Varnost bitov pri diskretnemgo

Podatki: (p, α, β, i),
kjer je p praštevilo, α primitiven element grupe $\mathbb{Z}_p^*$ in i poljubno naravno število, ki je manjše ali enako $\log_2(p-1)$.

Cilj: izračunati bit (oznaka: $L_i(\beta)$) logaritma $\log_\alpha \beta$ za fiksna α in p (začnemo šteti z desne).

$L_1(\beta)$ lahko najdemo s pomočjo Eulerjevega kriterija za kvadratne ostanke po modulu p:

Ker je $w^2 \equiv x^2 \pmod p \iff p|(w-x)(w+x)$ oziroma $w \equiv \pm x \pmod p$, velja

$$\{x^2 \bmod p \mid x \in \mathbb{Z}_p^*\} = \left\{\alpha^{2i} \bmod p \;\middle|\; 0 \le i \le \frac{p-3}{2}\right\}.$$

Od tod pa sledi

$$\beta \text{ kvadratni ostanek} \iff 2|\log_\alpha \beta \text{ tj. } L_1(\beta) = 0,$$

element β pa je kvadratni ostanek če in samo če je

$$\beta^{(p-1)/2} \equiv 1 \pmod p.$$

Sedaj pa si oglejmo še primer, ko je $i > 1$.

Naj bo $p - 1 = 2^s t$, kjer je t liho število.
Potem za $i \le s$ ni težko izračunati $L_i(\beta)$,
verjetno pa je težko izračunati $L_{s+1}(\beta)$,
kajti v nasprotnem primeru bi bilo možno uporabiti hipotetični podprogram za rešitev DLP v $\mathbb{Z}_p$.

Zgornjo trditev bomo dokazali za $s = 1$ oziroma $p \equiv 3 \pmod 4$. Tedaj sta kvadratna korena iz β po modulu p števili $\pm\beta^{(p+1)/4} \bmod p$.

Za $\beta \neq 0$ velja $L_1(\beta) \neq L_1(p-\beta)$, saj iz

$$\alpha^a \equiv \beta \pmod p \implies \alpha^{a+(p-1)/2} \equiv -\beta \text{ (m}$$

ker je $(p-1)/2$ liho število.

Če je $\beta = \alpha^a$ za neko sodo potenco a, potem

$$\alpha^{a/2} \equiv \beta^{(p+1)/4} \text{ ali } -\beta^{(p+1)/4} \pmod p)$$

Katera izmed teh dveh možnosti je praviln ugotovimo iz $L_2(\beta)$, saj velja

$$L_2(\beta) = L_1(\alpha^{a/2}).$$

Algoritem za računanje diskretnega logaritma v $\mathbb{Z}_p$ za $p \equiv 3 \pmod 4$:

1. $x_0 = L_1(\beta)$, $\beta = \beta/\alpha^{x_0} \bmod p$, $i := 1$
2. **while** $\beta \neq 1$ **do**
3. $\quad x_i = L_2(\beta)$
4. $\quad \gamma = \beta^{(p+1)/4} \bmod p$
5. $\quad$ **if** $L_1(\gamma) = x_i$ **then** $\beta = \gamma$
6. $\quad$ **else** $\beta = p - \gamma$
7. $\quad \beta = \beta/\alpha^{x_i} \bmod p$, $i := i + 1$

Dokaz pravilnosti zgornjega algoritma:

Naj bo

$$x = \log_\alpha \beta = \sum_{i \ge 0} x_i 2^i$$

in definirajmo za $i \ge 0$:

$$Y_i = \left\lfloor \frac{x}{2^{i+1}} \right\rfloor$$

in naj bo β_0 vrednost β v koraku 1.
Za $i \ge 1$, pa naj bo β_i vrednost β v zadnjem koraku pri i-ti iteraciji **while** zanke.

Z indukcijo pokažemo za vsak $i \ge 0$:

$$\beta_i \equiv \alpha^{2Y_i} \pmod p.$$

Iz $2Y_i = Y_{i-1} - x_i$ sledi $x_{i+1} = L_2(\beta_i)$ za $i \ge 0$
ter končno še $x_0 = L_1(\beta)$. ■

Končni obsegi

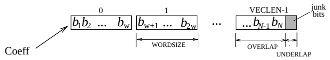
Primer končnega obsega: $\mathrm{GF}(2^4)$

Izberimo $f(x) = 1 + x + x^4 \in \mathrm{GF}(2)[x]$.
Naj bo $a_0 + a_1 x + a_2 x^2 + a_3 x^3 = (a_0, a_1, a_2, a$
Elementi obsega $\mathrm{GF}(2^4)$ so:

(1000)	(1100)	(1010)	(1111)
(0100)	(0110)	(0101)	(1011)
(0010)	(0011)	(1110)	(1001)
(0001)	(1101)	(0111)	(0000)

Element končnega obsega v predstavimo kot vektor. V hardwaru ponavadi delamo v GF(2), torej je v 01-vektor, ki ga hranimo v registru dolžine n, in je vsota vektorjev enaka XOR po koordinatah.

