Elliptic curves for SNARK and proof systems

Aurore Guillevic[1]

[1]Univ Rennes, Inria, CNRS, IRISA – France

Séminaire Caramba
Nancy, 5 décembre 2024

joint work with Simon Masson

These slides at https://people.rennes.inria.fr/Aurore.Guillevic/talks/2024-10-ECC/24-10-30-ECC-Aurore.pdf zk-SNARK

Elliptic Curves and Pairings

Proof-friendly curves

More embedded curves

More families of embedded curves

Outline

zk-SNARK

Elliptic Curves and Pairings

Proof-friendly curves

More embedded curves

More families of embedded curves

Zero-knowledge proofs (ZKP)

Alice

I know the solution to this complex equation

Bob

No idea what the solution is but Alice claims to know it

Examples:
On this chess board, I know mat in 3 moves
I know where is Wally/Waldo on this drawing
I know a solution to this sudoku grid
I know a preimage of this hash function value

Challenge ←

Response →

Zero-knowledge proofs (ZKP)

Alice

I know the solution to
this complex equation

Examples:
On this chess board, I know mat in 3 moves
I know where is Wally/Waldo on this drawing
I know a solution to this sudoku grid
I know a preimage of this hash function value

Bob

No idea what the solution is
but Alice claims to know it

Challenge ←

Response →

- **Sound**: **Alice** has a wrong solution $\Longrightarrow$ **Bob** is not convinced.

Zero-knowledge proofs (ZKP)

Alice

I know the solution to this complex equation

Examples:
On this chess board, I know mat in 3 moves
I know where is Wally/Waldo on this drawing
I know a solution to this sudoku grid
I know a preimage of this hash function value

Bob

No idea what the solution is but Alice claims to know it

Challenge ←

Response →

- **Sound**: **Alice** has a wrong solution $\implies$ **Bob** is not convinced.
- **Complete**: **Alice** has the solution $\implies$ **Bob** is convinced.

Zero-knowledge proofs (ZKP)

Alice

I know the solution to
this complex equation

Examples:
On this chess board, I know mat in 3 moves
I know where is Wally/Waldo on this drawing
I know a solution to this sudoku grid
I know a preimage of this hash function value

Bob

No idea what the solution is
but Alice claims to know it

Challenge ←

Response →

- **Sound**: **Alice** has a wrong solution $\Longrightarrow$ **Bob** is not convinced.
- **Complete**: **Alice** has the solution $\Longrightarrow$ **Bob** is convinced.
- **Zero-knowledge**: **Bob** does NOT learn the solution.

Example: Sigma protocol

Alice **Bob**

I know $x \in \mathbf{Z}_q$ such that
$g^x = y$ in $\mathbf{G}$, $\#\mathbf{G} = q$ prime

Example: Sigma protocol

Alice **Bob**

I know $x \in \mathbf{Z}_q$ such that
$g^x = y$ in $\mathbf{G}$, $\#\mathbf{G} = q$ prime

$n \xleftarrow{\$} \mathbf{Z}_q$ $\xrightarrow{A = g^n}$

Example: Sigma protocol

Alice | **Bob**

I know $x \in \mathbf{Z}_q$ such that
$g^x = y$ in $\mathbf{G}$, $\#\mathbf{G} = q$ prime

$n \xleftarrow{\$} \mathbf{Z}_q$

$A = g^n$ $\longrightarrow$

$\longleftarrow$ c

$c \xleftarrow{\$} \mathbf{Z}_q$

Example: Sigma protocol

Alice | **Bob**

I know $x \in \mathbf{Z}_q$ such that
$g^x = y$ in $\mathbf{G}$, $\#\mathbf{G} = q$ prime

$n \xleftarrow{\$} \mathbf{Z}_q$ $\quad \xrightarrow{A = g^n}$

$\xleftarrow{c}$ $\quad c \xleftarrow{\$} \mathbf{Z}_q$

$s = n + c \cdot x \bmod q$ $\quad \xrightarrow{s}$

Example: Sigma protocol

Alice		**Bob**
I know $x \in \mathbf{Z}_q$ such that $g^x = y$ in $\mathbf{G}$, $\#\mathbf{G} = q$ prime		
$n \xleftarrow{\$} \mathbf{Z}_q$	$\xrightarrow{A = g^n}$	
	$\xleftarrow{c}$	$c \xleftarrow{\$} \mathbf{Z}_q$
$s = n + c \cdot x \bmod q$	$\xrightarrow{s}$	$g^s \stackrel{?}{=} A \cdot y^c$ with $A \cdot y^c = g^n \cdot g^{x \cdot c}$ then $g^n \cdot g^{x \cdot c} = g^{n + x \cdot c}$

Hide the verification
in the exponents
(the scalar field)

Non-Interactive Zero-Knowledge (NIZK) Sigma protocol

Alice **Bob**

I know x such that $g^x = y$

$\mathbf{G}, g, y$

$$n \xleftarrow{\$} \mathbf{Z}_q, \ A = g^n$$
$$c = H(A, y)$$
$$s = n + c \cdot x \bmod q$$

Non-Interactive Zero-Knowledge (NIZK) Sigma protocol

Alice | **Bob**

I know x such that $g^x = y$

$\mathbf{G}, g, y$

$n \xleftarrow{\$} \mathbf{Z}_q,\ A = g^n$

$c = H(A, y)$

$s = n + c \cdot x \bmod q$ $\longrightarrow$ $\pi = (A, c, s)$

Non-Interactive Zero-Knowledge (NIZK) Sigma protocol

Alice | **Bob**

I know x such that $g^x = y$

$\mathbf{G}, g, y$

$$n \xleftarrow{\$} \mathbf{Z}_q,\ A = g^n$$
$$c = H(A, y)$$
$$s = n + c \cdot x \bmod q$$

