Univerza v Ljubljani
Fakulteta za matematiko in fiziko

Matematika – raziskovalna smer (podiplomski študij)

Andrej Muhič

Problem diskretnega logaritma na eliptični krivulji

Ljubljana, 2009

Kazalo

Povzetek

Prvi uporaben kriptografski sistem javnih ključev RSA se je pojavil leta 1978. RSA temelji na temu, da je problem faktorizacije števila težek. Podobno obstaja tudi kriptografija, ki je zgrajena okoli zahtevnosti problema diskretnega logaritma v končnih grupah. V letu 1985 je bila predlagan kriptografski sitem, ki izhaja iz problema diskretnega logaritma na eliptični krivulji (ECDLP).

V delu naredimo pregled do sedaj znanih napadov na problem ECDLP. Problem je soroden navadnemu diskretnemu logaritmu, le da tukaj seštevamo točke na eliptični krivulji. Operacija seštevanja točk je komutativna, zato jo bomo pisali aditivno (za razliko od multiplikativnega zapisa v $\mathbb{Z}_p$). Iščemo točko Q, za katero velja $kP = Q$. V delu navedemo nekaj osnovnih pojmov in operacij iz teorije eliptičnih krivulj in definiramo kaj je eliptična krivulja ter na kakšen način iz nje napravimo grupo. Naš glavni cilj je opisati ideje različnih metod za reševanje ECDLP. Posebno pozornost bomo namenili napadoma s parjenji. Predstavili bomo, kakšne posledice imajo do zdaj znani napadi pri implementaciji protokolov, ki slonijo na ECDLP.

Ključne besede:
problem diskretnega logaritma, eliptične krivulje, supersingularne krivulje, anomalne krivulje

Uvod

Ukvarjali se bomo s problemom diskretnega logaritma na eliptični krivulji (ECDLP). Kriptografijo temelječo na eliptičnih krivuljah (ECC) sta predlagala Victor Miller in Neal Koblitz v osemdesetih letih. Kriptografski protokoli, ki temeljijo na eliptičnih krivuljah (EC), počasi zamenjuje RSA kriptografijo javnih ključev. Protokoli EC so učinkovitejši, poleg tega jih od leta 2006 priporoča tudi NSA kot algoritme, ki so priporočljivi za varovanje zaupnih ameriških podatkov in sistemov. Njihova prednost je tudi večja izbira problemov, saj za fiksen obseg obstaja veliko različnih eliptičnih krivulj. Veliko protokolov temelji na temu, da je problem ECDLP težek. Zato je izjemno pomembno, da poznamo možne napade, in lahko tako naredimo varno implementacijo protokolov. V delu bomo podali pregled možnih napadov. Poizkusili bomo opisati vsaj njihove glavne ideje.

Navedimo nekaj osnov potrebnih za razumevanje problema. **Eliptična krivulja** E nad obsegom K je podana implicitno z enačbo

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

kjer so $a_1, a_2, a_3, a_4, a_6 \in K$ in $\Delta \neq 0$. Δ je diskriminatna krivulje E definirana kot

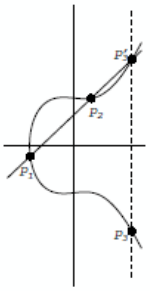
$$\begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

Neničelnost diskriminante nam zagotavlja, da nimamo večkratnih ničel. Če karakteristika obsega ni enaka 2 ali 3, lahko eliptično krivuljo zapišemo v **Weierstrassovi** obliki

$$E : y^2 = x^3 + Ax + B.$$

Zahteva o neničelnosti diskriminante se poenostavi v $4A^3 + 27B^2 \neq 0$. Tudi v primeru karakteristike 3 ali 2 lahko zapis nekoliko poenostavimo, več o tem lahko izvemo v [10].

Presenetljivo dejstvo je, da lahko nad eliptično krivuljo uvedemo aditivno operacijo na način, ki ga ponazarja slika.



Za podani točki $P = (x_1, y_1)$ in $Q = (x_2, y_2)$ skonstruiramo premico določeno s P in Q. Točka $P + Q$ je tretja točka na tej premici prezrcaljena čez x os. V primeru, da je $P = Q$, vzamemo za premico kar tangento na krivuljo. Če je premica skozi P in Q navpična,

definiramo $P + Q = \infty$. Za vsako točko definiramo še $P + \infty = P$. Z nekaj truda lahko preverimo, da na tak način dobimo abelovo grupo, glej izrek 2.1 v [2]. V grupi eliptične krivulje obravnavamo problem diskretnega logaritma.

Problem diskretnega logaritma na eliptični krivulji (ECDLP)
Podana je eliptična krivulja E nad končnim obsegom F_q in točka $P \in E(F_q)$ stopnje n. Podana je točka $Q \in \langle P \rangle$. Pri EDCLP iščemo naravno število $0 \leq \ell \leq n - 1$, da velja $Q = \ell P$. Število $\ell = \log_P Q$ je diskretni logaritem Q v bazi P. Če ima točka P velik praštevilski red, večina verjame, da ima problem veliko časovno zahtevnost.

Struktura dela bo naslednja. V osrednjem delu si ogledamo možne napade na ECDLP:

- Shankovo metodo mali, veliki korak,
- Pollardovi methodi, ρ metodo in λ (kengurujsko) metodo,
- Pohlig-Hellmanov algoritem,
- Menezes-Okamoto-Vanstoneov (MOV) napad z uporabo Weilovega parjenja,
- Frey-Rückov napad z uporabo Tateovega parjenja,
- napade na anomalne eliptične krivulje (npr. eliptične krivulje nad $\mathbb{F}_p$ s p točkami) avtorjev Semaev, Satoh-Araki in Smart,
- druge napade.

Prvi trije napadi so uporabni v splošni grupi, medtem ko so ostali napadi specializirani za eliptične krivulje. Na koncu podamo še priporočila za varno implementacijo, kot so izbira primernega končnega obsega in krivulje.

1 Metode v splošni grupi

Najprej si bomo ogledali nekaj napadov, ki delujejo v poljubni grupi. Zanimajo nas eliptične krivulje, zato bomo grupo G predstavili aditivno. Omejimo se na ciklično podgrupo, tj. $\langle P \rangle$ za nek $P \in G$. Naj bo N red grupe G. Za naše potrebe ga lahko nadomestimo z neko njegovo zgornjo mejo, torej ga sploh ni potrebno natančno izračunati. Moč množice $\mathcal{M}$ označimo z $\#\mathcal{M}$.

Izrek 1.1 (Hassejev izrek) *Naj bo E eliptična krivulja nad končnim obsegom $\mathbb{F}_q$, potem za moč grupe $E(\mathbb{F}_q)$ velja*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

1.1 Metoda mali, veliki korak

Metoda potrebuje približno $O(\sqrt{N})$ korakov in $O(\sqrt{N})$ prostora. Tako je uporabna samo za ne prevelike N. Za $N \approx 2^{80}$ potrebujemo približno $80 \cdot 2^{40}$ bitov $= 10\,\text{TB}$ pomnilnika in okoli mesec časa na enem procesorju.

---

1. Izberi $m > \sqrt{N}$ in izračunaj mP.
2. Izračunaj iP za $0 \leq i < m$ in rezultate shrani v seznam.
3. Računaj točke $Q - jmP$ za $j = 0, 1, \ldots, m-1$, dokler ne trčiš v točko na seznamu.
4. Če velja $iP = Q - jmP$, dobimo $Q \equiv kP$, kjer je $k \equiv i + jm \pmod{N}$.

Točki 2. pravimo **mali** korak, točki 3. pa **veliki** korak. Prepričajmo se, da algoritem deluje. Velja $m^2 > N$, torej lahko predpostavimo $0 \leq k < m^2$. Število k je oblike $k = k_0 + mk_1$, kjer velja $k_0 \equiv k \pmod{m}$ in $0 \leq k_0 < m$. Če definiramo $k_0 = i$ in $k_1 = j$, kjer sta i in j iz 4. koraka zgornjega algoritma, potem sledi

$$Q - k_1 mP = kP - k_1 mP = k_0 P.$$

Torej obstaja trčenje. Za eliptične krivulje lahko uporabimo Hassejev izrek, iz katerega sledi

$$m^2 \geq q + 1 + 2\sqrt{q}.$$

Za štetje točk na eliptični krivulji definirani nad končnim obsegom $\mathbb{F}_q$ lahko uporabimo Schoofov algoritem. Iz Hassejevega izreka vidimo, da je število kandidatov za $\#E(\mathbb{F}_q)$ končno. Če določimo $\#E(\mathbb{F}_q) \pmod{M}$, kjer je $M > 4\sqrt{q}$, bomo že enolično določili število točk. Torej lahko izračunamo $\#E(\mathbb{F}_q) \pmod{p}_i$ za nekaj majhnih praštevil p_i. Če velja $M = \prod_i p_i > 4\sqrt{q}$, lahko uporabimo kitajski izrek o ostankih in določimo $\#E(\mathbb{F}_q)$ mod M. Časovna zahtevnost Schoofovega algoritma je $O(\log^8 q)$. O Schoofovem algoritmu lahko izvemo več v [10].