V softwaru pa hranimo binarni vektor v v besedah (npr. long integers)



V splošnem obstaja veliko število različnih baz za GF(q^m) nad GF(q).

Definirajmo operaciji '+' in '×' v GF(p^n):

$$(a_0,\ldots,a_{n-1})+(b_0,\ldots,b_{n-1})=(c_0,\ldots,c_{n-1}),$$

kjer je $c_i = a_i + b_i \pmod p$.

$$(a_0,\ldots,a_{n-1})\times(b_0,\ldots,b_{n-1})=(r_0,\ldots,r_{n-1}),$$

kjer je $(r_0,\ldots,r_{n-1})$ ostanek produkta $(a_0,\ldots,a_{n-1})\times(b_0,\ldots,b_{n-1})$ pri deljenju z nerazcepnim polinomom $f(x)$ stopnje n.

Primer: $(1011)+(1001)=(0010)$

$(1011)\times(1001)$
$=(1+x^2+x^3)(1+x^3)=1+x+x^5+x^6$
$=(x^4+x+1)(x^2+x)+(1+x+x^2+x^3)$
$=(1111)$

Končni obseg GF$(2^4)^*$: izberemo $f(x) = 1$ -
GF$(2^4)^*$ je generiran z elementom $\alpha = x$.

$\alpha_0 = (1000)$	$\alpha_8 = (1010)$
$\alpha_1 = (0100)$	$\alpha_9 = (0101)$
$\alpha_2 = (0010)$	$\alpha_{10} = (1110)$
$\alpha_3 = (0001)$	$\alpha_{11} = (0111)$
$\alpha_4 = (1100)$	$\alpha_{12} = (1111)$
$\alpha_5 = (0110)$	$\alpha_{13} = (1011)$
$\alpha_6 = (0011)$	$\alpha_{14} = (1001)$
$\alpha_7 = (1101)$	$\alpha_{15} = \alpha^0 = 1$

Log tabela

log	elt		log	elt
0	(1000)		8	(1010)
1	(0100)		9	(0101)
2	(0010)		10	(1110)
3	(0001)		11	(0111)
4	(1100)		12	(1111)
5	(0110)		13	(1011)
6	(0011)		14	(1001)
7	(1101)			

Zech log tabela

$1+\alpha^i=\alpha^{z(i)}$				
i	$z(i)$		i	$z(i)$
∞	0		7	9
0	∞		8	2
1	4		9	7
2	8		10	5
3	14		11	12
4	1		12	11
5	10		13	6
6	13		14	3

Računanje v **polinomski bazi** je odvisno od izbire polinoma $f(x)$.

Da bi pospešili redukcijo (po množenju ali kvadriranju), si ponavadi izberemo za $f(x)$ nerazcepni **trinom** (to je $x^n + x^m + 1$).

Na žalost nerazcepni trinomi ne obstajajo za poljubno velikost končnega obsega. V tem primeru uporabljamo *pentonome* ali *helptonome*.

Znano je, da ima vsak končni obseg GF(p^n) b
podobsegom GF(p) naslednje oblike:

$$B=\{\beta,\beta^p,\cdots,\beta^{p^{n-1}}\}.$$

V praksi so takšne baze, ki jih imenujemo **nor**
zelo praktične za hardwersko implementacijo m
v obsegu GF(p^n), še posebej, kadar je $p = 2$.

Implementacija

Potenciranje opravimo z algoritmom kvadriraj in množi:

$$\alpha^{21} = (\alpha)(\alpha^4)(\alpha^{16})$$

Najprej izračunamo faktorje α, α^2, α^4, α^8, α^{16}, in jih nato zmnožimo.

Namesto 20 množenj smo jih potrebovali le 6.

Ali je lahko kvadriranje hitrejše od (splošnega) množenja?

NE!

$$ab = \frac{(a+b)^2 - a^2 - b^2}{2}.$$

Če je kvadriranje 'lahko', potem tudi splošno množenje ni dosti težje od seštevanja.

