Optimizing Quantum Oracle for Standard Hash Algorithms

Korea University
Sangheon Lee, Mingyu Cho

September 20, 2020

Table of Contents

Introduction

Previous Work

- Studied the basics of quantum computing and Grover's Algorithm
- Analysis of reversible quantum S-DES oracle and its construction
- Implementation of quantum S-DES oracle with Grover's Algorithm in Microsoft Q#

Motivation

- Targeting SHA-2/3
  - Current de facto standard hash algorithm
- Goal is to perform a preimage attack.
  - The most straightforward to apply Grover's Algorithm.
  - It will be assumed that Grover's Algorithm(or some variation of it) will be applied
  - Therefore target is to optimize the quantum oracle for SHA-2/3.

Recap: Grover's Algorithm

- Searching in an unordered database among 2^n elements takes $\tilde{\mathcal{O}}(2^{n/2})$ time complexity and $\tilde{\mathcal{O}}(n)$ quantum space complexity
- Proved to be optimal in general
- Specifically, improved Grover's Algorithm for collision search yields $\tilde{\mathcal{O}}(2^{n/3})$ time complexity and (quantum) space complexity [BHT98]
  - However, quantum queries are costly in this algorithm

Chailloux's Algorithm [CNPS17]

- Use poly-time qubits and reduce time complexity to $\tilde{\mathcal{O}}(2^{2n/5})$ for collision search and $\tilde{\mathcal{O}}(2^{3n/7})$ for multi-target preimage attacks with additional classic memory

SHA-2/3 Pre-image Attack Cost Estimation [ADMG+16]

- Suggest cost metric for quantum computation based on surface code
- Theoretically implement reversible SHA-2/3 quantum circuits
- Estimate required physical resources and its scale

Expectations

- Focus on micro-scale improvement(regarding quantum oracle)
- May be able to reduce the cost in at least one of the following metrics:
  - The cost metric from before
  - The raw number of gates
  - The number of levels after achieving parallelization
- Main target will be the cost metric, not the gates or the levels

In-depth Topics

- Surface code(Toric code) : topological quantum error correcting code
- Cost metric based on surface code
- T-par [AMM14] : an quantum circuit optimization tool
- Advanced quantum circuit (in-place adder, *etc.*)

Surface Code

Surface code and physical qubits

This summary is heavily based on [FMMC12].

- Surface code is a method to construct *logical* qubits from physical qubits with acceptable relativce error tolerance [CRSS97]
- Logical qubits are more efficient than their physical counterparts
- The tolerance of surface codes to errors is high as about 1%
- However, ensuring high tolerance requires massive physical qubits and sequential Toffoli gates
  - "We assume an error rate approximately one-tenth the threshold rate, which implies that we need about 14,500 physical qubits per logical qubit to give a sufficiently low logical error rate to successfully execute the algorithm"

Surface code and physical qubits

- However, ensuring high tolerance requires massive physical qubits and sequential Toffoli gates
  - "A much larger part of the surface code is however needed to generate and purify the special ancilla $|A_L\rangle$ states that are used in the Toffoli gates.""
  - Applying Shor's Algorithm to 2,000-bit integer requires 2.2×10^{12} $|A_L\rangle$ states and takes about 26.7 hours
  - The surface code needs to generate these states in a timely manner

Surface code and physical qubits

- However, ensuring high tolerance requires massive physical qubits and sequential Toffoli gates
  - "We assume an error rate approximately one-tenth the threshold rate, which implies that we need about 14,500 physical qubits per logical qubit to give a sufficiently low logical error rate to successfully execute the algorithm"
  - In result, 58 million qubits are required for computation
  - Additionally 1 billion qubits are required for generating $|A_L\rangle$ states
- Hopefully, "the size of the quantum computer is quite sensitive tothe error rate in the physical qubits."
  - "For example, improving the overall error rate by about a factor of ten, as detailed in Appendix M, can reduce the number of physical qubits by about an order of magnitude, to about 130 million, although leaving the execution time unchanged."

Introduction: Qubit operators

Quantum computation is based on qubits: two-level quantum systems

- Based on quantum physics and election spins

These electron spins can be reprensented by various operators such as Pauli-X, Y, Z operators.