$\xrightarrow{\pi = (A, c, s)}$

$$g^s \stackrel{?}{=} A \cdot y^c$$
$$c \stackrel{?}{=} H(A, y)$$

Non-Interactive Zero-Knowledge (NIZK) Sigma protocol

Alice

Bob

I know x such that $g^x = y$

$$\underbrace{\mathbf{G}, g, y}_{\text{Setup}}$$

$$\underbrace{n \xleftarrow{\$} \mathbf{Z}_q,\ A = g^n \quad c = H(A, y) \quad s = n + c \cdot x \bmod q}_{\text{Prove}}$$

$$\xrightarrow{\underbrace{\pi = (A, c, s)}_{\text{proof}}}$$

$$\underbrace{g^s \stackrel{?}{=} A \cdot y^c \quad c \stackrel{?}{=} H(A, y)}_{\text{Verify}}$$

zk-SNARK: Zero-Knowledge Succinct Non-interactive ARgument of Knowledge

"I have a *computationally sound*, *complete*, *zero-knowledge*, **succinct**, **non-interactive** proof that a statement is true and that I know a related secret".

Succinct

A proof is very short and easy to verify.

Non-interactive

No interaction between the prover and verifier for proof generation and verification (except the proof message).

ARgument of Knowledge

Honest verifier is convinced that a computationally bounded prover knows a secret information.

zk-SNARKs in a nutshell

Main ideas:

1. Reduce a general statement satisfiability to a polynomial equation satisfiability.
2. Use Schwartz–Zippel lemma to succinctly verify the polynomial equation with high probability.
3. Use homomorphic hiding cryptography to blindly verify the polynomial equation.
4. Make the protocol non-interactive.

Needs of groups for proof systems and SNARK

Statement

group $\mathbf{G}'$ of prime order over $\mathbb{F}_q$ / Hash function over base field $\mathbb{F}_q$

- `ed_25519` signature verification
$q = 2^{255} - 19$
- Hash function verification $y = H(x)$
H: Poseidon, Anemoi...

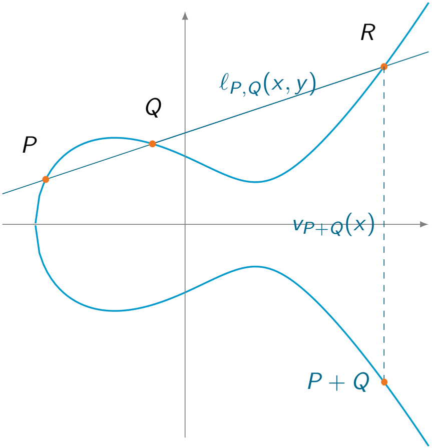
Proof

group $\mathbf{G}$ of prime order q over $\mathbb{F}_p$

Group where multiplication in the exponents is possible: given g^a, g^b, compute g^{ab} without knowing a, b
$\rightarrow \approx$ pairing-friendly curves

Outline

Elliptic curve $E/\mathbb{F}_p$: $y^2 = x^3 + ax + b$, $a, b \in \mathbb{F}_p$, $p \geq 5$, group law



- $E(\mathbb{F}_p)$ has an efficient group law $\to$ $\mathbf{G}_1$ (chord and tangent rule)
- $\#E(\mathbb{F}_p) = p + 1 - t$, trace t: $|t| \leq 2\sqrt{p}$
- large prime $q \mid p + 1 - t$ coprime to p
- $E(\mathbb{F}_p)[q] = \{P \in E(\mathbb{F}_p) : [q]P = \mathcal{O}\}$ has order q
- $E[q] \simeq \mathbf{Z}/q\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ (for crypto)
- only generic attacks against DLP on well-chosen genus 1 and genus 2 curves
- optimal parameter sizes

Pairing as a black box

$(\mathbf{G}_1, +), (\mathbf{G}_2, +), (\mathbf{G}_T, \cdot)$ three cyclic groups of large prime order q
Pairing: map $e : \mathbf{G}_1 \times \mathbf{G}_2 \to \mathbf{G}_T$

1. bilinear: $e(P_1 + P_2, Q) = e(P_1, Q) \cdot e(P_2, Q)$, $e(P, Q_1 + Q_2) = e(P, Q_1) \cdot e(P, Q_2)$
2. non-degenerate: $e(G_1, G_2) \neq 1$ for $\langle G_1 \rangle = \mathbf{G}_1$, $\langle G_2 \rangle = \mathbf{G}_2$
3. efficiently computable.

Most often used in practice: swap scalars, multiply in the exponents

$$e([a]P, [b]Q) = e([b]P, [a]Q) = e(P, Q)^{ab} \ .$$

Can multiply only once!

$\rightsquigarrow$ Many applications in asymmetric cryptography.

