Families of Fast Elliptic Curves from \mathbb{Q} -curves

Benjamin Smith (INRIA & École polytechnique)

nain

$\mathcal{E}: y^2 = x^3 + Ax + B$ an ordinary elliptic curve over \mathbb{F}_p , \mathbb{F}_{p^2}

$\mathbb{Z}/N\mathbb{Z} \cong \mathcal{G} \subset \mathcal{E}$ a prime-order subgroup

an endomorphism

 $\psi: \mathcal{E} \to \mathcal{E}$

Smith. Families of Fast Elliptic Curves from Q-curves

How do we choose \mathcal{E}/\mathbb{F}_q ?

1. Strong group structure: *almost-prime order*, *secure quadratic twist order*

- 2. Fast cryptographic operations: \oplus , [2], and [m]
- 3. Fast \mathbb{F}_q -arithmetic: eg. $q = 2^n e$ with tiny e

We want *all three* of these properties *at once* but in practice, the 3 properties are not orthogonal.



 $\mathcal{G} \cong \mathbb{Z}/N\mathbb{Z}$ is embedded in \mathcal{E} , which has a much richer structure than $\mathbb{Z}/N\mathbb{Z}$: $\operatorname{End}(\mathcal{G}) = \mathbb{Z}/N\mathbb{Z}$ but $\operatorname{End}(\mathcal{E}) \supset \mathbb{Z}[\pi_a]$, where $\pi_a: (x, y) \mapsto (x^q, y^q)$ is Frobenius. If $\psi \in \text{End}(\mathcal{E})$ satisfies $\psi(\mathcal{G}) \subset \mathcal{G}$ (and this happens pretty much all the time): $\psi(P) = [\lambda_{\psi}]P$ for all $P \in \mathcal{G}$ We call λ_{ψ} the *eigenvalue* of ψ on \mathcal{G} .



Suppose ψ has eigenvalue $-N/2 < \lambda_{\psi} < N/2$ with $|\lambda_{\psi}| > \sqrt{N}$ (ie, not unusually small) Fundamental cryptographic operation:

 $P \mapsto [m]P = P \oplus \cdots \oplus P$ (*m* times).

If $m \equiv a + b\lambda_{\psi} \pmod{N}$ then $[m]P = [a]P \oplus [b]\psi(P) \qquad \forall P \in \mathcal{G}$.

LHS costs $\log_2 m$ double/add iterations; RHS costs $\log_2 \max(|a|, |b|)$ double/add iters + cost(ψ).

RHS (multiexponentiation) wins if we can

1. Find *a* and *b* significantly shorter than *m*;

OK: $|\lambda_{\psi}| > \sqrt{N} \implies \log_2 \max(|a|, |b|) \le \frac{1}{2} \log_2 N + \epsilon$

2. Evaluate ψ fast (time/space < a few doubles)

Gallant–Lambert–Vanstone (GLV), CRYPTO 2001: Start with an explicit CM curve $/\overline{\mathbb{Q}}$, reduce mod p.

Let
$$p \equiv 1 \pmod{4}$$
; let $i = \sqrt{-1} \in \mathbb{F}_p$. Then the curves $\mathcal{E}_a : y^2 = x^3 + ax$

have explicit CM by $\mathbb{Z}[i]$: an extremely efficient endomorphism

$$\psi: (x, y) \longmapsto (-x, \sqrt{-1}y).$$

Big $\lambda_{\psi} \equiv \sqrt{-1} \pmod{N} \implies$ half-length multiscalars.

An example of what can go wrong:

The 256-bit prime $p = 2^{255} - 19$ offers very fast \mathbb{F}_p -arithmetic. Want *N* to have at least 254 bits, and a secure quadratic twist

The
$$\mathbb{F}_{p}$$
-isomorphism classes of \mathcal{E}_{a} : $y^{2} = x^{3} + ax$
are represented by $a = 1, 2, 4, 8$ in \mathbb{F}_{p} .

