Isogenies for the Cryptology : methods and applications

L. De Feo

École Polytechnique, Paris, France

February 25, 2009
dipartimento di Matematica
Università di Pisa

Public key Cryptography

Doing crypto with **no shared secret**

Public key encryption

$$\boxed{\text{known only by Alice}} \longrightarrow sk, \quad pk \longleftarrow \boxed{\text{known by everyone}}$$

Alice **Bob**

- m cleartext,
- encryption $c = E_{pk}(m)$,

$$\xleftarrow[\text{public channel}]{c}$$

- decryption $D_{sk}(c) = m$.

Security

- It must be *computationally hard* to deduce sk from pk,
- it must be *computationally hard* to deduce m or sk from (c, pk),
- etc…
- Many hard problems come from number theory.

RSA

The protocol

- p, q two equally large random primes, $N = pq$,
- Secret key p, q and $d \in (\mathbb{Z}/\varphi(N)\mathbb{Z})^*$,
- Public key N and $e = d^{-1} \bmod \varphi(N)$.
- Encryption = Decryption = modular exponentiation : $m = c^d = (m^e)^d$,

Security

- Factor $N \Rightarrow$ compute $\varphi(N) \Rightarrow$ compute $d = e^{-1} \mod \varphi(N) \Rightarrow$ break RSA.
- Breaking RSA $\overset{?}{\Rightarrow}$ Factorisation.
- Factorisation is subexponential by MQS, ECM, NFS.
- RSA-576 broken in 2003, RSA-640 broken in 2005,
- currently many systems use RSA-1024
- RSA-2048 is currently recommended by RSA,
- NIST recommends to switch to ECC-256.

Diffie-Hellman key agreement

The protocol

Alice **Bob**

A cyclic group $\mathcal{G} = \langle g \rangle$,

- picks a at random, computes g^a
- picks b at random, computes g^b

$$\xrightarrow{\quad g^a \quad}$$

$$\xleftarrow{\quad g^b \quad}$$

- computes $K_{ab} = \left(g^b\right)^a$
- computes $K_{ab} = \left(g^a\right)^b$

Security

- Discrete log $\Rightarrow$ DH, DH $\overset{?}{\Rightarrow}$ Discrete log
- $\#\mathcal{G}$ must have a large prime factor,
- $O\left(\sqrt{\#\mathcal{G}}\right)$ attacks : Pollard rho, BSGS,
- subexponential attacks : NFS ($\mathcal{G} = (\mathbb{Z}/n\mathbb{Z})^*$),
- polynomial attacks : quantum computing.

Algebraic curves

Algebraic curves

- (Non-singular) Projective varieties of dimension 1,
- $\mathrm{Pic}^0(C)$ isomorphic to the *Jacobian* $\mathrm{Jac}(C)$,
- classified by topological genus g,
- $C(\mathbb{C})$ is isomorphic to the complex g-torus.

Jacobians over finite fields

- $\mathrm{Jac}(C)$ is an abelian variety of dimension g,
- group law induced by group law on the *divisors* $\mathrm{Div}(C)$,
- the number of *rational points* over $\mathbb{F}_q$ of $\mathrm{Jac}(C)$ is finite,
- $\mathrm{Jac}_{\mathbb{F}_q}(C)$ **is a finite group**.

Figure: the 2-torus

Hyperelliptic curves

Imaginary hyperelliptic curves

- Plane curves ($C \subset \mathbb{P}^2(\mathbb{K})$) of genus g,
- $C \ : \ Y^2 = X^{2g+1} + h(X)Y + f(X)$
- efficient representation of $\mathrm{Jac}_{\mathbb{K}}(C)$ and group law via Mumford coordinates.

Special case: elliptic curves

- genus 1,
- $E \ : \ Y^2 = X^3 + aX + b$,
- $\mathrm{Jac}_{\mathbb{K}}(E) \simeq E(\mathbb{K})$,
- group law by chord-tangent.

