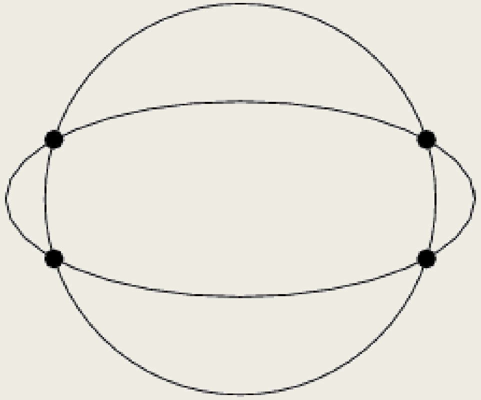
ELLIPTIC CURVES IN CRYPTOGRAPHY

Youssef El Housni
EY

Summary

- *Pre- Big Bang: Circles and ellipses…*
- *Post- Big Bang:* The mathematical foundations of elliptic curves
- *Biodiversity:* Elliptic curves *species*
- *Homo genus:* Elliptic curves in cryptography
- *Fire control:* Pairings in cryptography

Pre- Big Bang



Apollonius of Perga (ca. 262–190 BCE)
Isaac Newton 1669
Leonard Euler 1773
Colin McLaurin 1742
Adrien-Marie Legendre 1786 +
Niels Henrik Abel & Carl Jacobi 1825 +
Gauss 30y before (not published)

Circle

Equation : $x^2 + y^2 = r^2$ or $\begin{cases} x = r.\cos(\theta) \\ y = r.\sin(\theta) \end{cases}$

Area : πr^2

Circumference : $2\pi r$

Ellipse

Equation : $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ or $\begin{cases} x = a.\cos(\theta) \\ y = b.\sin(\theta) \end{cases}$

Area : πab

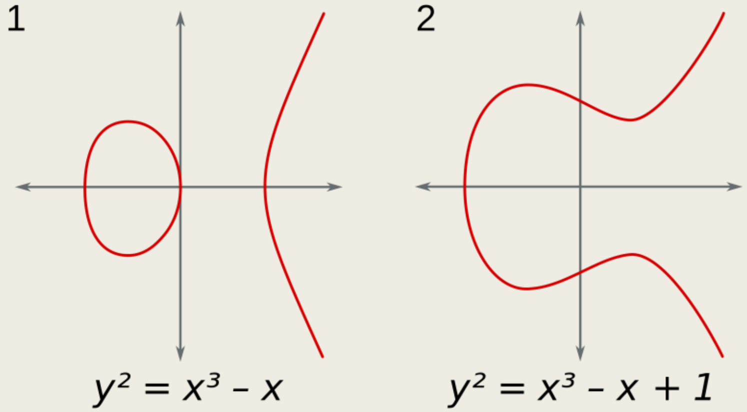
Circumference : $4a \int_0^{\frac{\pi}{2}} \sqrt{1 - k^2 sin^2(\theta)} d\theta$

where $k = 1 - \frac{b^2}{a^2}$

-- Studying the inverse of elliptic integrals leads to some doubly periodic functions which came to be known as elliptic functions (let's call them ℘(z) in the sequel, because ℘ looks nice). Furthermore, all the derivatives are doubly periodic with the same periods and satisfy a cubic differential equation.

- Setting x=℘ (z) and y=℘'(z) gives a parameterization of the cubic curve known today as an elliptic curve.

Big Bang



Short Weierstass elliptic curve E / K (where $char(K) \neq 2,3$)

$y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$

Elliptic curves over K are isomorphic to E

$\phi : E' \to E$ where $\phi(x, y) = (u^{-2}x, u^{-3}y)$ for some $u \in K^*$

The class of isomorphisms (and twists) is defined by the j-invariant :

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

Post- Big Bang

We refine the definition of an elliptic curve over K $(char(K) \neq 2,3)$ as follows:

$$\{(x,y) \in K^2 \mid y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0\} \cup \{O\}$$

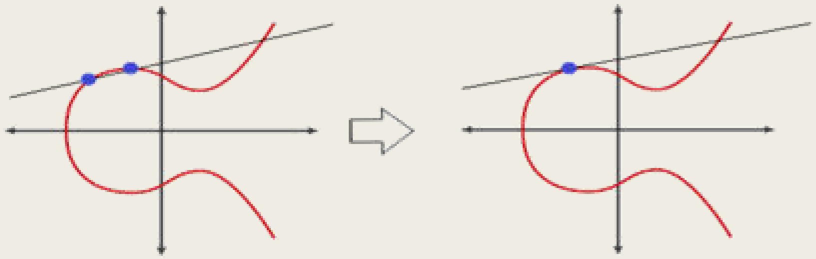
With 0 the point at ∞ (projective geometry). We can define a group over elliptic curves. Specifically:

- the elements of the group are the points of an elliptic curve,
- the **identity element** is the point O,
- the **inverse** of a point P is the one symmetric about the x-axis,
- addition is given by the following rule: **given 3 aligned, non-zero points P, Q and R, their sum $\boldsymbol{P+Q+R=0}$.**

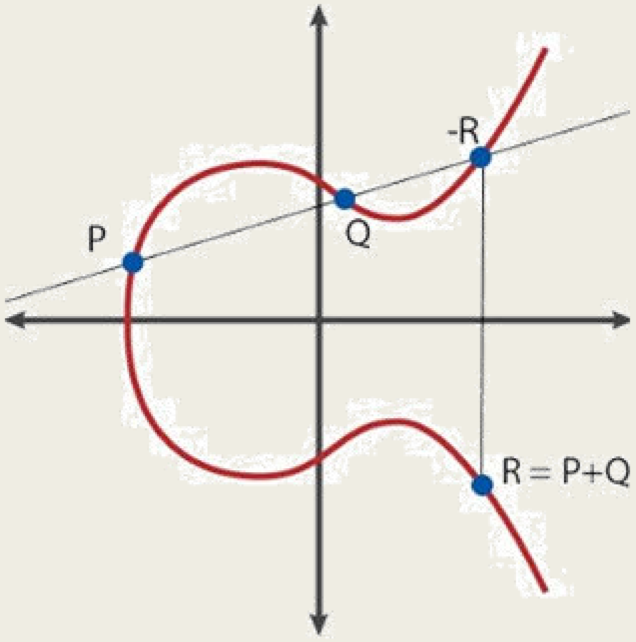
Note that with the last rule, we only require three aligned points without respect to order. This means that, if P , Q and R are aligned, then $P + (Q + R) = Q + (P + R) = R + (P + Q) = \cdots = 0$. Thisway, wehaveintuitivelyproved that the **addition** operator is associative and commutative: We are in an **abelian group**.

But how do we actually compute the sum of two arbitrary points?

Post- Big Bang



- **What if** $P = 0$ **or** $Q=0$**?**
  We can't draw any line (0 is not on the xy-plane). But given that we have defined 0 as the identity element, $P + 0 = P \ \forall P$.
- **What if** $P = -Q$**?**
  The line going through the two points is vertical, thus does not intersect the curve in a third point. But P is the inverse of Q, then we have $P + Q = P + (-P) = 0$.
- **What if** $P = Q$**?** There are an infinite number of lines passing through the point. We take the line tangent to the curve, why? consider $Q' \neq P$, as Q' tends towards P the line passing through P and Q' becomes tangent to the curve.
- **What if** $P \neq Q$**, but there is no third point** R**?**
  We are in a case very similar to the previous one. In fact, we are in the case where the line passing through P and Q is tangent to the curve. Let us assume that P is the tangency point, then $P + Q = -P$. If Q were the tangency point, then $P + Q = -Q$.



Geometric addition

Post- Big Bang

Elliptic curve: $y^2 = x^3 + ax + b$

Line: $y = mx + n$

where: $m = \frac{y_P - y_Q}{x_P - x_Q}$ and $n = y_P - mx_P = y_Q - mx_Q$

or $m = \frac{3x_P^2 + a}{2y_P}$ and $n = y_P - mx_P$

Intersection: $x^3 - m^2x^2 + (a - 2m^2x_P - 2y_P)x + (b + 2y_Px_P - y_P^2 - mx_P^2) = 0$

→ Vieta's formulae to the rescue:

If x_n are roots of $P(x) = \sum p_i x^i$ then $\sum x_i = -\frac{p_{n-1}}{p_n}$. Thus, $x_P + x_Q + x_R = m^2$

$char(K)$	$Condition$	m	$Coordinates\ of\ P + Q$
$\neq 2,3$	$x_P \neq x_Q$	$\frac{y_P - y_Q}{x_P - x_Q}$	$x = m^2 - x_P - x_Q$ $y = -m(x - x_P) - y_P$
$\neq 2,3$	$x_P = x_Q$	$\frac{3x_P^2 + a}{2y_P}$	$x = m2 - 2xP$ $y = -m(x - xP) - yP$

Geometric addition

Post- Big Bang

Other than addition, we can define another operation: scalar multiplication, that is:

$$nP = \underbrace{P + P + \dots + P}_{n\,times}$$

where n is a natural number. $O(2^k)$

It may seem that nomputing nP requires n additions. However there is a fast algorithm called **double and add.**

