TOWARDS HYBRID QUANTUM–CLASSICAL CIPHERSUITE PRIMITIVES

by

H Shelton Jacinto

A dissertation

submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy in Electrical and Computer Engineering

Boise State University

May 2020

BOISE STATE UNIVERSITY GRADUATE COLLEGE

DEFENSE COMMITTEE AND FINAL READING APPROVALS

of the dissertation submitted by

H Shelton Jacinto

Dissertation Title: Towards Hybrid Quantum–Classical Ciphersuite Primitives

Date of Final Oral Examination: 6th April 2020

The following individuals read and discussed the dissertation submitted by H Shelton Jacinto, and they evaluated the presentation and response to questions during the final oral examination. They found that the student passed the final oral examination.

Nader Rafla, Ph.D., P.E.	Chair, Supervisory Committee
Hao Chen, Ph.D.	Member, Supervisory Committee
Liljana Babinkostova, Ph.D.	Member, Supervisory Committee

The final reading approval of the dissertation was granted by Nader Rafla, Ph.D., P.E., Chair of the Supervisory Committee. The dissertation was approved by the Graduate College at Boise State University.

For my wife, Bethany, and my children, Daniel and Emma.

ACKNOWLEDGMENTS

I would like to express my gratitude to everyone who supported me throughout the course of preparing the work for this dissertation. I am most thankful for their guidance, invaluable constructive criticism, and friendly advice during my work. I would like to especially thank my advisor, Dr. Nader Rafla, for putting up with my crazy ideas and ensuing mathematical jargon when completing my research, his support and guidance when things got tough, and his endless cheesy jokes and general camaraderie, my committee members Dr. Hao Chen and Dr. Liljana Babinkostova for taking the time to review my research avenues and collaborate in finding new ways to solve them, and my old lab-mates Luka Daoud, Kamran Latif, Danyal Mohammadi, and Marcus Pearlman for their friendship and fellowship during the ups and downs of completing a dissertation.

I would also like to show my deepest thanks for the opportunity brought to me at the Air Force Research Lab in Rome, NY by Dr. Bryant Wysocki and Dr. Timothy Kroecker, to collaboratively research with the Quantum Information Science (QIS) group under a fellowship that will prove to be a lifelong connection. Of the QIS group I would like to especially thank Dr. Paul Alsing for his endless questioning, Dr. James Schneeloch for his thoughts and discussions into the characterization of entanglement, Dr. Christopher Tison for his endless assistance when dealing with optimizers, Dr. Matthew Smith for exposing me to the hardware and design aspects of integrated silicon photonics, Dr. Shannon Ray for working with me to help narrow down possible solutions to my entropy problem, and my largest support, Dr. Michael Fanto for all of

his assistance in teaching me how to operate in a photonics lab, handling the mountain of government paperwork to keep me at AFRL, and for countless discussions about new collaboration and research avenues possible within the quantum photonics and quantum computing teams.

I want to also take this opportunity to thank the countless experts in quantum fields for their discussions with me at various conferences, including Dr. Anne Broadbent for her discussions with me about my observational entropy problem, Dr. Zvika Brakerski for his brief discussion with me about quantum homomorphism, and Dr. Philip Walther (and students) for discussing their works and possible avenues of collaboration with regards to implementation of quantum homomorphic schemes, blind quantum computing, and applications of the integrated silicon single photon processor.

And last but certainly not least, I would like to thank my family, my wife, and my children for their effort to keep me motivated to finish my dissertation work in a timely fashion; to stay focused on what needed to be accomplished.

ABSTRACT

With the dawn of quantum computing in scale, current secure classical primitives are at risk. Protocols with immediate risk of breach are those built on the advanced encryption standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms. To secure classical data against a quantum adversary, a secure communications ciphersuite must be developed. The ciphersuite developed in this work contains components that do not necessarily rely on quantum key distribution (QKD), due to recent insecurities found when a QKD–based protocol is faced with a quantum eavesdropper.

A set of quantum–classical ciphersuite primitives were developed using less common mathematical methods where a quantum adversary will take a non–deterministic polynomial-time to find a solution, but still easy enough for communicating classical computers to evaluate. The methods utilized for this work were created from random walks, lattices, symplectic mappings, combinatorics, and others. The hardware methods developed in this work rely on either classical laser-light, or entangled quantum states, with matching optimization developed from global optimization theories.

The result of this work is the creation of non–QKD hybrid quantum-classical set of secure ciphersuite primitives, built and expanded from existing classical and post-quantum security schemes, for both classical and quantum information. In the tight integration between quantum and classical computers, the security of classical systems with quantum interaction is essential.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CRP – Challenge Response Pair

CSPRNG – Cryptographically Secure Pseudo-Random Number Generator

DSA – Digital Signature Algorithm

ECDH – Elliptic Curve Diffie-Hellman

FPGA – Field Programmable Gate Array

HMAC – Hash Message Authentication Code

IID – Independent and Identically Distributed

IP – Intellectual Property

LWE – Learning With Errors

MITM – Man-in-the-Middle

MZI – Mach-Zehnder Interferometer

OTP – One-Time-Pad

POWF – Physical One-Way Function

PPM – Parts Per Million (10^{-6})

PRNG – Pseudo-Random Number Generator

PUF – Physically Unclonable Function

QDMA – Quantum Direct Memory Access

QHF – Quantum Hash Function

QIA – Quantum Identity Authentication

QKD – Quantum Key Distribution

QPP – Quantum Photonic Processor

QPU – Quantum Processing Unit

QTP – Quantum Teleportation

QW – Quantum Walk

RAM – Random Access Memory

RLWE – Ring Learning With Errors

ROM – Read Only Memory

RSA – Rivest-Shamir-Adelman

SSL – Secure Socket Layer

TLS – Transport Layer Security

CHAPTER 1

INTRODUCTION

The prospects of quantum computing[1] have driven the search for fully functional quantum processing units. Recent success in developing proof-of-concept quantum processors in several technological mediums such as trapped-ions, superconducting materials, and photonics, has prompted the question of how to integrate the processors into our daily lives in a manner that classical computers have filled for decades.

When we look at where quantum computers will fit into our daily regime of computer usage, the most obvious short-term application is as an acceleration co-processor. Back in the early 1980s there were processors with math co-processors [1], and once the technology had adapted where mathematics co-processors were commonplace, they were integrated into the main processing unit. In the later 1980s and 1990s, there was the rise of discrete graphics co-processors [2] in the form of graphics processing units (GPUs), which are still commonplace today due to their efficiency in calculating and displaying visual media. The near-term for quantum will be similar; a main processor with some form of quantum offloading for both efficiency and speed in calculating specific problem sets that are easier when utilizing quantum mechanics.

With quantum offloading in mind, the first step of mass quantum utilization is the integration of quantum processing units into our communications to help speed up

[1]For a brief introduction to some quantum computing math basics, please refer to Appendix A.

and secure ourselves against any malicious quantum adversary. By utilizing methods of multi-party access devised recently in the homomorphic space [3, 4] with a strong, secure key-exchange, this becomes a distinct possibility. Data encoded into entangled qubits, controlled by a classical computer, can afford the computational overhead necessary for larger learning-with-errors key agreements that are suitable for multiple parties to communicate with differing permissions to data access [5]. The three major topics of interest to make this dream become a reality are quantum computational structures, secure learning-with-errors based key exchange agreements, and the basis of quantum homomorphic schemes for working, and computing, on secure data.

The concept of the need for security has been well established and with the advent of shared-resource computing, the risk of information leakage further increases. In many instances information may be of an extremely private, confidential, or proprietary nature. Due to the value of private information which can be transmitted by means of technology, there is an inherent need to secure the information through the entire process of collection, processing, transmission, reception, and consumption. The data transmitted and consumed by computer users needs protection both in classical computational systems and quantum computational systems.

By utilizing quantum primitives, such as interference, entanglement, and superposition, intertwined with classical computing ideals, a secured quantum–classical hybrid communications protocol and ciphersuite primitives need to be developed for communication between a classical computer and quantum devices, or even quantum-to-quantum computing communication applications.

1.1 Motivation

Many researchers are focused on researching secure primitives for a post-quantum era when quantum computers are at scale and are ubiquitous devices in our lives [6]. There has been much excellent research in this field of post-quantum cryptography between classical computers and a quantum eavesdropping adversary [7, 8, 9], but there is a distinct lack of research on current quantum-to-quantum computing secure primitives, their integration into classical computing systems and the interactions between classical and quantum clusters. All communications requiring any form of secrecy should be estimated to be at least NP-hard, e.g. take a non-deterministic polynomial amount of time to solve, for a quantum adversary. In an example where a classical computer is operating with a single or a cluster of quantum devices, the classical computer should not need to worry about one of the quantum devices being an adversary while interfaced with another quantum device.

Ideally, quantum computing would be capable of blind server-sided computation but there are several hurdles to be passed before this can be a reality due to the necessitated usage of large entangled cluster states. Until this time, there is still a lack of security in current protocols, as found by a NIST report in 2016 [6]. This work will solve both the necessity for large entangled cluster states and overcome classical limitations in post-quantum primitives, i.e. excessively large key sizes, output string lengths, and the insecurity of known primitives such as the Rivest-Shamir-Adleman (RSA) public-key cryptosystem, the elliptic-curve DiffieHellman (ECDH) key agreement, and the digital signature algorithm (DSA).