Theorem (Hasse-Weil bound)

$$(\sqrt{q} - 1)^{2g} \leqslant \# \mathrm{Jac}_{\mathbb{F}_q}(C) \leqslant (\sqrt{q} + 1)^{2g}$$

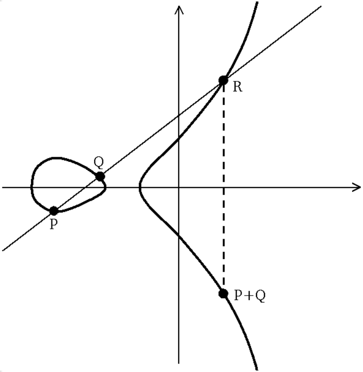


Figure: point addition on an elliptic curve

Arithmetics of elliptic curves

j-invariant

$$j(E) = \frac{1728(4a)^3}{16(4a^3 + 27b^2)}$$

Two elliptic curves are isomorphic over $\mathbb{C}$ iff they have the same j-invariant.

Multiplication

- $[m]P = \underbrace{P + P + \cdots + P}_{m \text{ times}}$ $\qquad [m](X,Y) = \left(\frac{\phi_m(X,Y)}{\psi_m^2(X,Y)}, \frac{\omega_m(X,Y)}{\psi_m^3(X,Y)}\right)$
- ψ_m is the m-division polynomial, $\deg_X \psi^2 \approx m^2$

Torsion

- $E[m] \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ if m prime to the characteristic p
- $E[p^k] \cong \begin{cases} \mathbb{Z}/p^k\mathbb{Z} & \textit{ordinary} \text{ case} \\ \{\mathcal{O}\} & \textit{supersingular} \text{ case} \end{cases}$

Counting points I: Schoof's algorithm

Theorem (Hasse)

- *E defined over $\mathbb{F}_q$,*
- *$\varphi : (X,Y) \mapsto (X^q, Y^q)$ is the Frobenius morphism,*
- *its minimal polynomial is $\varphi^2 - [t] \circ \varphi + [q]$,*
- *then $\#E(\mathbb{F}_q) = q + 1 - t$.*

Computing t ([Schoof '95])

- Modular algorithm: compute $t \bmod \ell$ for small primes $\ell < O(\log q)$ and compose by CRT.
- Let $P \in E[\ell]$, then $$\psi_\ell(P) = 0$$ $$\varphi^2(P) + [q \bmod \ell]P = [t \bmod \ell]\varphi(P)$$
- try all $t \in [0, \ldots, \ell - 1]$ until the equation is verified,
- to keep complexity low, work modulo the ℓ-division polynomial.
- Can be generalised to hyperelliptic jacobians.

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $I(X,Y) = \left(\frac{a(X,Y)}{b(X,Y)}, \frac{c(X,Y)}{d(X,Y)}\right)$,
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^*\bar{\mathbb{K}}(E)]$,
- separable, inseparable, purely inseparable like $\bar{\mathbb{K}}(E')/\mathcal{I}^*\bar{\mathbb{K}}(E)$,
- group morphism: $I(P+Q) = \mathcal{I}(P) + \mathcal{I}(Q)$, $\mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Multiplication

$$\begin{aligned}[m] : E(\bar{\mathbb{K}}) &\to E(\bar{\mathbb{K}}) \\ P &\mapsto [m]P\end{aligned}$$

separable if $(m,p) = 1$, $\deg[m] = m^2$, $\ker \mathcal{I} = E[m]$,

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $I(X,Y) = \left(\frac{a(X,Y)}{b(X,Y)}, \frac{c(X,Y)}{d(X,Y)}\right)$,
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)]$,
- separable, inseparable, purely inseparable like $\bar{\mathbb{K}}(E')/\mathcal{I}^* \bar{\mathbb{K}}(E)$,
- group morphism: $I(P+Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Small Frobenius map

$$\begin{aligned} \varphi_p : E(\bar{\mathbb{K}}) &\rightarrow E^{(p)}(\bar{\mathbb{K}}) \\ (X,Y) &\mapsto (X^p, Y^p) \end{aligned}$$

where $E^{(p)} \ : \ Y^2 + = X^3 + a^p X + b^p$ if $p = \mathrm{char}(\mathbb{K})$,
purely inseparable, $\deg \varphi_p = p$, $\ker \varphi_p = \{\mathcal{O}\}$.