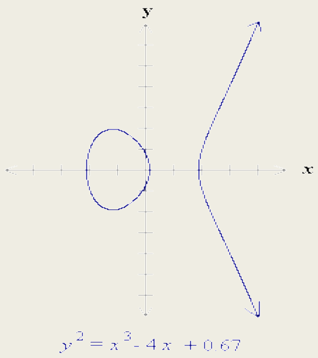
e.g. Take $n = 151$, its binary representation is 100101112 and can be turned into a sum of powers of two: $151 = 2^7 + 2^4 + 2^2 + 2^1 + 2^0$ In view of this, we can write:

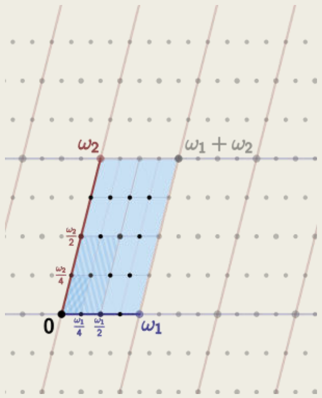
$$151P = 2^7P + 2^4P + 2^2P + 2^1P + 2^0P$$

Other algorithms:

- Double-and-add always (side-channels), fixed and sliding window methods (precomputation), NAF methods (negation is free), GLV and GLS methods (efficient endomorphisms)…
- Montgomery ladder (differential x-addition), Edwards (unified formulae)…

Biodiversity





→ *Biodiversity in **fields***

- What does $E(\mathbb{R})$ look like?

Analytically, E(R) is isomorphic to the circle group S^1 or to two copies of the circle group $S^1 \times C_2$.

- What does $E(\mathbb{C})$ look like?

The points of an elliptic curve with coordinates in the complex numbers form a torus

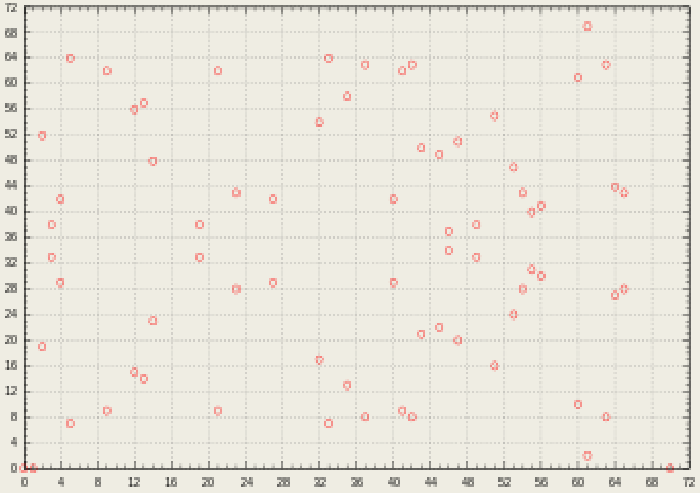
- What does $E(\mathbb{Q})$ look like?

The group of rational points E($\mathbb{Q}$) is a subgroup of the group of real points E($\mathbb{R}$)

Theorem (Mordell 1922) E(Q)
Theorem (Mazur 1977) E(Q)
Conjecture (Elkies 2006, highest rank)
Theorem (Siegel 1928) E(Z)
Theorem (Hasse 1922) E(Fp)

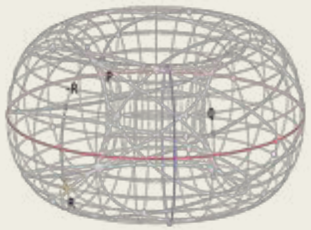
What does $E(\mathbb{Z})$ look like?

E($\mathbb{Z}$) is usually not a subgroup of E($\mathbb{Q}$)

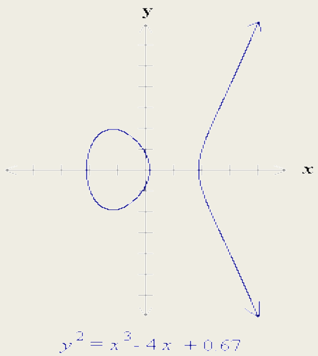


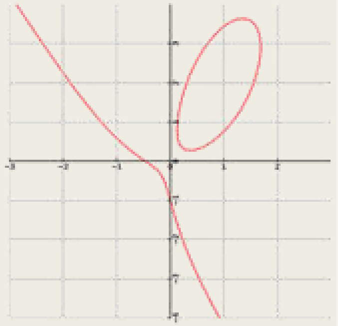
- What does $E(\mathbb{F}_p)$ look like?

