Canonical Lift Methods

Fré Vercauteren

Katholieke Universiteit Leuven

29-30 August 2005

Frobenius Endomorphism

- Let E be an elliptic curve over a finite field $\mathbb{F}_q$ with $q = p^n$
- Recall the q-th power Frobenius endomorphism

$$F_q : E \to E : (x, y) \mapsto (x^q, y^q)$$

- Characteristic polynomial of F_q was of the form

$$\chi(T) = T^2 - \mathrm{Tr}(F_q)T + \mathrm{Deg}(F_q) = T^2 - tT + q = 0$$

and $\#E(\mathbb{F}_q) = \chi(1) = q + 1 - t$

Factorisation of $\chi(T)$ over p-adic's

- $\mathbb{Q}_p$ is field of p-adic numbers, with valuation ring $\mathbb{Z}_p$
- Assume that $t \not\equiv 0 \bmod p$, then

$$\chi(T) \equiv T^2 - tT \equiv T(T - t) \bmod p$$

- Conclusion: $\chi(T)$ splits over $\mathbb{Z}_p$ as

$$\chi(T) = (T - \lambda)(T - \frac{q}{\lambda})$$

  with λ the unique root such that $\lambda \equiv t \bmod p$ (λ is unit)
- Conclusion: $t = \lambda + q/\lambda$, since $|t| \leq 2\sqrt{q}$ only need approximation of λ modulo p^N with $N > n/2 + 2$

How to Compute λ?

- Since $\lambda \in \mathbb{Z}_p$, need to lift the situation to p-adic integers
- Given elliptic curve E over $\mathbb{F}_q$, can we find $\mathcal{E}$ over $\mathbb{Z}_q$ s.t.
- Reduction of $\mathcal{E}$ modulo p equals E
- $\mathcal{E}$ comes with "lifted Frobenius endomorphism $\mathcal{F}_q$" with the same characteristic polynomial

$$\chi(F_q; T) = \chi(\mathcal{F}_q; T)$$

- Assume that we could compute $\mathcal{E}$ and $\mathcal{F}_q$, then how to proceed?

How to Compute λ?

- Let $E : f(x,y) = 0$ over field $\mathbb{K}$, then there exists an invariant differential

$$\omega = \frac{dx}{\partial f / \partial y}$$

- Morphism $\phi : E_1 \to E_2$ induces by pullback a map $\Omega_2 \to \Omega_1$

$$\phi^*(gdh) = \phi^*(g) d\phi^*(h) = (g \circ \phi) d(h \circ \phi)$$

- Invariant: since $\tau_P^* \omega = \omega$
- Linearization: ϕ, ψ 2 isgonies from $E_1 \to E_2$ then

$$(\phi \oplus \psi)^* \omega = \phi^* \omega + \psi^* \omega$$

- Pullback of regular differential by isogeny again regular, so

$$\phi^* \omega = c\omega \, , c \in \mathbb{K}$$

How to Compute λ?

- Since $\mathcal{F}_q$ satisfies $T^2 - tT + q = 0$, the constant $\mathcal{F}_q^* \omega = c\omega$ satisfies
$$c^2 - tc + q = 0$$
- Conclusion: c is either λ or q/λ but which one?
- Use that $\mathcal{F}_q \equiv F_q \bmod p$ and clearly $F_q^* \overline{\omega} \equiv 0 \bmod p$, so
$$c = \frac{q}{\lambda}$$
- Efficiency: would need extra n precision to recover λ and trace t
- Solution: consider the dual $\widehat{\mathcal{F}}_q$ of $\mathcal{F}_q$, then $\widehat{\mathcal{F}}_q^* \omega = \lambda\omega$

Canonical Lift

- The canonical lift $\mathcal{E}$ of an ordinary elliptic curve E over $\mathbb{F}_q$ is an elliptic curve over $\mathbb{Q}_q$ which satisfies:
- the reduction of $\mathcal{E}$ modulo p equals E,
- the ring homomorphism $\mathrm{End}(\mathcal{E}) \to \mathrm{End}(E)$ induced by reduction modulo p is an isomorphism.
- Deuring showed that the canonical lift $\mathcal{E}$ always exists and is unique up to isomorphism.