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $I(X,Y) = \left(\frac{a(X,Y)}{b(X,Y)}, \frac{c(X,Y)}{d(X,Y)}\right)$,
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^*\bar{\mathbb{K}}(E)]$,
- separable, inseparable, purely inseparable like $\bar{\mathbb{K}}(E')/\mathcal{I}^*\bar{\mathbb{K}}(E)$,
- group morphism: $I(P+Q) = \mathcal{I}(P) + \mathcal{I}(Q)$, $\mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Frobenius endomorphism

$$\begin{aligned} \varphi_q : E(\bar{\mathbb{K}}) &\to E(\bar{\mathbb{K}}) \\ (X,Y) &\mapsto (X^q, Y^q) \end{aligned}$$

if $\mathbb{K} = \mathbb{F}_q$ then $E^{(q)} = E$,
purely inseparable, $\deg \varphi_q = q$, $\ker \varphi_q = \{\mathcal{O}\}$.

Isogenies

$$E(\bar{\mathbb{K}}) \xrightarrow{\mathcal{I}} E'(\bar{\mathbb{K}})$$

Isogeny

- Rational map: $I(X,Y) = \left(\frac{a(X,Y)}{b(X,Y)}, \frac{c(X,Y)}{d(X,Y)}\right)$,
- onto, finite kernel, $\deg \mathcal{I} = [\bar{\mathbb{K}}(E') : \mathcal{I}^* \bar{\mathbb{K}}(E)]$,
- separable, inseparable, purely inseparable like $\bar{\mathbb{K}}(E')/\mathcal{I}^*\bar{\mathbb{K}}(E)$,
- group morphism: $I(P+Q) = \mathcal{I}(P) + \mathcal{I}(Q), \quad \mathcal{I}(\mathcal{O}_E) = \mathcal{O}_{E'}$

Examples

Separable isogenies

$$\mathcal{I}(X,Y) = \left(\frac{g(X)}{h^2(X)}, Y\left(\frac{g(X)}{h^2(X)}\right)'\right)$$

separable, $\deg \mathcal{I} = \# \ker \mathcal{I} \approx \deg h$.

Dual isogeny

$$\begin{tikzcd} E \arrow[r, "\mathcal{I}"] \arrow[dr, "{[m]}"'] & E' \arrow[d, "\hat{\mathcal{I}}"] \\ & E \end{tikzcd}$$

Theorem (Dual isogeny)

$\mathcal{I}$ of degree m, there is an unique dual isogeny $\hat{\mathcal{I}}$ s.t.

$$\hat{\mathcal{I}} \circ \mathcal{I} = [m]_E$$

$$\mathcal{I} \circ \hat{\mathcal{I}} = [m]_{E'}$$

Examples

- $[p] = V \circ \varphi_p$, $\quad V$ separable,
- m prime to p, $\quad [m] = \hat{\mathcal{I}} \circ \mathcal{I} \quad$ separable.

Intermezzo: Index calculus (or why are large genus curves bad)

Mumford representation

Elements of $\mathrm{Jac}(C)$ are represented as

$$(a(X), b(X)) \in \mathbb{K}[X] \times \mathbb{K}[X], \qquad \deg b < \deg a \leqslant g$$

Let B be an integer, elements s.t. $\deg a \leqslant B$ are called B-smooth.

Index calculus

Given $D_1 \in \mathrm{Jac}(C)$, $D_2 \in \langle D_1 \rangle$, find λ s.t. $D_2 = [\lambda]D_1$.

- Chose B *large enough*,
- random walk $D_i = \alpha_i D_1 + \beta_i D_2$, store D_i if B-smooth,
- when enough smooth divisors, compute by linear algebra $\alpha D_1 + \beta D_2 = 0$,
- then $\lambda = -\frac{\alpha}{\beta} \bmod \#\langle D_1 \rangle$.

Theorem ([Enge, Stein '02])

If $B = O(\log L(\frac{1}{2}, \rho))$, then the ratio of B-smooth divisors is $L(1/2, O(-1/\rho))$.

Applications I : Breaking discrete logs

DLP reductions

- A curve C_1 with hard DLP and an instance (g, h) ,
- a curve C_2 with easy DLP,
- an isogeny $\mathcal{I} : C_1 \rightarrow C_2$ which kernel does not contain g,
- bring the DLP in C_2 via $\mathcal{I}$ and solve it.

