Deuring Correspondence and Public Key Cryptography

Oral Comprehensive Examination

Gaurish Korpal

December 07, 2023

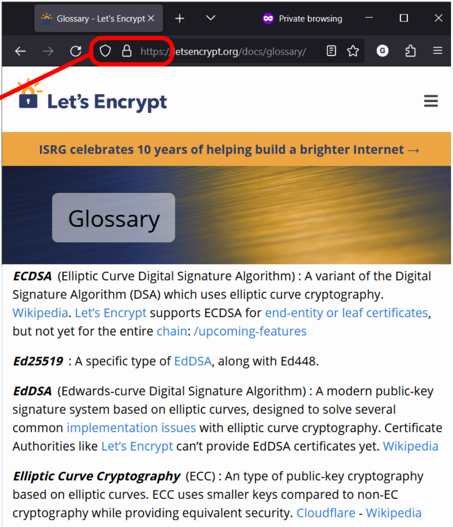
The University of Arizona

Table of contents

Appetizer: Discrete logarithm

Public Key Cryptography

You are securely connected to this website. **Key exchange** allows two parties to agree on a common secret using only publicly exchanged information. **Digital signature** allows parties to authenticate themselves.



Public Key Cryptography

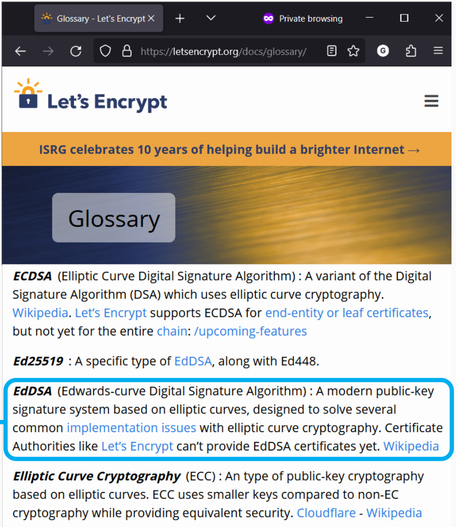
Let’s Encrypt is the world’s largest certificate authority with over 2.53 billion certificates issued.

Public Key Cryptography

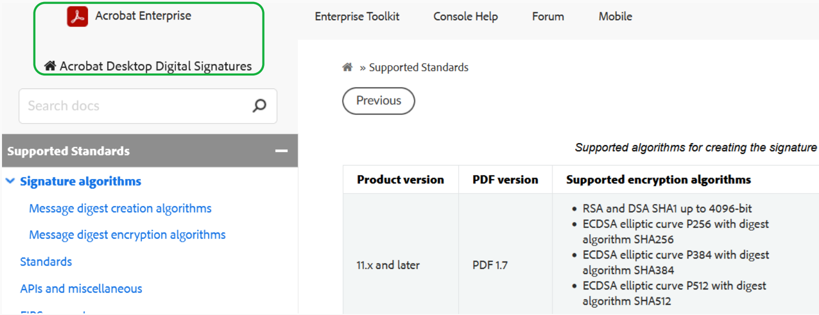
For 128-bit security, DSA (based on DLP) needs 4096-bit keys, but ECDSA (based on ECDLP) only needs 256-bit key.

Public Key Cryptography

EdDSA is not ECDSA over a different curve. Rather, it is a *Schnorr signature* implemented for the Ed25519 Edwards curve.



Preparation for Schnorr


Acrobat Enterprise

Acrobat Desktop Digital Signatures

Enterprise Toolkit Console Help Forum Mobile

Search docs

» Supported Standards

Previous

Supported Standards

Signature algorithms

Message digest creation algorithms

Message digest encryption algorithms

Standards

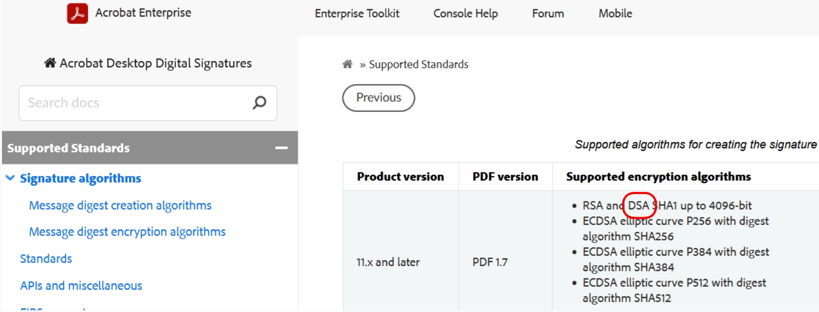
APIs and miscellaneous

Supported algorithms for creating the signature

Product version	PDF version	Supported encryption algorithms
11.x and later	PDF 1.7	• RSA and DSA SHA1 up to 4096-bit • ECDSA elliptic curve P256 with digest algorithm SHA256 • ECDSA elliptic curve P384 with digest algorithm SHA384 • ECDSA elliptic curve P512 with digest algorithm SHA512

Most of us have used Adobe Acrobat Sign to digitally sign PDF documents.

Preparation for Schnorr



Acrobat Enterprise

Enterprise Toolkit Console Help Forum Mobile

Acrobat Desktop Digital Signatures

Search docs

Supported Standards

- **Signature algorithms**
  - Message digest creation algorithms
  - Message digest encryption algorithms
- Standards
- APIs and miscellaneous

» Supported Standards

Previous

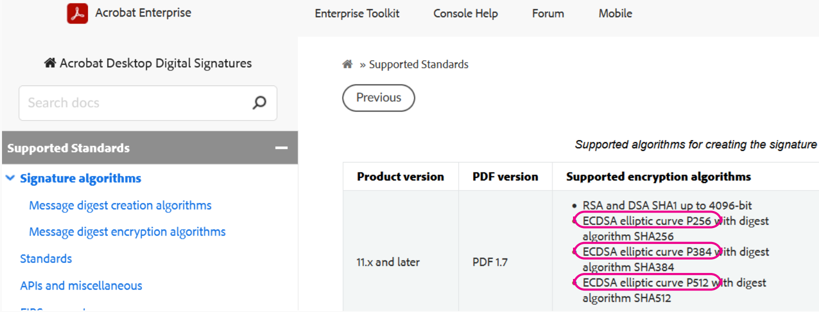
Supported algorithms for creating the signature

Product version	PDF version	Supported encryption algorithms
11.x and later	PDF 1.7	• RSA and DSA SHA1 up to 4096-bit • ECDSA elliptic curve P256 with digest algorithm SHA256 • ECDSA elliptic curve P384 with digest algorithm SHA384 • ECDSA elliptic curve P512 with digest algorithm SHA512

Let $(\mathbb{G}, \cdot)$ be a finite abelian group of prime order ℓ. The *discrete logarithm problem* (DLP) in $\mathbb{G}$ is: given $\langle g\rangle = \mathbb{G}$ and $h \in \mathbb{G}$, find an integer $k \in \{0, \ldots, \ell - 1\}$ such that $g^k = h$.

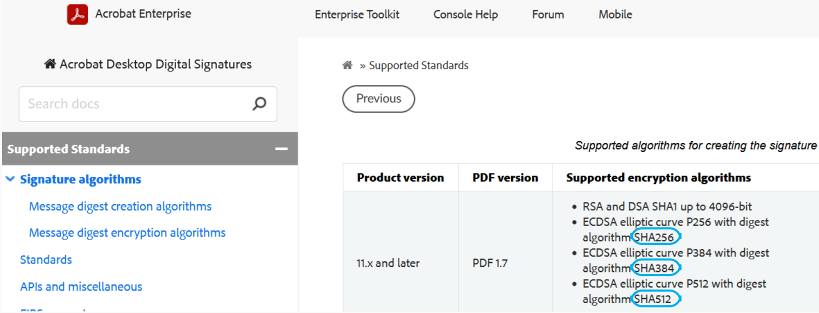
Number of operations for generic $\mathbb{G}$ is $\sqrt{\#\mathbb{G}}$.

Preparation for Schnorr



Let p be a prime larger than 3 and $q = p^n$ for $n > 0$. An elliptic curve E over finite field $\mathbb{F}_q$ can be written as $E : y^2 = x^3 + ax + b$ where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$, along with an extra point $\mathcal{O}_E$. Points on E form a group with $\mathcal{O}_E$ as the neutral element. P be a point on E of prime order ℓ, then $\mathbb{G} = \langle P \rangle$ with the exponentiation replaced with scalar point multiplication, we get ECDLP.

