Post-Quantum Cryptosystems based on Elliptic Curve Isogenies

Federico Pintore

Department of Mathematics,
University of Trento

ITASEC18 - Milan, 8th February 2018

NIST - Call for Proposals

SIKE: Supersingular Isogeny Key Encapsulation

Azarderakhsh, Campagna, Costello, De Feo, Hess, Jalali, Koziel, LaMacchia, Longa, Naehirng, Renes, Spoukharev, Urbani

Finite Fields

Let p be a prime integer.

With $\mathbb{F}_p$ we denote the finite field with p elements:

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

Finite Fields

Let p be a prime integer.

With $\mathbb{F}_p$ we denote the finite field with p elements:

$$\mathbb{F}_p = \{0, 1, \ldots, p-1\}$$

If $p = 4k - 1$, then the equation $x^2 + 1 = 0$ has not solutions in $\mathbb{F}_p$ and

$$\mathbb{F}_{p^2} = \{s_0 + s_1 \cdot i \mid s_0, s_1 \in \mathbb{F}_p\}$$

is a quadratic extension of $\mathbb{F}_p$, with $i^2 = 1$.

Elliptic curves

A Montgomery curve (a special form of an elliptic curve) *E*, defined over $\mathbb{F}_{p^2}$, is described by an equation:

$$By^2 = x^3 + Ax^2 + x \qquad \text{with} \;\; A, B \in \mathbb{F}_{p^2}$$

Elliptic curves

A Montgomery curve (a special form of an elliptic curve) *E*, defined over $\mathbb{F}_{p^2}$, is described by an equation:

$$By^2 = x^3 + Ax^2 + x \qquad \text{with } \; A, B \in \mathbb{F}_{p^2}$$

Given an extension field $\mathbb{K}$ of $\mathbb{F}_{p^2}$, the set

$$E(\mathbb{K}) = \{(x_0, y_0) \in \mathbb{K} \times \mathbb{K} \mid By_0^2 = x_0^3 + Ax_0^2 + x_0\} \cup \{\infty\}$$

is an additive group. In particular, $E(\mathbb{F}_{p^2})$ is a finite group.

Elliptic Curves

The elliptic curve E is supersingular if:

$$p \mid (p^2 + 1 - \#E(\mathbb{F}_{p^2}))$$

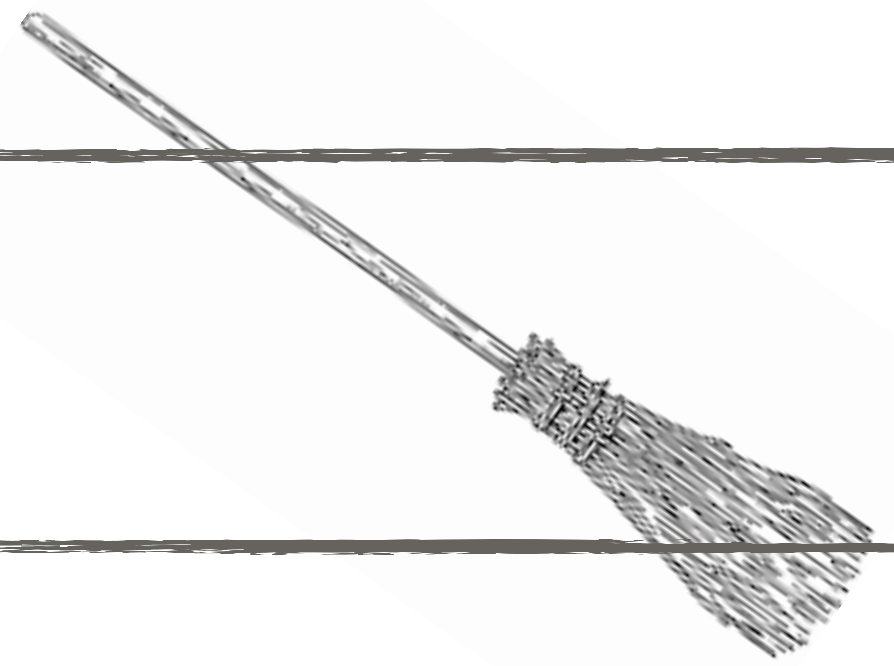
Elliptic Curves

The elliptic curve E is supersingular if:

$$p \mid (p^2 + 1 - \#E(\mathbb{F}_{p^2}))$$

The j - invariant of E is:

$$j(E) = \frac{256(A^2-3)^3}{A^2-4}$$



Two elliptic curves are isomorphic <u>if and only if</u> they have the same j - invariant

Elliptic Curves

The elliptic curve *E* is supersingular if:

$$p \mid (p^2 + 1 - \#E(\mathbb{F}_{p^2}))$$

The *j* - invariant of *E* is:

