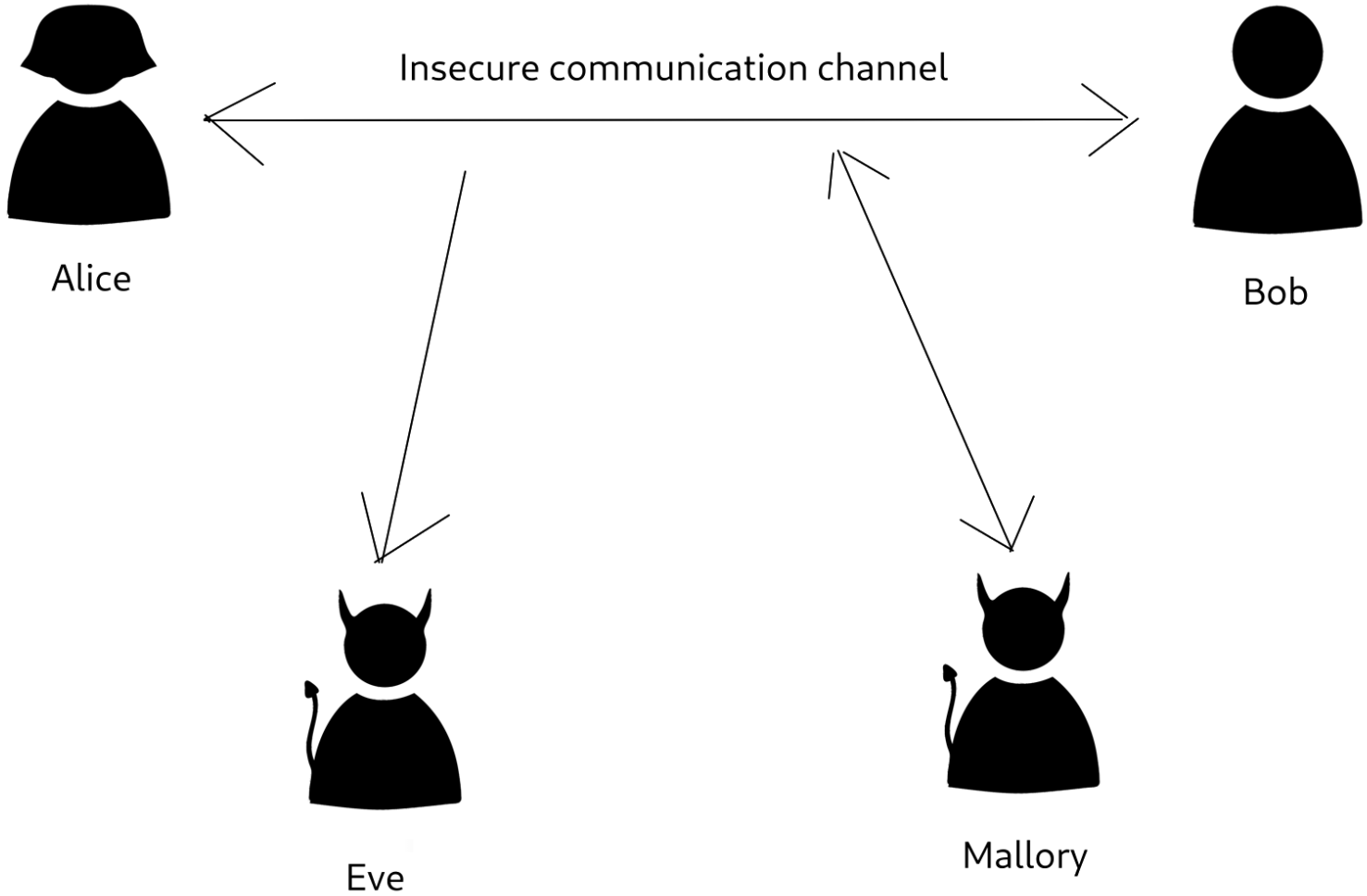
Elliptic Curves in Post-Quantum Cryptography