DA!

V normalni bazi končnega obsega GF(2^n)
je kvadriranje ciklični zamik,
množenje pa ostane težko v splošnem.

V praksi so normalne baze zelo praktične za hardwarsko implementacijo množenja v obsegu GF(p^n), še posebej, kadar je $p = 2$. in je kvadriranje ***cikličen zamik***.

S tem namenom so Mullin, Onyszchuk, Vans
Wilson [MOVW88] definirali **optimalne nor**
baze (ONB) kot tiste baze, katerih število koef
v reprezentaciji elementov β^{p^i+1}, $i = 0, \cdots, n-$
na bazo B je natanko $2n-1$. Z drugimi b
$n \times n$ dimenzionalna matrika $T = (t_{mk})$, de
z $\beta\beta^{p^m} = \sum_{k=0}^{n-1} \beta^{p^k} t_{mk}$, vsebuje natanko
neničelnih elementov.

Ni težko preveriti, da je število $2n-1$ ab
spodnja meja (DN).

Izrek (Mullin et al. [MOVW]):
Obseg GF(p^n) *vsebuje optimalno normalno bazo v naslednjih primerih*

(i) $n+1$ *je praštevilo in* p *primitiven element obsega* GF$(n+1)$,

(ii) $p = 2$, $2n+1$ *je praštevilo in bodisi 2 je primitiven element obsega* GF$(2n+1)$ *bodisi* n *je lih in 2 generira kvadratne ostanke obsega* GF$(2n+1)$.

Mullin et al. [MOVW] so postavili hipotezo, da za $p = 2$ obstajajo optimalne normalne baze natanko tedaj kadar velja en izmed pogojev (i) in (ii).

Hipotezo sta leta 1992 dokazala Gao in Lenstra.

Grupa na eliptični krivulji

Za kriptografijo sta jo leta 1985 prva
predlagala Neal Koblitz in Victor Miller.

Eliptična krivulja E nad obsegom $\mathbb{Z}_p$
je definirana z Weierstrassovo enačbo:

$$\boldsymbol{y^2 = x^3 + ax + b} \qquad (1)$$

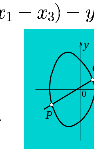
kjer sta $a, b \in \mathbb{Z}_p$ in $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$
($GF(2^m)$: $y^2 + xy = x^3 + ax^2 + b$).

$$E(\mathbb{Z}_p) := \{(x,y) \mid x, y \in \mathbb{Z}_p, \text{ ki ustrezajo (1)}\} \cup \mathcal{O}.$$

Pravilo za seštevanje

1. $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E(\mathbb{Z}_p)$,
kjer $P \neq -Q := (x_2, -y_2)$.
Potem je $P + Q = (x_3, y_3)$, kjer je
$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & ; \text{za } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & ; \text{za } P = Q. \end{cases}$$



2. $P + \mathcal{O} = \mathcal{O} + P = P \quad$ in $\quad P + (-P) =$
za vsak $P \in E(\mathbb{Z}_p)$.

Množica $E(\mathbb{Z}_p)$ je sestavljena iz točk (x, y), $x, y \in \mathbb{Z}_p$, ki ustrezajo zgornji enačbi, vključno s točko neskončno $\mathcal{O}$.

Izrek (Hasse).

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

Schoofov algoritem izračuna $|E|$ v $O((\log p)^8)$ bitnih operacijah.

Grupa E je izomorfna $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, kjer je $n_2 | n_1$ in $n_2 | (p-1)$, tako da lahko najdemo ciklično podgrupo $\mathbb{Z}_{n_1}$, ki jo uporabimo za ElGamalov kriptosistem.

Podeksponentno metodo **index calculus** zaenkrat ne znamo uporabiti pri DLP na eliptični grupi (razen če ni eliptična krivulja supersingularna).

Zato si lahko izberemo eliptično krivuljo s ciklično podgrupo velikosti (samo) okoli 2^{160}.

Primer: EC nad GF(2^4)

- Naj bo GF(2^4) generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_1(\mathrm{GF}(2^4))$ $= \{(x, y) : y^2 + xy = x^3 + \alpha^4 x^2 + 1\} \cup \{\mathcal{O}\}$.
- $E_1(\mathrm{GF}(2^4))$ tvori grupo za seštevanje z $\mathcal{O}$ kot identiteto.

