Useful Stuff

Benjamin Smith

INRIA Saclay–Île-de-France
Laboratoire d'Informatique de l'École polytechnique (LIX)

12/09/2011

-1: *Context*

Let $G = \langle P \rangle$ be a finite cyclic group; write $N = \#G$.

- G is abelian;
- 0 denotes the identity element,
- $+$ the group operation,
- $-$ the inverse operation.

"Exponentiation" in G by an integer m is written

$$[m]P = P + \cdots + P \quad (m \text{ times}).$$

The first practical key exchange algorithm was invented by Williamson (1974 at GCHQ, UK), then rediscovered by Diffie and Hellman (in 1976) It is still used, with only light modifications.

DH Key Exchange

Alice and Bob want to establish a common secret key.

1. They agree, publicly, on a group $G = \langle P \rangle$ of order N;
2. Alice chooses some secret $a \in [1..N-1]$, and publishes $A = [a]P$;
3. Bob chooses some secret $b \in [1..N-1]$, and publishes $B = [b]P$;
4. Alice and Bob can now compute the shared secret $K = [a]B = [b]A = [ab]P$.

Computational Diffie–Hellman Problem (CDHP)

The security of DH key exchange (and DSA) depends on the "hardness" of the CDHP for G:

Given P, $[a]P$, and $[b]P$, compute $[ab]P$.

Discrete Logarithm Problem (DLP)

For the groups G that we use in practice, the CDHP is believed to be equivalent to the DLP for G:

Given P and $[a]P$, compute a.

Exhaustive search: can find a in time $\rightarrow O(N)$.

The Baby-Step Giant-Step (BSGS) Algorithm

1. Fix $0 < s < N$ (giant step size).
2. Compute $S_1 = \{P, [s]P, [2s]P, \ldots, [\lfloor N/s \rfloor s]P\}$
3. Compute $S_2 = \{Q, [2]Q, [3]Q, \ldots, [s]Q$
4. Find an element in $S_1 \cap S_2$: ie $[as]P = [b]Q$
5. Conclude $n = as \cdot b^{-1} \pmod{N}$.

- Space requirements: $O(N/s) + O(s)$ group elements
- Time: $O(N/s) + O(s) + O(\min(s, N/s)$ group ops
- Best choice: $s \sim \sqrt{N}$: DLP solution in $\widetilde{O}(\sqrt{N})$

Note: can also use BSGS to determine the group order N.

Fundamental Theorem of Finite Abelian Groups

$$G \cong \prod_{i=1}^{n} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})$$

for some positive integer n, primes p_i, and exponents e_i.

Pohlig–Hellman Theorem

Suppose $G \cong \prod_{i=1}^{n} (\mathbb{Z}/p_i^{e_i}\mathbb{Z})$, so $N = \#G = \prod_{i=1}^{n} p_i^{e_i}$.

We can solve the DLP in G in $O(\sum_{i=1}^{n} e_i(\log N + \sqrt{p_i}))$ group operations.

Moral: the DLP in G is essentially only as hard as the DLP in its largest prime-order subgroup; so *G is only as secure as its largest prime-order subgroup.*

Also: other $O(\sqrt{N})$ algorithms (Pollard ρ, λ, kangaroo...)

We can always solve the DLP in $O(\sqrt{N})$ time and space.

- This is worst case, and
- Independent of the concrete representation of G

Some choices of G have much easier DLP solutions...

Eg. $G = \mathbb{Z}/N\mathbb{Z}$. Solve the DLP via Euclid's algorithm.

Our challenge

To construct groups that are cryptographically efficient, in the sense that they are

- **compact** (lots of group per bit),
- **fast** (easy to compute group operations), and
- **secure** (hard DLPs relative to their size).

Natural candidates: algebraic groups over $\mathbb{F}_q$.

- Elements are tuples of elements of $\mathbb{F}_q$,
- Group operations are defined by polynomial functions.