Preparation for Schnorr



A *cryptographic hash function* H takes arbitrary length bit strings as input and produces a fixed-length bit string as output, such that it is preimage resistant (can't find input of given output), second preimage resistant (can't find a different input leading to given output), and collision resistant (can't find two inputs with same output).

Schnorr signature, Step 1: Σ-protocol

Let $\mathbb{G} = \langle g \rangle$ where $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of prime order ℓ.

Schnorr signature, Step 1: Σ-protocol

Let $\mathbb{G} = \langle g \rangle$ where $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of prime order ℓ. The prover P randomly chooses (secret) $k \in \{0, \ldots, \ell - 1\}$ and publishes $h = g^k \pmod{p}$.

Schnorr signature, Step 1: Σ-protocol

Let $\mathbb{G} = \langle g \rangle$ where $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of prime order ℓ. The prover P randomly chooses (secret) $k \in \{0, \ldots, \ell - 1\}$ and publishes $h = g^k \pmod{p}$. Now, P can prove "knowledge" of a discrete logarithm k to a verifier V:

$$\text{P} \xrightarrow{\mathbb{G}, p, h} \text{V}$$

$$t \xleftarrow{\$} \{0, \ldots, \ell - 1\}$$
$$e \leftarrow g^t \pmod{p}$$

$$\xrightarrow{\text{commitment: } e}$$

$$r \leftarrow \{0, \ldots, \ell - 1\}$$

$$s \leftarrow t + rk \pmod{\ell} \qquad\qquad g^s \stackrel{?}{=} eh^r \pmod{p}$$

Schnorr signature, Step 1: Σ-protocol

Let $\mathbb{G} = \langle g \rangle$ where $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of prime order ℓ. The prover P randomly chooses (secret) $k \in \{0, \ldots, \ell - 1\}$ and publishes $h = g^k \pmod{p}$. Now, P can prove "knowledge" of a discrete logarithm k to a verifier V:

$$\mathsf{P} \xrightarrow[]{\;\mathbb{G},p,h\;} \mathsf{V}$$

$$t \xleftarrow{\$} \{0, \ldots, \ell - 1\}$$
$$e \leftarrow g^t \pmod{p}$$

$\xrightarrow{\text{commitment: } e}$

$$r \leftarrow \{0, \ldots, \ell - 1\}$$

$\xleftarrow{\text{challenge: } r}$

$$s \leftarrow t + rk \pmod{\ell} \qquad\qquad g^s \stackrel{?}{=} eh^r \pmod{p}$$

Schnorr signature, Step 1: Σ-protocol

Let $\mathbb{G} = \langle g \rangle$ where $g \in (\mathbb{Z}/p\mathbb{Z})^\times$ is an element of prime order ℓ. The prover P randomly chooses (secret) $k \in \{0, \ldots, \ell - 1\}$ and publishes $h = g^k \pmod{p}$. Now, P can prove “knowledge” of a discrete logarithm k to a verifier V:

$$\mathsf{P} \quad \overset{\mathbb{G}, p, h}{\text{- -}} \quad \mathsf{V}$$

$$t \overset{\$}{\leftarrow} \{0, \ldots, \ell - 1\}$$
$$e \leftarrow g^t \pmod{p}$$

$$\xrightarrow{\text{commitment: } e}$$

$$r \leftarrow \{0, \ldots, \ell - 1\}$$

$$\xleftarrow{\text{challenge: } r}$$

$$s \leftarrow t + rk \pmod{\ell} \xrightarrow{\text{response: } s} g^s \overset{?}{=} eh^r \pmod{p}$$

Schnorr signature, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain.

Schnorr signature, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain. The key generation algorithm G outputs a pair (k, h) such that $h = g^k \pmod{p}$, where k is the *secret signing key* and h is the *public verification key*.

Schnorr signature, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain. The key generation algorithm G outputs a pair (k, h) such that $h = g^k \pmod{p}$, where k is the *secret signing key* and h is the *public verification key*.

Signing $(\mathbb{G}, g, k, \mathrm{H}, m)$

1. $t \xleftarrow{\$} \{1, \ldots, \ell - 1\}$
2. $e \leftarrow g^t \pmod{p}$
3. $r \leftarrow \mathrm{H}(m \| e)$
4. $s \leftarrow t + rk \pmod{\ell}$
5. return $\sigma := (e, s)$

Schnorr signature, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain. The key generation algorithm G outputs a pair (k, h) such that $h = g^k \pmod{p}$, where k is the *secret signing key* and h is the *public verification key*.

Signing $(\mathbb{G}, g, k, \mathrm{H}, m)$

1. $t \xleftarrow{\$} \{1, \ldots, \ell - 1\}$
2. $e \leftarrow g^t \pmod{p}$
3. $r \leftarrow \mathrm{H}(m \| e)$
4. $s \leftarrow t + rk \pmod{\ell}$
5. return $\sigma \coloneqq (e, s)$

Verification $(\mathbb{G}, g, h, \mathrm{H}, m, \sigma)$

1. $r \leftarrow \mathrm{H}(m \| e)$
2. return $g^s \stackrel{?}{=} eh^r \pmod{p}$

Secure?

On Dec 20, 2016, NIST initiated the process.

Neal Koblitz | University of Washington
Alfred Menezes | University of Waterloo

In August 2015, the NSA released a major policy statement on the need for postquantum cryptography. Certain peculiarities in its wording and timing have puzzled many people and given rise to speculation concerning the NSA, elliptic curve cryptography, and quantum-safe cryptography. Of the various theories that have been proposed, some seem more plausible than others, but a definitive explanation is elusive.

"It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key." —Winston Churchill, 1939 (in reference to the Soviet Union)

In August 2015, the US government's NSA released a major policy statement on the need to develop standards for postquantum cryptography (PQC).[1] The NSA, like many other organizations, believes that the time is right to make a major push to design public-key cryptographic protocols whose security depends on hard problems that can't be solved efficiently by a quantum computer. Ever since Peter Shor's pioneering work more than 20 years ago,[2] it has been known that both the integer factorization problem, upon which RSA is based, and the elliptic curve discrete logarithm problem (ECDLP), upon which elliptic curve cryptography (ECC) is based, can be solved in polynomial time by a quantum computer.

The NSA announcement will give a tremendous boost to efforts to develop, standardize, and commercialize quantum-safe cryptography. While standards for new postquantum algorithms are several years away, in the immediate future the NSA is encouraging vendors to add quantum resistance to existing protocols by means of conventional symmetric-key tools such as the Advanced Encryption Standard (AES). Given the NSA's strong interest in PQC, the demand for quantum-safe cryptographic solutions by governments and industry will likely grow dramatically in the coming years.

Most of the NSA statement was unexceptionable. However, one passage was puzzling and unexpected:[1]

> For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.… Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy.

November/December 2016 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

Secure?

In 1994, quantum algorithm for solving the DLP. Unfortunately, that is the hard-problem used by state-of-the-art digital signatures.

Neal Koblitz | University of Washington
Alfred Menezes | University of Waterloo

In August 2015, the NSA released a major policy statement on the need for postquantum cryptography. Certain peculiarities in its wording and timing have puzzled many people and given rise to speculation concerning the NSA, elliptic curve cryptography, and quantum-safe cryptography. Of the various theories that have been proposed, some seem more plausible than others, but a definitive explanation is elusive.

"It is a riddle wrapped in a mystery inside an enigma; but perhaps there is a key." —Winston Churchill, 1939 (in reference to the Soviet Union)

In August 2015, the US government's NSA released a major policy statement on the need to develop standards for postquantum cryptography (PQC).[1] The NSA, like many other organizations, believes that the time is right to make a major push to design public-key cryptographic protocols whose security depends on hard problems that can't be solved efficiently by a quantum computer. Ever since Peter Shor's pioneering work more than 20 years ago,[2] it has been known that both the integer factorization problem, upon which RSA is based, and the elliptic curve discrete logarithm problem (ECDLP), upon which elliptic curve cryptography (ECC) is based, can be solved in polynomial time by a quantum computer.

The NSA announcement will give a tremendous boost to efforts to develop, standardize, and commercialize quantum-safe cryptography. While standards for new postquantum algorithms are several years away, in the immediate future the NSA is encouraging vendors to add quantum resistance to existing protocols by means of conventional symmetric-key tools such as the Advanced Encryption Standard (AES). Given the NSA's strong interest in PQC, the demand for quantum-safe cryptographic solutions by governments and industry will likely grow dramatically in the coming years.