A simple generalization is that a quantum key distribution (QKD) approach to security would be the easy answer, but this is swiftly countered. In 2007, it was

found that a known plaintext attack could be used to entirely reveal the contents of a string, of a distributed key by QKD, when a part of a plaintext was known to the eavesdropper, Eve, through the mutual information security criterion between Eve and legitimate users, Alice and Bob [10]. To help fix this issue, the trace distance criterion was introduced by M. Koashi in 2009 [11], showing that the distance between the distributed quantum state and an ideal quantum state with Eve's quantum system decouples from the quantum system shared between Alice and Bob.

Leading into the work by M. Koashi was the work by Shor and Preskill in 2000, proving that entanglement-based QKD is equivalent to prepare and measure QKD systems such as BB84 [12]. The proof employed the same mutual information criterion, thus this approach was applied to the trace distance criterion in 2009 [11]. Yuen immediately followed with his criticisms on the security of QKDs [13], with a general warning that the security of QKD is not sufficient and that the trace distance measure will not provide "universal composability" which is supposed to guarantee independent and identically distributed (IID) keys. With this information in focus, a large motivator for this dissertation work is to develop a system that does not rely on QKD but instead on small states of entangled qubits or qubits that undergo entanglement during processing, a system where entanglement distribution is the major resource of interest.

1.2 Dissertation Overview

1.2.1 Thesis Statement

The objective of this research is to answer the following question:

Can a set of secure communication primitives be designed that will work interchangeably between classical and quantum computers; if so, how do we use the primitives together?

Specifically, if we have a set of secure primitives operating together in an asymmetric client-server model connection between a classical and a quantum computer, is it possible to secure their communications in a manner in which a quantum adversary will be met with a NP-hard problem?

1.2.2 Research Objectives

The objectives and main areas investigated are summarized as follows:

1. The development of a non-QKD approach towards secure communication; important where we do not want the complexities and side-channel attacks present in a standard QKD protocol. The original proposed work covers the development of a new form of quantum hashing inspired by sponge functions, with the benefit that quantum mechanics will necessitate that the function is reversible and may also be composable.

2. The development and utilization of a quantum photonic processor (QPP) with 1 ppm resolution for entangled photon usage and processing. The previous platform was originally developed as a joint work between AFRL and MIT [14], where the controlling hardware and software was completely renewed such that there is now very high resolution control of the QPP to enable fine-grained control over phase settings operating on single photons. The work here leads into an updated photonics processor.

3. The utilization of quantum teleportation (QTP) theory for inter-quantum-processor communication, where there is the ability to utilize teleportation within a quantum homomorphic scheme that can effectively link two adjoint lattices with the communication of inconsequential information over a classical channel.

4. The final development of many components required for a quantum ciphersuite such that there can exist a lattice-based key exchange protocol, a loss-less hash-based compression stream cipher, and an efficient identity authentication mechanism.

1.3 Contributions

The contributions of this work may appear varied, but all work together to form one common goal: A ciphersuite is developed that is hybrid quantum-classical in the sense that both are required to create a secured method of communication that does not require QKD. While continuing to complete this research, several other items needed to be developed that should have their own individual showcase and also count as contributions to the field developed during the completion of the main contributions.

Contributions and their brief descriptions are as follows:

1. Development of the first quantum sponge function, capable of absorbing an arbitrary amount of information and producing a keyed and reversible arbitrary-size output stream that can be used in other applications.

2. Development of the first physically unclonable function based on an all-optical linear interferometer array with the additional capability to be reconfigured, and capable to be used for identity verification and hardware keying.

3. Development of the embedding mechanism to map a quantum hash onto a lattice to be used in alternate methods other than just hashing. This development also includes the arbitrary extensions of a quantum walk through a feedback mechanism.

4. The development of an alternate to hardware identity authentication utilizing physically unclonable functions which is a method of multiparty authentication with single photons, including an optional mechanism to have a multiparty contribution key.

5. Development of a new method of optimizing the linear interferometer network to generate arbitrary output profiles through a topological graph optimization technique.

1.4 Dissertation Layout

The work in this dissertation is organized in the following manner: Chapter 1 (this chapter) explains the research motivation and dissertation overview, including objectives and contributions. Chapter 2 explains the construction of a quantum sponge function, from the base classical sponge to the conception of methods necessary to build a quantum sponge from hash-base to the constructing of a connected graph. Chapter 3 describes two new methods of identity and message authentication, with limited experimentation, based on optical physically unclonable functions, and a strict photon-only authentication protocol. Chapter 4 describes a simple method of turning a quantum-walk-based hash function and associated developed quantum sponge function from Chapter 2 into a simultaneous message passing model with classical side-information. Chapter 5 shows the theory behind a quantum photonics processor

that was used for experimentation in Chapter 3 along with, most importantly, the optimization technique developed and utilized to enable fine-grain control of output data. Chapter 6 gently touches on a developed command-line quantum photonics processor simulator. Chapter 7 wraps-up the work with conclusions, recommendations, and future direction that this dissertation has led to and that research to expect in the future in similar fields of quantum cybersecurity.

CHAPTER 2

THE QUANTUM SPONGE

Sponge functions, as originally described by G. Bertoni et al. [15], were derived in the search for a cryptographic hash function that behaves similarly to a random oracle. An image of the architecture of a sponge function is shown in Figure 2.1. Since iterated hash functions often have state collisions (collisions in the chaining value), the ideal structure of a collision-less hash function was proposed in the form of a *sponge* function by G. Bertoni et al. A function with a finite state was developed in Bertoni et al.'s work, where an arbitrary sponge function could only be distinguished from a random oracle due to their respective inner collisions (collisions where two differing message sets may produce a collision of the *internal* state, not the output chaining value). Since a random oracle can take any input string and map it to an arbitrarily long output string, the theoretical sponge construction should be able to satisfy all the security criteria listed for a good hash function [16]. The output of the random oracle is also completely random, where any produced bits should be uniformly and independently distributed for any input, but for an application to work as a sponge function there is a constraint of an identical input generating an identical output over any number of trials. The mapping of input string to an arbitrarily long output string is essential for the work shown in this dissertation and serves as the basis for extension on many fronts, described in further chapters.

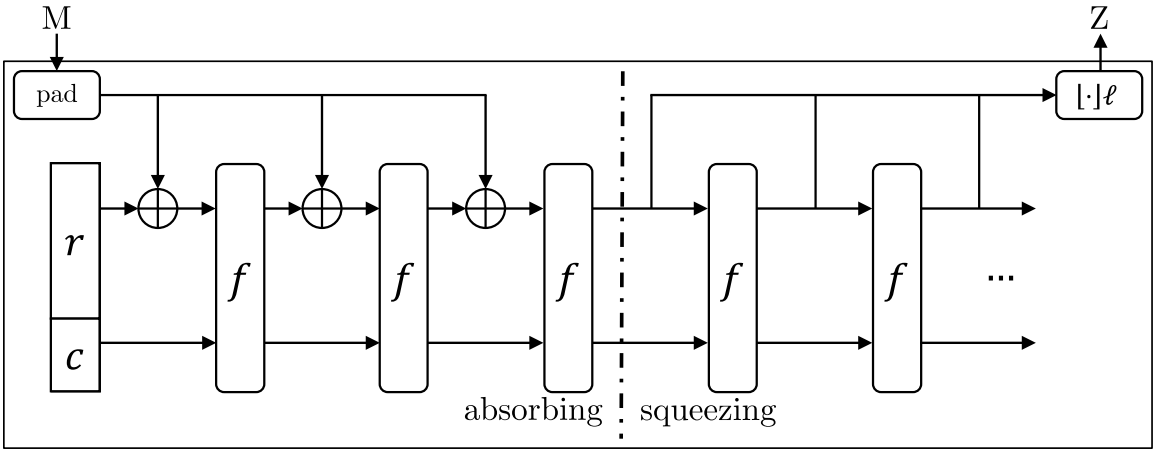


Figure 2.1: Sponge architecture showing the different sections and phases of the sponge construction [17]. A message M is input into the sponge with some padding and the function f that makes up the sponge is calculated based on a given rate $r = \log_2 |\mathcal{A}|$ and capacity $c = \log_2 |\mathcal{C}|$ of the sponge. Outputs can be arbitrarily squeezed out, shown by Z.

2.1 Classical Sponges

All previous hash functions such as MD-5 [18], SHA-1 [19], and SHA-2 [20] were iterative functions, prior to the development of the sponge construction, meaning that the iterated hash functions operated on the chaining of values iteratively modified by a function, whereby a message was the argument, as originally built upon the Merkle-Damgård construction [21, 22]. Unfortunately, it is a fairly unreachable goal to have an iterated function be as strong as a random oracle, but there are two methodologies that can be followed. The first method would be to make the hash function be non-streamable, a blow to data processing and hashing that needs to be completed on-the-fly, since data would need to be stored into memory prior to computation. Examples of non-streamable functions would be those similar to compression algorithms operating on data-at-rest, and are generally not a quality choice due to insecurities in methods of compression algorithms [23]. The second method would be to follow an iterated

function approach and deal with state collisions; this method was chosen for the final sponge construction due to its ease of state manipulation, and possibility of continued operation in a non-linear function space, generating possible one-to-many morphisms for further obfuscation of information.