Finite Fields

- $\mathbb{F}_q$ is the finite field with q elements;
- q is a power of some prime p;
- Algebraic closure: $\overline{\mathbb{F}}_q = \bigcup_{i \geq 1} \mathbb{F}_{q^i}$.
- Algorithmically, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$;
- $\mathbb{F}_q \cong \mathbb{F}_p[x]/f(x)$ for *any* irreducible f (with $q = p^{\deg f}$)
- Note: choice of f affects computational efficiency

Frobenius

- *Frobenius* is the q-powering map on $\overline{\mathbb{F}}_q$:

$$\sigma : x \mapsto x^q.$$

- $\mathbb{F}_{q^i} = \mathrm{Fix}(\sigma^i)$ for all $i \geq 1$.
- Objects are **defined over** $\mathbb{F}_{q^k}$ if they are fixed by σ^k.
- Eg. a set $\{a, b, c\}$ is defined over $\mathbb{F}_{q^k}$ if $\{a, b, c\} = \{\sigma(a), \sigma(b), \sigma(c)\}$

The Galois group of $\overline{\mathbb{F}}_q/\mathbb{F}_q$ is (topologically) generated by Frobenius:

$$\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) = \widehat{\mathbb{Z}}$$

We will work with objects defined over $\mathbb{F}_q$.

Our basic unit of measurement is therefore $\log q$.

- $\log q = \text{const} \times \#\text{bits required to store elements of } \mathbb{F}_q$.

L-notation: for $0 \leq \alpha \leq 1$ and $c > 0$,

$$L_q[\alpha, c] := \exp((c + o(1))(\log q)^{\alpha}(\log\log q)^{1-\alpha})$$

- $L_q[0, c] = O((\log q)^c)$ (polynomial in $\log q$)
- $L_q[1, c] = O(q^c)$ (exponential in $\log q$)
- For $0 < \alpha < 1$, $L_q[\alpha, c]$ is **subexponential**: bigger than polynomial, but smaller than exponential.
- "Soft O": $\widetilde{O} \implies$ ignore factors of $\log\log q$, etc.

Multiplicative group $\mathbb{G}_m(\mathbb{F}_q)$

Consider the multiplicative group

$$\mathbb{G}_m(\mathbb{F}_q) = \mathbb{F}_q^\times = (\mathbb{F}_q \setminus \{0\}, \times).$$

- If $G \subset \mathbb{G}_m(\mathbb{F}_q)$ is a prime-order subgroup, then $N = \#G \leq q-1$.
  - Best case: $q = hN+1$, h small, N prime.
  - Worst case: $q = 2^r + 1$.
- Computing in $\mathbb{G}_m(\mathbb{F}_q)$ is very fast.
- Index Calculus $\implies$ subexponential $L_q[1/3, c]$ DLP in $\mathbb{G}_m(\mathbb{F}_q)$.

We see that the hardness of the DLP depends heavily on the concrete representation of the group.

We want groups of about the same size and speed as $\mathbb{G}_m(\mathbb{F}_q)$, but with a much harder DLP...

...which leads us to Elliptic Curves:

- curves over $\mathbb{F}_q$ whose points form an abelian group.
- For comparable space and speed of computation, we can get
  - $N = O(q)$,
  - with the full $\sqrt{N} = L_q[1, 1/2]$ complexity for DLPs.

0: *Algebraic Curves*

Plane *curves* over $\mathbb{F}_q$ are defined by polynomials over $\mathbb{F}_q$:

$$\mathscr{C} : f(x,y) = 0 \qquad \text{(affine), or}$$
$$\mathscr{C} : F(X,Y,Z) = 0 \qquad \text{(projective)}$$

Projective planes: traditional *flat*/conventional $\mathbb{P}^2$:

$$(X : Y : Z) = (\lambda X : \lambda Y : \lambda Z) \quad \text{for all } \lambda \in \overline{\mathbb{F}}_q \setminus \{0\}$$

we usually take $x = X/Z$, $y = Y/Z$.

...also *weighted* projective planes, eg $\mathbb{P}(a,b,c)$

$$(X : Y : Z) = (\lambda^a X : \lambda^b Y : \lambda^c Z) \quad \text{for all } \lambda \in \overline{\mathbb{F}}_q \setminus \{0\}$$

(typically $(a,b,c) = (1,g+1,1)$, $x = X/Z$, $y = Y/Z^{g+1}$.)

The *genus* of a curve measures its geometric complexity.

Lines: eg $\mathscr{L} : X + Y - 3Z = 0$ in $\mathbb{P}^2$. *Genus 0*

Conics: eg $\mathscr{C} : X^2 + Y^2 - Z^2 = 0$ in $\mathbb{P}^2$. *Genus 0*

Elliptic curves: eg $\mathscr{E} : y^2 = x^3 + ax + b$. *Genus 1*

Genus 2 curves: eg $\mathscr{C} : y^2 = x^5 - 5x^3 + 5x + t$.

