SIDH - supersingular isogeny Diffie-Hellman key exchange

Supersingular isogeny key exchange for beginners (Craig Costello)

Grafovi izogenija: • vrhovi su j-invarijante supersingularnih e. krivulja mod p (je $\mathbb{F}_p$ ili $\mathbb{F}_{p^2}$)

• dva vrha su spojena bridom ako postoji izogenija stupnja ℓ (ℓ je obično 2 ili 3) između eliptičkih krivulja s danim j-invarijantama

graf je nesamjeren zbog dualnih izogenija

graf je povezan, $\ell+1$ regularan uz par iznimki (npr. za $\ell=2$, $j \in \{0, 4, 242\}$)

Odabir parametara: • $p = 2^{e_A} 3^{e_B} - 1$ gdje su e_A i e_B takvi da je $2^{e_A} \approx 3^{e_B}$

dva generatora

$$E(\mathbb{F}_{p^2}) \simeq \mathbb{Z}/(p+1)\mathbb{Z} + \mathbb{Z}/(p+1)\mathbb{Z} \simeq \mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z} + \mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z}$$

$\langle P \rangle$ $\langle Q \rangle$

ova činjenica je jedna od karakterizacija supersingularnosti – sve takve krivulje imaju jednak broj točaka nad $\mathbb{F}_{p^2}$ i jednaku grupovnu strukturu

svaki element grupe je oblika $[\alpha]P + [\beta]Q$ za neke $\alpha, \beta \in \mathbb{Z}/2^{e_A}3^{e_B}\mathbb{Z}$

općenito, izogene eliptičke krivulje imaju jednak broj točaka.

Opis protokola:

- fiksiramo se krivulju E iz grafa
- Alice za svoju tajnu odabere izogeniju stupnja 2^{e_A} (odnosno podgrupu reda 2^{e_A}) dok Bob odabere izogeniju stupnja 3^{e_B}

Preciznije, $\langle P_A, Q_A \rangle = E[2^{e_A}] \simeq \mathbb{Z}/2^{e_A}\mathbb{Z} \times \mathbb{Z}/2^{e_A}\mathbb{Z}$ i

$\langle P_B, Q_B \rangle = E[3^{e_B}] \simeq \mathbb{Z}/3^{e_B}\mathbb{Z} \times \mathbb{Z}/3^{e_B}\mathbb{Z}$

su javni generatori danih podgrupa. Alice i Bob generiraju svojih tajnih grupa definiranjem kao linearne kombinacija

$S_A = P_A + [k_A] Q_A$, gdje je $k_A \in \{0, 1, \dots, 2^{e_A} - 1\}$

$S_B = P_B + [k_B] Q_B$, gdje je $k_B \in \{0, 1, \dots, 3^{e_B} - 1\}$

generatori tajnih cikličkih podgrupa

tajni ključ

Konstrukcija ključeva: Alice odabere $k_A \in \{0, 1, \dots, 2^{e_A} - 1\}$,

izračuna tajnu izogeniju $\phi_A : E \to E_A = E / \langle S_A \rangle$ (kompozicijom e_A izogenija stupnja 2) i objavi

kao javni ključ $PK_A = (E_A, P_B', Q_B') := (\phi_A(E), \phi_A(P_B), \phi_A(Q_B))$

Bobove javne točke

Analogno, Bobov javni ključ je $PK_B = (E_B, P_A', P_B')$ Alicini javne točke

(izogenija $\varnothing_B$ je sada stupnja 3^{e_B})

