Cryptographic primitives from elliptic curve isogenies

An overview and some preliminary results

Federico Pintore
University of Oxford - UK

Trento, 11th February 2019

A security model in modern Cryptography

Proofs of security of cryptographic primitives are among the features distinguishing modern cryptography from classical cryptography.

A security model in modern Cryptography

Proofs of security of cryptographic primitives are among the features

distinguishing modern cryptography from classical cryptography.

Provable security

A security model which requires a formal proof that

breaking the scheme is as difficult as solving

a well-known and supposedly difficult mathematical problem

A security model in modern Cryptography

Proofs of security of cryptographic primitives are among the features distinguishing modern cryptography from classical cryptography.

Provable security

A security model which requires a formal proof that

breaking the scheme is as difficult as solving

a well-known and supposedly difficult mathematical problem

Breaking the scheme $\Rightarrow$ solving the difficult mathematical problem

The threat of quantum computers

Hard mathematical problems:

- **integer factorisation: RSA, …**
- **discrete logarithm problems over finite fields: DSA, …**
- **discrete logarithm problems over elliptic curves:**

  Elliptic Curve Cryptography (since 1985)

The threat of quantum computers

For classical computers

Hard mathematical problems:

- **integer factorisation: RSA, …**
- **discrete logarithm problems over finite fields: DSA, …**
- **discrete logarithm problems over elliptic curves:**

  Elliptic Curve Cryptography (since 1985)

The threat of quantum computers

For classical computers

Hard mathematical problems:

- **integer factorisation: RSA, …**
- **discrete logarithm problems over finite fields: DSA, …**
- **discrete logarithm problems over elliptic curves:**
  Elliptic Curve Cryptography (since 1985)

Shor (1994): ***those problems are easy for quantum computers!***

A new class of hard mathematical problems

Problems supposed hard also for quantum computers:

- Bounded decoding problem → Code-based Cryptography
- Second pre-image problem for hash functions → Hash-based Cryptography
- Solving systems of multivariate polynomial equations (over finite fields) → Multivariate Cryptography
- Computational lattice problems → Lattice-based Cryptography
- Isogeny problems → Isogeny-based Cryptograpy

Post-quantum Cryptography

The above cryptography's branches compose Post-quantum Cryptography,

which studies algorithms that:

- can be implemented in classical computers;
- are thought to be secure even against quantum computers.

Post-quantum Cryptography

The above cryptography's branches compose Post-quantum Cryptography,

which studies algorithms that:

- can be implemented in classical computers;
- are thought to be secure even against quantum computers.

To PROTECT OUR CURRENT DATA, it is fundamental to IMPLEMENT POST-QUANTUM CRYPTOSYSTEMS before the (possible) advent of QUANTUM COMPUTERS.

Post-quantum Cryptography

The above cryptography's branches compose Post-quantum Cryptography,

which studies algorithms that:

- can be implemented in classical computers;
- are thought to be secure even against quantum computers.

To PROTECT OUR CURRENT DATA, it is fundamental to IMPLEMENT POST-QUANTUM CRYPTOSYSTEMS before the (possible) advent of QUANTUM COMPUTERS.

NIST (National Institute of Standards and Technology) has initiated a process to

solicit, evaluate, and standardise one or more quantum-resistant public-key cryptographic algorithms

in December 2016 (first round's results published at the end of Jan 2019).

Isogeny-based Cryptography

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

$$E_1 \text{ and } E_2 \text{ over } \mathbb{F}_{p^2}\text{, compute an isogeny}$$

$$\varphi : E_1 \to E_2$$

of a given degree *d*.

SIKE: isogeny-based key-exchange protocol submitted to NIST process

Outline of the talk

1. Isogenies and their properties

2. The isogeny assumptions

3. Cryptographic protocols

4. What it is missing and open problems

5. A new path for Isogeny-based Cryptography

What is an isogeny?

Let E_1, E_2 be two elliptic curves defined over a finite field $\mathbb{F}_{p^n}$:

$$E_i : y^2 = x^3 + A_i x + B_i \qquad A_i, B_i \in \mathbb{F}_{p^n} \qquad i = 1, 2$$

The sets

$$E_i(\overline{\mathbb{F}_{p^n}}) = \{P = (x, y) \in \overline{\mathbb{F}_{p^n}} \times \overline{\mathbb{F}_{p^n}} \mid y^2 = x^3 + A_i x + B_i\} \cup \{\infty\}$$

are abelian groups with respect to an addition having ∞ as identity.

$E_i(\mathbb{F}_{p^n})$ is the subgroup of rational points.

What is an isogeny?

Let E_1, E_2 be two elliptic curves defined over a finite field $\mathbb{F}_{p^n}$:

$$E_i : y^2 = x^3 + A_i x + B_i \qquad A_i, B_i \in \mathbb{F}_{p^n} \qquad i = 1, 2$$

The sets

$$E_i(\overline{\mathbb{F}_{p^n}}) = \{P = (x, y) \in \overline{\mathbb{F}_{p^n}} \times \overline{\mathbb{F}_{p^n}} \mid y^2 = x^3 + A_i x + B_i\} \cup \{\infty\}$$

are abelian groups with respect to an addition having ∞ as identity.

$E_i(\mathbb{F}_{p^n})$ is the subgroup of rational points.

An isogeny from E_1 to E_2 is a non-constant morphism

$$\varphi : E_1 \to E_2$$

$$(x, y) \mapsto \left(\frac{f_1(x, y)}{g_1(x, y)}, \frac{f_2(x, y)}{g_2(x, y)} \right) \qquad f_1, f_2, g_1, g_2 \in \mathbb{F}_{p^{kn}}[x, y]$$

sending ∞ in ∞. We will say that φ is defined over the extension $\mathbb{F}_{p^{kn}}$.