Rešitve enačbe: $y^2 + xy = x^3 + \alpha^4 x^2 + 1$ nad

$(0, 1)$	
$(1, \alpha^6)$	$(1, \alpha^{13})$
(α^3, α^8)	(α^3, α^{13})
(α^5, α^3)	(α^5, α^{11})
(α^6, α^8)	(α^6, α^{14})
(α^9, α^{10})	(α^9, α^{13})
(α^{10}, α^1)	(α^{10}, α^8)
$(\alpha^{12}, 0)$	$(\alpha^{12}, \alpha^{12})$

Primer seštevanja v $E_1(\mathrm{GF}(2^4))$:

Naj bo $P_1 = (\alpha^6, \alpha^8)$, $P_2 = (\alpha^3, \alpha^{13})$.

- $P_1 + P_2 = (x_3, y_3)$:

$$\begin{aligned} x_3 &= \left(\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3}\right)^2 + \frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3} + \alpha^6 + \alpha^3 + \alpha^4 \\ &= \left(\frac{\alpha^3}{\alpha^2}\right)^2 + \frac{\alpha^3}{\alpha^2} + \alpha^2 + \alpha^4 = 1 \end{aligned}$$

$$\begin{aligned} y_3 &= \left(\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3}\right)(\alpha^6 + 1) + 1 + \alpha^8 \\ &= \left(\frac{\alpha^3}{\alpha^2}\right)\alpha^{13} + \alpha^2 = \alpha^{13} \end{aligned}$$

- $2P_1 = (x_3, y_3)$:

$$\begin{aligned} x_3 &= (\alpha^6)^2 + \frac{1}{(\alpha^6)^2} \\ &= \alpha^{12} + \alpha^3 = \alpha^{10} \end{aligned}$$

$$\begin{aligned} y_3 &= (\alpha^6)^2 + \left(\alpha^6 + \frac{\alpha^8}{\alpha^6}\right)\alpha^{10} + \alpha^{10} \\ &= \alpha^3 + (\alpha^6 + \alpha^2)\alpha^{10} = \alpha^8 \end{aligned}$$

Še en primer EC nad GF(2^4)

- Naj bo GF(2^4) generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_2(\mathrm{GF}(2^4))$ $= \{(x, y) : y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1\} \cup \{\mathcal{O}\}$.
- $E_2(\mathrm{GF}(2^4))$ tvori grupo za seštevanje z $\mathcal{O}$ kot identiteto.

Iščemo rešitve enačbe

$$y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1$$

nad GF(2^4). Ta enačba ima samo 8 rešitev:

(α^2, α^8)	(α^2, α^{14})
$(\alpha^{10}, 1)$	$(\alpha^{10}, \alpha^{13})$
$(\alpha^{11}, 0)$	(α^{11}, α^6)
(α^{13}, α^5)	(α^{13}, α^9)

Primer: EC nad GF(23)

- Naj bo $p = 23$.
- $y^2 = x^3 + x + 1$, (i.e., $a = 1$, $b = 1$).
  Velja: $27a^3 + 16b^2 = 3 \cdot 1^3 + 16 \cdot 1^3 = 19 \neq 0$ v GF(23).
- $E_3(\mathrm{GF}(23)) = \{(x, y) : y^2 = x^3 + x + 1\} \cup \{\mathcal{O}\}$.
- $E_3(\mathrm{GF}(23))$ tvori grupo za seštevanje z $\mathcal{O}$ kot identiteto.

Rešitve enačbe $y^2 = x^3 + x + 1$ nad $\mathbb{Z}_{23}$:

(0, 1)	(6, 4)	(-11,-4)
(0,-1)	(6,-4)	(-10, 7)
(1, 7)	(7, 11)	(-10,-7)
(1,-7)	(7,-11)	(-6, 3)
(3, 10)	(9, 7)	(-6,-3)
(3,-10)	(9,-7)	(-5, 3)
(4, 0)	(11, 3)	(-5,-3)
(5, 4)	(11,-3)	(-4, 5)
(5,-4)	(-11,4)	(-4,-5)

Primera seštevanja na $E_3(\mathrm{GF}(23))$

1. $P_1 = (3, 10)$, $P_2 = (9, 7)$,
   $P_1 + P_2 = (x_3, y_3)$.

   $\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{Z}_{23}$.

   $x_3 = 11^2 - 3 - 9 = 6 - 3 - 9 = -6$,
   $y_3 = 11(3 - (-6)) - 10 = 11(9) - 10$
   $= 89 = 20 = -3$.
   Sledi $P_1 + P_2 = (-6, -3)$.

