ON THE KEY GENERATION IN SQISIGN

HIROSHI ONUKI

Department of Mathematical Informatics, The University of Tokyo, Japan
ORCID 0000-0002-0202-8918 E-mail: onuki@mist.i.u-tokyo.ac.jp

Abstract. SQISign is an isogeny-based signature scheme that has short keys and signatures and is expected to be a post-quantum scheme. Its security depends on the hardness of the problem to find an isogeny between given two elliptic curves over $\mathbb{F}_{p^2}$, where p is a large prime. For efficiency reasons, a public key in SQISign is taken from a set of supersingular elliptic curves with a particular property. In this paper, we investigate the security related to public keys in SQISign. First, we show some properties of the set of public keys. Next, we show that a key generation procedure used in implementing SQISign could not generate all public keys and propose a modification for the procedure. In addition, we confirm the latter result through an experiment.

1. Introduction. The study of post-quantum cryptography (PQC) is increasingly important due to the rapid progress in quantum computers. Isogeny-based cryptography is one of the candidates for PQC and attracts attention because of its short keys and ciphertext. Indeed, SIKE [JAC+], an isogeny-based KEM, is one of the round 4 submissions to the NIST PQC standardization process [NIS].

Isogeny-based cryptography is based on the hardness of a problem to find a secret isogeny between given two elliptic curves. Many isogeny-based key exchanges and encryption schemes are known, for example, [Cou06, RS06, JDF11, CLM+18]. On the other hand, a practical signature scheme based on isogenies was not known until recently. In 2019, Beullens, Kleinjung, and Vercauteren [BKV19] proposed an isogeny-based signature scheme CSI-FiSh, with short keys and signatures. However, CSI-FiSh needs a subexponential computational effort to generate public parameters. As a result, its currently known parameter is only for 128 bits security.

SQISign is an isogeny-based signature scheme proposed by De Feo, Kohel, Leroux, Petit, and Wesolowski [DFKL+20a] in 2020. It has shorter keys and signatures, and its

2020 *Mathematics Subject Classification*: Primary 11T71 Secondary 94A60
Key words and phrases: post-quantum cryptography, isogenies, supersingular elliptic curves
The paper is in final form and no version of it will be published elsewhere.

validation of signatures is faster than CSI-FiSh. In particular, the total public key and signature size of SQISign is five times shorter than that of CSI-FiSh in 128 bits security. However, SQISign needs about the same time for generating a signature as CSI-FiSh. For security, SQISign assumes a new computational hardness related to isogenies, and validation of its hardness seems to need more research.

Furthermore, SQISign takes its public keys from supersingular elliptic curves with a particular property to shorten the signature size and accelerate the signing. In particular, a public key in SQISign is a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ such that there exists an isogeny $E_0 \to E$ of a prime degree less than $p^{1/4}$, where E_0 is a public parameter and is the curve with j-invariant 1728. There are no studies on whether the isogeny-finding problem between such E and E_0 is as difficult as the problem for random curves over $\mathbb{F}_{p^2}$.

1.1. Contributions. This paper discusses the security of the key generation in SQISign.

First, we investigate the properties of public keys in SQISign as supersingular elliptic curves. Let E_0 and E be as above. Then there exists an isogeny $E_0 \to E$ of a prime degree N. We show the following:

- The degree of an isogeny $E_0 \to E$ prime to N is greater than $p^{3/4}/4$. This means that E is relatively far from E_0 in isogeny graphs.
- The probability that E is defined over $\mathbb{F}_p$ is greater than $1/(p^{1/4}+1)$, much higher than that of a random supersingular elliptic curve $\mathbb{F}_{p^2}$.

The former ensures a certain lower bound of the computational cost of an attack. On the other hand, the latter shows that E tends to be weak against an attack. Nevertheless, this weakness is easily avoidable by discarding curves over $\mathbb{F}_p$ from public keys.

Next, we analyze the key generation procedure proposed in [DFKL+20b, Supplementary Material D], which accelerates the key generation. We show that this procedure could not generate all public keys and confirm that by an experiment. In addition, we propose a modification for this procedure, which has a small overhead and is expected to generate all public keys uniformly.

2. Preliminary. We recall the mathematical background of SQISign. We refer the reader to [Sil09] for elliptic curves and isogenies and [Voi21] for quaternion algebras.

2.1. Isogenies. An *isogeny* is a nonzero rational group homomorphism between elliptic curves. Let E and E' be elliptic curves over a field K. An isogeny $\varphi : E \to E'$ induces a map $\varphi^* : \overline{K}(E') \to \overline{K}(E)$ defined by $\varphi^*(f) = f \circ \varphi$, where $\overline{K}$ is an algebraic closure of K, and $\overline{K}(E)$ and $\overline{K}(E')$ are the function fields of E and E', respectively. The *degree* of φ is the degree of field extension $\overline{K}(E)/\varphi^*(\overline{K}(E'))$ and is denoted by $\deg \varphi$. We say φ is *separable* (resp. *inseparable*) if this extension is *separable* (resp. *inseparable*). There exists a unique isogeny $\psi : E' \to E$ such that $\psi \circ \varphi$ and $\varphi \circ \psi$ are the multiplication by $\deg \varphi$ on E and E', respectively. We call this the *dual isogeny* of φ and denote it by $\hat{\varphi}$.

The kernel of an isogeny is a finite group, and the order of the kernel is equal to the degree of the isogeny if the isogeny is separable. Conversely, for an elliptic curve E and its finite subgroup G, there exists a separable isogeny with kernel G. This isogeny is

unique up to isomorphism on its codomain. We denote the codomain by E/G. Given E and G, we can compute E/G by using Vélu's formula [Vél71]. It takes $O(\#G)$ operations on the field of definition of E and G by classical method and $\tilde{O}(\sqrt{\#G})$ by improvement [BDFLS20].

For an elliptic curve E, an *endomorphism* on E is an isogeny or the zero map from E to E. The set of endomorphisms on E forms a ring by the addition on E and the composition of maps. We call this ring the *endomorphism ring* of E and denote it by $\mathrm{End}(E)$.

2.2. Isogeny Problems. We are interested in the following problem.

Problem 1. Given two supersingular elliptic curves E_1 and E_2 over $\mathbb{F}_{p^2}$, find an isogeny from E_1 to E_2.

Isogeny-based cryptography is based on the hardness of this problem, i.e., it is considered that this problem cannot be solved in polynomial time in $\log p$ even by using a quantum computer. We add some conditions to the input and the output in individual protocols.