$= (\varnothing_B(E), \varnothing_B(P_A), \varnothing_B(Q_A))$

Protokol: Alice izračuna tajnu podgrupu generiranu s $S_A' = P_A' + [k_A] Q_A'$

na E_B i zatim izračuna tajnu izogeniju

Bobovi javni podaci

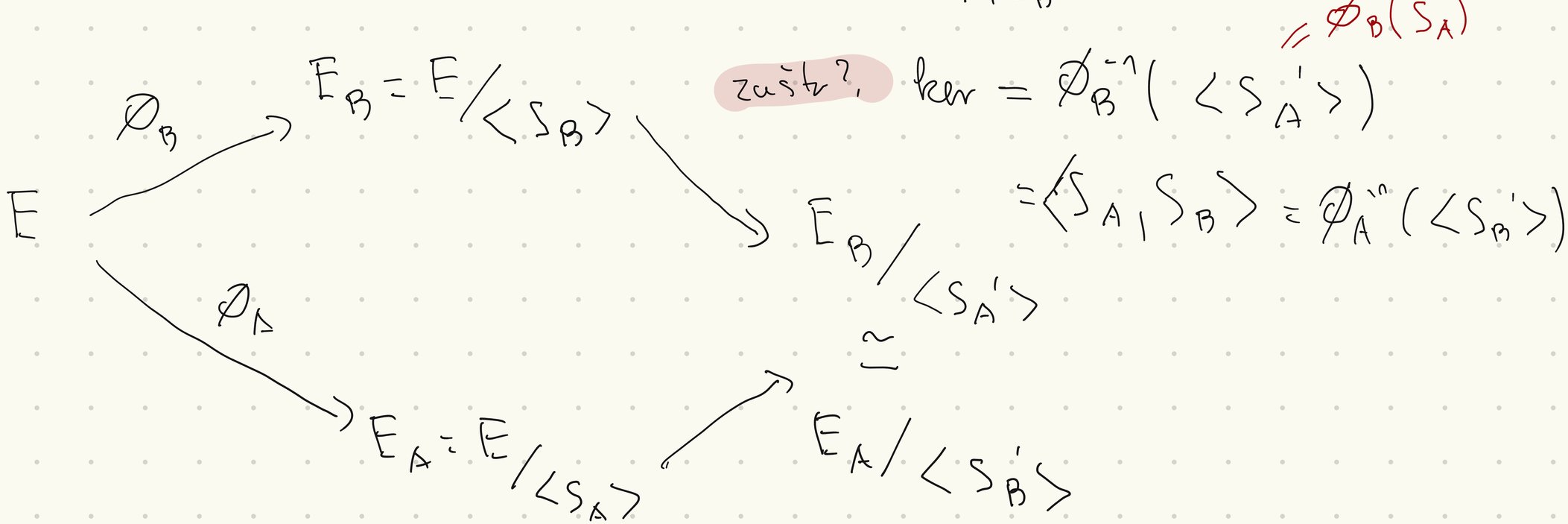
$\varnothing_A' : E_B \to E_{AB} = E_B / \langle S_A' \rangle$ i kao njihovu zajedničku

tajnu izračunat $j(E_{AB}) =: j_{AB}$

- Bob sličnu kao i Alice, izračuna $j_{BA} = j(E_{BA})$ gdje je

$$E_{BA} = E_A / \langle S_B' \rangle \quad \text{i} \quad S_B' = P_B' + [k_B] Q_B' \in E_A.$$

Zašto je $j_{AB} = j_{BA}$? Jer je $E_{AB} \simeq E / \langle S_A, S_B \rangle \simeq E_{BA}$.



$= \varphi_B(S_A)$

zašto? $\ker = \varphi_B^{-1}(\langle S_A' \rangle)$

$= \langle S_A, S_B \rangle = \varphi_A^{-1}(\langle S_B' \rangle)$

Sigurnost:

Osnovna pretpostavka sigurnost SIDH-a je da točke koji se javljaju u protokolu ne pomažu pri "razbijanju šifre" te da je za razbijanje sigurnost nužno efikasno rješiti ovaj problem.

Problem: Za dane supersing. el. krivulje E i E_A izračunajte izogeniju $\phi: E \to E_A$ stupnja ℓ^e.

(izogeniju $\phi_A: E \to E_A$ stupnja 2^{e_A} je tajni ključ od Alice, E i E_A su javni)

Konkretan primjer: $p = 2^{216}3^{137} - 1$; $\varphi_A : E \to E_A$ $\deg \varphi_A = 2^{216}$

meet in the middle algoritam: izračunaj sve krivulje koji su

2^{108} izogene krivulji E i sve koji su 2^{108} izogene krivulji E_A

te pronađi krivulju u presjeku – velika je šansa da će "kompozicija"

tih putova upravo biti tajna izogenija od Alice

problem: algoritam zahtijeva

previše memorije

postoji inačica tog algoritma (Oorschot-Wiener) koji koristi

manji memorij

Kvantni napadi na SIDH nisu bitno bolji od klasičnih.