(Smooth) **quartics**: eg $\mathscr{C} : X^3Y + Y^3Z + Z^3X = 0$. *Genus 3*

Rational points

Suppose $\mathscr{C} : F(x,y) = 0$ is a curve over $\mathbb{F}_q$ of genus g.

$$\mathscr{C}(\mathbb{F}_{q^k}) := \left\{(\alpha,\beta) \in \mathbb{F}_{q^k}^2 : F(\alpha,\beta) = 0\right\}.$$

...extends to projective curves (add points at infinity)

Weil bounds

$$(q^k+1) - 2g\sqrt{q^k} \leq \#\mathscr{C}(\mathbb{F}_{q^k}) \leq (q^k+1) + 2g\sqrt{q^k}$$

So $\#\mathscr{C}(\mathbb{F}_{q^k})$ is in $O(q^k)$.

The **Function field** of $\mathscr{C} : F(x,y) = 0$ is

$$\mathbb{F}_q(\mathscr{C}) = \mathbb{F}_q(x)[y]/(F(x,y)).$$

Elements are quotients of polynomials:

- in x and y: for example,

$$g_1 = \frac{x + 2y - z}{x^2 - 3}$$

- in X, Y, Z *with equal weighted degree*:

$$\frac{(X + 2Y - Z)Z}{X^2 - 3Z^2} \quad \text{when } \mathscr{C} \subset \mathbb{P}^2 = \mathbb{P}(1,1,1)$$

$$\frac{XZ^g + 2Y - Z^{g+1}}{X^2 Z^{g-1} - 3Z^{g+1}} \quad \text{when } \mathscr{C} \subset \mathbb{P}(1, g+1, 1)$$

Consider curves $\mathscr{C} : F(x,y) = 0$, $\mathscr{D} : G(u,v) = 0$.

A *morphism* $\Phi : \mathscr{C} \to \mathscr{D}$ is defined by

$$\Phi : (x,y) \longmapsto (\Phi_u(x,y), \Phi_v(x,y))$$

where Φ_u and Φ_v are functions on $\mathscr{C}$, and $G(\Phi_u, \Phi_v) = 0$.

Morphisms of curves $\leftrightarrow$ function field extensions.

The function field extension corresponding to Φ is

$$\Phi^* : \mathbb{F}_q(\mathscr{D}) \to \mathbb{F}_q(\mathscr{C}),$$

where $\Phi^*(u) = \phi_u$ and $\Phi^*(v) = \phi_v$.

The *degree* of a morphism Φ is defined by

$$\deg \Phi := [\mathbb{F}_q(\mathscr{C}) : \mathbb{F}_q(\mathscr{D})]$$

An *isomorphism* is a morphism of degree 1.

Function fields correspond to nonsingular curves
(Technically: the function field is a birational invariant)

So talking about curves = talking about function fields

Functions have Zeroes and Poles

Zeroes : "numerator 0"

- g_1 has a zero at $(1,-1)$
- G_2 has a zero at $(1:1:3)$

Poles : "denominator 0"

- g_1 has a double pole at $(\sqrt{3},1)$
- G_2 has a pole at $(1:4:-1)$

Watch out: affine x and y have *poles at infinity*

Can view functions Φ in $\mathbb{F}_q(\mathscr{C})$ as morphisms $\Phi : \mathscr{C} \to \mathbb{P}^1$;
then Zeroes $= \Phi^{-1}((0:1))$ and Poles $= \Phi^{-1}((1:0))$

$v_P(f) :=$ *order of vanishing* of a function f at a point P

- $v_P(f) = 3 \implies f$ has a zero at P with multiplicity 3
- $v_P(f) = -5 \implies f$ has a pole at P with multiplicity 5
- $v_P(f) = 0 \implies f$ takes a nonzero value at P

Given a function $f \neq 0$ in $\mathbb{F}_q(\mathscr{C})$, its *(principal) divisor* is the *formal sum*

$$\operatorname{div}(f) := \sum_{P \in \mathscr{C}(\overline{\mathbb{F}}_q)} v_P(f) P.$$

Principal divisors encode function data:

$$\operatorname{div}(f) = \operatorname{div}(g) \iff f = \alpha g \quad \text{for some } \alpha \in \overline{\mathbb{F}}_q^\times.$$

More generally, a *divisor* on $\mathscr{C}$ is a formal sum

$$D = \sum_{P \in \mathscr{C}(\overline{\mathbb{F}}_q)} n_P P$$

where the n_P are integers, with all but finitely many $n_P = 0$.