To describe the new sponge construction, it should be understood that the sponge function takes a variable-length input string of $m \in \mathcal{A} \subseteq \mathbb{Z}_2$ characters for some alphabet $\mathcal{A}$, in this case a binary alphabet, and produces an infinite output $z \in \mathcal{A} \subseteq \mathbb{Z}_2$. Since the sponge's state evolves over time, it can be assumed that a fresh sponge will have internal values at an arbitrary position $\mathcal{C}$, $0 \in \mathcal{C}$. The internal state of the sponge, $\mathcal{S} = (\mathcal{S}_\mathcal{A}, \mathcal{S}_\mathcal{C}) \in \mathcal{A} \times \mathcal{C}$ will have an initial value of $(0, 0)$. The evaluation of the sponge function transformation f is described in two distinct phases:

Absorbing: For each input character m_i, the state is updated as

$$\mathcal{S} \leftarrow f(\mathcal{S}_\mathcal{A} + m_i, \mathcal{S}_\mathcal{C})\,. \tag{2.1}$$

Squeezing: An infinite-length output z is produced as a single character j, $z_j \in \mathcal{A}$, at a time through the evaluation

$$z_j = \mathcal{S}_\mathcal{A}\,, \tag{2.2}$$

and through updating the state as

$$\mathcal{S} \leftarrow f(\mathcal{S})\,. \tag{2.3}$$

The sponge's operation makes it a useful tool for infinite recursive generation of output products. Specifically, an example can be shown for any given message m that

absorbs information into the state under the function f such that $\mathcal{S} = \mathcal{S}_f[m]$ forms a path m to the sponge $\mathcal{S}$ under f. The recursion of this function can be described by:

$$\mathcal{S}_f[\,\cdot\,] = (0,0)\,, \tag{2.4}$$
$$\mathcal{S}_f[x^n \in \mathcal{A} | a_i \in \mathcal{A}] = f(\mathcal{S}_f[x] + a)\,,$$

where " | " is the concatenation operator between symbols.

Interestingly, when a random sponge is analyzed with a given $\mathcal{A}$, the set $\mathcal{C}$, and an initial value $(0,0)$, the mapping from the sponge's function f itself entirely determines the sponge function, thus there will be a total of $(|\mathcal{A}||\mathcal{C}|)^{|\mathcal{A}||\mathcal{C}|}$ possible sponge functions with subsets of transformative and permutive sponges. The properties of sponge functions make them prime candidates for hashing within the scope of quantum computation, due to their computational complexity, easily built upon with quantum walks.

2.2 A New Sponge: Quantum Sponge

For the quantum sponge to be built, many important theories need to be taken from the mathematics community and intertwined with existing quantum theories. The quantum variant of a sponge function would need to meet the criteria listed in Equations 2.1, 2.2, and 2.3. To enable this work, the theoretic standpoint of a sponge function must be identified to see how to translate an arbitrary input into an arbitrary quantum output. Simply, an extended version of a quantum hash function (QHF) must be built.

2.2.1 Quantum Hash Base for the Sponge

The work by Y. Yang et al. serves to emphasize the usage of quantum hash functions and their applications for privacy [24] and is summarized below. The QW-based hash function described is a slightly modified version of a discrete QW with two quantum systems, one for both a walker p and a coin c [25]. A walker-coin system can be denoted by a vector in the Hilbert space $\mathcal{H}_t = \mathcal{H}_p \otimes \mathcal{H}_c$, with the motion of the walk conditioned by the coin state via a conditional shift operator:

$$\hat{S} = \sum_x (|x+1, 0\rangle \langle x, 0| + |x-1, 1\rangle \langle x, 1|) , \tag{2.5}$$

where the summation of Equation 2.5 denotes the sum over all possible positions. The total evolution of the quantum system can then be implemented by repeating a global unitary operator:

$$\hat{U} = \hat{S}\big(\hat{I} \otimes \hat{C}\big) , \tag{2.6}$$

where $\hat{I}$ and $\hat{C}$ are the identity and coin operators, respectively, as applied to the coin state. The final state after t steps is then expressed as:

$$|\psi\rangle_t = \big(\hat{U}\big)^t |\psi\rangle_0 = \sum_x \sum_v \lambda_{x,v} |x, v\rangle \ , \tag{2.7}$$

with the probability of locating the walker at position x after t steps is:

$$Pr(x, t) = \sum_{v \in \{0,1\}} | \langle x, v| \big(\hat{U}\big)^t |\psi\rangle_{initial} |^2 , \tag{2.8}$$

where $|\psi\rangle_{initial}$ represents the initial state of the total quantum system.

For a discrete-time QW, a coin operator can be fixed, with a resulting probability

distribution relying on the initial coin state and step number [24]. If a coin operator at each step depends on a binary message to construct a quantum hash function by the modification of a one-dimensional two-particle discrete-time QW on a circle described by D. Li et al. [26], the resulting output probability distribution can be utilized as the hash value. In the scheme shown in [26], the coin's state operates as the control parameter, thus keying the quantum hash function: The n-th bit of an input message controls the n-th step of the quantum walk.

The construction of the quantum hash function is as follows:

1. Select parameters $(n, (\alpha, \beta, \chi, \delta))$ and provide information regarding the initial amplitudes of the coin state and provide the message of arbitrary length; n is the node number of a circle, $(\alpha, \beta, \chi, \delta)$ are the amplitudes of the initial coin state $|v, \tau\rangle = (\alpha |00\rangle + \beta |01\rangle + \chi |10\rangle + \delta |11\rangle)$.

2. Run a one-dimensional two-particle discrete-time QW on a circle under control of the message and generate the hash value (probability distribution).

3. If a classical form is wanted, multiply all values in the resulting probability distribution by a normalization factor, based on the size of the computed state, to form the binary hash value (i.e. $10^n \pmod{\|\mathcal{A}_{classical}\|}$).

The hash function described has a full detailed construction shown in Appendix B, but a generalization of this procedure can be shown for any polynomial representation of a Boolean function (message) as described by F. Ablayev and A. Vasiliev. [27] and serves as an extension to Equation 2.7.

Letting $t = 2^n$ and parameter set $\vec{B} = \{b_1, b_2, \ldots, b_k\} \subset \mathbb{Z}_q$, a generalized quantum hash function can be defined where $\psi_{t,\vec{B}} : \{0,1\}^n \mapsto (\mathcal{H}_t^2)^{\otimes(\log d+1)}$ for some input $m' \in \{0,1\}^n$ as:

$$|\psi_{t,\vec{B}}(x)\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \left(cos\frac{2\pi b_i x}{t} |0\rangle + sin\frac{2\pi b_i x}{t} |1\rangle \right). \tag{2.9}$$

It then follows from Equation 2.9 that a quantum hash $|\psi_{t,\vec{B}}(x)\rangle$ of an n-bit string x consists of $(\log d + 1)$ qubits. The result is that the controlling set $\vec{B}$ of the hashing parameters determines the size of the hash and provides the function $\psi_{t,\vec{B}}$ with collision resistance.

2.2.2 Mapping from Quantum Hash to Polynomial

Since the quantum hash can be constructed to take classical or quantum information and map it to a "hashed" version of the data, where in this sense the term hash is used rather lightly[1], the next step is to map the output to a polynomial representation.

Luckily, A. Dragt's lectures from 1982 describe that the Hamiltonian created by the developed set of unitary transformations, created by the quantum hashing process, can be represented as a symplectic mapping [28]. More specifically it should be possible by Dragt's Hamiltonian transformation to show that that there is a possible integration of Hamiltonian systems using polynomial maps.

Specifically, an example where some arbitrary 8-dimensional (three qubit) space can be represented through denoting a possible collection of eight phase-space variables, $q_{\theta i}, p_{\theta i}\ \forall i \in \{1,2,3,4\}$, by symbol z_θ:

[1] In this scheme the reversibility aspects of unitary quantum operations are still obeyed.

$$z_\theta = \{q_{\theta 1}, q_{\theta 2}, q_{\theta 3}, q_{\theta 4}, p_{\theta 1}, p_{\theta 2}, p_{\theta 3}, p_{\theta 4}\} \,. \tag{2.10}$$

Interestingly, the Lie operator [28] that corresponds to the phase-space function $f(z_\theta)$, notated as $\mathcal{L}_f(z_\theta)$, where $\mathcal{L}_f$ is the Lie group on f, is defined by its action on a phase-space function $g(z_\theta)$ as:

$$\mathcal{L}_f(z_\theta)g(z_\theta) = [f(z_\theta), g(z_\theta)] \,. \tag{2.11}$$

The relation in Equation 2.11 simply denotes a standard Poissonian of the functions $f(z_\theta)$ and $g(z_\theta)$. The Lie transformation function can then be defined as:

$$e^{\mathcal{L}_f(z_\theta)} = \sum_{n=0}^{\infty} \frac{\mathcal{L}_f(z_\theta)^n}{n!} \,. \tag{2.12}$$

The total effect of the Hamiltonian system on a qubit is formally just the action of a map, $\mathcal{M}$, that takes the qubit from an initial state $z_\theta^{initial}$ to some final state z_θ^{final}:

$$z_\theta^{final} = \mathcal{M} z_\theta^{initial} \,. \tag{2.13}$$

It is possible to show that $\mathcal{M}$ is a symplectic map [28] by considering the map's Jacobian, M, to satisfy the symplectic condition:

$$M^\intercal J M = J \,, \tag{2.14}$$

where J is the fundamental symplectic matrix.

Following the Dragt-Finn factorization [29], the symplectic map can be factorized as:

$$\mathcal{M} = \hat{M} e^{\mathcal{L}_f(z_{\theta 1})} e^{\mathcal{L}_f(z_{\theta 2})} \ldots e^{\mathcal{L}_f(z_{\theta n})} e^{\mathcal{L}_f(z_{\theta n+1})} \,, \tag{2.15}$$

where $f(z_{\theta n})$ denotes a homogeneous polynomial in z_θ of degree n, uniquely determined by the factorization of the fundamental symplectic matrix. The infinite product of Lie transformations then represents the non-linearity of $\mathcal{M}$.

