Główną motywacją dla badań w dziedzinie obliczeń kwantowych jest obietnica osiągnięcia znacznego przyspieszenia obliczeniowego dla problemów algorytmicznych kluczowych w wielu obszarach technologii, w tym kryptografii i optymalizacji. Kwantowe przetwarzanie informacji zostało wprowadzone jako rozwiązanie problemów pojawiających się w klasycznej informatyce. Do tej pory rozwijano dwa główne zastosowania obliczeń kwantowych: protokoły kwantowe, których poziom bezpieczeństwa jest nieosiągalny dla protokołów opartych na informacji klasycznej, oraz algorytmy kwantowe, które mogą przełamać ograniczenia szybkości konwencjonalnych komputerów. W drugim przypadku najbardziej znanymi algorytmami są algorytm Shora, który może faktoryzować liczby w czasie wielomianowym oraz algorytm Grovera do wyszukiwania w bazie danych, który osiąga złożoność pierwiastkową względem rozmiaru bazy.

O ile duże zainteresowanie w obszarze obliczeń kwantowych jest w pełni uzasadnione nowymi teoretycznymi osiągnięciami, naukowcy wciąż odkrywają nowe ograniczenia. Problemem jest dekompozycja operacji unitarnych, w szczególności na sprzęt o ustalonej topologii z dużymi ograniczonymi. Co więcej, okazało się, że algorytmy kwantowe są wrażliwe na zakłócenia, co ma niekorzystny wpływ na wyniki obliczeń. Doprowadziło to do opracowania nowej gałęzi informatyki kwantowej – teorii kwantowych kodów korekcyjnych. W przypadku kwantowych protokołów kryptograficznych wykryto ataki sprzętowe oparte na lukach bezpieczeństwa konwencjonalnej elektroniki. To pokazało, że teoretyczne bezpieczeństwo potwierdzone prawami fizyki może być nieosiągalne w zastosowaniach.

Nowatorskość prezentowanego projektu opiera się na oryginalnym podejściu do analizy algorytmów kwantowych, opartym na badaniu danych wejściowych. Za jego pomocą scharakteryzujemy zastosowanie algorytmów kwantowych w rzeczywistych scenariuszach, biorąc pod uwagę, że algorytmy są narażone na ataki, w tym te oparte na dostarczaniu szkodliwych danych.

Ponieważ kwantowe wyszukiwanie przestrzenne zostało dobrze przeanalizowane pod kątem wydajności, planujemy wykorzystać tę rodzinę algorytmów jako punkt wyjścia dla projektu. Rozpatrzymy ataki algorytmiczne oparte na wyjątkowej konfiguracji i niedokładnej implementacji algorytmu. Celem takich ataków jest celowe i systematyczne zwiększenie czasowej złożoności obliczeniowej. Przedstawimy formalny opis odporności rodziny algorytmów kwantowego przeszukiwania przestrzennego. Opiszemy związek między strukturą sieci a zdolnością do przeprowadzenia ataku algorytmicznego. Opiszemy, w jaki sposób można wykorzystać wiedzę o ataku algorytmicznym, aby zmniejszyć jego wpływ oraz jak skuteczność ataku zależy od modelu grafu losowego używanego do opisu danych. Nasze wyniki zapewnią powiązanie struktury danych ze złożonością algorytmów kwantowych.