on hard problems related to isogenies, see [7, 10, 11].

Problem 1 *Given two supersingular curves E, E' defined over $\mathbb{F}_{p^2}$, find an isogeny $\phi\colon E \to E'$.*

This problem is the most general problem related to finding isogenies. The fastest known algorithm for finding isogenies between supersingular curves in general takes $O(\sqrt{p}\log^2 p)$ [3]. It can be viewed as a graph navigation problem on a Ramanujan graph.

In SIDH, we choose a prime of the form $p = \ell_A^{e_A}\ell_B^{e_B} \cdot f \pm 1$ where ℓ_A and ℓ_B are small primes and f is a cofactor. We fix a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$. Furthermore, $E[\ell_A^{e_A}] = \mathbb{Z}/\ell_A^{e_A}\mathbb{Z} \oplus \mathbb{Z}/\ell_A^{e_A}\mathbb{Z} = \langle P_A, Q_A \rangle$, $E[\ell_B^{e_B}] = \mathbb{Z}/\ell_B^{e_B}\mathbb{Z} \oplus \mathbb{Z}/\ell_B^{e_B}\mathbb{Z} = \langle P_B, Q_B \rangle$.

Problem 2 *Let $\phi_A\colon E \to E_A$ be an isogeny with its kernel $\langle R_A \rangle$ where R_A is a point of order $\ell_A^{e_A}$. Given $E_A, \phi_A(P_B), \phi_A(Q_B)$, find a generator of $\langle R_A \rangle$.*

This is the computational supersingular isogeny (CSSI) problem upon which SIDH relies [8]. It can be reduced to a claw finding problem. Its classical and quantum complexities are $\mathcal{O}(p^{1/4})$ and $\mathcal{O}(p^{1/6})$, respectively. Recently, the van Oorschot-Wiener (vOW) golden collision finding algorithm [1, 4] was argued to be the most efficient quantum algorithm for CSSI.

Problem 3 *Given a supersingular curve E defined over $\mathbb{F}_{p^2}$, determine the endomorphism ring of E.*

For some special curves, the endomorphism rings are easy to compute, but for an arbitrary supersingular curve, finding its endomorphism ring is hard. The best quantum algorithm still runs in exponential complexity [13]. Problems 1 and 3 are known to be equivalent [7, 10].

2.3 Identification Protocol Based on Endomorphism Ring

We briefly describe the Galbraith-Petit-Silva [10] identification protocol.

1. The public key is (E_0, E_1), and the private key is an isogeny $\phi\colon E_0 \to E_1$.
2. The prover chooses a random walk of degree L from E_1 in the graph, arriving at a curve E_2 with $\psi\colon E_1 \to E_2$. The prover sends E_2 to the verifier.
3. The verifier randomly chooses a challenge bit b and sends b to the prover.
4. If $b = 0$, the prover answers ψ. If $b = 1$, the prover publishes a new isogeny $\eta\colon E_0 \to E_2$, where $\eta \neq \psi\phi$.
5. The verifier accepts the proof if the answer is indeed an isogeny betweem E_1 and E_2 or between E_0 and E_2.

The GPS signature scheme uses four key algorithms in the process of computing a new path η: loading the isogeny chains, translating from an isogeny to an quaternion ideal, finding a new path (using the quaternion isogeny path algorithm) and translating from the new ideal back to an isogeny. The reason that a new path η is published instead of the original isogeny $\psi\phi$ is that publishing $\psi\phi$ might reveal information about the secret ϕ. In order to produce a new path to avoid the leakage of the secret key, the quaternion isogeny path algorithm [14] is used.

Definition 1. *A signature* Π=(KeyGen, Sign, Verify) is said to be existentially unforgeable under adaptive chosen-message attacks if for all probabilistic polynomial time adversaries $\mathcal{A}$ with access to the oracle $\mathcal{O}$,

$$\left|\Pr\left[\begin{array}{c}(\mathrm{PK},\mathrm{SK}) \leftarrow \mathsf{KeyGen}(1^\lambda); \sigma_\mathrm{i} \leftarrow \mathcal{O}(\mathrm{m_i}) \text{ for } 1 \le \mathrm{i} \le \mathrm{k};\\ (m,\sigma) \leftarrow \mathcal{A}(\mathrm{PK}, \mathrm{m_i}, \sigma_\mathrm{i}) :\\ \mathsf{Verify}(m,\sigma) = 1 \textit{ and } m \neq m_i\end{array}\right]\right| \le \mathrm{negl}(\lambda).$$

Theorem 1 ([10]). *If the identification is non-trival and recoverable, then the signature derived from this identification using the Fiat-Shamir transform is secure against chosen-message attacks in the random oracle model.*

2.4 Quaternion Isogeny Path Algorithm

The quaternion isogeny path algorithm from Kohel et al. [14] plays an important role in finding a new ideal that corresponds to another isogeny path between two curves. [10] used the power-smooth version of the quaternion ℓ-isogeny algorithm to compute another path from E_0 to E_2 in the quaternion algebra. The new path is independent of E_1 and corresponds to an ideal J.