GHS ([Gaudry, Hess, Smart '02])

- E elliptic curve defined over $\mathbb{F}_{2^{nk}}$,
- $\mathrm{Res}(E)$ abelian variety of dimension n defined over $\mathbb{F}_{2^k}$, group isomorphic to E,
- C hyperelliptic curve of genus g,
- $\phi : \mathrm{Jac}_{\mathbb{F}_{2^k}}(C) \rightarrow \mathrm{Res}(E)$,
- lift DLP via ϕ, solve by index calculus.

Genus 3 curves ([Smith '08])

- H hyperelliptic curve of genus 3,
- C non-hyperelliptic smooth plane quartic of genus 3,
- $\phi : \mathrm{Jac}(H) \rightarrow \mathrm{Jac}(C)$,
- DLP in C is easier,
- works for 18.57% of all genus 3 hyperelliptic curves.

Applications II : key escrow cryptosystem

Key escrow

Escrow authority	**Alice**	**Bob**
Escrow key	Secret key	Public key
	$\xleftarrow{\text{encrypted message}}$	
decrypts with escrow key	decrypts with secret key	

Time of escrow key decryption $\gg$ time of secret key decryption.

Elliptic curve trapdoor system ([Teske '06])

- Secret key: E_p, elliptic curve not vulnerable to GHS + ECC secret key
- Public key: E_p + ECC public key,
- Escrow key: E_s, vulnerable to GHS attack, $\mathcal{I} : E_s \to E_p$.

Intermezzo: Modular polynomials

Theorem

Let H be a $\mathbb{K}$-rational finite subgroup of E, then there is an unique curve E' defined over $\mathbb{K}$ and a separable isogeny $\mathcal{I} : E \to E'$ having kernel H.

$$0 \longrightarrow H \longrightarrow E \xrightarrow{\mathcal{I}} E' \longrightarrow 0$$

We note E/H for E'.

Modular polynomial $\Phi_\ell(X, Y)$

- $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ contains $\ell + 1$ cyclic subgroups of order ℓ,
- there are $\ell + 1$ elliptic j-invariants (not necessarily in $\mathbb{K}$) ℓ-isogenous to E,
- $\Phi_\ell(X, Y)$: minimal polynomial of the *modular function* $j(\ell\tau)$,
- $\Phi_\ell(j(E), j(E')) = 0$ iff E and E' are ℓ-isogenous,
- $\deg \Phi_\ell = \ell + 1$, (huge) integer coefficients, still useful modulo p.

Counting points II : SEA (see [Schoof '95])

Schoof

- $\varphi^2 - [t] \circ \varphi + [q] = 0$, compute $t \bmod \ell$ for primes $< O(\log q)$,
- computations done modulo division polynomial of degree $O(\ell^2)$.

Elkies

- $E[\ell]$ contains subgroups E_i of order ℓ,
- if E_1 defined over $\mathbb{K}$, find isogenous curve E/E_1,
- compute $\mathcal{I} : E \to E/E_1$, then $\deg \mathcal{I} = O(\ell)$,
- consider φ_{E_1} to find $t \bmod \ell$, computations done modulo $\mathcal{I}$.
- Works for half of the primes.

Atkin

- Works for the other half of primes,
- uses simpler equation (in a field extension) $\varphi_{E_1} = [k]_{E_1}$.

Computing isogenies

Which problem?

- Velu's formulae: being given the points of the kernel, it is an easy task to compute the isogeny, than the curve E'.
- SEA case: harder to find the kernel (and the isogeny), being given E'.