Most of the NSA statement was unexceptionable. However, one passage was puzzling and unexpected:[1]

> For those partners and vendors that have not yet made the transition to Suite B algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.... Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, necessitating a re-evaluation of our cryptographic strategy.

November/December 2016 Copublished by the IEEE Computer and Reliability Societies 1540-7993/16/$33.00 © 2016 IEEE

Entrée: Supersingular isogeny graph

Supersingular elliptic curves

Recall, p is a prime larger than 3 and $q = p^n$ for $n > 0$. For $E/\mathbb{F}_q$ we have $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

Supersingular elliptic curves

Recall, p is a prime larger than 3 and $q = p^n$ for $n > 0$. For $E/\mathbb{F}_q$ we have $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

Supersingular elliptic curve

An elliptic curve over $\mathbb{F}_q$ is called *supersingular* if $p \mid t$.

Supersingular elliptic curves

Recall, p is a prime larger than 3 and $q = p^n$ for $n > 0$. For $E/\mathbb{F}_q$ we have $\#E(\mathbb{F}_q) = q + 1 - t$, where $|t| \leq 2\sqrt{q}$.

Supersingular elliptic curve

An elliptic curve over $\mathbb{F}_q$ is called *supersingular* if $p \mid t$.

Example

$E_1 : y^2 = x^3 + x$ over $\mathbb{F}_{23}$ is a supersingular elliptic curve because $\#E(\mathbb{F}_{23}) = 24$ and $t = 0$.

Isogeny

Isogeny

An isogeny between two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ is a non-constant rational function that maps points from E to points on E' and is compatible with the group law.

Isogeny

Isogeny

An isogeny between two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ is a non-constant rational function that maps points from E to points on E' and is compatible with the group law. In fact, an isogeny $\phi : E \to E'$ exists iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Isogeny

An isogeny between two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ is a non-constant rational function that maps points from E to points on E' and is compatible with the group law. In fact, an isogeny $\phi : E \to E'$ exists iff $\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q)$.

Example

For $E_1 : y^2 = x^3 + x$ and $E_2 : y^2 = x^3 + 19x$ over $\mathbb{F}_{23}$ we have

$$\begin{aligned} \phi : E_1 &\to E_2 \\ (x, y) &\mapsto \left(\frac{x^2+1}{x}, \frac{x^2y - y}{x^2}\right) \end{aligned}$$

Degree of isogeny

Degree of (separable) isogeny

The degree of a (separable) isogeny $\phi : E \to E'$ over $\mathbb{F}_q$, is the number of points on E, taken over any extension field of $\mathbb{F}_q$, mapping to $\mathcal{O}_{E'}$.

Degree of isogeny

Degree of (separable) isogeny

The degree of a (separable) isogeny $\phi : E \to E'$ over $\mathbb{F}_q$, is the number of points on E, taken over any extension field of $\mathbb{F}_q$, mapping to $\mathcal{O}_{E'}$.

Example

The degree of $\phi : E_1 \to E_2$ defined above is 2, because $(0, 0)$ and $\mathcal{O}_{E_1}$ are the only two points mapping to $\mathcal{O}_{E_2}$.

Degree of isogeny

Degree of (separable) isogeny

The degree of a (separable) isogeny $\phi : E \to E'$ over $\mathbb{F}_q$, is the number of points on E, taken over any extension field of $\mathbb{F}_q$, mapping to $\mathcal{O}_{E'}$.

Example

The degree of $\phi : E_1 \to E_2$ defined above is 2, because $(0, 0)$ and $\mathcal{O}_{E_1}$ are the only two points mapping to $\mathcal{O}_{E_2}$.

Degree is multiplicative: $\deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$

Isomorphism

Isomorphism

An isogeny of degree 1 is called an isomorphism.

Isomorphism

Isomorphism

An isogeny of degree 1 is called an isomorphism. That is, two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ are isomorphic over $\mathbb{F}_q$ if there exists a polynomial map over $\mathbb{F}_q$ that maps points on E to points on E' in a one-to-one way which is compatible with the group operation.

Isomorphism

Isomorphism

An isogeny of degree 1 is called an isomorphism. That is, two elliptic curves $E/\mathbb{F}_q$ and $E'/\mathbb{F}_q$ are isomorphic over $\mathbb{F}_q$ if there exists a polynomial map over $\mathbb{F}_q$ that maps points on E to points on E' in a one-to-one way which is compatible with the group operation.

Example

For $E_1 : y^2 = x^3 + x$ and $E_3 : y^2 = x^3 + 2x$ over $\mathbb{F}_{23}$ we have

$$\begin{aligned}\tau : E_1 &\to E_3 \\ (x, y) &\mapsto (-5x, -6y)\end{aligned}$$

Isomorphism class label

j-invariant

The j-invariant uniquely describes isomorphism classes over an algebraic closure of $\mathbb{F}_q$.

Isomorphism class label

j-invariant

The j-invariant uniquely describes isomorphism classes over an algebraic closure of $\mathbb{F}_q$. For $E : y^2 = x^3 + ax + b$ we have

$$j(E) = 1728 \frac{4a^3}{(4a^3 + 27b^2)}$$

Isomorphism class label

j-invariant

The j-invariant uniquely describes isomorphism classes over an algebraic closure of $\mathbb{F}_q$. For $E : y^2 = x^3 + ax + b$ we have

$$j(E) = 1728 \frac{4a^3}{(4a^3 + 27b^2)}$$

Note that two curves having the same j-invariant need not be isomorphic over $\mathbb{F}_q$.

Isomorphism class label

j-invariant

The j-invariant uniquely describes isomorphism classes over an algebraic closure of $\mathbb{F}_q$. For $E : y^2 = x^3 + ax + b$ we have

$$j(E) = 1728 \frac{4a^3}{(4a^3 + 27b^2)}$$

Note that two curves having the same j-invariant need not be isomorphic over $\mathbb{F}_q$.

Example

We have $j(E_1) = j(E_2) = j(E_3) = 1728 \pmod{23} = 3$. But E_1 and E_2 are not isomorphic over $\mathbb{F}_{23}$.

Isomorphism class label

j-invariant

The j-invariant uniquely describes isomorphism classes over an algebraic closure of $\mathbb{F}_q$. For $E : y^2 = x^3 + ax + b$ we have

$$j(E) = 1728 \frac{4a^3}{(4a^3 + 27b^2)}$$

Note that two curves having the same j-invariant need not be isomorphic over $\mathbb{F}_q$.

Example

We have $j(E_1) = j(E_2) = j(E_3) = 1728 \pmod{23} = 3$. But E_1 and E_2 are not isomorphic over $\mathbb{F}_{23}$.

If E is supersingular, then we can replace "algebraic closure of $\mathbb{F}_q$" with $\mathbb{F}_{p^2}$.

Supersingular isomorphism classes

The number of supersingular isomorphism classes over an algebraic closure of $\mathbb{F}_p$, with representative curves defined over $\mathbb{F}_{p^2}$, is $S_p := \left\lfloor \frac{p}{12} \right\rfloor + \epsilon$ where $\epsilon \in \{0, 1, 2\}$.

Supersingular isomorphism classes

The number of supersingular isomorphism classes over an algebraic closure of $\mathbb{F}_p$, with representative curves defined over $\mathbb{F}_{p^2}$, is $S_p := \left\lfloor \frac{p}{12} \right\rfloor + \epsilon$ where $\epsilon \in \{0, 1, 2\}$.

Example

$S_{23} = 3$ with the classes represented by the j-invariants $0, 3, 19$.

Supersingular ℓ-isogeny graph

Let ℓ be a prime different from p. The supersingular ℓ-isogeny graph over an algebraic closure of $\mathbb{F}_q$ is the directed multigraph $G_\ell(p)$ whose vertices belong to the set of isomorphism classes of supersingular elliptic curves $\{j(E_1), \ldots, j(E_s)\}$ with $s = S_p$ and $E_i/\mathbb{F}_{p^2}$; there is a directed edge $[E_i, E_{i'}]$ for each equivalence class (same kernel) of ℓ-isogenies from E_i to $E_{i'}$.