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \; : \; E(\mathbb{F}_p)[q] \times E(\mathbb{F}_{p^k})[q] \longrightarrow \mathbb{F}_{p^k}^*, \quad e([a]P, [b]Q) = e(P, Q)^{ab}$$

Cryptographic pairing

Modified Weil or Tate pairing on an elliptic curve

Discrete logarithm problem with one more dimension.

$$e \;:\; E(\mathbb{F}_p)[q] \times E(\mathbb{F}_{p^k})[q] \longrightarrow \mathbb{F}_{p^k}^*, \quad e([a]P,[b]Q) = e(P,Q)^{ab}$$

Attacks

- inversion of e : hard problem (exponential)
- discrete logarithm computation in $E(\mathbb{F}_p)$: hard problem (exponential, in $O(\sqrt{q})$)
- discrete logarithm computation in $\mathbb{F}_{p^k}^*$: **easier, subexponential** $\rightarrow$ take a large enough field

Finding pairing-friendly curves

Designed on purpose: otherwise $k \approx q$

Choose prime integer q, degree k then obtain p: inefficient curve

Design families: parameterized $p(x), q(x), t(x)$

- Complex Multiplication (CM) equation: $t^2 - 4p = -Dy^2$
- (Compute $t^2 - 4p$, get its square-free factorization)
- D discriminant, square-free (in number theory, if $D = 1, 2 \bmod 4$ then $D \leftarrow 4D$)

SEA: from coefficients to parameters

$E/\mathbb{F}_p \colon y^2 = x^3 + ax + b$

Schroof–Elkies–Atkin (SEA)

compute trace t

order $q = p + 1 - t$

iterate over a, b until q is prime

CM: from parameters to coefficients

base field $\mathbb{F}_p$, trace t, order q

CM equation $t^2 - 4p = -Dy^2$

compute Hilbert Class polynomial $H_D(X)$

compute a root j, $H_D(j) = 0 \bmod p$

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

$E/\mathbb{F}_p \colon y^2 = x^3 + \frac{3j}{j-1728}x + \frac{2j}{1728-j}$

First ordinary pairing-friendly curves: MNT [MNT01]

Miyaji, Nakabayashi, Takano, $\#E(\mathbb{F}_p) = p(x) + 1 - t(x) = q(x)$

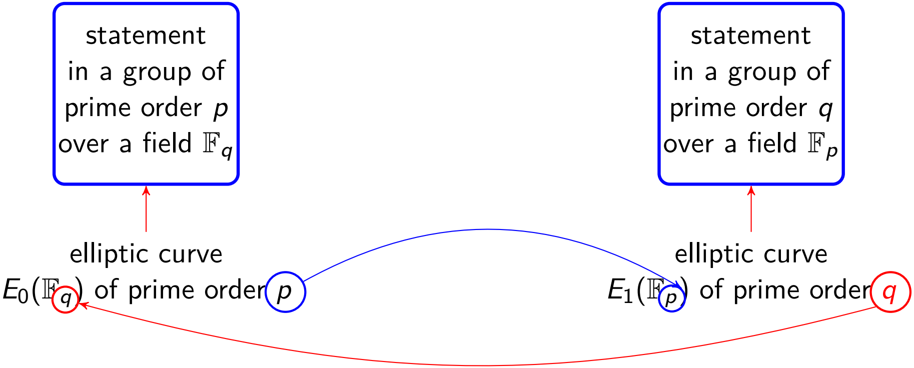
$$k = 3 \begin{cases} t(x) = -1 \pm 6x \\ q(x) = 12x^2 \mp 6x + 1 \\ p(x) = 12x^2 - 1 \\ Dy^2 = 12x^2 \pm 12x - 5 \end{cases}$$

$$k = 4 \begin{cases} t(x) = -x,\ \ x + 1 \\ q(x) = x^2 + 2x + 2,\ \ x^2 + 1 \\ p(x) = x^2 + x + 1 \\ Dy^2 = 3x^2 + 4x + 4 \end{cases}$$

$$k = 6 \begin{cases} t(x) = 1 \pm 2x \\ q(x) = 4x^2 \mp 2x + 1 \\ p(x) = 4x^2 + 1 \\ Dy^2 = 12x^2 - 4x + 3 \end{cases}$$

CODA [MS18]:
$k = 6$, 753 bits, $E_6 \approx 137$ bits of security, $D = -241873351932854907$, seed $u =$
`0xaa3a58eb20d1fec36e5e772ee6d3ff28c296465f137300399db8a5521e18d33581a262716214583d3b89820dd0c000`
$k = 4$, 753 bits, $E_4 \approx 113$ bits of security

Cycle of curves: unlimited chains of SNARKs [BCTV14]



MNT-4 and MNT-6 curves form a cycle

$k = 4$, MNT-4: $t = -x$, order $q = x^2 + 1$, field $p = x^2 + x + 1$

$k = 6$, MNT-6 ($x \leftrightarrow 2x$): $t' = 1 - x$, order $p = x^2 + x + 1$, field $q = x^2 + 1$

Unique known cycle of pairing-friendly curves. Impossibility results: [CCW19, BMUS23]

New constructions with higher dimensional curves [CCN24, CK24]

Very popular pairing-friendly curves: Barreto-Naehrig (BN) [BN06]

$$E_{BN}: \ y^2 = x^3 + b, \ p \equiv 1 \bmod 3, \ D = 3 \text{ (ordinary)}, \ j_E = 0$$

$$\begin{aligned} p &= 36u^4 + 36u^3 + 24u^2 + 6u + 1 \\ t &= 6u^2 + 1 \\ q &= p + 1 - t = 36u^4 + 36u^3 + 18u^2 + 6u + 1 \\ t^2 - 4p &= -3(6u^2 + 4u + 1)^2 \ \rightarrow \ \text{no CM method needed} \end{aligned}$$

Comes from the Aurifeuillean factorization of $\Phi_{12} : \Phi_{12}(6u^2) = q(u)q(-u)$