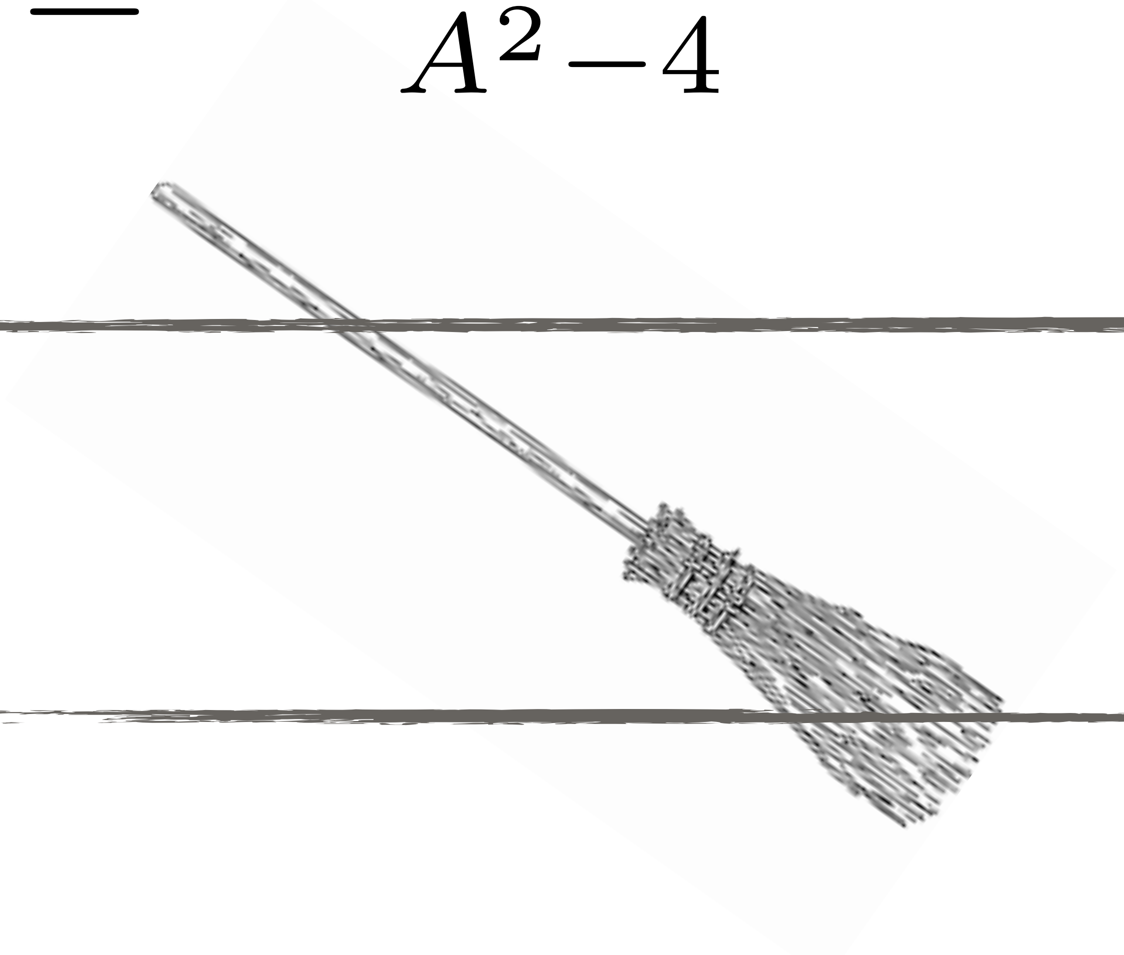
$$j(E) = \frac{256(A^2-3)^3}{A^2-4}$$

For a given integer *m* by *E[m]* we denote the set:

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

If $p \nmid m$, then:

$$E[m] \simeq \mathbb{Z}_m \times \mathbb{Z}_m$$



Two elliptic curves are isomorphic <u>if and only if</u> they have the same *j* - invariant

Isogenies

Let us consider the set of all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.

Isogenies

Let us consider the set of all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.

Two of them, *E₁* and *E₂*, are isogenous if there exists a rational map

$$\begin{aligned}\phi: \quad & E_1 && \to && E_2 \\ & (x,y) && \mapsto && \left(\frac{p_1(x)}{q_1(x)}, y\frac{p_2(x)}{q_2(x)}\right)\end{aligned}$$

such that:

- $p_1(x), q_1(x), p_2(x), q_2(x) \in \mathbb{F}_{p^2}[x]$
- $\phi : E_1(\mathbb{F}_{p^2}) \to E_2(\mathbb{F}_{p^2})$ **is a group homomorphism**

Isogenies

Let us consider the set of all supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.

Two of them, E_1 and E_2, are isogenous if there exists a rational map

$$\begin{array}{rccc} \phi : & E_1 & \to & E_2 \\ & (x,y) & \mapsto & \left(\frac{p_1(x)}{q_1(x)}, y\frac{p_2(x)}{q_2(x)}\right) \end{array}$$

such that:

- $p_1(x), q_1(x), p_2(x), q_2(x) \in \mathbb{F}_{p^2}[x]$
- $\phi : E_1(\mathbb{F}_{p^2}) \to E_2(\mathbb{F}_{p^2})$ **is a group homomorphism**

- E_1 and E_2 are isogenous if and only if

$$\#E_1(\mathbb{F}_{p^2}) = \#E_2(\mathbb{F}_{p^2})$$

- $Ker(\phi) = \{P \in E_1 \mid \phi(P) = \infty\}$
- $\mid Ker(\phi) \mid = \deg(\phi)$
- for any subgroup $H \subset E_1(\mathbb{F}_{p^2})$, there is a unique isogeny $\phi : E_1 \to E'$ with kernel H (and degree $|H|$)
- Velu's formula to find $\phi : E_1 \to E'$

Isogenies

$$S_{p^2} = \#\{j \in \mathbb{F}_{p^2} \mid j \text{ is the } j\text{-invariant of a supersingular curve}\}$$

$$\boxed{S_{p^2} = \lfloor \tfrac{p}{12} \rfloor + r, \qquad r \in \{0, 1, 2\}}$$

ALL SUPERSINGULAR ELLIPTIC CURVES OVER $\mathbb{F}_{p^2}$ ARE IN THE SAME ISOGENY CLASS.