Problem 1 can be solved in $\tilde{O}(p)$ operations on $\mathbb{F}_{p^2}$ by a brute-force attack since the number of supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to isomorphism is $\lfloor \frac{p}{12} \rfloor + \varepsilon$, where $\varepsilon = 0, 1, 2$ depending on $p \bmod 12$. In particular, a random walk from E_1 (a composition of isogenies of a small degree) is expected to meet E_2 after $O(p)$ steps. Some algorithms improve the computational complexity from $\tilde{O}(p)$ to $\tilde{O}(p^{1/2})$. We focus on the following two algorithms in this paper.

2.2.1. *Meet-in-the-Middle algorithm* [Gal99]. This algorithm is based on the birthday paradox. To solve Problem 1, one makes distinct $p^{1/2}$ isogenies from E_1 and E_2. These isogenies include isogenies φ from E_1 and ψ from E_2 of the same codomain with a high probability. The composition $\hat{\psi} \circ \varphi$ is an isogeny we want. This algorithm runs in $\tilde{O}(p^{1/2})$ operations and requires storage for size $\tilde{O}(p^{1/2})$. If one knows that there is an isogeny from E_1 to E_2 of a smooth degree $d < p$, then the number of operations and the storage size in this algorithm can be improved to $\tilde{O}(d^{1/2})$.

2.2.2. *Delfs-Galbraith algorithm* [DG16]. This algorithm is based on the fact that the number of supersingular elliptic curves over $\mathbb{F}_p$ up to isomorphism is $\tilde{O}(p^{1/2})$. The first step is to find isogenies to curves over $\mathbb{F}_p$ from E_1 and E_2, respectively. One can do this with a high probability by computing $O(p^{1/2})$ isogenies. Let $\varphi_1 : E_1 \to F_1$ and $\varphi_2 : E_2 \to F_2$ be such isogenies. The second step is to find an isogeny between F_1 and F_2. This step can be done by computing $O(p^{1/2})$ isogenies over $\mathbb{F}_p$. Let $\psi : F_1 \to F_2$ is such an isogeny. Then the composition $\widehat{\varphi_2} \circ \psi \circ \varphi_1$ is an isogeny we want. This algorithm also runs in $\tilde{O}(p^{1/2})$ operations but requires size $O(\log p)$ storage. In addition, we can use the Meet-in-the-Middle algorithm for finding ψ [DG16, Algorithm 1]. This part runs in $\tilde{O}(p^{1/4})$ and requires storage for size $\tilde{O}(p^{1/4})$.

2.3. Quaternion Algebras. A *quaternion algebra* over $\mathbb{Q}$ is a division algebra B represented by

$$B = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = a, j^2 = b, ij = -ji \tag{1}$$

for some $a, b \in \mathbb{Q}^\times$. For $\alpha = x + yi + zj + tij \in B(x, y, z, t \in \mathbb{Q})$, we define a *canonical involution* of α is defined by $x - yi - zj - tij$ and denote it by $\bar{\alpha}$. The *reduced norm* of α is defined by $\alpha\bar{\alpha}$ and denoted by $n(\alpha)$. Note that $n(\alpha) = x^2 - ay^2 - bz^2 + abt^2 \in \mathbb{Q}$.

A quaternion algebra B over $\mathbb{Q}$ is *ramified* at a place v of $\mathbb{Q}$ if $B \otimes_{\mathbb{Q}} \mathbb{Q}_v$ is not isomorphic to the algebra of 2×2 matrices over $\mathbb{Q}_v$. For a prime p, there exists a quaternion algebra ramified exactly at p and ∞. Such an algebra is unique up to isomorphism. We denote it by $B_{p,\infty}$. For $B_{p,\infty}$, we can take a as a negative integer and $b = -p$ in (1). In the case $p \equiv 3 \pmod 4$, we can take $a = -1$. This is the case we are interested in.

An *order* of a quaternion algebra B is a subring of B that is a $\mathbb{Z}$-module of rank 4. Let $\mathcal{O}$ be an order of B. For $\alpha \in \mathcal{O}$, we have $n(\alpha) \in \mathbb{Z}$. For an ideal I of $\mathcal{O}$, we define the *reduced norm* of I by $\gcd\{n(\alpha) \mid \alpha \in I\}$ and denote it by $n(I)$. Two left $\mathcal{O}$-ideals I and J are *equivalent* if there exists $\alpha \in B$ such that $I = J\alpha$. A *maximal order* is an order that is not contained in any other order. For a subset $\Lambda \subseteq B$, we define its *left order* $\mathcal{O}_{\mathrm{L}}(\Lambda)$ and *right order* $\mathcal{O}_{\mathrm{R}}(\Lambda)$ as

$$\mathcal{O}_{\mathrm{L}}(\Lambda) = \{\alpha \in B \mid \alpha\Lambda \subseteq \Lambda\}, \quad \mathcal{O}_{\mathrm{R}}(\Lambda) = \{\alpha \in B \mid \Lambda\alpha \subseteq \Lambda\}. \tag{2}$$

For two maximal orders $\mathcal{O}$ and $\mathcal{O}'$, a *connecting ideal* of $\mathcal{O}$ and $\mathcal{O}'$ is an ideal I satisfying $\mathcal{O}_{\mathrm{L}}(I) = \mathcal{O}$ and $\mathcal{O}_{\mathrm{R}}(I) = \mathcal{O}'$.

Let p be a prime and K an imaginary quadratic field in which p does not split. Then there exists an inclusion $K \hookrightarrow B_{p,\infty}$. We say an order $\mathfrak{O}$ of K is *optimally embedded* in a maximal order $\mathcal{O}$ of $B_{p,\infty}$ if there exists an inclusion $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$ and there is no inclusion $\kappa : \mathfrak{O}' \hookrightarrow \mathcal{O}$ such that $\mathfrak{O} \subsetneq \mathfrak{O}'$ and $\kappa|_{\mathfrak{O}} = \iota$. We need the following lemma for our result.

LEMMA 2 ([Kan89, Theorem 2']). *Suppose that two orders $\mathfrak{O}_1$ and $\mathfrak{O}_2$ in K are optimally embedded in a maximal order in $B_{p,\infty}$ with different images. Then the inequality $D_1 D_2 \geq p^2$ holds, where D_1 and D_2 are the discriminants of $\mathfrak{O}_1$ and $\mathfrak{O}_2$, respectively.*

2.4. The Deuring Correspondence. Let E be an elliptic curve over a finite field of characteristic p. We say that E is *supersingular* if $\mathrm{End}(E)$ is isomorphic to a maximal order of $B_{p,\infty}$. If E is supersingular, then the j-invariant $j(E)$ is in $\mathbb{F}_{p^2}$. On the other hand, for any maximal order $\mathcal{O}$ of $B_{p,\infty}$, there exists a supersingular elliptic curve over $\mathbb{F}_{p^2}$ whose endomorphism ring is isomorphic to $\mathcal{O}$. In addition, we have a one-to-one correspondence (the *Deuring correspondence*) between $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$-conjugate classes of supersingular j-invariants over $\mathbb{F}_{p^2}$ and isomorphism classes of maximal orders in $B_{p,\infty}$.

Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$ and $\mathcal{O}$ maximal order of $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$. By fixing an isomorphism, we identify $\mathrm{End}(E)$ with $\mathcal{O}$. Then, we have the following correspondence between isogenies from E and left $\mathcal{O}$-ideals. For an isogeny $\varphi : E \to E'$, we define

$$I_\varphi \coloneqq \{\alpha \in \mathcal{O} \mid \alpha(P) = O \text{ for all } P \in \ker\varphi\}, \tag{3}$$

where O is the identity element of E. Then I_φ is a left $\mathcal{O}$-ideal. Conversely, for a left $\mathcal{O}$-ideal I, we define an isogeny φ_I as an isogeny with kernel $E[I] \coloneqq \cap_{\alpha \in I} \ker\alpha$. Under this correspondence, we have $\deg\varphi = n(I_\varphi)$, and two left $\mathcal{O}$-ideals I and J are equivalent

if and only if $E/E[I] \cong E/E[J]$. An isomorphism

$$B_{p,\infty} \to \mathrm{End}(E/E[I]) \otimes_{\mathbb{Z}} \mathbb{Q}, \quad \alpha \mapsto \frac{1}{n(I)} \varphi_I \circ \alpha \circ \widehat{\varphi_I} \tag{4}$$

induces an isomorphism $\mathcal{O}_{\mathrm{R}}(I) \to \mathrm{End}(E/E[I])$. This isomorphism induces a correspondence between left $\mathcal{O}_{\mathrm{R}}(I)$-ideals and isogenies from $\mathrm{End}(E/E[I])$. Under this correspondence, the canonical involution $\bar{I} \coloneqq \{\bar{\alpha} \mid \alpha \in I\}$ corresponds to the dual isogeny $\widehat{\varphi_I}$.

Given a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, computing a maximal order isomorphic to $\mathrm{End}(E)$ is as hard as the isogeny problem over $\mathbb{F}_{p^2}$ [EHL+18, Wes22]. On the other hand, we know isomorphisms to maximal orders for some special curves. The following example is essential for this paper. Let p be a prime satisfying $p \equiv 3 \pmod 4$. We take $B_{p,\infty}$ so that $i^2 = -1$ and $j^2 = -p$. We define an elliptic curve

$$E_0 : y^2 = x^3 + x \tag{5}$$

over $\mathbb{F}_{p^2}$ and a $\mathbb{Z}$-submodule

$$\mathcal{O}_0 \coloneqq \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+ij}{2} \tag{6}$$

of $B_{p,\infty}$. Then E_0 is supersingular, $\mathcal{O}_0$ is a maximal order, and $\mathrm{End}(E_0)$ is isomorphic to $\mathcal{O}_0$. The elliptic curve E_0 has two non-integer endomorphisms, ι and π, defined as

$$\iota : (x, y) \mapsto (-x, \xi y) \text{ and } \pi : (x, y) \mapsto (x^p, y^p), \tag{7}$$

where $\xi \in \mathbb{F}_{p^2}$ is a square root of -1. We have an isomorphism from $\mathrm{End}(E_0)$ to $\mathcal{O}_0$ defined as $\iota \mapsto i$ and $\pi \mapsto ij$.

2.5. KLPT algorithm. KLPT (Kohel-Lauter-Petit-Tignol) algorithm is a core algorithm in SQISign. This subsection overviews the original algorithm by [KLPT14] and a generalized algorithm by [DFKL+20a].

An order $\mathcal{O}$ of $B_{p,\infty}$ is *special p-extremal* if $\mathcal{O}$ is a maximal order and contains a subring $R + jR$ such that R is a quadratic order of minimal discriminant in $\mathcal{O}$. In the case $p \equiv 3 \pmod 4$, the order $\mathcal{O}_0$ defined in (6) is special p-extremal by taking $R = \mathbb{Z}[i]$. The order $\mathcal{O}_0$ is isomorphic to the endomorphism ring of an elliptic curve with j-invariant 1728 and is used in the proposed parameter of SQISign. Thus, we consider this order in this paper.

The original KLPT algorithm [KLPT14] takes an ideal I of a special p-extremal order $\mathcal{O}$ and outputs an ideal J equivalent to I with a smooth reduced norm. One can give a condition on the reduced norm $n(J)$ as input, and the success probability of the algorithm is higher with a larger $n(J)$. By applying an improvement by Petit and Smith [PS18], the algorithm terminates in a polynomial time in $\log p$ with a high probability if $n(J) \geq p^3$.

The Deuring correspondence says that we can regard the KLPT algorithm as an algorithm transforming an isogeny into an isogeny of a smooth degree.

De Feo et al. [DFKL+20a] generalized the KLPT algorithm. Their generalized KLPT algorithm transforms an ideal of any maximal order. Let $\mathcal{O}_0$ be a special p-extremal order and $\mathcal{O}$ a maximal order. The input of the generalized KLPT algorithm is a connecting ideal I_0 of $\mathcal{O}_0$ and $\mathcal{O}$ and a left $\mathcal{O}$-ideal I. Its output is a left $\mathcal{O}$-ideal J equivalent to I with a smooth reduced norm. In this algorithm, the condition on the reduced norm

$n(J)$ is stronger than that of the original. In particular, the generalized KLPT algorithm requires $n(J) \geq p^3 N^3$, where N is the minimum of the reduced norms inert in R of ideals equivalent to I_0.

3. SQISign.

In this section, we recall the protocol and some features of SQISign.

3.1. Protocol.

Let $\mathcal{O}_0$ be a special p-extremal order and E_0 a supersingular elliptic curve over $\mathbb{F}_{p^2}$ whose endomorphism ring is isomorphic to $\mathcal{O}_0$. We consider the following zero-knowledge proof. The public parameters are p, $\mathcal{O}_0$, and E_0. The protocol proves the knowledge of a secret isogeny $\tau : E_0 \to E_A$ with a public key E_A. Note that one can compute the correspondence between isogenies and ideals of $\mathcal{O}_0$ defined in Section 2.4 (for detailed algorithms, see [DFKL+20a, DFLW22]). The protocol is as follows:

1. The prover computes an isogeny $\psi : E_0 \to E_1$ and sends E_1 as a commitment to the verifier.
2. The verifier computes an isogeny $\varphi : E_1 \to E_2$ and sends φ and E_2 as a challenge to the prover.
3. The prover computes ideals I_τ and $I_{\varphi\circ\psi\circ\hat{\tau}}$, applies the generalized KLPT algorithm to these ideals, and obtains an ideal J corresponding to an isogeny from E_A to E_2. Then s/he computes the isogeny σ corresponding to J and sends σ as a response to the verifier.
4. The verifier check that σ is an isogeny from E_A to E_2 and the kernel of $\hat{\varphi} \circ \sigma$ is cyclic.