The degree of D is

$$\deg D := \sum_P n_P.$$

All functions have an equal number of zeroes and poles, so

$$\deg(\operatorname{div}(f)) = 0 \quad \text{for all } f \in \overline{\mathbb{F}}_q^\times(\mathscr{C}).$$

- The divisors on $\mathscr{C}$ form a group $\mathrm{Div}(\mathscr{C})$
- deg is additive $\implies$ we have a subgroup $\mathrm{Div}^0(\mathscr{C}) = \{D \in \mathrm{Div}(\mathscr{C}) : \deg(D) = 0\} \subset \mathrm{Div}(\mathscr{C})$
- $\mathrm{div}(f \cdot g) = \mathrm{div}(f) + \mathrm{div}(g) \implies$ subgroup $\mathrm{Prin}(\mathscr{C}) := \{\mathrm{div}(f) : f \in \overline{\mathbb{F}}_q(\mathscr{C})\} \subset \mathrm{Div}^0(\mathscr{C}) \subset \mathrm{Div}(\mathscr{C})$
- These groups are boring, and way too big!

The quotient groups are particularly interesting:

$$\mathrm{Pic}(\mathscr{C}) := \mathrm{Div}(\mathscr{C})/\mathrm{Prin}(\mathscr{C})$$

$$\mathrm{Pic}^0(\mathscr{C}) := \mathrm{Div}^0(\mathscr{C})/\mathrm{Prin}(\mathscr{C}).$$

The image of D in $\mathrm{Pic}\mathscr{C}$ is denoted by $[D]$.

Frobenius acts on divisors:

$$\sigma\Big(\sum_P n_P P\Big) := \sum_P n_P \sigma(P).$$

- $\mathrm{Div}^0(\mathscr{C})(\mathbb{F}_{q^k}) := \{D \in \mathrm{Div}^0(\mathscr{C}) : \sigma(D) = D\}$
- $\mathrm{Pic}^0(\mathscr{C})(\mathbb{F}_{q^k}) := \{[D] \in \mathrm{Pic}^0(\mathscr{C}) : [\sigma(D)] = [D]\}$

$\mathrm{Pic}^0(\mathscr{C})$ has a geometric structure:
it is $\cong$ to an abelian variety $J_{\mathscr{C}}$ called the *Jacobian*.

$$\mathrm{Pic}^0(\mathscr{C})(\mathbb{F}_{q^k}) \cong J_{\mathscr{C}}(\mathbb{F}_{q^k}) \quad \text{for all } k > 0.$$

The Riemann–Roch (R–R) theorem

(the swiss army knife for curves)

- We chop $\mathbb{F}_q(\mathscr{C})$ up into slices $L(D)$ for each divisor D.
- $L(D) =$ vector space $\{f \in \mathbb{F}_q(\mathscr{C}) : \text{poles}(f) \leq D\}$.
- R–R: computes slice dimensions:

$$\dim(L(D)) - \dim(L(K_{\mathscr{C}} - D)) = \deg(D) - g + 1.$$

  where $K_{\mathscr{C}} =$ *canonical divisor* associated to the differentials on $\mathscr{C}$.
- *Explicit* R–R: computes generators for $L(D)$.

For the moment, we will leave R–R as abstract magic.

R–R describes the size and "shape" of $\mathrm{Pic}^0(\mathscr{C})$:

- $J_{\mathscr{C}} \sim \mathscr{C}^{(g)}$ (the g-fold symmetric product)
- $\Longrightarrow \dim J_{\mathscr{C}} = g$
- $\Longrightarrow \#J_{\mathscr{C}}(\mathbb{F}_{q^k}) \sim q^{gk}$

Example

Let $\mathscr{C}/\mathbb{F}_q$ be a smooth curve of genus 0
(ie defined by a linear or quadratic equation).

- All divisor classes of the same degree are identical
- $\mathrm{Div}^0(\mathscr{C}) = \mathrm{Prin}(\mathscr{C})$
- $J_{\mathscr{C}} = 0$ (...so $\mathscr{C}$ is not much use for crypto)

Explicit R–R $\Longrightarrow$ defining equations of curves
(eg. Weierstrass equation of an elliptic curve)

We use explicit R–R to compute distinguished representatives of divisor classes...

$\Longrightarrow$ bounded representations for group elements

$\Longrightarrow$ algorithms for group operations

$\Longrightarrow$ equality tests

$\Longrightarrow$ models for $J_{\mathscr{C}}$

1: *Elliptic Curves*

The Weierstrass Model

Let $\mathscr{C}$ be a curve of genus 1, and $O_{\mathscr{C}}$ a point in $\mathscr{C}(\mathbb{F}_q)$.