KEY EXCHANGE PROTOCOL: Public Parameters

- **two positive integers e_2 and $e3$**
- **a prime** $p = 2^{e_2}3^{e_3} - 1$
- **the finite field** $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$
- **a supersingular elliptic curve E_0 over** $\mathbb{F}_{p^2}$ **:**

$$E_0 : y^2 = x^3 + x \qquad\qquad j(E_0) = 1728$$

- $\#E_0(\mathbb{F}_{p^2}) = (2^{e_2}3^{e_3})^2$
- P_2, Q_2 **s.t.** $E_0[2^{e_2}] =< P_2, Q_2 >$
- P_3, Q_3 **s.t.** $E_0[3^{e_3}] =< P_3, Q_3 >$

Public and private keys

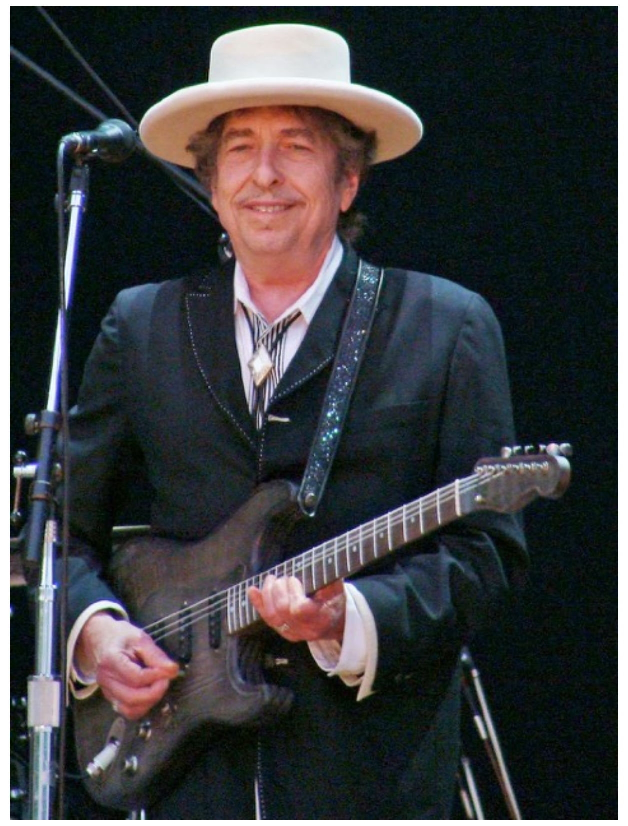
Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$

Public and private keys

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

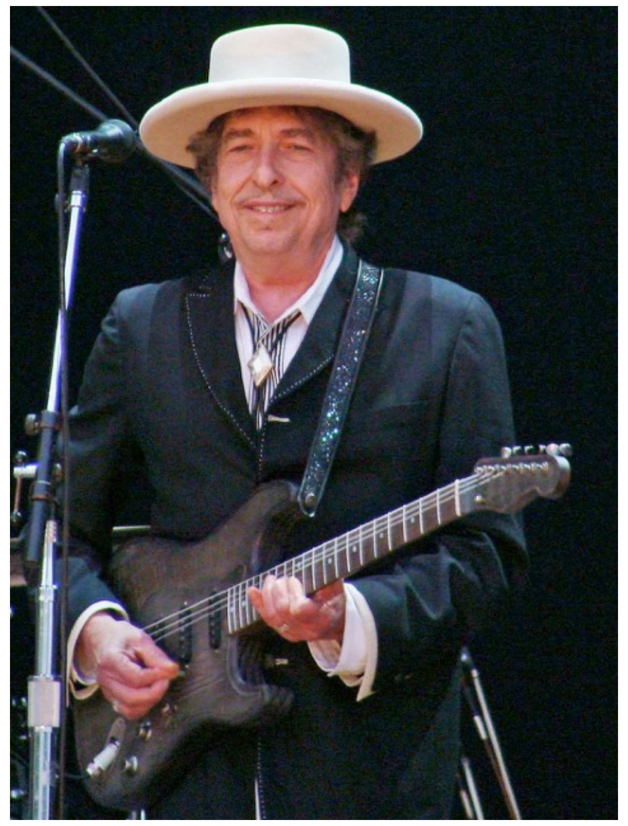
Public and private keys

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



Public and private keys

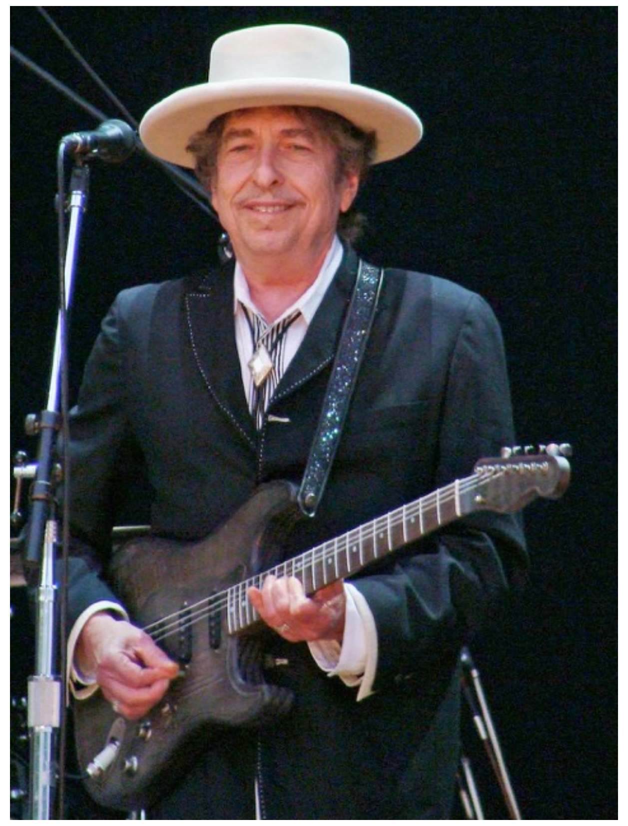
Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$