By using this procedure, each element on a lattice or ring can be represented by a symplectic map. Similarly, if two of these maps were to be concatenated together following the Campbell–Baker–Hausdorff theorem [30], a single map is formed of the entire possible n-degree map-space.

Since the number of Lie transformations is infinite according to Equation 2.15, the map $\mathcal{M}$ should be truncated. Unfortunately the truncation of $\mathcal{M}$ to some polynomial order P will violate the symplectic condition. Instead, Dragt shows a simple method of refactoring $\mathcal{M}$ in terms of several (smaller) symplectic maps that can be evaluated without truncation; polynomial maps [28].

The actions on the phase-space are equivalent to solving for the Hamiltonian's morphism between one set of operators to another set of operators. For some time-dependent operation, the previous set defined in Equation 2.10 can be examined. Consider the following expanded example: the action of $e^{\mathcal{L}(q_1^3)}$ on q_1, p_1 in some two-dimensional phase-space.

Setting up the operations to solve for a time-dependent basis leads to:

$$\frac{dq_1}{dt} = \frac{\partial h}{\partial p_1}\,, \quad \frac{dp_1}{dt} = -\frac{\partial h}{\partial q_1}\,, \tag{2.16}$$

meaning that $h = q_1^3$, where solving for a simple case of $t = 0,\ -1$ will result in:

$$q_1(t) = q_1(0)\,, \quad p_1(t) = p_1(0) - 3q_1(0)^2 t\,. \tag{2.17}$$

It is obvious then, that taking the original phase-space parameters and mapping through smaller symplectic maps will result in some form of polynomial representation. The symplectic maps $e^{\mathcal{L}_h(z_\theta)}$ directly contribute to the polynomial mappings of the phase-space variables into themselves. The result, then, is easily coded where the following will be easily generalized into a higher dimension:

1. All polynomials following the form $h(z_\theta)$, where both the phase-space variable and the variable's canonical conjugate do not appear together can easily give rise to the polynomial symplectic maps through the operator $e^{\mathcal{L}_h(z_\theta)}$.

2. If there exists a canonical conjugate to a variable and it is paired with the original phase-space variable, $\{q_i, p_i\}$, and it is present in the resulting polynomial $h(z_\theta)$, then it will only appear in functions of the collection of the phase-space variables[2], $\hat{z_\theta}$ with some polynomials a and g where the form is:

   (a) $a(\hat{z_\theta})q_{\theta i} + g(p_{\theta i}, \hat{z_\theta})$,

   (b) $a(\hat{z_\theta})p_{\theta i} + g(q_{\theta i}, \hat{z_\theta})$,

   (c) Integer powers of $h(z_\theta)$.

2.2.3 Making a Connected Graph of Polynomial Nodes

Now that there is a polynomial mapping shown for the Hamiltonian operators and map, $\mathcal{M}$, it is easy to see that the minimum of two relations is preserved for the symplectic map and is easily changed based on the quantum technology. In this sense, both position-momentum or phase relations are preserved by the symplectic map. The coordinates are continuous variables and thus are the Hilbert space where

[2]The collection of phase-space variables is understood to be all variables that are linked in the initial phase-space set that make-up the original Hamiltonian operator on the system.

the state lives in infinite-dimension. The way to see how the coordinates relate is to refer back to Equation 2.10. The equation works except for a generalized change in a q-qubit system with arbitrary polynomial components $\hat{q_{\theta i}}$ and $\hat{p_{\theta i}}$:

$$\hat{z_{\theta n}} = (\hat{q_{\theta 1}}, \ldots \hat{q_{\theta n}}, \hat{p_{\theta 1}}, \ldots \hat{p_{\theta n}}) \,. \tag{2.18}$$

Following from Equation 2.18, a vector of generalized canonical coordinates is in place, where the canonical commutation relation [31] is simply expressed as:

$$[\hat{z_{\theta n}}, \hat{z_{\theta n}}^{\intercal}] = i\hbar\Omega \,, \tag{2.19}$$

where

$$\Omega = \begin{bmatrix} \mathbf{0} & I_n \\ -I_n & \mathbf{0} \end{bmatrix}$$

for an $n \times n$ identity matrix, I_n, and Planck constant $\hbar$. The form of Equation 2.19 is astoundingly similar to Equation 2.11, and indeed this is true: The canonical commutation relation is operating under the position and momentum or phase operators under a generalized Heisenberg equation in the phase-space.

Taking the calculation a bit further reveals that there is a physical realization of the polynomial nodes within the Hilbert space. Since many physical situations only require quadratic Hamiltonians of the form:

$$\hat{H} = \frac{1}{2} \hat{z_{\theta n}}^{\intercal} K \hat{z_{\theta n}} \,, \tag{2.20}$$

for K being a $2n \times 2n$ symmetric matrix, a useful restriction is revealed. The restriction allows for the reconfiguration of the Heisenberg equation as:

$$\frac{d\hat{z_{\theta n}}}{dt} = \Omega K \hat{z_{\theta n}} \, . \tag{2.21}$$

The change is again showing the similarity between Equation 2.21 and Equation 2.16. Since the solution to both of the equations must preserve the canonical commutation relation, it is thus true that the time-evolution of the system or, general message evolution of the mapped polynomials, will be equivalent to the action in a real symplectic group, $Sp(2n, \mathbb{R})$, on the phase-space.

2.2.4 Traversing the Connected Graph

To better describe the Hamiltonian operations that occur in the polynomial mapping scheme to nodes on a graph within a Hilbert space, examine what is shown in Figure 2.2. There are certain transitions possible within the mapping, but all follow their respective path from node along an edge to a neighboring node.

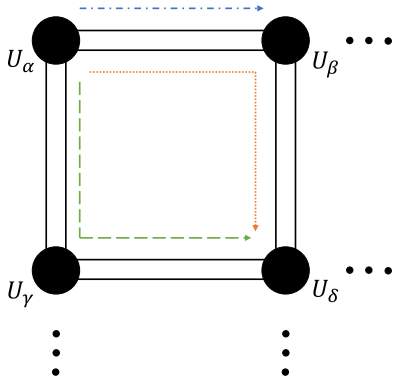


Figure 2.2: Polynomial node transitions highlighting the map of a quantum hash to its representation as a set of Hamiltonian operations, here as single unitary operation, where there exists a map of several distinct sets of operations that can be navigated through from a single unitary node to another along its closest edge.

To better describe what the operators are in Figure 2.2, it can be considered that each point is made in the following method, from the result of a set of unitary

transformations described after completing the standard quantum hashing function shown in Equation 2.9. Given some hash result, taking an initial state $|\psi_0\rangle$ with successively applied unitaries, there is a global unitary, U_{total}, representation.

$$|\psi_{total_0}\rangle = \underbrace{U_0 U_1 \ldots U_n}_{U_\alpha} |\psi_0\rangle \tag{2.22}$$

From this, there will also be other possible global unitaries acting on an initial state, such as:

$$|\psi_{total_1}\rangle = \underbrace{U_0 U_1 \ldots U_n U_{n+1}}_{U_\beta} |\psi_0\rangle \tag{2.23}$$

$$|\psi_{total_2}\rangle = \underbrace{U_0 U_1 \ldots U_n U_{n+1} U_{n+2}}_{U_\gamma} |\psi_0\rangle \tag{2.24}$$

$$|\psi_{total_3}\rangle = \underbrace{U_0 U_1 \ldots U_n U_{n+1} U_{n+2} U_{n+3}}_{U_\delta} |\psi_0\rangle \tag{2.25}$$

In general, it is possible to describe the transitions from one polynomial unitary-representing node to the next through a transition operator. Suppose that the current system is on node U_α and an operation is applied to the two-dimensional plane depicted in Figure 2.2. From the figure, a simple unitary transition operator, $\mathscr{U}_n^{trans}$, where n represents n-number can be applied such that the following would be true:

$$U_\delta = \mathscr{U}_2^{trans} U_\alpha \,. \tag{2.26}$$

Here, it becomes obvious that the estimated endpoint can be determined by the resulting transition unitary from a start point to an end point.

2.2.5 Arbitrary Length Extension of Quantum Sponge

Following from Section 2.2.4, a method to traverse a polynomially-connected graph is developed, but there is still the missing enabling component for arbitrary-input and arbitrary-output lengths necessitated by the quantum sponge function. Specifically, it becomes a question of what does the length extension *mean* in the context of this work? For this work, the arbitrary length-extension operates in terms of increasing the order of the polynomial generated, as shown in Section 2.2.2. Interestingly, a closer look needs to be taken at the actual unitary dynamics of the system. There is work by A. Nahum et al. that focuses on the dynamics within a gaseous system and the resulting quantum entanglement growth [32]; which is able to be applied directly to the work here to describe the changes present in the connected graph of transitional polynomial representations of Hamiltonian operations, due to the data effectively encoded into transitional states, as is shown in Equation 2.20 and Equation 2.21, that have a slice-dependence where the node being operated on is within its own order 'slice' with dependence on the interconnecting nodes, or pseudo-time-dependence in the related vocabulary for the work by A. Nahum et al..

