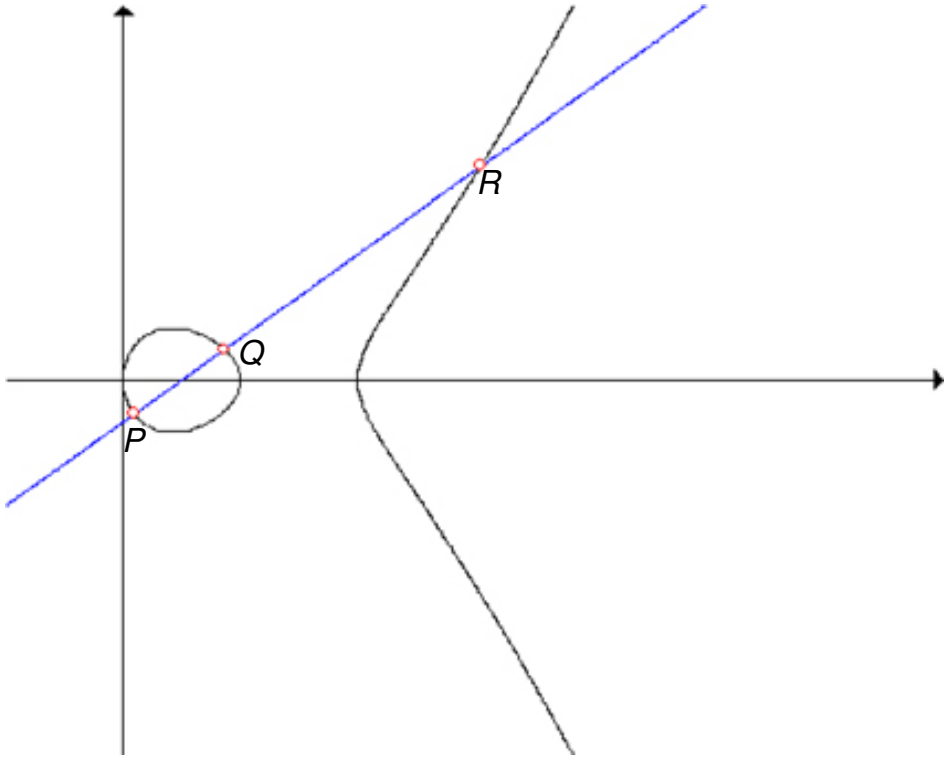
Hyperelliptisk kurve kryptografi

Christian Robenhagen Ravnshøj

NKS November 2007

Gruppelov på elliptisk kurve



$$P \oplus Q \oplus R = 0.$$

Elliptisk kurve kryptografi

Gruppelov giver krypto baseret på elliptisk kurve diskret log:

$$\text{Givet } P, [n](P) \in E(k), \text{ find } n.$$

Protokoller

- Diffie-Hellman nøgle udvekslings og ElGamal kryptering
- *Parringsbaseret* krypto.