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$

- φ has a finite kernel. We define $deg(\varphi)$ as $\#Ker(\varphi)$ (separable isogeny)

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$
- φ has a finite kernel. We define $deg(\varphi)$ as $\#Ker(\varphi)$ (separable isogeny)
- the composition of two isogenies of degrees d_1, d_2 is an isogeny of degree $d_1 d_2$

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$
- φ has a finite kernel. We define $deg(\varphi)$ as $\#Ker(\varphi)$ (separable isogeny)
- the composition of two isogenies of degrees d_1, d_2 is an isogeny of degree $d_1 d_2$
- a composite-degree isogeny can be factorised into the composition of prime-degrees isogenies

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$
- φ has a finite kernel. We define $deg(\varphi)$ as $\#Ker(\varphi)$ (separable isogeny)
- the composition of two isogenies of degrees d_1, d_2 is an isogeny of degree $d_1 d_2$
- a composite-degree isogeny can be factorised into the composition of prime-degrees isogenies
- Tate's theorem: E_1, E_2 are isogenous over $\mathbb{F}_{p^n}$ iff $\#E_1(\mathbb{F}_{p^n}) = \#E_2(\mathbb{F}_{p^n})$

Some properties (1)

- φ is a group homomorphism between $E_1(\overline{\mathbb{F}_{p^n}})$ and $E_2(\overline{\mathbb{F}_{p^n}})$
- φ has a finite kernel. We define $deg(\varphi)$ as $\#Ker(\varphi)$ (separable isogeny)
- the composition of two isogenies of degrees d_1, d_2 is an isogeny of degree $d_1 d_2$
- a composite-degree isogeny can be factorised into the composition of prime-degrees isogenies
- Tate's theorem: E_1, E_2 are isogenous over $\mathbb{F}_{p^n}$ iff $\#E_1(\mathbb{F}_{p^n}) = \#E_2(\mathbb{F}_{p^n})$
- φ admits a dual isogeny $\hat{\varphi} : E_2 \to E_1$ having the same degree d and such that

$$\hat{\varphi} \circ \varphi = \varphi \circ \hat{\varphi} = [d]$$

Endomorphisms and supersingular elliptic curves

An endomorphism of E is an isogeny $\psi : E \to E$.

Endomorphisms and supersingular elliptic curves

An endomorphism of E is an isogeny $\psi : E \to E$.

The set $End(E)$ of all endomorphisms of E is a ring

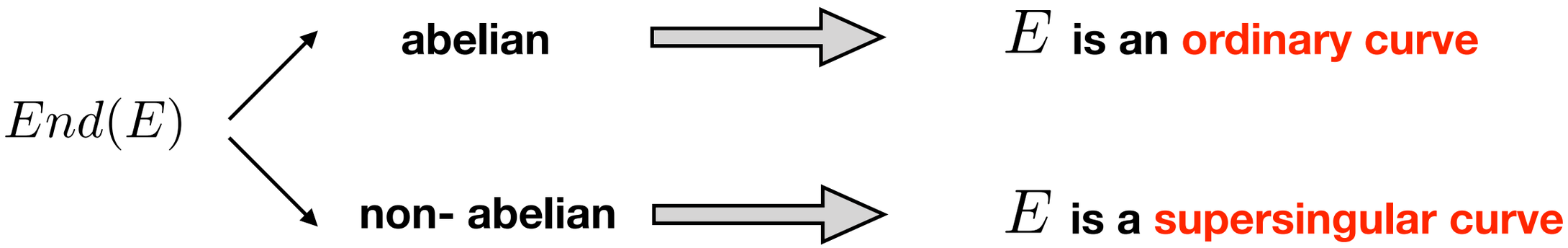
with respect to pointwise addition and composition.

Endomorphisms and supersingular elliptic curves

An endomorphism of E is an isogeny $\psi : E \to E$.

The set $End(E)$ of all endomorphisms of E is a ring

with respect to pointwise addition and composition.



Isomorphisms

An isomorphism is an isogeny of degree 1.

Isomorphisms

An isomorphism is an isogeny of degree 1.

↓

if φ is defined over the base Field $\mathbb{F}_{p^m}$, then $\varphi: E_1(\mathbb{F}_{p^m}) \longrightarrow E_2(\mathbb{F}_{p^m})$ is a group isomorphism.

Isomorphisms

An isomorphism is an isogeny of degree 1.

↓

if φ is defined over the base Field $\mathbb{F}_{p^m}$, then $\varphi: E_1(\mathbb{F}_{p^m}) \longrightarrow E_2(\mathbb{F}_{p^m})$ is a group isomorphism.

Given an elliptic curve $E : y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_{p^n}$, we define its j-invariant as:

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

Isomorphisms

An isomorphism is an isogeny of degree 1.

↓

if φ is defined over the base Field $\mathbb{F}_{p^m}$, then $\varphi: E_1(\mathbb{F}_{p^m}) \longrightarrow E_2(\mathbb{F}_{p^m})$ is a group isomorphism.

Given an elliptic curve $E : y^2 = x^3 + Ax + B$ defined over $\mathbb{F}_{p^n}$, we define its j-invariant as:

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

Theorem: two elliptic curves defined over $\mathbb{F}_{p^n}$ are isomorphic (on some extension field) iff they have the same *j*-invariant.

Some properties (2)

- for each supersingular curve E defined over an extension of $\mathbb{F}_p$ it holds $j(E) \in \mathbb{F}_{p^2}$

Some properties (2)

- for each supersingular curve E defined over an extension of $\mathbb{F}_p$ it holds $j(E) \in \mathbb{F}_{p^2}$

Working in $\mathbb{F}_{p^2}$ is sufficient to consider all possible supersingular elliptic curves (modulo isomorphisms).

Some properties (2)

- for each supersingular curve E defined over an extension of $\mathbb{F}_p$ it holds $j(E) \in \mathbb{F}_{p^2}$

Working in $\mathbb{F}_{p^2}$ is sufficient to consider all possible supersingular elliptic curves (modulo isomorphisms).

- Theorem: given a subgroup $G \subset E(\mathbb{F}_{p^2})$ there exist, and are unique modulo isomorphisms, a supersingular elliptic curve E/G and an isogeny $\varphi : E \to E/G$, both defined over $\mathbb{F}_{p^2}$, s.t. $Ker(\varphi) = G$.

Some properties (2)

- for each supersingular curve E defined over an extension of $\mathbb{F}_p$ it holds $j(E) \in \mathbb{F}_{p^2}$

Working in $\mathbb{F}_{p^2}$ is sufficient to consider all possible supersingular elliptic curves (modulo isomorphisms).