$E(\mathbb{F}_p)$ is a finite group



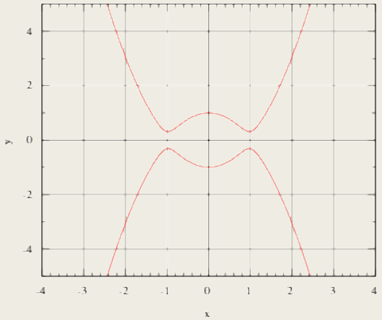
Biodiversity

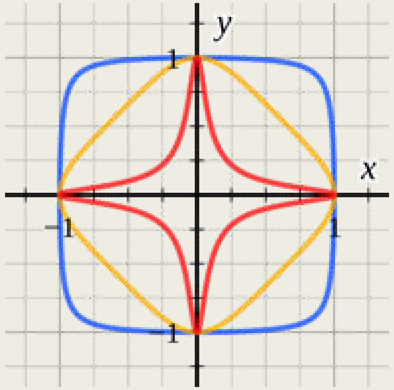




→ *Biodiversity in* ***shapes***

- General Weirestrass : $Ax^3 + Bx^2y + Cxy^2 + Dy^3 + Ex^2 + Fxy + Gy^2 + Hx + Iy + J = 0$
- Short Weierstrass : $y^2 = x^3 + ax + b,\ (char \neq 2, 3)$
- Normal Legendre : $y^2 = x(x-1)(x-\lambda),\ (char \neq 2, 3)$
- Montgomery : $Ay^2 = x^3 + Bx + x$
- Edwards: $x^2 + y^2 = 1 - dx^2y^2$
- Jacobi quartics : $x^2 = y^4 - d^2 + 1$
- Hessian : $x^3 - y^3 + 1 = dxy$





→ *Biodiversity in* ***coordinates***

Affine or projective: (modified) jacobian, inverted, Lopez-Dahab…

Peter L. Montgomery 1987
Hessian: Bernstein, Lange, Kohel
Edwards: Harold Edwards, Bernstein, Lange

http://hyperelliptic.org/EFD/g1p/index.html

Homo genus (Homo Sapiens)

- $E(\mathbb{F}_p)$: $\{(x,y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + ax + b \ (mod\ p),\ 4a^3 + 27b^2 \neq 0\ (mod\ p)\} \cup \{0\}$
- Group order: How many points are on $E(\mathbb{F}_p)$? → Schoof's algorithm (Bordeaux, 1995)

Hasse theorem: $|p+1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$

Frobenius endomorphism $\phi_p: E(\overline{\mathbb{F}_p}) \to E(\overline{\mathbb{F}_p})$ where $\phi_p(x,y) = (x^p, y^p)$ and has the characteristic polynomial $\xi(x) = x^2 - tx + p$

Chinese remainder theorem

- Cyclic subgroup order : the smallest positive integer s.t. $nP = 0$

Lagrange theorem: $n \mid \#E(\mathbb{F}_p)$ then $\frac{\#E(\mathbb{F}_p)}{n} = h \in \mathbb{N}$

Find a generatorof order n: n(hP)=0 $\forall$P $\in E(\mathbb{F}_p)$

Homo genus (Homo Erictus)

- The disrete logarithm problem (DLP): Given a, b in a cyclic group G, it is computationally hard to recover the integer k such that $a = b^{\mathrm{k}}$
- The problem is quickly computable in a few special cases so choosing the group G is critical and a popular choice that provides good security assumptions is $\mathbb{F}_p$
- Best algortihm: General Number Field Sieve (GNFS) with sub-exponential complexity

$$L_n\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right] = \exp\left(\left(\sqrt[3]{\frac{64}{9}} + o(1)\right)(\ln^{\frac{1}{3}} n)(\ln^{\frac{2}{3}} \ln n)\right)$$

- The disrete logarithm problem over elliptic curves (ECDLP): Given two points P, Q in $E(\mathbb{F}_p)$ it is computationally hard to recover the integer k such that $P = kQ$
- Best algorithm: Pollard's ρ with complexity $\sim O(\sqrt{n})$

Reproduction of Homo Sapiens

→ Purpose : ECDH (key exchange), ECDSA (signatures), ~~EC-ElGamal (encryption) …~~

(Koblitz 1985)

- Shape : Weierstrass, Montgemery, Edwards …
- Field $\mathbb{F}_p$: bit-length of p, $char \neq\ 2,3$ …
- Group order n: bit-length, length ratio with p, prime/composite order…
- Coefficients a and b (or d): nothing up my sleeve, number of twists…
- Frobenius trace: $t = 1$ tricial DL (SSSS attack), $t = 0$ supersingular curve …
- Complex Multiplication discriminant : $|D| = \frac{4p-t^2}{y^2}$ small ?
- Security of the curve twists…
- Big embedding degree… (pairings)

Reproduction of Homo Sapiens

→ Most popular curve: NIST P-256 $y^2 = x^3 - \mathbf{3}x + b \ (mod\ p)$ of **Weierstrass** shape defined over $\mathbb{F}_{\boldsymbol{p}}$