Security level	$\log_2 q$	$\log_2 p$	k	finite field	$\rho = \log p / \log q$
102	256	256	12	3072	1
123	384	384	12	4608	1
132	448	448	12	5376	1

Formerly BN-254 in Euthereum with seed `0x44e992b44a6909f1`

Barreto, Lynn, Scott curves [BLS03]

Any k, $3 \mid k$, $18 \nmid k$ possible
BLS12 ($k = 12$) becomes more and more popular, replacing BN curves

$$E_{\mathrm{BLS}} : \; y^2 = x^3 + b, \; p \equiv 1 \bmod 3, \; D = 3 \text{ (ordinary)}$$

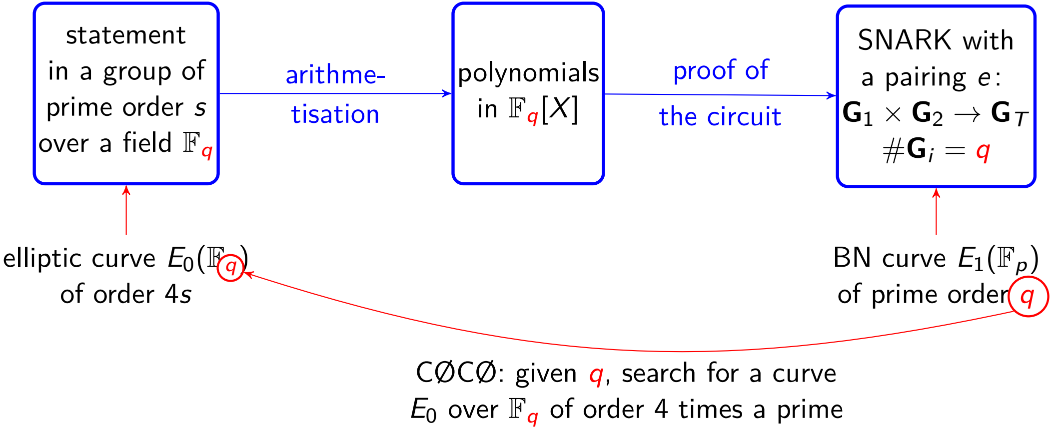
$$\begin{aligned} p &= (u-1)^2/3(u^4 - u^2 + 1) + u \\ t &= u + 1 \\ q &= (u^4 - u^2 + 1) = \Phi_{12}(u) \\ p + 1 - t &= \underbrace{(u-1)^2/3}_{\text{cofactor}}(u^4 - u^2 + 1) \end{aligned}$$

$$t^2 - 4p = -3y(u)^2 \; \rightarrow \; \text{no CM method needed}$$

BLS12-381 (Zcash [Bow17]) with seed `-0xd201000000010000`
BLS12-377 (Zexe [BCG+]) with seed `0x8508c00000000001`

Outline

CØCØ embedded curve: Kosba et al. construction [KZM+15]



Embedded SNARK-friendly curves

Usually a twist-secure elliptic curve in Montgomery or (twisted) Edwards form

Input: base field $\mathbb{F}_q$
Output: an embedded curve over $\mathbb{F}_q$ of order $4s$ or $8s$ with prime s
Procedure: Increment the curve coefficients until a suitable curve is found
(Nothing-up-my-sleeves strategy)

CØCØ [KZM+15] with BN-254a,
JubJub [ZCa21] or Bandersnatch [MSZ21] with BLS12-381,
first attempt to generalize Bandersnatch [SEH24]

Bandersnatch [MSZ21]

- Find an embedded elliptic curve E' over $\mathbb{F}_{q_{\text{BLS12-381}}}$ of trace t', above BLS12-381
- With a small discriminant D' in $t'^2 - 4q = -D'y'^2$ to allow faster scalar multiplication with GLV
- twist-secure: $q + 1 - t'$, $q + 1 + t'$ contain a large prime
- Use the CM method

$u = -\texttt{0xd201000000010000}$, $q = u^4 - u^2 + 1$ is prime (BLS12-381)
The trace t' can be any integer in the range $(-2\sqrt{q}; 2\sqrt{q})$
Idea: enumerate small D', get t', order s, twist order s' until s, s' contain a large prime

Bandersnatch curve: $D' = 2$ (i.e. $D' = -8$), $s = 2^2 \times p_{253}$, $s' = 2^7 \cdot 3^3 \times p_{244}$
Is it a *magical* curve? It is *too good to be true*?

Outline

More Bandersnatch curves

Extend the search space for discriminants D'
Rewrite the algorithm to enumerate the curves much faster

We get more embedded twist-secure curves with BLS12-381:

- $D = 2$, Bandersnatch
- $D = 1030258$, $r = 4p_{253}$, $r' = 2^3 \cdot 7p_{250}$
- $D = 1429201$, $r = 4p_{253}$, $r' = 2^8 \cdot 5p_{245}$
- $D = 1470074$, $r = 2^9 p_{246}$, $r' = 2^2 \cdot 3^4 \cdot 5p_{245}$
- $D = 1992138$, $r = 2^7 p_{248}$, $r' = 2^2 \cdot 3^2 \cdot 79p_{244}$
- $D = 7636102$, $r = 2^2 p_{253}$, $r' = 2^3 \cdot 3^2 \cdot 23p_{245}$
- $\ldots$

More embedded prime-order curves with BLS12-381:

- $D = 6673027$, r prime, $r' = c \cdot p_{234}$ (twist-secure)
- $D = 7321939$, r prime, $r' = c' \cdot p_{206}$

