Nr rejestracyjny: 2015/18/E/ST2/00327; Kierownik projektu: dr Karol Mieczysław Horodecki

W ostatnich latach nasza cywilizacja potrafi generować więcej bajtów zapisanej informacji w ciągu kilku dni, niż ilość bajtów informacji, która była zapisana od zarania dziejów ludzkości do czasów współczesnych. W ramach efektu „globalnej wioski" rośnie również potrzeba przesyłania tejże informacji na dalekie odległości. Jej spory procent stanowią tak zwane dane wrażliwe, podlegające ochronie prawnej, dotyczące naszej prywatności lub dóbr intelektualnych, do których mamy prawa autorskie. Wszystkie te dane podlegają dzisiaj przeróżnym atakom, a ich ochrona w czasie przesyłania i przechowywania stanowi niezwykle ważny problem.
Problemowi temu wychodzi naprzeciw kryptografia kwantowa - szybko rozwijająca się dziedzina kwantowej informatyki, której celem jest zapewnienie bezpiecznego przekazu informacji gwarantowanego przez prawa teorii fizycznej – mechaniki kwantowej. Tego problemu dotyczy również kryptografia post-kwantowa, która między innymi opiera się na fizycznej zasadzie niemożności przesyłania informacji szybciej niż światło. Dziedziny te łączą trzy dyscypliny: fizykę, matematykę i informatykę. Korzystając z aksjomatów fizyki, można udowodnić na gruncie matematyki, że informatyczny cel – bezpieczeństwo przekazu informacji, zostanie osiągnięty jeśli informacja przeznaczona do zaszyfrowanego przekazu, zostanie zakodowana odpowiednio – stosownie do tak zwanego protokołu kryptograficznego.
Celem konkretnych protokołów kryptograficznych jest zapewnienie jednego z dwóch zasobów: bezpiecznego losowego ciągu bitów - bezpiecznej losowości lub bezpiecznego, losowego ciągu bitów współdzielonego tylko przez osoby zaufane, czyli tak zwanego klucza kryptograficznego.
W obecnej chwili protokoły kwantowo-kryptograficzne są już dostępne komercyjnie i jakkolwiek nie pozwalają na prosty podsłuch, mają istotny słaby punkt – są wrażliwe na nowoczesne rodzaj ataków – włamania hakerów. Teoria dotycząca takich ataków nie jest w chwili obecnej dostatecznie rozwinięta. Kilkanaście publikacji w tej tematyce, dotyczy głównie ataków typu „koń Trojański" , które sprowadzają się do ingerencji w system w czasie rzeczywistym, zaś atak, który następuje w czasie produkcji lub przed użyciem urządzenia, nie jest jeszcze dobrze zbadany. Problem tych ataków dotyczy również kryptografii post-kwantowej.
Wobec takiego problemu, jednym z trzech głównych celów projektu jest zbadanie jak zależy ilość otrzymanego zasobu kryptograficznego (klucza i losowości) od siły i rodzaju ataku hakerów. Zamierzamy wypracować model teoretyczny pozwalający ocenić bezpieczeństwo przekazu nawet w przypadku częściowego włamania.
Kolejnym słabym punktem kryptografii kwantowej w jej oryginalnym podejściu, jest fakt, że użytkownik jest zmuszony zaufać specyfikacji urządzenia. Zaufanie takie bywa nieuzasadnione z powodu niedokładności produkcji lub wręcz złej woli producenta, który może świadomie przygotować urządzenie pozwalające na podsłuch. Z tego względu kolejnym celem projektu będzie badanie możliwości bezpiecznej komunikacji w przypadku zmowy producenta urządzeń z osobą podsłuchującą poprzez korelacje między urządzeniami kryptograficznymi. Badania będą miały również na celu stworzenie teorii bezpiecznej losowości jako tak zwanej teorii zasobu.
Podjęte badania będą zatem w dużej mierze dotyczyć tak zwanej kryptografii niezależnej od urządzenia, użytkownik będzie ufał tylko statystykom wyników urządzenia, a nie jego specyfikacji. Jednak z uwagi na znacznie wyższe zaawansowanie technologii zakładającej zaufanie do producenta, poświęcimy także uwagę tradycyjnemu scenariuszowi kryptografii kwantowej, gdzie zaufanie to ma miejsce.
Oczekujemy, że wyniki badań pozwolą na bardziej świadome korzystanie z urządzeń kwantowo-kryptograficznych użytkownikom, pozwalając na bezpieczną komunikację nawet przy założeniu częściowej kontroli nad nimi lub ich niesprawności w wyniku szumu. Mamy również nadzieję, że wypracowane w kontekście kryptografii techniki pomogą głębiej zbadać i zrozumieć naturę kwantowych zasobów przewidywanych przez mechanikę kwantową takich jak kwantowe splątanie, kwantowa nielokalność oraz kontekstualność, leżących u podstaw współczesnych kwantowych technologii.
W związku z opisanym na wstępie trudnym problemem przed którym stoi cywilizacja XXI wieku, który bezsprzecznie można nazwać wiekiem informacji, badania dotyczące ochrony przed różnorodnymi atakami na jej bezpieczeństwo, należą dzisiaj do jednych z najbardziej oczekiwanych.