Mickaël Montessinos

Vilnius University

Monday 23rd May, 2022

Cryptography: Communication through insecure channels



The discrete logarithm assumption

Definition (Discrete logarithm)

Let $\mathbb{G}$ be a cyclic group of order r, and let g be a generator of $\mathbb{G}$. Let $h \in \mathbb{G}$. Then the discrete logarithm of base g of h, written $\log_g(h)$, is the unique element $x \in \mathbb{Z}_r$ such that

$$h = g^x.$$

The discrete logarithm assumption

Given a certain cyclic group $\mathbb{G}$, we assume that there is no polynomial-time algorithm (i.e polynomial in the logarithm of $|\mathbb{G}|$) which, given a generator g of $\mathbb{G}$ and some $h \in \mathbb{G}$, computes $\log_g(h)$.

The Diffie Hellman key exchange

Diffie & Hellman, 1976

Alice		**Bob**
g generates $\mathbb{F}_p^\times$		
$x_A \leftarrow\!\!\$\ \mathbb{Z}_{p-1}$		
$y_A \leftarrow g^{x_A}$		
	$\xrightarrow{p, g, y_A}$	
		$x_B \leftarrow\!\!\$\ \mathbb{Z}_{p-1}$
		$y_B \leftarrow g^{x_B}$
	$\xleftarrow{y_B}$	
$\mathsf{k}_A \leftarrow y_B^{x_A} = g^{x_B x_A}$		$\mathsf{k}_B \leftarrow y_A^{x_B} = g^{x_A x_B}$

The quantum menace

Theorem (Shor, 1994)

There exists a bounded-error quantum polynomial time algorithm which, on input a generator $g \in \mathbb{F}_p^\times$ and $X = g^x$, outputs x.

In practice

- A concrete implementation of Shor's algorithm for solving the Discrete Logarithm Problem on NIST standardized curve P-256 would need 2330 qubits. (Roetteler, Naehrig, Svore, Lauter 2017)
- The largest quantum processing unit currently announced has 127 qubits (IBM Eagle, November 2021).
- IBM's projections aim for 1121 qubits in 2023.

Some definitions

Definition (Elliptic curve)

An elliptic curve is a projective curve defines over a field k (assuming $\mathrm{char}\ k \neq 2, 3$) given by an equation of the form

$$E : y^2 = x^3 + Ax + B$$

such that $\Delta = -16(4A^3 + 27B^2) \neq 0$.

Definition (j-invariant)

The j-invariant of an elliptic curve E is $j = -1728\frac{(4A)^3}{\Delta}$. It characterises the isomorphy class of E over $\overline{k}$.

Some more definitions

Group structure

The set of k-rational points $E(k)$ of an elliptic curve E/k admits a structure of abelian group, with its neutral element O being the unique point at infinity.

Definition (Isogeny)

An isogeny between two elliptic curves E/k and E'/k is an algebraic map that is also a group homomorphism.
The *degree* of an isogeny is a non-negative integers measuring the algebraic complexity of an isogeny.
An n-isogeny is an isogeny of degree n.
An isogeny is *separable* if its degree equals the cardinal of its Kernel.

An example of isogeny

Example

Let $m \in \mathbb{Z}$. The multiplication-by-m map $[m] : \begin{array}{ccc} E & \to & E \\ P & \mapsto & \underbrace{P + P + \ldots + P}_{m \text{ times}} \end{array}$

is an isogeny of degree m^2.

Theorem

There is a one-to-one correspondence between separable isogenies with domain E/k up to isomorphism and finite subgroups of $E(\overline{k})$.
The correspondence is given by $\varphi \mapsto \mathrm{Ker}\ \varphi$.

Example

The kernel of a multiplication-by-m map is the m-torsion part of $E(\overline{k})$. If m is coprime with p, it is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^2$.
A curve $E/\mathbb{F}_{p^n}$ is supersingular if $[p]$ is purely inseparable (i.e it is injective).