Primer 1.2 Naj bo $G = E(\mathbb{F}_{41})$, kjer je E podana z $y^2 = x^3 + 2x + 1$. Naj bo $P = (0, 1)$ in $Q = (30, 40)$. Po Hassejevem izreku vemo, da velja $N \leq 54$. Tako lahko uporabimo $m = 8$. Točke iP za $1 \leq i \leq 7$ so

$$(0,1), (1,39), (8,23), (38,38), (23,23), (20,28), (26,9).$$

Izračunamo še $Q - jmP$ za $j = 0, 1, 2$. Dobimo

$$(30, 40), (9, 25), (26, 9),$$

našli smo trk z $7P$. Torej velja

$$(30, 40) = (7 + 2 \cdot 8)P = 23P.$$

1.2 Pollardovi ρ in λ metodi

Slabost metode mali, veliki korak je, da zahteva veliko prostora. Pollardovi metodi imata približno enako časovno zahtevnost, vendar veliko manjšo prostorsko zahtevnost. Najprej si bomo ogledali ρ metodo in jo nato posplošili na λ metodo.

Naj bo G končna grupa reda N in P element reda n. Glavna ideja ρ metode je poiskati različna para števil v $\mathbb{Z}_n$ (c', d') in (c'', d''), tako da velja

$$c'P + d'Q = c''P + d''Q.$$

Potem velja

$$(c' - c'')P = (d'' - d')Q = (d'' - d')\ell P.$$

Torej dobimo $\ell = \log_P(Q)$, kjer je $\ell = (c' - c'')(d'' - d')^{-1}$.

Na prvi pogled bo dobra naslednja implementacija. Izberemo si naključna števila $c, d \in [0, n-1]$ in shranjujemo trojice $(c, d, cP + dQ)$ v tabeli, dokler se dve tretji komponenti ne ujemata. Če se komponenti ujemata, pravimo da je prišlo do trčenja. Iz paradoksa rojstnih dni dobimo, da je pričakovano število korakov in prostorska zahtevnost $O(\sqrt{\frac{\pi n}{2}})$. Taka implementacija ne bo boljša od metode mali, veliki korak.

Implementacijo lahko izboljšamo na naslednji način. Izberemo si naključno funkcijo $f : G \to G$, konkretna možna izbira funkcije bo predstavljena v nadaljevanju. Začnemo z naključnim elementom X_0, in izvajamo iteracijo $X_{i+1} = f(X_i)$. Množica G je končna, tako prej ali slej velja $X_{i_0} = X_{j_0}$ za $i_0 < j_0$. Očitno je, da potem velja

$$X_{i_0+s} = f^s(X_{i_0}) = f^s(X_{j_0}) = X_{j_0+s}.$$

Torej je zaporedje X_i periodično s periodo $d = j_0 - i_0$. Prostorsko zahtevnost lahko izboljšamo tako, da upoštevamo periodičnost. Izračunamo lahko pare (X_i, X_{2i}), za $i = 1, 2, \ldots$ in obdržimo samo trenutni par (prejšnjih parov ne hranimo). Uporabimo zvezo

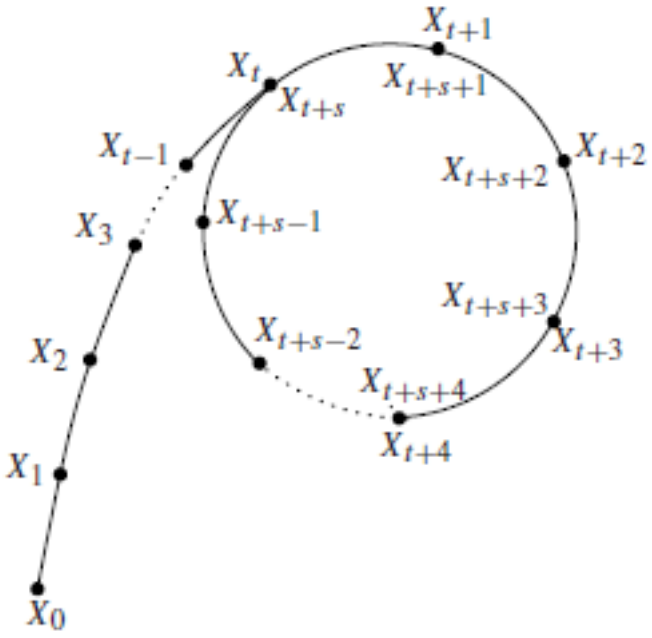
$$X_{i+1} = f(X_i), \quad X_{2(i+1)} = f(f(X_{2i})).$$

Če je $i \geq i_0$ večkratnik d, potem se indeksa $2i$ in i razlikujeta za večkratnik d. Tako velja $X_i = X_{2i}$. Iz $d \leq j_0$ in $i_0 < j_0$, dobimo, da obstaja trčenje za $i < j_0$.

Druga možnost je, da shranimo samo točke z določeno lastnostjo, npr. točke z indeksom deljivim z 2^k.

Pričakovano dolžina repa je $t \approx \sqrt{\frac{\pi n}{8}}$, pričakovana dolžina cikla je prav tako $s \approx \sqrt{\frac{\pi n}{8}}$. Skupaj dobimo, da je pričakovano število korakov približno $\sqrt{\frac{\pi n}{2}}$. Če uporabljamo samo pare oblike (X_i, X_{2i}), dobimo da je pričakovano število korakov $t \leq k \leq t + s$.

Izbrati moramo primerno funkcijo f. Funkcija mora delovati naključno, iz ujemanja točk je potrebno znati razbrati uporabno informacijo. Predstavimo eno možno izbiro. Grupo G



Slika 1: Slika oblike ρ, ki ponazarja Pollardov algoritem

razdelimo v s približno enako velikih disjunktnih podmnožic $S_1, S_2, \ldots, S_s$. Dobra izbira je $s \approx 20$. Izberemo $2s$ naključnih števil $a_i, b_i \bmod N$. Definiramo

$$M_i = a_i P + b_i Q.$$

Preslikavo definiramo kot

$$f(g) = g + M_i \quad \text{za } g \in S_i.$$

Funkcijo f si lahko predstavljamo kot naključni sprehod v G s koraki M_i.

Opišimo še idejo Pollarodove λ metode, ki je namenjena paralelizaciji. Začnemo z r naključnimi točkami $P_0^{(1)}, \ldots, P_0^{(r)}$. Dobimo zaporedja, definirana kot

$$P_{i+1}^{(j)} = f(P_i^{(j)}),\ 1 \leq j \leq r.$$

Očitno lahko zaporedja računamo paralelno. Ko najdemo trčenje med dvema zaporedjema, dobimo zvezo, iz katere lahko izračunamo rešitev diskretnega logaritma. Če dve ločeni zaporedji trčita, bosta od trka naprej enaki. Za dve začetni točki je slika procesa podobna grški črki λ. Od tukaj izhaja tudi ime metode. Če uporabimo M procesorjev, se časovna zahtevnost M-krat zmanjša.

Drugo ime metode je kengurujska metoda. Podana sta dva naključna sprehoda "miren kenguru" in "divji kenguru." V prvem naključnem sprehodu beležimo vsako 10 točko in preverimo, če imamo trčenje z drugim. Torej "miren kenguru" lovi sprehod "divji keguru."

Omenimo še, da sta obe Pollardovi metodi verjetnostni, medtem ko je metoda mali, veliki korak deterministična.

Algoritem 1 Pollardov ρ algoritem

1. Izberi naključni števili a_0, b_0. $P_0 = a_0P + b_0Q$ je začetna točka sprehoda.
2. Izračunamo

$$P_{j+1} = P_j + M_j = (u_jP + v_jQ) + (a_iP + b_iQ) = (u_j + a_i)P + (v_j + b_i)Q.$$

   Tako je $(a_{j+1}, b_{j+1}) = (u_j + a_i, v_j + b_i)$.
3. Ko velja $P_{j_0} = P_{i_0}$, dobimo

$$u_{j_0}P + v_{j_0}Q = u_{i_0}P + v_{i_0}Q \Rightarrow (u_{i_0} - u_{j_0})P = (v_{j_0} - v_{i_0})Q.$$

4. Če velja $D(v_{j_0} - v_{i_0}, N) = a$, dobimo

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \bmod \frac{N}{a}.$$

5. Dobimo a izbir za k. Ker je a ponavadi majhen, lahko preizkusimo vse možnosti, dokler ne dobimo $Q = kP$.

Primer 1.3 Rešujemo 113 bitni EDCLP problem. Eliptična krivulja E je podana nad praštevilskim obsegom $\mathbb{F}_p$, točka P ima praštevilski red n. Predpostavimo, da sta p in n 113 bitni števili. Na voljo imamo $M = 10000$ računalnikov, ki izvedejo eno iteracijo algoritma v $10\,\mu s$. Zapomnimo si samo podatke z indeksom deljivim z 2^{30}. Pričakovano število iteracij vsakega računalnika je približno

$$\frac{\sqrt{\pi 2^{113}}}{2 \cdot 10000} \approx 9 \cdot 10^{13}.$$

Tako je pričakovan čas za reševanje problema tri leta. Za shranjevanje podatkov na osrednjem računalniku porabimo

$$\frac{1}{2^{30}} \frac{\sqrt{\pi 2^{113}}}{2} 112 \cdot 3 \,\text{bitov} \approx 3.3\ GB$$

pomnilnika. Torej je problem težek, vendar primeren samo za kratkoročno varnost.