2. $P_1 = (3, 10)$, $2P_1 = (x_3, y_3)$,

   $\lambda = \frac{3(3^2)+1}{20} = \frac{5}{20} = \frac{1}{4} = 6$.

   $x_3 = 6^2 - 6 = 30 = 7$,
   $y_3 = 6(3 - 7) - 10 = -24 - 10 = -1$.

   Sledi $2P_1 = (7, -11)$.

$P = (0, 1)$ je generator:

P=(0, 1)	
$2P$=(6,-4)	$15P$=(9, 7)
$3P$=(3,-10)	$16P$=(-6,3)
$4P$=(-10,-7)	$17P$=(1,7)
$5P$=(-5,3)	$18P$=(12,-4)
$6P$=(7,11)	$19P$=(-4,5)
$7P$=(11,3)	$20P$=(5,4)
$8P$=(5,-4)	$21P$=(11,-3)
$9P$=(-4,-5)	$22P$=(7 -11)
$10P$ =(12,4)	$23P$=(-5,-3)
$11P$=(1,-7)	$24P$=(-10,7)
$12P$=(-6,-3)	$25P$=(3,10)
$13P$=(9,-7)	$26P$=(6,4)
$14P$=(4,0)	$27P$=(0,-1)

Log – antilog tabela

log	elt	log	elt
0	$\mathcal{O}$	14	(4,0)
1	(0,1)	15	(9,7)
2	(6,-4)	16	(-6,3)
3	(3,-10)	17	(1,7)
4	(-10,-7)	18	(-1,-4)
5	(-5,3)	19	(-4,5)
6	(7,11)	20	(5,4)
7	(11,3)	21	(1,-3)
8	(5,-4)	22	(7,-11)
9	(-4,-5)	23	(-5,-3)
10	(-1,4)	24	(-10,7)
11	(1,-7)	25	(3,10)
12	(-6,-3)	26	(6,4)
13	(9,-7)	27	(0,-1)

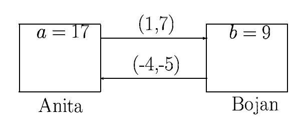
Antilog – log tabela

elt	log	elt	log
$\mathcal{O}$	0	(9,7)	15
(0,1)	1	(9,-7)	13
(0,-1)	27	(1,3)	7
(1,7)	17	(1,-3)	21
(1,-7)	11	(-11,4)	10
(3,10)	25	(-11,-4)	18
(3,-10)	3	(-10,7)	24
(4,0)	14	(-10,-7)	4
(5,4)	20	(-6,3)	16
(5,-4)	8	(-6,-3)	12
(6,4)	26	(-5,3)	5
(6,-4)	2	(-5,-3)	23
(7,11)	6	(-4,5)	19
(7,-11)	22	(-4,-5)	9

Diffie–Hellmanov protokol nad E(GF

Javni parametri:

$$y^2 = x^3 + x + 1$$
$$P = (0, 1)$$



- Anita izračuna $17P = (1,7)$,
- Bojan izračuna $9P = (-4,-5)$,
- Anita izračuna $17(-4,-5) = (6,4)$,
- Bojan izračuna $9(1,7) = (6,4)$.

Anita in Bojan imata skupno točko $(6,4)$.

Računanje logaritmov

Izračunaj $\log_P(9,7)$**.**

Izračunaj naslednjo tabelo:

elt	(0,1)	(7,11)	(-6,-3)	(12,-4)	(-10,7)
log	1	6	12	18	24

Če je $k = \log_P(9,7)$, potem velja $kP = (9,7)$.

- Računamo
  $(9,7) + P,\ \ (9,7) + 2P,\ \ \ (9,7) + 3P, \ldots,$
  vse, dokler ne dobimo element iz tabele.
- Tako dobimo: $(9,7) + 3P = (12,-4)$.
- Iz tabele preberemo $(12,-4) = 18P$.
- Sledi $(9,7) + 3P = 18P$
  oziroma $(9,7) = 15P$, torej $k = 15$.

- Če je $|E(\mathrm{GF}(q))| = n$, lahko posplošimo n
  $E(\mathrm{GF}(23))$ na naslednji način:
  - naredi tabelo (i, iP) velikosti $\sqrt{n}$,
  - za iskanje logaritma elementa v t
    potrebujemo največ $\sqrt{n}$ seštevanj točk.
- Če je $q \approx 10^{40}$, potem je $|E(\mathrm{GF}(q))| \approx 10^{40}$
  in ima tabela 10^{20} vrstic.

  To je očitno popolnoma nedosegljivo.