We recall the quaternion isogeny path algorithm briefly, adopting the notations in [10]. The inputs are a special maximal order $\mathcal{O}_0$ in the quaternion algebra $B_{p,\infty}$ and a corresponding left $\mathcal{O}_0$ ideal I given by a $\mathbb{Z}$-basis of elements in $\mathcal{O}_0$. This is equivalent to inputting two maximal orders $\mathcal{O}_0$ and $\mathcal{O}_1$, as the right order $\mathcal{O}_1$ of I is the set $\{h \in B_{p,\infty} \mid Ih \subset I\}$. The algorithm aims to find a new ideal J such that $J = Iq$ for some $q \in B^*_{p,\infty}$. Here are the main steps of the process:

1. Find I' such that I' has a prime norm N and $I' = Iq$.
2. Choose $\alpha \in I'$ such that $\gcd(\mathrm{Nrd}(\alpha), N^2) = N$, so that $I' = \mathcal{O}_0 N + \mathcal{O}_0\alpha$.
3. Set a bound $s = \frac{7}{2}\log p$, and odd integers $S_1 > p\log p$ and $S_2 > p^3 \log p$.
4. Find $a, b, c, d \in \mathbb{Z}$ such that $NS_1 = a^2 + b^2 + p(c^2 + d^2)$. Then set $\beta_1 = a + bi + cj + dk$ of norm NS_1.
5. Find $\beta_2 \in \mathbb{Z}j + \mathbb{Z}k$ such that $\beta_1\beta_2 = \alpha \bmod N\mathcal{O}_1$, and set $\beta_2 = Cj + Dk$.
6. Find β_2' of norm S_2 such that $\beta_2' - \lambda\beta \in N\mathcal{O}_0$ for some $\lambda \in \mathbb{Z}$.
7. Return $J = I'\overline{\beta_1\beta_2'}/N$.

We see that the norm of the new ideal J is $S = \frac{\mathrm{Nrd}(I')\,\mathrm{Nrd}(\beta_1\beta_2')}{N^2} = S_1S_2$ with $\log S \approx \frac{7}{2}\log p$, and an improvement in [16] reduces its norm to $\frac{5}{2}\log p$. The large norm of the new ideal is the root of the difficulty in implementing GPS signatures. We remark that implementing the quaternion isogeny path algorithm is of independent interest separating from the GPS signature scheme—it breaks the quaternion order analog of the CGL hash function [3], and also can be used to compute the j-invariant corresponding to a quaternion order. We also note here that the quaternion isogeny path algorithm in [10] is just suitable for the case that the input quaternion order is $\mathcal{O}_0$. However, we believe that it will also work for any other input quaternion after a little modification to the step 4 of the above algorithm which is also of independent interest. So in the following, we still call it the quaternion isogeny path algorithm even the input is not the special order $\mathcal{O}_0$.

3 Digital Signature Based on Endomorphism Ring

3.1 Modified Identification Protocol

We propose a modified identification protocol based on that of Section 2.3, using multi-bit challenges.

Phase 1 (done once)

Perform random walks ϕ_i from E_0 to $E_{A,i}$, where $i \in \{0, 1, ..., s-1\}$.

Phase 2 (repeated $t = \frac{\lambda}{\log s}$ times)

1. The prover sends the verifier a random walk w from E_0 to some curve E_B.
2. The verifier responds with $b \in \{0, 1, ..., s-1\}$.
3. The prover computes a dual isogeny $\hat{\phi}_b$ and with the quaternion isogeny path algorithm, produces a path w_b' between $E_{A,b}$ and E_B. The prover sends w_b' to the verifier.
4. The verifier accepts the proof if the answer is really an isogeny from $E_{A,b}$ to E_B.

Fig. 1: The multiple bit version of the identification protocol.

We give a brief analysis of the properties of the above protocol. It is obvious that this identification is non-trivial and recoverable.

Completeness. Just follow the procedure in Figure 1 and the verifier accepts the proof.

Soundness. Suppose we are given transcripts $(\mathrm{CMT}, \mathrm{c}, \mathrm{d}, \mathrm{RSP}_1, \mathrm{RSP}_2)$, where $\mathrm{CMT} = E_B$. For two different challenges c and d, we can compute two isogenies $w'_c \colon E_{A,c} \to E_B$ and $w'_d \colon E_{A,d} \to E_B$. Then we can obtain an isogeny $\hat{w'_d} w'_c$ from $E_{A,c}$ to $E_{A,d}$, which is a solution to Problem 4 that we propose in the following section.

Zero-knowledge. This simulator is almost identical as the one for the classical graph isomorphism. If the verifier is dishonest, we can remove these rounds from the simulator transcript. The distributions of the transcript $(\mathrm{CMT}, \mathrm{c}, \mathrm{RSP})$ are indistinguishable from the real one. The data revealed in step 3 is an isogeny produced by the quaternion isogeny path algorithm and this algorithm leaks no information about the input isogeny.

3.2 Proposed Digital Signature Scheme

In [10] it is proved that that any 2-special sound identification scheme can be transformed into a non-trivial scheme by running t sessions in parallel, where $t \geq \lambda/c$ with security parameter λ and challenge bit length c. Hence, one of the main reasons that this kind of signature scheme is of low efficiency is that the signature has to run t times. Using the multi-bit challenge approach, the resulting signatures gain higher efficiency and a smaller size. Algorithms 1, 2, and 3 present the resulting signature scheme using the Fiat-Shamir transform in the classical case.

Public Parameters. A security parameter λ and a prime p of the form $4 \cdot \ell_1 \cdots \ell_n - 1$ where ℓ_i is a small prime. The prime p satisfies $p \equiv 3 \bmod 4$. Small fixed parameters B, S_1, S_2, where $B = 2(1+\epsilon)\log p$, $\epsilon > 0$, $S_k = \prod_i \ell_{k,i}^{e_{k,i}}$, $\ell_{k,i}^{e_{k,i}} < B$, $\gcd(S_1, S_2) = 1$ and $\prod_i \left(\frac{2\sqrt{\ell_{k,i}}}{\ell_{k,i}+1}\right)^{e_{k,i}} < (p^{1+\epsilon})^{-1}$. A supersingular curve $E_0/\mathbb{F}_{p^2} : y^2 = x^3 + x$, and a cryptographic hash function H with at least λ bits of output. Suppose that the length of the challenge is $\log s$, i.e. $t = \lambda / \log s$.