Where: $\boldsymbol{p} = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$ (Solinas **prime** number of Generelized Mersenne number) of 256 **bit-length** and

$\boldsymbol{b}$ =41058363725152142129326129780047268409114441015993725554835256314039467401291

that comes from a seed $s = c49d3608\ 86e70493$ 6a6678e1 139d26b7 819f7e90

The curve has prime **order** $n = 115792089210356248762697446949407573529996955224135760342422259061068512044369$

of 256 **bit length.**

The Frobenius trace: $t = 89188191154553853111372247798585809583$ (ordinary curve)

CM **discriminant** : $|D| = 455213823400003756884736869668539463648899917731097708475249543966132856781915$

Only one **twist** (quadratic) of order $n' = 3317349640749355357762425066592395746459685764401801118712075735758936647$ (**241** bits)

Cofactor of the **twist** is $3 \times 5 \times 13 \times 179$

Embedding degree of the curve

$$k = 38597363070118749587565815649802524509998985074711920114140753020356170681456$$

And **embedding degree of the twisted curve**

$$k' = 16586748203746776788812125332961978732298428822009005593560378678794683 23$$

Fire control

André Weil (1940) in the military prison in Rouen

Let $E(\mathbb{F}_p)$ be an EC and G a subgroup of order n (remember $n|p+1-t$)

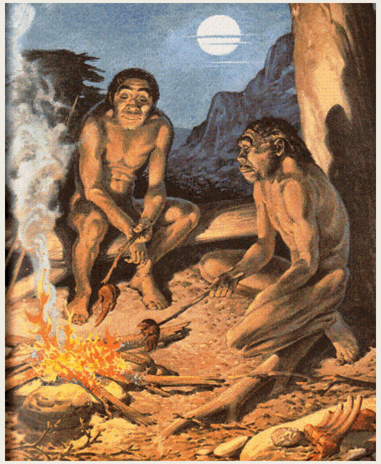
A (cryptographic) pairing (of type 1) on elliptic curves is a map $e: G \times G \to \mathbb{F}_{p^k}$ where k is the smallest positive integer s.t. $n|p^k - 1$. The pairing must be:

- Bilinear: $e(P+R,Q) = e(P,Q)e(P,R)$ and $e(P,R+Q) = e(P,R)e(P,Q)$ thus $e(aP,bQ) = e(P,Q)^{ab}$
- Non-degenerate: $\forall P \ \exists Q \ \ e(P,Q) \neq 1$ and $\forall Q \ \exists P \ \ e(P,Q) \neq 1$
- Efficiently computable !

e.g. : Weil, Tate, Optimal Ate…

→ Illustration example : $e(\vec{u},\vec{v}) = \det\begin{pmatrix} u_0 & u_1 \\ v_0 & v_1 \end{pmatrix} = u_0 v_1 - u_1 v_0$

Alternacy: $e(\vec{u},\vec{v})$=-$e(\vec{v},\vec{u}) \to e(\vec{u},\vec{u}) = 0$ (or any linear comibation of $\vec{u}$)



Fire control

Types of pairings $\hat{e}: G_1 \times G_2 \to \mathbb{F}_{p^k}$

- Type 1: $G_1 = G_2$

Distorsion maps f (only on supersingular) $\hat{e}(P, Q) = e(P, f(Q))$.

e.g. Supersingular curves with k = 2 admit particularly simple distortion maps, namely, $\psi(x, y) = (\zeta_3 x, y)$ for $y^2 = x^3 + 1$ over $p \geq 5$ and p ≡ 2 (mod 3), where ζ_3 is primitive third root of unity in $\mathbb{F}_{p^2}$

- Type 2: $G_1 \neq G_2$

There is an efficiently computable monomorphism φ from G_2 to G_1.

Reductionist proofs but hashing or random sampling in G_2 seems to be impossssible.

- Type 3: $G_1 \neq G_2$

there is no apparent, efficiently computable monomorphism G_2 to G_1

Fire control: Destructive use

MOV attack (Weil pairing) and Frey-Rück attack (Tate pairing)

Let $Q = nP$ with P and Q public and n secret we have $\underbrace{e(P,Q)}_{public} = \underbrace{e(P,P)}_{public}{}^{n}$

Tranfer the ECDLP over $\boldsymbol{E}(\mathbb{F}_{\boldsymbol{p}})$ *(best attack Pollard with quadratic complexity)*

to DLP over $\mathbb{F}_{\boldsymbol{p}^{\boldsymbol{k}}}$ *(best attack GNFS with sub-exponential complexity)*

So k has to be big enough (e.g. P-256 k is 255 bits, supersignular EC $k \leq 6$)