Large characteristic (see [Bostan, Morain, Salvy, Schost 08])

'92	Elkies	$O(\ell^2)$
'92	Atkin	$O(\ell \mathsf{M}(\ell))$
'98	Elkies	$O(\ell^2)$
'08	Bostan, Morain, Salvy, Schost	$O(\mathsf{M}(\ell))$

Small characteristic

'94	Couveignes I	$O(\ell^3)$
'96	$p = 2$, Lercier	$O(\ell^3)$
'96	Couveignes II (+ [D.F. '07])	$O(\ell \mathsf{M}_{\mathsf{pol}}(\ell))$

Computing isogenies: Couveignes II

Interpolating an isogeny

- G a *large enough* subgroup,
- G' its image by $\mathcal{I}$,
- interpolate over the points of G,
- deduce the isogeny by rational reconstruction.

$$E(\bar{\mathbb{F}}_q) \supset G \xrightarrow{\quad\mathcal{I}\quad} G' \subset E'(\bar{\mathbb{F}}_q)$$

$$\Downarrow$$

$$A(X_P) = A(X_{P'}) \quad \text{for every } P \in G,\ P' = \mathcal{I}(P)$$

$$\Downarrow$$

$$\frac{g(X)}{h^2(X)}$$

G is chosen to be $E[p^k]$

Intermezzo : p-torsion of ordinary elliptic curves

p^k-torsion

- $E[p^k]$ cyclic group isomorphic to $\mathbb{Z}/p^k\mathbb{Z}$,
- $\mathcal{I}(E[p^k]) = E'[p^k]$ if $(\ell, p) = 1$,
- points not necessarily defined over $\mathbb{K}$.

p^k-torsion tower

$(\mathbb{K} = \mathbb{U}_0, \dots, \mathbb{U}_k)$ is the tower of field extensions of minimal degree s.t. for any i

$$E[p^i] \subset E(\mathbb{U}_i).$$

Remark (Structure of $(\mathbb{U}_0, \dots, \mathbb{U}_k)$)

There is a i_0 s.t. $\mathbb{U}_{i_0} = \mathbb{U}_0$ and for $i \geqslant i_0$

$$[\mathbb{U}_{i+1} : \mathbb{U}_i] = p,$$

Methods I : Artin-Schreier towers

Definition (Artin-Schreier polynomial)

$\mathbb{K}$ a field of characteristic p, $\alpha \in \mathbb{K}$

$$X^p - X - \alpha$$

is an Artin-Schreier polynomial.

Theorem

$\mathbb{K}$ finite. $X^p - X - \alpha$ irreducible $\Leftrightarrow$ $\mathrm{Tr}_{\mathbb{K}/\mathbb{F}_p}(\alpha) \neq 0$.
If $\eta \in \mathbb{K}$ is a root, then $\eta + 1, \ldots, \eta + (p-1)$ are roots.

Definition (Artin-Schreier extension)

$\mathcal{P}$ an irreducible Artin-Schreier polynomial.

$$\mathbb{L} = \mathbb{K}[X]/\mathcal{P}(X).$$

$\mathbb{L}/\mathbb{K}$ is called an Artin-Schreier extension.

Methods I : Artin-Schreier towers

$$
\begin{array}{l}
\mathbb{U}_k = \frac{\mathbb{U}_{k-1}[X_k]}{P_{k-1}(X_k)} \\
\Big| \, p \\
\mathbb{U}_{k-1} \\
\vdots \\
\mathbb{U}_1 = \frac{\mathbb{U}_0[X_1]}{P_0(X_1)} \\
\Big| \, p \\
\mathbb{U}_0 = \mathbb{F}_{p^d} = \frac{\mathbb{F}_p[X_0]}{Q(X_0)}
\end{array}
$$

Towers over finite fields

$$P_i = X^p - X - \alpha_i$$

We say that $(\mathbb{U}_0, \dots, \mathbb{U}_k)$ is defined by $(\alpha_0, \dots, \alpha_{k-1})$ over $\mathbb{U}_0$.

ANY separable extension of degree p can be expressed this way

Voloch formulae

Given E, compute $(\alpha_0, \dots, \alpha_{k-1})$ that define the p^k-torsion tower of E.

Methods II : Fast arithmetics in Artin-Schreier towers

$$\begin{array}{c} \mathbb{U}_k \\ | \\ \mathbb{U}_{k-1} \\ \vdots \\ \mathbb{U}_1 \\ | \\ \mathbb{U}_0 \end{array}$$

Primitive towers ([D.F., Schost '09])

- Find special towers s.t. $\mathbb{U}_i = \mathbb{F}_p[X_i]$, where $X_i^p - X_i - \alpha_{i-1} = 0$,
- use polynomial basis to perform fast arithmetics (FFT multiplication, Newton inversion, etc.),
- generalise to any tower using isomorphism algorithms.