- R–R on $D = 2O_{\mathscr{C}} \implies \exists x \in \mathbb{F}_q(\mathscr{C})$ with $v_{O_{\mathscr{C}}}(x) = -2$
- R–R on $D = 3O_{\mathscr{C}} \implies \exists y \in \mathbb{F}_q(\mathscr{C})$ with $v_{O_{\mathscr{C}}}(y) = -3$
- R–R on $D = 6O_{\mathscr{C}} \implies \exists$ *Weierstrass equation*

$$\mathscr{C} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with a_1, a_2, a_3, a_4, a_6 in $\mathbb{F}_q$

- ($O_{\mathscr{C}}$ is now the unique point at infinity)
- Involution: $(x, y) \mapsto (x, -y - a_1x - a_3)$

We are (mostly) interested in **nonsingular** $\mathscr{C}$
(partial derivatives in x and y are never both 0 on $\mathscr{C}$).

An **Elliptic Curve** is a pair $(\mathscr{C}, O_{\mathscr{C}})$
where $\mathscr{C}$ is nonsingular of genus 1 and $O_{\mathscr{C}}$ is in $\mathscr{C}(\mathbb{F}_q)$.

We have a map $\mathscr{C} \to \mathrm{Pic}^0(\mathscr{C}) = J_{\mathscr{C}}$ defined by

$$P \longmapsto [P - O_{\mathscr{C}}]$$

Explicit R–R $\implies$ every $[D]$ in $\mathrm{Pic}^0(\mathscr{C})$ has a representative in the form $P - O_{\mathscr{C}}$

$\implies \mathscr{C}$ is isomorphic to $J_{\mathscr{C}}$!
(Elliptic Curves are Jacobians of genus 1 curves)

We identify $\mathscr{C}(\mathbb{F}_{q^k})$ with $J_{\mathscr{C}}(\mathbb{F}_{q^k})$

Q: So what is the explicit group law?
A: Ask Laurent!

Formulæ for the group law depend on the choice of **model** for the curve:

- the defining equation used for the function field /
- a concrete manifestation of the curve in some space

For example, we have a wide range of choices of Weierstrass models...

Consider

$$\mathscr{C} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

If $p \neq 2$, can change variables to ensure the form

$$\mathscr{C} : y^2 = x^3 + b_2x^2 + b_4x + b_6.$$

If $p \neq 3$, we can remove the trace term:

$$\mathscr{C} : y^2 = x^3 + c_4x + c_6.$$

- Weierstrass model *(universal)*
- Montgomery & Edwards models
  (fewer field ops per group op, some restrictions)
- Many, many more...

Crucial point:

- Same abstract curve lurking behind the scenes.
- $O(1)$ field ops to change models: choice of model affects operational efficiency, but not DLP hardness.

The j-invariant

Function $j : \{\text{Curves of genus 1 over } \mathbb{F}_q\} \to \mathbb{F}_q$ such that

$$j(\mathscr{C}) = j(\mathscr{C}') \implies \mathscr{C} \cong \mathscr{C}'.$$

If $\mathscr{C} : y^2 = x^3 + c_4 x + c_6$, then

$$j(\mathscr{C}) = \frac{1728 c_4^3}{c_4^3 + \frac{27}{4} c_6^2}.$$

Note: j is surjective, so there are $O(q)$ isomorphism classes of genus 1 curves over $\mathbb{F}_q$ (exponential in $\log q$)!

Elliptic Curve Group Orders

The Weil bounds tell us

$$q^k + 1 - 2\sqrt{q^k} \leq \mathscr{C}(\mathbb{F}_{q^k}) \leq q^k + 1 + 2\sqrt{q^k}$$

(elliptic curves over $\mathbb{F}_{q^k}$ are groups with $O(q^k)$ elements)

Deuring's Theorem

If p is prime, then for every $p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$ there exists an elliptic curve $\mathscr{C}/\mathbb{F}_p$ such that $\#\mathscr{C}(\mathbb{F}_p) = N$.

Group Structure

Clearly $\mathscr{C}(\mathbb{F}_{q^k})$ is finite. FTAG + Weil pairing $\Longrightarrow$

$$\mathscr{C}(\mathbb{F}_{q^k}) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

where $d_1 | d_2$ and $d_1 | (q^k - 1)$

Elliptic Curves over $\mathbb{F}_q$ are algebraic machines that construct groups of order $O(q^k)$ from extensions of $\mathbb{F}_{q^k}$.

That is: each $\mathscr{C}/\mathbb{F}_q$ is a covariant functor
$\mathbb{F}_q$-**Algebras** $\to$ **Abelian Groups**

Degenerate Elliptic Curves

What happens if we use a *singular* Weierstrass equation?