The zero-knowledgeness of this protocol is based on the assumption that it is hard to compute the secret τ from the output σ of the generalized KLPT algorithm. SQISign is a signature scheme obtained by applying the Fiat-Shamir transform to the above protocol.

3.2. Parameters.

It is required that the degree of the isogeny is smooth and its kernel is defined over a small field for efficient computation of isogenies. Since we use supersingular elliptic curves over $\mathbb{F}_{p^2}$, it is desired that the kernel of an isogeny is defined over $\mathbb{F}_{p^2}$.

Costello [Cos20] proposed a method to compute isogenies using quadratic twists, by which the $(p+1)$-torsion subgroup and the $(p-1)$-torsion subgroup of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ can be defined over $\mathbb{F}_{p^2}$. On the other hand, the degree of the response σ is equal to the reduced norm of an output of the generalized KLPT algorithm, i.e., greater than p^3. Therefore, the kernel of σ cannot be defined over $\mathbb{F}_{p^2}$ even by using a quadratic twist. The solution by [DFKL+20a] is to separate σ into small-degree isogenies whose kernels are defined over $\mathbb{F}_{p^2}$. To determine the kernels of intermediate isogenies, one needs to transport the information of the ideal I_σ by isogenies whose degrees are prime to $\deg \sigma$. The degree of this auxiliary isogeny must be greater than $p^{3/2}$ in the original method [DFKL+20a], and it was improved to $p^{5/4}$ by [DFLW22].

Proposed parameters of SQISign by [DFKL+20a, DFLW22] use an isogeny of degree a power of two for σ due to the computational efficiency. For defining the kernels of σ and the auxiliary isogeny over $\mathbb{F}_{p^2}$, the characteristic p is chosen to satisfy

$$p + 1 = 2^f T_1 S_1 \text{ and } p - 1 = 2 T_2 S_2,$$

where $f \geq 2$, $T := T_1 T_2$ is a smooth odd integer and the degree of the auxiliary isogeny, and S_1, S_2 are cofactors not used for isogenies. To achieve λ bits of classical security and $\lambda/2$ bits of quantum security, it is necessary that $p \approx 2^{2\lambda}$. Examples of p's of 128 bits of classical security can be found in [DFKL+20a, DFLW22].

The reason that $p+1$ has a big power of 2, i.e., $p \equiv 3 \pmod 4$, is to take E_0 as in (5) and $\mathcal{O}_0$ as in (6). In the rest of this paper, we mainly consider this case.

3.3. Key Generation. We use the notation in the protocol in Section 3.1. The dominant part of signing computation in SQISign is to compute the response isogeny σ. The cost of this part is almost proportional to $\log(\deg \sigma) = \log(n(J))$. As we stated in Section 2.5, the reduced norm of J is greater than $p^3 N^3$, where N is the minimum of the degrees inert in R of the isogeny from E_0 to E_A. Typically, we have $N \approx p^{1/2}$ (see [KLPT14, Section 3.1]). On the other hand, [DFKL+20a] proposed to choose E_A such that $N < p^{1/4}$. We denote the set of isomorphism classes of such curves by $\mathcal{K}_p$, i.e.,

$$\mathcal{K}_p := \{E_A \mid \exists \tau : E_0 \to E_A \text{ s.t. } \deg \tau < p^{1/4} \text{ and } \deg \tau \text{ is inert in } R\}/\sim . \tag{8}$$

This reduces the degree of σ from $p^{9/2}$ to $p^{15/4}$. The reason for taking the bound $p^{1/4}$ is so that the cardinality of $\mathcal{K}_p$ is about $p^{1/2}$. This makes the cost of a brute-force attack for the secret isogeny $O(p^{1/2}) = O(2^\lambda)$ in a classical computer. [DFKL+20a] claimed that other attacks like as in Section 2.2 do not improve this cost, i.e., restricting public keys in $\mathcal{K}_p$ does not reduce the security of SQISign.

The key generation procedure proposed in [DFKL+20a] is as follows:

1. Select a prime $N < p^{1/4}$ inert in R uniformly at random.
2. Select a left $\mathcal{O}_0$-ideal I of reduced norm N uniformly at random.
3. Compute a left $\mathcal{O}_0$-ideal J equivalent to I whose reduced norm is a power of 2 by the KLPT algorithm.
4. Compute the isogeny τ corresponding to J and obtain a public key E_A as the codomain of τ.

Note that there are $N+1$ left $\mathcal{O}_0$-ideals of reduced norm N, and this procedure does not sample a public key in $\mathcal{K}_p$ uniformly at random (the sampling is weighted by the inverse of $N+1$).

An alternative key generation procedure was proposed in [DFKL+20b, Supplementary Material D]. This alternative procedure replaces Step 2 and Step 3 above with the following.

2'. Set $e := \lceil \log_2 p \rceil$ and take $\gamma \in \mathcal{O}_0$ of reduced norm $N 2^e$ at random.
3'. Set $I := \mathcal{O}_0 \gamma + \mathcal{O}_0 N$ and $J := \mathcal{O}_0 \bar{\gamma} + \mathcal{O}_0 2^e$.

Here, I is equivalent to J and it holds $n(I) = N$ and $n(J) = 2^e$. Since $2^e \geq p$, we can expect that there exists an isogeny from E_0 to E_A of degree 2^e for all public keys E_A. An advantage of the alternative key generation procedure is to reduce the degree of τ from p^3 to p. This reduces the computational cost of τ by about one-third.

The quaternion γ in the alternative procedure can be obtained by RepresentInteger (Algorithm 1) or alternatively FullRepresentInteger (Algorithm 2) if $\mathcal{O}_0$ is defined as (6). In these algorithms, Cornacchia(M) is Cornacchia's algorithm [CP05, Algorithm 2.3.12],

Algorithm 1: $\mathsf{RepresentInteger}_{\mathcal{O}_0}(M)$ [DFKL+20b, Algorithm 1]

Input : $M \in \mathbb{Z}$ such that $M > p$.
Output: $\gamma \in R + jR$ of reduced norm M.

