Kubične krivulje v kriptografiji

Miha Avsec

Ljubljana, 30. marec 2020

Motivacija

Zakaj bi uporabljali kubične krivulje za namene kriptografije?

- Kubične krivulje nam zagotavljajo večjo varnost glede na dolžino uporabljenega ključa.

AES	*ECC*	*RSA*
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	521	15360

- Krajši ključi predstavljajo prednost predvsem v okoljih s slabšo procesorsko močjo in omejenim pomnilnikom (pametne kartice, IoT, ...).

Projektivna ravnina

Projektivna ravnina $\mathbb{P}^2$ nad poljem $\mathbb{F}$ je kvocientni prostor $\mathbb{F}^3 - \{0\}/\sim$, kjer je ekvivalenčna relacija $\sim$ podana z $(a, b, c) \sim (\alpha a, \alpha b, \alpha c)$ za vsak neničelni $\alpha \in \mathbb{F}$. Točke v $\mathbb{P}^2$ so torej podane s homogenimi koordinatami $[a, b, c] = [\alpha a, \alpha b, \alpha c]$ za vse $\alpha \neq 0$.

Homogen polinom

Polinom P je *homogen* stopnje d, če velja

$$P(\lambda x, \lambda y, \lambda z) = \lambda^d P(x, y, z) \text{ za vse } \lambda \in \mathbb{F}.$$

.

Algebraična krivulja

Algebraična krivulja, podana s homogenim polinomom P, je množica točk

$$\mathcal{C}_P = \{A \in \mathbb{P}^2, P(A) = 0\}.$$

Kubična krivulja

Kubična krivulja je algebraična krivulja, podana s homogenim polinomom stopnje 3. V splošnem je polinom oblike

$$a_{300}x^3 + a_{210}x^2y + a_{201}x^2z + a_{120}xy^2 + a_{102}xz^2 + \\ + a_{012}yz^2 + a_{030}y^3 + a_{003}z^3 + a_{111}xyz + a_{021}y^2z,$$

kjer so $a_{ijk} \in \mathbb{F}$. Ta zapis vsebuje 10 koeficientov, vendar se lahko v gladkih primerih polinom poenostavi z ustrezno zamenjavo spremenljivk.

Gladkost

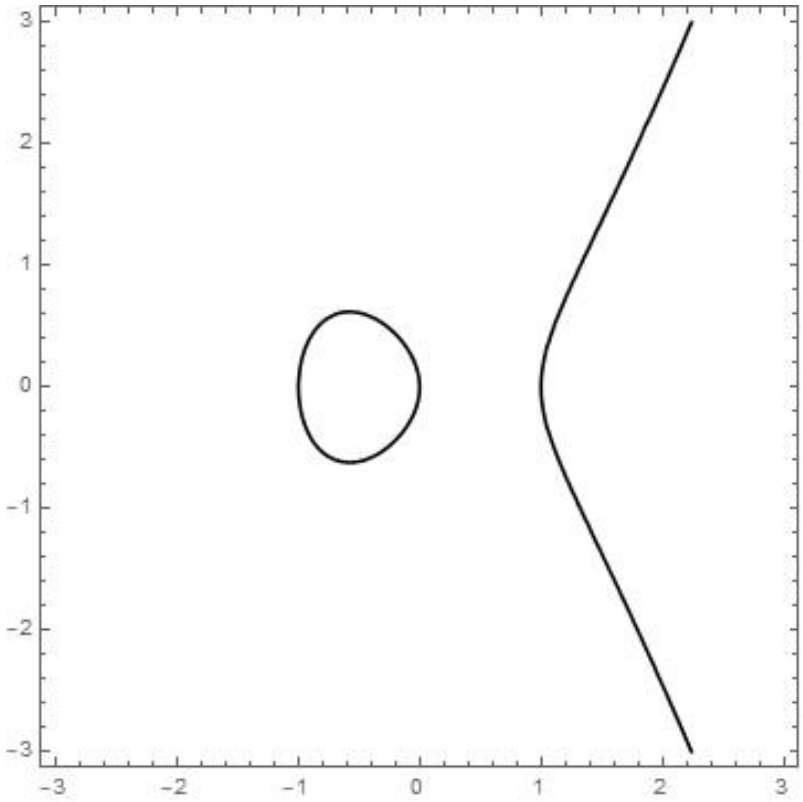
Algebraična krivulja je *gladka*, če nima singularne točke.

