Post-quantum secure key-exchange

Simon MASSON `simon.masson@loria.fr`

Advisors: Aurore Guillevic, Emmanuel Thomé

December 5, 2019 **Journée d'Automne de l'École Doctorale IAEM** **Nancy, France**

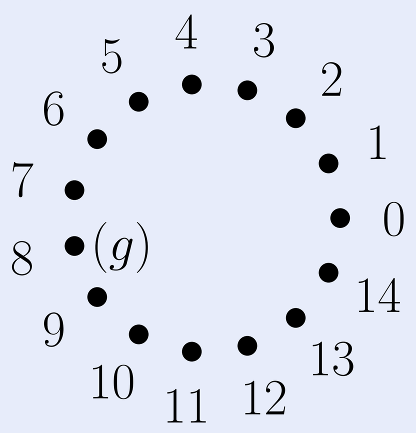
Discrete logarithm problem in cryptography

Given a cyclic group $(G, \star)$ with a generator g, and another element h, find the integer s such that $h = g^{\star s} := \underbrace{g \star g \star \ldots \star g}_{s \text{ times}}$.

This problem is **exponentially hard** in some particular groups. Even with your laptop, you cannot solve it in such groups.

Example 1. $(\mathbb{Z}/n\mathbb{Z}, +)$

Let n be an integer ≥ 2.
With the addition law,
$G = \mathbb{Z}/n\mathbb{Z}$ is a cyclic group.



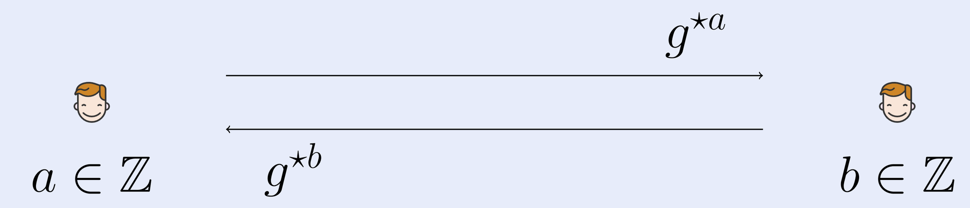
For $n = 15$, $g = 8$ is a generator.
The discrete logarithm is **easy**:
if $h = s \times 8$, we recover s using a division:
$s = h/8$

Example 2. Invertibles of a finite field $\mathbb{F}_{p^k}^{\times}$

The set of invertibles of a finite field $\mathbb{F}_{p^k}$ is a cyclic group for the multiplication law. Subexponential algorithms compute the discrete logarithm on these groups. The discrete logarithm problem is solved in **subexponential** time: it is the *flagship* topic of CARAMBA team (LORIA).

Diffie-Hellman

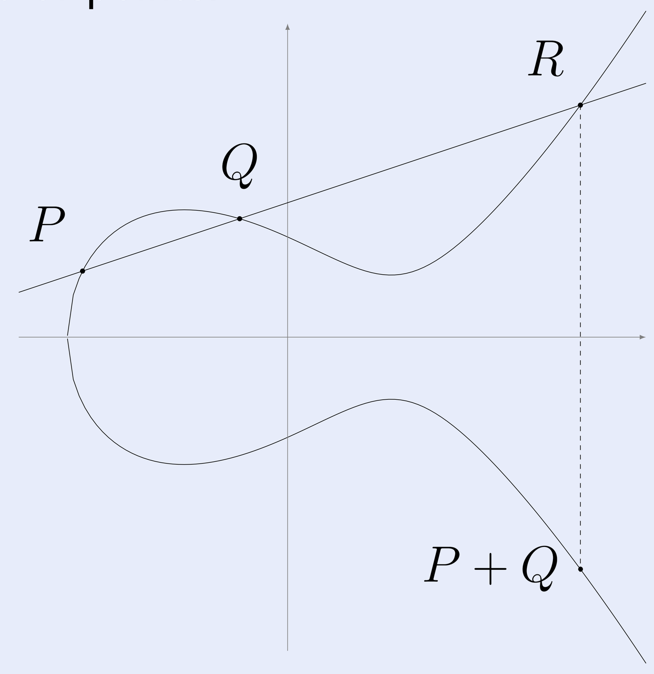
Let $G = \langle g \rangle$ with a hard discrete logarithm problem.
Alice and Bob can share a common secret:



Step 1. Alice and Bob choose secret integers a and b
Step 2. Alice sends to Bob $g^{\star a}$
Step 3. Bob sends to Alice $g^{\star b}$
Step 4. The common secret is $(g^{\star a})^{\star b}$