Algorithm 1 $\mathsf{KeyGen}(\lambda)$

1: Perform s random isogeny walks ϕ_m of degree S_1 from E_0 to curves $E_{A,m}$ with j-invariant $j_{A,m}$, where $m \in \{0, 1, ..., s-1\}$.
2: Compute the ideal $I_{A,m}$ corresponding to each isogeny.
3: Compute $\mathcal{O}_{A,m} = \mathrm{End}(E_{A,m})$.
4: $pk \leftarrow (j_{A,0}, j_{A,1}, .., j_{A,s-1})$.
5: $sk \leftarrow (I_{A,0}, I_{A,1}, ..., I_{A,s-1})$ or $(\mathcal{O}_{A,0}, \mathcal{O}_{A,1}, ..., \mathcal{O}_{A,s-1})$.
6: **return** (pk, sk).

Since we set the challenge bit to be $\log s$, we compute s isogenies during the generation of the public and secret keys. This key generation procedure can be

Algorithm 2 $\mathsf{Sign}(sk, m)$

for $i = 1$ to t **do**
  Perform a random isogeny walk w_i of degree S_2 from E_0 to $E_{B,i}$ with j-invariant $j_{B,i}$, and compute the corresponding ideal $I_{B,i}$.
  Compute the hash value $h = H(m, j_{B,1}, j_{B,2}, .., j_{B,t})$ and set $h \leftarrow b_1||b_2||...||b_t$, where $b_i \in \{0, 1, ..., s-1\}$.
end for
for $i = 1$ to t **do**
  Compute the dual isogeny $\hat{\phi}_{b_i}$ and the corresponding ideal I_{A,b_i}^{-1}.
  On input $I_{A,b_i}^{-1} I_{B,i}$ and $\mathcal{O}_{A,b_i}$, perform the modified quaternion isogeny path algorithm to produce a new ideal J_i between $\mathcal{O}_{A,b_i}$ and $\mathcal{O}_{B,i}$. Then translate J_i to an isogeny w_i' between j_{A,b_i} and $j_{B,i}$.
  Set $z_i \leftarrow w_i'$.
end for
The signature is $\sigma = (h, z_1, z_2, ..., z_t)$.

Algorithm 3 $\mathsf{Verify}(pk, m, \sigma)$

for $i = 1$ to t **do**
  Use z_i to compute the image curve $j_{B,i}$ from j_{A,b_i}.
end for
Then compute $h' \leftarrow H(m, j_{B,1}, j_{B,2}, ..., j_{B,t})$.
if $h' = h$ **then**
  return 1.
end if

performed in advance. Although the public and secret keys can be generated offline, the number s cannot be too large, or else large storage will be needed. An illustration of how to generate the key pairs is presented in Figure 2. The path can be represented by the isogeny between two j-invariants of curves or the ideal connecting two endomorphism rings. By taking $B = 2(1+\epsilon)\log p$, we can guarantee that the output of random walks is uniformly distributed as proved in [10].

During the Sign step, the commitments of our scheme are different from those in [10]. We perform the isogeny from j_0 to j_B but not from j_A to j_B. As the number of j_A's is s, there would be $s \cdot t$ isogenies to be computed which costs too much. So we use instead the path from j_0 to j_B. In this case additional dual isogenies and the inverse of ideals have to be computed, but it is not hard to do that. As for the z_i's, since an isogeny can be determined by its kernel point and the Montgomery curve has a special structure in $\mathbb{P}_1$, each z_i can be set as the x-coordinate of R_i where $\ker w_i' = \langle R_i \rangle$. For the i-th round, we clarify in Figure 3 how to find a new path J_i.

Efficiency. We provide a rough estimate for the parameters and efficiency for our version of the signature scheme. For classical security, we choose $\log p = 2\lambda$. For λ bits of security, we set $t = \lambda / \log s$. The uniform distribution of random

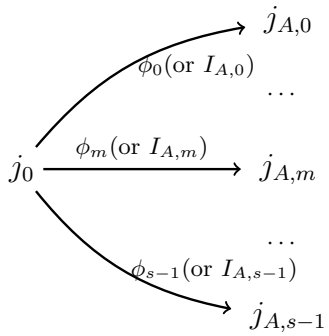

Fig. 2: Illustration of KeyGen.

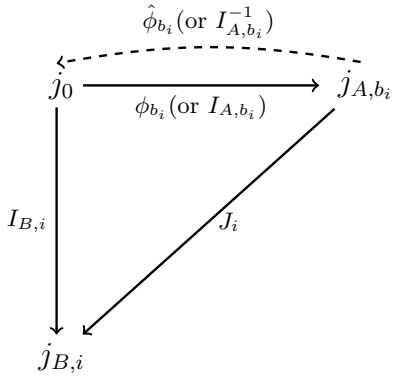

Fig. 3: Find one new path for the i-th parallel round.

walk output requires that the output walk has length $2(1+\varepsilon)\log p \approx 4\lambda$ in GPS signatures, and the public keys are 6λ bits. Hence, in our multi-bit signature, if s isogeny walks are computed, then the size of the private key and public key increases by a factor of s. The average size of our signature is $\lambda + \frac{\lambda}{\log s}(2(1+\varepsilon)\log p) \approx \frac{4}{\log s}\lambda^2$. We mention that the verification of GPS signature and ours both have a cost about $\mathcal{O}(\lambda^4)$ bit operations, but not $\mathcal{O}(\lambda^6)$ bit operations as stated in [10]. We only require $\lambda/\log s$ calls to the four key algorithms in the GPS scheme, which reduces the overall cost by a factor of $\log s$. An asymptotic comparison between GPS signatures and ours is listed in Table 1, and a concrete comparison in Table 2 using $\log s = 8$. By contrast, the shorter signature version of Seasign [6] uses $\log s = 16$. If we also take $\log s = 16$, the signature size will be halved, but the size of private and public key will be quite large.