Canonical Lift: Alternative Characterisation

- $\mathcal{E}$ is the canonical lift of E.
- Reduction modulo p induces an isomorphism $\mathrm{End}(\mathcal{E}) \simeq \mathrm{End}(E)$.
- The q-th power Frobenius $F_q \in \mathrm{End}(E)$ lifts to an endomorphism $\mathcal{F}_q \in \mathrm{End}(\mathcal{E})$.
- The p-th power Frobenius isogeny $F_p : E \to E^\sigma$ lifts to an isogeny $\mathcal{F}_p : \mathcal{E} \to \mathcal{E}^\Sigma$, with Σ the Frobenius substitution.

Conclusion: last property implies that the j-invariant of $\mathcal{E}$ has to satisfy

$$\Phi_p\big(j(\mathcal{E}), \Sigma\big(j(\mathcal{E})\big)\big) = 0$$

Canonical Lift: Lubin-Serre-Tate

- Let E be an ordinary elliptic curve over $\mathbb{F}_q$ with j-invariant $j(E) \in \mathbb{F}_q \setminus \mathbb{F}_{p^2}$.
- Then the system of equations

$$\Phi_p\big(X, \Sigma(X)\big) = 0 \text{ and } X \equiv j(E) \pmod{p},$$

has a unique solution $J \in \mathbb{Z}_q$, which is the j-invariant of the canonical lift $\mathcal{E}$ of E (defined up to isomorphism).

- Example: $\Phi_2(X, Y) = X^3 + Y^3 - X^2Y^2 + 1488(XY^2 + X^2Y) - 162000(X^2 + Y^2) + 40773375XY + 8748000000(X + Y) - 157464000000000$
- When $j(E) \in \mathbb{F}_{p^2}$, then isomorphic to curve over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$, so can use simple enumeration.

Canonical Lift: Satoh's Algorithm

- To compute $j(\mathcal{E}) \bmod p^N$, Satoh considered E together with all its conjugates $E_i = E^{\sigma^i}$ with $0 \leq i < n$
- Let $F_{p,i}$ denote the p-th power Frobenius isogeny, then

$$E_0 \xrightarrow{F_{p,0}} E_1 \xrightarrow{F_{p,1}} \cdots \xrightarrow{F_{p,n-2}} E_{n-1} \xrightarrow{F_{p,n-1}} E_0.$$

- Satoh lifts cycle $(E_0, E_1, \ldots, E_{n-1})$ simultaneously

$$\begin{tikzcd}
\mathcal{E}_0 \arrow[r, "\mathcal{F}_{p,0}"] \arrow[d, "\pi_1"'] & \mathcal{E}_1 \arrow[r, "\mathcal{F}_{p,1}"] \arrow[d, "\pi_1"'] & \cdots \arrow[r, "\mathcal{F}_{p,n-2}"] & \mathcal{E}_{n-1} \arrow[r, "\mathcal{F}_{p,n-1}"] \arrow[d, "\pi_1"'] & \mathcal{E}_0 \arrow[d, "\pi_1"'] \\
E_0 \arrow[r, "F_{p,0}"] & E_1 \arrow[r, "F_{p,1}"] & \cdots \arrow[r, "F_{p,n-2}"] & E_{n-1} \arrow[r, "F_{p,n-1}"] & E_0,
\end{tikzcd}$$

Canonical Lift: Weierstrass Model

$$
\begin{array}{lcll}
p = 2 & : & y^2 + xy = x^3 + a_6, & j(E) = 1/a_6 \\
p = 3 & : & y^2 = x^3 + x^2 + a_6, & j(E) = -1/a_6 \\
p > 5 & : & y^2 = x^3 + 3ax + 2a, & j(E) = 1728a/(1+a)
\end{array}
$$

Given j-invariant $j(\mathcal{E})$ of the canonical lift of E, a Weierstrass model for $\mathcal{E}$ is given by

$$
\begin{array}{lcll}
p = 2 & : & y^2 + xy = x^3 + 36\alpha x + \alpha, & \alpha = 1/\left(1728 - j(\mathcal{E})\right) \\
p = 3 & : & y^2 = x^3 + x^2/4 + 36\alpha x + \alpha, & \alpha = 1/\left(1728 - j(\mathcal{E})\right) \\
p > 5 & : & y^2 = x^3 + 3\alpha x + 2\alpha, & \alpha = j(\mathcal{E})/\left(1728 - j(\mathcal{E})\right)
\end{array}
$$

How to compute λ ?

