NIST Post-Quantum Cryptography Competition

(National Instit. of Standards and Technology)

- 2016: 23 signature schemes, 59 encryption shemes
- 22.7.2020 - treća runda - 7 finalista + (5+3) alternativa

(SIKE)

superingularne eliptičke krivulje

Tip	PKE/KEM	Signature
rešetke	• CRYSTAL-KYBER • NTRU • SABER	• crystals-dilithium • falcon
kodovi	• klasični McEliece	
multivarijatne		• Rainbow

NTRU: A Ring-Based Public Key Cryptosystem (Hoffstein, Pipher, Silverman)

NTRU – $O(N^2)$ operacija za enkripciju i dekripciju poruke duljine N

– $O(N)$ duljina ključa

Oznake: • tri cjelobrojna parametra $(\underline{N}, \underline{p}, \underline{q})$ i četiri skupa polinoma $\underline{\mathcal{L}_f}, \underline{\mathcal{L}_g}, \underline{\mathcal{L}_\varphi}$ i $\underline{\mathcal{L}_m}$ stupnja $N-1$ s cjelobrojnim koeficijentima

javni podaci

• pretp. $(p,q)=1$ i $q \gg p$

• $R = \mathbb{Z}[X] / (X^N - 1)$ i $F \in R$ pišemo kao $[F_0, \dots, F_{N-1}]$

gdje je $F(x) = \sum_{i=0}^{N-1} F_i x^i$; $\circledast$ množenje u R

Npr. $F \circledast G = H$ gdje je $H_k = \sum_{i=0}^{k} F_i G_{k-i} + \sum_{i=k+1}^{N-1} F_i G_{N+k-i}$

$$= \sum_{i+j \equiv k \pmod N} F_i G_j \quad (\text{jer je } x^N = 1 \text{ u } R)$$

Generiranje ključeva: (Cathy i Dan)

1. Dan slučajno odabere dva polinoma $f, g \in \mathcal{L}_g$ (što je to?) takve da $f(x)$ ima mult. inverz modulo p i q. Označimo te inverze s F_q i F_p

tj. $F_q \circledast f \equiv 1 \pmod q$ i $F_p \circledast f \equiv 1 \pmod p$.

2. Nadalje, Dan računa $h \equiv F_q \circledast g \pmod q$.

Njegov javni ključ je polinom h, a privatni ključ polinom f.
(i radi bržeg računanja F_p).

Enkripcija: Pretp. da Cathy želi poslati poruku Danu.

Ona prvo odabire poruku $m \in \mathcal{L}_m$. Zatim, slučajno odabire polinom $\phi \in \mathcal{L}_\phi$ i koristeći Danov javni ključ h računa

$$e \equiv p\phi \circledast h + m \pmod q$$

koji šalje kao enkriptiranu poruku Danu.

Dekripcija: Za dekripciju poruke e, Dan prvo računa

$$a \equiv f \circledast e \pmod{q}$$ gdje za koeficijente

od a bira brojeve iz intervala $\langle -q/2, q/2 \rangle$ te tako

gleda na a kao na polinom s cjelobrojnim koeficijentima.

Računanjem $F_p \circledast a \pmod{p}$ Dan nalazi

izvornu poruku m.

zašto?

Zašto ovo funkcionira? Vrijedi

$$a \equiv f \circledast e \equiv f \circledast p\phi \circledast h + f \circledast m \pmod q$$

$$\equiv f \circledast p\phi \circledast F_q \circledast g + f \circledast m \pmod q$$

$$\equiv p\phi \circledast g + f \circledast m \pmod q$$

ključno (jer je $q >> p$)

Za odgovarajući izbor parametara možemo postići da se gotovo u svih koeficijenti od $p\phi \circledast g + f \circledast m$ nalaze u intervalu $\langle -\frac{q}{2}, \frac{q}{2} \rangle$.

Ako Dan reducira koef. od $f \circledast e$ modulo q (u interval $\langle -\frac{q}{2}, \frac{q}{2} \rangle$) dobit će polinom $a = p\phi \circledast g + f \circledast m$ u R.

Reduciranjem a modulo p dobiva polinom $f \circledast m \pmod p$

te množenjem s F_p dobiva poruku $m \pmod p$

Odabir parametara

malo analize

Def. Za $F \in R$, definiramo širinu

$$|F|_\infty = \max_i F_i - \min_i F_i$$

kao i centriranu L^2 normu na R

$$|F|_2 = \left(\sum_i (F_i - \bar{F})^2 \right)^{\frac{1}{N}}$$ gdje je $\bar{F}$ prosjek F_i-ova.

Propozicija: Za svaki $\varepsilon > 0$ postoje konstante $\gamma_1, \gamma_2 > 0$ (koje ovise o ε i N) t.d. za slučajno odabrane polinome $F, G \in R$ s vjerojatnošću $\geq 1-\varepsilon$ vrijedi

$$\gamma_1 |F|_2 |G|_2 \leq |F \circledast G|_\infty \leq \gamma_2 |F|_2 |G|_2$$

Primjedba: U praksi omjer $\frac{\gamma_2}{\gamma_1}$ nije "velik".