Več o Pollardovem ρ algoritmu lahko izvemo v [11].

1.3 Pohlig-Hellmanova metoda

Naj bosta $P, Q \in G$, spet iščemo tak k, da bo veljalo $Q = kP$. Predpostavimo, da poznamo moč grupe $\#\langle P \rangle = N$ in faktorizacijo

$$N = \prod_i q_i^{e_i}.$$

S Pollig-Hellmanovim algoritmom bi radi poiskali $k \bmod q_i^{e_i}$ za vsak i. Potem lahko uporabimo kitajski izrek o ostankih in združimo rešitve v $k \bmod N$.

Naj bo q praštevilo in q^e največja potenca, ki deli N. Število k zapišemo v bazi q,

$$k = k_0 + k_1 q + k_2 q^2 + \cdots + k_{e-1} q^{e-1}, \text{ kjer je } 0 \leq k_i < q.$$

Z naslednjim algoritmom lahko določimo koeficiente $k_0, \ldots, k_{e-1}$.

Algoritem 2 Pohlig-Hellmanov algoritem

1. Izračunaj
$$P_0 = \frac{N}{q}P,\ Q_0 = \frac{N}{q}Q = k(\frac{N}{q}P) = kP_0 = k_0 P.$$
Dobiš $k_0 = \log_{P_0} Q_0$.

2. Če je $e = 1$, končaj, drugače nadaljuj.

3. Naj bo $Q_1 = \frac{N}{q^2}Q = (Q - k_0 P)$. Velja
$$Q_1 = \frac{N}{q^2}(Q - k_0 P) = \frac{N}{q^2}(Q - k_0 P) = \frac{N}{q^2}(k - k_0)P = (k - k_0)\left(\frac{N}{q^2}P\right)$$
$$= (k_0 + k_1 q - k_0)(\frac{N}{q^2}P) = k_1(\frac{N}{q}P) = k_1 P_0.$$
Dobiš $k_1 = \log_{P_0} Q_1$.

4. Na koraku t dobiš $k_t = \log_{P_0} Q_t$, kjer je
$$Q_t = \frac{n}{q^{t+1}}(Q - k_0 P - k_1 q P - k_2 q^2 P - \cdots - k_{t-1} q^{t-1} P)$$
Če je t enak $e - 1$, končaj. V nasprotnem primeru naredi še en korak.

5. Vrni
$$k \equiv k_0 + k_1 q + \ldots k_{e-1} q^{e-1} \pmod{q^e}.$$

Primer 1.4 Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_{7919}$, podana z enačbo

$$y^2 = x^3 + 1001x + 75.$$

Naj bo
$$P = (4023, 6036) \in E(\mathbb{F}_{7919}).$$

Red P je enak
$$N = 7889 = 7^3 \cdot 23.$$

1. Najprej določimo $\ell_1 = \ell \bmod 7^3$. Zapišemo $l_1 = k_0 + k_1 7 + k_2 7^2$ in izračunamo
$$P_0 = 7^2 23P = (7801, 2071),$$
$$Q_0 = 7^2 23Q = (7801, 2071).$$

Torej velja $Q_0 = P_0$ in $k_0 = 1$. Nadaljujemo z

$$Q_1 = 7 \cdot 23(Q - k_0 P) = (7285, 14).$$

Krajši račun pokaže

$$Q_1 = 3P_0,$$

tako je $k_1 = 3$. V zadnjem koraku izračunamo

$$Q_2 = 23(Q - P - 3 \cdot 7P) = (7285, 7905)$$

in $Q_2 = 4P_0$. Tako dobimo $l_1 = 1 + 3 \cdot 7 + 4 \cdot 7^2 = 218$.

2. Izračunajmo še $\ell_2 = \ell \bmod 23$. Dobimo

$$P_0 = 7^3 P = (7190, 7003)$$

$$Q_0 = 7^3 Q = (2599, 759).$$

Ugotovimo, da velja $Q_0 = 10P_0$, tako je $\ell_2 = 10$.

3. Rešimo sistem kongruenc

$$\ell \equiv 218 \bmod 7^3,$$

$$\ell \equiv 10 \bmod 23.$$

Tako dobimo $\ell = 4334$.

2 Index-calculus

Omenimo še najhitrejši napad na problem diskretnega logaritma v $\mathbb{F}_p^*$, ki se ga da razširiti na napad v multiplikativni grupi končnega obsega. Njegova časovna zahtevnost je podeksponentna. Na žalost ni splošno uporaben za reševanje ECDLP. Navedimo samo dve glavni težavi. Prva težava je, da ne poznamo splošnega postopka, kako dvigniti točke nad $\mathbb{Q}$. Druga težava je, da za zapis dvignjenih točk (ulomkov) potrebujemo preveliko število števk. Več o analizi možnega napada lahko najdemo v [1]. Obstaja sicer nekaj napadov, ki index-calculus uporabijo posredno, vendar njihova ideja ni splošno uporabna.

3 Napadi, ki slonijo na izomorfizmih

Reševanje EDCLP poizkusimo prevesti na problem lažjega diskretnega logaritma v drugi grupi s pomočjo izomorfizma. Tipična primera sta Weilovo parjenje in Tate-Lichtenbaumovo parjenje. Z njuno pomočjo reduciramo problem na reševanje diskretnega logaritma v multiplikativni grupi končnega obsega. Tako lahko v določenih primerih dobimo algoritme s subeksponentno časovno zahtevnostjo.

3.1 Motivacija napadov

MOV napad je poimenovan po Menezesu, Okamoti in Vanstonu. Napad uporablja Weilovo parjenje za prevedbo diskretnega logaritma v $E(\mathbb{F}_q)$ na problem v $\mathbb{F}_{q^m}^*$. Diskretne logaritme v končnih obsegih lahko napademo z metodo index-calculus, torej jih lahko rešimo hitreje kot ECDLP, če le ni m prevelik. Za supersingularne krivulje lahko ponavadi vzamemo kar $m = 2$, zmeraj lahko vzamemo $m < 6$, torej je za posebne krivulje problem ECDLP lažji. S kriptografskega stališča je to neugodno, saj lahko na supersingularnih krivuljah računamo hitreje in so primerne za učinkovito implementacijo.

Za eliptično krivuljo E nad obsegom $\mathbb{F}_q$ definiramo torzijsko podgrupo reda n,

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\} \text{ z operacijo seštevanja točk.}$$

Definicija 3.1 Eliptična krivulja nad obsegom karaketeristike p je **supersingularna**, če velja $E[p] \simeq 0$.

Izrek 3.2 (Obstoj Weilovega parjenja) *Naj bo E eliptična krivulja nad obsegom K in n tako naravno število, da karakterisitika obsega K ne deli n. Grupa μ_n je sestavljena iz n-tih korenov enote v $\overline{K}$. Pod takimi pogoji obstaja* **Weilovo parjenje**, *preslikava*

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

ki zadošča

1. *e_n je* **bilinearno** *v vsaki spremenljivki. Veljajo enakosti*

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

   in

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

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

2. *e_n je* **nedegerirano** *v vsaki spremenljivki. Iz $e_n(S, T) = 1$ za vsak $T \in E[n]$ sledi $S = \infty$, analogno iz $e_n(S, T) = 1$ za vsak $S \in E[n]$ sledi $T = \infty$.*

3. *$e_n(T, T) = 1$ za vsak $T \in E[n]$.*

4. *$e_n(T, S) = e_n(S, T)^{-1}$ za vsak $S, T \in E[n]$. Lastnost je posledica 3 in 1.*

5. *$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ za vse avtomorfizme σ obsega $\overline{K}$, kjer je σ identiteta na koeficientih E.*

6. *$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ za vse neseparabilne avtomorfizme α krivulje E. Če koeficienti krivulje ležijo v končnem obsegu $\mathbb{F}_q$, enakost velja tudi za Frobeniusov endomorfizem $\phi_q(x) = x^q$.*

Weilovo parjenje ima lepe lastnosti. Izrek nam zagotavlja samo njegov obstoj, za definicijo potrebujemo še nekaj osnov o divizorjih. V naslednjem razdelku naštejemo poglavitne definicije in izpeljemo nekaj izrekov, ki so ključni za razumevanje.. Podane so le osnovne ideje potrebne za motivacijo napadov.