Table 1: Comparison about Galbraith-Petit-Silva endomorphism ring signature [10] with ours in key size and cost. "$\log s$" is the challenge bit and it is a positive integer.

Scheme	**Private Key**	**Public key**	**Signature size**	**Sign cost**	**Verify cost**
GPS17 [10]	4λ	6λ	$\frac{11}{2}\lambda^2$	$\mathcal{O}(\lambda^6)$	$\mathcal{O}(\lambda^4)$
Ours	$4s\lambda$	$4s\lambda$	$\frac{4}{\log s}\lambda^2$	$\mathcal{O}(\lambda^6)$	$\mathcal{O}(\lambda^4)$

Security. Recall that the signature is accepted if and only if for every step, the prover can find a path that leads to a curve with the correct j-invariant. To ensure that the scheme is secure, the probability of each potential j must be nearly uniformly likely to be the j-invariant of the resulting curve. The random

Table 2: A concrete efficiency comparison at the security level of 128 bits and we choose our challenge bit $\log s = 8$. These sizes are all counted in bytes. We list the performance of the shorter signature version of SeaSign [6].

Scheme	**Private Key**	**Public key**	**Signature size**
GPS17 [10]	64	96	11264
SeaSign[6]	16	$4032 \cdot 10^3$	944
Ours	16384	16384	1024

walk theorem proven in [10] states that for every j-invariant $\tilde{j}$ we have

$$|Pr[j = \tilde{j}] - \frac{1}{N_p}| \leq \prod_{i=1}^{r} \left(\frac{2\sqrt{\ell_i}}{\ell_i + 1} \right)^{e_i},$$

where N_p is the number of all supersingular j-invariants over $\mathbb{F}_{p^2}$. In order to make the isogeny path random, the right-hand term of the above formula should be smaller than $(p^{1+\epsilon})^{-1}$ for any positive ϵ. We guarantee this in our parameters by using $B = 2(1+\epsilon)\log p$.

The single-bit version of the GPS signature scheme has been proved to be secure in the random oracle model under a chosen message attack in Theorem 10 of [10], if Problem 1 is computationally hard. For the multi-bit version, the signature derived from the non-trivial canonical recoverable identification still works. But we can also consider the security reduction from another perspective. We treat this signature with multi-bit challenges as a kind of multi-signature, but in the case that the only one signer has multiple public keys signing one message. This idea is inspired by the smaller signature version of SeaSign.

We recall the forking lemma from Bellare and Neven [2].

Lemma 1. *Fix an integer $q \geq 1$. Let A be a randomized algorithm that takes input $h_1, \ldots, h_q \in \{0,1\}^t$ and outputs (J, σ) where J is an integer $1 \leq J \leq q$ with probability γ. The forking algorithm proceeds as follows: $h_1, \ldots, h_q$ are chosen randomly in $\{0,1\}^t$. $A(h_1, \ldots, h_q)$ outputs (J, σ) with $J \geq 1$. Then randomly choose $h'_J, \ldots, h'_q \in \{0,1\}^t$. $A(h_1, \ldots, h_{J-1}, h'_J, \ldots, h'_q)$ outputs (J', σ'). Then the probability that $J = J'$ and $h'_J \neq h_J$ is larger than $\gamma(\frac{\gamma}{q} - \frac{1}{2^t})$.*

Note that by the forking lemma, there are two signatures for some $b_k \neq b'_k$. Hence we can get two paths J'_k and J_k to j_{B_k} from j_{A,b'_k} and j_{A,b_k}, respectively. So $(J'_k)^{-1}J_k$ is the path from j_{A,b_k} to j_{A,b'_k}. Therefore, we propose a new assumption for our multi-bit signature scheme.

Problem 4 *Given $\{j_{A,0}, .., j_{A,s-1}\}$, produced by performing s random isogeny walks of degree ℓ^e from E_0 with j-invariant j_0, compute an ideal I corresponding to an isogeny $E_{A,m} \to E_{A,m'}$ with j-invariants $j_{A,m}$ and $j_{A,m'}$ for $m \neq m'$.*

This problem can be easily reduced to Problem 3. If Problem 3 is solved, then we can compute the endomorphism rings $\mathcal{O}_{A,m}$ and $\mathcal{O}_{A,m'}$ corresponding to $j_{A,m}$

and $j_{A,m'}$, respectively. Then we compute an ideal I which is a left $\mathcal{O}_{A,m}$-ideal and its right order is isomorphic to $\mathcal{O}_{A,m'}$ for $m \neq m'$. The quaternion isogeny path algorithm will now work to find an isogeny path between curves $E_{A,m}$ and $E_{A,m'}$. The main reduction is given in Algorithm 9 in [7].

Theorem 2. *If Problem 4 is computationally hard, then our multi-bit challenge signatures are existentially unforgeable under chosen-message attacks in the random oracle model.*

Proof (sketch). Suppose there is a probabilistic polynomial time adversary $\mathcal{A}$ against the signature. Then the public key is known to $\mathcal{A}$, and $\mathcal{A}$ can query the hash function H and the signing oracle $\mathcal{O}_{sign}$. Suppose the adversary $\mathcal{A}$ can make at most q hash oracle queries and n signing oracle queries. In order to simulate the random oracles, $\mathcal{A}$ should maintain the hash list L_H and the signature list L_{sign} corresponding to the queries and answers of the H-oracle and $\mathcal{O}_{sign}$.

