Opis obszaru badawczego

Implementacja i testowanie bezpieczeństwa algorytmów kryptografii post-kwantowej

Bartosz Naskręcki, cyberbezpieczeństwo

1. Charakterystyka obszaru badawczego

W dynamicznie rozwijającym się świecie gwarantem naszego bezpieczeństwa w sieci są algorytmy szyfrowania oparte na fundamentalnie trudnych matematycznie operacjach takich jak mnożenie czy potęgowanie. W ostatnich 30. latach do grona takich podstawowych operacji dołączyły operacje na krzywych eliptycznych, teoria samokorygujących kodów i operacje kratowe. Obecnie podstawowym działaniem Unii Europejskiej oraz amerykańskiego NIST jest wdrożenie standardów nowych algorytmów, które będą odporne na klasyczne ataki komputerów kwantowych oparte na algorytmie faktoryzacji Shora i algorytmie Grovera. W rozpoczętym w 2016 roku konkursie NIST zgłoszonych zostało szereg kandydatów na algorytmy post-kwantowe: opartych na izogeniach krzywych eliptycznych, opartych na teorii samokorygujących kodów oraz na operacjach wektorowych na kratach. Budowane są różne drastycznie nowe koncepcje schematów bezpieczeństwa, które wymagają starannego przeanalizowania i implementacji zgodnej z najwyższymi wymogami efektywności i ochrony. W 2024 roku wyłoniono już pierwsze standardy nowej kryptografii.

2. Motywacja

Dla współczesnych inżynierów oprogramowania i inżynierów cyberbezpieczeństwa ważnym aspektem warsztatu pracy jest zapoznanie się z najnowszą dokumentacją i algorytmami implementującymi przyszłe standardy kryptografii post-kwantowej. Tak jak RSA i wymiana Diffiego-Hellmana stanowiły fundament bezpieczeństwa w dziedzinie kryptografii matematycznej przez 30 lat, tak teraz algorytmy post-kwantowe będą filarami naszego cyberbezpieczeństwa przez kolejnych kilka dekad. Opanowanie warsztatu matematycznego związanego z najnowszymi ideami jest zarówno ciekawe poznawczo jak i bardzo wartościowe jeśli chodzi o wachlarz budowanych kompetencji inżyniera przyszłości.

3. Obecny poziom badań

W ramach projektów z zakresu geometrii arytmetycznej badam wraz ze studentami granice bezpieczeństwa algorytmów szyfrowania grafowego opartego na izogeniach krzywych eliptycznych. Testujemy granice bezpieczeństwa stosując wyrafinowane techniki algebraiczne oparte na najnowszych pracach. W zakresie pozostałych dwóch typów algorytmów: opartych na kodach i na kratach mam przygotowany program badawczy służący szybkiemu wdrożeniu studenta do tematyki i rozpoczęciu prac nad testowaniem i optymalizacją istniejących algorytmów. Tematyka kodów oraz krat jest obecnie omawiana na nowym przedmiocie z podstaw cyberbezpieczeństwa i algorytmiki post-kwantowej.

4. Tematyka badawcza

Obejmuje trzy główne nurty: uczenie z błędami (learning with errors), izogenie krzywych eliptycznych, kody Goppy i algorytm McElliece, algorytm NTRU i jego warianty. Do każdego z projektów dołączony jest starannie przygotowany program badawczy służący wdrożeniu, testowaniu oraz zrozumieniu podstaw omawianej tematyki. W zakres badań wchodzi intensywne zapoznawanie się z dokumentacją (white papers) oraz najnowszymi pracami (2020+) z zakresu ataków na testowane algorytmy.

5. Wymagania odnośnie członków projektu

Zakładam, że studenci przeszli podstawowy kurs algebry i teorii liczb. Potrafią swobodnie programować w języku Python oraz w wybranym wydajnym języku niskopoziomowym (np. C). Oczekuję gotowości do udziału w intensywnym seminarium szkoleniowym z zakresu wymaganego przygotowania matematycznego obejmującego algorytmikę teorioliczbową i algebraiczną.

6. Literatura

1. Post-Quantum Cryptography (Springer, 2009), https://link.springer.com/book/10.1007/978-3-540-88702-7
2. Post-quantum cryptography (ENISA, 2021), https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation
3. Post-quantum cryptography (NIST, 2025), https://csrc.nist.gov/projects/post-quantum-cryptography