Menezes, Okamoto, Vanstone (1993)
G. Frey and H.-G. Rück (1994)

Fire control: Constructive use

One-round tripartite Diffie-Hellman *(Antoine Joux, 2000)*

Given Alice (a/aG), Bob (b/bG) and Cécile (c/cG) the secret is

$$e(G,G)^{abc} = e(aG,bG)^{c} = e(aG,cG)^{b} = e(cG,bG)^{a}$$

BLS (short) signatures *(Boneh, Lynn, Shacham, 2004)*

Alice (a/A=aG) signs a message $m \in \{0,1\}^*$ as $S = aH(m)$ where H hashes m into G_1

Anyone can verify $e(S,G) = e(A,H(m))$

Identity-based encryption *(Boneh, Franklin, 2001)*

Pairing-based zero knowledge proofs (zkSNARKs) (Jens Groth, 2006)

…

[BGN05] Pairing-based double-homomorphic encryption scheme
[Groth06] NIZK proofs for practical language (pairing-product equations)

Pairing-friendly elliptic curves

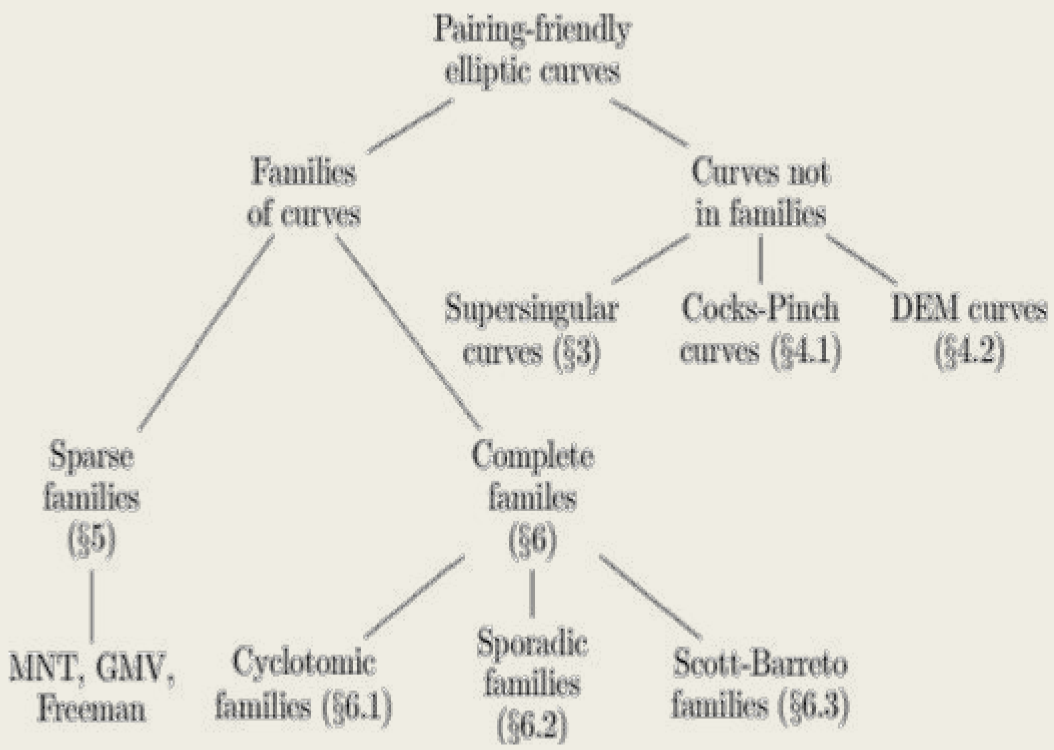
From CM theory an EC $\boldsymbol{E}(\mathbb{F}_{\boldsymbol{p}})$ satisfies

$4p = t^2 - Dy^2$ and $4r = (t-2)^2 + Dy^2$

Where t is the Frobenius trace, r the subgroup order, D the CM discriminat (Frobenius map discriminant) and y an integer.

Pairing-friendliness conditions:

- $\mathrm{n} = \#E(\mathbb{F}_p) = p + 1 - t$ where $|t| < 2\sqrt{p}$
- $r|n$
- $r|p^k - 1$
- $t^2 - 4p = Dy^2$ (with small |D|)



Freeman, Scott, Teske (2006)

Pairing-friendly elliptic curves

- **Cocks-Pinch strategy** *(C. Cocks and R.G.E. Pinch in an unpublished manuscript, 2001)*

1. Fix D, k and choose a prime r.

   Require that k divides r − 1 and −D is a square mod r.