The supersingular ℓ-isogeny graph

- 2-SSIG is 3-regular.
- Has 38 vertices but its diameter is 7.
- Walking on the graph is computationaly easy.
- Pathfinding in the graph is conjectured to be intractable (for large p)

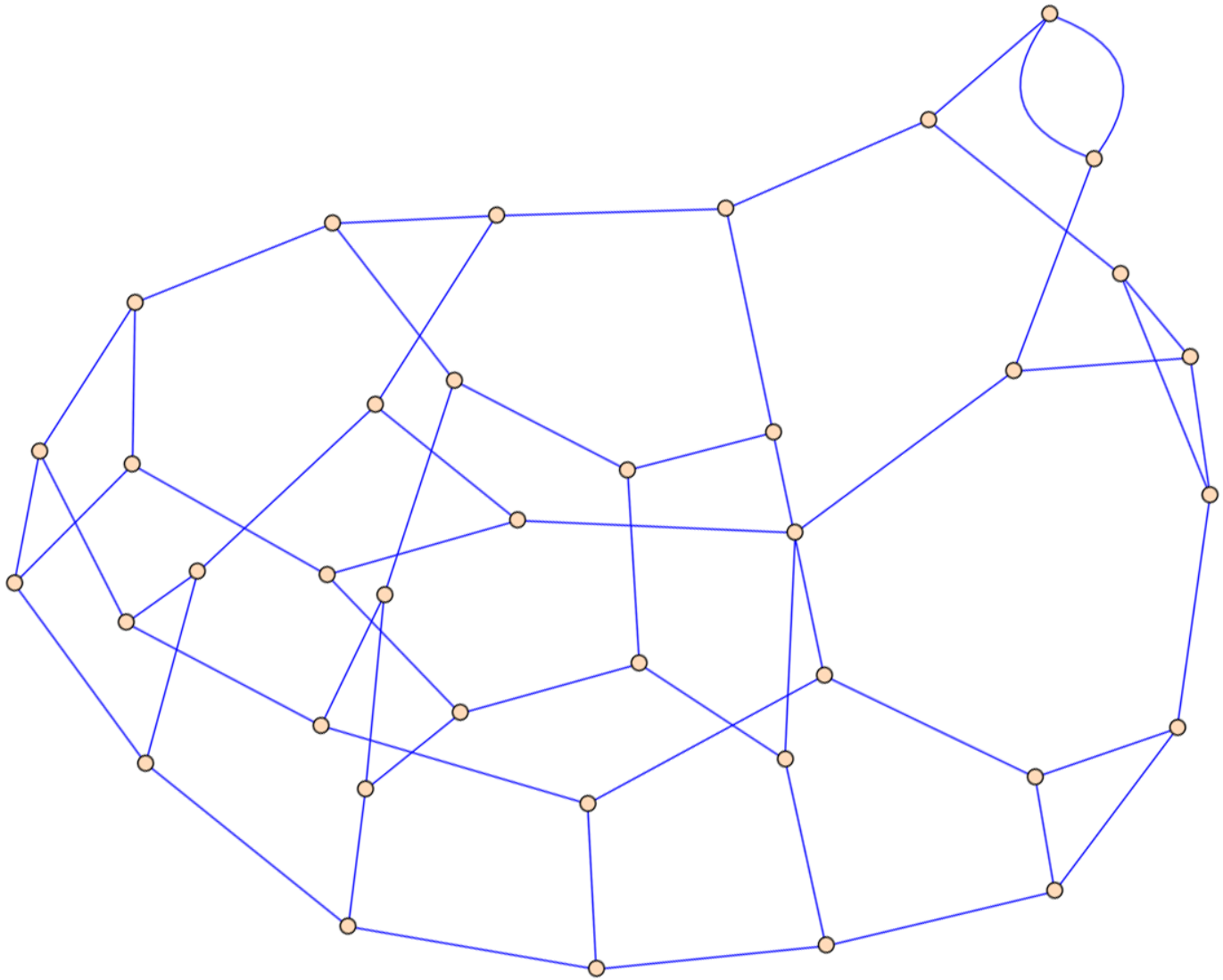


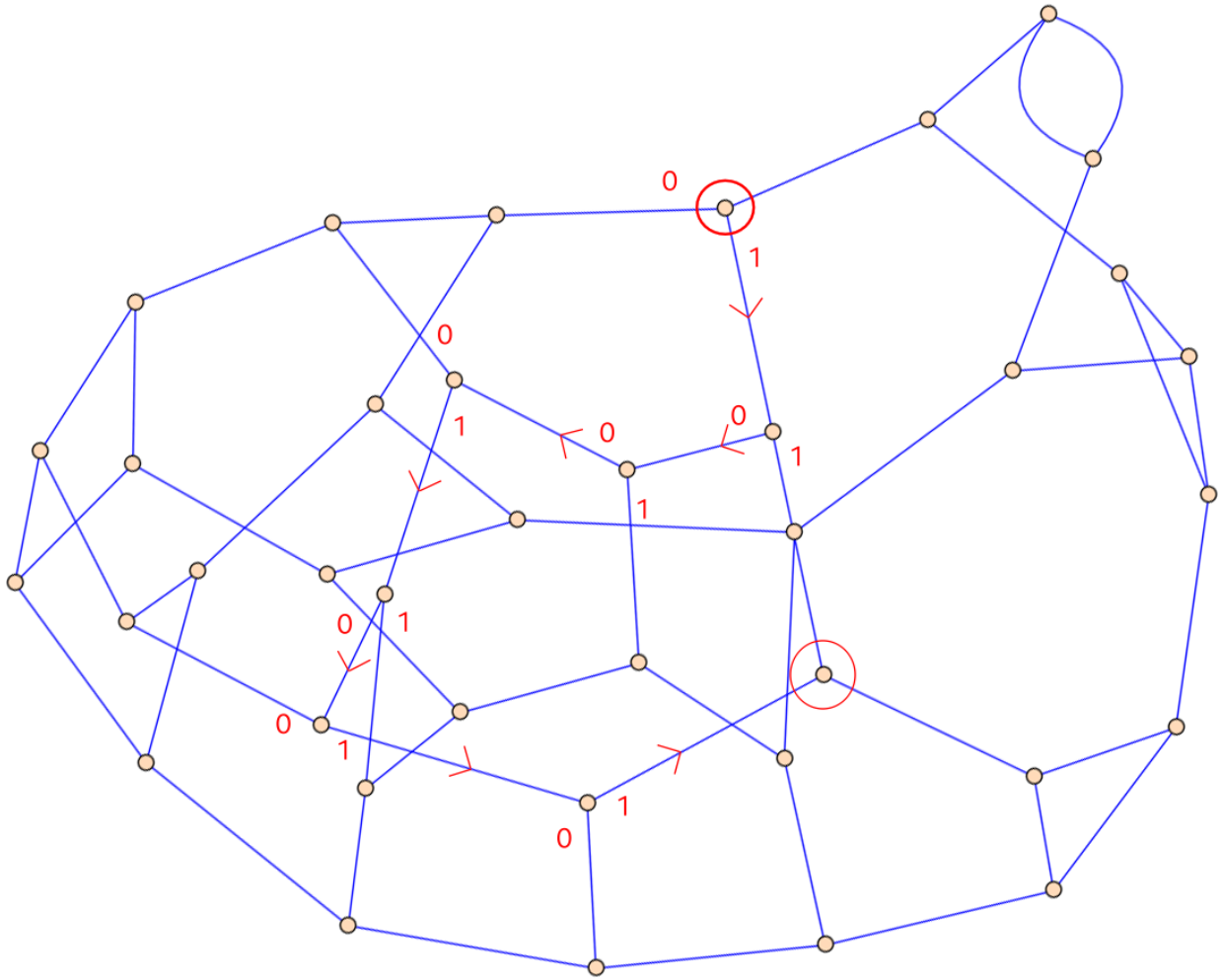
Figure: The 2-supersingular isogeny graph over $\mathbb{F}_{457^2}$