Ova propozicija povezuje $| \, |_2$ norma s $| \, |_\infty$ normom

Prostor parametara. Prostor poruka $\mathcal{L}_m$ se sastoji od

svih polinoma modulo p. Za p neparan uzimamo

$$\mathcal{L}_m = \{ m \in R : m \text{ ima koef. između } -\tfrac{1}{2}(p-1) \text{ i } \tfrac{1}{2}(p-1) \}$$

Neka je $\mathcal{L}(d_1, d_2) = \{ F \in R : F \text{ ima } d_1 \text{ koeficijenata jednakih}$

vrlo specijalno $\quad 1, d_2 \text{ jednakih } -1, \text{ ostatak su nule} \}$

Odaberimo sada tri prirodna broja $d_f, d_g, d \in \mathbb{N}$

zbog invertibilnosti od f

Neka su $\mathcal{L}_f = \mathcal{L}(d_f, d_f - 1)$, $\mathcal{L}_g = \mathcal{L}(d_g, d_g)$ i $\mathcal{L}_\phi = \mathcal{L}(d, d)$.

polinomi s koef u skupu $\{-1, 0, 1\}$

Uočimo da $f \in \mathcal{L}_f$, $g \in \mathcal{L}_g$ i $\phi \in \mathcal{L}_\phi$ imaju L^2-normu

$$|f|_2 = \sqrt{2d_f - 1 - N^{-1}}, \quad |g|_2 = \sqrt{2d_g} \quad \text{i} \quad |\phi|_2 = \sqrt{2d}.$$

očito

Uvjet za dekripciju

nije dovoljno

Za uspješnu dekripciju poruke nužno je da

(*) $$|f \circledast m + p\phi \circledast g|_\infty < q.$$

želimo da su svi koef. u intervalu $\langle -\frac{q}{2}, \frac{q}{2} \rangle$

Eksperimentalno! se pokaže da je taj uvjet (*) gotovo uvijek zadovoljen ako odaberemo parametre t.d.

$$\|f \otimes m\|_\infty \leq \frac{9}{4} \quad i \quad \|p\phi \otimes g\|_\infty \leq \frac{9}{4}.$$

Gornja propozicija sugerira da odaberemo f, ϕ i g t.d.

$$\|f\|_2 \|m\|_2 \approx \frac{9}{4 r_2} \quad i \quad \|\phi\|_2 \|g\|_2 \approx \frac{9}{4 p r_2} \quad \text{za } r_2$$

koji "odgovara" nekom malom ε. Npr. eksperiment sugerira da za $N = 107, 167$ i 503 vrijednosti za r_2 su redom $0.35, 0.27$ i 0.17

Sigurnost

javni ključ $\rightarrow h \equiv F_q \circledast g \pmod q$

$\uparrow$ mod q inverz privatnog ključa f

1. Brute force napad

Napadač može pokušati pogoditi privatni ključ testirajući za sve $f \in \mathcal{L}_f$ ima li

$$f \circledast h \equiv f \circledast F_q g \stackrel{?}{\equiv} g \pmod q \quad \text{male koeficijente.}$$

(sjetimo se $g \in \mathcal{L}_g = \mathcal{L}(d_g, d_g)$ ima samo koef. u skupu $\{0, 1, -1\}$.)

ili može testirati (prolazeći kroz $\mathcal{L}_g$) koef. od $g \circledast h^{-1} \pmod q$.

$(\equiv f \pmod q)$

U praksi prostor $\mathcal{L}_g$ je manji od $\mathcal{L}_f$ pa je sigurnost

od ovog napada određena s $\# \mathcal{L}_g = \frac{1}{d_g!} \frac{N!}{(N-2d_g)!}$.

Također, napadač može testirati $\boxed{e - p \cdot \phi \circledast h \pmod q}$

kao napad na individualnu poruku e (gdje ϕ prolazi kroz $\mathcal{L}_\phi$).

Tu je sigurnost određena s $\# \mathcal{L}_\phi = \frac{1}{d!} \sqrt{\frac{N!}{(N-2d)!}}$.

$e \equiv p \phi \circledast h + m \pmod q$

2. Meet-in-the-middle napadi

A meet-in-the-middle attack on NTRU Private key (Howgrave, Silverman, Whyte)

Ugrubo, napadač može (umjesto da pretražuje $f \in \mathcal{L}_f$) pretraživati parove $f_1, f_2 \in \mathcal{L}_f$ za koje $f_1 \circledast h$ i $-f_2 \circledast h$ imaju koeficijente otprilike iste veličine (u nadi da će pogoditi kombinaciju za koju je $f = f_1 + f_2$). Ovaj napad zahtijeva puno memorije (jer treba memorirati sve vrijednosti $f_1 \circledast e$ koji se računaju) kao i dobar algoritam koji će efikasno provjeriti ima li npr. $-f_2 \circledast h$ "slične" koef. nekom polinomu iz baze podataka.

