Poszt-kvantum kriptográfiai algoritmusok matematikája

Markó Anna Erzsébet
Témavezető: Szabó István

A jelenleg gyakorlatban használt klasszikus kriptográfiai algoritmusok jelentős része olyan számelméleti problémák bonyolultságán alapszik, mint a prímfaktorizáció vagy a diszkrét logaritmus probléma. Ma már ismeretes, hogy ezek a problémák kvantumszámítógépekkel hatékonyan megoldhatóak - ezt először Peter Shor látta be 1994-ben. Nagyméretű kvantumszámítógépek mellett például az RSA, ECDSA, ECDH, DSA nem biztonságosak többé, így megnőtt az igény a poszt-kvantum kriptográfiai algoritmusok iránt. Ennek okán 2016-ban az NIST (National Institute for Standards and Technology) egy pályázati kiírás keretében, elindította a poszt-kvantum kriptográfiai algoritmusok standardizációjának folyamatát. Ennek keretében 2022. júliusában standardizálásra kiválasztották a CRYSTALS-Kyber kulcscsere protokollt, illetve a CRYSTALS-Dilithium, FALCON és SPHINICS$^+$ digitális aláírásokat. Ezenkívül megmaradtak lehetséges jelölteknek a jövőbeni standardizációra a következő kulcscsere protokollok: BIKE, Classic McEliece, HQC, SIKE. A félév során ezeken az eljárásokon keresztül jártam körül pár, a poszt-kvantum kriptográfia által kihasznált problémát, illetve protokollt.

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

Definíció (Shortest Vector Problem - SVP)**.** Adott L rácson keressük a legrövidebb nem nulla vektort: $\lambda(L) := \inf_{\mathbf{v} \in L \setminus \mathbf{0}} \|\mathbf{v}\|$.

Definíció (Closest Vector Problem - CVP)**.** Adott L rács és $\mathbf{v} \in \mathbb{R}^n$ mellett keressük azt az $\mathbf{u} \in L$ vektort, amely a legközelebb van $\mathbf{v}$-hez: $\mathbf{u} = \inf_{\mathbf{u} \in L} \|\mathbf{u} - \mathbf{v}\|$.

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.

Definíció (Short Integer Solution Problem - SIS)**.** Adott $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ és λ mellett keressünk $\mathbf{x} \in \mathbb{Z}^m$ vektort, amire $\|\mathbf{x}\| \leq \lambda$ és $\mathbf{A}\mathbf{x} = 0$.

A CRYSTALS-Dilithium és a CRYSTALS-Kyber eljárások az LWE probléma egy változata, a Module-LWE bonyolultságán alapszik. A standardizálásra kerülő digitális aláírások közül az NIST elsődlegesen is a CRYSTALS-Dilithiumot ajánlja. Ez a Module-LWE mellett a SIS egy variációját, a SelfTargetMSIS bonyolultságát is használja.

A FALCON szintén rácselméleti protokoll, viszont ez NTRU alapú. Az NTRU során faktorgyűrűben számolunk. A FALCON titkos kulcsát az $f, g, F, G \in \mathbb{Z}_q[x]/(x^n + 1)$ polinomok

adják, melyekre teljesül, hogy $fG - gF \equiv q \mod (x^n + 1)$. A nyilvános kulcs h, amire teljesül, hogy $h \equiv gf^{-1} \mod (x^n + 1)$.

A négy standardizációra kiválasztott protokoll közül a SPHINICS$^+$ az egyetlen nem rácselméleten - hanem hash-függvényeken - alapuló eljárás. A következő körbe került jelöltek közül egyik sem rácselméleten alapszik, várhatóan a jövőben valamelyik kiválasztásra is kerül majd, ezzel is növelve ezek arányát.

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 $e_0 + e_1 h = y$.

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

Definíció (Lineáris kód)**.** Legyen $\mathcal{R} = \mathbb{F}_q$. Egy C kódot lineárisnak nevezünk, ha lineáris altere az $\mathbb{F}_q$ feletti $\mathcal{R}^n$ vektortérnek.

Definíció (Bináris Goppa-kód)**.** Legyen $g(x)$ egy t-ed fokú, irreducibilis polinom $\mathbb{F}_{2^m}$ véges test felett, és $\sigma_1, \dots \sigma_n$ különböző $\mathbb{F}_{2^m}$-beli elemek, amelyek nem gyökei g-nek Ekkor a bináris Goppa kód: $C = \{c \in \{0,1\}^n : \sum_{i=1}^{n} \frac{c_i}{x - \sigma_i} \equiv 0 \mod g(x)\}$

A BIKE, Classic McEliece és HQC kódalapú protokollok. A BIKE alapját a QCSD és QCCF problémák bonyolultsága adja, a Classic McEliace bináris Goppa-kódokat használ, ami egy lineáris, hibajavító kód. A HQC a Ring-LWE egy kódalapú változata.

A SIKE (Supersingular Isogeny Key Encapsulation) a Diffie-Hellman kulcscsere SIDH (Supersingular Isogeny Diffie-Hellman) változatán alapszik.

Irodalomjegyzék

[1] Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process, 2022
`https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf`

[2] PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates
`https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4`

[3] Kinorányi Dóra: Poszt-kvantum kriptográfia
`https://web.cs.elte.hu/blobs/diplomamunkak/bsc_matelem/2021/kinoranyi_dora.pdf`

[4] A. Nitaj: The Mathematics of the NTRU Public Key Cryptosystem
`https://nitaj.users.lmno.cnrs.fr/ntru3final.pdf`

[5] ETSI TR 103 823 V1.1.2 (2021-10): CYBER; Quantum-Safe Public-Key Encryption and Key Encapsulation
https://www.etsi.org/deliver/etsi_tr/103800_103899/103823/01.01.02_60/tr_103823v01010

[6] O. Regev: The Learning with Errors Problem
https://cims.nyu.edu/~regev/papers/lwesurvey.pdf

[7] P.-A. Fouque, J. Hoffstein, P. Kirchne, V. Lyubashevsky, T. Pornin, T. Prest, T. Ricosset, G. Seiler, W. Whyte, Z. Zhang: Falcon: Fast-Fourier Lattice-based Compact Signatures over NTRU
https://falcon-sign.info/falcon.pdf