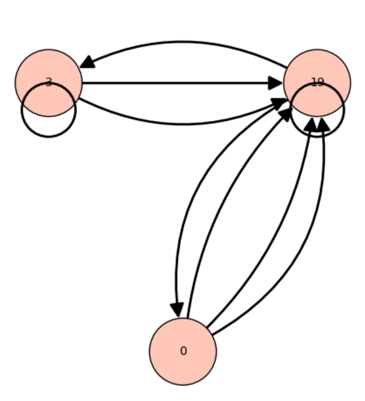
Supersingular ℓ-isogeny graph

Let ℓ be a prime different from p. The supersingular ℓ-isogeny graph over an algebraic closure of $\mathbb{F}_q$ is the directed multigraph $G_\ell(p)$ whose vertices belong to the set of isomorphism classes of supersingular elliptic curves $\{j(E_1), \ldots, j(E_s)\}$ with $s = S_p$ and $E_i/\mathbb{F}_{p^2}$; there is a directed edge $[E_i, E_{i'}]$ for each equivalence class (same kernel) of ℓ-isogenies from E_i to $E_{i'}$. Hence the out-degree of each vertex is $\ell + 1$.

Supersingular ℓ-isogeny graph

Let ℓ be a prime different from p. The supersingular ℓ-isogeny graph over an algebraic closure of $\mathbb{F}_q$ is the directed multigraph $G_\ell(p)$ whose vertices belong to the set of isomorphism classes of supersingular elliptic curves $\{j(E_1), \ldots, j(E_s)\}$ with $s = S_p$ and $E_i/\mathbb{F}_{p^2}$; there is a directed edge $[E_i, E_{i'}]$ for each equivalence class (same kernel) of ℓ-isogenies from E_i to $E_{i'}$. Hence the out-degree of each vertex is $\ell + 1$.

Example: $G_2(23)$



Endomorphism ring

The endomorphism ring of E, $\mathrm{End}_{\mathbb{F}_q}(E)$, is the set of $\mathbb{F}_q$-isogenies from E to itself, together with the zero map $[0] : E \to E$ given $[0](P) = \mathcal{O}_E$.

Endomorphism ring

The endomorphism ring of E, $\mathrm{End}_{\mathbb{F}_q}(E)$, is the set of $\mathbb{F}_q$-isogenies from E to itself, together with the zero map $[0] : E \to E$ given $[0](P) = \mathcal{O}_E$. In particular, for isogenies over an algebraic closure of $\mathbb{F}_q$, we write $\mathrm{End}(E)$.

Endomorphism ring

The endomorphism ring of E, $\mathrm{End}_{\mathbb{F}_q}(E)$, is the set of $\mathbb{F}_q$-isogenies from E to itself, together with the zero map $[0] : E \to E$ given $[0](P) = \mathcal{O}_E$. In particular, for isogenies over an algebraic closure of $\mathbb{F}_q$, we write $\mathrm{End}(E)$.

Example

For $E_1 : y^2 = x^3 + x$ over $\mathbb{F}_{23}$, we have

$$\mathrm{End}(E_1) = \mathbb{Z}\,\mathrm{id} + \mathbb{Z}\iota + \mathbb{Z}\frac{\iota + \pi}{2} + \mathbb{Z}\frac{\mathrm{id} + \iota \circ \pi}{2}$$

where $\pi, \iota \in \mathrm{End}(E_1)$ such that $\pi(x, y) = (x^{23}, y^{23})$ and $\iota(x, y) = (-x, \alpha y)$ is an isomorphism over $\mathbb{F}_{23^2} = \mathbb{F}_{23}(\alpha)$ with $\alpha^2 + 1 = 0$.

Endomorphism ring

The endomorphism ring of E, $\mathrm{End}_{\mathbb{F}_q}(E)$, is the set of $\mathbb{F}_q$-isogenies from E to itself, together with the zero map $[0] : E \to E$ given $[0](P) = \mathcal{O}_E$. In particular, for isogenies over an algebraic closure of $\mathbb{F}_q$, we write $\mathrm{End}(E)$.

Example

For $E_1 : y^2 = x^3 + x$ over $\mathbb{F}_{23}$, we have

$$\mathrm{End}(E_1) = \mathbb{Z}\,\mathrm{id} + \mathbb{Z}\iota + \mathbb{Z}\frac{\iota + \pi}{2} + \mathbb{Z}\frac{\mathrm{id} + \iota \circ \pi}{2}$$

where $\pi, \iota \in \mathrm{End}(E_1)$ such that $\pi(x, y) = (x^{23}, y^{23})$ and $\iota(x, y) = (-x, \alpha y)$ is an isomorphism over $\mathbb{F}_{23^2} = \mathbb{F}_{23}(\alpha)$ with $\alpha^2 + 1 = 0$. Moreover, $\iota \circ \iota = [-1]$, $\pi \circ \pi = [-23]$, and $\iota \circ \pi = -\pi \circ \iota$; i.e. $\mathrm{End}(E_1)$ is a non-commutative ring.

Maximal orders

Deuring correspondence - I

E is a supersingular elliptic curve over $\mathbb{F}_q$ if and only if $\mathrm{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$.

Maximal orders

Deuring correspondence - I

E is a supersingular elliptic curve over $\mathbb{F}_q$ if and only if $\mathbf{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$.

Quaternion algebra

A quaternion algebra over $\mathbb{Q}$ is of the form $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{ij}$, where $\mathbf{i}^2, \mathbf{j}^2 \in \mathbb{Q}^\times$, and $\mathbf{ij} = -\mathbf{ji}$. In particular, we have

$$B_{p,\infty} = \begin{cases} \mathbf{i}^2 = -1, \mathbf{j}^2 = -1 & \text{if } p = 2 \\ \mathbf{i}^2 = -1, \mathbf{j}^2 = -p & \text{if } p \equiv 3 \pmod 4 \\ \mathbf{i}^2 = -2, \mathbf{j}^2 = -p & \text{if } p \equiv 5 \pmod 8 \\ \mathbf{i}^2 = -\ell, \mathbf{j}^2 = -p & \text{if } p \equiv 1 \pmod 8 \end{cases}$$

where $\ell \equiv 3 \pmod 4$ is a prime quadratic non-residue mod p.

Deuring correspondence - I

E is a supersingular elliptic curve over $\mathbb{F}_q$ if and only if $\mathrm{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$.

Quaternion (maximal) order

$O \subseteq \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ is called an *order* if O is a ring whose elements are integral, $\mathbb{Z} \subseteq O$, and contains a basis for $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ as $\mathbb{Q}$-vector space. Moreover, an order $O \subsetneq B$ is called *maximal* if it is not properly contained in another order.

Maximal orders

Deuring correspondence - I

E is a supersingular elliptic curve over $\mathbb{F}_q$ if and only if $\mathbf{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$.

Example

In $B_{23,\infty} = \langle \mathbf{i}, \mathbf{j} \mid \mathbf{i}^2 = -1, \mathbf{j}^2 = -23, \mathbf{ij} = -\mathbf{ji} \rangle$, two examples of maximal orders are

$$O_1 = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\frac{\mathbf{i}+\mathbf{j}}{2} + \mathbb{Z}\frac{1+\mathbf{ij}}{2}; \text{ and}$$

$$O_2 = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\frac{1+\mathbf{j}}{2} + \mathbb{Z}\frac{\mathbf{i}(1+\mathbf{j})}{2}$$

Note that O_1 is isomorphic to $\mathbf{End}(E_1)$ we saw above.

Maximal orders

Deuring correspondence - I

E is a supersingular elliptic curve over $\mathbb{F}_q$ if and only if $\mathrm{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$.

Mestre-Oesterle-Ribet

$$\left\{\begin{array}{l}\text{isomorphism classes}\\ \text{of supersingular}\\ \text{elliptic curves over } \overline{\mathbb{F}}_p\end{array}\right\} \Big/ \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \longleftrightarrow \left\{\begin{array}{l}\text{maximal orders}\\ \text{of } B_{p,\infty}\end{array}\right\} /\cong$$

That is, there is one-to-one correspondence if $j(E) \in \mathbb{F}_p$ and two-to-one correspondence if $j(E) \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$.

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) \cong O \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_{\mathrm{L}}(O)$.

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) \cong O \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_{\mathrm{L}}(O)$.

Quaternion (left) O-ideal

$I \subseteq \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ is called an *ideal* if I is a $\mathbb{Z}$-module that contains a basis for $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$ as $\mathbb{Q}$-vector space. Furthermore, given an order O of $\mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$, I is called a *left O-ideal* if $\alpha I \subseteq I$ for all $\alpha \in O$.