Selects a private $sk_B \in [1, \ldots, 2^{e_2} - 1]$

Public and private keys

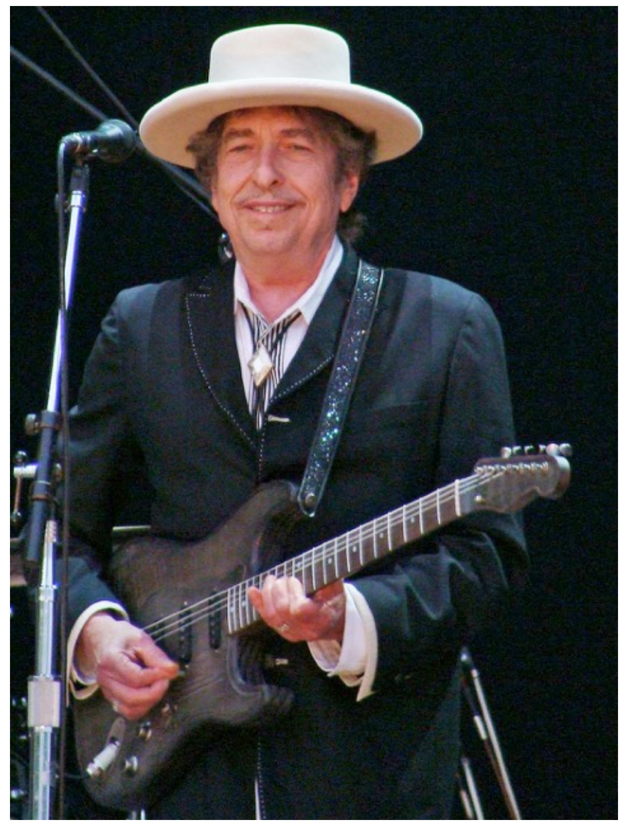
Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$



- **Selects a private** $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- **Computes** $P_2 + sk_B Q_2$

Public and private keys

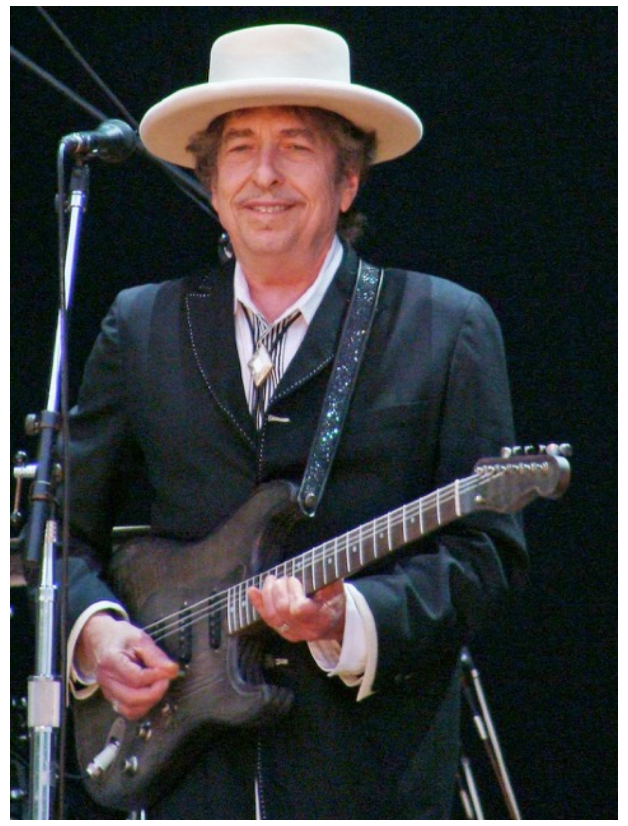
Public parameters: $\mathbb{F}_{p^2}, E_0, P_2, Q_2, P_3, Q_3$



- **Selects a private** $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- **Computes** $P_2 + sk_B Q_2$
- $< P_2 + sk_B Q_2 > \subset E_0[2^{e_2}]$ **is a subgroup of order** 2^{e_2}