- Theorem: given a subgroup $G \subset E(\mathbb{F}_{p^2})$ there exist, and are unique modulo isomorphisms, a supersingular elliptic curve E/G and an isogeny $\varphi : E \to E/G$, both defined over $\mathbb{F}_{p^2}$, s.t. $Ker(\varphi) = G$.

- Velu's formulas allow to compute both E/G and φ with a complexity linear in $\#G$.

The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

or a subgroup $G \subseteq E_1(\mathbb{F}_{p^2})$ such that $E_1/G \simeq E_2$

The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

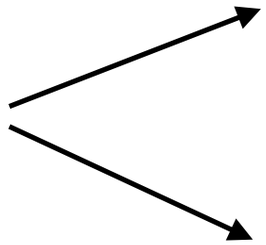
E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

or a subgroup $G \subseteq E_1(\mathbb{F}_{p^2})$ such that $E_1/G \simeq E_2$

Complexities of best know solving algorithms



The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

or a subgroup $G \subseteq E_1(\mathbb{F}_{p^2})$ such that $E_1/G \simeq E_2$

Complexities of best know solving algorithms

Classical $O(\sqrt[4]{p})$

The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

or a subgroup $G \subseteq E_1(\mathbb{F}_{p^2})$ such that $E_1/G \simeq E_2$

Complexities of best know solving algorithms

- **Classical** $O(\sqrt[4]{p})$
- **Quantum** $O(\sqrt[6]{p})$

The isogeny assumptions

Isogeny problem: given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of a given degree $d \simeq \sqrt{p}$ **.**

or a subgroup $G \subseteq E_1(\mathbb{F}_{p^2})$ such that $E_1/G \simeq E_2$

Complexities of best know solving algorithms

- **Classical** $O(\sqrt[4]{p})$
- **Quantum** $O(\sqrt[6]{p})$

<u>Non standard assumptions</u>: variations of the above problem, that are assumed as hard as the original problem.

First cryptographic protocols

- **CLG Hash function** (Charles, Lauter, Goren - 2009)
- **SIDH Key Exchange** (Jao, De Feo - 2011)
- **Encryption Scheme** (Jao, De Feo, Plût - 2014)
- **Zero-knowledge Proof** (Jao, De Feo, Plût - 2014)

The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime p and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

$m = (0, 1, 1, 0, ..., 0)$

Given an integer ℓ, the set

$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

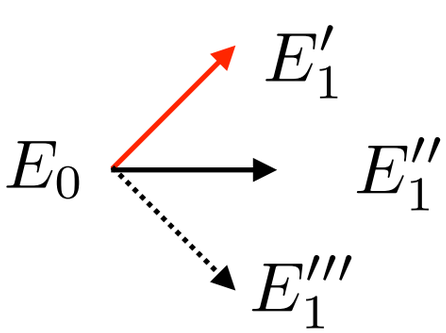
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

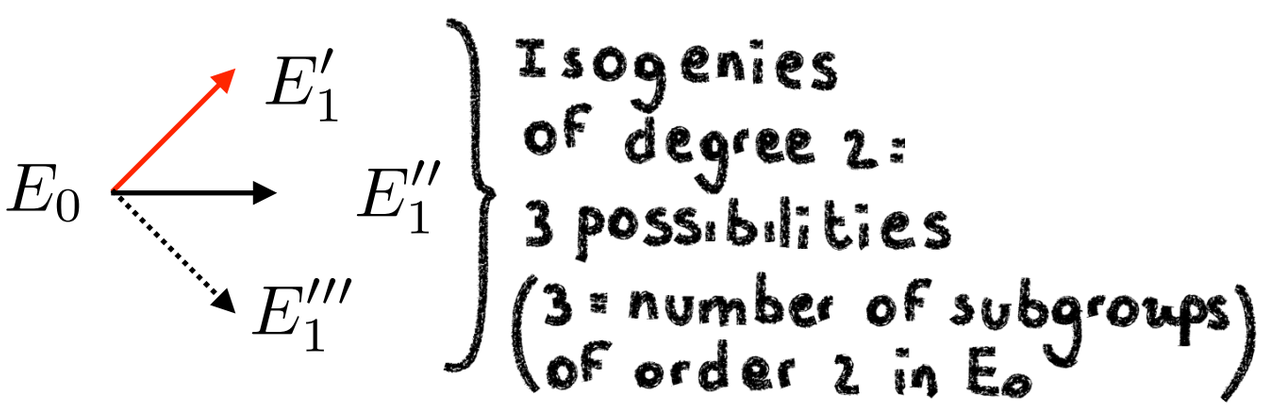
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

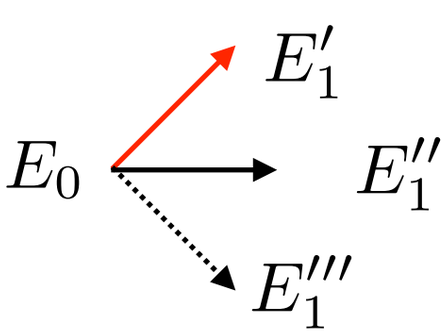
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

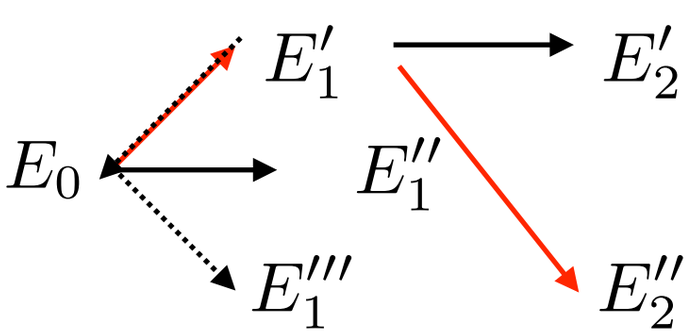
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