Parring på elliptisk kurve

- $E/\mathbb{F}_q$ elliptisk kurve.
- En parring er en bilineær afbildning

$$e : E[n] \times E[n] \longrightarrow \mu_n \subseteq \mathbb{F}_{q^k}.$$

Hyperelliptisk kurve $\mathcal{C}$

- Kan skrives på formen

$$y^2 = f(x),$$

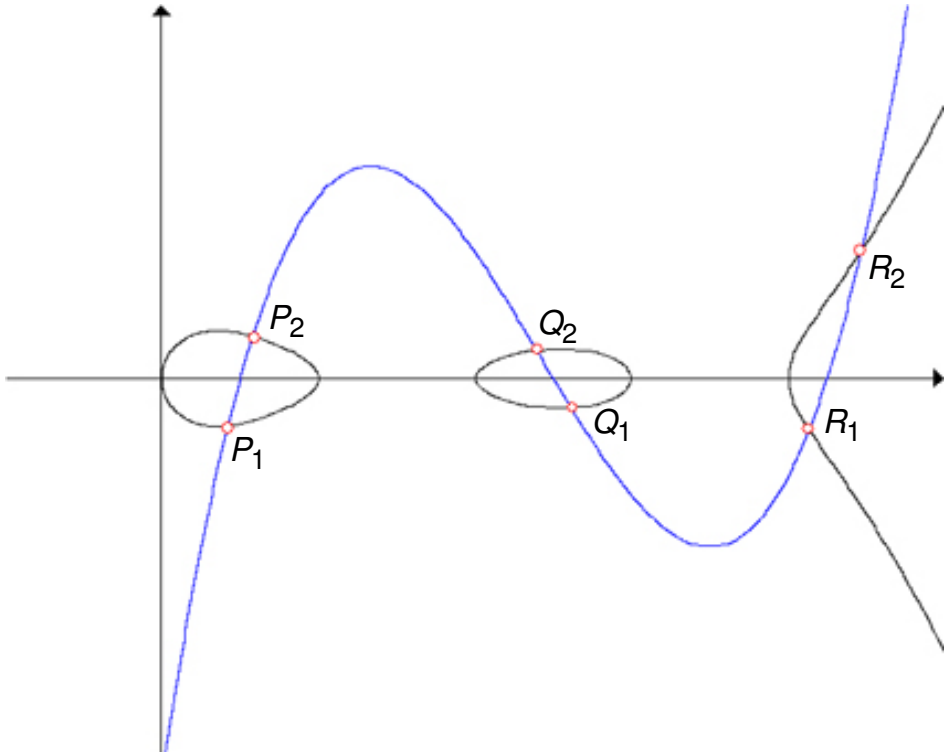
hvor $f \in \mathbb{F}_q[x]$ af $\deg(f) = 6$ og ingen dobbeltrødder.

- Jacobianten defineret som kvotient

$$\mathcal{J}_{\mathcal{C}} = \mathrm{Div}_0(C)/\mathcal{P}(C)$$

$\mathrm{Div}_0(C)$: grad nul divisorer
$\mathcal{P}(C)$: divisorer af rationale funktioner.

Gruppelov på hyperelliptiske kurver



$$(P_1 + P_2) \oplus (Q_1 + Q_2) \oplus (R_1 + R_2) = 0.$$

Krypto på hyperelliptiske kurver

- Baseret på diskret log.
- Parringsbaseret krypto muligt.

Egenskaber for parring

Findes parringer $\varepsilon : \mathcal{J}_{\mathcal{C}}[\ell] \times \mathcal{J}_{\mathcal{C}}[\ell] \to \mu_\ell < \mathbb{F}_{q^k}^\times$ som er

- Ikke-degenereret: $(\forall X \in \mathcal{J}_{\mathcal{C}}[\ell] : \varepsilon(X, Y) = 1) \Longrightarrow Y = \mathcal{O}$.
- Bilineær:

$$\varepsilon(X_1 + X_2, Y) = \varepsilon(X_1, Y) \cdot \varepsilon(X_2, Y),$$
$$\varepsilon(X, Y_1 + Y_2) = \varepsilon(X, Y_1) \cdot \varepsilon(X, Y_2).$$

- Anti-symmetrisk: $\varepsilon(X, Y) = \varepsilon(Y, X)^{-1}$.
- Galois-invariant: $\forall \sigma \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q) : \varepsilon(X, Y)^\sigma = \varepsilon(X^\sigma, Y^\sigma)$.

Indlejringsgrad

Betragt et primtal $\ell \mid |\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)|$, hvor $\ell \nmid q$.

Definition (Indlejringsgrad)

Indlejringsgraden af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* k, *så* $q^k \equiv 1 \pmod{\ell}$.

Definition (Total indlejringsgrad)

Den totale indlejringsgrad af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* κ, *så* $\mathcal{J}_{\mathcal{C}}[\ell] \subseteq \mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^\kappa})$.

Indlejringsgrad

Betragt et primtal $\ell \mid |\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)|$, hvor $\ell \nmid q$.

Definition (Indlejringsgrad)

Indlejringsgraden af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* k*, så* $q^k \equiv 1 \pmod{\ell}$.

Definition (Total indlejringsgrad)

Den totale indlejringsgrad af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* κ*, så* $\mathcal{J}_{\mathcal{C}}[\ell] \subseteq \mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^\kappa})$.