Public and private keys

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

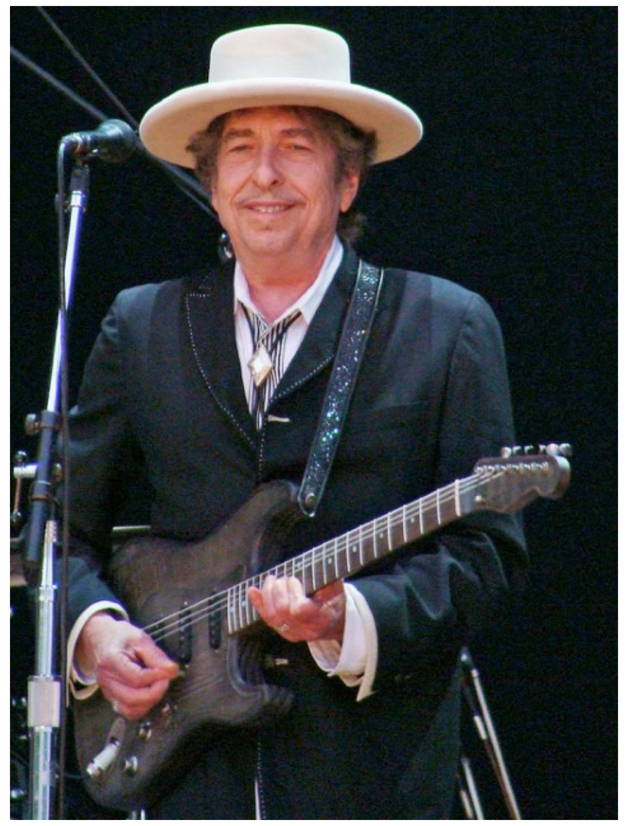


- **Selects a private** $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- **Computes** $P_2 + sk_B Q_2$
- $< P_2 + sk_B Q_2 > \subset E_0[2^{e_2}]$ **is a subgroup of order** 2^{e_2}

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

Public and private keys

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

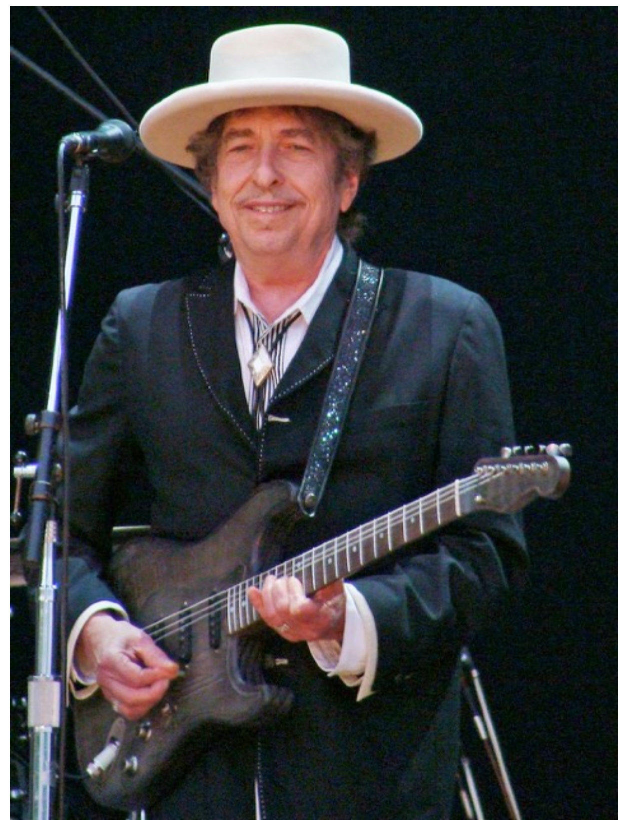


- **Selects a private** $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- **Computes** $P_2 + sk_B Q_2$
- $< P_2 + sk_B Q_2 > \subset E_0[2^{e_2}]$ **is a subgroup of order** 2^{e_2}

- **Selects a private** $sk_A \in [1, \ldots, 3^{e_3} - 1]$
- **Computes** $P_3 + sk_A Q_3$

Public and private keys

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

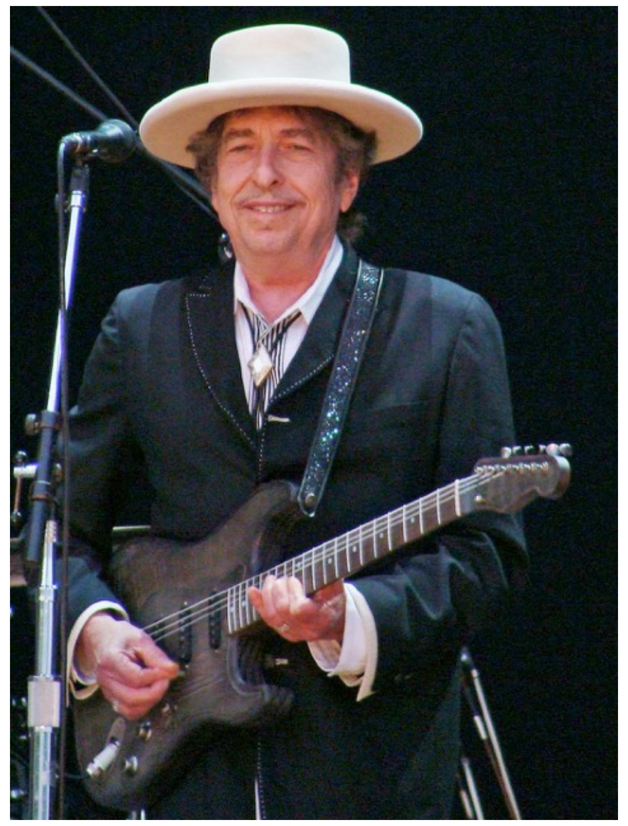


- **Selects a private** $sk_B \in [1, \ldots, 2^{e_2} - 1]$
- **Computes** $P_2 + sk_B Q_2$
- $< P_2 + sk_B Q_2 > \subset E_0[2^{e_2}]$ **is a subgroup of order** 2^{e_2}

- **Selects a private** $sk_A \in [1, \ldots, 3^{e_3} - 1]$
- **Computes** $P_3 + sk_A Q_3$
- $< P_3 + sk_A Q_3 > \subset E_0[3^{e_3}]$ **is a subgroup of order** 3^{e_3}