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\operatorname{End}(E) \cong O \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_{\mathrm{L}}(O)$.

Left-ideal class set

We say ideals I, J are in the *same left class*, $I \sim_{\mathrm{L}} J$, if there exists $\alpha \in B^{\times}$ such that $I\alpha = J$. Furthermore, the left equivalence class is denoted by $[I]_{\mathrm{L}}$. In particular, we have

$$\mathrm{Cls}_{\mathrm{L}}(O) := \{[I]_{\mathrm{L}} \mid I \text{ is an } \textit{invertible} \text{ left } O\text{-ideal}\}$$

$\mathrm{Cls}_{\mathrm{L}}(O)$ has has the structure of a *pointed set* with distinguished element $[O]_{\mathrm{L}} \in \mathrm{Cls}_{\mathrm{L}}(O)$.

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) \cong O \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_L(O)$.

Example

Let $O_2 \subset B_{23,\infty}$ as above. Then we have $\mathrm{Cls}_L(O_2) = \{[I_1]_L, [I_2]_L, [I_3]_L\}$ with

$$I_1 = 2\mathbb{Z}(1+\mathbf{j}) + 2\mathbb{Z}\mathbf{i}(1+\mathbf{j}) + 4\mathbb{Z}\mathbf{j} + 4\mathbb{Z}\mathbf{ij},$$
$$I_2 = 2\mathbb{Z}(1+3\mathbf{j}) + 2\mathbb{Z}\mathbf{i}(1+3\mathbf{j}) + 8\mathbb{Z}\mathbf{j} + 8\mathbb{Z}\mathbf{ij}, \text{ and}$$
$$I_3 = 2\mathbb{Z}(1+3\mathbf{j}+4\mathbf{ij}) + 2\mathbb{Z}(\mathbf{i}+4\mathbf{j}+3\mathbf{ij}) + 16\mathbb{Z}\mathbf{j} + 16\mathbb{Z}\mathbf{ij}$$

Here $[I_1]_L$, $[I_2]_L$, and $[I_3]_L$ correspond to the isomorphism classes of supersingular curves represented by j-invariants 3, 19, and 0, respectively.

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathbf{End}(E) \cong O \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathbf{Cls}_{\mathrm{L}}(O)$.

Waterhouse

$E[I] := \{P \in E(\overline{\mathbb{F}}_p) \mid \phi(P) = 0 \ \forall \text{ separable } \phi \in I\}$, where I is a nonzero left $\mathbf{End}(E)$-ideal. $\phi_I : E \to E/E[I]$ with $\mathbf{deg}(\phi_I) = \#E[I]$.

$I(H) := \{\phi \in \mathbf{End}(E) \mid \phi(P) = 0 \text{ for all } P \in H\}$, where $H \leq E(\overline{\mathbb{F}}_p)$ is finite. If $\phi : E \to E'$ an isogeny, then $I_\phi := I(\mathbf{ker}(\phi))$ a left $\mathbf{End}(E)$-ideal and right $\mathbf{End}(E')$-ideal (connecting ideal).

Left ideals

Deuring correspondence - II

Fix, E, a supersingular elliptic curve over $\overline{\mathbb{F}}_p$ with $\mathrm{End}(E) \cong \mathcal{O} \subseteq B_{p,\infty}$. There is a bijection between isomorphism classes over $\overline{\mathbb{F}}_p$ and the left class set $\mathrm{Cls}_{\mathrm{L}}(\mathcal{O})$.

Waterhouse

- $E[I(H)] = H$ and $I(E[I]) = I$ (overloaded notation).
- If $I \sim_{\mathrm{L}} J$ then $E/E[I] \cong E/E[J]$.
- $\phi_{I.J} = \tau_J \circ \phi_I$ and $I_{\tau \circ \phi} = I_\phi \cdot I_\tau$
- $\phi_{\overline{I}} = \widehat{\phi_I}$ (dual isogeny) and $I_{\widehat{\phi}} = \overline{I_\phi}$
- $\deg(\phi_I) = \mathrm{nrd}(I)$ and $\mathrm{nrd}(I_\phi) = \deg(\phi)$

Eichler orders

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\gcd(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Eichler orders

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\gcd(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Eichler order

An *Eichler order* $O \subset B$ is the intersection of two (not necessarily distinct) maximal orders. Therefore, maximal orders are also Eichler orders.

Eichler orders

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\gcd(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Level of an Eichler order

The level of an Eichler order O, is defined as the ratio of the reduced discriminant of order O and the discriminant of the quaternion algebra $B = \mathbb{Q}\langle \mathbf{i}, \mathbf{j} \rangle$.

$$\mathrm{lev}(O) = \frac{\mathrm{discrd}(O)}{\mathrm{disc}(B)}$$

From the definition of (reduced) discriminants it follows that maximal orders are Eichler orders of level 1.

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\gcd(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Example

$O_3 = O_1 \cap O_2 = \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\mathbf{j} + \mathbb{Z}\dfrac{1 + \mathbf{i} + \mathbf{j} + \mathbf{ij}}{2}$ is an Eichler order of level 2, because $\mathrm{discrd}(O_3) = 46$ and $\mathrm{disc}(B_{23,\infty}) = 23$. Therefore, if $\phi \in \mathrm{End}(E, C) \cong O_3$ then $\phi \in \mathrm{End}(E)$ such that $\phi(C) = C$ with $\#C = 2$.

Eichler orders

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\gcd(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Kohel

Fix a base point (E_0, C_0), where $C_0 \leq E(\overline{\mathbb{F}}_p)$ is a cyclic subgroup of order M. Then $\mathrm{End}(E_0, C_0)$, the subring of $\mathrm{End}(E_0)$ that maps C_0 to itself, is an Eichler order of level M and reduced discriminant pM.

Eichler orders

Deuring correspondence - III

(E, C) is a pair of supersingular elliptic curve over $\overline{\mathbb{F}}_p$ and cyclic subgroup of order M with $\mathbf{gcd}(p, M) = 1$ iff $\mathrm{End}(E, C) \cong O(M) \subseteq B_{p,\infty}$ an Eichler order of level M.

Kohel

Let $\mathcal{S}_M$ be the category of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ equipped with a cyclic M-isogeny (under isogenies identifying the cyclic subgroups).
Let $\mathcal{I}_M$ be the category of left $\mathrm{End}(E_0, C_0)$-ideals (under module homomorphisms).

Then the functor $\mathrm{Hom}(-, (E_0, C_0))$ from $\mathcal{S}_M$ to $\mathcal{I}_M$ is an equivalence of categories.

Spectral graph theory

Deuring correspondence lets us use the relationship between quaternion algebras and modular forms to study the eigenvalues of the adjacency matrix of $G_\ell(p)$.

Spectral graph theory

Deuring correspondence lets us use the relationship between quaternion algebras and modular forms to study the eigenvalues of the adjacency matrix of $G_\ell(p)$.

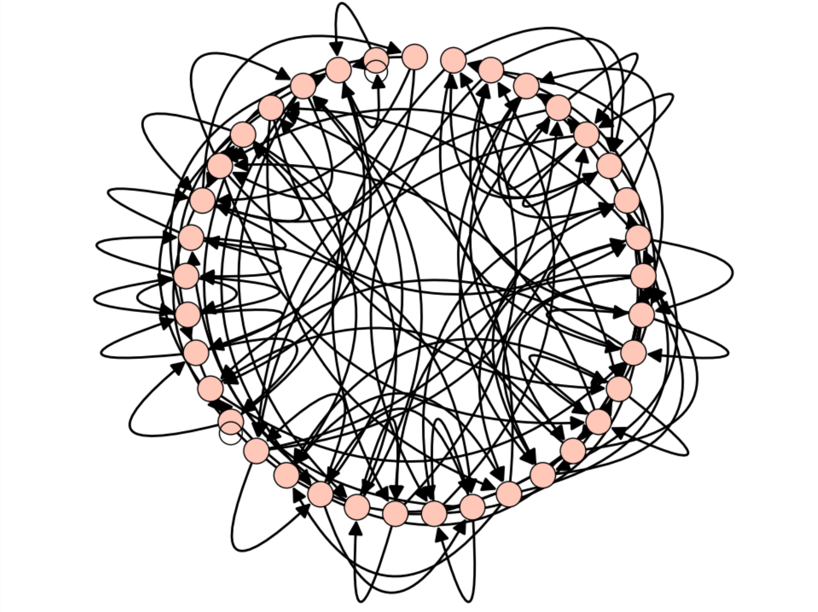
1. $G_\ell(p)$ is connected with diameter $O(\log p)$, where the constant in the bound is independent of ℓ. That is, the largest number of vertices which must be traversed in order to travel from one vertex to another when paths which backtrack, detour, or loop are excluded from consideration is $O(\log p)$.

