Streszczenie projektu:

Kryptografia kwantowa oferuje bezprecedensowy poziom bezpieczeństwa, ale jest podatna na ataki na poziomie implementacji, które wykorzystują różnice pomiędzy teoretycznym modelem urządzeń a ich fizyczną realizacją. Co więcej, niektóre ataki hakerskie mogą sztucznie wywołać takie różnice. Powoduje to sytuację, w której obecna generacja technologii kwantowych jest mniej godna zaufania niż dobrze sprawdzone rozwiązania klasyczne. Nowa wersja kryptografii kwantowej - niezależna od urządzeń może rozwiązać ten problem, ponieważ z definicji jest odporna na wady fizyczne. Jej nazwa wzięła się stąd, że przy testowaniu bezpieczeństwa nie bierze się pod uwagę wewnętrznej pracy sprzętu. Jedyną wartością jest rozkład prawdopodobieństwa danych na wyjściu.

Niestety, najnowocześniejsze eksperymenty niezależne od urządzeń są o wiele rzędów wielkości za wolne i działają na znacznie mniejsze odległości niż te wymagane do celów praktycznych. Celem projektu jest poprawa podstaw teoretycznych, na których opiera się niezależna od urządzeń kryptografia kwantowa, do takiego poziomu, że stanie się ona możliwa do implementacji w rzeczywistych zastosowaniach. Osiągniemy to poprzez zbadanie nowych testów nieklasyczności, które są podstawą całej kryptografii kwantowej, usprawnienie dowodów bezpieczeństwa i wynalezienie nowych konfiguracji eksperymentalnych.

Związek z tematem poruszanym w programie:

Bezpieczeństwo i prywatność w systemach zdecentralizowanych i rozproszonych jest niemożliwe bez bezpiecznej komunikacji i prywatnych liczb losowych, które są dokładnie tymi komponentami, które poprawiamy w naszym projekcie. Konkretne docelowe rezultat, do których odnosi się nasz projekt to:

1. Projektowanie hybrydowych rozwiązań software-hardware w zakresie bezpieczeństwa i prywatności - Natura niezależnej od urządzeń kryptografii kwantowej to badanie wzajemnego oddziaływania sprzętu i oprogramowania. Stworzymy nowe pomysły sprzętowe i zaprojektujemy protokoły dostosowane do tego sprzętu.

2. Projektowanie modeli weryfikacyjnych dla rzeczywistych zastosowań rozwiązań z zakresu prywatności i bezpieczeństwa -Większość zadań naszego projektu sprowadza się do opracowania metod weryfikacji, jak daleko rzeczywista wersja danego urządzenia jest od idealnego przypadku.