Level embedding ([D.F., Schost '09])

- Express the morphisms between the levels to switch back to the multivariate representation.
- Going down is easy: bivariate reduction modulo $X_i^p - X_i - \alpha_{i-1}$.
- Going up much harder:
  - trace formulae,
  - truncated power series arithmetics,
  - transposition principle.

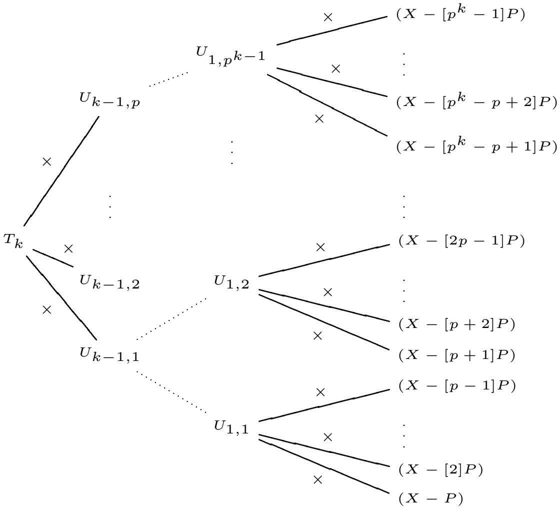
"From every *linear algorithm* computing a linear application we can deduce another *linear algorithm* computing the transpose application using *about* the same space and time resources."

Category theory justification

$$
\begin{tikzcd}
 & {} \arrow[r] & {} \arrow[dr] & & {} \arrow[r] & {} \arrow[dr] & \\
a \arrow[ur] \arrow[rrr, dashed, "f_2"'] \arrow[rrr, phantom, shift left=5ex, "C_2"] & & & b \arrow[ur] \arrow[rrr, dashed, "f_1"'] \arrow[rrr, phantom, shift left=5ex, "C_1"] & & & c
\end{tikzcd}
$$

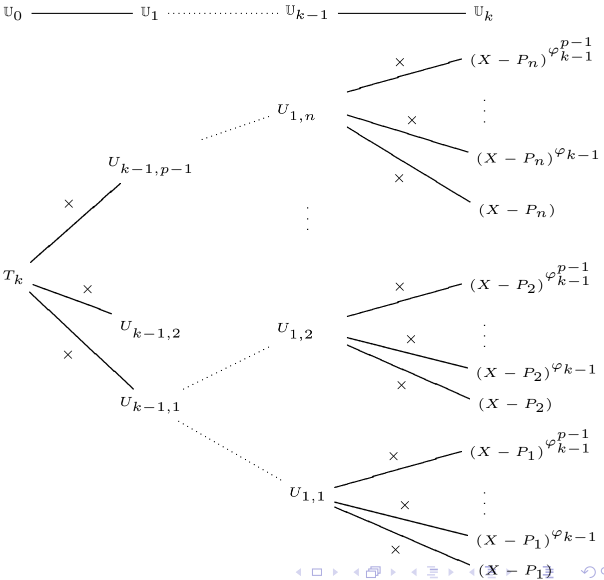
Methods III : beyond fast interpolation ([D.F. '07])

Subproduct tree



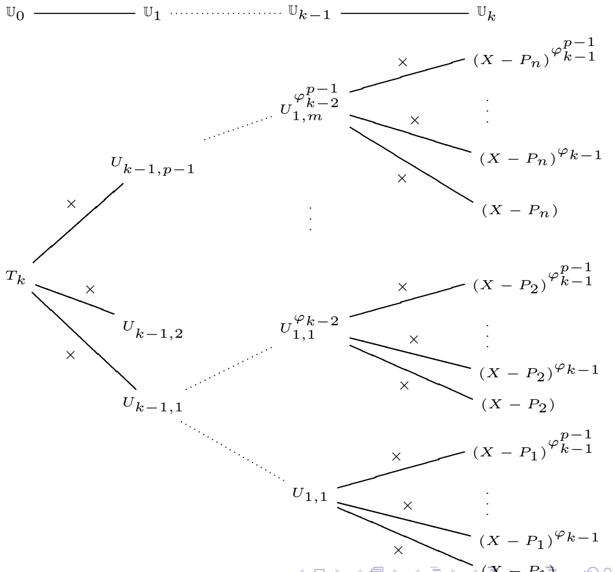
Methods III : beyond fast interpolation ([D.F. '07])