Spectral graph theory

Deuring correspondence lets us use the relationship between quaternion algebras and modular forms to study the eigenvalues of the adjacency matrix of $G_\ell(p)$.

1. $G_\ell(p)$ is connected with diameter $O(\log p)$, where the constant in the bound is independent of ℓ. That is, the largest number of vertices which must be traversed in order to travel from one vertex to another when paths which backtrack, detour, or loop are excluded from consideration is $O(\log p)$.
2. $G_\ell(p)$ is an *expander graph*, i.e. simultaneously sparse and highly connected. Therefore, the natural random walk on $G_\ell(p)$ converges to its limiting distribution as rapidly as possible.

$G_2(431)$ with 37 vertices and diameter 7



Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ such that $\mathcal{O} \cong \mathrm{End}(E)$.

Easier problems

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ such that $\mathcal{O} \cong \mathrm{End}(E)$.

Easier problems

1. Given maximal order $\mathcal{O} \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathrm{End}(E(j)) \cong \mathcal{O}$.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathrm{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathrm{End}(E)$.

Easier problems

1. Given maximal order $O \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathrm{End}(E(j)) \cong O$.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $\mathcal{O} \subseteq B_{p,\infty}$ such that $\mathcal{O} \cong \mathrm{End}(E)$.

2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathrm{End}(E)$.

Easier problems

1. Given maximal order $\mathcal{O} \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathrm{End}(E(j)) \cong \mathcal{O}$.

2. Find all the maximal orders (up to isomorphism) of $B_{p,\infty}$.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathbf{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathbf{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.

Easier problems

1. Given maximal order $O \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathbf{End}(E(j)) \cong O$.
2. Find all the maximal orders (up to isomorphism) of $B_{p,\infty}$.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathbf{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathbf{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.

Easier problems

1. Given maximal order $O \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathbf{End}(E(j)) \cong O$.
2. Find all the maximal orders (up to isomorphism) of $B_{p,\infty}$.
3. Given maximal orders $O, O' \subseteq B_{p,\infty}$ find an ideal I that is left O-ideal and right O'-ideal.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathrm{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathrm{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.
4. Given a maximal order in $B_{p,\infty}$, determine the ideal class set.

Easier problems

1. Given maximal order $O \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathrm{End}(E(j)) \cong O$.
2. Find all the maximal orders (up to isomorphism) of $B_{p,\infty}$.
3. Given maximal orders $O, O' \subseteq B_{p,\infty}$ find an ideal I that is left O-ideal and right O'-ideal.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathbf{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathbf{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.
4. Given a maximal order in $B_{p,\infty}$, determine the ideal class set.

Easier problems

1. Given maximal order $O \subseteq B_{p,\infty}$, find a supersingular j-invariant such that $\mathbf{End}(E(j)) \cong O$.
2. Find all the maximal orders (up to isomorphism) of $B_{p,\infty}$.
3. Given maximal orders $O, O' \subseteq B_{p,\infty}$ find an ideal I that is left O-ideal and right O'-ideal.
4. Given p, determine (all) supersingular j-invariants in $\mathbb{F}_{p^2}$.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathrm{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathrm{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.

Equivalent and quantum-safe

- All three problems are known to be equivalent.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathbf{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathbf{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.

Equivalent and quantum-safe

- All three problems are known to be equivalent.
- The fact that $\mathbf{End}(E)$ is non-commutative makes these problems resistant to known quantum algorithms.

Problems about supersingular elliptic curves

Difficult problems

1. Given $E/\mathbb{F}_{p^2}$, find a maximal order $O \subseteq B_{p,\infty}$ such that $O \cong \mathrm{End}(E)$.
2. Given $E/\mathbb{F}_{p^2}$, chosen uniformly at random, determine $\mathrm{End}(E)$.
3. Given $j, j' \in \mathbb{F}_{p^2}$ find an isogeny $\phi : E \to E'$ such that $j(E) = j$ and $j(E') = j'$.

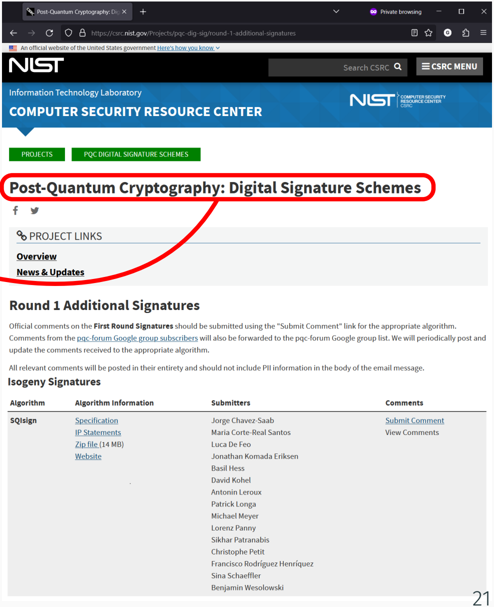
Equivalent and quantum-safe

- All three problems are known to be equivalent.
- The fact that $\mathrm{End}(E)$ is non-commutative makes these problems resistant to known quantum algorithms.
- We can rewrite these problems in terms of cyclic M-isogenies and Eichler orders of level M. For SQIsign, we assume that given $E/\mathbb{F}_{p^2}$ it is *difficult* to find a (non-trivial) cyclic endomorphism of E of smooth degree.

Dessert: Quantum-safe signature

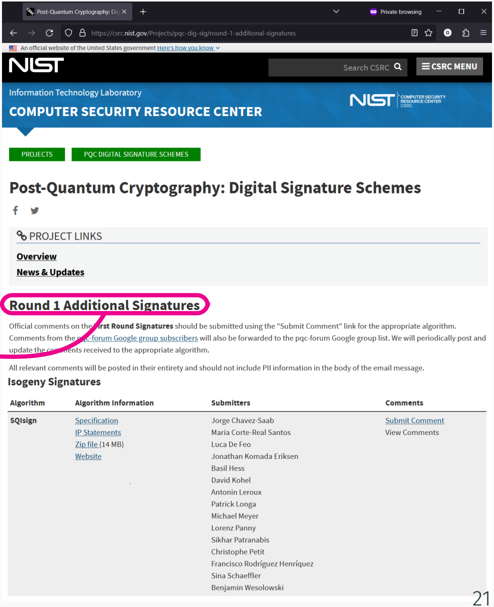
NIST list

In 2022, NIST selected two lattice-based signatures (*CRYSTALS-Dilithium* and *FALCON*) and one hash-based signature (*SPHINCS+*)



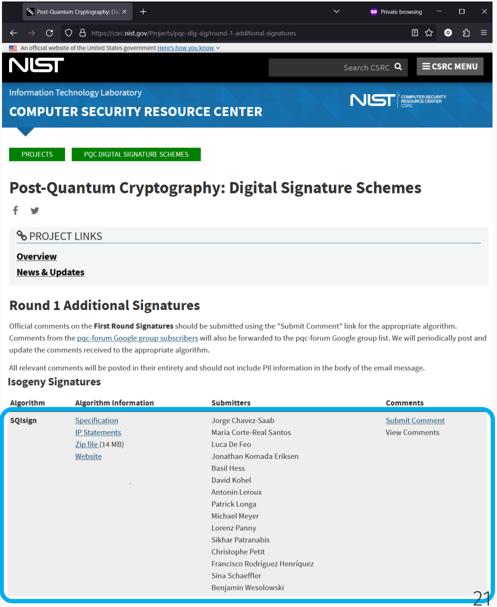
NIST list

Signature schemes with short signatures and fast verification; not based on structured lattices.



NIST list

Only submission based on isogeny; shortest signatures; fast verification; complex signing procedure



Post-Quantum Cryptography: Dig ×

https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures

An official website of the United States government Here's how you know

NIST

Search CSRC

CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

PQC DIGITAL SIGNATURE SCHEMES

Post-Quantum Cryptography: Digital Signature Schemes

PROJECT LINKS

Overview

News & Updates

Round 1 Additional Signatures

Official comments on the **First Round Signatures** should be submitted using the "Submit Comment" link for the appropriate algorithm. Comments from the pqc-forum Google group subscribers will also be forwarded to the pqc-forum Google group list. We will periodically post and update the comments received to the appropriate algorithm.