Izrek

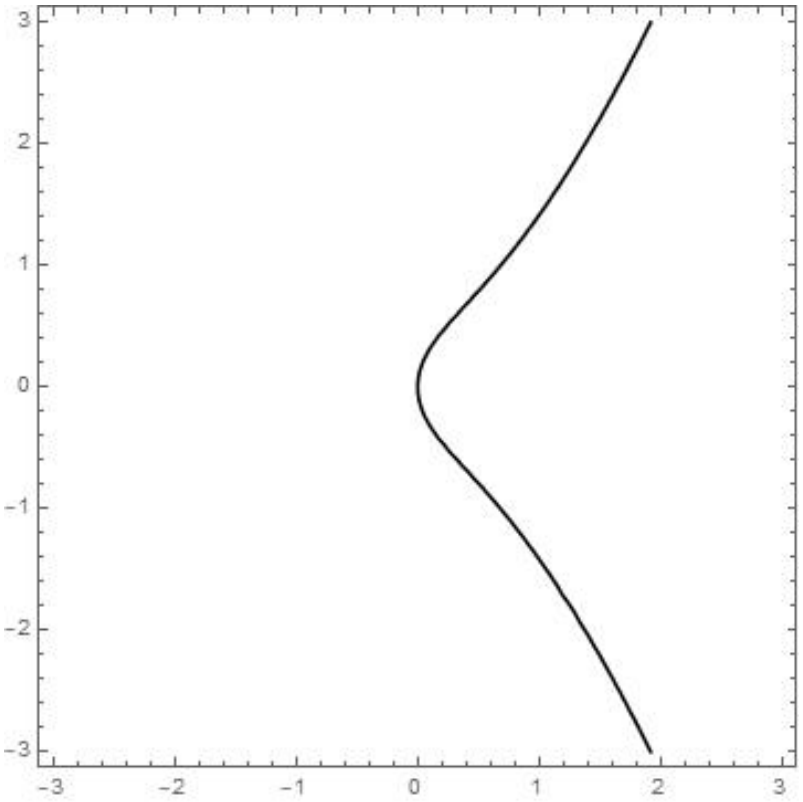
Enačbo gladke kubične krivulje nad algebraično zaprtim poljem lahko zapišemo v Weierstrassovi obliki

$$y^2z = x^3 + axz^2 + bz^3.$$

Zgled v projektivni ravnini $z = 1$



Slika: $y^2 = x^3 - x$



Slika: $y^2 = x^3 + x$

Grupa nad kubičnimi krivuljami

Za definicijo grupe na kubičnih krivuljah nad $\mathbb{C}$ najprej uvedimo pomožno operacijo

$$* : \mathcal{C}_P \times \mathcal{C}_P \to \mathcal{C}_P,$$

tako da za poljubni točki A, B na krivulji velja:

$$A * B = \begin{cases} A & \text{če je } A = B \text{ prevoj}, \\ C & \text{če je } \overline{AB} \cap \mathcal{C}_P = \{A, B, C\}, \\ A & \text{če je } \overline{AB} \text{ tangenta v } A, \text{ ter } A \neq B, \\ B & \text{če je } \overline{AB} \text{ tangenta v } B, \text{ ter } A \neq B, \\ C & \text{če je } A = B \text{ in } \{\text{tangenta v A}\} \cap \mathcal{C}_P = \{A, C\}. \end{cases}$$

Izrek

Kubična krivulja $(\mathcal{C}_P,+)$ je Abelova grupa za operacijo

$$\begin{array}{rccc} + : & \mathcal{C}_P \times \mathcal{C}_P & \to & \mathcal{C}_P \\ & (A,B) & \mapsto & (A*B)*O\ , \end{array}$$

kjer je O poljubna izbrana točka na krivulji $\mathcal{C}_P$.

Opomba

Za kubično krivuljo v Weierstrassovi obliki za točko O ponavadi izberemo takoimenovano točko v neskončnosti, oblike $[0,1,0]$, ki jo označimo z ∞.

Eliptične krivulje mod n

Za dani števili a, $b \in \mathbb{Z}/p\mathbb{Z}$ je *kubična krivulja* nad poljem $\mathbb{Z}/p\mathbb{Z}$ množica točk

$$E_{(a,b)}(\mathbb{Z}/p\mathbb{Z}) = \left\{[x, y, z] \in \mathbb{P}^2(\mathbb{Z}/p\mathbb{Z}) : y^2 z = x^3 + axz^2 + bz^3\right\}.$$

Drugače povedano, afina kubična krivulja je množica rešitev Weierstrassove enačbe

$$y^2 = x^3 + ax + b,$$

pri čemer upoštevamo zvezo med afinimi in projektivnimi koordinatami točk:

$$(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 \Leftrightarrow [x, y, 1] \in \mathbb{P}^2(\mathbb{Z}/p\mathbb{Z}).$$