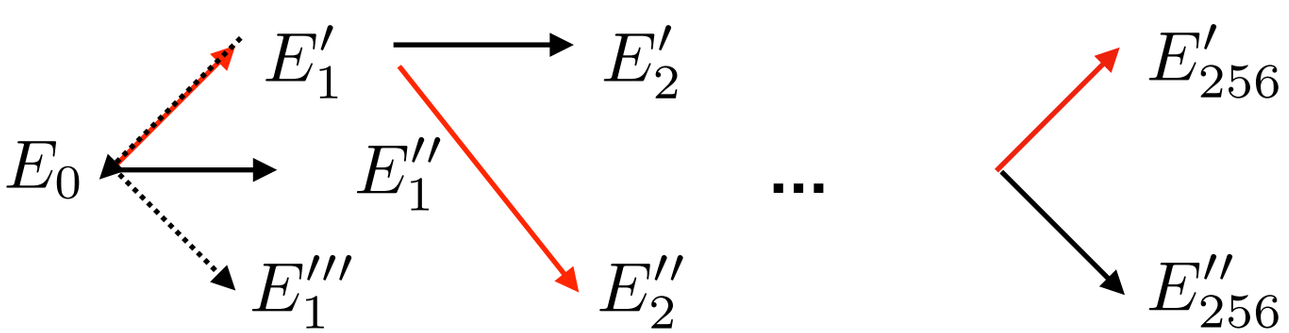
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



The CLG Hash function

It is a provable pre-image resistant hash function:

finding pre-images implies the resolution of the isogeny problem.

Parameters:

- a large prime *p* and a supersingular curve E_0 over $\mathbb{F}_{p^2}$
- a small prime ℓ, e.g. $\ell = 2$
- a *big* message space, e.g. $(\mathbb{F}_2)^{256}$

Given an integer ℓ, the set

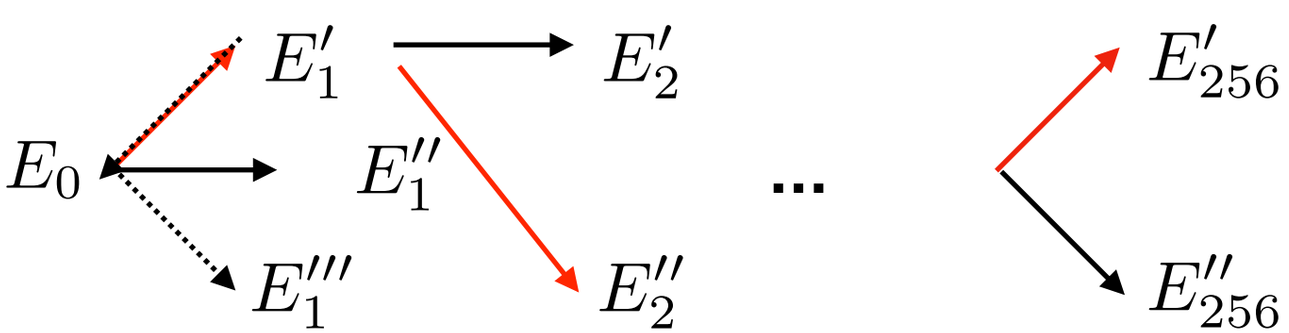
$$E_0[\ell] = \{P \in E_0(\overline{\mathbb{F}_{p^2}}) \mid \ell P = \infty\}$$

is isomorphic to

$$\mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

if $gcd(p, \ell) = 1$.

$$m = (0, 1, 1, 0, ..., 0)$$



$$H(m) = j(E'_{256})$$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$

It always exists!

- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$ $\quad p>3$, so $E_0[2^{e_2}] \simeq \mathbb{Z}_{2^{e_2}} \times \mathbb{Z}_{2^{e_2}}$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$ $E_0[2^{e_2}], E_0[3^{e_3}] \subseteq E_0(\mathbb{F}_{p^2})$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

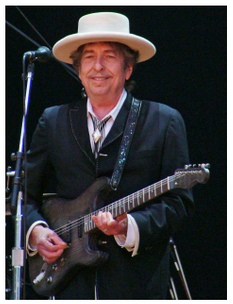
Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

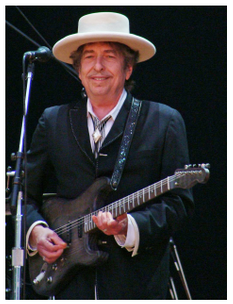
- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$



SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- two positive integers, e_2 and e_3, s.t. $2^{e_2} \simeq 3^{e_3}$
- a prime $p = 2^{e_2} 3^{e_3} f \pm 1$ and the finite field $\mathbb{F}_{p^2}$
- a supersingular elliptic curve E_0 over $\mathbb{F}_{p^2}$, s.t. $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 s.t. $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 s.t. $E_0[3^{e_3}] =< P_3, Q_3 >$

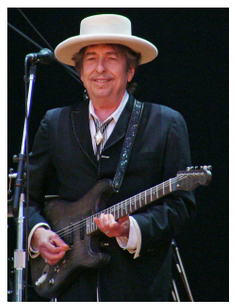


- Selects a secret $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- $G_B =< P_2 + sk_B Q_2 > \subset E_0[2^{e_2}]$ ($ord(G_B) = 2^{e_2}$)
- Computes $\phi_B : E_0 \to E_B = E_0/G_B$ and $\phi_B(P_3), \phi_B(Q_3)$

SIDH - Supersingular Isogeny Diffie-Hellman

Public Parameters

- **two positive integers, e_2 and e_3, s.t.** $2^{e_2} \simeq 3^{e_3}$
- **a prime** $p = 2^{e_2} 3^{e_3} f \pm 1$ **and the finite field** $\mathbb{F}_{p^2}$
- **a supersingular elliptic curve E_0 over** $\mathbb{F}_{p^2}$ **, s.t.** $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2} 3^{e_3} f)^2$
- P_2, Q_2 **s.t.** $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 **s.t.** $E_0[3^{e_3}] =< P_3, Q_3 >$



Selects a secret $sk_A \in [1, \ldots, 3^{e_3} - 1]$

$$G_A =< P_3 + sk_A Q_3 > \subset E_0[3^{e_3}] \quad (ord(G_A) = 3^{e_3})$$

Computes $\phi_A : E_0 \to E_A = E_0/G_A$ **and** $\phi_A(P_2), \phi_A(Q_2)$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

Computes $\phi_{AB} : E_A \to E_{AB}$ with

kernel $< \phi_A(P_2) + sk_B\phi_A(Q_2) >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