Definicija 3.3 Naj bo E eliptična krivulja. Vsaki točki $P \in E(\overline{K})$ pridružimo formalni simbol $[P]$. **Divizor** D na krivulji E je končna linearna kombinacija

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

Divizor je element proste abelove grupe generirane s simboli $[P_j]$, kjer so točke $P_j \in E(\overline{K})$. Grupo divizorjev označimo z $\mathbf{Div}(E)$. Definiramo še **stopnjo** in **vsoto** divizorja

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

$$\mathrm{sum}\left(\sum_j a_j[P_j]\right) = \sum_j a_j P_j \in E(\overline{K}).$$

Divizorji s stopnjo 0 tvorijo podgrupo, ki jo označimo z $\mathbf{Div}^0(E)$. Vsota nam poda surjektivni homomorfizem $\mathrm{sum} : \mathbf{Div}^0(E) \to E(\overline{K})$. Njegovo jedro so ravno divizorji funkcij, ki jih bomo še definirali.

Eliptična krivulja E je podana kot $y^2 = x^3 + Ax + B$. **Funkcija na E** je racionalna funkcija

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

ki je definirana za vsaj eno točko v $E(\overline{K})$. Od zdaj naprej s funkcijo mislimo funkcijo definirano nad E

Funkcija ima **ničlo** v točki P, če zavzame vrednost 0 v točki P. Podobno ima funkcija **pol** v točki P, če zavzame vrednost ∞ v točki P.

Izrek 3.4 *Za poljubno točko P obstaja funkcija u_P, tako da lahko vsako funkcija f zapišemo v obliki*

$$f = u_P^r g, \text{ kjer je } r \in \mathbb{Z} \text{ in } g(P) \neq 0, \infty.$$

Eksponentu r bomo rekli **stopnja** *točke P funkcije f in ga označili z*

$$\mathrm{ord}_P(f) = r.$$

■

Če ima funkcija f v točki P ničlo, potem je $r = \mathrm{ord}_P(f) > 0$ in pravimo, da ima ničla večkratnost r. V tem primeru pišemo $f(P) = 0$. V primeru, ko ima funkcija f v P pol, je $-r = \mathrm{ord}_P(f) < 0$, večkratnost pola je r. Dokaz izreka najdemo v [13, izrek 4.1]. To izkoristimo za naslednjo definicijo.

Definicija 3.5 Naj bo f funkcija na E, ki ni identično enaka 0. **Elementarni divizor** funkcije f je

$$\mathrm{div}(f) = \sum_{P \in E(\overline{K})} \mathrm{ord}_P(f)[P] \in \mathbf{Div}(E).$$

Da je definicija res dobra, vidimo iz naslednjih trditev.

Trditev 3.6 *Naj bo E eliptična krivulja in f funkcija na E, ki ni identično enaka 0. Potem velja:*

- *f ima samo končno mnogo ničel in polov,*
- $\deg(\mathrm{div}(f)) = 0$.
- *Če funkcija f nima ničel in polov (tj. $\mathrm{div}(f) = 0$), potem je f konstantna funkcija.*

■

Dokaz trditve lahko najdemo v [14, poglavje 8, trditev 1].

Trditev 3.7 *Naj bo E eliptična krivulja in D divizor na E z $\deg(D) = 0$. Potem obstaja funkcija f na E, za katero velja*

$$\mathrm{div}(f) = D \iff \mathrm{sum}(D) = \infty.$$

Takim divizorjem pravimo **glavni** *divizorji, njihov grupo označimo z* $\mathbf{Prin}(E)$.

Lema 3.8 *Naj bosta P_1, P_2 točki na $ax + by + c$. Potem velja*

$$[P_1] + [P_2] = [-P_3] + [\infty] + \mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right), \tag{2}$$

kjer je $P_3 = (x_3, y_3)$ tretja točka na premici skozi P_1, P_2.

Dokaz. Če $b \neq 0$, velja

$$\mathrm{div}(ax + by + c) = [P_1] + [P_2] + [P_3] - 3[\infty],$$

saj ima $ax + by + c$ pol stopnje 3 v neskončnosti. Premica skozi $P_3 = (x_3, y_3)$ in $-P_3$ je $x - x_3 = 0$. Njen divizor je enak

$$\mathrm{div}(x - x_3) = [P_3] + [-P_3] - 2[\infty].$$

Tako sledi

$$\mathrm{div}\left(\frac{ax + by + c}{x - x_3}\right) = \mathrm{div}(ax + by + c) - \mathrm{div}(x - x_3) = [P_1] + [P_2] - [-P_3] - [\infty].$$

■

Dokaz trditve 3.7 Podajmo še dokaz zadnje trditve v eno smer. Iz leme vemo, da lahko $[P_1] + [P_2]$ zamenjamo z $[P_1 + P_2] + [\infty] + \mathrm{div}(g)$. Poleg tega velja

$$\mathrm{sum}(\mathrm{div}(g)) = P_1 + P_2 - (P_1 + P_2) - \infty = \infty.$$

Iz enačbe (2) v lemi ugotovimo, da iz $P_1 + P_2 = \infty$, sledi $[P_1] + [P_2] = 2[\infty] +$ divizor funkcije. Torej lahko vsoto izrazov s pozitivnimi koeficienti zapišemo kot $[P] + n_1[\infty] +$ divizor funkcije. Podobno lahko naredimo tudi za izraze z negativnimi koeficienti. Skupaj dobimo

$$D = [P] - [Q] + n[\infty] + \mathrm{div}(g_1),$$

kjer velja $\mathrm{sum}(\mathrm{div}(g_1)) = \infty$. Iz trditve 3.6 sklepamo, da velja $\deg(\mathrm{div}(g_1)) = 0$. Dobimo

$$0 = \deg(D) = 1 - 1 + n + 0 = n.$$

Tako velja

$$D = [P] - [Q] + \mathrm{sum}(\mathrm{div}(g_1)) = P - Q.$$

Če velja $\mathrm{sum}(D) = \infty$, potem je $P - Q = \infty$. Iz tega sledi $D = \mathrm{div}(g_1)$. Kaj pa obratno? Iz $D = \mathrm{div}(f)$, sledi $[P] - [Q] = \mathrm{div}(f/g_1)$, posledično mora veljati $P = Q$. Dokaz je precej tehničen in ga izpustimo, najdemo ga lahko v [2, str. 345]. Tako dobimo $[P] = [Q]$. ∎

Posledica 3.9 *Preslikava*

$$\mathrm{sum} : \mathbf{Div}^0(E)/(\text{glavni divizorji}) \to E(\overline{K})$$

je izomorfizem grup.

Navedli smo dovolj lastnosti divizorjev, da lahko opišemo konstrukcijo Weilovega parjenja. Osnovni predpostavki sta, da število n ne deli karakteristike K in velja $E[n] \subseteq E(K)$. Radi bi konstruirali parjenje

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

kjer so μ_n n-ti koreni enote v $\overline{K}$. Po trditvi 3.7 za točko $T \in E[n]$ obstaja funkcija f, za katero velja $\mathrm{div}(f) = n[T] - n[\infty]$. Izberemo si točko $T' \in E[n^2]$, za katero velja $n^2T' = nT$. Pokazali bomo, da obstaja funkcija g, za katero velja

$$\mathrm{div}(g) = \sum_{R \in E[n]} ([T' + R] - [R]).$$

To je očitno res, saj velja

$$\mathrm{sum}\left(\sum_{R \in E[n]} ([T' + R] - [R])\right) = \sum_{R \in E[n]} T' + R - R = \sum_{R \in E[n]} T' = n^2T' = nT = \infty.$$

Upoštevali smo, da je $\#E[n] = n^2$, po [2, izrek 3.2] velja namreč $E[n] \simeq \mathbb{Z}_n \oplus \mathbb{Z}_n$, saj n ne deli karakteristike obsega. Več o strukturi grup $E[n]$ in $E(\mathbb{F}_q)$ lahko najdemo v poglavjih 3 in 4 [2]. Opazimo še, da funkcija g ni odvisna od izbire T', saj za drug možen T'' velja $T'' = T' + R$, kjer je $R \in E[n]$. Naj bo n funkcija $P \mapsto nP$. Izračunajmo

$$\mathrm{div}(f \circ n) = n\left(\sum_{R \in E[n]} [T' + R]\right) - n\left(\sum_{R \in E[n]} [R]\right) = \mathrm{div}(g^n).$$

Torej sledi, da je kompozitum $f \circ n$ enak funkciji g^n pomnoženi s konstanto. BŠS lahko izberemo tak f, da velja

$$f \circ n = g^n.$$

Naj bo $S \in E[n]$ in $P \in E(\overline{K})$. Potem velja

$$g(P + S)^n = f(n(P + S)) = f(nP) = (f \circ n)(P) = g(P)^n.$$

Torej je $g(P+S)/g(P) \in \mu_n$. V resnici je izraz neodvisen od izbire P in g. Neodvisnost od izbire P ni trivialna in temelji na temu, da je $g(P+S)/g(S)$ zvezna funkcija spremenljivke P v topologiji Zariskega.