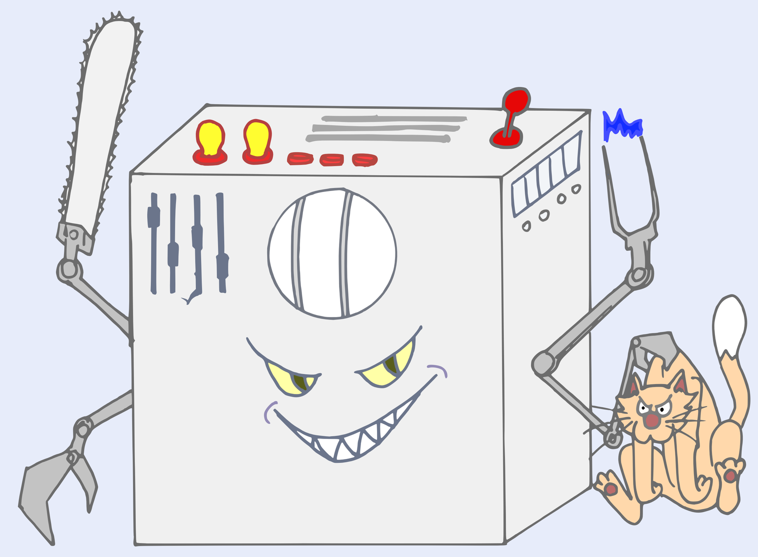
Example 3. Elliptic curves

Points of an elliptic curve defined over $\mathbb{F}_p$ with the geometric group law described below is a finite abelian group. The discrete logarithm problem is solved in **exponential** time on this group. The best algorithm is $O(\sqrt{\#G})$ on a cyclic subgroup of the curve group of points.



Quantum computer

Discrete logarithm problem on a quantum computer is solved in **polynomial** time for finite fields and elliptic curves !



Rachel Deyts (2018)

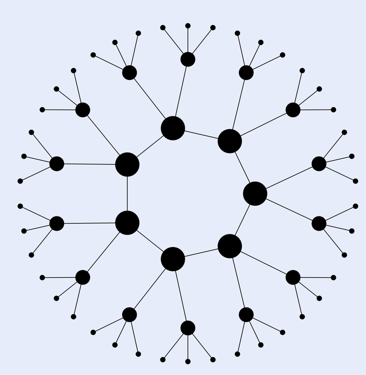
Isogeny of elliptic curves

An isogeny is a morphism of elliptic curves $\varphi : E_1 \longrightarrow E_2$ such that $\varphi(0_{E_1}) = 0_{E_2}$. Recover the isogeny φ from the two curves E_1 and E_2 is **hard** when $\deg(\varphi)$ is large, even with a quantum computer.

Diffie-Hellman becomes post-quantum resistant using isogenies.

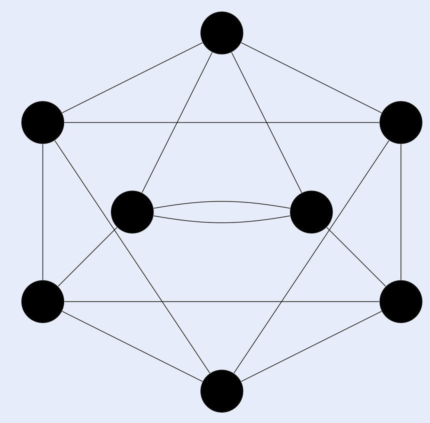
NIST Standardization key-exchange:
Alice and Bob choose a secret walk on the graph of supersingular curves defined over $\mathbb{F}_{p^2}$ (also possible over $\mathbb{F}_p$).
They publish their target curves and additional informations.
They compute their walk from the other curve to get a common shared curve.

Isogeny graph over $\mathbb{F}_p$



Example of degree 3 isogeny graph over $\mathbb{F}_p$.
The graph is a volcano.

Isogeny graph over $\mathbb{F}_{p^2}$



Example of degree 3 isogeny graph over $\mathbb{F}_{p^2}$.
The graph is expander.

Contributions

Cocks-Pinch curves of embedding degrees five to eight and optimal ate pairing computation
with Aurore Guillevic and Emmanuel Thomé
`ia.cr/2019/431`
In revision for Design, Codes and Cryptography journal.

Verifiable delay functions from supersingular isogenies and pairings
with Luca De Feo, Christophe Petit and Antonio Sanso
`ia.cr/2019/166`
Accepted at Asiacrypt 2019 conference.

Loria Laboratoire lorrain de recherche en informatique et ses applications

THALES

CARAMBA

Inria