Delitelj

Naj bo K polje in naj bo P točka na krivulji $E(\overline{K})$. Za vsako točko P definirajmo formalen simbol $[P]$. *Delitelj* D na krivulji E je končna linearna kombinacija takih simbolov s celoštevilskimi koeficienti

$$D = \sum_j a_j[P_j], \ a_j \in \mathbb{Z}.$$

Definicija

Definirajmo *vsoto* in *stopnjo* delitelja kot

$$\text{sum}(\sum_j a_j[P_j]) = \sum_j a_j P_j \ \in E(\overline{K}),$$

$$\deg(\sum_j a_j[P_j]) = \sum_j a_j \ \in \mathbb{Z}.$$

Definicija

Naj bo E eliptična krivulja nad poljem K. Funkcija na E je racionalna funkcija

$$f(x, y) \in \overline{K},$$

ki je definirana za vsaj eno točko na $E(\overline{K})$. Funkcija torej zavzame vrednosti v $\overline{K}$.

Trditev

Naj bo P točka na krivulji E. Potem obstaja funkcija u_P, kateri rečemo uniformizator, z lastnostjo $u_P(P) = 0$, za katero velja, da lahko vsako funkcijo $f(x, y)$ nad E zapišemo kot

$$f = u_P^r g, \text{ za nek } r \in \mathbb{Z}, \text{ kjer } g(P) \neq 0 \text{ in } \frac{1}{g(P)} \neq 0.$$

Definicija

Številu r iz trditve rečemo red funkcije f v točki P in ga označimo z $ord_P(f)$.

Definicija

Naj bo f funkcija nad E, ki ni identično enaka 0. Definirajmo delitelj funkcije f kot

$$div(f) = \sum_{P \in E(\overline{K})} ord_P(f)[P] \in Div(E).$$

Endomorfizem

Definicija

Naj bo K polje nad katerim je definirana eliptična krivulja E. Endomorfizem na E je homomorfizem $\alpha : E(\overline{K}) \to E(\overline{K})$, ki je podan z racionalno funkcijo. Torej obstajata racionalni funkciji R_1 in R_2 s koeficienti v $\overline{K}$ za kateri velja

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

za vse $(x, y) \in E(\overline{K})$.

Standardizirana oblika

Endomorfizem α lahko zapišemo v standardizirani obliki

$$\alpha(x, y) = (r_1(x), r_2(x)y), \text{ kjer je} r_1(x) = \frac{p(x)}{q(x)}.$$

Definicija

Stopnja endomorfizma je definirana kot

$$deg(\alpha) = \begin{cases} \max\{\deg p(x), \deg q(x)\} & \text{če } \alpha \not\equiv 0, \\ 0 & \text{če } \alpha \equiv 0. \end{cases}$$

Definicija

Netrivialni endomorfizem α je separabilen, če je odvod $r_1'(x) \not\equiv 0$.

Diffie-Hellmanova izmenjava ključev nad eliptičnimi krivuljami

1. Alice in Bob se dogovorita za elitpično krivuljo E nad končnim obsegom $\mathbb{F}_q$, ter za točko $P \in E(\mathbb{F}_q)$.
2. Alice se odloči za naklučno skrivno število $a \in \mathbb{N}$, in izračuna $P_a = aP$, ter to pošlje Bobu.
3. Bob se odloči za naključno skrivno število $b \in \mathbb{N}$, in izračuna $P_b = bP$, ter to pošlje Alice.
4. Alice izračuna $aP_b = abP$.
5. Bob izračuna $bP_a = baP$.

Problem diskretnega logaritma

Definicija

Naj bosta $a, b \in \mathbb{N}$*, ter naj bo* p *praštevilo. Iščemo število* k *tako da bo*

$$a^k \equiv b \ (mod \ p).$$

Problem Diffie-Hellmanove izmenjave ključev lahko prevedemo na problem diskretnega logaritma na sledeč način

- Vzemi aP in izračunaj a tako, da rešiš problem diskretnega logaritma.
- Izračunaj $a(bP)$.

Velja torej:

$$\mathrm{DL} \Rightarrow DH$$

Napadi na diskretni logaritem

- Index Calculus
- Mali korak velik korak
- Pollar rho
- Pollar lambda
- Pohlig-Hellman

Index Calculus

Pričakovana časovna zahtevnost algoritma je $O(e^{\sqrt{2 \ln p \ln \ln p}})$.