Computes $\phi_{AB} : E_A \to E_{AB}$ **with kernel** $< \phi_A(P_2) + sk_B\phi_A(Q_2) >$

Computes $\phi_{BA} : E_B \to E_{BA}$ **with kernel** $< \phi_B(P_3) + sk_A\phi_B(Q_3) >$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

Computes $\phi_{AB} : E_A \to E_{AB}$ **with kernel** $< \phi_A(P_2) + sk_B\phi_A(Q_2) >$

Computes $\phi_{BA} : E_B \to E_{BA}$ **with kernel** $< \phi_B(P_3) + sk_A\phi_B(Q_3) >$

Since $\langle \phi_A(P_2) + sk_B \phi_A(Q_2) \rangle = \phi_A(G_B)$
we have $\ker(\phi_{AB} \circ \phi_A) = \langle G_A, G_B \rangle$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

Computes $\phi_{AB} : E_A \to E_{AB}$ **with kernel** $< \phi_A(P_2) + sk_B\phi_A(Q_2) >$

Computes $\phi_{BA} : E_B \to E_{BA}$ **with kernel** $< \phi_B(P_3) + sk_A\phi_B(Q_3) >$

Since $\langle \phi_A(P_2) + sk_B \phi_A(Q_2) \rangle = \phi_A(G_B)$
we have $\ker(\phi_{AB} \circ \phi_A) = \langle G_A, G_B \rangle$

Since $\langle \phi_B(P_3) + sk_A \phi_B(Q_3) \rangle = \phi_B(G_A)$
we have $\ker(\phi_{BA} \circ \phi_B) = \langle G_A, G_B \rangle$

SIDH - Supersingular Isogeny Diffie-Hellman

Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public key: $E_B, \phi_B(P_3), \phi_B(Q_3)$

Private key: sk_B, ϕ_B

Public key: $E_A, \phi_A(P_2), \phi_A(Q_2)$

Private key: sk_A, ϕ_A

Sends $E_B, \phi_B(P_3), \phi_B(Q_3)$

Sends $E_A, \phi_A(P_2), \phi_A(Q_2)$

Computes $\phi_{AB} : E_A \to E_{AB}$ **with kernel** $< \phi_A(P_2) + sk_B\phi_A(Q_2) >$

Computes $\phi_{BA} : E_B \to E_{BA}$ **with kernel** $< \phi_B(P_3) + sk_A\phi_B(Q_3) >$

The two curves obtained by Alice and Bob are isomorphic

THEY HAVE THE SAME *j*-INVARIANT!

SIDH - Supersingular Isogeny Diffie-Hellman

SIDH's security relies on a non standard isogeny problem:

Given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of given degree $d = 2^{e_2} \simeq \sqrt{p}$

knowing how φ **acts on a basis** $\{P_3, Q_3\}$ **of** $E_0[3^{e_3}]$**.**

SIDH - Supersingular Isogeny Diffie-Hellman

SIDH's security relies on a non standard isogeny problem:

Given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of given degree $d = 2^{e_2} \simeq \sqrt{p}$

knowing how φ **acts on a basis** $\{P_3, Q_3\}$ **of** $E_0[3^{e_3}]$**.**

It is assumed that the above problem is as hard as the original isogeny problem.

SIDH - Supersingular Isogeny Diffie-Hellman

SIDH's security relies on a non standard isogeny problem:

Given a prime *p* and two supersingular isogenous curves,

E_1 **and** E_2 **over** $\mathbb{F}_{p^2}$**, compute an isogeny**

$$\varphi : E_1 \to E_2$$

of given degree $d = 2^{e_2} \simeq \sqrt{p}$

knowing how φ **acts on a basis** $\{P_3, Q_3\}$ **of** $E_0[3^{e_3}]$**.**

It is assumed that the above problem is as hard as the original isogeny problem.

No counterexamples so far, except for active attacks

The NIST submission: SIKE

3.17 SIKE

SIKE was the only candidate based on arithmetic properties of elliptic curves over finite fields. While quantum computers will break currently deployed elliptic curve cryptosystems, SIKE uses pseudo-random walks on supersingular isogeny graphs of curves, which are not known to be susceptible to quantum attacks. The nature of SIKE allows for a key exchange algorithm which is very similar to the classic Diffie-Hellman. The submission includes a CPA-secure encryption scheme which is converted to a CCA-secure KEM via a standard transformation.

SIKE has the smallest key sizes among all the remaining submissions, with public keys less than 750 bytes even for its level 5 security parameters. Another advantage of SIKE is that it can leverage existing optimized code for elliptic curve operations and can thus be easily combined with traditional elliptic curve cryptography to create a hybrid classical/post-quantum scheme. The SIKE scheme also benefits from much research into protecting elliptic curve operations from side-channel attacks.

The basic security problem upon which SIKE relies, finding isogenies between supersingular elliptic curves, has not been studied as much as some of the security problems associated with other submissions. Another drawback is that the performance of SIKE seems to be an order of magnitude slower than many of the other candidates.

The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

Prover **Verifier**

The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

Prover **Verifier**

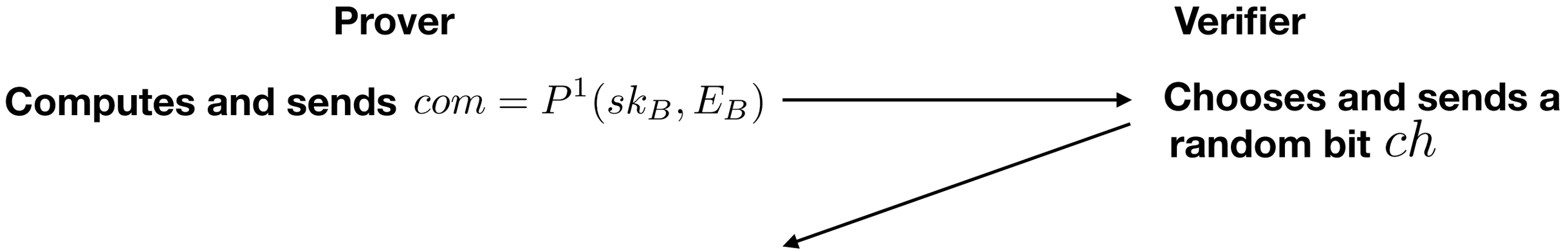
Computes and sends $com = P^1(sk_B, E_B)$ $\longrightarrow$