- From before: the dual $\widehat{\mathcal{F}}_q$ of $\mathcal{F}_q$, then $\widehat{\mathcal{F}}_q^* \omega = \lambda \omega$
- The diagram implies

$$\widehat{\mathcal{F}}_q = \widehat{\mathcal{F}}_{p,0} \circ \widehat{\mathcal{F}}_{p,1} \circ \cdots \circ \widehat{\mathcal{F}}_{p,n-1}$$

- Consider $\omega_i = \omega^{\Sigma^i}$ for $0 \leq i < n$ and let c_i be defined by

$$\widehat{\mathcal{F}}_{p,i}^*(\omega_i) = c_i \, \omega_{i+1},$$

- Conclusion: $\lambda = \prod_{0 \leq i < d} c_i$
- Commutative squares are conjugates, so $c_i = \Sigma^i(c_0)$ and

$$\lambda = \mathrm{No}_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0)$$

How to compute c_0 ?

$$\begin{tikzcd} \mathcal{E}_1 \arrow[rr, "\widehat{\mathcal{F}}_{p,0}"] \arrow[dr, "\nu_0"'] & & \mathcal{E}_0 \\ & \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \arrow[ur, "\lambda_0"'] & \end{tikzcd}$$

- Know equations of $\mathcal{E}_0$ and $\mathcal{E}_1$, assume we know $\mathrm{Ker}\widehat{\mathcal{F}}_{p,0}$
- Vélu's formulas: compute an equation of $\mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ and isogeny ν_0
- Since $\mathrm{Ker}(\nu_0) = \mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$, there exists an isomorphism $\lambda_0 : \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \to \mathcal{E}_0$ that makes diagram commutative

How to compute c_0 ?

$$
\begin{tikzcd}
\mathcal{E}_1 \arrow[rr, "\widehat{\mathcal{F}}_{p,0}"] \arrow[dr, "\nu_0"'] & & \mathcal{E}_0 \\
& \mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \arrow[ur, "\lambda_0"'] &
\end{tikzcd}
$$

- Vélu's construction: choses holomorphic differential such that action of ν_0 is trivial
- Conclusion: it is sufficient to compute the action of λ_0 on ω_0

Computing $\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$?

- Note that $\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ is a subgroup of order p of $\mathcal{E}_1[p]$.
- Let $H_0(x)$ be $H_0(x) = \prod_{P \in (\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0}) \setminus \{\mathcal{O}\})/\pm} (x - x(P))$
- $H_0(x)$ divides the p-division polynomial $\Psi_{p,1}(x)$ of $\mathcal{E}_1$
- Lemma: $H_0(x) \in \mathbb{Z}_q[x]$ is the unique monic polynomial that divides $\Psi_{p,1}(x)$ and such that $H_0(x)$ is squarefree modulo p of degree $(p-1)/2$
- Need to modifiy Hensel since reduction mod p of $H_0(x)$ not coprime with $\Psi_{p,1}$

How to compute c_0?