2. Compute $t = 1 + x^{\frac{r-1}{k}}$ for x a generator of $(\mathbb{Z}/\mathbb{Z})^{\times}$.
3. Compute $y = \frac{t-2}{\sqrt{-D}} \; (mod\ r)$
4. Compute $p = \frac{(t^2 + Dy^2)}{4}$ (in $\mathbb{Q}$).
5. If p is an integer and prime, use CM method to construct elliptic curve over $\mathbb{F}_p$ with an order-r subgroup.

→ y is constructed so that CM equations are automatically satisfied.

→ Since t, y are essentially random integers in $[0, r)$, $\mathrm{p} \approx r^2$, so $\rho \approx 2$.

Pairing-friendly elliptic curves

- **Complex Multiplication method**

Once we find an elliptic curve that has a field size p, and order r a Frobenius trace t, a CM discriminant D and an embedding degree k that verifies all the requirements needed, the method starts by:

1. Find any root j of the Hilbert polynomial $H_D(x)$ (if j = 0 or 1728 we wind up with special curves)
2. Set $l = \frac{j}{1728-j} \ (mod\ p)$

then the curve is $y^2 = x^3 + 3lc^2 + 2lc^3$. First, we pick c=1 so the curve has an order p+t+1 or p-t+1. Then we choose a random point and multiply it by p-t+1 if it 0 then the curve is $y^2 = x^3 + 3lx + 2l$ otherwise it is a quadratic twist and we choose c to be some quadratic nonresidue c' and the curve is

$$y^2 = x^3 + 3kc'^2 + 2kc'^3$$

Pairing-friendly elliptic curves

- **MNT curves strategy** (A. Miyaji, M. Nakabayashi, and S. Takano, 2001)

First used by Miyaji-Nakabayashi-Takano; also used by Scott-Barreto (2006), Barreto-Naehrig (2006) and Freeman (2008) (paremetrize integers by polynomials)

1. Fix D, k, and choose polynomials $t(x), h(x)$. $h(x) = 1$ if searching for curves of prime order.
2. Choose $r(x)$ an irreducible factor of $\Phi_k\ (t(x) - 1)$.
3. Compute $p(x) = h(x)r(x) + t(x) - 1$.
4. Find integer solutions (x, y) to CM equation $Dy^2\ =\ 4h(x)r(x) - (t(x) - 2)^2$
5. If $p(x)$, $r(x)$ are both prime, use CM method to construct elliptic curve over $\mathbb{F}_{p(x)}$ with $h(x)r(x)$ points.

Pairing-friendly elliptic curves

- **MNT curves strategy**

If $f(x) = 4h(x)r(x) - (t(x) - 2)^2$ has $deg \geq 3$ the eq. $Dy^2 = f(x)$ has finitely many solutions. We need to choose h(x), r(x) and t(x) so that f(x) is quadratic or has multiple roots.

→ Goal: Choose *t* (*x*), find factor *r* (*x*) of $\Phi_k(t(x) - 1)$, such that *f*(*x*) is quadratic.

→ Solution:

1. Choose *t*(*x*) linear; then *r*(*x*) is quadratic, and so is *f*(*x*).
2. Use standard algorithms to find solutions (*x*,*y*) to $Dy^2 = f(x)$ (Pell-Fermat equation)
3. If no solutions of appropriate size, or *q*(*x*) or *r*(*x*) not prime, choose different *D* and try again.

- Scott-Barreto extend MNT idea by allowing “cofactor” $h(x) \neq 1$. Find many more suitable curves than original MNT construction.
- Barreto-Naehrig: Choose *t*(*x*), find factor *r*(*x*) of $\Phi_{12}(t(x) - 1)$, such that *f*(*x*) has multiple root.

Cycles of pairing-friendly elliptic curves

An aliquot cycle (Silverman, Stange 2011) of length m is s.t.
$\#E_1(\mathbb{F}_{p_1}) = p_m,\ \#E_2(\mathbb{F}_{p_2}) = p_1, \#E_3(\mathbb{F}_3) = p_2, \dots, \#E_m(\mathbb{F}_{p_m}) = p_{m-1}$

If all curves are pairing-friendly, it is a pairing-friendly cycle (Chiesa, Chua, Weidner 2018)

- Application: Recursive zkSNARKs (BCCT13, BCTV15)
- Consutructions: MNT curves (libsnark), chains (ZEXE 2018)

References

- **Books**

- Joseph H. Silverman, John Tate, « Rational Points on Elliptic Curves » *a.k.a « Silverman 0 »*
- Joseph H. Silverman, « The Arithmetic of Elliptic Curves » *a.k.a « Silverman 1 »*
- Joseph H. Silverman, « Advanced Topics in the Arithmetic of Elliptic Curves » a.k.a « Silverman2 »
- David A. Cox, « Primes of the form $x^2 + ny^2$ »