All relevant comments will be posted in their entirety and should not include PII information in the body of the email message.

Isogeny Signatures

Algorithm	Algorithm Information	Submitters	Comments
SQIsign	Specification IP Statements Zip file (14 MB) Website	Jorge Chavez-Saab Maria Corte-Real Santos Luca De Feo Jonathan Komada Eriksen Basil Hess David Kohel Antonin Leroux Patrick Longa Michael Meyer Lorenz Panny Sikhar Patranabis Christophe Petit Francisco Rodríguez Henríquez Sina Schaeffler Benjamin Wesolowski	Submit Comment View Comments

Preparation for SQIsign

Let λ be the security parameter.

- Fix a prime $p \equiv 3 \pmod 4$ with $\log_2(p) \approx 2\lambda$. such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{5/4}$ and f is as big as possible.

Preparation for SQIsign

Let λ be the security parameter.

- Fix a prime $p \equiv 3 \pmod 4$ with $\log_2(p) \approx 2\lambda.$ such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{5/4}$ and f is as big as possible.
- Let $N2^f = MM'$ such that M is a λ-bit integer consisting all the smallest factors, and M' is a 2λ-bit integer.

Preparation for SQIsign

Let λ be the security parameter.

- Fix a prime $p \equiv 3 \pmod 4$ with $\log_2(p) \approx 2\lambda.$ such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{5/4}$ and f is as big as possible.
- Let $N2^f = MM'$ such that M is a λ-bit integer consisting all the smallest factors, and M' is a 2λ-bit integer.
- Let $L = 2^e \simeq p^{15/4}$, where e is greater than the diameter of $G_2(p)$.

Preparation for SQIsign

Let λ be the security parameter.

- Fix a prime $p \equiv 3 \pmod 4$ with $\log_2(p) \approx 2\lambda.$ such that the $N2^f$-torsion subgroup is defined over a small extension of $\mathbb{F}_{p^2}$ for smooth number $N \simeq p^{5/4}$ and f is as big as possible.
- Let $N2^f = MM'$ such that M is a λ-bit integer consisting all the smallest factors, and M' is a 2λ-bit integer.
- Let $L = 2^e \simeq p^{15/4}$, where e is greater than the diameter of $G_2(p)$.
- Fix $E_0 : y^2 = x^3 + x$ with known endomorphism ring $O_0 := \mathrm{End}(E_0)$.

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove "knowledge" of $O_1 := \mathbf{End}(E_1)$ to a verifier V:

P	V
$\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -)$ of degree M'	
$E_1' = \phi'(E_0)$	
	$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$
	$\tau \leftarrow \mathbf{Hom}((E_1', C), -)$
$\eta : E_1 \to E_2',\ \mathbf{ker}(\widehat{\tau} \circ \eta)$ cyclic	$\eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2'),\ \mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=}$ cyclic

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove "knowledge" of $O_1 \coloneqq \mathbf{End}(E_1)$ to a verifier V:

$$\text{P} \xrightarrow{\quad p, E_0, O_0, M, L, E_1 \quad} \text{V}$$

$$\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -) \text{ of degree } M'$$

$$E_1' = \phi'(E_0)$$

$$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$$

$$\tau \leftarrow \mathbf{Hom}((E_1', C), -)$$

$$\eta : E_1 \to E_2', \ \mathbf{ker}(\widehat{\tau} \circ \eta) \text{ cyclic}$$

$$\eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2'), \ \mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=} \text{cyclic}$$

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove "knowledge" of $O_1 := \mathbf{End}(E_1)$ to a verifier V:

$$\mathsf{P} \xrightarrow{p, E_0, O_0, M, L, E_1} \mathsf{V}$$

$$\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -) \text{ of degree } M'$$

$$E_1' = \phi'(E_0)$$

$$\xrightarrow{E_1'}$$

$$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$$

$$\tau \leftarrow \mathbf{Hom}((E_1', C), -)$$

$$\eta : E_1 \to E_2', \ \mathbf{ker}(\widehat{\tau} \circ \eta) \text{ cyclic}$$

$$\eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2'), \ \mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=} \text{cyclic}$$

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove "knowledge" of $O_1 \coloneqq \mathbf{End}(E_1)$ to a verifier V:

$$\mathsf{P} \quad \xrightarrow{\;p, E_0, O_0, M, L, E_1\;} \quad \mathsf{V}$$

$$\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -) \text{ of degree } M'$$

$$E_1' = \phi'(E_0)$$

$$\xrightarrow{\;E_1'\;}$$

$$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$$

$$\tau \leftarrow \mathbf{Hom}((E_1', C), -)$$

$$\xleftarrow{\;\tau : E_1' \to E_2'\;}$$

$$\eta : E_1 \to E_2', \ \mathbf{ker}(\widehat{\tau} \circ \eta) \text{ cyclic}$$

$$\eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2'), \ \mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=} \text{cyclic}$$

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove “knowledge” of $O_1 := \mathbf{End}(E_1)$ to a verifier V:

$$\mathsf{P} \xrightarrow[\qquad\qquad\qquad]{p,E_0,O_0,M,L,E_1} \mathsf{V}$$

$$\phi' \xleftarrow{\$} \mathbf{Hom}(E_0,-) \text{ of degree } M'$$

$$E_1' = \phi'(E_0)$$

$$\xrightarrow{E_1'}$$

$$C \leq E_1'(\overline{\mathbb{F}}_p), C \cong \mathbb{Z}/M\mathbb{Z}$$

$$\tau \leftarrow \mathbf{Hom}((E_1', C), -)$$

$$\xleftarrow{\tau : E_1' \to E_2'}$$

$$\eta : E_1 \to E_2',\ \mathbf{ker}(\widehat{\tau} \circ \eta) \text{ cyclic} \xrightarrow{\qquad \eta \qquad} \eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2'),\ \mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=} \text{cyclic}$$

SQIsign, Step 1: Σ-protocol

The prover P chooses a random isogeny $\phi : E_0 \to E_1$ such that $\mathbf{deg}(\phi)$ is a prime smaller than $2^{\lambda/2}$, leading to a random elliptic curve E_1. P keeps ϕ secret and publishes E_1. Now, P can prove "knowledge" of $O_1 := \mathbf{End}(E_1)$ to a verifier V:

$$\begin{tikzcd}
E_0 \arrow[r, "\text{secret: } \phi"] \arrow[d, "\text{secret: } \phi'"'] & E_1 \arrow[d, squiggly, "\eta", "\text{response}"'] \\
E_1' \arrow[r, dashed, "\tau", "\text{challenge}"'] & E_2'
\end{tikzcd}$$

Computing L-isogeny $\eta : E_1 \to E_2'$

1. Translate isogeny $\tau \circ \phi' \circ \widehat{\phi}$ to left O_1-ideal $I := \bar{I}_\phi \cdot I_{\phi'} \cdot I_\tau$ (*`isogeny-to-kernel-to-ideal`*).
2. From I, I_ϕ get $J \in [I]_L$ with $\mathbf{nrd}(J) = L$.
3. Translate left O_1-ideal J to η (*`ideal-to-kernel-to-isogeny`*)

SQIsign, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain (based on a compression algorithm).

SQIsign, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain (based on a compression algorithm). The key generation algorithm G outputs a pair $(\mathcal{O}_1, E_1)$ such that $\mathcal{O}_1 = \mathrm{End}(E_1)$, where $\mathcal{O}_1$ is the *secret signing key* and E_1 is the *public verification key*.

SQIsign, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain (based on a compression algorithm). The key generation algorithm G outputs a pair $(\mathcal{O}_1, E_1)$ such that $\mathcal{O}_1 = \mathbf{End}(E_1)$, where $\mathcal{O}_1$ is the *secret signing key* and E_1 is the *public verification key*.

Signing $(M', M, L, \mathcal{O}_1, \mathrm{H}, m)$

1. $\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -)$ of degree M'
2. $E_1' = \phi'(E_0)$
3. $b = \mathrm{H}(m \| j(E_1'))$
4. $\tau = \mathbf{Decompress}(E_1', b)$
5. $\eta : E_1 \to E_2'$, $\ker(\widehat{\tau} \circ \eta)$ cyclic
6. return $\sigma \coloneqq (E_1', \eta)$

SQIsign, Step 2: Fiat-Shamir transformation

Choose a *random oracle* cryptographic hash function H with appropriate domain and codomain (based on a compression algorithm). The key generation algorithm G outputs a pair (O_1, E_1) such that $O_1 = \mathbf{End}(E_1)$, where O_1 is the *secret signing key* and E_1 is the *public verification key*.