SQISign: compact post-quantum signatures from quaternions and isogenies: De Feo, Kohel, Leroux, Petit, Wesolowski

- shema za digitalni potpis (signature scheme) : NIST-1 sigurnost : potpis 204 byta
  tajni ključ 16 byta
  javni ključ 64 byta

  → bolji od postojećih postkvantnih shema

- zero-knowledge svojstv identifikacijskog protokola

  ↑ bazirano na novom algoritm. za traženje izogenija između supersing. eliptičkih krivulja s poznatim prstenom endomorfizama.
  (quaternion ℓ-isogeny problem)

KLPT (Kohel, Lauter, Petit, Tignol) algoritam za problem traženja kvaterniorskih izogenija → zadnji cilj generalizacija ovog algoritma

Deuringova korespondencija:

$\mathcal{O}_0 \simeq End(E_0)$

$\varphi : E_0 \to E_1$

izogenija s.s. e. krivulja

bijekcija

lijevi integralni $\mathcal{O}_0$ - ideal I

$nr(I) = \deg \varphi$

norma ideala I je broj $\#\mathcal{O}_0/I$; vrijedi mult. $nr(IJ) = nr(I)nr(J)$

$End(E_1)$ je desni red tog ideala

Opis korespodencij: za integralni lijevi $\mathcal{O}_0$-ideal I definiramo

"I-torzija" →

$$E_0[I] = \{P \in E_0(\overline{\mathbb{F}}_p) : \alpha(P) = 0 \text{ za sve } \alpha \in I\}$$

$$\rightsquigarrow \varphi_I : E_0 \longrightarrow E_0/E_0[I] \quad \text{je tražena izogenija}$$

Obratno, za danu izogeniju φ definiramo ideal jezgre

$$I_\varphi = \{\alpha \in \mathcal{O}_0 : \alpha(P) = 0 \text{ za sve } P \in \ker(\varphi)\}$$

Napomena: Gore identificiramo $\mathrm{End}(E_0)$ s $\mathcal{O}_0$ (tj. fiksiramo neki izomorfizam)

Ekvivalencija redova i ideala

- Dva reda $\mathcal{O}_1$ i $\mathcal{O}_2$ (u kv. algebri $B_{p,\infty}$) su ekvivalentna (ili konjugirana) ako postoji $\beta \in B_{p,\infty}^{\times}$ t.d. $\beta \mathcal{O}_1 \beta^{-1} = \mathcal{O}_2$

- Dva lijeva $\mathcal{O}$-ideala I i J (neki red) su ekvivalentna ako postoji $\beta \in B_{p,\infty}^{\times}$ t.d. $I = J\beta$. Skup klasa ekvivalencija označavamo s $Cl(\mathcal{O})$

Važno: Ako su $\varphi : E_0 \to E_1$ i $\psi : E_0 \to E_1$ dvije izogenije onda su I_φ i I_ψ ekvivalentni lijevi $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$ ideali

KLPT algoritam: Za dani ideal I pronađi ekvivalentni ideal $J \sim I$ dane norme. Npr. norma može biti neki konkretni ℓ^e ili bilo koja potencija od ℓ.

(pregled)

Rješenje problema se svodi na traženje elementa u I dane norme.

Lema: Za svaki integralni ideal I preslikavanje

$$\chi_I(\alpha) = I\frac{\bar{\alpha}}{nr(I)}$$ je surjekcija iz $I \setminus \{0\}$

na skup idealа ekvivalentnih s I. Za $\alpha \neq \beta$, $\chi_I(\alpha) = \chi_I(\beta)$

ako i samo ako $\alpha = \beta\delta$ za neki $\delta \in G_R(I)^*$.

