Poszt-kvantum kriptográfiai algoritmusok matematikája

Markó Anna

Témavezető: Szabó István

2022.12.22.

Klasszikus kriptográfia

- Nyilvános kulcsú titkosítás, kulcscsere, digitális aláírás
- Biztonságuk alapja: prímfaktorizáció, diszkrét logaritmus probléma
- RSA, ECC, AES, DSA

Poszt-kvantum kriptográfia jelentősége

- CRQC: cryptanalytically relevant quantum computer
- Shor algoritmus(1994)

Algoritmus	CRQC hatása
RSA	Nem biztonságos többé
DSA	Nem biztonságos többé
ECDSA, ECDH	Nem biztonságos többé
AES	Nagyobb kulcsméret kell

Poszt-kvantum algoritmusok standardizációja

- NIST: National Institute for Standards and Technology

Kulcscsere	Digitális aláírás
CRYSTALS-Kyber	CRYSTALS-Dilithium, FALCON SPHINICS$^+$

- Lehetséges jelöltek: BIKE, Classic McEliece, HQC, SIKE

Rácselméleti problémák

Definíció (Rács):

Legyen $(b_1, \ldots, b_n)$ egy $\mathbb{R}^n$-beli bázis. Ekkor az $L = \{\sum_{i=1}^{n} \lambda_i b_i : \lambda_i \in \mathbb{Z}\}$ halmazt a $(b_1, \ldots, b_n)$ bázis által generált rácsnak nevezzük.

- A legrövidebb/legközelebbi vektor problémája

Definíció (Learning With Errors - LWE):

Adott $\mathbb{Z}_q$ q-adrendű gyűrű, $\mathbf{s} \in \mathbb{Z}_q^n$ és χ valószínűségi eloszlás. Legyen $\mathbf{a} \in \mathbb{Z}_q^n$ uniform eloszlásból és $\mathbf{e} \in \mathbb{Z}_q$ χ szerinti eloszlásból. A feladat meghatározni $\mathbf{s}$-et tetszőlegesen sok $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + \mathbf{e})$ pár ismeretében.

- CRYSTALS-Kyber, CRYSTALS-Dilithium

Falcon

- Titkos kulcs: $f, g, F, G \in \mathbb{Z}_q[x]/(x^n + 1)$
  $fG - gF \equiv q \mod (x^n + 1)$
- Nyilvános kulcs: h
  $h \equiv gf^{-1} \mod (x^n + 1)$

Kódalapú protokollok matematikai alapja

Definíció (Quasi-cyclic Syndrome Decoding Problem - QCSD):

Legyen $\mathcal{R} = \mathbb{F}_2[x]/(x^n - 1)$. Adott $h, y \in \mathcal{R}$, $t > 0$. Keresendő $(e_0, e_1) \in \mathcal{R}^2$ vektor, amire teljesül, hogy $|e_0| + |e_1| = t$ és $e_0 + e_1 h = y$.

- Quasi-cyclic Codeword Finding Problem - QCCF)
- Goppa-kód
- BIKE, Classic McEliece, HQC