Grover-Based Key Search on a Block Cipher

Authors: Aleksi Talman

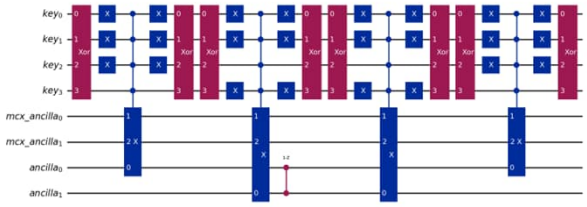
Introduction

Grover's Algorithm provides a quadratic speedup for unstructured search problems, making it a central tool for evaluating the future security of symmetric cryptography. This poster summarizes the main findings from a continuation project arising from the completion of a Master's Thesis "*Exploring Grover's Algorithm in Brute Force Attacks*", written during the first year of the *BLimPQC* project. The initial work done in the Master's Thesis implemented an 8-bit key search on an older IBM device comparing its performance to a classical search, while the continuation project builds upon the thesis switching focus towards smaller key sizes and more recent QPUs.

Grover's Algorithm for a key search

Grover's algorithm relies on the oracle function to be able to distinguish the correct solution from all the other candidates. In this quantum key search implementation, the goal is to identify the correct secret key without relying on any prior knowledge of it. The key search problem can be created into a quantum oracle that marks the correct key by applying a phase flip when the candidate key satisfies the encryption relation for all the plaintext blocks.

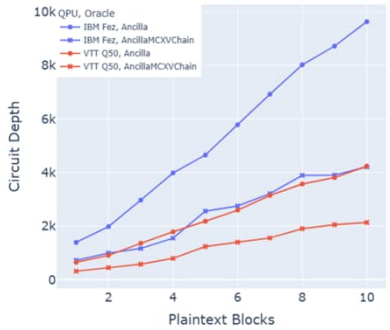
The oracle must identify such secret key *k* that $m \oplus k = c$, where both the plaintext *m* and the ciphertext *c* are known. The plaintext is encrypted in blocks, and the length of the plaintext must satisfy $|m| \equiv 0 \pmod{n}$. The search space consists of $N = 2^n$ quantum states that represent the secret key candidates for a key length of *n*.



The custom oracle when n = 4, plaintext length is $2n$ and ancilla qubits are used to save intermediary results of each ciphertext comparison.

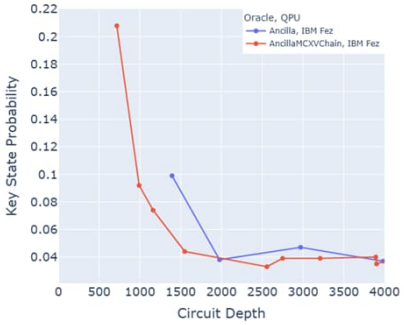
Results

The ancilla based oracle proved to be the correct approach for performing a Grover-based key search on a block cipher. Compared to the oracle implemented during the Master's Thesis, which requires only *n* qubits, the ancilla oracle requires $\frac{|m|}{n}$ additional qubits, dictated by the amount of plaintext blocks. As the number of blocks increases, the number of multi-qubit gates grows linearly, causing a steep rise in circuit depth. In an additional effort to reduce the circuit depth, an optimized version of the *MCX Gate* was explored. By using the *MCX VChain* variant, the circuit depth reduced by nearly *50%*.



Circuit depths for varying plaintext lengths in a 4-bit block cipher key search executed on different quantum hardware using varying oracle implementations.

A practical depth limit was also identified: once the circuit depth exceeds *~1500*, the correct state is no longer distinguishable from the overall distribution due to noise. For shallower circuits, the correct state remains identifiable, though its probability does not exceed *25%.*



Searched key state probability as a function of circuit depth for a 4-bit block cipher key search using varying oracles executed on *IBM Fez.*

VTT Q50 has a more connected topology than the IBM Fez, thus it can provide a *~50%* reduction in circuit depth for this key search implementation. Despite this advantage, the device currently produces only noisy results, preventing distinguishable amplification of the searched state. Execution fidelity compared to ideal simulation remains near zero.

Conclusions

- **Oracle constructions utilizing ancilla qubits enable key searches on a block cipher.**
- **The minimum qubit requirement for a Grover-based block cipher key search is $n + \frac{|m|}{n}$. Qubit requirement will increase if additional optimization measures or more complex encryption functions require additional qubits to be used.**
- **A practical circuit depth limit of *1500* was identified: circuits below this threshold still amplify the searched state, while deeper circuits suffer from noise.**
- **Higher qubit connectivity improves Grover-based implementations by reducing circuit depth.**
- **Execution fidelity remains near zero.**

Contact: Aleksi Talman, Associate Research Scientist
Tel. +358 5033 88993, aleksi.talman@vtt.fi