Dokaz: d.z. (pogledajte originalni članak)

Budući da je $nr(\chi_I(\alpha)) = \frac{n(\alpha)}{n(I)}$, nalaženje ideala $J \sim I$

norme N je ekvivalentno nalaženju $\alpha \in I$ norme $n(I) \cdot N$

Ideja: Prvo ćemo rijesiti ovaj problem za $\mathcal{O}_0$- ideale I

gdje je $\mathcal{O}_0$ specijalan ekstremni red. (special extremal order) Za takve

redove kvadratna forma koja odgovara normi

ima oblik koji pojednostavljuje rješavanje jednadžbe $nr(\alpha) = n(7)N$.

(u kv. algebri $B_{p,\infty} = \mathbb{Q}[i,j]$) je maksimalan red $\mathcal{O}_0$ koji sadrži

podred s ort. dekompozicijom $R + jR$ gdje je $R = \mathbb{Z}[w] \subset \mathbb{Q}[i]$

kvadratni red t.d. je w element najmanje norme u $\mathcal{O}_0$.

$R \subset (jR)^+$

↖ minimalno diskriminirajuće.

Primjer: Red $G_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+k}{2} \rangle$ gdje je $i^2 = -1$, $j^2 = -p$

odgovara e.k. j-invarijanti 1728 kad je $p \equiv 3(4)$, je specijalan ekstremum reel jer sadrži podred $\mathbb{Z}[i] + j\,\mathbb{Z}[i]$.

U nastavku za ekstremum G_0 fiksiramo oznake za j, R i w.

4 procedure koji se koriste u KLPT algoritmu

ekstremna

1. za dani lijevi $\mathcal{O}_0$-ideal I pronaći ekvivalentan lijevi $\mathcal{O}_0$-ideal proste norme EquivalentPrimeIdeal(I)

2. za dani $M \in \mathbb{N}$, $M > p_1$, pronaći $\gamma \in \mathcal{O}_0$ norme M

Represent Integer$_{\mathcal{O}_0}(M)$

3. za dani ideal I norme N i $\gamma \in \mathcal{O}_0$ norme Nm pronaći $(C_0 : D_0) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ takav da za $\mu_0 = j((C_0 + \omega D_0)$ vrijedi $\gamma\mu_0 \in I$. IdealModConstraint(I, γ)

4. za dani prost broj N i $C_0, D_0 \in \mathbb{Z}$ naći $\mu = \lambda\mu_0 + N\mu_1 \in \mathcal{O}_0$

norme koja dijeli F gdje je $\mu_0 = j(C_0 + \omega D_0)$

(ili potencija od ℓ)

Strong Approximation$_{\ell,F}(N, C_0, D_0)$

$R = \mathbb{Z}[\omega]$, $R \subset (jR)^+$, $j^2 = -p$

Represent Integer$_{\mathcal{O}_0}(M)$ vraća $\gamma = x + \omega y + j(z + \omega t) \in \mathcal{O}_0$

norme M. Ideja je slučajno odabrati z i t iz nekog intervala

te zatim izračunati x i y t.d. $nr(\gamma) = N$. Ono što je važno je

da norma u ovom redu ima jedno stacan oblik $nr(\gamma) = f(x,y) + p \cdot f(z,t)$

↑ norma u $\mathbb{Z}[\omega]$

$KLPT_{\ell^\bullet}(I)$ Za dani lijevi $\mathcal{O}_0$-ideal računa $J \sim I$ norme $\ell^\bullet$

1. izračunaj $L :=$ EquivalentPrimeIdeal(I) gdje je
$L := \chi_I(\delta)$ za neki $\delta \in I$ t.d. $N := nr(L)$

2. izračunaj $\gamma :=$ RepresentInteger$_{\mathcal{O}_0}(N\ell^{e_0})$ za neki $e_0 \in \mathbb{N}$

3. izračunaj $(C_0 : D_0) :=$ IdealModConstraint(L, γ)

4. izračunaj $v :=$ StrongApproximation$_{\ell^\bullet}(N, C_0, D_0)$ i označi
$\beta := \gamma v$ i e t.d. $n(\beta) := N\ell^e$

5. vrati $J := \chi_L(\beta)$