Uzgadnianie informacji oraz wzmocnienie prywatności w kwantowych protokołach dystrybucji klucza

dr Miriam Kosik, specjalność - Cyberbezpieczeństwo

Charakterystyka obszaru badawczego

Proponowany obszar badawczy leży na pograniczu informatyki klasycznej i kwantowej - obejmuje badania łączące kryptografię kwantową oraz klasyczne algorytmy korekcji błędów. Istotną częścią protokołów kwantowej dystrybucji klucza jest etap tzw. **postprocessingu**, który następuje już po zakończeniu wymiany kwantowych bitów i wykonywany jest całkowicie przy pomocy klasycznego kanału komunikacji. Na skutek niedoskonałości aparatury oraz potencjalnych ataków klucz ustalony po obu stronach przy użyciu kanału kwantowego nie jest jednakowy. Postprocessing ma na celu usunięcie różnic w kluczu oraz zminimalizowanie informacji jaką może uzyskać potencjalny podsłuchiwacz. Do postprocessingu należy: oszacowanie poziomu różnic w kluczu ustalonym po obu stronach, usunięcie tych różnic oraz wzmocnienie prywatności (usunięcie informacji u potencjalnego podsłuchiwacza).

Motywacja

Postprocessing stanowi istotną część kwantowych protokołów kryptograficznych i jest kluczowym czynnikiem decydującym o ich bezpieczeństwie. Rozwijanie nowych technik w tej dziedzinie ma na celu poprawę bezpieczeństwa kwantowych protokołów dystrybucji klucza, dostosowanie ich do standardów kryptograficznych, jak również polepszenie złożoności obliczeniowej algorytmów, co w praktyce umożliwi szybsze generowanie kwantowych kluczy.

Tematyka badawcza

Zależnie od zainteresowań studentów istnieje możliwość skoncentrowania badań na różnych aspektach proponowanej tematyki. Przykładowo, dla osób zainteresowanych bardziej praktyczną stroną tematu prace mogą objąć implementację określonych algorytmów w wybranym języku programowania lub statystyczną analizę skuteczności różnych algorytmów korekcji błędów. Natomiast w podejściu bardziej teoretycznym prace mogą skupić się na podsumowaniu znanych algorytmów postprocessingu i oszacowaniu ilości informacji ujawnianej w różnych schematach QKD z uwzględnieniem fazy klasycznej.

Wymagania

Przydatna będzie znajomość podstaw algebry liniowej, wiedza z zakresu teorii informacji, kombinatoryki i umiejętność programowania. Przewidywana liczba studentów: 1 lub 2 osoby.

Literatura

1. Ramona Wolf, *Quantum Key Distribution. An Introduction with Exercises*, Springer 2021.
2. Ramona Wolf - wykłady: https://youtu.be/C5jpRPlSUR4?si=KIbdNIr6gbNiT4s1 .
3. Wykłady TU Delft OpenCourseWare - materiały do kursu *Quantum Cryptography*: https://ocw.tudelft.nl/courses/quantum-cryptography/
4. John Baylis, *Error-correcting codes: A mathematical introduction*, 1998.