Walking on the 2-SSIG

(Charles, Goren, Lauter 2009)

Velu's formula: $E/\langle(x_0, 0)\rangle : y^2 = x^3 - (4a + 15x_0^2)x + (8B - 14x_0^2)$

Path: 1001011



Towards a supersingular Diffie-Hellman key exchange protocol

Setting

A suitable prime p is selected, as well as a base supersingular curve E_0. Alice and Bob both generate a secret isogeny φ_A (resp. φ_B) from E_0 to E_A (resp. to E_B).

Problem

How to compose φ_A and φ_B in a commutative way, when their domains and codomains do not even match?

Composition of isogenies

Composing isogenies and the subgroup correspondence

$$E \xrightarrow{\varphi} E/H \xrightarrow{\varphi'} E/H'$$

$$\iff \text{Ker } \varphi' = \varphi(H')$$

Cyclic isogenies

An isogeny is *cyclic* if its kernel is a cyclic group: $H =< P >$.
Then the situation becomes

$$E \xrightarrow{\varphi} E/ < P > \xrightarrow{\varphi'} E/ < P, Q >$$

$$\iff \text{Ker } \varphi' =< \varphi(Q) >$$

SIDH

De Feo, Jao 2011

Choose parameters s.t $\ell_A^{e_A}\ell_B^{e_B} f \pm 1 = p$ is prime and a starting curve $E_0/\mathbb{F}_{p^2}$ with $\#E_0(\mathbb{F}_{p^2}) = (p \mp 1)^2$. Then $E_0(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p \mp 1)\mathbb{Z})^2$. Choose a basis (P_A, Q_A) of $E_0[\ell_A^{e_A}]$ and a basis (P_B, Q_B) of $E_0[\ell_B^{e_B}]$.

Alice		**Bob**
$n_A \leftarrow\$ \mathbb{Z}_{\ell_A^{e_A}}$		
$E_A \leftarrow E_0/\langle P_A + n_A Q_A \rangle$		
$\varphi_A \leftarrow (E \to E_A)$		
	$\xrightarrow{E_A, \varphi_A(P_B), \varphi_A(Q_B)}$	
		$n_B \leftarrow\$ \mathbb{Z}_{\ell_B^{e_B}}$
		$E_B \leftarrow E_0/\langle P_B + n_B Q_B \rangle$
		$\varphi_B \leftarrow (E_0 \to E_B)$
	$\xleftarrow{E_B, \varphi_B(P_A), \varphi_B(Q_A)}$	
$E_{BA} \leftarrow E_B/\langle \varphi_B(P_A + n_A Q_A) \rangle$		$E_{AB} \leftarrow E_A/\langle \varphi_A(P_B + n_B Q_B) \rangle$

Many more protocols!

- CSIDH (CLMPR 2018): key exchange based on the CM-action by the class group of an imaginary quadratic order.
- CSI-FiSH (BKV 2019): signature scheme based on the CSIDH setting.
- SQISign (DKLPW 2020): signature scheme based on quaternionic multiplication.
- Séta (DDFKLPSW 2021): encryption scheme based on torsion-point attacks on SIDH.
- Many more...

Open Problems

- Improve efficiency of existing protocols. Designing better algorithms for isogeny computations and related tasks.
- Cryptanalysis of existing protocols. Computing endomorphism rings of supersingular elliptic curves, torsion point attacks...
- Design new protocols.
- Producing hard curves. It is currently unknown how to produce a supersingular elliptic curve in a way that does not reveal information about its endomorphism ring.

Theorem (KLPT14,EHLMP18, W21)

The problems of pathfinding in the supserinsular ℓ-isogeny graph and of computing the endomorphism ring of a given supersingular elliptic curve are equivalent.