Querying H-oracle with $(m, j_1, \ldots, j_t)$: If there exists $(m, j_1, \ldots, j_t, h) \in L_H$ then return h. Otherwise, $\mathcal{A}$ randomly chooses h, returns h and records $(m, j_1, \ldots, j_t, h)$ in L_H.

Querying $\mathcal{O}_{sign}$ with message m: The simulator chooses random bit-string $b_1, \ldots, b_t \in \{0, 1, \ldots, s-1\}$. For $i = 1, \ldots, t$, the simulator computes a random isogeny walk z_i from E_0 to $E_{B,i}$. We update the hash list that $H(m, j_{B,1}, \ldots, j_{B,t}) = b_1 \ldots b_t$, unless the random oralce has already been defined on this input in which case the simulation fails. Then return and record $(b_1 \ldots b_t, z_1, \ldots, z_t)$ in the list L_{sign}. This simulation fails at a negligible probability according to the above random walk theorem. Hence, the output is a valid signature and is indistinguishable from the real signature.

We consider the case that when the adversary replays the same tape, one of the hash queries is answered with a different binary string. With non-negligible probability $\mathcal{A}$ outputs a forgery $(b'_1 \ldots b'_t, z'_1, \ldots, z'_t)$ for the same message m and the same $(m, j_{B,1}, \ldots, j_{B,t})$ to H with a output $b'_1 \ldots b'_t$. Without loss of generality, we assume that $b_k \neq b'_k$. Then the isogeny paths z_k from $\mathcal{O}_{A,k}$ to $\mathcal{O}_{B,k}$ and z'_k from $\mathcal{O}_{A,k'}$ to $\mathcal{O}_{B,k'}$ with $\mathcal{O}_{B,k} = \mathcal{O}_{B,k'}$ are such that $(z'_k)^{-1} z_k$ is a solution to Problem 4.

4 Analysis and Implementation of Galbraith-Petit-Silva Signature

Parameters. We first choose an odd and power-smooth number $n = \prod_{i=1}^{r} \ell_i$ such that $p = 4n - 1$ is a prime. These ℓ_i are selected as distinct odd primes; a straightforward way is to choose n as the product of the first few primes. For example, we take $n = 3 \times 5 \times 7$ and then $p = 419$ is prime. Table 3 shows the primes that we adopt, where the notion $[a, b]$ means all primes in the range $[a, b]$ and $[a, b] + [c]$ means all primes $[a, b]$ along with c. The global curve E_0 is chosen

Table 3: The choice of the global parameters.

n	Notation	$\log_2 p$
$3 \times 5 \times 7$	$[3, 10]$	8.711
$3 \times 5 \times \cdots \times 19$	[3,20]	24.210
$3 \times 5 \times \cdots \times 43 \times 97$	$[3, 43] + [97]$	61.138
$3 \times 5 \times \cdots \times 113$	$[3, 113]$	155.469
$3 \times 5 \times \cdots \times 373 \times 587$	$[3, 373] + [587]$	510.668

as $y^2 = x^3 + x$ over $\mathbb{F}_{p^2}$ with the initial j-invariant 1728 and the endomorphism ring $\mathcal{O}_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \rangle$.

There are four main algorithms invovled in the signature scheme, including loading isogenies, translating the isogeny to the ideal, finding a new ideal, and translating the new ideal to the isogeny. The loading isogenies algorithm inherits the strategy of SIDH to run in a sequential manner. To be precise, suppose that the degree of an isogeny is $\prod_{i=1}^{r} \ell_i^{e_i}$; then we split it into e_i successive ℓ_i-isogenies for every i.

Minkowski Basis Computation. Up to dimension four basis, Minkowski is arguably optimal compared to all other known reductions, since it can reach all the so-called successive minima. Given a basis $\{v_1, v_2, \ldots, v_n\}$, v_i must have a norm smaller or equal to $v_i + \sum_{j=1, j\neq i}^{n} a_j v_j$ for any combinations of integers a_j in the Minkowski-reduced basis. In the quaternion algebra setting, we focus on the $n = 4$ case. We set $i = 1$ for illustration purposes here. Denote by v_{ij} the j-th coordinate of the vector v_i. We have

$$||v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4|| = \sum_{j=1}^{4} s_j (v_{1j} + a_2 v_{2j} + a_3 v_{3j} + a_4 v_{4j})^2$$

where $s_1 = s_2 = 1$ and $s_3 = s_4 = p$. In the quaternion algebra, the inner product of two elements $v_1 + v_2 i + v_3 j + v_4 k$ and $w_1 + w_2 i + w_3 j + w_4 k$ is $v_1 w_1 + v_2 w_2 + p v_3 w_3 + p v_4 w_4$. Then for each $k = 2, 3, 4$ we have

$$\begin{aligned} \frac{d}{da_k} ||v_1 + a_2 v_2 + a_3 v_3 + a_4 v_4|| &= \sum_{j=1}^{4} 2 v_{kj} s_j (v_{1j} + a_2 v_{2j} + a_3 v_{3j} + a_4 v_{4j}) \\ &= 2(\boldsymbol{v_k} \cdot \boldsymbol{v_1} + a_2 \boldsymbol{v_k} \cdot \boldsymbol{v_2} + a_3 \boldsymbol{v_k} \cdot \boldsymbol{v_3} + a_4 \boldsymbol{v_k} \cdot \boldsymbol{v_4}). \end{aligned}$$