The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

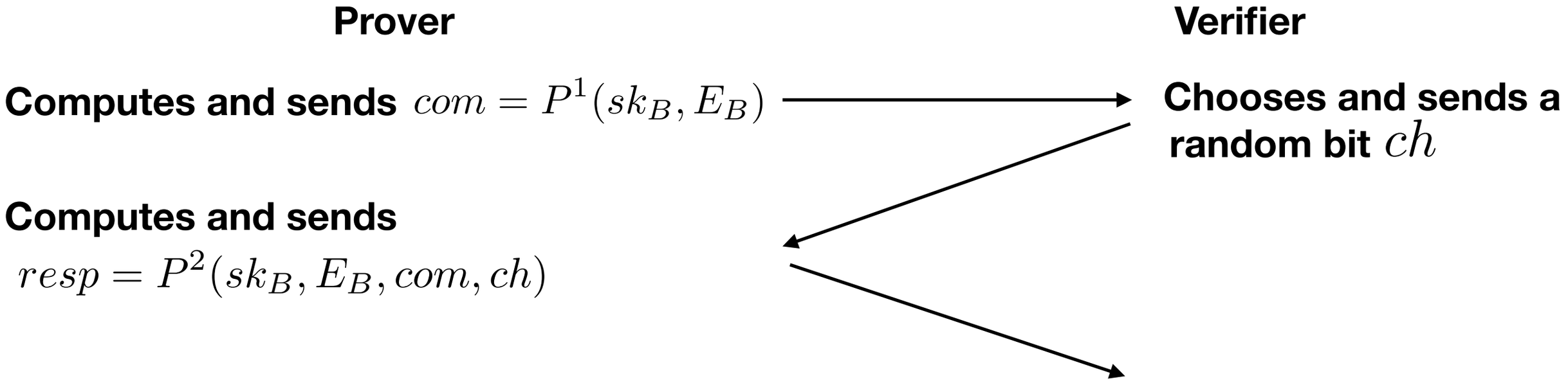


The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

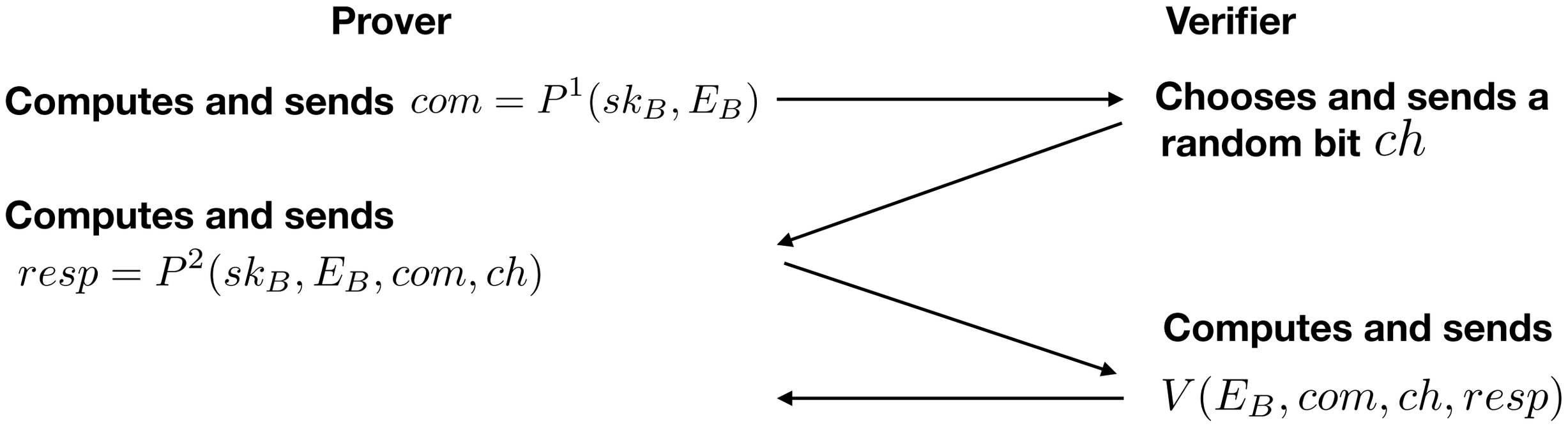


The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key

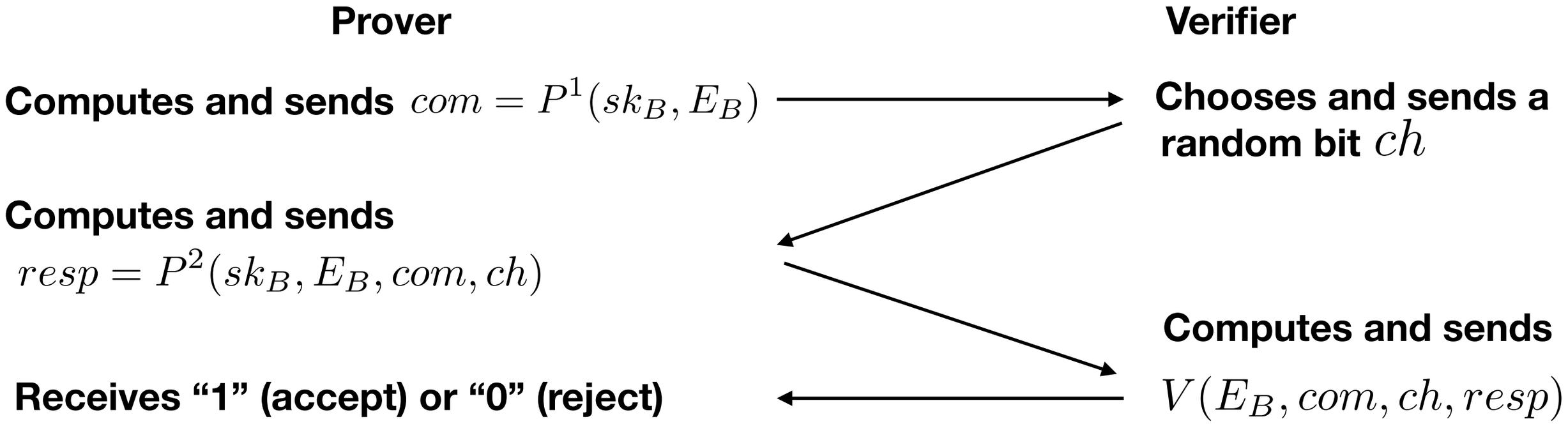


The zero-knowledge proof

It is a $\sum$ - protocol $((P^1, P^2), V)$ which:

- allows to prove knowledge of the secret key sk_B, ϕ_B
  corresponding to a public key $E_B, \phi_B(P_3), \phi_B(Q_3)$

- without revealing anything about the secret key



Zero-knowledge proof properties

1. **Completness: if the prover is the legitimate owner, the verifier accepts their proof.**

Zero-knowledge proof properties

1. **Completness**: if the prover is the legitimate owner, the verifier accepts their proof.

2. **Special-Soundness**: if the prover convinces twice the verifier - on the same commitment but different challenges - then the prover must be the legitimate owner.

Zero-knowledge proof properties

1. Completness: if the prover is the legitimate owner, the verifier accepts their proof.

2. Special-Soundness: if the prover convinces twice the verifier - on the same commitment but different challenges - then the prover must be the legitimate owner.

3. Honest-verifier Zero-Knowledge: the verifier cannot distinguish between a valid interaction and a simulated interaction.

From ZK proofs to Digital Signatures

A $\sum$-protocol can be turned into a non-interactive protocol.

Classically, this is done through the well-known Fiat-Shamir construction which exploits an hash function $H : \{0,1\}^* \to S_{ch}$ to compute the challenge as

$$ch = H(pk_B, com)$$

From ZK proofs to Digital Signatures

A $\sum$-protocol can be turned into a non-interactive protocol.

Classically, this is done through the well-known Fiat-Shamir construction which exploits an hash function $H : \{0,1\}^* \to S_{ch}$ to compute the challenge as

$$ch = H(pk_B, com)$$

A non-interactive zero-knowledge proof leads to

a digital signature scheme adding a message *m* to the public key.

From ZK proofs to Digital Signatures

A $\sum$-protocol can be turned into a non-interactive protocol.

Classically, this is done through the well-known Fiat-Shamir construction which exploits an hash function $H : \{0,1\}^* \to S_{ch}$ to compute the challenge as

$$ch = H(pk_B, com)$$

A non-interactive zero-knowledge proof leads to
a digital signature scheme adding a message *m* to the public key.

The Fiat-Shamir construction could be not safe in a quantum setting,
where it has been replaced by the Unruh's transform.

What is missing

- **Group key-exchange**
- **Efficient digital signature algorithm**
- **Aggregate multi-signature**
- **Attribute-based encryption**
- **Privacy-preserving digital signatures**

…advanced cryptographic schemes…

Open problems

- **Efficiency**

- **Security of non-standard problems**

- **Development of advanced primitives**

New directions in Isogeny-based Cryptography

A new key-exchange protocol

based on supersingular isogenies

has been proposed recently: CSIDH.

New directions in Isogeny-based Cryptography

A new key-exchange protocol

based on supersingular isogenies

has been proposed recently: CSIDH.

Let p be a prime of the form $4\ell_1\ell_2\cdots\ell_r - 1$ (ℓ_i distinct odd primes).

New directions in Isogeny-based Cryptography

A new key-exchange protocol

based on supersingular isogenies

has been proposed recently: CSIDH.

Let p be a prime of the form $4\ell_1\ell_2\cdots\ell_r - 1$ (ℓ_i distinct odd primes).

For each supersingular elliptic curve E defined over $\mathbb{F}_p$, we have

$$End_p(E) = \{\psi : E \to E \mid \psi \ \ endomorphism \ \ over \ \ \mathbb{F}_p\} \simeq \mathcal{O}$$

where $\mathcal{O}$ is an order in the imaginary quadratic field $\mathbb{Q}[\sqrt{-p}]$.

New directions in Isogeny-based Cryptography

A new key-exchange protocol

based on supersingular isogenies

has been proposed recently: CSIDH.

Let p be a prime of the form $4\ell_1\ell_2\cdots\ell_r - 1$ (ℓ_i distinct odd primes).

For each supersingular elliptic curve E defined over $\mathbb{F}_p$, we have

$$End_p(E) = \{\psi : E \to E \mid \psi \ \ endomorphism \ \ over \ \ \mathbb{F}_p\} \simeq \mathcal{O}$$

where $\mathcal{O}$ is an order in the imaginary quadratic field $\mathbb{Q}[\sqrt{-p}]$.

$Ell_p(\mathbb{Z}[\sqrt{-p}])$ is the set of all supersingular curves E over $\mathbb{F}_p$ s.t.

$$End_p(E) \simeq \mathbb{Z}[\sqrt{-p}]$$

New directions in Isogeny-based Cryptography

The ideal class group $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ acts transitively on $Ell_p(\mathbb{Z}[\sqrt{-p}])$:

$$* : \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}]) \times Ell_p(\mathbb{Z}[\sqrt{-p}]) \to Ell_p(\mathbb{Z}[\sqrt{-p}])$$

$$([I], E) \qquad \mapsto \qquad I * E$$

Given $G_I = \{P \in E | \alpha(P) = \infty \ \ \forall \alpha \in I\}$, the action is defined as $I * E = E/G_I$.

New directions in Isogeny-based Cryptography

The ideal class group $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ acts transitively on $Ell_p(\mathbb{Z}[\sqrt{-p}])$:

$$* : \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}]) \times Ell_p(\mathbb{Z}[\sqrt{-p}]) \to Ell_p(\mathbb{Z}[\sqrt{-p}])$$

$$([I], E) \qquad \mapsto \qquad I * E$$

Given $G_I = \{P \in E | \alpha(P) = \infty \ \ \forall \alpha \in I\}$, the action is defined as $I * E = E/G_I$.

For some ideals, this action can be computed efficiently.

