



## **RADICAL ISOGENIES !**

Wouter Castryck, Thomas Decru, Frederik Vercauteren

Rump session ANTS-XIV, New Zoomland, 1 July 2020

A historical painting depicting a large gathering, likely a Soviet congress or a military assembly, in a grand hall. A man in a dark suit stands on a raised platform, gesturing with his right arm raised. Behind him, several red banners are visible, one with the word 'СОЮЗ' (Union) partially legible. The crowd below is dense and filled with people, many of whom are clapping and raising their hands in approval. The scene is lit with warm, indoor lighting, and the architecture features high ceilings and large windows.

Comrades ! Are you also struggling with computing  
endless chains of  $N$ -isogenies between elliptic curves ?

Yes, in SIDH !

... and in  
CSIDH !

YES !

YES !

YES !

YES !

YES !

YES !

YES !

... over finite fields  $F_q$  with  $\gcd(N - 1, q) = 1$  ?

Yes, in  
CSIDH !

YES !

YES !

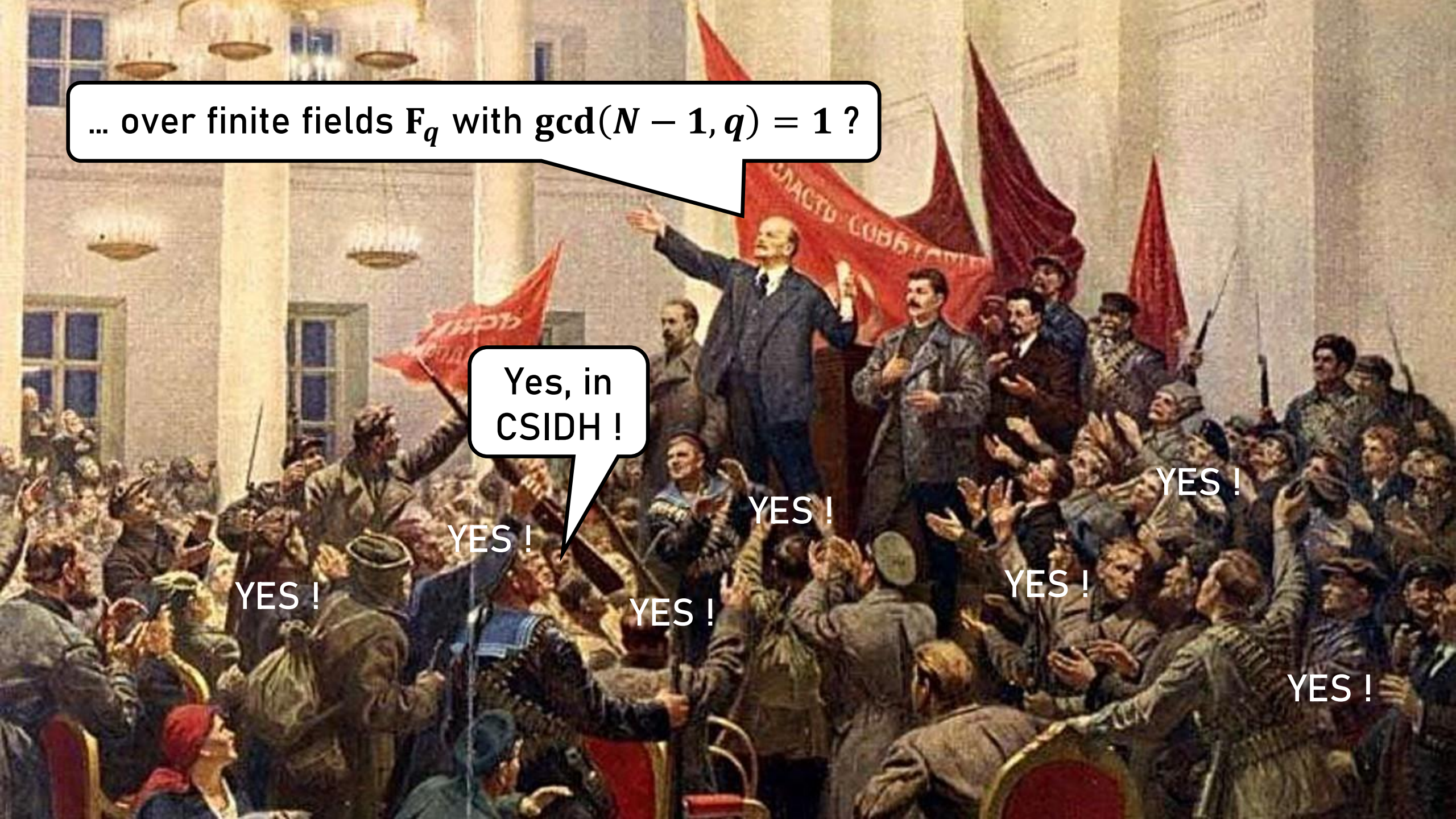
YES !