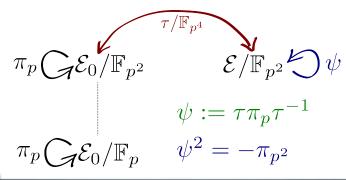
Largest prime
$$N \mid \#\mathcal{E}_a(\mathbb{F}_p) = \begin{cases} 199b & \text{if } a = 1 \\ 175b & \text{if } a = 4 \\ 239b & \text{if } a = 2 \\ 173b & \text{if } a = 8 \end{cases}$$
 quad twist pair

Limitation: Very few other CM curves with fast ψ (because there are very few tiny CM discriminants)
Problem: To use GLV endomorphisms, we need to vary p. (Solution: forget endomorphisms, use fast p eg. Curve25519)

Galbraith-Lin-Scott (GLS), EUROCRYPT 2009

GLV: Not enough curves $/\mathbb{F}_p$ have low-degree endomorphisms **GLS**: But O(p) curves over \mathbb{F}_{p^2} have degree-p endomorphisms p-th powering on \mathbb{F}_{p^2} nearly free: $(x_0 + x_1\sqrt{\Delta})^p = x_0 - x_1\sqrt{\Delta}$.

Original recipe: Take any curve / \mathbb{F}_p , extend to \mathbb{F}_{p^2} , twist π_p .





Original GLS (with twisting isomorphism τ/\mathbb{F}_{p^4}):

$$\psi: \mathcal{E} \xrightarrow{\tau} \mathcal{E}_0 \xrightarrow{\pi_p} \mathcal{E}_0 \xrightarrow{\tau^{-1}} \mathcal{E}$$

Simplified: push π_p to the right, then $\psi = \pi_p \circ \phi$:

$$\mathcal{E} : y^{2} = x^{3} + Ax + B$$

$$1 \downarrow \phi :=^{(p)_{T} - 1} \circ \tau \qquad \mathbb{F}_{p^{2}} \text{-iso. } \phi : \text{special } A, B$$

$$(p)\mathcal{E} : y^{2} = x^{3} + A^{p}x + B^{p}$$

$$p \downarrow \pi_{p} \qquad \pi_{p} : (x, y) \mapsto (x^{p}, y^{p})$$

$$\mathcal{E} : y^{2} = x^{3} + Ax + B$$
Existence of $\phi \implies$ weak subfield twist.

Smith. Families of Fast Elliptic Curves from Q-curves

Twist-insecurity is a pity: GLS ψ are *fast*.

Example: Take any A, B in \mathbb{F}_p for any $p \equiv 5 \pmod{8}$ (so $\sqrt{-1}$ in \mathbb{F}_p , $(-1)^{1/4}$ in \mathbb{F}_{p^2} nonsquare).

Take any A, B, in \mathbb{F}_p : $\mathcal{E}/\mathbb{F}_{p^2}: y^2 = x^3 + \sqrt{-1}Ax + (-1)^{3/4}B$ Conjugate curve: ${}^{(p)}\mathcal{E}/\mathbb{F}_{p^2}: y^2 = x^3 + \sqrt{-1}Ax - (-1)^{3/4}B$

Isomorphism $\phi: (x, y) \mapsto (-x, \sqrt{-1}y)$ composed with π_p gives

$$\psi:(x,y)\longmapsto(-x^p,\sqrt{-1}y^p).$$

Good scalar decompositions: $\lambda_{\psi} \equiv \sqrt{-1} \pmod{N}$.

So what do we do in this paper? Aim: flexibility of GLS, without weak twists. Twist-insecurity in GLS comes from deg $\phi = 1$ in

$$\psi: \mathcal{E} \xrightarrow{\phi} {}^{(p)} \mathcal{E} \xrightarrow{\pi_p} \mathcal{E}$$

Solution: relax deg ϕ . Let ϕ be a *d*-isogeny, tiny *d*:

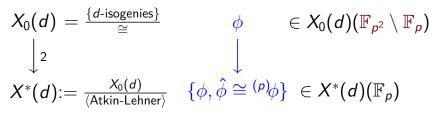
$$\psi: \mathcal{E} \xrightarrow[d]{\phi} {}^{(p)}\!\mathcal{E} \xrightarrow[p]{\pi_p} \mathcal{E}$$

Yields O(p) curves over \mathbb{F}_{p^2} , but they're not subfield twists, so they can be twist-secure.