Indlejringsgrad

Betragt et primtal $\ell \mid |\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)|$, hvor $\ell \nmid q$.

Definition (Indlejringsgrad)

Indlejringsgraden af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* k, *så* $q^k \equiv 1 \pmod{\ell}$.

Definition (Total indlejringsgrad)

Den totale indlejringsgrad af $\mathcal{J}_{\mathcal{C}}$ er det *mindste tal* κ, *så* $\mathcal{J}_{\mathcal{C}}[\ell] \subseteq \mathcal{J}_{\mathcal{C}}(\mathbb{F}_{q^\kappa})$.

Matrix representation

- $\varepsilon : \mathcal{J}_{\mathcal{C}}[\ell] \times \mathcal{J}_{\mathcal{C}}[\ell] \to \mu_\ell = \langle \zeta \rangle$ bilineær parring, $X, Y \in \mathcal{J}_{\mathcal{C}}[\ell]$ divisorer.
- $\mathcal{B}$ basis for $\mathcal{J}_{\mathcal{C}}[\ell]$ over $\mathbb{F}_\ell$. Skriv $X = \vec{x} \in \mathbb{F}_\ell^4$ og $Y = \vec{y} \in \mathbb{F}_\ell^4$ mht. $\mathcal{B}$.
- findes matrice $\mathcal{E} \in \mathrm{Mat}_4(\mathbb{F}_\ell)$, så

$$\varepsilon(X, Y) = \zeta^a \iff \vec{x}^T \mathcal{E} \vec{y} = a.$$

Setup

- Identificer q-potens Frobenius endomorfien φ på $\mathcal{J}_{\mathcal{C}}$ med en rod $\omega \in \mathbb{C}$ i det karakteristiske polynomium for φ.
- Antag en indlejring $\imath : \mathfrak{O}_{\mathbb{Q}(\omega)} \hookrightarrow \mathrm{End}(\mathcal{J}_{\mathcal{C}})$ findes.
- Lad $\ell \mid |\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)|$ være et primtal. Antag ℓ unramified i $\mathbb{Q}(\omega)$ og $\ell \nmid q(q-1)$.

Sætning (Anti-symmetriske parringer)

Hvis $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_q)[\ell]$ er cyklisk, så kan vi vælge en basis $\mathcal{B}$ for $\mathcal{J}_{\mathcal{C}}[\ell]$, så alle ikke-degenererede, bilineære, anti-symmetriske og Galois-invariante parringer på $\mathcal{J}_{\mathcal{C}}[\ell]$ er givet ved matricer på formen

$$\mathcal{E}_{a,b} = \begin{bmatrix} 0 & a & 0 & 0 \\ -a & 0 & 0 & 0 \\ 0 & 0 & 0 & b \\ 0 & 0 & -b & 0 \end{bmatrix}, \qquad a, b \in \mathbb{F}_\ell^\times$$

med hensyn til $\mathcal{B}$.

Bevis

C.R. Ravnshøj, Pairings on Jacobians of Hyperelliptic Curves. Preprint, september 2007.
`http://arxiv.org/abs/0709.0175`

Elliptisk kurve med CM

- Enhver kurve $E/\mathbb{F}_p$ kan løftes til kurve $E^{\uparrow}/\mathbb{C}$.
- E har CM ved K, hvis $\mathrm{End}(E) \simeq \mathfrak{O}_K$.
- $E/\mathbb{C}$ med CM ved $K = \mathbb{Q}(\sqrt{D})$, $D < 0$.
- E svarer til helt ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$.

j-invarianten

- $j_E = j([\mathfrak{a}])$ algebraisk helt tal; afhænger kun af $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O}_K)$.
- Minimalpolynomium

$$H_D(X) = \prod_{i=1}^{h_D} (X - j(\mathfrak{a}_i)),$$

  hvor $\mathrm{Cl}(\mathfrak{O}_K) = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_{h_D}]\}$.
- Rødderne i $H_D(X) \pmod p$ udgør j-invarianterne for elliptiske kurver $E/\mathbb{F}_p$ med CM ved K.