Definicija 3.10 Weilovo parjenje lahko definiramo kot

$$e_n(S,T) = \frac{g(P+S)}{g(P)}.$$

Ker je g določen do množenja s skalarjem natančno, je definicija neodvisna od izbire g. Funkcijo g izberemo tako, da velja

$$\mathrm{div}(g) = \sum_{R \in E[n]} ([T'+R] - [R]),$$

kjer je $T' \in E[n^2]$.

Iz definicije lahko izpeljemo lastnosti Weilovega parjenja. Npr. linearnost v prvi spremenljivki sledi iz

$$e_n(S_1,T)e_n(S_2,T) = \frac{g(P+S_1)}{g(P)}\frac{g(P+S_1+S_2)}{g(P+S_1)} = e_n(S_1+S_2,T).$$

Dokaz ostalih lastnosti najdemo v [2, str. 350-354].

Izrek 3.11 (Modificirano Tate-Lichtenbaumovo parjenje) *Naj bo E eliptična krivulja nad $\mathbb{F}_q$. Naj bo n naravno število, tako da $n \mid q-1$. Naj bo $E(\mathbb{F}_q)[n]$ množica elementov redov, ki delijo n. Podan je še $\mu_n = \{x \in \mathbb{F}_q \mid x^n = 1\}$. Za podani točki $P \in E(\mathbb{F}_q)[n]$ in $Q \in E(\mathbb{F}_q)$ izberemo $R \in E(\overline{\mathbb{F}_q})$, ki zadošča $nR = Q$. Naj bo e_n Weilovo parjenje in $\phi = \phi_q$ Frobeniusov endomorfizem $x \to x^q$. Potem lahko definiramo*

$$\tau_n(P,Q) = e_n(P, R - \phi(R)).$$

Parjenje

$$\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n$$

je dobro definirano nedegerirano bilinearno parjenje.

Če bi hoteli biti natančni, bi za drugo spremenljivki morali pisati $Q + nE(\mathbb{F}_q)$, saj smo v prostoru odsekov. Tak zapis je neroden za uporabo, zato pišemo samo Q. Tako nedegeriranost v drugi spremenljivki pomeni, da iz enakosti $\tau_n(P,Q) = 1$ za vsak P sledi $Q \in nE(\mathbb{F}_q)$. Nedegeriranost v prvi spremenljivki pomeni, da iz $\tau_n(P,Q) = 1$ za vsak Q sledi $P = \infty$. Opomnimo še, da nikakor ne velja $E(\mathbb{F}_q)[n] = E[n]$, saj so točke v $E[n]$ iz algebraičnega zaprtja. Dokaz izrek najdemo v [2, izrek 3.17]. Več o parjenjih lahko najdemo v enajstem poglavju [2].

3.2 MOV napad

MOV napad uporabi Weilovo parjenje za prevedbo diskretnega logaritma v $E(\mathbb{F}_q)$ na problem DLP v $\mathbb{F}^*_{q^m}$. Tam lahko problem DLP napademo z metodo index-calculus.

Naj bo E eliptična krivulja nad obsegom $\mathbb{F}_q$. Torzijska podgrupa $E[N]$ vsebuje točke v algebrajskem zaprtju obsega, katerih red deli N. Če velja $D(q,N) = 1$ in $P,Q \in E[N]$, bomo pokazali, da je Weilovo parjenje $e_N(P,Q)$ N-ti koren enote. Izračunamo ga lahko relativno hitro.

Lema 3.12 *Podana je eliptična krivulja E nad obsegom $\mathbb{F}_q$ in točki $P,Q \in E(\mathbb{F}_q)$. Red točke P je enak N, za red velja $D(q,N) = 1$. Potem obstaja k, da velja $Q = kP$, če in samo če velja $NQ = \infty$ in je Weilovo parjenje $e_N(P,Q) = 1$.*

Dokaz. Če je $Q = kP$ in $NQ = kNP = \infty$, potem velja

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Dokažimo še drugo smer. Naj velja $NQ = \infty$. Sledi, da je $Q \in E[N]$. Velja še $D(N, q) = 1$, tako iz izreka 3.2 v [2] dobimo $E[N] \simeq \mathbb{Z}_N \oplus \mathbb{Z}_N$. Izberemo tako točko R, da je $\{P, R\}$ baza za $E[N]$. Potem velja

$$Q = aP + bR.$$

Vemo, da velja $e_N(P, R) = \zeta$, kjer je ζ N-ti koren enote. Enakost sledi iz lastnosti Weilovega parjenja, glej [2, posledica 3.10]. Sklepamo lahko, da iz $e_N(P, Q) = 1$ sledi

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b.$$

Torej velja $b \equiv 0 \bmod N$ in $bR = \infty$. Dobili smo $Q = aP$. ∎

Idejo dokaza leme izkoristi MOV napad na ECDLP. Dodajmo še, da je verjetnost, da se

Algoritem 3 MOV napad na ECDLP

Izberimo m tako, da velja

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

Vse točke $E[N]$ imajo koordinate v $\overline{\mathbb{F}}_q = \cup_{j \geq 1} \mathbb{F}_{q^j}$, torej tak m obstaja. Grupa μ_N N-tih korenov enote je vsebovana v $\mathbb{F}_{q^m}$, saj velja $E[N] \subseteq E(\mathbb{F}_{q^m})$. Torej lahko računamo v $\mathbb{F}_{q^m}$.

1. Izberi naključno točko $T \in E(\mathbb{F}_{q^m})$.
2. Izračunaj red r točke T.
3. Naj bo $D(r, N) = d$. Točka $T_1 = (r/d)T$ ima red d, ki deli N. Dobimo $T_1 \in E[N]$.
4. Izračunaj $\zeta_1 = e_N(P, T_1)$ in $\zeta_2 = e_N(Q, T_1)$, ζ_1 in ζ_2 sta iz $\mu_d \subseteq \mathbb{F}^*_{q^m}$.
5. Poišči diskretni logaritem k, da velja $\zeta_2 = \zeta_1^k$ v $\mathbb{F}^*_{q^m}$. Dobimo $k \bmod d$.
6. Ponavljaj postopek z naključnimi točkami T, dokler ni najmanjši skupni večkratnik dobljenih d enak N. Tako dobimo $k \bmod N$.

zgodi situacija $d = 1$ v algoritmu majhna. To lahko vidimo iz strukture grupe $E(\mathbb{F}_q)$, o kateri lahko več izvemo iz izreka 4.1 [2]. Tako zadošča nekaj iteracij, da dobimo $k \bmod N$. Če bomo morali izbrati prevelik m, bo problem v končnem obsegu enako zahteven kot problem na eliptični krivulji. Porabimo namreč m-krat več bitov za zapis števil, poleg tega bo, kljub podeksponentni časovni zahtevnosti metode index-calculus v končnem obsegu $\mathbb{F}_{q^m}$, problem prezahteven. Za izračun Tateovega parjenje potrebujemo $O(\log q)$ časa, tako izračun ne prispeva bistveno k zahtevnosti problema.

Posebej so na MOV napad občutljive *supersingularne* krivulje in krivulje za katere velja $\#E(\mathbb{F}_q) = q - 1$. Za prve lahko najdemo $m \leq 6$, za zadnje pa vzamemo kar $m = 2$. Uporaba takih krivulj ni varna.

3.3 Frey-Rückov napad

V nekaterih situacijah lahko za reševanje ECDLP uporabimo Tate-Lichtenbaumovo parjenje τ_n. Najprej potrebujemo nekaj ozadja za opis ideje napada.

Lema 3.13 *Naj bo ℓ praštevilo, za katerega velja $\ell \mid (q-1)$, $\ell \mid \#E(\mathbb{F}_q)$ in $\ell^2 \nmid \#E(\mathbb{F}_q)$. Grupa $E(\mathbb{F}_q)[\ell]$ naj bo ciklična, njen generator je P. Sledi, da je $\tau_\ell(P,P)$ primitivni ℓ-ti koren enote.*

Dokaz. Naj velja $\tau_\ell(P,P) = 1$, potem je $\tau_\ell(uP,P) = 1$ za vsak $u \in \mathbb{Z}$. Ker je parjenje τ_ℓ nedegenerirano, sledi $P \in \ell E(\mathbb{F}_q)$. Torej lahko zapišemo $P = \ell P_1$. Velja tudi $\ell^2 P_1 = \ell P = \infty$. Ker velja $\ell^2 \nmid \#E(\mathbb{F}_q)$, nimamo točk reda ℓ^2. Točka P_1 ima tako red 1 ali ℓ. Veljati bi moralo $P = \ell P_1 = \infty$, kar je v protislovju s tem, da je P generator. ∎

Dobimo naslednjo idejo. Naj bosta P in $E(\mathbb{F}_q)$ taka kot v lemi in naj velja $Q = kP$. Potem lahko izračunamo

$$\tau_\ell(P,Q) = \tau_\ell(P,P)^k.$$

Torej smo določili $k \bmod \ell$, saj je $\tau_\ell(P,P)$ ℓ-ti koren enote. Podobno kot pri Weilovem parjenju smo reducirali ECDLP na problem v multiplikativni grupi končnega obsega, kjer je problem lažji.