Ovime sigurnosni nivo smanjuje na $\sqrt{\#\mathcal{L}_g}$ i $\sqrt{\#\mathcal{L}_\phi}$.

3. Napad na ponovljene poruke.

Ako Cathy pošalje istu poruku m više puta koristeći isti javni ključ, ali različit ϕ, onda se napadačica Betty može domoći velikog dijela poruke m jer ako Cathy odašilje $e_i \equiv \phi_i \circledast h + m \pmod q$ (koji Betty presreće) onda Betty može izračunati

$(e_i - e_1) \circledast h^{-1} \pmod q$ odnosno $\phi_i - \phi_1 \pmod q$. No kako su koef. ϕ-ova iz skupa $\{-1, 0, 1\}$ ovime može odrediti $\phi_i - \phi_1$, a iz toga može odrediti veliki broj koef. od ϕ_1, a onda i od m ako preostale koef. od ϕ_1 uspije pogoditi brute force metodom.

šta su to rešetke?
što je LLL-algoritam?

4. Napadi bazirani na rešetkama.

i) Napad na privatni ključ. Promotrimo sljedeću $2N \times 2N$ matricu (gdje će parametar α biti kasnije odabran)

$$(f_0, \dots, f_{N-1}, *, \dots, *)$$

$$\left(\begin{array}{cccc|cccc} \alpha & & & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ & \alpha & & & h_{N-1} & h_0 & \cdots & h_{N-2} \\ & & \ddots & & \vdots & \vdots & \ddots & \vdots \\ 0 & & & \alpha & h_1 & h_2 & \cdots & h_0 \\ \hline & & & & q & & & 0 \\ & & 0 & & & q & & \\ & & & & & & \ddots & \\ & & & & 0 & & & q \end{array}\right) = \begin{pmatrix} \alpha f_0 \\ \vdots \\ \alpha f_{N-1} \end{pmatrix}^T$$

$$(F \circledast G)_k = \sum_{i+j \equiv k \,(N)} F_i G_j$$

Neka je L rešetka generirana s retcima matrice ($\det L = q^N \alpha^N$)

Budući da je javni ključ jednak $h = g \circledast f^{-1}$ rešetka L

$h \circledast f \equiv g \pmod q$

$\Uparrow$

$h \equiv F_q \circledast g \pmod q$

$F_q \circledast f \equiv 1 \pmod q$

točni

će sadržavati vektor $\tau = (\alpha f, g)$ (zašto?)

prethodna stranica.

?

Heuristika, očekivana veličina najmanjeg vektora u

slučajnoj matrici dimenzije n i determinante D je između

$$D^{\frac{1}{n}} \sqrt{\frac{n}{2\pi e}} \quad \text{i} \quad D^{\frac{1}{n}} \sqrt{\frac{n}{\pi e}}.$$

U našem slučaju je

$n = 2N$ i $D = q^N \alpha^N$ pa je očekivana najmanja duljina

(ne puno) veća od

$$\boxed{s = \sqrt{\frac{N \alpha q}{\pi e}}.}$$

Implementaciji LLL-algoritma (par riječi o tome) će

imati najbolji šansu za locirati τ ako napadač odabere α

tako da maksimizira $\dfrac{s}{|\tau|_2}$ ✓ još jedna heuristika?

$\leftarrow$ τ treba biti što je manji mogući u odnosu na očekivanu duljinu najmanjeg vektora

tj. napadač treba odabrati α t.d. maksimizira

$$\frac{\alpha}{\alpha^2|f|_2^2 + |g|_2^2} = \left(\alpha|f|_2^2 + \alpha^{-1}|g|_2^2\right)^{-1} \quad \text{odnosno}$$

ako odabere $\alpha = \dfrac{|g|_2}{|f|_2}$. ✓ $\leftarrow$ javni podaci (jer $f \in \mathcal{L}_f$ i $g \in \mathcal{L}_g$)

Za tako odabrani α označimo s $|\tau|_2 = c_n s$.

(što je manji c_n, lakše je naći τ.) Može li se reći nešto precizniji od ovoga? Složenost je $O\left(e^{c_n \cdot N}\right)$?

(ii) Napad na poruku. Slično kao i gore, $\tau = (\alpha m, \phi) \dots$

(iii) Napad lažnim ključem.

Pretp. da u rešetci od male proje uspijemo pronaći neki mali vektor oblika $\tau' = (\alpha f', g')$ takav da za

$$f' \circledast e \equiv p \phi \circledast g' + m \circledast f' \pmod q$$ vrijedi

$$|p \phi \circledast g' + m \circledast f'|_\infty < q$$ onda će

takav f' dekriptirati danu poruku (zašto?).

Eksperimentalno iskustvo pokazuje da lažni ključevi ne predstavljaju sigurnosnu prijetnju.