When a_2, a_3, a_4 are the numbers that give the minimal possible norm, we have

$$\begin{pmatrix} \boldsymbol{v_2} \cdot \boldsymbol{v_1} \\ \boldsymbol{v_3} \cdot \boldsymbol{v_1} \\ \boldsymbol{v_4} \cdot \boldsymbol{v_1} \end{pmatrix} + a_2 \begin{pmatrix} \boldsymbol{v_2} \cdot \boldsymbol{v_2} \\ \boldsymbol{v_3} \cdot \boldsymbol{v_2} \\ \boldsymbol{v_4} \cdot \boldsymbol{v_2} \end{pmatrix} + a_3 \begin{pmatrix} \boldsymbol{v_2} \cdot \boldsymbol{v_3} \\ \boldsymbol{v_3} \cdot \boldsymbol{v_3} \\ \boldsymbol{v_4} \cdot \boldsymbol{v_3} \end{pmatrix} + a_4 \begin{pmatrix} \boldsymbol{v_2} \cdot \boldsymbol{v_4} \\ \boldsymbol{v_3} \cdot \boldsymbol{v_4} \\ \boldsymbol{v_4} \cdot \boldsymbol{v_4} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This can be solved as

$$\begin{pmatrix} a_2 \\ a_3 \\ a_4 \end{pmatrix} = - \begin{pmatrix} \boldsymbol{v_2 \cdot v_2} & \boldsymbol{v_2 \cdot v_3} & \boldsymbol{v_2 \cdot v_4} \\ \boldsymbol{v_3 \cdot v_2} & \boldsymbol{v_3 \cdot v_3} & \boldsymbol{v_3 \cdot v_4} \\ \boldsymbol{v_4 \cdot v_2} & \boldsymbol{v_4 \cdot v_3} & \boldsymbol{v_4 \cdot v_4} \end{pmatrix}^{-1} \begin{pmatrix} \boldsymbol{v_2 \cdot v_1} \\ \boldsymbol{v_3 \cdot v_1} \\ \boldsymbol{v_4 \cdot v_1} \end{pmatrix}.$$

The resulting a_2, a_3, a_4 might not be integers and we can replace them by the nearest integers. After finding the optimal $v_1 + a_2v_2 + a_3v_3 + a_4v_4$, we replace v_1 with this expression and repeat this procedure for all $i = 1, 2, 3, 4$. This Minkowski method manages to bring N down to $p^{0.5+o(1)}$ in the finding new path algorithm.

Improvements for Isogeny-to-Ideal. First we recall the runtime analysis of this algorithm given by Galbraith-Petit-Silva. This algorithm finds a point Q_i of order $\ell_i^{e_i}$ that generates the kernel of ϕ_i by considering the kernel polynomial ψ_i of the $\ell_i^{e_i}$-isogeny which takes a total of $\ell_i^{e_i}$ steps. The next step is to find $\alpha_i \in I$ satisfying $\alpha_i Q_i = \infty$, where I is the ideal generated in the previous step. The algorithm identifies the basis $\beta_1, \beta_2, \beta_3, \beta_4$ of I and tries a random solution to $\alpha = \omega\beta_1 + x\beta_2 + y\beta_3 + z\beta_4$ by setting ω, x, y randomly to see if there is a z satisfying this condition. The new ideal is the set as $I_{i-1}\ell_i^{e_i} + \mathcal{O}_0\alpha_i$. This involves an average of $\ell_i^{e_i}$ tries to find the suitable α and computing αQ_i takes $\mathcal{O}(\log^2 p)$ bit operations.

Next, the algorithm needs to perform point halving due to the fact that the coefficient of elements in the associated ideal can be non-integer, with denominator at most 2. Nevertheless, the original algorithm chooses points that have odd order N. For each a we have $\frac{a}{2} \equiv a(\frac{N+1}{2}) \mod N$ and so for each point P of order N we have $\frac{a}{2}P \equiv a(\frac{N+1}{2})P$. Thus we save the cost of point halving.

The main improvement comes from the step of finding ω, x, y, z satisfying $(\omega\beta_1 + x\beta_2 + y\beta_3 + z\beta_4)Q_i = \infty$. We can break down the $\ell_i^{e_i}$ tries into solving a modular ℓ_i equivalence for e_i times. When at step j, we want $\alpha(\ell_i^{e_i})Q_i = \infty$, or in other words $\omega(\ell_i^{e_i-j})P_1 + x(\ell_i^{e_i-j})P_2 + y(\ell_i^{e_i-j})P_3 + z(\ell_i^{e_i-j})P_4 = \infty$, where $P_i = \beta_i Q_i$ for $i = \{1, 2, 3, 4\}$. The procedure goes as follows at each step j:

1. Set $S = \omega(\ell_i^{e_i-j})P_1 + x(\ell_i^{e_i-j})P_2 + y(\ell_i^{e_i-j})P_3 + z(\ell_i^{e_i-j})P_4$. Notice that S has order either 1 or ℓ_i. This is true if $j = 1$, and for $j > 1$ it follows from the loop invariant that we had $\omega(\ell_i^{e_i-j+1})P_1 + x(\ell_i^{e_i-j+1})P_2 + y(\ell_i^{e_i-j+1})P_3 + z(\ell_i^{e_i-j+1})P_4 = \infty$ from the previous step.
2. Choose ω', x', y' randomly from $\{0, 1, \ldots, \ell_i\}$. In the case of $j = 1$, care must be taken so that not all ω', x', y' are divisible by ℓ_i.
3. Consider the point $T = S + \omega'(\ell_i^{e_i-1})P_1 + x'(\ell_i^{e_i-1})P_2 + y'(\ell_i^{e_i-1})P_3$, and see whether T and $(\ell_i^{e_i-1}P_4)$ are linearly dependent in the ℓ_i torsion space. If so, solve for $T + z'(\ell_i^{e_i-1})P_4 = \infty$. Otherwise, repeat the loop.
4. Now that $S + \omega'(\ell_i^{e_i-1})P_1 + x'(\ell_i^{e_i-1})P_2 + y'(\ell_i^{e_i-1})P_3 + z'(\ell_i^{e_i-1})P_4 = \infty$, we update $\omega = \omega + \omega'(\ell_i^{j-1}), x = x + x'(\ell_i^{j-1}), y = y + y'(\ell_i^{j-1}), z = z + z'(\ell_i^{j-1})$. This update gives $\omega(\ell_i^{e_i-j})P_1 + x(\ell_i^{e_i-j})P_2 + y(\ell_i^{e_i-j})P_3 + z(\ell_i^{e_i-j})P_4 = \infty$.