A 1-dimensional model can be examined to see how the entanglement dimension increases with successive movements across the lattice, or with successive entangling operations applied. If a chain of quantum spins is considered within a local Hilbert space of q-dimension, the open boundary condition can be initially taken with the bounds of the lattice $x = 1, \ldots, L$. Since only the unitary dynamics matter at this point, a full density matrix $\rho = |\psi\rangle \langle\psi|$ can be used to represent a pure state. Looking at entanglement across a single cut at position x, a reduced density matrix ρ_x can be defined by splitting the 1-dimension chain into two halves at x and tracing out the

left- or right-hand side. The n-th Renyi entropy [33] for a cut at x is defined as

$$S_n(x) = \frac{1}{1-n} \log_q(\text{Tr } \rho_x^n) \,. \tag{2.27}$$

Taking log base q, where $\lim_{n\to 1}$, the Reyni entropy becomes the von Neumann entropy,

$$S_{vN}(x) = -\text{Tr } \rho_x \ln \rho_x \,. \tag{2.28}$$

Importantly, a constraint on the von Neumann entropy can be made where neighboring nodes may only differ by at most one change. The constraint on changes between nodes is described by

$$|S_{vN}(x+1) - S_{vN}(x)| \leq 1 \,. \tag{2.29}$$

Examining the relation of growth of bipartite entropies, $S(x, m)$, with message m, starting from a base state, there will be growth in the entropy of the system with each subsequent message change, depending on the unitary operation applied. Figure 2.3 shows how the transition and increase in entropies described would work.

Starting where $\lim_{n\to 0}$ of the Reyni entropy occurs, known as the Hartley entropy, S_0, the bond dimension of message nodes can be calculated. Keeping the initial state size q finite, in a given message transition, a unitary can be applied at node x. Applying the unitary may change the Hartley entropy at the selected message node, but the connected message nodes requiring distinct unitary transitions will not change. The reason this is true is due to the previous constraint on transitions from Equation 2.29, such that the maximum value allowed by the constraint, with $Pr(change) = 1$, will be:

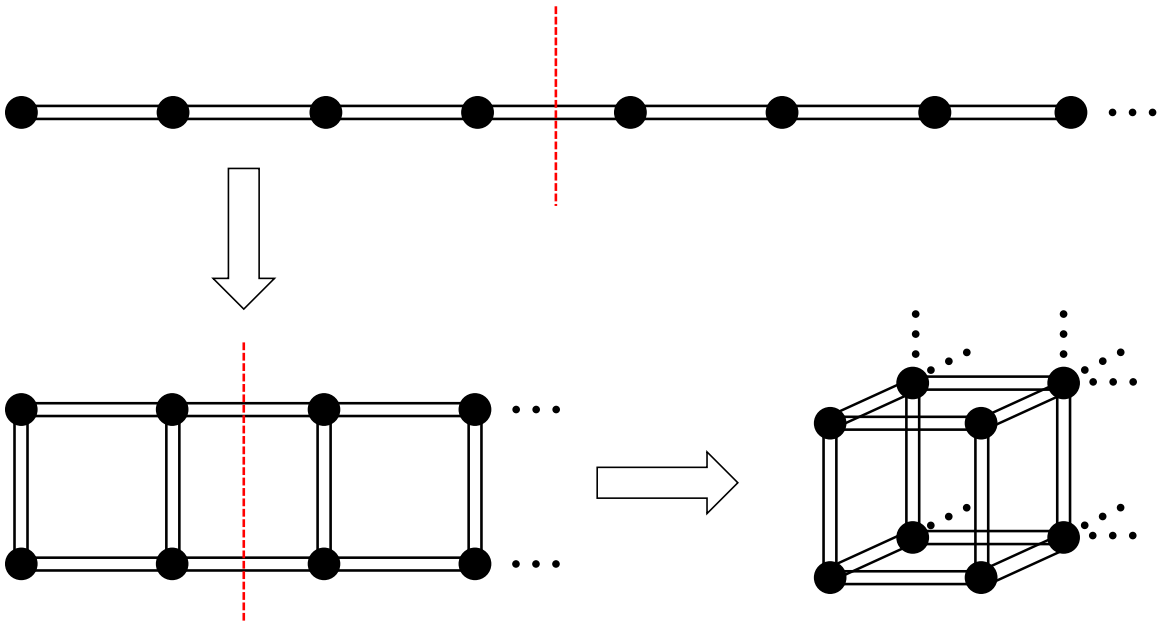


Figure 2.3: Dynamic message changes in a chain of message nodes depending on where an entropic cut occurs, supported by an entangling unitary transition. The entropy of a d-dimensional message chain increases with each successive operation.

$$S_0(x, m+1) = \min(S_0(x-1, m),\ S_0(x+1, m)) + 1\,. \tag{2.30}$$

This entropic relation can be generalized naturally to higher dimensions, cut by a d-dimensional disordered membrane embedded into $(d+1)$-dimensional space-time. By using CNOT gates to increase entanglement in the system, the cut of the higher dimension will reveal a larger dimensionality within the chosen subspace. Interestingly, the entanglement $S(m)$ for a region A whose boundary ∂A becomes a temporal thickness m, will terminate on the upper bound of a 'time-slice' (message-slice). The total volume of the space-time subspace is $|\partial A| \times m$, leading to the scaling of the membrane's energy and thus entanglement. The sub-leading terms are subsequently used to encode universal information.

By entanglement, a d-dimensional noisy quantum system will result in systems

where $d = 1$ and $d = 2$ exist with unique dynamic phase and nontrivial critical exponents. The result for disordered systems where $d = 1$ and $d = 2$ is derived from the early Ising models of systems with pinning [34], and can be applied to any system of quantum interconnect, as described in the 1986 work by D. Fisher [35]. If a lattice is present, or in this work, a topology of interconnected nodes similar to Figure 2.3, two stable phases and dynamical phase transitions are possible in $d = 3$ and higher, since the membrane can be pinned by the lattice of message nodes. If a quantum system is taken that is infinite in one direction and of size L in the other $(d-1)$-directions; considering the entanglement for a perpendicular cut to the infinite direction will yield to $S(m)$ growing indefinitely for the given geometry. This is ideal, since the developed geometry can be extended upon indefinitely, therefore allowing for a map of the generated quantum hash into this space to form the quantum sponge function.

2.2.6 Bounding of Expanded Quantum Sponge to User Requirement

Up until this point, the quantum sponge has the ability to be mapped and to grow fairly unconstrained, with matching unitary transition sequences. Since the quantum sponge, including the repeated entanglements, continues to grow, this necessitates that when someone is expecting an arbitrary output, they should provide a growth argument, $\mathcal{G}_{max}$.

To properly constrain the output of the quantum sponge, the uniform boundedness principle can be applied, where the details of the uniform boundedness principle can be seen in Appendix C. Why can the uniform boundedness principle be applied? The reasoning is quite clear, since the quantum state exists within a large Hilbert space, it must be remembered that the Hilbert space is a vector space over the complex

numbers with an inner product. The Hilbert space is then complete with respect to the inner product, where the Hilbert space is then directly a Banach space whose norm is determined by the inner product. Eventually, the size set by the user will need to follow:

$$\mathcal{G}_{max} \leq \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \left\| \mathscr{U}_i^{trans} \right\| \left\| \left| \psi \right\rangle_j \right\|, \tag{2.31}$$

where the value of i, j limits the number of either entanglements or number of traversal unitaries applied.

The space keeps expanding until the point at which $\mathcal{G}_{max}$ is satisfied for some arbitrary i, j, depending upon whether the user places an alternate restriction on the number of unitary transitions or on the total number of entanglements that take place. Following the uniform boundedness principle then shows that for a fixed message node, the family of points are point-wise bounded by $\mathcal{G}_{max}$, i.e. the message point and any branches from the message point up to $\mathscr{U}_i^{trans}$ are Banach (sub)spaces, detailed in Appendix D, of the total Hilbert space defined by $\left| \psi \right\rangle_j$. Thus, all of the requirements to apply the uniform boundedness principle are fulfilled, such that the linear unitary operator's ability is effectively finite with respect to the user's requirement.

2.3 General Quantum Sponge Application

When reviewing the construction of the quantum sponge, at its core, a pattern emerges. As a QW-based hash is expanded, mapped to a polynomial representation, and traversed topologically, for each successive step, the unitary transformation could potentially be immense. The fact that there are potentially large changes in dimensionality when referring to successive steps provides an excellent platform to construct secure primitives. A secure primitive constructed on a path arbitrary in length leaves

little room for an adversary to estimate origin or sequence on successive steps on the path, never mind being able to form assumptions of the dimensionality of the system. An optimal application for the quantum hash function and sponge extension will be further described in Chapter 4. Additionally, the movement between nodes of polynomial mapping serves the potential application of state traversal solely along vertexes of the mapping, instead of necessitating an edge; described in more detail in Chapter 5.

CHAPTER 3

AUTHENTICATION METHODS

Authentication is an important part of any ciphersuite, as authentication provides a secure method of authenticating not only entities, but other components in a network, such as keys and messages. Identity authentication is generally the first method of authentication thought of when authentication is mentioned, because this primitive allows for the protection of the communication from an eavesdropper, Eve, pretending to be a legitimate user. It is important to make any protocol or ciphersuite have resilience and resistance to an eavesdropper, such that the sent messages are only accessed by the authenticated user. In an authentication scheme, the receiver verifies the creator of the information, as where in identity authentication specifically, the identity is generally a machine or an individual, where an entity that tries to prove itself is known as a *prover*, and the entity that verifies the other's identity is the *verifier*.

In general, an identity authentication scheme works because a sender pre-registers 'secret' information regarding his/her identity, in a database held by the receiver, prior to any communication. When communication is initiated, an identity authentication occurs where the receiver can receive the secret information from the sender and verify the information against the previously registered information in the database.

