# Insert Title Here

Korea University
Sangheon Lee, Mingyu Cho

September 15, 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

- (blah blah blah)

# 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

(blah blah blah)

# In-depth Topics

# 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.*)

# 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.