Up to isomorphism, there are essentially only two examples; we can apply a singular version of explicit R–R.

1. Nodal cubic: $\mathscr{C} : y^2 = x^2(x-1)$ is singular at $(0,0)$, and
$$\mathrm{Pic}^0(\mathscr{C})(\mathbb{F}_{q^k}) \cong \mathbb{G}_m(\mathbb{F}_{q^k}).$$
2. Cuspidal cubic: $\mathscr{C} : y^2 = x^3$ is singular at $(0,0)$, and
$$\mathrm{Pic}^0(\mathscr{C})(\mathbb{F}_{q^k}) \cong \mathbb{G}_a(\mathbb{F}_{q^k}).$$

2: *Hyperelliptic Curves*

Hyperelliptic Curves of genus g

- **Affine model**:

$$\mathscr{C} : y^2 + h(x)y = f(x) \quad \text{(affine model)},$$

with $\deg f = 2g+1$ or $2g+2$, and $\deg h \leq g+1$

- **Projective model**:

$$\mathscr{C} : Y^2 + H(X,Z)Y = F(X,Z) \quad (\text{in } \mathbb{P}(1,g+1,1))$$

with $\deg F = 2g+2$, $\deg H = g+1$.

- **Hyperelliptic involution**:

$$\begin{aligned} \iota : (X:Y:Z) &\longmapsto (X:-Y-H(X,Z):Z) \\ (x,y) &\longmapsto (x,-y-h(x)) \end{aligned}$$

- From now on: $\mathscr{C} : y^2 + h(x)y = f(x)$ with $\deg f = 2g+1$ (ie $Z | F(X,Z)$)
- Single point $P_\infty = (1:0:0)$ at infinity.

A divisor D on $\mathscr{C}$ is **semi-reduced** if

$$D = \sum_{i=1}^{r} P_i - rP_\infty \quad \exists r$$

where the $P_i \neq P_\infty$ and $P_i \neq \iota(P_j)$ for all $1 \leq i,j \leq r$.

A semi-reduced divisor D as above is **reduced** if $r \leq g$.

R–R: each divisor class contains a unique reduced divisor.

Let $D : P_1 + \cdots + P_r - rP_\infty$ be a semi-reduced divisor. The **Mumford representation** of D (and of $[D]$) is

$$(a(x), y - b(x))$$

where $a(x) = \prod_{i=1}^{r}(x - x(P_i))$,
$\deg b < r$, and $b(P_i) = y(P_i)$ for all $1 \le i \le r$.
Reduced if $r \le g$.

Note: a, b are in $\mathbb{F}_{q^k}[x]$ iff $[D] \in \mathrm{Pic}^0(\mathscr{C})(\mathbb{F}_{q^k})$.

Theorem: $\{\text{reduced Mumford ideals}\} \longleftrightarrow \mathrm{Pic}^0(\mathscr{C})$.
and the bijection is compatible with Frobenius.

Group Structure

$$J_{\mathscr{C}}(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \cdots \times \mathbb{Z}/d_{2g}\mathbb{Z}$$

with $d_1 | d_2 | \cdots | d_{2g}$.

Geometrically (over $\overline{\mathbb{F}}_q$), if $\ell \neq p$ is prime then

$$J_{\mathscr{C}}(\overline{\mathbb{F}}_q)[\ell^k] \cong (\mathbb{Z}/\ell^k\mathbb{Z})^{2g}$$

and

$$J_{\mathscr{C}}(\overline{\mathbb{F}}_q)[p^k] \cong (\mathbb{Z}/p^k\mathbb{Z})^r \quad \text{where } 0 \leq r \leq g.$$

All that's missing is the group law...
How do we "add" Mumford representatives of divisor classes on

$$\mathscr{C} : y^2 + h(x)y = f(x)?$$

Algorithm: Cantor Composition

- **Input**:
  $[D_1] = (a_1(x), y - b_1(x)), [D_2] = (a_2(x), y - b_2(x))$
1. Use the extended Euclidean algorithm to compute polynomials d, u_1, u_2, and u_3 such that
   $d = \gcd(a_1, a_2, b_1 + b_2 + h) = u_1 a_1 + u_2 a_2 + u_3(b_1 + b_2 + h)$.
2. Set $a_3 := a_1 a_2 / d^2$;
3. Set $b_3 := b_1 + (u_1 a_1 (b_2 - b_1) + u_3 (f - b_1^2 - b_1 h))/d \pmod{a_3}$
- **Output**: $[D_1 + D_2] = (a_3(x), y - b_3(x))$

How do we turn a semi-reduced divisor class on

$$\mathscr{C} : y^2 + h(x)y = f(x)$$

into a reduced divisor class?