- For $p > 3$, $\mathcal{E}_1$ has equation $y^2 = x^3 + a_1 x + b_1$
- Vélu: $\mathcal{E}_1/\mathrm{Ker}(\widehat{\mathcal{F}}_{p,0})$ has equation $y^2 = x^3 + \alpha_1 x + \beta_1$

$$\alpha_1 = (6 - 5p)a_1 - 30(h_{0,1}^2 - 2h_{0,2})$$
$$\beta_1 = (15 - 14p)b_1 - 70(-h_{0,1}^3 + 3h_{0,1}h_{0,2} - 3h_{0,3}) + 42a_1 h_{0,1}$$

where $h_{0,k}$ is coefficient of $x^{(p-1)/2-k}$ in $H_0(x)$

- λ_0 to $\mathcal{E}_0 : y^2 = x^3 + a_0 x + b_0$ is $\lambda_0 : (x, y) \to (u_0^2 x, u_0^3 y)$ with

$$u_0^2 = \frac{\alpha_1}{\beta_1}\frac{b_0}{a_0}$$

- Let $\omega_0 = dx/y$ then $\lambda_0^*(\omega_0) = u_0^{-1}\omega_{1,K}$ with $\omega_{1,K} = dx/y$
- Conclusion: $c_0 = u_0^{-1}$

Satoh's Algorithm: Example

- Let $p = 5$, $d = 7$, $\mathbb{F}_{p^d} \simeq \mathbb{F}_p(\theta)$ with $\theta^7 + 3\theta + 3 = 0$
- Elliptic curve $E : y^2 = x^3 + x + a_6$

$$a_6 = 4\theta^6 + 3\theta^5 + 3\theta^4 + 3\theta^3 + 3\theta^2 + 3.$$

- The j-invariant of canonical lift with precision 6 then is

$$J_0 \equiv 6949T^6 + 6806T^5 + 14297T^4 + 2260T^3 + 13542T^2 + 13130T + 15215,$$

with $\mathbb{Z}_q \simeq \mathbb{Z}_p[T]/\big(G(T)\big)$ and $G(T) = T^7 + 3T + 3$.

- Values for a, b of $\mathcal{E} : y^2 = x^3 + ax + b$

$$\begin{aligned} a &\equiv 6981T^6 + 8408T^5 + 1033T^4 + 8867T^3 + 15614T^2 + 3514T + 675 \\ b &\equiv 4654T^6 + 397T^5 + 5897T^4 + 703T^3 + 5201T^2 + 7551T + 450 \end{aligned}$$

Satoh's Algorithm: Example

- Polynomial H describing the kernel of $\mathcal{F}_p$

$$H(x) \equiv x^2 + (1395T^6 + 7906T^5 + 3737T^4 + 9221T^3 + 9207T^2 + 5403T + 7401)x \\ + 6090T^6 + 206T^5 + 5259T^4 + 7576T^3 + 3863T^2 + 8903T + 7926$$

- Recover α and β as

$$\begin{aligned} \alpha &\equiv 11086T^6 + 2618T^5 + 6983T^4 + 13192T^3 + 15324T^2 + 13544T + 10550 \\ \beta &\equiv 4940T^6 + 3060T^5 + 14966T^4 + 6589T^3 + 7934T^2 + 6060T + 12470 \end{aligned}$$

- Norm of $(\alpha b)/(\beta a)$ and taking the square root,

$$\mathrm{Tr}(F_q) = 433 \quad \text{and} \quad |E(\mathbb{F}_{p^d})| = 77693$$

AGM Algorithm

INPUT: Elliptic curve $E : y^2 + xy = x^3 + \overline{c}$ over $\mathbb{F}_{2^d}$
OUTPUT:Trace of Frobenius modulo 2^{N-1}

1. $a \leftarrow 1$ and $b \leftarrow (1 + 8c) \bmod 2^4$ $\quad c$ arbitrary lift of $\overline{c}$
2. **For** $i = 5$ **To** N **Do**
   2.1 $(a, b) \leftarrow ((a + b)/2, \sqrt{ab}) \bmod 2^i$
3. $a_0 \leftarrow a$
4. **For** $i = 0$ **To** $d - 1$ **Do**
   4.1 $(a, b) \leftarrow ((a + b)/2, \sqrt{ab}) \bmod 2^N$
5. $t \equiv \dfrac{a_0}{a} \bmod 2^{N-1}$