YES !

YES !

YES !

YES !



Are you also fed up with sampling random  $F_q$ -rational points and multiplying by  $\#E(F_q)/N$ , before applying Vélu, at each step ?



YES !

YES !

YES !

YES !

YES !

YES !

YES !

Behold, we present to you:



**RADICAL ISOGENIES !**



**RADICAL ISOGENIES !**

**RADICAL ISOGENIES !**

**RADICAL ISOGENIES !**

**RADICAL ISOGENIES !**

Observation: for each  $N \geq 2$  there exist concrete **radical formulas**

$$\begin{aligned} x_1 & \left( a_1, a_2, a_3, a_4, a_6, x_0, y_0, \sqrt[N]{\rho(a_1, a_2, a_3, a_4, a_6, x_0, y_0)} \right) \\ y_1 & \left( a_1, a_2, a_3, a_4, a_6, x_0, y_0, \sqrt[N]{\rho(a_1, a_2, a_3, a_4, a_6, x_0, y_0)} \right) \end{aligned}$$

such that for whatever cyclic  $N$ -isogeny we computed using Vélu

$$E_0: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad P_0 = (x_0, y_0)$$

$$\downarrow \varphi$$

$$E_1 = E_0 / \langle P_0 \rangle \longrightarrow E_2 = E_1 / \langle P_1 \rangle$$

these produce a point  $P_1 = (x_1, y_1) \in E_1$  extending  $\varphi$  to a cyclic  $N^2$ -isogeny.

Proof 1:

- Forgetful map between modular curves

$$X'_1(N) = \{(E_0, P_0, P_1)\}$$



$$X_1(N) = \{(E_0, P_0)\}$$

is a **simple radical extension** (analysis of Galois groups).

Proof 2 (in progress, but more explicit):

- Conjectural formula that will be discussed in next week's workshop.
- Leads to concrete formula for  $\rho$  in terms of well-known modular units.

Example: for  $N = 5$ , assume w.l.o.g. that we are in Tate normal form:

$$E_0: y^2 + (1 - b)xy - by = x^3 - bx^2, \quad P_0 = (0, 0).$$

Then Vélu produces

$$E_1: y^2 + (1 - b)xy - by = x^3 - bx^2 - (5b^3 + 10b^2 - 5b)x \\ - (b^5 + 10b^4 - 5b^3 + 15b^2 - b).$$

We can take

$$x_1 = (\sqrt[5]{b}^3 + \sqrt[5]{b}^2 + 2\sqrt[5]{b} - 2)b + 5\sqrt[5]{b}^4 - 3\sqrt[5]{b}^3 + 2\sqrt[5]{b}^2 - \sqrt[5]{b} \\ y_1 = (\sqrt[5]{b}^2 - \sqrt[5]{b} - 1)b^2 + (\sqrt[5]{b}^3 - 10\sqrt[5]{b}^2 + 13\sqrt[5]{b} - 11)b \\ + 5\sqrt[5]{b}^4 - 3\sqrt[5]{b}^3 + \sqrt[5]{b}^2.$$

Putting  $(E_1, P_1)$  back into Tate normal form yields recursive formulas.



If our field contains all  $N^{\text{th}}$  roots of unity, then:  $N$  options for  $\sqrt[N]{\rho}$ . This gives generators for all cyclic subgroups of  $E_1$  that extend  $\varphi$  to a cyclic  $N^2$ -isogeny.

Over  $\mathbf{F}_q$  with  $\gcd(q - 1, N) = 1$  there is a unique choice for  $\sqrt[N]{\rho}$ , which can be computed by mere exponentiation:

- costs  $\approx \frac{3}{2} \log(q)$
- scalar multiplication costs  $\approx 11 \log(q)$

Leads to speed-up factor of up to **50** for chains of  $N$ -isogenies (decays with  $N$ ).

Speeds up CSIDH-512 by about 18%.