Public and private keys

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

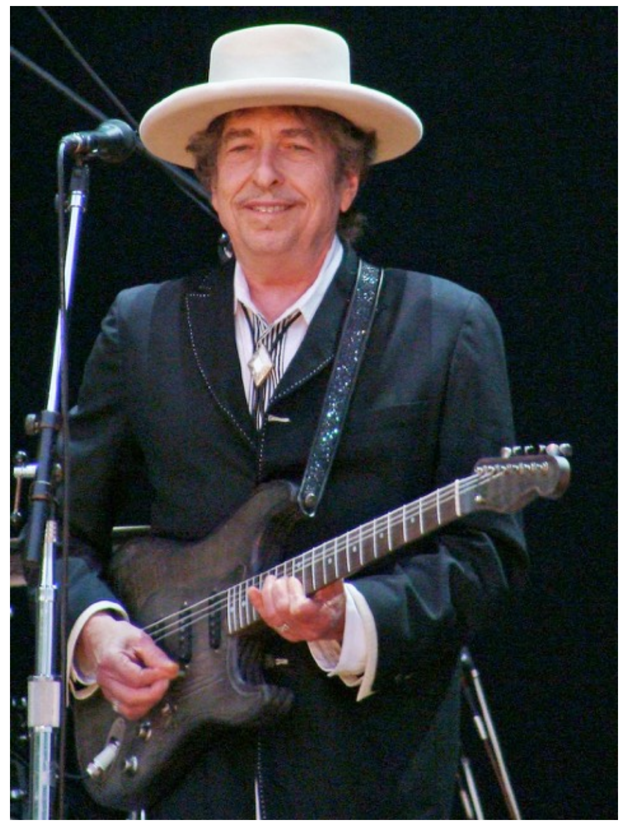
$P_2 + sk_B Q_2$ 

 $P_3 + sk_A Q_3$

Public and private keys

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

$P_2 + sk_B Q_2$



Computes the unique isogeny

$$\phi_B : E_0 \to E_B$$

having kernel

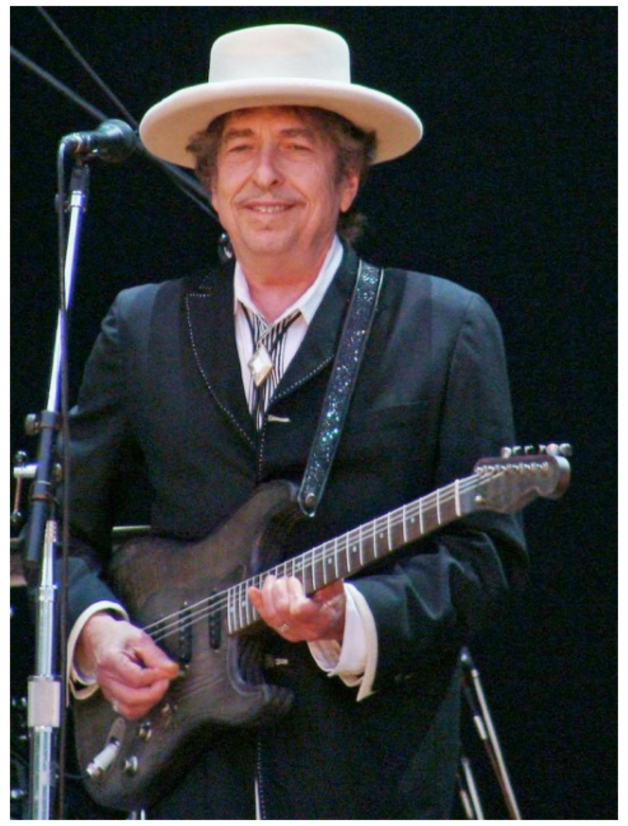
$$H_B =< P_2 + sk_B Q_2 >$$

$P_3 + sk_A Q_3$

Public and private keys

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

$P_2 + sk_B Q_2$



Computes the unique isogeny

$$\phi_B : E_0 \to E_B$$

having kernel

$$H_B = < P_2 + sk_B Q_2 >$$

$P_3 + sk_A Q_3$

Computes the unique isogeny

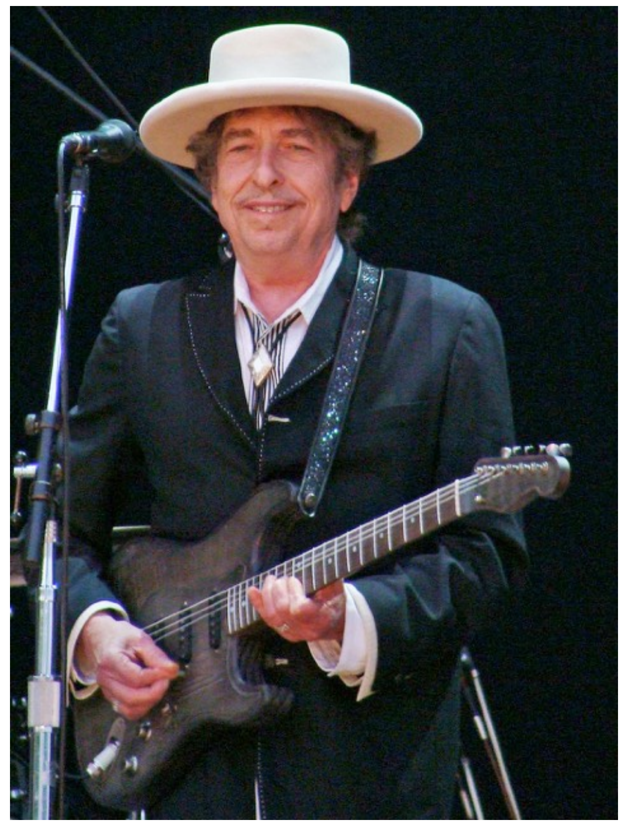
$$\phi_A : E_0 \to E_A$$

having kernel

$$H_A = < P_3 + sk_A Q_3 >$$

Public and private keys

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



Public key: E_B

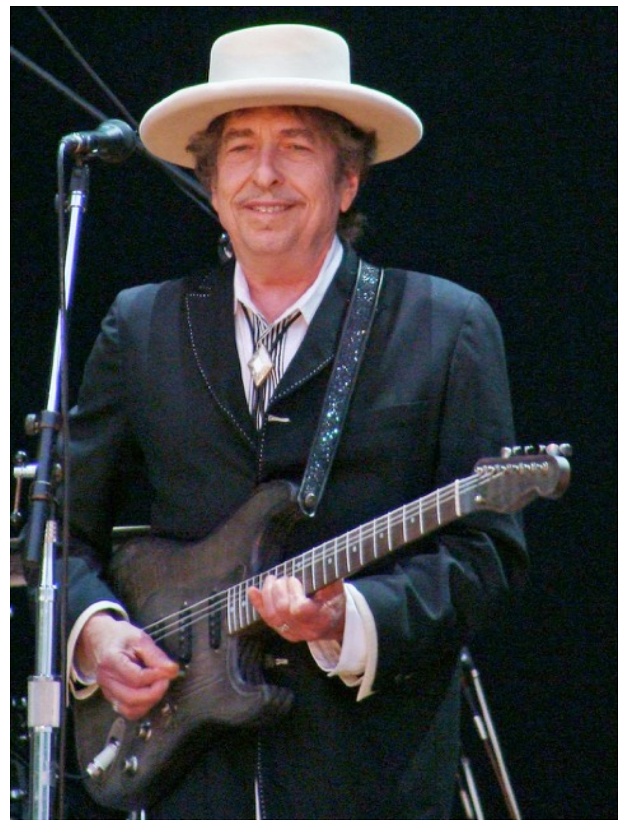
Private key: sk_B, ϕ_B

Public key: E_A

Private key: sk_A, ϕ_A