Če hočemo, da bo ECDLP težek, moramo izbrati tako krivuljo, da obstajala točka reda ℓ, kjer bo ℓ veliko praštevilo in

$$q^m \not\equiv 1 \pmod{\ell} \text{ za vse majhne } m.$$

Recimo, da obstaja točka reda n v $E(\mathbb{F}_q)$ in $n \nmid q-1$. Vedno lahko $\mathbb{F}_q$ razširimo do obsega $\mathbb{F}_{q^m}$, tako da velja $n \mid q^m - 1$ in potem lahko uporabimo Tate-Lichtenbaumovo parjenje. Točke s praštevilskim redom se pogosto uporabljajo v kriptografskih protokolih. V primeru, ko je red točke P praštevilski, lahko uporabimo tudi Weilovo parjenje. To vidimo iz naslednje trditve.

Trditev 3.14 *Naj bo E eliptična krivulja nad $\mathbb{F}_q$. Za preštevilo ℓ naj velja $\ell \mid \#E(\mathbb{F}_q)$, $E[\ell] \not\subseteq E(\mathbb{F}_q)$ in $\ell \nmid q(q-1)$. Potem velja*

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

Dokaz. Če velja $E[\ell] \subseteq E(\mathbb{F}_{q^m})$, potem je, po [2, posledica 3.11], $\mu_\ell \subseteq \mathbb{F}_{q^m}$ Torej velja $q^m \equiv 1 \pmod{\ell}$. Obratna smer je težja. Naj bo $q^m \equiv 1 \pmod{\ell}$. Točka $P \in E(\mathbb{F}_q)$ ima red ℓ. Obstaja točka $Q \in E[\ell]$, kjer $Q \notin E(\mathbb{F}_q)$. Pokazali bomo, da sta P in Q neodvisni točki reda ℓ. Recimo, da nista. Potem obstajata $u, v \in \mathbb{Z}$, da velja $uP = vQ$ in $u, v \not\equiv 0 \pmod{\ell}$. Tako dobimo $Q = v^{-1}uP \in E(\mathbb{F}_q)$, kar je protislovje. Točki P in Q tvorita bazo za $E[\ell]$.

Naj bo ϕ_q Frobeniusov endomorfizem. Delovanje ϕ_q na bazo $\{P,Q\}$, torzijske podgrupe $E[\ell]$, inducira matriko $(\phi_q)_t$. Ker velja še $P \in E(\mathbb{F}_q)$, dobimo $\phi_q(P) = P$, saj ϕ_q fiksira točke obsega $\mathbb{F}_q$. Zapišimo $\phi_q(Q) = bP + dQ$. Torej ima matrika obliko

$$(\phi_q)_t = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}.$$

Iz [2, izrek 4.10] vemo, da velja

$$\operatorname{tr}((\phi_q)_\ell) = q + 1 - \#E(\mathbb{F}_q) \bmod \ell.$$

Po predpostavki imamo $\#E(\mathbb{F}_q) \equiv 0 \pmod{\ell}$, torej velja

$$1 + d \equiv q + 1 \pmod{\ell}.$$

Tako velja $d \equiv q \pmod{\ell}$. Potenca matrike se izraža kot

$$\begin{pmatrix} 1 & b \\ 0 & q \end{pmatrix}^m \equiv \begin{pmatrix} 1 & b\frac{q^m-1}{q-1} \\ 0 & q^m \end{pmatrix} \pmod{\ell}.$$

Po predpostavki vemo, da $q \not\equiv 1 \pmod{\ell}$. Torej velja

$$\phi_q^m = 1 \text{ na } E[\ell] \iff (\phi_q)_\ell^m \equiv I \pmod{\ell} \iff q^m \equiv 1 \pmod{\ell}.$$

Zaključimo, da velja $E[\ell] \subseteq E(\mathbb{F}_{q^m})$, če in samo če velja $\phi_q^m = 1$ na $E[\ell]$. To sledi iz

$$(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y).$$

Za več glej lemo 4.5 [2]. ∎

Če velja $E[n] \subseteq E(\mathbb{F}_{q^m})$, lahko uporabimo MOV napad ali Frey-Rückov napad s Tate-Lichtenbaumovim parjenjem. Problem reduciramo na problem diskretnega logaritma v končnem obsegu $\mathbb{F}_{q^m}^*$. Tate-Licthenbaumovo parjenje je v splošnem hitrejše, več o tem v [3]. V obeh primerih je ideja enaka. Izberemo si naključno točko R in izračunamo parjenji s P in $Q = kP$. Nato rešimo problem v končnem obsegu. Ko imamo dovolj zvez $k \equiv k_\ell \pmod{\ell}$, uporabimo kitajski izrek o ostankih. Velika prednost Tate-Lichtenbaumovega parjenja je, da je za njegovo uporabo dovolj le, da je vsaj ena točka iz $E[n]$ v $E(\mathbb{F}_q)$.

4 Anomalne krivulje

MOV napad deluje, samo če lahko uporabimo Weilovo parjenje. Zato so bile predlagane eliptične krivulje nad $\mathbb{F}_q$, za katere velja

$$\#E(\mathbb{F}_q) = q.$$

Take krivulje so **anomalne** krivulje. ECDLP za grupo anomalne krivulje $E(\mathbb{F}_q)$, kjer je q praštevilo (potenca praštevila), je možno hitro rešiti. Tako te krivulje niso direktno primerne za uporabo.

Omejimo se na primer $q = p$, kjer je p praštevilo. Weilovo parjenje ni definirano na $E[p]$, ozr. če ga definiramo, je trivialno. Torej ne moremo uporabiti MOV napada. Na žalost se izkaže, da lahko uporabimo druge metode in problem rešimo še hitreje. Več podrobnosti lahko najdemo v [9].

Opomnimo še, da je anomalnost krivulje posledica obsega, nad katerim jo gledamo. Če je E anomalna nad $\mathbb{F}_q$, ni nujno da je anomalna nad $\mathbb{F}_{q^n}$, za $n > 1$. Tako se lastnost anomalnosti bistveno razlikuje od supersingularnosti, ki je neodvisna od izbire obsega in je v resnici lastnost algebraičnega zaprtja. Torej lahko izkoristimo anomalnost krivulje za pohitritev operacij v $E(\mathbb{F}_{q^n}) \subseteq E(\overline{\mathbb{F}}_q)$, kjer krivulja ni več anomalna.

Izognimo se podrobnostim in opišimo samo idejo napada. Naj bo E eliptična krivulja nad $\mathbb{F}_p$ v Weierstrassovi obliki $y^2 = x^3 + Ax + B$. Podani sta še točki P, Q na E. Iščemo k, da bo veljalo $Q = kP$. Eliptična krivulja E je anomalna, torej velja $\#E(\mathbb{F}_p) = p$.

Za racionalno število a/b, kjer sta a in b tuji, lahko zapišemo $a/b = p^r a_1 b_1$, kjer $p \nmid a_1 b_1$. Tako definiramo **p-adično evalucijo** kot

$$v_p(a/b) = r.$$

Oglejmo si nekaj primerov:

$$v_2(7/40) = v_2(2^{-3}7/5) = -3, \quad v_5(50/3) = v_5(5^2 2/3) = 2, \quad v_7(1/2) = 9.$$

Če je $\tilde{E}$ eliptična krivulja nad $\mathbb{Z}$, podana z $y^2 = x^3 + \tilde{A}x + \tilde{B}$, lahko za naravno število $r \geq 1$ definiramo

$$\tilde{E}_r = \{(x, y) \in \tilde{E}(\mathbb{Q}) \mid v_p(x) \leq -2r,\, v_p(y) \leq -3r\} \cup \{\infty\}.$$

Koordinata x (y) točke v $\tilde{E}_r$ ima v imenovalcu vsaj p^{2r} (p^{3r}). To so točke blizu ∞, gledano po modulu p^2. Navedimo naslednji izrek, saj bo ključen za razumevanje ideje napada. Njegov dokaz najdemo v [2, str. 200].

