Smeu Florin-Ion, 342 C3

# Proiect Introducere in Criptologie

# Atac de aflare a cheii secrete pentru algoritmul Kyber

## Descriere algoritm

Kyber este un algoritm key encapsulation mechanism (KEM), a carui securitate se bazeaza pe dificultatea rezolvarii problemei learning with errors (LWE) pe latice. Kyber este unul dintre algoritmii candidati in proiectul de criptografie post-quantum NIST. El dispune de seturi diferite de parametri care vizeaza niveluri de securitate diferite. Concret, Kyber-512 vizeaza securitatea aproximativ echivalentă cu AES-128, Kyber-768 vizeaza securitatea aproximativ echivalentă cu AES-192, iar Kyber-1024 vizează securitatea aproximativ echivalentă cu AES-256.

## Descriere atac

Initial, Alice genereaza o pereche de chei, PA (public key) si sA (secret key). Ambele chei sunt vectori de polinoame. Spre exemplu, pentru K = 512, cheia este reprezentata de 512 coeficienti a doua polinoame de cate 256 de coeficienti. Pentru K = 1024 cheia va fi formata din 4 vectori de 256 coeficienti. Acesti coeficienti sunt alesi in intervalul [-2, 2].
Scopul atacului este aflarea coeficientilor din cheia secreta a lui Alice, sA.
Pentru fiecare vector din cheia secreta a lui Alice (pot fi 2, 3, sau 4 vectori) si pentru fiecare coeficient din vectorul respectiv, atacatorul va crea doua ciphertexturi c1 si c2, o cheie publica a lui Bob, PB, cat si un plaintext, m.  Interogand oracolul de mai multe ori, atacatorul obtine un parametru h pentru care mesajul returnat de oracol contine pe prima pozitie valoarea 1. Printr-o ecuatie simpla, stiind h, atacatorul poate descoperi coeficientul potrivit din cheia secreta a lui Alice.

## Implementare

Am implementat atacul pornind de la implementarea oficiala a algoritmului Kyber, realizata in limbajul C, disponibila pe Github. Fisierul attack.c este implementarea propriu-zisa a atacului si contine atacuri asupra celor trei versiuni de securitate a algoritmului Kyber: 512, 768, 1024, cat si oracolul care va da informatii atacatorului.

## Rulare

Pentru a crea executabilele necesare atacului, fisierul Makefile_attack in directorul /kyber/ref va primi ca argument tipul de atac:

- Ex: make -f Makefile_attack attack<K>, unde K poate lua valorile 512, 768, 1024.

Dupa acest pas, se poate rula atacul:

- Ex: ./attack<K>, K fiind ca in cazul precedent 512, 768 sau 1024, in functie de executabilul disponibil.

## Referinte

[1] An Efficient Key Mismatch Attack on the NIST Second Round Candidate Kyber, Yue Qin, Chi Cheng, Jintai Ding, IEEE Transactions on 2019

[2] CRYSTALS-KYBER Algorithm Specifications And Supporting Documentation, Roberto Avanzi, Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint,
Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, Damien Stehlé, April 2019