Improvements for Ideal-to-Isogeny. If we just translate the original ideal with a small norm, but not the newly-generated ideal from the quaternion isogeny path algorithm, Algorithm 2 in [10] can work out the correct isogeny path. But if we want to translate the new ideal with a large norm, we have to modify some steps. For example, if we take the prime $p = 4 \cdot 3 \cdot 5 \cdot 7 - 1$, we can produce a new ideal with norm $3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23$. If we then want to translate this new ideal back to an isogeny, we first have to compute bases for the $3^2, \ldots, 23$ torsion. However, all of these torsion points are no longer defined on $\mathbb{F}_{p^2}$, but over large extension fields.

We discuss the details and complexities of the ideal-to-isogeny algorithm that involves constructing torsion subgroups and their associated finite field extensions. Recall that the ideal J returned by the quaternion isogeny path algorithm has a norm of S which may be divisible by prime powers. Write the norm of ideal J as $n = \prod_{i=1}^{r} \ell_i^{e_i}$. In order to construct the isogeny ϕ corresponding to J, we must construct a point P_i for each prime power dividing n. Then a generator of the kernel of ϕ is the point $\sum_{i=1}^{r} P_i \in E_0(\overline{\mathbb{F}})$. The required torsion subgroups fall into two main types:

1. $\ell_i^{e_i} \mid p + 1$,
2. $\ell_i^{e_i} \nmid p + 1$.

For the type 1, torsion subgroups will exist in $E_0(\mathbb{F}_{p^2})$. For the other type of prime powers we will need to work over some extension field $\mathbb{F}_{p^d}$ for $d \in \mathbb{N}$. We now examine how to determine d explicitly in this type. Fix $\ell^e = \ell_i^{e_i}$ for simplicity. The x-coordinates of the ℓ^e-torsion points are the roots of the division polynomial $\psi_{\ell^e}(x)$. While this polynomial has degree $\frac{\ell^{2e}-1}{2}$ for odd ℓ and is guaranteed to split over an extension of that degree, the minimal extension we are required to work over may be smaller. We determine the extension degree d as follows: factor $\psi_{\ell^e}(x)$ over $\mathbb{F}_p$ and set d_0 to be the lowest common multiple (LCM) of the degrees of each factor.

For the type 2, we still have two cases to discuss. One case can be $d = 2d_0$ if $\ell^{2e} \mid \#E_0(\mathbb{F}_{p^{2d_0}})$. This is due to the fact that the y-coordinates are required to solve $y^2 = x^3 + x$ and therefore should be defined over a quadratic extension of the field containing x. For the other case, we set $d = 4d_0$through experimental observation.

Once the extension d is determined for $E_0[\ell^e]$, we turn to solving for the kernel point $P \in E_0[\ell^e]$. The procedure is to find a basis for $E_0[\ell^e]$, and then solve for P (see [10, §4.4]).

The final step is to determine the isogeny with kernel $\langle \sum_{i=1}^{r} P_i \rangle \subset E_0(\overline{\mathbb{F}}_p)$. Suppose each point P_i is defined over an extension of degree d_i, $1 \leq i \leq r$. If we naively add all the points P_i together then we would end up in an extension of degree $\mathrm{LCM}\{d_i : 1 \leq i \leq r\}$. Instead we propose a new method which only requires arithmetic in an extension of degree $\max\{d_i : 1 \leq i \leq r\}$, using the fact that all supersingular elliptic curves have j-invariants in $\mathbb{F}_{p^2}$.

For each $1 \leq i \leq r$:

Table 4: The performance of these main algorithms in Galbraith-Petit-Silva signature [10]. "LI" represents loading the isogeny chains. "Is-to-Id" means translation from an isogeny to an ideal. "Id-to-Is" means translation from an ideal to an isogeny and this ideal is not the newly-generated one by the quaternion isogeny path algorithm, but just the ideal after "Is-to-Id". "New-Path" means the quaternion isogeny path algorithm. These times are listed in seconds.

n	$\log_2 p$	LI	Is-to-Id	Id-to-Is	New-Path
$[3, 10]$	8.711	0.100	0.0734	0.064	0.109
$[3, 20]$	24.210	0.217	0.2146	0.366	0.190
$[3, 43] + [97]$	61.138	1.000	1.356	0.883	0.492
$[3, 113]$	155.469	6.356	9.442	6.989	2.297
$[3, 373] + [587]$	510.668	174.917	126.520	173.020	45.270

1. construct the isogeny $\phi_i \colon E_{i-1} \to E_i'$ with kernel $\langle P_i \rangle$,
2. compute the j-invariant $j_i = j(E_i')$,
3. construct the elliptic curve E_i with j-invariant j_i and coefficients in $\mathbb{F}_{p^2}$,
4. construct the isomorphism $f_i \colon E_i' \to E_i$,
5. set $P_{i+1} \leftarrow f_i(\phi_i(P_i))$.