The other versions of authentication, specifically message authentication, work

where the sender and receiver have a secure channel that may be in an untrusted environment. Within the untrusted environment there is the potential for an eavesdropper to intercept and manipulate messages, or impersonate either the sender or receiver in what is commonly known as a 'man-in-the-middle' (MITM) attack. The message authentication techniques help to overcome the falsification of identity when sending messages by appending or applying user-specific information to the message between a prover and verifier.

When examining potential methods of solving issues revealed to MITM attacks in networks and communications, a common classical hardware technique comes to mind: physically unclonable functions (PUFs) and physical one-way functions (POWFs). The question of how to implement these devices in a 'quantum' way is of interest and relevance to this work since hybrid quantum–classical primitives are necessary to develop a ciphersuite.

3.1 Classical PUFs

Classical CMOS-based PUFs are physical primitives that utilize process fabrication variance to create unique physical one-way functions. Unlike non-volatile memory where information can be stored and read digitally, information in CMOS-based PUFs is directly extracted from inherent lithographic variation, making static PUFs impossible to be duplicated; even within the original manufacturing process [36]. Other common forms of electronic PUFs include arbiter PUFs [37] that utilize delay to measure difference in transmission times of two competing pathways to generate a digital response, butterfly PUFs [38, 39] that examine output from a set of cross-coupled latches, and random-access memory (RAM) PUFs [40] that are based

on randomly distributed mismatches between two transistors where the repeatable start-up conditions of cells are treated as digital responses.

The operating scheme for all types of PUFs remains identical. Given a set of specific inputs, referred to as the challenge, a PUF will generate a unique output response due to the randomness present in the device. These inputs and specific outputs are known as the challenge-response pairs (CRPs). The manufacturer/user of the PUF enrolls the device by generating and recording all of the viable CRPs. The user can later verify the identity of the integrated or remote PUF by challenging the device and comparing the response to the expected response.

3.1.1 Classical PUFs in Quantum Systems

The application of classical PUFs, or PUFs whose base operating point relies on classical binary information, has not been studied in depth as a field of interest. The most relevant work with regards to application is related to the readout of classical PUFs, and will be described in detail in Section 3.2.4. The most recent and relevant work in the field of classical PUFs, as applied to quantum systems, can be seen in a survey on PUFs and their security, with a quantum emphasis, written by M. Arapinis et al. in late 2019 [41].

3.2 Optical PUF Hardware Photon Authentication

A major component of this work was the development of a physically unclonable function (PUF) based on an integrated silicon photonic platform[1]. PUFs have been suggested as a means to securely authenticate a networked device or remote user. The

[1]The platform for the PUF is photonic to the author's fellowship and affiliation during his PhD studies. Realistically, several other controllable photonic devices may be used a PUFs or POWFs.

current state-of-the-art means of authentication begins with the usage of a classical secret key or token stored within a read-only memory (ROM). A PUF is of particular interest since they often form the basis of the hardware primitives necessary to replace these shared secret keys with a non-reproducible physical object or device.

PUFs based on optical measurements have been proposed with differing operating bases, where either the scattering of laser-light from bulk inhomogeneous media [42], or multi-mode fiber [43], or non-linear interaction in specialized integrated devices [44] are observed. One of the main reasons that electronic PUFs are commonly implemented into field programmable gate arrays (FPGAs) and other protected IPs is because of the electronic PUFs' ease of integration into the many existing CMOS-process devices as well as their low size, their low weight, and their low power requirements.

Optical PUFs often require non-trivial bulk optics and ancillary support, such as micron-accurate positioning stages [42] or bulk disordered materials [43]. A more compact solution was conceived by Grubel et al. [44], utilizing integrated optics, however, these integrated optical PUFs require a set of completely custom-designed devices for the sole purpose of use as a PUF. In this work it is shown that any large enough and well-connected enough array of linear optical devices[2] can be used both for its designed purpose and as an optical PUF.

In this work, a linear optical interferometric circuit is described, without the original intent to be utilized as a PUF[3], and demonstrates how a small sub-circuit behaves as a weak PUF but has the possibility to further meet the criteria of a

[2]The array of linear optical devices was available due to the author's fellowship and affiliation during his PhD studies. The device utilized for this work was originally developed between the author's fellowship organization and MIT [14].

[3]The original application for the device was as a 'lab-on-chip' to allow for quantum telecommunication experimentation.

strong PUF. In addition, it is shown how the scale of an integrated optical circuit intrinsically carries enough randomness from multi-input interference via adjustments of Mach-Zehnder interferometers (MZIs) to act as a practical PUF.

3.2.1 Optical PUF and Randomness

The device used and simulated in testing of the all-optical PUF is the device as described in greater detail, ahead in Chapter 5. To understand this work however, requires only the knowledge that MZIs are basic optical components that are analogous to thermo-optic switches. Electrical settings on the device act on the waveguide material to control how much light travels down consecutive pathways. This work was completed using two PUF devices consisting of 10 MZIs, each pumped by a Keysight laser (model 81606A) through a simple waveguide. Each PUF device has 8 output ports, each connected to a single standard positive-intrinsic-negative (PIN) photodiode (Precision Micro Optics model DPRM-412). The subset devices used within the photon manipulation tool are triangular-shaped with a light cone dispersion region, with a representation of a single 10-MZI lightcone shown in Figure 3.1.

Of importance to note, is that each of the MZIs within the lightcone structure are composed of two symmetrical beamsplitters, where each beamsplitter is thermo-optically controlled using an integrated resistive heating device (more on that later). Since randomness in the output of the device is essential to the basic operation of a PUF, it is important to understand where sources of randomness are located for the device used in this work. The first source of randomness for this device is the $\approx 15.43\%$ variation between resistive heaters, as measured, due to fabrication variances. An additional source of randomness, having a far more significant effect on the device, are the two directional couplers within each MZI. The

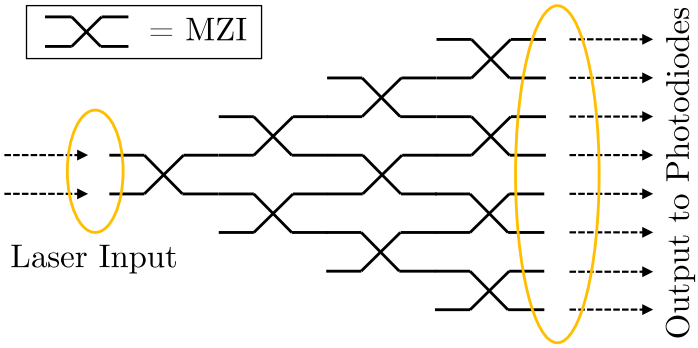


Figure 3.1: Optical PUF lightcone depicting the graphic representation of the subset devices utilized within the photon manipulation device. The laser input is arbitrarily user-chosen between the two input waveguides in the lightcone region, with the 8 output ports each connected to a single standard PIN photodiode. The figure inset shows a single 'cross' depicting the operation of a single MZI.

couplers are designed to be a nominal 50:50 split but fabrication defects stemming from variation in the etching process, sidewall roughness, and variation in minute distances between waveguides leads to unpredictable splitting ratios near 50%. An additional source of unpredictability leading to potential for randomness in the device comes from a minor design flaw: Since many of the MZIs share ground leads, positive feedback ground-loops are formed when a single MZI's voltage is set and the cascading MZI's resistive elements return a very complicated function of voltages, induced by association to the active element. The effect of ground-loop feedback is approximately -45 dB as measured by M. Prabhu [45]. It can be expected that the positive feedback ground-loop voltage errors may be a minor factor in the device's overall behavior. To minimize thermo-optic effects, the device was held at a steady temperature slightly above ambient throughout testing.

The photon manipulation device is large enough to act as two distinct 10-MZI devices with identical structure due to the original device being composed of 88 MZIs. Two devices were programmed to be used for comparison by taking the photon ma-

nipulation device and pumping laser-light into two space-like separated sections such that the light from one 10-MZI lightcone will not reach the other 10-MZI lightcone, either directly or through reflections other than those coupled into the slab-mode. In addition, the two devices are electrically separated so that no positive ground-loop feedback effects can exist between the devices. Using the photon manipulation device in this manner means that fabrication and interconnection differences between the two halves of the device are minimized. Any similarly fabricated device to be utilized as a PUF will inherently possess additional random variance compared to the devices under test, especially due to the tunability of MZIs. The additional random variance may be calculated for additional fabricated devices by Markov chains for mutual information.

3.2.2 PUF Metrics and Notation

The definition of a weak or strong PUF given by C. Herder et al. [36] is applied. A weak PUF is described as: *a*) Having a number of CRPs linearly related to the number of components, *b*) being robust against environmental effects i.e. having stable CRPs, *c*) having unpredictable responses to any stimulus and, *d*) being extremely impractical to reproduce. A strong PUF is characterized by all of the previous statements regarding weak PUFs with the addition of: *e*) Having enough CRPs such that the number is exponential in the number of challenge bits and *f*) that the readout will reveal only the response $R = f(C)$, plus noise, and nothing else.

One metric chosen to test the difference between CRPs is the Euclidean distance, ℓ^2-norm, of the N outputs. To measure the Euclidean distance, the analog response of each detector is divided into even-sized subsets; each of which is larger than the estimated noise of the *system*. For testing, a subset of size 0.5% of the total power

detected across the N outputs was chosen based on the minimum detector sensitivities, scaled by normalization factors between CRPs.