Public and private keys

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



Public key: E_B

Private key: sk_B, ϕ_B

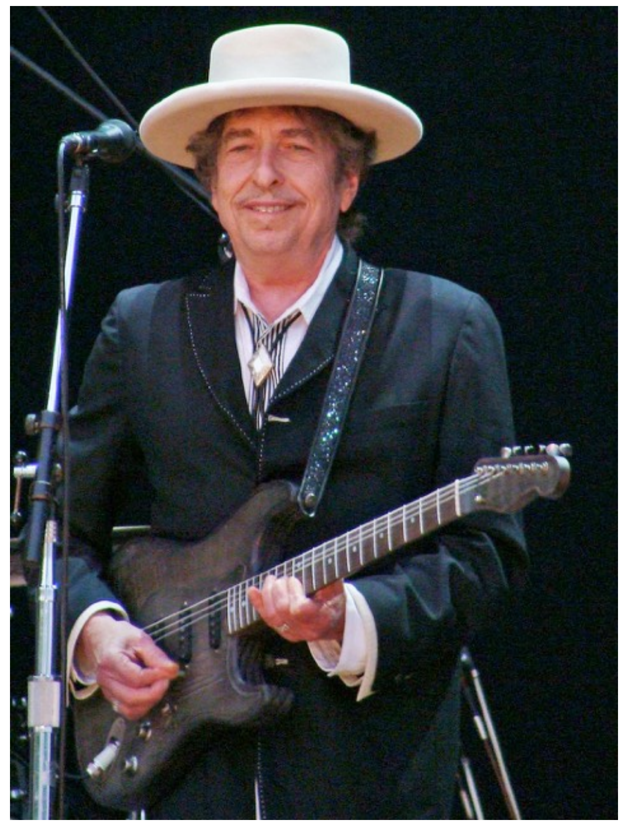
Public key: E_A

Private key: sk_A, ϕ_A

Computes $\phi_B(P_3), \phi_B(Q_3)$ **and sends**

Public and private keys

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



Public key: E_B

Private key: sk_B, ϕ_B

Public key: E_A

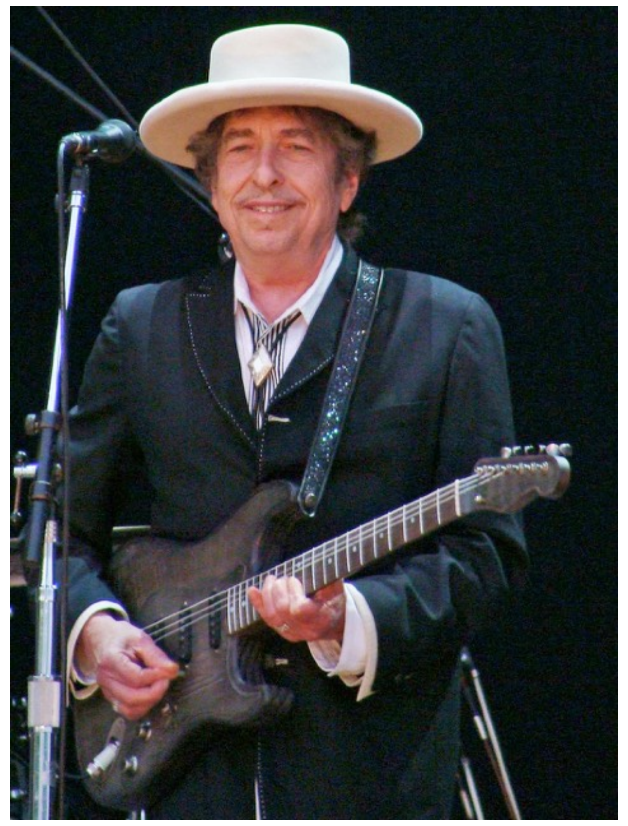
Private key: sk_A, ϕ_A

Computes $\phi_B(P_3), \phi_B(Q_3)$ **and sends**

Computes $\phi_A(P_2), \phi_A(Q_2)$ **and sends**

Public and private keys

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



Public key: E_B

Private key: sk_B, ϕ_B

Public key: E_A

Private key: sk_A, ϕ_A

Computes $\phi_B(P_3), \phi_B(Q_3)$ **and sends**

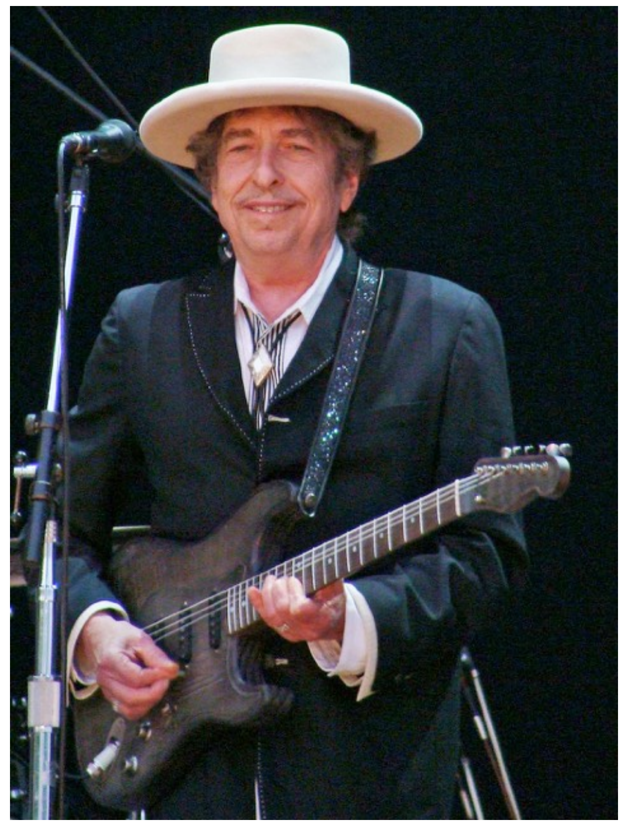
Computes $\phi_A(P_2), \phi_A(Q_2)$ **and sends**

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

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