Qubit operators

Basic recap of Pauli operators and qubit operators:

- Ground state for $\hat{Z}$ axis : $|g\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
- Excited state : $|e\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$
- $\hat{Z} = \hat{\sigma_z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, with eigenvalues $+1$ and -1 for $|g\rangle$, $|e\rangle$.
- $\hat{X} = \hat{\sigma_x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, with eigenvalues $+1$ and -1 for
  $|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|g\rangle + |e\rangle)$,
  $|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|g\rangle - |e\rangle)$.
- $\hat{Y} = -i\hat{\sigma_y} = \hat{Z}\hat{X} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, which is real unlike $\hat{\sigma_y}$.

Qubit operators

These qubit operators satisfy the following:

$$\begin{aligned} \hat{X}^2 = -\hat{Y}^2 = \hat{Z}^2 = I \\ \hat{X}\hat{Z} = -\hat{Z}\hat{X} \\ [\hat{X}, \hat{Y}] = \hat{X}\hat{Y} - \hat{Y}\hat{X} = -2\hat{Z} \end{aligned} \tag{1}$$

Also note that each measurement based on each quantum operators yields one of its eigenstates. For example, M_Z will return $|g\rangle$ or $|e\rangle$, while M_X will return $|+\rangle$ or $|-\rangle$.

Qubit errors

Qubits errors are random $\hat{X}$ bit-flip and/or $\hat{Z}$ phase-flip.

- These single-qubit errors can be undone after detection
  - Erroneous $\hat{Z}$ can be cancelled with another $\hat{Z}$ since $\hat{Z}^2 = I$
- Also, applying qubit operation does not alter the probability of its eigenstate

Thus detection, rather than correction, is the key point of surface code.

Qubit errors

- However since $[\hat{X}, \hat{Z}] \neq \hat{0}$, sequential measurements of $\hat{X}$ and $\hat{Z}$ might conflict each other (since $\hat{X}\hat{Z} \neq \hat{Z}\hat{X}$).
- This problem can be avoided by measuring multi-qubits at once. Consider qubit a and b and operation $\hat{X}_a\hat{X}_b$ and $\hat{Z}_a\hat{Z}_b$, then these two operations do commute!

$$\begin{aligned}
[\hat{X}_a\hat{X}_b, \hat{Z}_a\hat{Z}_b] &= (\hat{X}_a\hat{X}_b)(\hat{Z}_a\hat{Z}_b) - (\hat{Z}_a\hat{Z}_b)(\hat{X}_a\hat{X}_b) \\
&= \hat{X}_a\hat{Z}_a\hat{X}_b\hat{Z}_b - \hat{Z}_a\hat{X}_a\hat{Z}_b\hat{X}_b \\
&= (-\hat{Z}_a\hat{X}_a)(-\hat{Z}_b\hat{X}_b) - (\hat{Z}_a\hat{X}_a)(\hat{Z}_b\hat{X}_b) \\
&= \hat{0}
\end{aligned} \tag{2}$$

References

References I

Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John Schanck, *Estimating the cost of generic quantum pre-image attacks on sha-2 and sha-3*, International Conference on Selected Areas in Cryptography, Springer, 2016, pp. 317–337.

Matthew Amy, Dmitri Maslov, and Michele Mosca, *Polynomial-time t-depth optimization of clifford+ t circuits via matroid partitioning*, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **33** (2014), no. 10, 1476–1489.

Gilles Brassard, Peter Høyer, and Alain Tapp, *Quantum cryptanalysis of hash and claw-free functions*, Latin American Symposium on Theoretical Informatics, Springer, 1998, pp. 163–169.

References II


André Chailloux, María Naya-Plasencia, and André Schrottenloher, *An efficient quantum collision search algorithm and implications on symmetric cryptography*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2017, pp. 211–240.


A Robert Calderbank, Eric M Rains, Peter W Shor, and Neil JA Sloane, *Quantum error correction and orthogonal geometry*, Physical Review Letters **78** (1997), no. 3, 405.


Austin G. Fowler, Matteo Mariantoni, John M. Martinis, and Andrew N. Cleland, *Surface codes: Towards practical large-scale quantum computation*, Physical Review A **86** (2012), no. 3.