To decrease or correct error within the testing of the PUF, the size of the voltage subset utilized in computation was increased from 0.1%. The increase in subset size serves to decrease the chances that any noise present on a particular channel straddles the bounds between two values. The increase in subset size also has the effect of a reduction in resolution for the ℓ^2 distance. An alternative option to decrease or correct error within the testing of the PUF is to increase the collection time, thus increasing the amount of averaging that results in a single CRP. The drawback to relying on increasing the collection time are latency requirements, which may hamper any fast electronics requiring the output of the PUF and may possibly allow an adversary additional time to perform side channel attacks.

The second set of metrics that are utilised to quantify the results of the PUF are the inter- and intra-device Hamming distances (HD_{inter}, HD_{intra}) along with the inter- and intra-device Euclidean norms ($\ell^2_{inter}, \ell^2_{intra}$). To analyze the results, the standard Hamming distances were modified between a response R_i and challenge C_i to reduce the effects of noise. The loose Hamming distance (LHD) can be analyzed between two noisy responses, R_i and R_j for all elements k as:

$$LHD = \sum_k f(R_i, R_j)_k = \begin{cases} 0, \forall k \text{ if } |R_{i,k} - R_{j,k}| < L \\ 1, \forall k \text{ if } |R_{i,k} - R_{j,k}| \geq L \end{cases} \tag{3.1}$$

Where $L \in \mathbf{N}$ defines the degree of looseness and $L = 1$ is the normal HD. In the case of the small PUFs, $L = 2$ is sufficient. The LHD definition is used to compensate for the experimental noise and rounding errors, as discussed below. In addition to the

LHD, the standard ℓ^2-norm is used, following the standard definition given by:

$$\|x\|_2 = \sqrt{\sum_i x_i^2}. \tag{3.2}$$

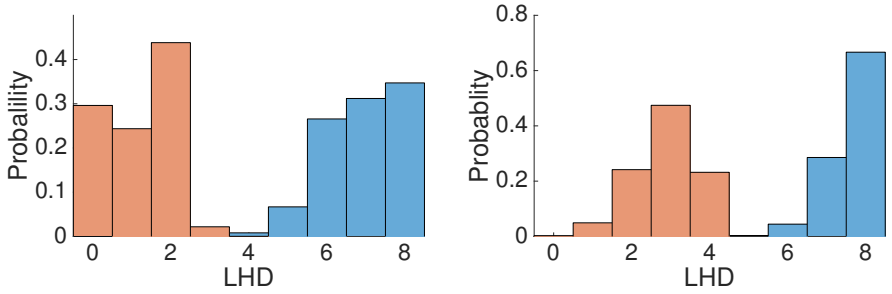
The major difference between these two metrics for non-binary data is that the Hamming distance represents the number of measurements which are different while the Euclidean norm gives a metric of the significance of differentiation. Interestingly, the Hamming distances are expanded upon and are used to determine the *uniqueness* of the device as described by R. Maes and I. Verbauwhede [46]. Uniqueness is a calculated estimate for the amount of entropy available from a PUF and can be applied to a similar population of PUFs with an identical architecture. The uniqueness, $\mathcal{U}n$, can be calculated for some challenge, C_i, as:

$$\mathcal{U}|_{C_i} = \left(\frac{2}{n(n-1)} \sum_{i=1}^{n-1} \sum_{j=i+1}^{n} \frac{LHD(R_i, R_j)}{m} \right) \times 100\%\,, \tag{3.3}$$

Analogous to Equation. 3.1, $L = 1$ gives the standard definition of uniqueness. Here, n is the number of PUFs in a population, and m represents the number of bits in the response from the PUF. An optimal uniqueness value for binary PUFs would be 50%, as this implies uncorrelated responses. Since the PUF is continuous via electronic control, the interpretation of Equation 3.3 must be modified. Given that $LHD = 0$, i.e. a complete collision, doesn't contribute to $\mathcal{U}|_{C_i}$ and a partial collision contributes only to the fraction that didn't collide, $\mathcal{U}|_{C_i}$ is counting non-colliding responses. Regardless of the looseness, this is equivalent to a target uniqueness between devices of 100%.

3.2.3 Results of PUF Testing

To test the optical PUF, several sets of data were generated. First, using the small section from Figure 3.1, 100,000 random CRPs were created and mirrored on each device, and a single CRP was repeated 5,000 times on each device. All of the CRPs were randomly selected in each variable from a uniform distribution over the $v2\pi$ voltage range required for a complete switching response of a typical MZI. For the analysis of the response of the small PUFs depicted in Figure 3.1, eight output intensities were measured via a polled array of photodiodes. The results are shown below.



(a) Device 1 **(b)** Device 2

Figure 3.2: Distinguishability of $\mathbf{LHD_{intra}}$, for both 10-MZI devices. LHD_{intra} between the same repeated challenge (orange) and between a typical challenge and random challenges (blue) on the same device.

Figure 3.2 shows the repeatability (orange) of the same challenge applied 5,000 times to each device. The two devices show a relatively low $LHD \leq 4$. The difference between Figure 3.2a and Figure 3.2b is accounted for by the differences in noise level, with a higher total noise on the second device[4]. The second dataset in both figures (blue) shows the difference between a typical CRP and the 100,000 randomly selected

[4]This difference is likely caused by photodetector variation due to differing production batches with a result of approximately 1.5 times the noise shown on the datasheet for the PIN photodiodes previously mentioned.

CRPs. The two devices show strong repeatability through the LHD by staying within a narrow variable range. The two devices additionally show strong metrics for distinguishability. The differences between a single challenge and response set to a differing challenge and its response set is easily identified. Ideally, $LHD_{intra} = 0$ should be true for a fixed challenge and $LHD_{intra} = 8$ for differing challenges. The ℓ^2-norm is necessary to provide an additional measure of the significance of the differences.

For applications of this PUF in authentication roles, the key importance is the inter-chip response to the same challenge. Figure 3.3 depicts the LHD_{inter} metric between 100,000 randomly chosen CRPs as they apply to both devices. The number of challenges is too large to test all possible settings. For 100,000 challenges mirrored between the two devices, Equation 3.3 can be analyzed to find a total uniqueness of 85.28%. LHD_{inter} is strongly centered around $LHD_{inter} = 8$, approximately 70% of challenges and responses have no measurement values in common, and less than 10% have more than two distinct measurements in common. There were no complete collisions[5] found during testing through numerical search of empirical results.

The commonality of the measurements are shown in Figure 3.4, where the blue data shows the ℓ^2_{inter} distance between the two devices for each challenge. The smallest ℓ^2_{inter} distance found was 11, with a mean of 58, median of 55, and standard deviation of 23. The orange data shows the ℓ^2_{intra} distance between a typical response and all other responses to the same challenge on a single device. The data shown is typical with limited overlap between histograms. Some CRPs appear to have more noise

[5]In this context a collision is considered to be complete where all output values are identical for two different given inputs, or partial where two similar inputs result in arbitrarily similar outputs; these are not fully distinguishable since a distinguisher can exist where a value can be differentiated from a random oracle [16].

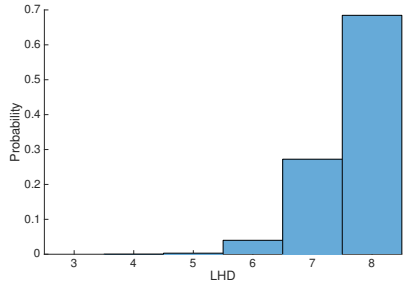


Figure 3.3: $\mathbf{LHD_{inter}}$ distances of small PUFs between 100,000 randomly chosen challenge-response pairs compared between the two 10-MZI devices.

than others and multiple datasets have shown no overlap at all between histograms, the least distinguishable of which is shown as an example in Figure 3.4, the ℓ^2_{intra} data shown here has a mean of 6, median of 5, and a standard deviation of 4.

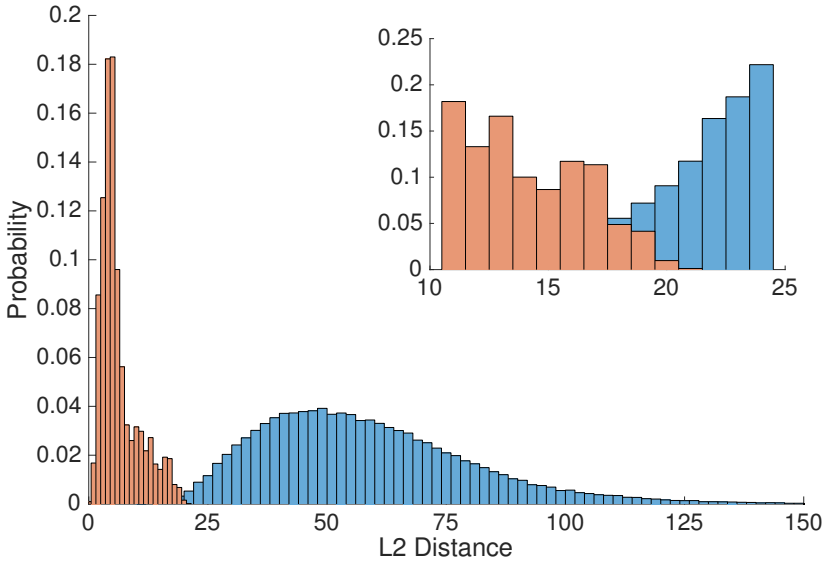


Figure 3.4: Euclidean distances of small PUFs, showing the distance between the response to identical voltage settings on both devices (ℓ^2_{inter}, blue) and the response of one device to the same repeated challenge (ℓ^2_{intra}, orange, typical). The inset shows the region of overlap.