Hyperelliptisk kurve med CM

- Enhver Jacobiant $\mathcal{J}_{\mathcal{C}}/\mathbb{F}_p$ kan løftes til Jacobiant $\mathcal{J}_{\mathcal{C}}^{\uparrow}/\mathbb{C}$.
- $\mathcal{C}$ har CM ved K, hvis $\mathfrak{O}_K \hookrightarrow \mathrm{End}(\mathcal{J}_{\mathcal{C}})$, hvor $[K : K_0] = 2$, $K_0 = K \cap \mathbb{R}$ kvadratisk tallegeme.
- $\mathcal{J}_{\mathcal{C}}$ svarer til helt ideal $\mathfrak{a} \subseteq \mathfrak{O}_K$.

j-invarianterne

- Tre j-invarianter j_1, j_2 og j_3; algebraiske tal.
- Klasse polynomier

$$H_k(X) = \prod_{i=1}^{s} \left(X - j_k^{(i)} \right), \quad k = 1, 2, 3,$$

  hvor $j_k^{(i)}$ er j-invarianterne til isomorfiklasserne af jacobianter; $H_k(X) \in \mathbb{Q}[X]$.
- Rødderne i $H_k(X) \pmod{p}$ udgør j-invarianterne for hyperelliptiske kurver $\mathcal{C}/\mathbb{F}_p$ med CM ved K.

Elliptiske kurver: $k = \kappa$

- For elliptisk kurve $E/\mathbb{F}_q$: hvis $k > 1$, så gælder

$$E[\ell] \subseteq E(\mathbb{F}_{q^k}) \iff q^k \equiv 1 \pmod{\ell}$$

- Altså: $E(\mathbb{F}_{q^m}) \simeq \mathbb{Z}/\ell\mathbb{Z} \iff k \nmid m$.

Setup

- Identificer p^m-potens Frobenius endomorfien φ på $\mathcal{J}_\mathcal{C}$ med en rod $\omega \in \mathbb{C}$ i det karakteristiske polynomium for φ.
- Antag en indlejring $\imath : \mathfrak{O}_{\mathbb{Q}(\omega)} \hookrightarrow \mathrm{End}(\mathcal{J}_\mathcal{C})$ findes.
- Lad $\ell \mid |\mathcal{J}_\mathcal{C}(\mathbb{F}_p)|$ være et primtal. Antag $\ell \neq p$ og $\ell \nmid D = \mathrm{disc}(\mathbb{Q}(\omega)_0)$.

Sætning (Indlejringsgrad for hyperelliptiske CM kurver)

Antag $\Re(\omega) = c_1 + c_2\sqrt{D}$, hvor $c_1, c_2 \in \mathbb{Z}$.

1. Hvis $\ell \nmid c_2$ og ℓ-Sylow undergruppen af $\mathcal{J}_{\mathcal{C}}(\mathbb{F}_p)$ ikke er cyklisk, så er $p^m \equiv 1 \pmod{\ell}$, i.e. $\mathcal{J}_{\mathcal{C}}$ er af indlejringsgrad $k \mid m$ med hensyn til ℓ.
2. Hvis $\ell \mid c_2$, så er

$$\mathcal{J}_{\mathcal{C}}(\mathbb{F}_{p^m})[\ell] \simeq \begin{cases} \mathbb{F}_\ell^2 & \text{hvis } p^m \not\equiv 1 \pmod{\ell}, \\ \mathbb{F}_\ell^4 & \text{hvis } p^m \equiv 1 \pmod{\ell}. \end{cases}$$

Bevis

C.R. Ravnshøj, Embedding Degree of Hyperelliptic Curves with Complex Multiplication. Preprint, maj 2007.
`http://arxiv.org/abs/0705.1443`

"Små" indlejringsgrader

- Parringsbaseret krypto kun interessant for "små" k; f.eks. $k \sim 30g$. Der er opnået små værdier for
  - $\mathcal{J}_{\mathcal{C}}$ reducibel, og
  - $\mathcal{J}_{\mathcal{C}}$ irreducibel og $\ell \sim \sqrt[4]{q}$.
- Mangler metode til at finde $\mathcal{J}_{\mathcal{C}}$ irreducibel og $\ell \sim q^2$, hvor k lille.

CM variant

- Fix K.
- Klasse polynomier givet.
- Specifik analyse mulig.