- **Papers**

- R. Schoof: Counting Points on Elliptic Curves over Finite Fields. J. Theor. Nombres Bordeaux 7:219–254, 1995. Available at http://www.mat.uniroma2.it/~schoof/ctg.pdf
- *Peter L. Montgomery (1987). "Speeding the Pollard and Elliptic Curve Methods of Factorization". Mathematics of Computation.* **48** *(177): 243–264. doi:10.2307/2007888. JSTOR 2007888.*
- *Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange and Christiane Peters (2008). "Twisted Edwards Curves" (PDF). Progress in Cryptology – AFRICACRYPT 2008. Lecture Notes in Computer Science.* **5023***. Springer-Verlag Berlin Heidelberg. pp. 389–405. doi:10.1007/978-3-540-68164-9_26. ISBN 978-3-540-68159-5.*
- *N. P. Smart (2001). The Hessian form of an Elliptic Curve. Springer-Verlag Berlin Heidelberg 2001. ISBN 978-3-540-42521-2.*
- *Olivier Billet, Marc Joye (2003). The Jacobi Model of an Elliptic Curve and the Side-Channel Analysis (PDF). Springer-Verlag Berlin Heidelberg 2003. ISBN 978-3-540-40111-7.*
- Arjen K. Lenstra and H. W. Lenstra, Jr. (eds.). "The development of the number field sieve". Lecture Notes in Math. (1993) 1554. Springer-Verlag.
- *Pollard, J. M. (1975), "A Monte Carlo method for factorization", BIT Numerical Mathematics,* **15** *(3): 331–334, doi:10.1007/bf01933667*
- "FIPS PUB 186-3: Digital Signature Standard (DSS). June 2009"(PDF). *csrc.nist.gov*
- *Menezes, Vanstone, Okamoto* « Reducing elliptic curve logarithms to logarithms in a finite field » 1993
- Gerhard Frey and Hans-Georg Rück. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. Comp., 62(206):865–874, 1994.
- Joux A. (2000) A One Round Protocol for Tripartite Diffie–Hellman. In: Bosma W. (eds) Algorithmic Number Theory. ANTS 2000. Lecture Notes in Computer Science, vol 1838. Springer, Berlin, Heidelberg
- *Dan Boneh; Ben Lynn & Hovav Shacham (2004). "Short Signatures from the Weil Pairing". Journal of Cryptology.* **17** *(4): 297–319. CiteSeerX 10.1.1.589.9141. doi:10.1007/s00145-004-0314-9.^*
- Dan Boneh, Matthew K. Franklin, "Identity-Based Encryption from the Weil Pairing", *Advances in Cryptology - Proceedings of CRYPTO 2001* (2001)
- « A TAXONOMY OF PAIRING-FRIENDLY ELLIPTIC CURVES », DAVID FREEMAN, MICHAEL SCOTT, AND EDLYN TESKE
- Ben-Sasson E., Chiesa A., Tromer E., Virza M. (2014) Scalable Zero Knowledge via Cycles of Elliptic Curves. In: Garay J.A., Gennaro R. (eds) Advances in Cryptology – CRYPTO 2014. CRYPTO 2014. Lecture Notes in Computer Science, vol 8617. Springer, Berlin, Heidelberg
- « On cycles of pairing-friendly elliptic curves » Alessandro Chiesa, Lynn Chua, Matthew Weidner

Appendix

Curve shape, representation	DBL	ADD	mADD	mDBL	TPL	DBL+ADD
Short Weierstrass projective	11	14	11	8		
Short Weierstrass projective with a4=-1	11	14	11	8		
Short Weierstrass projective with a4=-3	10	14	11	8		
Short Weierstrass Relative Jacobian[1]	10	11	(7)	(7)		18
Tripling-oriented Doche–Icart–Kohel curve	9	17	11	6	12	
Hessian curve extended	9	12	11	9		
Hessian curve projective	8	12	10	6	14	
Jacobi quartic XYZ	8	13	11	5		
Jacobi quartic doubling-oriented XYZ	8	13	11	5		
Twisted Hessian curve projective	8	12	12	8	14	
Doubling-oriented Doche–Icart–Kohel curve	7	17	12	6		
Jacobi intersection projective	7	14	12	6	14	
Jacobi intersection extended	7	12	11	7	16	
Twisted Edwards projective	7	11	10	6		
Twisted Edwards Inverted	7	10	9	6		
Twisted Edwards Extended	8	9	8	7		
Edwards projective	7	11	9	6	13	
Jacobi quartic doubling-oriented XXYZZ	7	11	9	6	14	
Jacobi quartic XXYZZ	7	11	9	6	14	
Jacobi quartic XXYZZR	7	10	9	7	15	
Edwards curve inverted	7	10	9	6		
Montgomery curve	4			3		