1 Set $m \coloneqq \lfloor \sqrt{M/p} \rfloor$.
2 Sample integers z, t from $[-m, m]$ at random and set $M' \coloneqq M - n(j(z + ti))$.
3 **if** $\mathsf{Corncchia}(M') = \perp$ **then**
4 Go back to Step 2.
5 Set $x, y \coloneqq \mathsf{Corncchia}(M')$.
6 **return** $\gamma \coloneqq x + yi + j(z + ti)$.

Algorithm 2: $\mathsf{FullRepresentInteger}_{\mathcal{O}_0}(M)$ [DFLW22, Algorithm 1]

Input : $M \in \mathbb{Z}$ such that $M > p$.
Output: $\gamma \in \mathcal{O}_0 = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}\frac{1+i}{2} + \mathbb{Z}\frac{i+ij}{2}$ of reduced norm M.

1 Set $m \coloneqq \lfloor \sqrt{4M/p} \rfloor$.
2 Sample an integer z from $[-m, m]$ at random.
3 Set $m' \coloneqq \lfloor \sqrt{4M/p - z^2} \rfloor$.
4 Sample an integer t from $[-m', m']$ at random and set $M' \coloneqq 4M - p(z^2 + t^2)$.
5 **if** $\mathsf{Corncchia}(M') = \perp$ **then**
6 Go back to Step 2.
7 Set $x, y \coloneqq \mathsf{Corncchia}(M')$.
8 **if** $x \not\equiv z \pmod 2$ or $y \not\equiv t \pmod 2$ **then**
9 Go back to Step 2.
10 **return** $\gamma \coloneqq (x + yi + j(z + ti))/2$.

which returns integers x, y such that $n(x + yi) = M$ or $\perp$ if such integers do not exist. Because $\mathsf{Cornacchia}(M)$ requires the prime factorization of M, we use an alternate of it, which returns $\perp$ if the factorization does not succeed within a certain effort, in practice. Note that there may be multiple solutions to $n(x + yi) = M$, and different solutions may generate different keys. Therefore, the output of $\mathsf{Cornacchia}(M)$ should be randomized.

The implementation[1] in [DFKL+20a] uses the alternative procedure. However, the security analysis of this procedure is left open.

4. Properties of the Public Keys. We consider the security of restricting public keys in a special set $\mathcal{K}_p$. In the rest of this paper, we let p be a prime such that $p \equiv 3 \pmod 4$, $\mathcal{O}_0$ a maximal order defined in (6), and E_0 a supersingular elliptic curve defined in (5).

4.1. Distance from E_0. Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$. If there is an isogeny from E_0 to E of a smooth degree $d < p$ and d is known, then the Meet-in-

[1] https://github.com/SQISign/sqisign

the-Middle attack finds the isogeny by $\tilde{O}(d^{1/2})$ operations, which is smaller than the cost of the general case. Therefore, we are interested in whether a curve in $\mathcal{K}_p$ has such an isogeny. The following theorem gives a lower bound of the smooth degree d.

THEOREM 3. *Let E be a supersingular elliptic curve in $\mathcal{K}_p$. Suppose that there exists an isogeny $\varphi : E_0 \to E$ such that $\deg\varphi$ is prime to N. Then $\deg(\varphi) \geq p^{3/4}/4$.*

Proof. Let n be the degree of φ. We have an embedding $\mathbb{Z} + ni\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ defined by $a + bni \mapsto a + b\varphi \circ \iota \circ \hat{\varphi}$. Therefore, there exists an order $\mathfrak{O} \supseteq \mathbb{Z} + ni\mathbb{Z}$ in $\mathbb{Q}(i)$ that is optimally embedded in $\mathrm{End}(E)$. On the other hand, an isogeny $E_0 \to E$ of degree N induces an optimal embedding $\mathbb{Z} + Ni\mathbb{Z} \hookrightarrow \mathrm{End}(E)$. Since n is prime to N, the above two embeddings are distinct. Therefore, from Lemma 2, we have $4N^2\mathrm{disc}(\mathfrak{O}) \geq p^2$. Since $\mathrm{disc}(\mathfrak{O}) \leq \mathrm{disc}(\mathbb{Z} + ni\mathbb{Z}) = 4n^2$, it follows that $n \geq p^{3/4}/4$ ∎

Theorem 3 implies that the computational complexity of the Meet-in-the-Middle attack to a public key is at least $\tilde{O}(p^{3/8})$. This means that a public key in SQISign tends to be far from E_0 and can be considered to be relatively secure against the Meet-in-the-Middle attack.

4.2. Public Keys over $\mathbb{F}_p$. For a supersingular elliptic curve E over $\mathbb{F}_p$, we can find an isogeny from E_0 to E by $\tilde{O}(p^{1/4})$ operations because E_0 is defined over $\mathbb{F}_p$. If we choose E uniformly at random from supersingular elliptic curves over $\mathbb{F}_{p^2}$, then the probability that E is defined over $\mathbb{F}_p$ is about $p^{-1/2}$. On the other hand, we show that the probability that a public key in SQISign is defined over $\mathbb{F}_p$ is greater than $1/(p^{1/4}+1)$ under the following plausible heuristic.

HEURISTIC 4. *Let N be sampled from primes less than $p^{1/4}$ and inert in $\mathbb{Z}[i]$ uniformly at random. Then the probability that $-p$ is a quadratic residue modulo N is $1/2$.*

Before stating our result, we recall an ideal class group action on supersingular elliptic curves over $\mathbb{F}_p$. Let E be a supersingular elliptic curve over $\mathbb{F}_p$. Then the $\mathbb{F}_p$-endomorphism ring is isomorphic to $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}[\frac{1+\sqrt{-p}}{2}]$, and the ideal class group of the isomorphic order acts on E. In particular, for an ideal I of the order, there exists an isogeny over $\mathbb{F}_p$ from E of degree the norm of I. Therefore, for an odd prime N splitting in $\mathbb{Q}(\sqrt{-p})$, there are two isogenies over $\mathbb{F}_p$ from E corresponding to two prime ideals above N in $\mathbb{Q}(\sqrt{-p})$. For more detail on the group action, see [DG16, CLM+18].

Now, we state our theorem on the probability that a public key is defined over $\mathbb{F}_p$.

THEOREM 5. *Let N be sampled from primes less than $p^{1/4}$ and inert in $\mathbb{Z}[i]$ uniformly at random. Let φ be sampled from isogenies from E_0 of degree N uniformly at random. Then, under Heuristic 4, the probability that the codomain of φ is defined over $\mathbb{F}_p$ is greater than $1/(p^{1/4}+1)$.*

Proof. There are exactly $N+1$ isogenies from E_0 of degree N. If $-p$ is a quadratic residue modulo N, then N splits in $\mathbb{Q}(\sqrt{-p})$. In this case, there are two isogenies over $\mathbb{F}_p$ from E_0 of degree N corresponding to two prime ideals above N in $\mathbb{Q}(\sqrt{-p})$. The codomains of these isogenies are defined over $\mathbb{F}_p$. Therefore, by Heuristic 4, the probability that the codomain of φ is at least $(1/2)(2/(N+1)) > 1/(p^{1/4}+1)$. ∎

This theorem says that SQISign of λ bits security generates a weak public key with a probability of at least $2^{-\lambda/2}$. This is still exponentially small and can easily be avoided by checking whether a public key is defined over $\mathbb{F}_p$.