Izrek 4.1 *Naj bo $\tilde{E}$ krivulja podana z $y^2 = x^3 + \tilde{A}x + \tilde{B}$, kjer sta $\tilde{A}$ in $\tilde{B} \in \mathbb{Z}$. Naj bo r pozitivno število in p praštevilo. Potem velja:*

- *$\tilde{E}_r$ je podgrupa $\tilde{E}(\mathbb{Q})$.*
- *Če je $(x, y) \in \tilde{E}(\mathbb{Q})$, potem velja $v_p(x) < 0$, če in samo če je $v_p(y) < 0$. V tem primeru obstaja $r \geq 1$, tako da velja $v_p(x) = -2r$, $v_p(y) = -3r$.*
- *Preslikava*

$$\begin{aligned} \lambda_r : \tilde{E}_r/\tilde{E}_{5r} &\to \mathbb{Z}_{p^{4r}} \\ (x, y) &\mapsto p^{-r}x/y \bmod p^{4r} \\ \infty &\mapsto 0 \end{aligned}$$

  je injektivni homomorfizem. Operacija v $\mathbb{Z}_{p^{4r}}$ je seštevanje.

- *Če je $(x, y) \in \tilde{E}_r$ in $(x, y) \notin \tilde{E}_{r+1}$, potem velja $\lambda_r(x, y) \not\equiv 0 \pmod{p}$.*

Preslikava λ_r je logaritem za $\tilde{E}_r/\tilde{E}_{5r}$. ∎

Definirajmo še homomorfizem redukcije po modulu p

$$\begin{gathered} \mathrm{red}_p : \tilde{E}(\mathbb{Q}) \to \tilde{E} \bmod p, \\ (x, y) \mapsto (x, y) \bmod p, \quad (x, y) \notin \tilde{E}_1, \\ \tilde{E}_1 \mapsto \{\infty\}. \end{gathered}$$

Da je red_p res homomorfizem z jedrom $\tilde{E}_1$ sledi iz [2, posledica 2.33] Preden opišemo idejo algoritma, pokažimo kako dvignemo krivuljo nad $\mathbb{Z}$.

Trditev 4.2 *Podana je eliptična krivulja E nad praštevilskim obsegom $\mathbb{F}_p$ in točki $P, Q \in E(\mathbb{F}_p)$. Krivulja je podana v Weierstrassovi obliki, $y^2 = x^3 + Ax + B$. Potem obstajajo cela števila $\tilde{A}, \tilde{B}, \tilde{x}_1, \tilde{x}_2, \tilde{y}_1, \tilde{y}_2$ in eliptična krivulja $\tilde{E}$ podana z enačbo*

$$y^2 = x^3 + \tilde{A}x + \tilde{B},$$

kjer je $\tilde{P} = (x_1, y_1)$, $\tilde{Q} = (x_2, y_2) \in \tilde{E}(\mathbb{Q})$, tako da velja

$$A \equiv \tilde{A}, \quad B \equiv \tilde{B}, \quad P \equiv \tilde{P}, \quad Q \equiv \tilde{Q} \pmod{p}.$$

Dokaz. Izberemo celi števili x_1, x_2, ki sta po modulu p enaki x-koordinatama P in Q. Najprej obravnavamo primer $x_1 \not\equiv x_2 \pmod{p}$. Prvič izberemo tak y_1, da z redukcijo $\tilde{P} = (x_1, y_1)$ po modulu p dobimo P. Določimo še tak y_2, da velja

$$y_2^2 \equiv y_1^2 \pmod{x_2 - x_1} \quad \text{in} \quad (x_2, y_2) \equiv Q \pmod{p}.$$

To lahko naredimo s kitajskim izrekom o ostankih, saj velja $D(p, x_2 - x_1) = 0$. Oglejmo si sistem enačb

$$\begin{aligned} y_1^2 &= x_1^3 + \tilde{A}x_1 + \tilde{B}, \\ y_2^2 &= x_2^3 + \tilde{A}x_2 + \tilde{B}. \end{aligned}$$

Sistem rešimo in dobimo

$$\tilde{A} = \frac{y_2^2 - y_1^2}{x_2 - x_1} - \frac{x_2^3 - x_1^3}{x_2 - x_1}, \quad \tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1.$$

Število $y_2^2 - y_1^2$ je deljivo z $x_2 - x_1$ po konstrukciji, torej sta $\tilde{A}$ in $\tilde{B}$ celi števili. Točki $\tilde{P}$ in $\tilde{Q}$ ležita na krivulji $\tilde{E}$.

Obravnavajmo še primer, ko velja $x_1 \equiv x_2 \pmod{p}$. Takrat velja $P = \pm Q$. Izberemo lahko kar $x_1 = x_2$. Nato izberemo y_1, ki je po modulu p enak y-koordinati P. Določimo še $\tilde{A}$, da velja $\tilde{A} \equiv A \pmod{p}$ in $\tilde{B} = y_1^2 - x_1^3 - \tilde{A}x_1$. Iz tega sledi, da $\tilde{P} = (x_1, y_1)$ leži na $\tilde{E}$. Definirajmo še $\tilde{Q} = \pm P$, tako se $\tilde{Q}$ reducira v $\pm P = Q \bmod p$.

Tako dobimo eliptično krivuljo $\tilde{E}$, saj velja

$$4\tilde{A}^3 + 27\tilde{B}^2 \equiv 4A^3 + 27B^2 \not\equiv 0 \pmod{p}.$$

Upoštevali smo, da je E eliptična krivulja. ∎

Algoritem 4 Skica napada na anomalne krivulje

1. Dvigni E, P in Q do $\mathbb{Z}$. Dobiš $\tilde{E}$, $\tilde{P}$ in $\tilde{Q}$.
2. Naj bo $\tilde{P}_1 = p\tilde{P}$, $\tilde{Q}_1 = p\tilde{Q}$. Velja $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1$, saj je $\mathrm{red}_p(p\tilde{P}) = p \cdot \mathrm{red}_p(\tilde{P}) = \infty$.
3. Če je $\tilde{P}_1 \in \tilde{E}_2$, izberi nove $\tilde{E}$, $\tilde{P}$ in $\tilde{Q}$ ter poizkusi znova. Drugače definiraj $\ell_1 = \lambda_1(\tilde{P}_1)$ in $\ell_2 = \lambda_1(\tilde{Q}_1)$

Na koncu dobiš $k \equiv \ell_2/\ell_1 \pmod{p}$.

Ideja deluje, ker za $\tilde{K} = k\tilde{P} - \tilde{Q}$ velja

$$\infty = kP - Q = \mathrm{red}_p(k\tilde{P} - \tilde{Q}) = \mathrm{red}_p(\tilde{K}).$$

Iz tega sledi $\tilde{K} \in \tilde{E}_1$. Izraz $\lambda_1(\tilde{K})$ je definiran in velja

$$\lambda_1(p\tilde{K}) = p\lambda_1(\tilde{K}) \equiv 0 \pmod{p}.$$

Tako dobimo

$$k\ell_1 - \ell_2 = \lambda_1(k\tilde{P}_1 - \tilde{Q}_1) = \lambda_1(kp\tilde{P} - p\tilde{Q}) = \lambda_1(p\tilde{K}) \equiv 0 \bmod p.$$

Dobili smo $k \equiv \ell_2/\ell_1 \bmod p$. Opomnimo še, da je dvig krivulje in točk nad $\mathbb{Z}$ ($\mathbb{Q}$) za anomalne krivulje enostaven, v splošnem to ne velja. Glej trditev 5.6 v [2].

Brez predpostavke, da je krivulja anomalna ne gre. Če ima $E(\mathbb{F}_p)$ moč N, moramo množiti $\tilde{P}, \tilde{Q}$ z N, da preslikamo $\tilde{P}, \tilde{Q}$ v E_1, kjer je definiran λ_1. Razliko $\tilde{K} = k\tilde{P} - \tilde{Q}$ tudi množimo z N. Če p deli N, velja $\lambda_1(N\tilde{K}) \equiv 0 \bmod p$. Prispevka točke $\tilde{K}$ se tako lahko znebimo, v nasprotnem primeru to ne velja.

Pri implementaciji algoritma v praksi naletimo na težave, če je p veliko praštevilo. Točka $\tilde{P}_1$ ima potem prevelike koordinate. Imenovalec in števec x koordinate točke $\tilde{P}_1$ imata lahko p^2 števk. Tej težavi se lahko izognemo, saj potrebujemo le $x/y \bmod p$. Videli bomo, da lahko delamo vse operacije modulo p^2.

Poizkusimo računati na $\tilde{E} \bmod p^2$. Pri izračunu $(x, y) = \tilde{P}_1 = p\tilde{P}$ imamo težave. Ker velja $\tilde{P}_1 \in \tilde{E}_2$, imamo v imenovalcu x koordinate že p^2. Torej ne moremo izluščiti informacije direktno iz $\lambda_1(\tilde{P}_1)$. Namesto tega najprej izračunamo $(p-1)\tilde{P} \bmod p^2$ in ga nato prištejemo $\tilde{P}$ in si zapomnimo p v imenovalcu. Tehnične podrobnosti najdemo v [2, str. 163-165]. Oglejmo si naslednji primer.