Algorithm: Cantor Reduction

- **Input**: $(a(x), y - b(x))$ (semi-reduced)

1 set $\widetilde{a} := a$ and $\widetilde{b} := b$;

2 set $a := (f - bh - b^2)/a$;

3 set $Q, b := \text{Quotrem}(-b - h, a)$;

4 while $\deg a > g$ do

  4a set $t := \widetilde{a} + Q(b - \widetilde{b})$;

  4b set $\widetilde{b} := b, \widetilde{a} := a, a := t$;

  4c set $(Q, b) := \text{Quotrem}(-b - h, a)$;

- **Output** $(a(x), y - b(x))$ **reduced**.

Summary

- **Hyperelliptic** $\mathscr{C} : y^2 + h(x)y = f(x)$ of genus g
- $\Longrightarrow$ **Jacobian** $J_{\mathscr{C}} \cong \mathrm{Pic}^0(\mathscr{C})$,
  a g-dimensional geometric abelian group;
- **Elements**: reduced Mumford $(a(x), y - b(x))$
- **Group law**: Cantor composition + Cantor reduction
- **Group structure**: $d_1 | d_2 | \cdots | d_{2g}$ s.t.

$$J_{\mathscr{C}}(\mathbb{F}_{q^k}) \cong \prod_{i=1}^{2g} (\mathbb{Z}/d_i\mathbb{Z})$$

- **Group order** (Weil bounds): $\#J_{\mathscr{C}}(\mathbb{F}_q) \sim O(q^g)$;

$$(q^{k/2} - 1)^{2g} \leq \#J_{\mathscr{C}}(\mathbb{F}_{q^k}) \leq (q^{k/2} + 1)^{2g}$$

- $\Longrightarrow$ can trade off g vs q for same order.

A *homomorphism* of Jacobians is a (geometric) morphism $J_{\mathscr{C}} \to J_{\mathscr{D}}$ that respects the group laws on $J_{\mathscr{C}}$ and $J_{\mathscr{D}}$.

- This is a much more restrictive definition than for homomorphisms $J_{\mathscr{C}}(\mathbb{F}_{q^k}) \to J_{\mathscr{D}}(\mathbb{F}_{q^k})$.
- "Geometric morphism" = defined by polynomials.
  $\implies$ can compute images without solving discrete logs.

Any morphism $J_{\mathscr{C}} \to J_{\mathscr{D}}$ that maps $0_{J_{\mathscr{C}}}$ to $0_{J_{\mathscr{D}}}$ is automatically a homomorphism.

Torelli: $\mathscr{C} \cong \mathscr{D}$ if and only if $J_{\mathscr{C}} \cong J_{\mathscr{D}}$.

Isogenies

An **isogeny** is a (geometrically) surjective homomorphism *with finite kernel*.

An isogeny $\phi : J_{\mathscr{C}} \to J_{\mathscr{D}}$ is defined over $\mathbb{F}_{q^k}$ if and only if $\ker\phi$ is defined over $\mathbb{F}_{q^k}$ (not necessarily $\ker\phi \subset J_{\mathscr{C}}(\mathbb{F}_{q^k})$!)

Isogenies generally act as isomorphisms for DLPs

Tate's theorem: There exists an isogeny $\phi : J_{\mathscr{C}} \to J_{\mathscr{D}}$ over $\mathbb{F}_{q^k}$ if and only if $\#\mathscr{C}(\mathbb{F}_{q^{ik}}) = \#\mathscr{D}(\mathbb{F}_{q^{ik}})$ for $1 \leq i \leq g$.

- This is not constructive: we don't even know $\deg\phi$...

Consider the elliptic curves

$$\begin{aligned} \mathscr{C}: &\quad y^2 = (x^2 + b_1 x + b_0)(x - a) \\ \mathscr{D}: &\quad y^2 = x^3 + -(4a + 2b_1)x^2 + (b_1^2 - 4b_0)x \end{aligned}$$

We have an isogeny $\phi : \mathscr{C} \longrightarrow \mathscr{D}$ defined by

$$\phi : (x, y) \longmapsto \left(\frac{x^2 + b_1 x + b_0}{x - a}, \frac{(x^2 - (2a)x - (b_1 a + b_0))y}{(x - a)^2} \right).$$

- $\ker \phi = \langle (a, 0) \rangle$ (note $(a, 0)$ has order 2).
- $\mathscr{D}$ is the **quotient** of $\mathscr{C}$ by $\langle (a, 0) \rangle$.
- the denominators of the functions defining ϕ correspond to the kernel of ϕ.