p^k-torsion tree

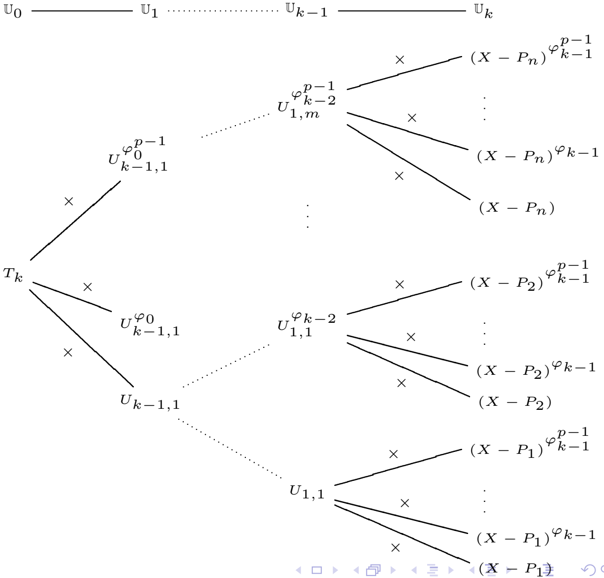


Methods III : beyond fast interpolation ([D.F. '07])

p^k-torsion tree



p^k-torsion tree



Some open problems

Computing isogenies for $g > 1$

- No analog of modular polynomials,
- no general formulas to compute isogenies.

Fast arithmetics for Artin-Schreier towers over function fields

- Analogous construction for primitive towers,
- level embeddings ?
- isomorphisms to general towers ?

Automatic deduction of transposed algorithms

- Semi-automatic techniques already used by hand,
- not yet know to hold for general programming languages,
- is it possible to write a transcompiler ?
- Generalise to other interesting dualities.

Bibliography

I. Blake, G. Seroussi & N. Smart
Elliptic Curves in Cryptography
LMS 265, Cambridge University Press, 1999

(edited by) I. Blake, G. Seroussi & N. Smart
Advances in Elliptic Curve Cryptography
LMS 317, Cambridge University Press, 2005

J.S. Milne.
Elliptic curves.
BookSurge Publishers, ISBN 1-4196-5257-5, 2006.

J.H. Silverman
The Arithmetic of Elliptic Curves
GTM 106, Springer-Verlag, 1986

Bibliography

A. Bostan, F. Morain, B. Salvy, É. Schost.
Fast algorithms for computing isogenies between elliptic curves.
Math. Comp. 77, 263, 1755-1778, 2008.

J.-M. Couveignes.
Computing ℓ-isogenies with the p-torsion.
Lecture Notes in Computer Science vol. 1122, pages 59–65, Springer-Verlag, 1996.

J.-M. Couveignes.
Isomorphisms between Artin-Schreier tower.
Math. Comp. 69(232): 1625–1631, 2000.

L. De Feo.
Calcul d'isogénies.
Master thesis. http://www.lix.polytechnique.fr/∼defeo

L. De Feo & É. Schost.
Fast arithmetics in Artin-Schreier towers over finite fields.
Preprint, 2009.

Bibliography

A. Enge, A. Stein.
Smooth ideals in hyperelliptic function fields.
Math. Comp. 71:1219-1230, 2002.

P. Gaudry, F. Hess, N. P. Smart.
Constructive and destructive facets of Weil descent on elliptic curves.
J. Cryptology 15:19-46, 2002.

R. Schoof.
Counting points on elliptic curves over finite fields.
J. de Théorie des Nombres de Bordeaux, 7:219-254, 1995.

B. Smith.
Isogenies and the Discrete Logarithm Problem in Jacobians of genus 3 hyperelliptic curves.
In *EUROCRYPT '08*, LNCS, 2008.

E. Teske.
Elliptic curve trapdoor system.
J. Cryptology 19:115-133, 2006.