5. Consideration for the Alternative Key Generation Procedure. This section shows that the alternative key generation procedure stated in Section 3.3 could not generate all public keys and propose a modification for the procedure.

This fact reduces the security of SQISign because a brute-force attack for secret keys is one of the best attacks currently known.

5.1. Lack of Keys. Let E_A be a public key in SQISign with an isogeny $\tau : E_0 \to E_A$ of degree N. We set $e := \lceil \log_2 p \rceil$ as in the alternative procedure. Then there are about p isogenies from E_0 of degree 2^e. On the other hand, the number of supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to isomorphism is about $\lfloor \frac{p}{12} \rfloor$. By the Ramanujan property of a supersingular isogeny graph, we can regard the codomains of the isogenies from E_0 of degree 2^e to be uniformly distributed in all supersingular elliptic curves over $\mathbb{F}_{p^2}$. Therefore, there are about 12 isogenies from E_0 to E_A of degree 2^e. However, these isogenies could not appear in the outputs of the alternative key generation procedure since the subroutine Cornacchia needs a prime factorization of a large integer.

Let $\varphi : E_0 \to E_A$ be an isogeny of degree 2^e and $\gamma = a + bi + c\frac{1+j}{2} + d\frac{i+ij}{2}$ be the quaternion corresponding to $\hat{\tau} \circ \varphi \in \mathrm{End}(E_0)$. Since $n(\gamma) = N2^e \approx p^{5/4}$, we need a prime factorization of size about $p^{5/4}$ to obtain γ. Furthermore, if we use RepresentInteger to generate γ in Step 2', then c and d must be even. Therefore, the probability that RepresentInteger outputs γ is about $1/4$ even if we can factorize large integers.

Consequently, the probability that E_A is obtained by the alternative procedure is $3 \times$ Prob(factorization success) if we use RepresentInteger, or $12 \times$ Prob(factorization success) if we use FullRepresentInteger. We estimate Prob(factorization success) below and show that the alternative procedure may not generate all public keys even by using FullRepresentInteger.

5.2. Success Probability of Factorization. The success probability of factorization depends on what method we use. In this paper, we consider a trial division combined with a primality testing. In particular, we factorize only integers of the form (B-smooth integer) $\times$ prime, where B is a smoothness bound. We call an integer of this form a *B-CF number*[2].

We let b be a positive integer and consider the probability that an integer less than 2^ν is a 2^b-CF number. We estimate this probability by

$$\frac{1}{2^\nu}\left(\sum_{s=b}^{\nu} 2^s \rho\left(\frac{s}{b}\right)\left(\mathrm{li}(2^{\nu-s}) - \mathrm{li}(2^{\nu-s-1})\right) + \mathrm{li}(\nu - b - 1)\right), \tag{9}$$

where ρ is the Dickman function and li is the logarithmic integral.

Table 1 shows the estimation in (9) and experimental estimation for $b = 10$. The formula (9) was computed by using SageMath [SD20]. The experiment was conducted

[2] "CF" stands for Cornacchia Friendly.

by using Julia language and considered two cases. The first is the percentage of 2^{10}-CF numbers to random integers less than 2^ν. The second is that of random integers represented by the sum of two integers. The codes are available at https://github.com/hiroshi-onuki/keys_in_sqisign. This result shows that there is no big difference between our estimation and the experiment, and the sum of two squares tends not to be a CF number. One of the reasons for the latter is that a smooth number tends not to be the sum of two squares. For example, the probability that a prime is the sum of two squares is about 1/2, but that of the product of two primes is about 1/4 (the two primes are equivalent to 1 modulo 4 or the two primes are the same).

		Experiment	
ν	Estimation in (9)	Random integer	Sum of squares
266	4.72%	6.82%	3.51%
269	4.66%	6.85%	3.48%
322	3.87%	5.83%	2.88%
400	3.10%	4.59%	2.33%
500	2.47%	3.67%	1.81%

Table 1. The estimation in (9) and experimental estimation with 100,000 samples for $b = 10$.

The alternative key generation procedure needs factorizations of about $N2^e$ or $4N2^e$ depending on using RepresentInteger or FullRepresentInteger. As in Table 1, factor 4 does not have a significant impact one the success probability of factorizations. Therefore, we should use FullRepresentInteger. For 128 bits security, SQISign uses p of size 2^{256} and then $4N2^e \approx 2^{322}$. Table 1 shows that 12 chances for a public key are too small to expect to generate the key. Even if we increase the smoothness bound to 2^{20} or 2^{30}, the probability estimated by (9) is 7.84% or 12.10%, respectively. These are still small, considering the tendency for the sum of two squares not to be smooth.

5.3. Proposed Modification. Instead of increasing the smoothness bound, we propose to increase the exponent e. If we add ε to e, the number of quaternions corresponding to each public key is 2^ε times larger. On the other hand, the computational cost of key generation increases by $\varepsilon/\lceil \log_2 p \rceil$. In the following, we show that a small overhead of computational cost can improve the distribution of public keys by the alternative procedure.

Let r be the probability that input of Cornacchia in the alternative procedure can efficiently be factorized. We assume that this probability does not depend on each public key. If we add ε to the exponent e then we can expect that there are $12 \cdot 2^\varepsilon$ quaternions corresponding to each public key. Therefore, the alternative procedure is expected to generate $12 \cdot 2^\varepsilon r$ quaternions corresponding to each public key, and the standard deviation of the number of the quaternions is $\sqrt{12 \cdot 2^\varepsilon r(1-r)}$. This gives us a way to determine ε. If we want α times the expected value to be greater than s times the standard deviation, then we determine ε satisfying

$$\left(\frac{s}{\alpha}\right)^2 \frac{1-r}{r} < 12 \cdot 2^\varepsilon. \tag{10}$$

Algorithm 3: The set of all left $\mathcal{O}_0$-ideals of degree N

Input : A prime N inert in $\mathbb{Z}[i]$.
Output: A numbred set $\mathcal{I}$ of all left $\mathcal{O}_0$-ideals of degree N

Set $\gamma \coloneqq \mathsf{RepresentInteger}(N2^e)$, where $e = \lceil \log_2 p \rceil$.
Set $I_0 \coloneqq \mathcal{O}_0\gamma + \mathcal{O}_0 N$.
Set $\mathcal{I} \coloneqq \{I_0\}$.
for $n \in [1, N]$ **do**
    Set $\alpha \coloneqq n + i$ otherwise.
    Append $I_n \coloneqq (I_0 \cap \mathcal{O}\alpha)\alpha^{-1}$ to $\mathcal{I}$.
return $\mathcal{I}$.