AGM over $\mathbb{R}$

- Let $a_0, b_0 \in \mathbb{R}$ with $a_0 \geq b_0 > 0$, then the AGM iteration for $k \in \mathbb{N}$ is defined as

$$(a_{k+1}, b_{k+1}) = \left(\frac{a_k + b_k}{2}, \sqrt{a_k b_k} \right)$$

- Lemma: $\lim a_k = \lim b_k = AGM(a_0, b_0)$
- For $a_k / b_k = 1 + \varepsilon_k$ with $\varepsilon_k < 1$, convergence is quadratic

$$\begin{aligned} \frac{a_{k+1}}{b_{k+1}} &= \frac{a_k + b_k}{2\sqrt{a_k b_k}} = \frac{2 + \varepsilon_k}{2\sqrt{1 + \varepsilon_k}} \\ &= 1 + \frac{\varepsilon_k^2}{8} - \frac{\varepsilon_k^3}{8} + O(\varepsilon_k^4). \end{aligned}$$

AGM over $\mathbb{Z}_q$

- For $c \in 1 + 8\mathbb{Z}_q$, denote by $\sqrt{c}$ the unique element $e \in 1 + 4\mathbb{Z}_q$ with $e^2 = c$.
- Given $a, b \in \mathbb{Z}_q$ with $a/b \in 1 + 8\mathbb{Z}_q$, then $a' = (a+b)/2$ and $b' = b\sqrt{a/b}$ also belong to $\mathbb{Z}_q$ and $a'/b' \in 1 + 8\mathbb{Z}_q$.
- However: the 2-adic AGM sequence will converge if and only if $a/b \in 1 + 16\mathbb{Z}_q$.
- For $a/b \in 1 + 8\mathbb{Z}_q$ the AGM sequence will not converge!
- But: AGM sequence $(a_k, b_k)_{k=0}^{\infty}$ can be used to compute the number of points on an ordinary elliptic curve

Elliptic Curve AGM

- Let $a, b \in 1 + 4\mathbb{Z}_q$ with $a/b \in 1 + 8\mathbb{Z}_q$ and $E_{a,b}$

$$E_{a,b} : y^2 = x(x - a^2)(x - b^2).$$

- Let $a' = (a+b)/2$, $b' = \sqrt{ab}$, then $E_{a,b}$ and $E_{a',b'}$ are 2-isogenous. The isogeny is given by

$$\begin{aligned} \psi : E_{a,b} &\quad\rightarrow\quad E_{a',b'} \\ (x, y) &\quad\longmapsto\quad \left(\frac{(x+ab)^2}{4x}, y\frac{(x-ab)(x+ab)}{8x^2} \right), \end{aligned}$$

- Kernel of ψ is $\langle (0,0) \rangle$.
- The action of ψ on the invariant differential is

$$\psi^* \left(\frac{dx}{y} \right) = 2\frac{dx}{y}.$$

Elliptic Curve AGM: Convergence

- AGM sequence $(a_k, b_k)_{k=0}^{\infty}$ does not converge at all ...
- Theorem: The sequence of elliptic curves E_{a_k,b_k} converges linearly towards the canonical lift $\mathcal{E}$ of E

$$j\left(E_{a_k,b_k}\right) \equiv \Sigma^k\left(j(\mathcal{E})\right) \pmod{2^{k+1}}.$$

- Proof: based on fact that the curves E_{a_k,b_k} and $E_{a_{k+1},b_{k+1}}$ are 2-isogenous, so

$$\Phi_2\left(j(E_{a_k,b_k}), j(E_{a_{k+1},b_{k+1}})\right) = 0$$

Elliptic Curve AGM: Relation with Frobenius

- Assume we have $a, b \in 1 + 4\mathbb{Z}_q$ with $a/b \in 1 + 8\mathbb{Z}_q$ with

$$j(\mathcal{E}_{a,b}) = j(\mathcal{E})$$

- Let $(a', b') = \left((a+b)/2, \sqrt{ab}\right)$, $\psi : \mathcal{E}_{a,b} \to \mathcal{E}_{a',b'}$ the AGM isogeny and $\mathcal{F}_2 : \mathcal{E}_{a,b} \to \mathcal{E}_{\Sigma(a),\Sigma(b)}$ the lift of the 2-nd power Frobenius, then we have the following diagram:

$$\begin{tikzcd}
\mathcal{E}_{a,b} \arrow[rr, "\mathcal{F}_2"] \arrow[dr, "\psi"'] & & \mathcal{E}_{\Sigma(a),\Sigma(b)} \\
& \mathcal{E}_{a',b'} \arrow[ur, "\lambda"'] &
\end{tikzcd}$$