For elliptic curves, isogenies are just (nonconstant) morphisms of elliptic curves mapping infinity to infinity.

When $g > 1$, homomorphisms $J_{\mathscr{C}} \to J_{\mathscr{D}}$ generally *do not* come from morphisms $\mathscr{C} \to \mathscr{D}$.

But if $\mathscr{C} \to \mathscr{D}$ is a nontrivial mapping (a covering), then we have an injection $J_{\mathscr{D}} \to J_{\mathscr{C}}$.
That is, $J_{\mathscr{D}}$ is a "subvariety" of $J_{\mathscr{C}}$.

Problem

Surjective homomorphisms are determined (up to $\cong$)
by their kernels.
So we should be able to take quotients of Jacobians
by finite subgroups...

But in general, *the quotient is not a Jacobian!*

Another example: let $\mathscr{C} \to \mathscr{D}$ be a nonconstant morphism,
where $\mathscr{C}$ has genus 5 and $\mathscr{D}$ has genus 1.

We have an injection $J_{\mathscr{D}} \to J_{\mathscr{C}}$,
so we would hope to use this to decompose $J_{\mathscr{C}}$:
that is, we want an isogeny $J_{\mathscr{D}} \times A \to J_{\mathscr{C}}$ for some group A.

But generally, A is not a Jacobian—so what is it?

3: *Abelian Varieties*

When the going gets weird, the weird turn pro.
—Hunter S. Thompson

Abelian Varieties

An abelian variety (AV) is a projective algebraic group.

- Automatically commutative
- Embedding in projective space typically complicated
- Watch out for polarizations...

Every AV is a quotient of a Jacobian.

AVs are powerful theoretical devices;
to compute with them, we use

- curves (and Picard groups)
- or theta functions.

If we have an injection $A \subset B$ of AVs,
then A is an **abelian subvariety** of B.

$\exists$ isogeny $B \to A \times C$
for some *complementary* abelian subvariety $C \subset B$
(with $A \cap C$ finite)
We say B is *reducible* or *split*.

A is *irreducible* or *simple* if it has no abelian subvarieties.

- Generic AVs are simple: split AVs are special.
- We tend to prefer simple AVs for DLP-based systems (otherwise map DLPs into the smaller subvarieties...)

Universal Property of the Jacobian

If $\phi : \mathscr{C} \to A$ is a morphism from a curve into an AV, then ϕ factors through $J_{\mathscr{C}}$:
that is, $\exists \phi' : J_{\mathscr{C}} \to A$ and $\iota : \mathscr{C} \to J_{\mathscr{C}}$ such that $\phi = \phi' \circ \iota$.

- Torelli's theorem: $\cong$ of curves $\iff$ $\cong$ of Jacobians.
- $\mathscr{C}$ embeds (canonically*) in $J_{\mathscr{C}}$
- $\mathscr{C}$ generates $J_{\mathscr{C}}$
- $g-1$ copies of $\mathscr{C}$ $\longrightarrow$ divisor on $J_{\mathscr{C}}$ called Θ.

Weil restrictions

Recall that $\mathbb{C}^g \cong \mathbb{R}^{2g}$ *(restriction of scalars)*.
A similar construction exists for AVs:
If A is a g-dimensional AV over $\mathbb{F}_{q^k}$, then
there exists a kg-dimensional AV W such that

$$W(\mathbb{F}_q) \cong A(\mathbb{F}_{q^k})$$

So we can trade extension degree for group dimension.

Weil descent attack

If $\mathscr{C}$ is an elliptic curve over $\mathbb{F}_{q^k}$,
and look for a nice curve $\mathscr{D}$ in its Weil restriction $W/\mathbb{F}_q$.
By the universal property, $J_{\mathscr{D}}$ maps into W.
With luck: solve DLP in $J_{\mathscr{D}}(\mathbb{F}_q)$.

Lots of curves of genus g over $\mathbb{F}_q \implies$ lots of groups.
Which ones should we use?

Bigger genus $\implies$ smaller fields.
Which genus should we use?

What about the base field $\mathbb{F}_q$? Does it matter?
Yes: Weil descent, extensions, pairings, ...

Ultimate question:
Why is the generic ECDLP over a prime field so hard?