Imaginary Quadratic Number Field

Let $d > 0$ a square-free integer.

$$K = \mathbf{Q}[x]/(x^2 + d) \simeq \mathbf{Q}(\sqrt{-d})$$

is a imaginary quadratic number field whose maximal order is $\mathcal{O}_K = \mathbf{Z}[\tau]$ where

$$\tau = \begin{cases} \sqrt{-d} & \text{if } d \not\equiv 3 \bmod 4, \\ \frac{1+\sqrt{-d}}{2} & \text{if } d \equiv 3 \bmod 4. \end{cases}$$

The norm of an algebraic integer $a + b\tau$, $a, b \in \mathbf{Z}$ is

$$N_{K/\mathbf{Q}}(a + b\tau) = \begin{cases} \mathrm{Res}(a + bX, X^2 + d) = a^2 + db^2 \text{ if } d \equiv 1, 2 \bmod 4 \\ \mathrm{Res}(a + bX, X^2 - X + \frac{d+1}{4}) = a^2 + ab + \frac{d+1}{4}b^2 \text{ if } d \equiv 3 \bmod 4. \end{cases}$$

Solving norm equation

Given positive integer n, find $\eta \in \mathbf{Z}[\tau]$ of norm $n \to$ sometimes no solution

Example: $K = \mathbf{Q}(\sqrt{-5})$, $\tau = \sqrt{-5}$. Solve for $\pi = a + b\tau \in \mathcal{O}_K$, $N_{K/\mathbf{Q}}(\pi) = a^2 + 5b^2 = p$ prime

- ramified primes $p = 2, 5$
- inert primes 11, 13, 17, 19, 31, 37, 53, 59, 71, 73, 79, 97
- splitting primes 3, 7, 23, 43, 47, 67, 83 but no solution
- splitting primes having solutions: $29 = N(3 \pm 2\tau)$, $41 = N(6 \pm \tau)$, $61 = N(4 \pm 3\tau)$, $89 = N(3 \pm 4\tau)$

In average (over 10^5 p): 1/2 are split, 1/4 have a solution π, $p = N(\pi)$.

- $-d$ is a square in half the cases
- prime ideal $\mathfrak{p}$ above p is principal with $1/h(K)$ chance, $h(K) =$ Class Number then $\pi = a + b\tau$ exists, $N_{K/\mathbf{Q}}(\pi) = p$

Algorithm 1: EmbeddedCurve($q, D_{\min}, D_{\max}$)

Input: prime integer q, minimum and maximum values of $D > 0$

Output: A list of traces and discriminants of embedded elliptic curves for $\mathbb{F}_q$

$\mathcal{L} \leftarrow \{\}$

for D from $D_{\min}$ to $D_{\max}$ **do**

  if D is square-free and $-D$ is a square modulo q **then**

    $$s \leftarrow \begin{cases} \sqrt{-D} \bmod q & d \not\equiv 3 \bmod 4 \\ \frac{1+\sqrt{-D}}{2} \bmod q & d \equiv 3 \bmod 4 \end{cases}$$

    lift s in $\mathbf{Z}$

    $\pi \leftarrow a + bX$ the shortest non-zero element of the lattice $\mathbb{Z}\langle q, X - s\rangle$

    if π has norm q **then**

      $$(t', y') \leftarrow \begin{cases} (2a, b) \text{ if } d \equiv 3 \bmod 4 \\ (2a + b, b) \text{ otherwise} \end{cases}$$

      if $r = q + 1 - t'$, $r' = q + 1 + t'$ contain a large prime **then**

        $\mathcal{L} \leftarrow \mathcal{L} \cup \{(D, t', y')\}$

return $\mathcal{L}$

Atkin-Morain, ECPP, and the CM method [AM93]

- internal step in ECPP: find an elliptic curve over $\mathbf{Z}/n\mathbf{Z}$ of non-prime order of known factorization
- enumerate small D until a curve is found
- For each D, solve a norm equation $n = A^2 + DB^2$ in $\mathcal{O}_K$, $K = \mathbf{Q}[\sqrt{-D}]$
- the curve trace is $t' = 2A$, check order
- Do not compute $H_{-D}(X)$ each time, only when a good D is found

Estimated chance to solve the norm equation $n = N_{K/\mathbf{Q}}(\eta)$: $\frac{1}{2h(K)}$
$\implies$ try many D until a solution is found.
$h(K)$ grows with D.

Example with $D = 6673027$

$q = q_{\text{BLS12-381}} = u^4 - u^2 + 1$ where
$u = \texttt{-0xd201000000010000} = -(2^{63} + 2^{62} + 2^{60} + 2^{57} + 2^{48} + 2^{16})$
$D = 6673027 \equiv 3 \bmod 4,\ h(D) = 360$
$s \leftarrow \frac{1+\sqrt{-D}}{2} \bmod q$
2-dim reduction (rows) GaussReduce $\begin{bmatrix} q & 0 \\ -s & 1 \end{bmatrix}$

$$\begin{bmatrix} 1255592171035763907508018190807600384\,45 & 1482238992058657727428069813863950\,67 \\ -494589405381030502681645767067595900\,14 & 4175602985391319630541315724119583204\,35 \end{bmatrix}$$

1st row $\rightarrow (a, b)$ such that $a^2 + ab + \frac{D+1}{4} b^2 = q$
$4q = (2a+b)^2 + Db^2$, embedded curve trace $t = 2a + b,\ y = b$
prime order $s = q + 1 - t = \frac{(t-2)^2 + Dy^2}{4}$,
twist order $q + 1 + t = 3^2 \cdot 19^2 \cdot 953 \cdot p_{234}$
PARI-GP: $j(E) \bmod q,\ E\colon y^2 = x^3 - 3x + b_q$,
$b_q = 10908001762325402974914188089519822993112853370962247355940024813778856917972$