Definicija

Naj bo p praštevilo in naj bo g generator grupe $\mathbb{F}_p^x$. Naj $L(h)$ označuje vrednost, da velja

$$g^{L(h)} \equiv h \ (mod \ p).$$

Očitno velja $L(h_1 h_2) = L(h_1) + L(h_2) \ (\text{mod } p)$.
Ideja napada:
Izračunaj $L(l)$ za dovolj praštevil l, da lahko iz tega izračunaš $L(h)$ za poljuben h.

Definicija

Naj bo E eliptična krivulja nad poljem K, ter naj bo $n \in \mathbb{N}$. Torizjske točke so množica

$$E[n] = \{P \in E(\overline{K}) | nP = \infty\}.$$

Izrek

Naj bo E eliptična krivulja nad poljem K in naj bo $n \in \mathbb{N}$. Če karakteristika polja K ne deli n, ali je enaka 0 potem

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$$

Definicija

Naj bo K polje in naj bo $n \in \mathbb{N}$ tak, da karakteristika K ne deli n.

$$\mu_n = \{x \in \overline{K} | x^n = 1\}$$

je grupa n-tih korenov enote grupe $\overline{K}$.

Trditev

Naj bo E eliptična krivulja definirana nad poljem K, in naj bo $n \in \mathbb{N}$. Predpostavimo, da karakteristika polja K ne deli n. Potem obstaja Weilovo parjenje

$$e_n : E[n] \times E[n] \to \mu_n,$$

za katerega velja:

- *e_n je bilinearna v obeh spremenljivkah*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

in

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

za vse $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

Trditev (nadaljevanje)

- e_n *je nedegenerirana v obeh spremenljivkah. To pomeni če je* $e_n(S,T) = 1$ *za vse* $T \in E[n]$ *potem* $S = \infty$*, ter obratno.*
- $e_n(T,T) = 1$ *za vse* $T \in E[n]$
- $e_n(T,S) = e_n(S,T)^{-1}$ *za vse* $S, T \in E[n]$
- $e_n(\rho S, \rho T) = \rho(e_n(S,T))$ *za vse avtomorfizme* ρ *iz* $\overline{K}$*, za katere je* ρ *identiteta na koeficientih* E*.*
- $e_n(\alpha(S), \alpha(T)) = e_n(S,T)^{deg(\alpha)}$ *za vse separabilne endomorfizme* α *polja* E*.*

Posledica

Naj bosta T_1, T_2 baza $E[n]$. Potem je $e_n(T_1, T_2)$ generator grupe μ_n.

MOV napad

MOV napad uporabi Weilovo parjenje, da pretvori problem diskretnega logaritma iz $E(\mathbb{F}_q)$ v problem diskretnega logaritma nad $\mathbb{F}_{q^m}^x$. Nato pa diskretni logaritem nad novim poljem napademo z Index calculus napadom. To deluje če velikost polja $\mathbb{F}_{q^m}$ ni dosti večja od velikosti polja $\mathbb{F}_q$. Postopek napada sledi poteku dokaza naslednje trditve.

Trditev

Naj bo E eliptična krivulja nad $\mathbb{F}_q$. Naj bosta $P, Q \in E(\mathbb{F}_q)$, ter naj bo N red točke P. Predpostavimo, da velja $gcd(N, q) = 1$. Potem obstaja tako število k, da velja $Q = kP$ natanko tedaj ko $NQ = \infty$ in $e_N(P, Q) = 1$.

MOV napad

Izberi m tako, da

$$E[N] \subset E(\mathbb{F}_{q^m}).$$

Ker imajo vse točke $E[N]$ koordiante v $\overline{\mathbb{F}_q} = \cup_{j \geq 1} \mathbb{F}_{q^j}$ tak m obstaja. Prav tako je μ_N v $\mathbb{F}_{q^m}$.

1. Izberi točko $T \in E(\mathbb{F}_{q^m})$.
2. Izračunaj red M točke T.
3. Naj bo $d = \gcd(M, N)$ in naj bo $T_1 = (M/d)T$. Potem ima T_1 red, ki deli N, torej je $T_1 \in E[N]$.
4. Izračunaj $\zeta_1 = e_N(P, T_1)$ in $\zeta_2 = e_N(Q, T_1)$. Tu sta ζ_1 in ζ_2 v $\mu_d \subset \mathbb{F}_{q^m}^{\times}$.
5. Reši problem diskretnega logaritma $\zeta_2 = \zeta_1^k$ v $\mathbb{F}_{q^m}^{\times}$. To nam da k mod d.
6. Ponovi za različne točke T dokler ni k določen.