The new construction, for d tiny (and prime):

$$\psi: \mathcal{E} \xrightarrow[d]{\phi} {}^{(p)}\!\mathcal{E} \xrightarrow[p]{\pi_p} \mathcal{E}$$

How do we find $\mathcal{E}/\mathbb{F}_{p^2}$ with $\phi: \mathcal{E} \to {}^{(p)}\mathcal{E}$? Use modular curves.





Smith. Families of Fast Elliptic Curves from Q-curves

A Q-curve of degree *d* is a non-CM $\widetilde{\mathcal{E}}/\mathbb{Q}(\sqrt{\Delta})$ with a *d*-isogeny $\widetilde{\phi} : \widetilde{\mathcal{E}} \to {}^{\mathscr{C}}\widetilde{\mathcal{E}}$...the number field analogue of what we want!

 \mathbb{Q} -curves are important in modern number theory, so we have lots of theorems, tables, universal families...

Key fact: $X_0(d) \cong \mathbb{P}^1$ for tiny d $\implies \phi \in X_0(\mathbb{F}_{p^2})$ lifts trivially to $\tilde{\phi} \in X_0(\mathbb{Q}(\sqrt{\Delta}))$ \implies the curves we want lift trivially to \mathbb{Q} -curves

Converse: find all possible $\phi : \mathcal{E} \to {}^{(p)}\mathcal{E}$ by reducing (universal) 1-parameter families of \mathbb{Q} -curves mod p

Example: Hasegawa gives a universal family of degree-2 \mathbb{Q} -curves. Reduce mod p, then compose with π_p ...

Take any
$$\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{\Delta})$$
. For every $t \in \mathbb{F}_p$, the curve
 $\mathcal{E}_t/\mathbb{F}_{p^2} : y^2 = x^3 - 6(5 - 3t\sqrt{\Delta})x + 8(7 - 9t\sqrt{\Delta})$
has an efficient (faster than doubling) endomorphism
 $\psi : (x, y) \longmapsto \left(f(x^p), \frac{y^p f'(x^p)}{\sqrt{-2}}\right)$ where $f(x^p) = \frac{-x^p}{2} - \frac{9(1 - t\sqrt{\Delta})}{(x^p - 4)}$
We have $\psi^2 = [\pm 2]\pi = 50$, $\lambda = t/\pm 2$ on cryptographic G

We have $\psi^2 = [\pm 2]\pi_{
ho^2}$, so $\lambda_\psi = \sqrt{\pm 2}$ on cryptographic ${\cal G}$.

Lots of choice: $p - \epsilon$ different *j*-invariants in \mathbb{F}_{p^2} Can find secure & twist-secure group orders



Take $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-1})$ where $p = 2^{127} - 1$ (Mersenne prime).

In the previous family, we find the 254-bit curve

 $\mathcal{E}_{9245}/\mathbb{F}_{p^2}$: $y^2 = x^3 - 30(1 - 5547\sqrt{-1})x + 8(7 - 83205\sqrt{-1})$

Looking at the curve and its twist:

 $\mathcal{E}_{9245}(\mathbb{F}_{p^2})\cong \mathbb{Z}/(2N)\mathbb{Z}$ and $\mathcal{E}'_{9245}(\mathbb{F}_{p^2})\cong \mathbb{Z}/(2N')\mathbb{Z}$

where N and N' are 253-bit primes.

On either curve, **253**-bit scalar multiplications $P \mapsto [m]P$ \mapsto **127**-bit multiexponentiations $P \mapsto [a]P \oplus [b]\psi(P)$ Secure group, fast scalar multiplication, fast field



More curves and endomorphisms

 $g(X_0(d)) = 0 \implies$ family of degree-dp endomorphisms

Applying the new construction, for any *p*:

- d = 1: (degenerate case) Twist-insecure GLS curves
- d = 2: Almost-prime-order curves + twists (see example)
- d = 3: Prime-order twist-secure curves Hasegawa: one-parameter universal curve family
- d = 5: Prime-order twist-prime-order curves Hasegawa \implies one-parameter family for fixed Δ
- $d \ge 7$: Slower prime-order twist-prime-order curves

For real applications: d = 2 should do.