For example, in the case of 128 bits security, we assume $r = 2\%$ (less than the probability in Table 1 for $\nu = 322$) and take $\alpha = 0.1$ and $s = 2$. Then taking $\varepsilon = 11$ satisfies the condition (10). This shows that by assuming the distribution can be approximated by a normal distribution, the numbers of quaternions corresponding to about 95.4% of keys are expected to be within 10% of the expected value by $11/256 \fallingdotseq 4.29\%$ overhead [3] of the computation cost.

5.4. Experiment. This subsection gives experimental results for the key distribution in the alternative procedure. The experiment was conducted by Julia language. The code is available at https://github.com/hiroshi-onuki/keys_in_sqisign.

Our experiment uses the characteristic p of 256 bits proposed in [DFKL+20a] and small degrees N of secret isogenies. In particular, we use

$$N \in \{211, 223, 227, 239, 251, 1019, 2003\}.$$

Note that $4N2^e \approx 2^{266} \sim 2^{269}$ in these cases. Therefore, the probability that a public key is generated by the alternative procedure is estimated in the rows $\nu = 266$ and $\nu = 269$ in Table 1.

The procedure of the experiment is as follows. First, we prepare a numbered set $(I_0, \ldots, I_N)$ of all left $\mathcal{O}_0$-ideals of reduced norm N. This can be done by Algorithm 3, which uses the fact that the quaternion i acts as a distortion map on the torsion subgroup $E_0[N]$ since N is inert in $\mathbb{Z}[i]$. Next, we generate a random left $\mathcal{O}_0$-ideal I of reduced norm N by the alternative procedure and check which I_n for $n = 1, \ldots, N$ is equal to I. The number of these random left ideals is $100N$ for each N.

Table 2 shows the numbers of distinct keys generated by the alternative procedure using RepresentInteger or FullRepresentInteger, and these numbers as percentages of the number of all keys of the corresponding reduced norm. This result shows that the alternative procedure hardly generates all keys even by using FullRepresentInteger.

In addition, the effectiveness of increasing the exponent e was checked by the same experiment. Fig. 1 to 7 shows histograms of keys generated by the alternative procedure

[3] More precisely, the computational cost of the key generation jumps up when the exponent exceeds a multiple of the degree of a separated isogeny.

	RepresentInteger		FullRepresentInteger	
N	Number	Number$/(N+1)$	Number	Number$/(N+1)$
211	8	3.77%	38	17.92%
223	52	23.21%	150	66.96%
227	48	21.05%	142	62.28%
239	84	35.00%	142	59.17%
251	24	9.52%	138	54.76%
1019	128	12.55%	424	41.57%
2003	264	18.16%	742	37.03%

Table 2. The numbers of distinct keys generated by the alternative procedure.

using FullRepresentInteger with $e = \lceil \log_2 p \rceil + \varepsilon$ for $\varepsilon = 0, 5, 11$. These figures show that the distributions of the keys are almost uniform in the case $\varepsilon = 11$. This confirms our estimation in Section 5.3.

Acknowledgements. This research was conducted under a contract of "Research and development on new generation cryptography for secure wireless communication services" among Research and Development for Expansion of Radio Wave Resources (JPJ000254), which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[BDFLS20] Daniel J. Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In Steven Galbraith, editor, *ANTS-XIV - 14th Algorithmic Number Theory Symposium*, volume 4 of *Proceedings of the Fourteenth Algorithmic Number Theory Symposium (ANTS-XIV)*, pages 39–55, Auckland, New Zealand, 2020. Mathematical Sciences Publishers.

[BKV19] Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019*, pages 227–247, Cham, 2019. Springer International Publishing.

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427, Cham, 2018. Springer International Publishing.

[Cos20] Craig Costello. B-SIDH: Supersingular isogeny Diffie-Hellman using twisted torsion. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 440–463, Cham, 2020. Springer International Publishing.

[Cou06] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. https://eprint.iacr.org/2006/291.

[CP05] Richard. Crandall and Carl B. Pomerance. *Prime Numbers: A Computational Perspective*. Springer New York, second edition, 2005.

[DFKL+20a] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and

isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

[DFKL+20b] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies (extended version). Cryptology ePrint Archive, Report 2020/1240, 2020. https://ia.cr/2020/1240.

[DFLW22] Luca De Feo, Antonin Leroux, and Benjamin Wesolowski. New algorithms for the Deuring correspondence: SQISign twice as fast. Cryptology ePrint Archive, Report 2022/234, 2022. https://ia.cr/2022/234.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016.

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin 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.

[Gal99] Steven D. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999.

[JAC+] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Geovandro Pereira, Joost Renes, Vladimir Soukharev, and David Urbanik. "SIKE - Supersingular isogeny key encapsulation", Submission to the NIST Post-Quantum Cryptography Standardization project; https://sike.org.

[JDF11] 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.

[Kan89] Masanobu Kaneko. Supersingular j-invariants as singular moduli mod p. *Osaka Journal of Mathematics*, 26(4):849–855, January 1989.

[KLPT14] David Kohel, Kristin 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.

[NIS] National Institute of Standards and Technology (NIST) "NIST Post-Quantum Cryptography Standardization", https://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[PS18] Christophe Petit and Spike Smith. An improvement to the quaternion analogue of the l-isogeny path problem, 2018. conference talk at MathCrypt 2018.

[RS06] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. https://eprint.iacr.org/2006/145.

[SD20] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2020. `https://www.sagemath.org`.

[Sil09] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2nd edition, 2009.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendues de l'Académie des Sciences*, 273:238–241, 1971.

[Voi21] J. Voight. *Quaternion Algebras*. Graduate Texts in Mathematics. Springer, 2021.

[Wes22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2021–62nd Annual IEEE Symposium on Foundations of Computer Science*, 2022.