Related work: plain/hybrid cycles of curves

Plain cycles: 2 plain prime-order elliptic curves (no pairing)

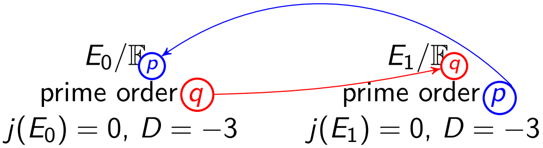
secp256k1/secq256k1, HALO: Tweedledum/tweedledee, HALO2: Pallas-Vesta – Pasta

1. start from any prime-order elliptic curve of small-enough discriminant D
2. swap scalar field order q and base field order p to get the 2nd curve parameters
3. use the CM method on (q, p, D) to get the 2nd curve coefficients

D small required, SafeCurve criterion $|D| \geq 2^{110}$ never satisfied

Hybrid cycles: a plain curve and a BN pairing-friendly curve, both prime order

BN254-Grumpkin, BN382-plain, Pluto (BN446) - Eris. Prime-order pairing-friendly curves are very rare, no better solution than BN known



ed_25519 as an embedded curve

$q = 2^{255} - 19$

- Curve25519 in Montgomery form

$E' \colon y^2 = x^3 + 48662x^2 + x$

- Ed25519 in twisted Edwards form

$E' \colon -x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2$

$E'(\mathbb{F}_q)$ of order $8r$, r prime

Prime p, curve $E/\mathbb{F}_p$
of prime order q

- $D = 65012179$
- $D = 103953715$

E' embedded curve of E

Outline

Families of embedded curves with BLS12

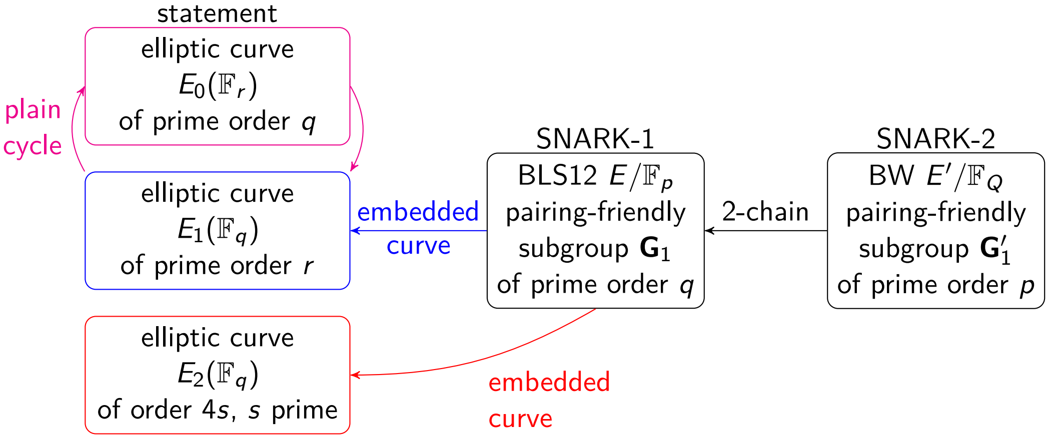
Sanso's first work [SEH24]. Idea: design families of embedded curves, whose parameters are given by polynomials, like families of pairing-friendly curves. Always the same story:

1. Do it for BLS12 curves: easy doing! (fastest optimal ate pairing computation, easiest cofactor clearing, subgroup membership testing, hashing, scalar multiplication with high-dimension GLV...)
2. generalize to other pairing-friendly curves: problems arise

With previous section point of view: Solve a norm equation for $q = x^4 - x^2 + 1$, $D = 3$
Obvious solution: $q = ((2x^2 - 1)^2 + 3(1)^2)/4$
embedded curve trace: $t' = 2x^2 - 1$,
embedded curve order: $s = ((t' - 2)^2 + 3(1)^2)/4 = x^4 - 3x^2 + 3$ irreducible *and* generating primes.

$$\implies \text{family!}$$

Generalization: Families of embedded curves for BLS12



BLS12 with embedded curves

seed	L	equation $E_{BLS}/\mathbb{F}_p$	p (bits)	q (bits)	embedded curve equation $E_{1,2}/\mathbb{F}_q$	plain cycle curve equation $E_0/\mathbb{F}_r$
`0xffff007fda000001`	25	$y^2 = x^3 + 1$	383	256	$E_1 \colon y^2 = x^3 + 19$	$y^2 = x^3 + 7$
$2^{64} - 2^{48} + 2^{39} - 2^{29} - 2^{27} + 2^{25} + 1$					$E_2 \colon y^2 = x^3 + 17$	
`0xfc3ec00400000001`	34	$y^2 = x^3 + 1$	383	256	$E_1 \colon y^2 = x^3 + 23$	$y^2 = x^3 + 29$
$2^{64} - 2^{58} + 2^{54} - 2^{48} - 2^{46} + 2^{34} + 1$					$E_2 \colon y^2 = x^3 + 29$	
`-0xef000ffefdffffff`	25	$y^2 = x^3 + 1$	382	256	$E_1 \colon y^2 = x^3 + 11$	$y^2 = x^3 + 17$
$-2^{64} + 2^{60} + 2^{56} - 2^{44} + 2^{32} + 2^{25} + 1$					$E_2 \colon y^2 = x^3 + 17$	
`0xdf07fffdfc000001`	26	$y^2 = x^3 + 1$	382	256	$E_1 \colon y^2 = x^3 + 11$	$y^2 = x^3 + 7$
$2^{64} - 2^{61} - 2^{56} + 2^{51} - 2^{33} - 2^{26} + 1$					$E_2 \colon y^2 = x^3 + 23$	