- Can show that $\mathrm{Ker}(\mathcal{F}_2) = \mathrm{Ker}(\psi)$, so exists an isomorphism

$$\lambda : \mathcal{E}_{a',b'} \to \mathcal{E}_{\Sigma(a),\Sigma(b)}$$

Elliptic Curve AGM: Relation with Frobenius

$$\begin{tikzcd}
\mathcal{E}_{a,b} \arrow[r, "\psi_0"] \arrow[d, "\mathrm{Id}"'] & \mathcal{E}_{a_1,b_1} \arrow[r, "\psi_1"] \arrow[d, "\lambda_1"'] & \mathcal{E}_{a_2,b_2} \arrow[r, "\psi_2"] \arrow[d, "\lambda_2"'] & {} & \cdots \arrow[r, "\psi_{n-1}"] & \mathcal{E}_{a_n,b_n} \arrow[d, "\lambda_n"'] \\
 & & & & \vdots & \\
\mathcal{E}_0 \arrow[r, "\mathcal{F}_{2,0}"] & \mathcal{E}_1 \arrow[r, "\mathcal{F}_{2,1}"] & \mathcal{E}_2 \arrow[r, "\mathcal{F}_{2,2}"] & {} & \cdots \arrow[r, "\mathcal{F}_{2,n-1}"] & \mathcal{E}_n = \mathcal{E}_0
\end{tikzcd}$$

- Since $\mathcal{E}_{a,b}$ is isomorphic to the canonical lift $\mathcal{E}$ of E,

$$\mathrm{Tr}(\mathcal{F}_{2,n-1} \circ \cdots \circ \mathcal{F}_{2,0}) = \mathrm{Tr}(\mathcal{F}_q) = \mathrm{Tr}(F_q).$$

- Diagram: $\mathcal{F}_{2,n-1} \circ \cdots \circ \mathcal{F}_{2,0} = \lambda_n \circ \psi_{n-1} \circ \cdots \circ \psi_0$
- ψ_k acts on invariant differential ω as multiplication by 2
- λ_n as multiplication by $\pm a_n/a_0$, so

$$\mathcal{F}_q^*(\omega) = \pm q \frac{a_n}{a_0}(\omega).$$

History of p-adic Point Counting

Elliptic Curves over $\mathbb{F}_{p^n}$	p	Time	Space
Satoh	$p \geq 5$	$O(n^{3+\varepsilon})$	$O(n^3)$
Skjernaa	$p = 2$	$O(n^{3+\varepsilon})$	$O(n^3)$
Fouquet-Gaudry-Harley	$p = 2, 3$	$O(n^{3+\varepsilon})$	$O(n^3)$
Vercauteren	all p	$O(n^{3+\varepsilon})$	$O(n^2)$
Mestre (AGM)	$p = 2$	$O(n^{3+\varepsilon})$	$O(n^2)$
Carls	all p, $p = 3$	$O(n^{3+\varepsilon})$	$O(n^2)$
Kohel	$p \leq 11$	$O(n^{3+\varepsilon})$	$O(n^2)$
Satoh-Skjernaa-Taguchi	all p	$O(n^{2+1/2+\varepsilon})$	$O(n^2)$
Kim et. al	all p GNB	$O(n^{2+1/2+\varepsilon})$	$O(n^2)$
Gaudry	$p = 2$	$O(n^{2+1/2+\varepsilon})$	$O(n^2)$
Lercier-Lubicz	all p GNB	$O(n^{2+\varepsilon})$	$O(n^2)$
Harley	all p	$O(n^{2+\varepsilon})$	$O(n^2)$