Signing $(M', M, L, O_1, \mathrm{H}, m)$

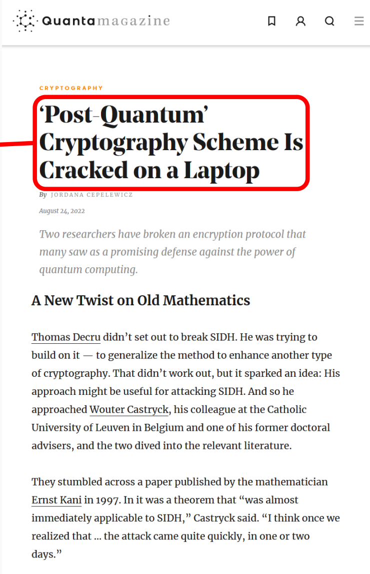
1. $\phi' \xleftarrow{\$} \mathbf{Hom}(E_0, -)$ of degree M'
2. $E_1' = \phi'(E_0)$
3. $b = \mathrm{H}(m \| j(E_1'))$
4. $\tau = \mathbf{Decompress}(E_1', b)$
5. $\eta : E_1 \to E_2'$, $\mathbf{ker}(\widehat{\tau} \circ \eta)$ cyclic
6. return $\sigma := (E_1', \eta)$

Verification $(M, L, E_1, \mathrm{H}, m, \sigma)$

1. $b = \mathrm{H}(m \| j(E_1'))$
2. $\tau = \mathbf{Decompress}(E_1', b)$
3. return $\eta \overset{?}{\in} \mathbf{Hom}(E_1, E_2')$, $\mathbf{ker}(\widehat{\tau} \circ \eta) \overset{?}{=}$ cyclic

Quantum-safe?

SIDH (2011-2022) reached Round 4 of NIST's quantum-safe KEM list.



Quanta magazine

CRYPTOGRAPHY

'Post-Quantum' Cryptography Scheme Is Cracked on a Laptop

By JORDANA CEPELEWICZ

August 24, 2022

Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.

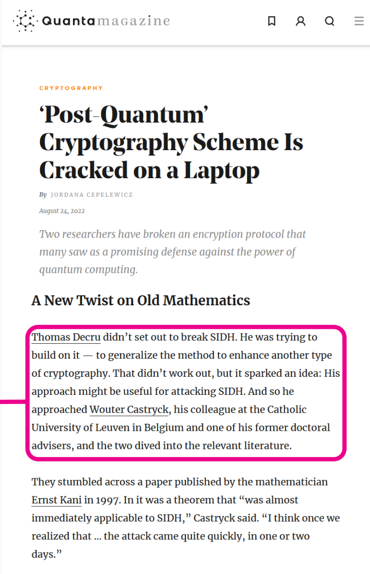
A New Twist on Old Mathematics

Thomas Decru didn't set out to break SIDH. He was trying to build on it — to generalize the method to enhance another type of cryptography. That didn't work out, but it sparked an idea: His approach might be useful for attacking SIDH. And so he approached Wouter Castryck, his colleague at the Catholic University of Leuven in Belgium and one of his former doctoral advisers, and the two dived into the relevant literature.

They stumbled across a paper published by the mathematician Ernst Kani in 1997. In it was a theorem that "was almost immediately applicable to SIDH," Castryck said. "I think once we realized that ... the attack came quite quickly, in one or two days."

Quantum-safe?

On August 5, 2022, Castryck and Decru posted a preprint outlining an efficient classical key recovery algorithm against SIDH.



Quantamagazine

CRYPTOGRAPHY

'Post-Quantum' Cryptography Scheme Is Cracked on a Laptop

By JORDANA CEPELEWICZ

August 24, 2022

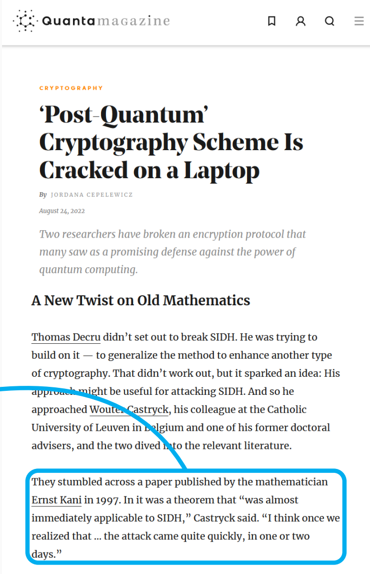
Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.

A New Twist on Old Mathematics

Thomas Decru didn't set out to break SIDH. He was trying to build on it — to generalize the method to enhance another type of cryptography. That didn't work out, but it sparked an idea: His approach might be useful for attacking SIDH. And so he approached Wouter Castryck, his colleague at the Catholic University of Leuven in Belgium and one of his former doctoral advisers, and the two dived into the relevant literature.

They stumbled across a paper published by the mathematician Ernst Kani in 1997. In it was a theorem that "was almost immediately applicable to SIDH," Castryck said. "I think once we realized that ... the attack came quite quickly, in one or two days."

SQISignHD uses this constructively: easier to generate public parameters & simpler signing procedure; but needs efficient implimentation of 4D isogeny.



Quanta magazine

CRYPTOGRAPHY

‘Post-Quantum’ Cryptography Scheme Is Cracked on a Laptop

By JORDANA CEPELEWICZ

August 24, 2022

Two researchers have broken an encryption protocol that many saw as a promising defense against the power of quantum computing.

A New Twist on Old Mathematics

Thomas Decru didn’t set out to break SIDH. He was trying to build on it — to generalize the method to enhance another type of cryptography. That didn’t work out, but it sparked an idea: His approach might be useful for attacking SIDH. And so he approached Wouter Castryck, his colleague at the Catholic University of Leuven in Belgium and one of his former doctoral advisers, and the two dived into the relevant literature.

They stumbled across a paper published by the mathematician Ernst Kani in 1997. In it was a theorem that “was almost immediately applicable to SIDH,” Castryck said. “I think once we realized that … the attack came quite quickly, in one or two days.”

Questions?

ECDSA

Choose a cryptographic hash function H with appropriate domain and codomain. The key generation algorithm G outputs a pair (k, Q) such that $Q = [k]P$, where k is the *secret signing key* and Q is the *public verification key*.

Signing $(\mathbb{G}, P, k, \mathrm{H}, m)$

1. $t \xleftarrow{\$} \{1, \ldots, \ell - 1\}$
2. $R \leftarrow [t]P$
3. $r \leftarrow x(R) \pmod{\ell}$
4. if $r = 0$ then goto Step 1.
5. $e \leftarrow \mathrm{H}(m)$
6. $s \leftarrow (e + kr)t^{-1} \pmod{\ell}$
7. if $s = 0$ then goto Step 1.
8. return $\sigma := (r, s)$

Verification $(\mathbb{G}, P, Q, \mathrm{H}, m, \sigma)$

1. $e \leftarrow \mathrm{H}(m)$
2. $u_1 \leftarrow es^{-1} \pmod{\ell}$, $u_2 \leftarrow rs^{-1} \pmod{\ell}$
3. $T \leftarrow [u_1]P + [u_2]Q$
4. return $r \stackrel{?}{=} x(T) \pmod{\ell}$

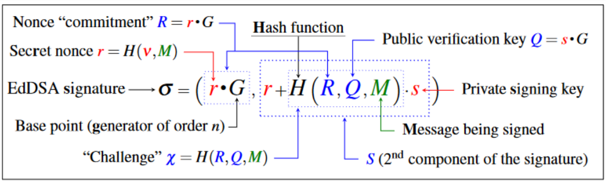
EdDSA, a footnote

Twisted Edwards model

A twisted Edwards curve defined over $\mathbb{F}_q$ is the curve

$$C : ax^2 + y^2 = 1 + dx^2y^2, \; a, d \in \mathbb{F}_q, \text{ and } ad(a-d) \neq 0$$

with two singular points. It is birationally equivalent to $E : v^2 = u^3 + 2(a+d)u^2 + (a-d)^2u$ such that every point has order divisible by 4.



NIST IR 8214B, Notes on Threshold EdDSA/Schnorr Signatures