Some technicalities

- $q(u) = u^4 - u^2 + 1 = \Phi_{12}(u)$ (BLS12) [SEH24]
  $q(u) = (u^6 + 37u^3 + 343)/343$ (KSS18), with Sagemath code at [Hop20]
  $q(u) = (u^8 + 48u^4 + 625)/61250$ (KSS16)
- Solve for $t'(u), y'(u)$ in $4q(u) = t'(u)^2 + Dy'(u)^2$

Solution:

- Combine Dai–Lin–Zhao–Zhou [DLZZ23] with Smith [Smi15, §4]
- BLS12 [SEH24] $t' = 2u^2 - 1$, $y' = 1$
- KSS16 $t' = (31(u/5)^4 + 1)/7$, $y' = (-17(u/5)^4 - 1)/14$
- KSS18 $t' = -20(u/7)^3 - 1$, $y' = -18(u/7)^3 - 1$
- Consider the quadratic twists, 3rd and 6-th twists ($D = 3$), 4-th twists ($D = 1$)

Our Algorithm

E has endomorphism ϕ, char. poly $\chi(X) = X^2 - t_\phi X + \deg_\phi$
$t_\phi^2 - 4\deg_\phi = -Dn^2$ and $-D$ matches E's in $t^2 - 4p = -Dy^2$

1. $\lambda(x) \leftarrow$ a root of $\chi(X)$ mod $q(x)$
   e.g. if $\chi(X) = X^2 + D$, $\lambda(x) = \sqrt{-D} = (t(x) - 2)/y(x) \bmod q(x)$
2. $U(x), V(x) \leftarrow \text{half-gcd}(q(x), \lambda(x))$
3. with Smith's technique [Smi15, §4], reduce the matrix
   $\begin{bmatrix} U(x) & -V(x) \\ -t_\phi U(x) + \deg_\phi V(x) & U(x) \end{bmatrix}$ whose determinant is

   $\det = U^2 - t_\phi UV + \deg_\phi V^2 = \text{Res}(\chi(X), U - VX)$
   to obtain a short row $(a_0(x), a_1(x))$
4. $(t', y') = (a_0, a_1)$ if $D = 1, 2 \bmod 4$,
   $(t', y') = (2a_0 - a_1, a_1)$ if $D = 3 \bmod 4$.

Example with KSS16

$E_{\mathrm{KSS16}}: y'^2 = x'^3 + ax'$, $j = 1728$, $D = 1$, $\chi = X^2 + 1$

1. $q(x) = (x^8 + 48x^4 + 625)/61250$, $\lambda_\phi = (x^4 + 24)/7 \bmod q(x)$
2. $U, V = (1, -\lambda_\phi) = (1, -(x^4 + 24)/7)$ (no half-gcd needed)
3. $\det \begin{bmatrix} \boldsymbol{b}_1 \\ \boldsymbol{b}_2 \end{bmatrix} = \det \begin{bmatrix} 1 & -(x^4+24)/7 \\ (x^4+24)/7 & 1 \end{bmatrix} = 1250 q(x)$
4. find integers $(i, j) \bmod 1250 = 2 \cdot 5^4$ such that the denominator simplifies in $(i\boldsymbol{b}_1 + j\boldsymbol{b}_2)/1250 = (i + j(x^4 + 24)/7, i(x^4 + 24)/7 - j)/1250$
5. $x \equiv 25, 45 \bmod 70$ by construction (KSS16) $\implies x \equiv 5 \bmod 10 \implies 5^4 \mid x^4$.
   Write $x = 10x_0 + 5 = 5(2x_0 + 1)) \implies$ it simplifies to $i + 807j \equiv 0 \bmod 2 \cdot 5^4$.
6. enumerate over (i, j) and keep those such that $(a_0, a_1) = (i\boldsymbol{b}_1 + j\boldsymbol{b}_2)$ satisfies $a_0^2 + a_1^2 = q(x)$

We obtain:

$$\begin{aligned} (i, j) =& (31, 17), \\ (t', y') =& (31\boldsymbol{b}_1 + 17\boldsymbol{b}_2)/1250 = ((17(x/5)^4 + 1)/14, (31(x/5)^4 + 1)/14)\ . \end{aligned}$$

Embedded curves for KSS16

Parameters (t', y') such that $q = (t'^2 + y'^2)/4$ with $D = 1$.

	(t', y') s.t. $q = (t'^2 + 4y'^2)/4$	$s = q + 1 - t'$	family
t', y'	$(31(u/5)^4 + 1)/7, (-17(u/5)^4 - 1)/7$	$(u^8 - 386u^4 + 5^5 \cdot 17)/61250$	(yes, c=2)
$-t', y'$	$(-31(u/5)^4 - 1)/7, (-17(u/5)^4 - 1)/7$	$(u^8 + 482u^4 + 5^4 \cdot 113)/61250$	(yes, c=2)
y', t'	$(-17(u/5)^4 - 1)/7, (31(u/5)^4 + 1)/7$	$(u^8 + 286u^4 + 5^4 \cdot 113)/61250$	(yes, c=32)
$-y', t'$	$(17(u/5)^4 + 1)/7, (31(u/5)^4 + 1)/7$	$(u^8 - 190u^4 + 5^5 \cdot 17)/61250$	(yes, c=20)

Valid seed: $2^{34} - 2^{32} + 2^{30} + 2^{26} - 2^5 - 2^3 - 1$=`0x343fffd7` (row 2), 254-bit order

Conclusion

Inspirations from 80's and 90's papers with modern software on nowadays'CPU solve our problems!