Performance. We implemented the main algorithms from the GPS signature scheme using Sage [18] and ran it on the cloud platform CoCalc for demonstrative purposes. We choose five values of n that make p prime. The results are listed in Table 4. It should be pointed out that translation from the new ideal to an isogeny is not included in this table, as we were not able to run it to completion.

When we attempt to implement translation from the new ideal to an isogeny, we have to generate these new large torsion points. First, we find the smallest extension fields containing these points. For example, when $p = 4 \cdot 3 \cdot 5 \cdot 7 - 1$, the new ideal produced by the quaternion isogeny path algorithm has a norm of $3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23$. All these torsion points are not so large, except for the 13^2-torsion point. The smallest extension field containing the 13^2-torsion points is $\mathbb{F}_{p^{156}}$, too big for Sage to manage in this computation, despite the fact that these torsion points can be precomputed in advance. We emphasize that the security level of this p is only 8.711 bits, which is obviously well short of cryptographic size. When we set $p = 4 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 - 1$, the new ideal norm will be $3^2 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19^2 \cdot 23^2 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 59$. The largest extension in this case is determind by the 23^2-torsion points. We tested it using Magma and found that the smallest extension degree needs to be $\mathbb{F}_{p^{1012}}$ in this case, which will be very expensive.

5 Conclusion

Our efforts to implement GPS signatures indicate that the scheme is impractical for parameters of cryptographic size. Translation from the new ideal to a new

Table 5: Torsion generation in translation from the new ideal to an isogeny. This is the case of $p = 4 \cdot 3 \cdot 5 \cdot 7 - 1$. "$i$-th torsion" means the order of the torsion point we compute. "Extension field" means the smallest field that the torsion point is defined over. "Time" is counted by seconds.

i-th torsion	Extension field	Time
3^2	$\mathbb{F}_{p^{12}}$	0.1452
5^2	$\mathbb{F}_{p^{20}}$	0.2517
7^2	$\mathbb{F}_{p^{28}}$	0.4287
11^2	$\mathbb{F}_{p^{88}}$	1.5817
13^2	$\mathbb{F}_{p^{156}}$	125.6406
17	$\mathbb{F}_{p^{32}}$	0.4609
19	$\mathbb{F}_{p^4}$	0.0584
23	$\mathbb{F}_{p^{44}}$	1.5015
29	$\mathbb{F}_{p^{28}}$	0.3422

isogeny is not as easy as indicated in the Ideal-to-Isogeny algorithm in [10]. Particular care needs to be taken to control the explosion of extension field degree in the computation of the torsion points. In addition, we also propose a variant signature scheme with multi-bit challenges that has smaller signature sizes and lower computational cost, at the expense of a large public key, but even ignoring the extra costs of our modified quaternion isogeny path algorithm, the scheme is still impractical even with these improvements unless all the necessary torsion points are precomputed in advance. Further efforts are still needed to make signatures based on endomorphism ring more viable at useful parameter sizes.

Acknowledgments. The authors would like to thank the anonymous reviewers for their detailed reviews and helpful comments. This work is supported by the National Natural Science Foundation of China (No.61872442, No. 61502487) and the National Cryptography Development Fund (No. MMJJ20180216), as well as NSERC, CryptoWorks21, Public Works and Government Services Canada, Canada First Research Excellence Fund, and the Royal Bank of Canada. Furthermore, Xiu Xu acknowledges the scholarship provided by the China Scholarship Council.

References

1. Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred J. Menezes, and Francisco Rodríguez-Henríquez. On the cost of computing isogenies between supersingular elliptic curves. In Carlos Cid and Michael J. Jacobson Jr., editors, *Selected Areas in Cryptography — SAC 2018*, pages 322–343, Cham, 2019. Springer International Publishing.
2. Mihir Bellare and Gregory Neven. Multi-signatures in the plain public-key model and a general forking lemma. In *Proceedings of the 13th ACM Conference on*

Computer and Communications Security, CCS '06, pages 390–399, New York, NY, USA, 2006. ACM.
3. Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, Jan 2009.
4. Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of the computational supersingular isogeny problem. Cryptology ePrint Archive, Report 2019/298, 2019. `https://eprint.iacr.org/2019/298`.
5. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.
6. Luca De Feo and Steven D. Galbraith. Seasign: Compact isogeny signatures from class group actions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology — EUROCRYPT 2019*, pages 759–789, Cham, 2019. Springer International Publishing.
7. Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology — EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.
8. Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3), January 2014.
9. Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology — ASIACRYPT 2016*, pages 63–91, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg.
10. Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology — ASIACRYPT 2017*, pages 3–33, Cham, 2017. Springer International Publishing.
11. Steven D. Galbraith and Frederik Vercauteren. Computational problems in supersingular elliptic curve isogenies. *Quantum Information Processing*, 17(10):265, Aug 2018.
12. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *Post-Quantum Cryptography*, pages 19–34, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.
13. David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.
14. David Kohel, Kristin E. Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.
15. Vadim Lyubashevsky. Fiat-shamir with aborts: Applications to lattice and factoring-based signatures. In Mitsuru Matsui, editor, *Advances in Cryptology — ASIACRYPT 2009*, pages 598–616, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.
16. Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the l-isogeny path problem. In *Proceedings of MATHCRYPT 2018*, 2018.
17. Anton Stolbunov. *Cryptographic schemes based on isogenies*. PhD thesis, Norwegian University of Science and Technology, 2012.
18. The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.5)*, 2019. `https://www.sagemath.org`.

19. Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.
20. Youngho Yoo, Reza Azarderakhsh, Amir Jalali, David Y. Jao, and Vladimir Soukharev. A post-quantum digital signature scheme based on supersingular isogenies. In Aggelos Kiayias, editor, *Financial Cryptography and Data Security*, pages 163–181, Cham, 2017. Springer International Publishing.