Public and private keys

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



Public key: E_B

Private key: sk_B, ϕ_B

Public key: E_A

Private key: sk_A, ϕ_A

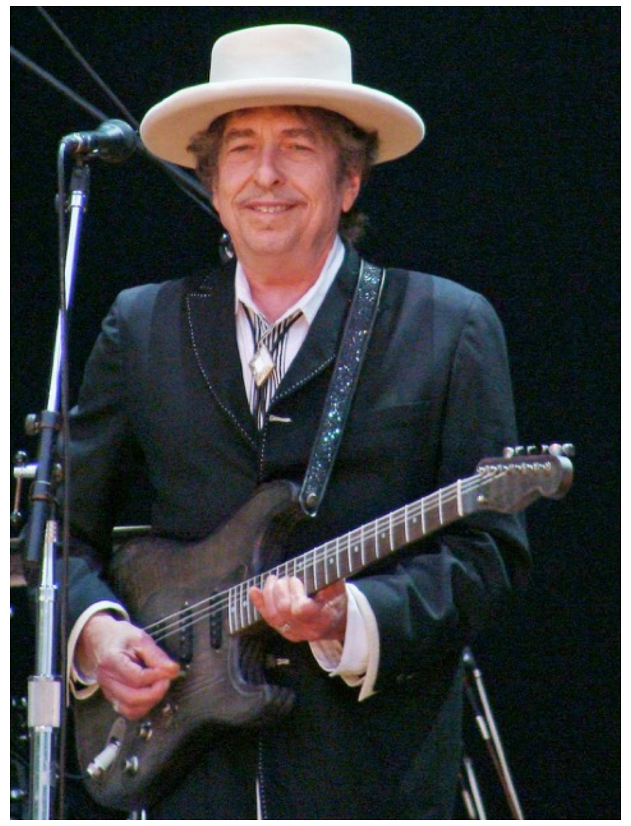
Computes $\phi_B(P_3), \phi_B(Q_3)$ **and sends**

Computes $\phi_A(P_2), \phi_A(Q_2)$ **and sends**

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 shared secret key



E_{AB} E_{BA}

The two curves obtained by Alice and Bob have the same j - invariant:

THEY ARE ISOMORPHIC!

Efficiency

Montgomery curves are used in order to **speed up computations** among points of the curves.

Isogenies are computed **composing**:

- isogenies of **degree 2** (by Bob)

- isogenies of **degree 3** (by Alice)

Security

The hard problem is:

given two supersingular isogenous curves, E and $E' = \phi(E)$, find ϕ

Best (known) attack: Claw Algorithm

Complexity: classical $O(p^{1/4})$ and quantum $O(p^{1/6})$

Thank you for your attention!

federico.pintore@unitn.it