- embedded curves as isolated points (Bandersnatch) are always possible to find with large enough D
- for SNARK, additional constraint $2^L \mid s-1$, larger search space $\rightarrow$ larger D $\rightarrow$ much longer time
- families require to change the seed $\rightarrow$ not always possible to replace BLS12-381
- next step: combine embedded families with outer curves families like Geppetto, BW6-751?
- still unknown: embedded and *pairing-friendly* elliptic curves
  (only known construction: starting from the pairing-friendly curve)
- preprint at https://inria.hal.science/hal-04750802

Thank you for your attention.

References I

A. O. L. Atkin and F. Morain.
Elliptic curves and primality proving.
Mathematics of Computation, 61(203):29–68, July 1993.

Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu.
Zexe: Enabling decentralized private computation.
ePrint:2018/962.

Eli Ben-Sasson, Alessandro Chiesa, Eran Tromer, and Madars Virza.
Scalable zero knowledge via cycles of elliptic curves.
In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 276–294. Springer, Berlin, Heidelberg, August 2014.

Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott.
Constructing elliptic curves with prescribed embedding degrees.
In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, *SCN 02*, volume 2576 of *LNCS*, pages 257–267. Springer, Berlin, Heidelberg, September 2003.

Marta Bellés-Muñoz, Jorge Jiménez Urroz, and Javier Silva.
Revisiting cycles of pairing-friendly elliptic curves.
In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part II*, volume 14082 of *LNCS*, pages 3–37. Springer, Cham, August 2023.

Paulo S. L. M. Barreto and Michael Naehrig.
Pairing-friendly elliptic curves of prime order.
In Bart Preneel and Stafford Tavares, editors, *SAC 2005*, volume 3897 of *LNCS*, pages 319–331. Springer, Berlin, Heidelberg, August 2006.

References II

Sean Bowe.
BLS12-381: New zk-SNARK elliptic curve construction.
Zcash blog, March 11 2017.
https://electriccoin.co/blog/new-snark-curve/.

Maria Corte-Real Santos, Craig Costello, and Michael Naehrig.
On cycles of pairing-friendly abelian varieties.
In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO'2024*, Santa Barbara, CA, August 2024. IACR, Springer-Verlag.
to appear, ePrint:2024/869.

Alessandro Chiesa, Lynn Chua, and Matthew Weidner.
On cycles of pairing-friendly elliptic curves.
SIAM Journal on Applied Algebra and Geometry, 3(2):175–192, 2019.

Craig Costello, Cédric Fournet, Jon Howell, Markulf Kohlweiss, Benjamin Kreuter, Michael Naehrig, Bryan Parno, and Samee Zahur.
Geppetto: Versatile verifiable computation.
In *2015 IEEE Symposium on Security and Privacy*, pages 253–270. IEEE Computer Society Press, May 2015.

Craig Costello and Gaurish Korpal.
Lollipops of pairing-friendly elliptic curves for composition of proof systems.
ePrint 2024/1627, 2024.

Yu Dai, Kaizhan Lin, Chang-An Zhao, and Zijian Zhou.
Fast subgroup membership testings for $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ on pairing-friendly curves.
Designs, Codes and Cryptography, 91(10):3141–3166, Oct 2023.
ePrint:2022/348.

References III

Daira Hopwood.
Halo optimizations and constructing graphs of elliptic curves.
https://github.com/daira/halographs/, 2020.

Ahmed Kosba, Zhichao Zhao, Andrew Miller, Yi Qian, Hubert Chan, Charalampos Papamanthou, Rafael Pass, abhi shelat, and Elaine Shi.
C∅c∅: A framework for building composable zero-knowledge proofs.
Cryptology ePrint Archive, Report 2015/1093, 2015.

A. Miyaji, M. Nakabayashi, and S. Takano.
New explicit conditions of elliptic curve traces for FR-reduction.
IEICE Transactions on Fundamentals, E84-A(5):1234–1243, 2001.
https://dspace.jaist.ac.jp/dspace/bitstream/10119/4432/1/73-48.pdf.

Izaak Meckler and Evan Shapiro.
Coda: Decentralized cryptocurrency at scale.
O(1) Labs whitepaper, 2018.
https://cdn.codaprotocol.com/v2/static/coda-whitepaper-05-10-2018-0.pdf https://coinlist.co/build/coda/pages/MNT4753.

Simon Masson, Antonio Sanso, and Zhenfei Zhang.
Bandersnatch: a fast elliptic curve built over the BLS12-381 scalar field.
Cryptology ePrint Archive, Report 2021/1152, 2021.

Antonio Sanso and Youssef El Housni.
Families of prime-order endomorphism-equipped embedded curves on pairing-friendly curves.
ePrint:2023/1662, 2024.

References IV

Benjamin Smith.
Easy scalar decompositions for efficient scalar multiplication on elliptic curves and genus 2 Jacobians.
Contemporary mathematics, 637:15, May 2015.
HAL:00874925.

ZCash.
What is jubjub?
https://z.cash/technology/jubjub/, 2021.