Algoritem 5 Napad na anomalne krivulje

- Dvigni E, P, Q do $\mathbb{Z}$. Dobiš $\tilde{E}$, $\tilde{P} = (x_1, y_1), \tilde{Q} = (x_2, y_2)$.
- Izračunaj
$$\tilde{P}_2 = (p-1)\tilde{P} \equiv (x', y') \pmod{p^2}.$$
Ulomki v izračunu $\tilde{P}_2$ ne smejo imeti p v imenovalcu. Tako so imenovalci obrnljivi in lahko izračunamo x', y'.
- Izračunaj
$$\tilde{Q}_2 = (p-1)\tilde{Q} \equiv (x'', y'') \pmod{p^2}.$$
- Izračunaj
$$m_1 = p\frac{y' - y_1}{x' - x_1}, \quad m_2 = p\frac{y'' - y_2}{x'' - x_2}.$$
- Če velja $v_p(m_2) < 0$ ali $v_p(m_1) < 0$, poizkusi z drugim $\tilde{E}$. Drugače končaj in vrni
$$k \equiv \frac{m_1}{m_2} \pmod{p}.$$

Primer 4.3 Naj bo E eliptična krivulja nad $\mathbb{F}_{853}$ podana z $y^2 = x^3 + 108x + 4$. Podani sta točki $P = (0, 2)$ in $Q = (536, 755)$. Velja $853P = \infty$. Ker je 853 praštevilo, sledi $\#E(\mathbb{F}_{853}) = 853$. Torej je krivulja anomalna. Ko dvignemo krivuljo nad $\mathbb{Z}$ dobimo

$$\tilde{E} : y^2 = x^4 + 7522715x + 4, \quad \tilde{P} = (0, 2), \quad \tilde{Q} = (563, 66436).$$

Nadaljujemo in izračunamo

$$\begin{aligned} \tilde{P}_2 &= 852\tilde{P} \equiv (159511, 58855) \pmod{853^2} \\ \tilde{Q}_2 &= 852\tilde{Q} \equiv (256463, 645819) \pmod{853^2}. \end{aligned}$$

Če ne uporabimo zapisa po modulu p^2, bi za zapis $\tilde{P}_2$ porabili več kot 10^5 števk. Izračunamo

$$m_1 = 853\frac{58855-2}{159511-0} = \frac{58853}{187}, \quad m_2 = 853\frac{645819-66436}{256463-563} = \frac{58853}{187}.$$

Dobimo $k \equiv \frac{m_1}{m_2} \equiv 234 \pmod{853}$.

To je edini napad, ki temelji na izomorfizmih, in ima polinomsko časovno zahtevnost. Anomalne krivulje so zato neprimerne za uporabo.

5 Drugi napadi

Zanimiv je tudi napad Xedni calculus. Iščemo k, tako da bo veljalo $Q = kP$ na eliptični krivulji E nad $\mathbb{F}_p$. Vemo, da lahko dvignemo krivuljo E in točki P, Q nad $\mathbb{Z}$ do $\tilde{E}$, $\tilde{P}$, $\tilde{Q}$. Če lahko najdemo k', da velja $\tilde{Q} = k'\tilde{P}$, potem smo rešili problem. V splošnem to ne velja, saj sta točki $\tilde{P}$ in $\tilde{Q}$ neodvisni. Opišimo Silvermanovo idejo, njen podroben opis najdemo v članku [5]. Začnimo z nekaj (do 9) točkami oblike $a_iP + b_iQ$ in jih dvignimo nad $\mathbb{Z}$. Zapiši poljubno kubično krivuljo, ki vsebuje dvige točk. Dobimo linearni sistem enačb za koeficiente kubične krivulje, ki ga lahko rešimo. Krivuljo pretvorimo v Weierstrassovo obliko. Večina krivulj nad $\mathbb{Q}$ ima ponavadi samo dve neodvisni točki. Torej bi lahko obstajala zveza med dvignjenimi točkami, s pomočjo katere bi lahko rešili ECDLP. Na žalost imajo dobljene krivulje veliko neodvisnih točk. Algoritem najbrž ni uspešen.Več o njegovi analizi lahko najdemo v [4].

Omenimo še GHS napad z Weilovim spustom, ki poizkuša reducirati problem ECDLP na eliptični krivulji nad obsegom $\mathbb{F}_{2^m}$ na problem jakobijana hipereliptične krivulje definirane na pravem podobsegu $\mathbb{F}_{2^m}$. Za hipereliptične krivulje obstaja posplošitev ideje metode index-calculus. Več o tem najdemo v [8]. Če se želimo takemu napadu izogniti, lahko izberemo obseg $\mathbb{F}_{2^m}$, kjer je m praštevilo. Razširitev ideje tega napada na obsege z liho karakteristiko lahko najdemo recimo v [7].

6 Zaključek

Ogledali smo si večino do zdaj znanih napadov na problem ECDLP. Podajmo nekaj zaključkov.

Če se hočemo izogniti napadu Pohlig-Hellman in Pollardovim napadom mora biti moč $\#E(\mathbb{F}_q)$ deljiva z dovolj velikim praštevilom $p > 2^{160}$. Za ta dva napada bi bilo najbolje izbrati $\#E(\mathbb{F}_q) = ph$, kjer je h majhno število.

Če se hočemo izogniti napadom, ki temljijo na izomorfizmih, dobimo dodatne omejitve. Za napade na anomalne krivulje, moramo preveriti, da ne velja $\#E(\mathbb{F}_q) = q$. Da se izognemo napadu z Weilovim ali Tate-Lichtenbaumovim parjenjem mora veljati, da ne obstaja majhen k, da velja $\#\langle P\rangle = n \mid q^k - 1$. Za $n > 2^{160}$ je dovolj, da ne obstaja $k \leq 20$. Neobčutljivost na napade z Weilovim spustom dosežemo, če uporabimo binarni obseg $\mathbb{F}_{2^m}$, kjer je m praštevilo.

Področje eliptičnih krivulj je zelo aktivno. Če hočemo narediti varno implementacijo, moramo slediti vedno novim možnim napadom. Kriptografski protokoli, ki temljijo na ECC, se smatrajo kot varni, saj že več kot 20 let ni bistvenega napredka pri reševanju

EDCLP. Opomnimo, da zdajšnji protokoli ne bili več varni že, če kdo odkrije algoritem časovne zahtevnosti $O(n^{\frac{1}{4}})$. Najbolj aktivno področje so trenutno parjenja in njihova uporaba v kriptografskih protokolih.

Literatura

[1] J. H. Silverman, J. Suzuki, Elliptic Curve Discrete Logarithms and the Index Calculus, *Advances in Cryptology — ASIACRYPT'98*, 110-125.

[2] L. C. Washington *Elliptic Curves: Number Theory and Cryptography, Second Edition*, Chapman & Hall/CRC, 2008

[3] S. Galbraith, K. Harrison, and D. Soldera, Implementing the Tate pairing. *In Algorithmic number theory (Sydney, Australia, 2002)*, volume 2369 of Lecture Notes in Comput. Sci., pages 324–337. Springer-Verlag, Berlin, 2002.

[4] M. J. Jacobson, N. Koblitz, J. H. Silverman, A. Stein, E. Teske. Analysis of the xedni calculus attack, *Des. Codes Cryptogr.*, 20(1):41– 64, 2000.

[5] J. H. Silverman, The xedni calculus and the elliptic curve discrete logarithm problem, *Des. Codes Cryptogr.*, 20(1):5–40, 2000.

[6] D. Hankerson, A. J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.

[7] C. Diem, The GHS-Attack in odd characteristic, *Journal of the Ramanujan Mathematical Society*, 18:1–32, 2003.

[8] N. Theriault, Index calculus attack for hyperelliptic curves of small genus, *Advances in cryptology —ASIACRYPT 2003, volume 2894 of Lecture Notes in Comput. Sci.*, pages 75–92. Springer-Verlag, Berlin, 2003.

[9] T. Satoh, K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Comment. Math. Univ. St. Paul.*, 47(1):81–92, 1998. Errata: 48 (1999), 211-213.

[10] J. Barbič, Schoofov algoritem, diplomsko delo, 2000.

[11] E. Schlegel, Pollardova ρ-metoda, magistrsko delo, 2003.

[12] P. Nose, Učinkovita aritmetika na eliptičnih krivuljah nad praštevilskimi obsegi, diplomsko delo, 2008.

[13] M. Korče, Weilovo parjenjev shemah za šifriranje, diplomsko delo, 2006.

[14] W. Fulton, *Algebraic curves*, Addison Wesley Publishing Company, 1974.