New directions in Isogeny-based Cryptography

The ideal class group $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ acts transitively on $Ell_p(\mathbb{Z}[\sqrt{-p}])$:

$$* : \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}]) \times Ell_p(\mathbb{Z}[\sqrt{-p}]) \to Ell_p(\mathbb{Z}[\sqrt{-p}])$$

$$([I], E) \qquad \mapsto \qquad I * E$$

Given $G_I = \{P \in E | \alpha(P) = \infty \ \ \forall \alpha \in I\}$, the action is defined as $I * E = E/G_I$.

For some ideals, this action can be computed efficiently.

Indeed, when $I_i =< \ell_i, 1 - \sqrt{-p} >$ the subgroup G_{I_i} is $E[\ell_i] \cap E(\mathbb{F}_p)$.

New directions in Isogeny-based Cryptography

The ideal class group $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$ acts transitively on $Ell_p(\mathbb{Z}[\sqrt{-p}])$:

$$* : \mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}]) \times Ell_p(\mathbb{Z}[\sqrt{-p}]) \to Ell_p(\mathbb{Z}[\sqrt{-p}])$$

$$([I], E) \qquad \mapsto \qquad I * E$$

Given $G_I = \{P \in E | \alpha(P) = \infty \ \ \forall \alpha \in I\}$, the action is defined as $I * E = E/G_I$.

For some ideals, this action can be computed efficiently.

Indeed, when $I_i =< \ell_i, 1 - \sqrt{-p} >$ the subgroup G_{I_i} is $E[\ell_i] \cap E(\mathbb{F}_p)$.

Most of the ideals I should be factorised as

$$I_1^{e_1} I_2^{e_2} \cdots I_r^{e_r}$$

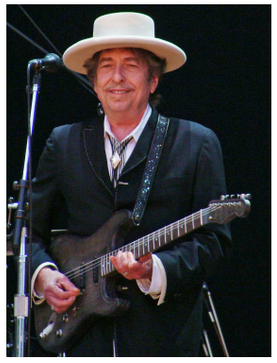
for suitable integers e_i.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.

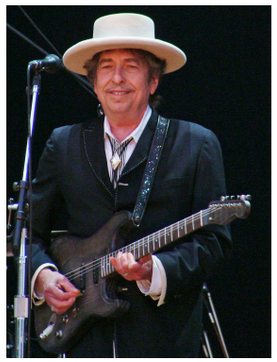
New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



New directions in Isogeny-based Cryptography

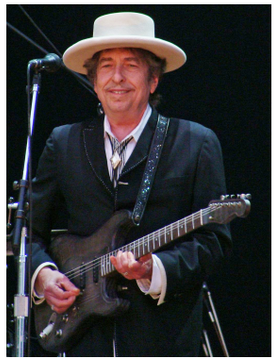
The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.

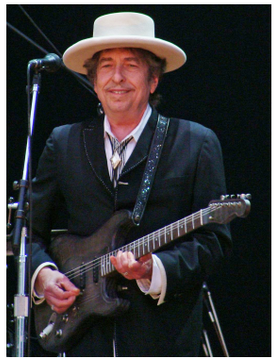


Chooses a random ideal I_B .

Chooses a random ideal I_A.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



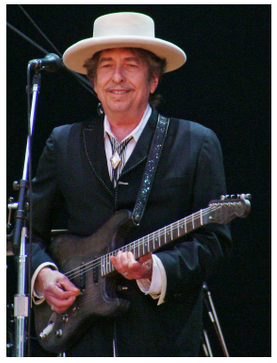
Chooses a random ideal I_B .

Chooses a random ideal I_A.

Computes and sends $I_B * E_0$. ⟶

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

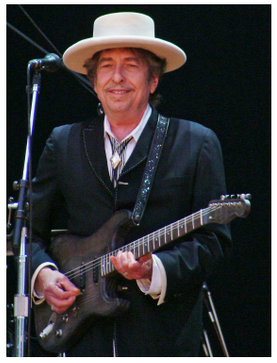
Computes and sends $I_B * E_0$.

Computes and sends $I_A * E_0$.

Chooses a random ideal I_A.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

Chooses a random ideal I_A.

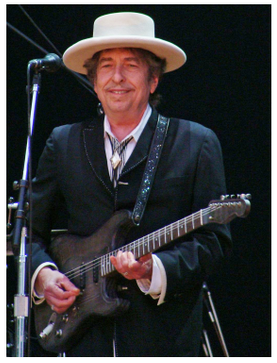
Computes and sends $I_B * E_0$.

Computes and sends $I_A * E_0$.

Computes $I_B * (I_A * E_0)$.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

Computes and sends $I_B * E_0$.

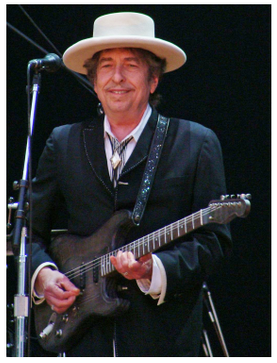
Computes and sends $I_A * E_0$.

Computes $I_B * (I_A * E_0)$.

Computes $I_A * (I_B * E_0)$.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

Computes and sends $I_B * E_0$.

Computes and sends $I_A * E_0$.

Computes $I_B * (I_A * E_0)$.

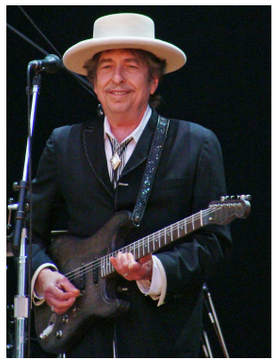
Chooses a random ideal I_A.

Computes $I_A * (I_B * E_0)$.

Security: the best know attack has subexponential complexity.

New directions in Isogeny-based Cryptography

The class-group action induces a key-exchange *a la* Diffie-Hellman.



Chooses a random ideal I_B .

Computes and sends $I_B * E_0$.

Computes $I_B * (I_A * E_0)$.

Chooses a random ideal I_A.

Computes and sends $I_A * E_0$.

Computes $I_A * (I_B * E_0)$.

Security: the best know attack has subexponential complexity.

Efficiency: slower than SIDH, the bottleneck is the isogenies computation.

Thanks for your attention

Questions?

Federico Pintore
federico.pintore@maths.ox.ac.uk

Trento, 11th February 2019