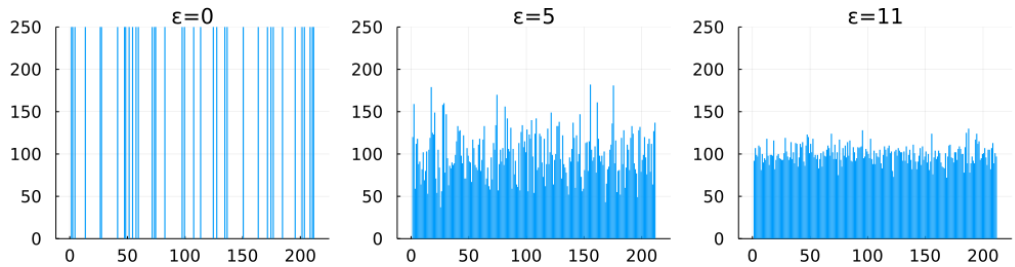

Fig. 1. The distribution of keys generated by the alternative procedure for $N = 211$.

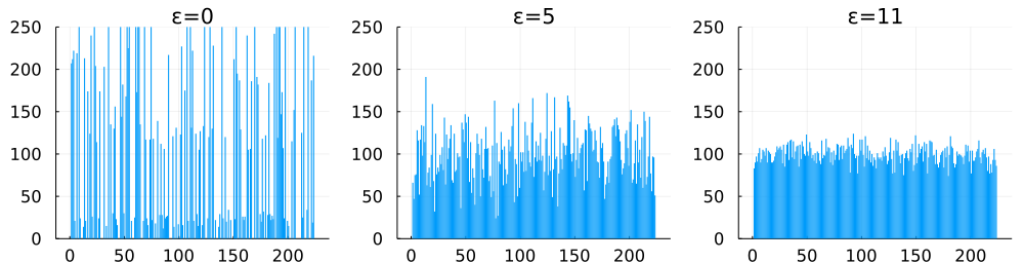

Fig. 2. The distribution of keys generated by the alternative procedure for $N = 223$.

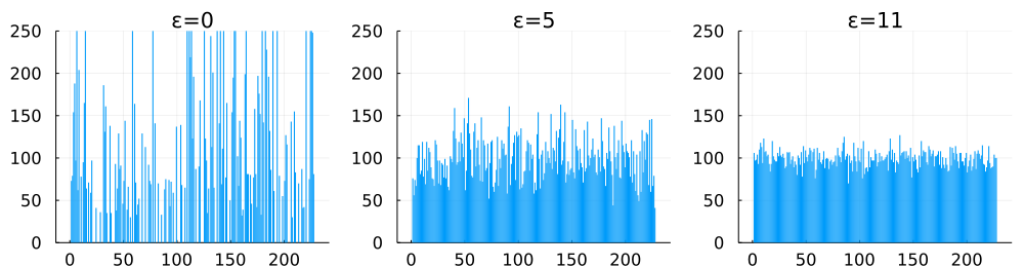

Fig. 3. The distribution of keys generated by the alternative procedure for $N = 227$.

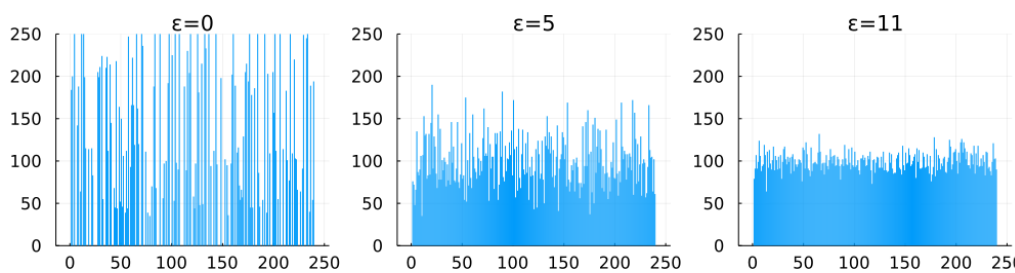

Fig. 4. The distribution of keys generated by the alternative procedure for $N = 239$.

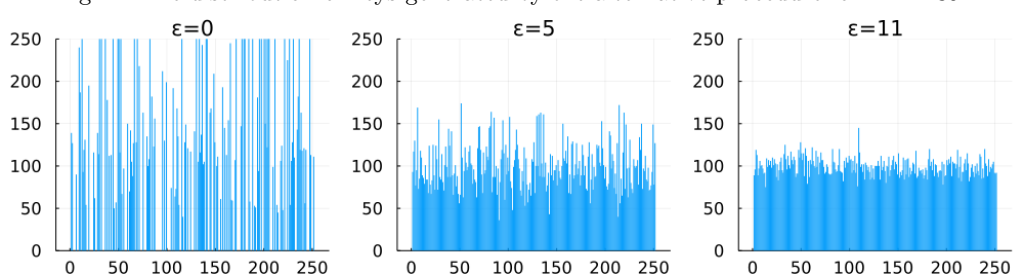

Fig. 5. The distribution of keys generated by the alternative procedure for $N = 251$.

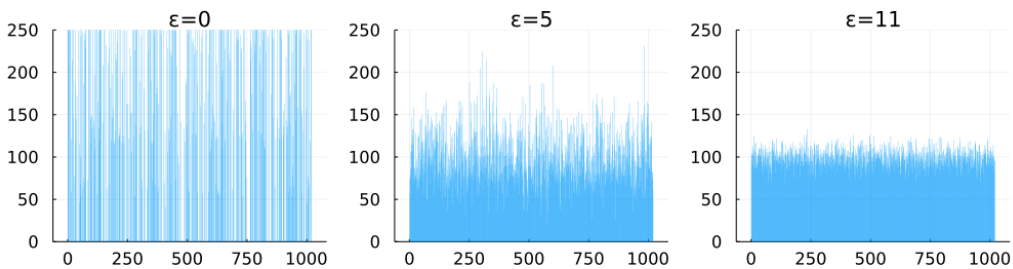

Fig. 6. The distribution of keys generated by the alternative procedure for $N = 1019$.

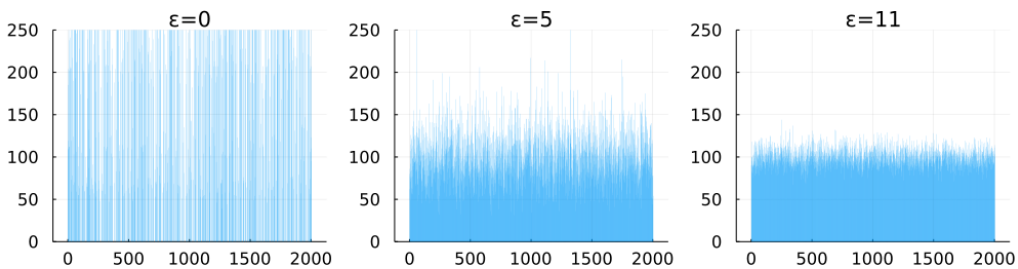

Fig. 7. The distribution of keys generated by the alternative procedure for $N = 2003$.