3.2.4 Optical PUF as an Authentication Mechanism

The general operation of a PUF authentication system can be summarised by the image shown in Figure 3.5. Shown is a general method where the device containing the optical PUF can be characterized with a set of challenges and a measured response can be captured by the verifier; called challenge-response pairs (CRPs). When the device is manufactured, it is characterized with possible challenges and the responses are measured. The CRPs are then stored and delivered to the purchaser of the device, often called the enrollment data. Once the device is in use away from the manufacturing facility and/or connected via an untrusted channel, one of the challenges can be applied to verify that the expected response is generated. If the verification is successful, the authenticity of the device can be assumed.

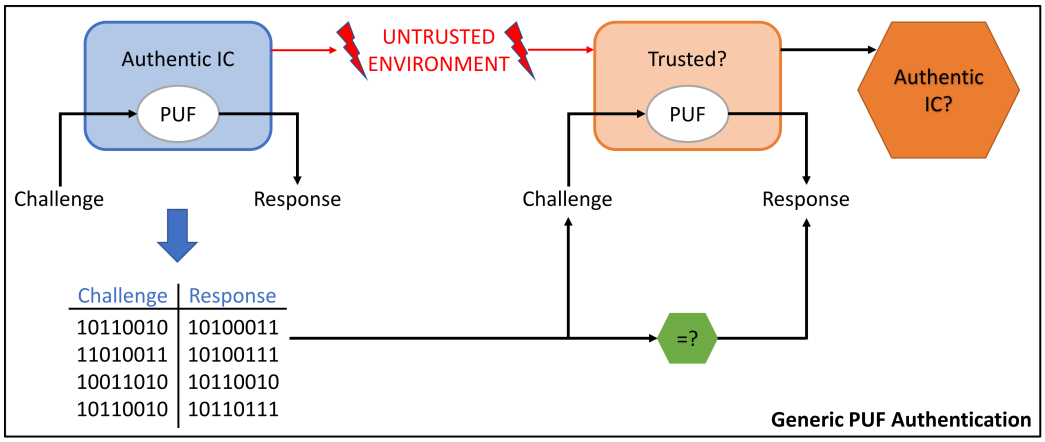


Figure 3.5: Generic PUF application detailing the operation of a PUF within a network or device communicating through an untrusted environment where the final value can be queried by a third-party to verify that the communication taking place is genuine. Once verified, communication can continue in an untrusted channel.

To utilize the optical PUF in a practical application, a more subtle approach is necessary. The challenge applied to the optical PUF is in the form of electrical settings sent through a control-module, while classical light, or single photons, are present at

the input ports. When the applied challenge is in the form of classical light, the MZIs will configure the light to a certain output profile, depicted by Figure 3.6. The output profile is in terms of normalized relative intensity across the measured photodiodes where a distinct histogram is formed for each provided set of challenges to the MZIs.

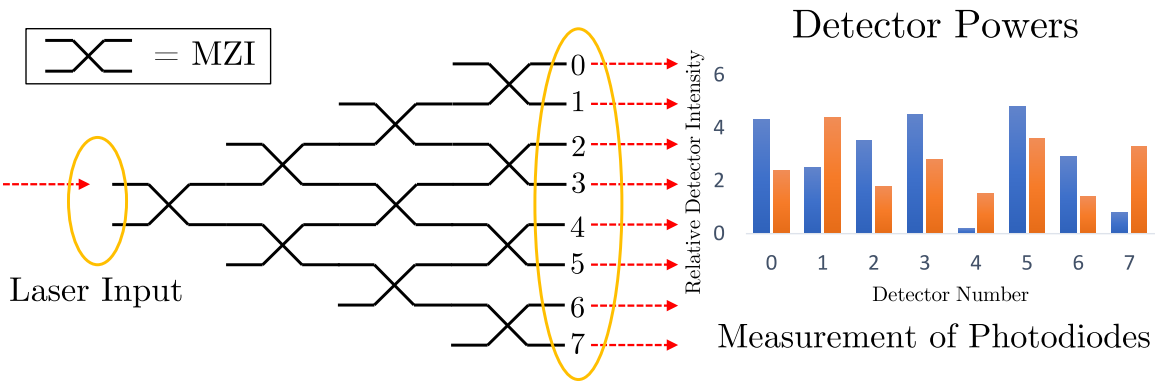


Figure 3.6: Optical PUF output profile from two challenges applied to the device in the form of MZI settings, with the right graph showing the resulting profile from the detector's response in terms of relative intensity. The blue/orange bars represent possible responses to a predefined set of two challenges. The MZI symbol is in the upper left, represented by a 'cross' where each MZI is composed similarly to the one shown later in Figure 5.2.

Similarly, the purely-quantum variant of utilizing the optical PUF will result in a set of MZI phase modulation settings being sent to the device as a challenge via the same control-module mentioned previously. The result will be an arbitrary state output from the device where the PUF has applied an arbitrary unitary transformation, U^{arb}, to the photons entering the device. The mathematical representation of a PUF authenticator with N input/output modes and q-many photons will be:

$$U_{q_i}^{arb} \left|\psi^{challenge}\right\rangle_{q_i} = \left|\psi^{response}\right\rangle_{q_i} , \tag{3.4}$$

$$\text{where } \left|\psi^{response}\right\rangle_{q_i} = \sum_{j=0}^{N} \alpha_{q_i}^{0} \left|j\right\rangle ,$$

for a q-many qubit (photon) input state with indexable qubits at position i. The response will be in a superposition state with some coefficients $\alpha_{q_i}^0$ on output modes $|j\rangle$ due to the natural structure of the PUF device shown in Figure 3.1. Since a single or multi-photon input, of an unknown state will enter the device, the resulting output density matrix, $\rho_{\psi^{response}}$, will have an additional weight constant ω_n and PUF weight constant ω_p, described further in Section 3.2.5, where each weight constant affects the separate $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ components of a qubit. The output response (histogram) from the PUF will then be projected from a measurement (or repeated measurements) of:

$$\rho_{q_i\psi^{response}} = |\psi^{response}\rangle_{q_i} \langle\psi^{response}|_{q_i} \tag{3.5}$$

$$= \omega_n\omega_p U_{q_i}^{\dagger arb}(a\,|-\rangle\langle-| + b\,|+\rangle\langle+|)U_{q_i}^{arb} \tag{3.6}$$

$$= \omega_n\omega_p U_{q_i}^{\dagger arb}(c\,|\,\mathbf{0}\,\rangle\langle\,\mathbf{0}\,| + d\,|\,\mathbf{1}\,\rangle\langle\,\mathbf{1}\,|)U_{q_i}^{arb}\,, \tag{3.7}$$

$$\text{where } |\mathbf{1}\rangle = \frac{i}{\sqrt{2}}(|+\rangle - |-\rangle)\,,$$

for differing polarization, either left = $|-\rangle$, right = $|+\rangle$, horizontal = $|0\rangle$, or vertical = $|1\rangle$.

The operation of a fully optical PUF in a quantum system has not been studied before, but, something similar was approached by B. Škorić et al. whereby a quantum readout protocol was developed to interface with a classical PUF [47]. The readout protocol is modified, described below, with key notational differences to fit this work and to allow for a reconfigurable, optical, PUF.

The quantum readout of the optical PUF is simple, where the challenge space of the device is a d-dimensional Hilbert space, $\mathcal{H}$, with a direct mapping to the response Hilbert space[6]. An arbitrary input challenge $|\psi^{challenge}\rangle \in \mathcal{H}$ is mapped through the

[6]Our device, being electronically reconfigurable, facilitates the mapping of an optical input

optical PUF, with response $\hat{R}$, such that $\hat{R}|\psi^{challenge}\rangle \in \mathcal{H}$. The response will be unique, up to the limit of uniqueness from Equation 3.3 where all nominal values of unique CRPs is *above* 50%[7], for each challenge applied, where $\hat{R}$ may not necessarily be unitary, but can be decomposed into a response coefficient matrix R and response unitary U^{arb} such that $\hat{R} = RU^{arb}$.

The authentication between two parties, Alice and Bob, works where the verifier (Alice) wants to check if Bob still possesses the optical PUF. Alice first retrieves the original shared enrollment data, then picks a random state, ψ, and prepares the state $\psi^{challenge} \in \mathcal{H}$ and sends it to Bob. Bob then lets the prepared particle interact with the optical PUF, resulting in the final response state $\psi^{response} = \hat{R}\psi^{challenge}$, which is then sent back to Alice. Since the result of the PUF response is in the density matrix, Alice then computes $\rho_{\psi^{response}}$ according to Equation 3.6. Alice is then able to repeat this process multiple times to be sure that Bob's PUF is the correct PUF being used.

3.2.4.1 General Security Measure of Optical PUF Authentication

The security of the protocol described is based on the no-cloning theorem, or in this work, the unclonability of the unknown quantum state by an eavesdropper [48, 49]. For each round of the optical PUF quantum authentication protocol described: A standard challenge-estimation attack, where an adversary who attempts to determine the challenge applied using measurement techniques, will only have a maximum probability of $\frac{2}{(1+d)}$ to cause a 'true' response from the PUF. The overall probability of a false positive decreases exponentially with the number of verification challenges that

combined with input phase settings into a 'challenge' Hilbert space with the response from the device being a 'response' Hilbert space.

[7]Uniqueness should be approximately 50%; this value is based on a binary PUF delivering results from $GF(2^n)$, where the reconfigurable optical device in question will show many more possibilities up to CRP_{max} depending on the initial challenge, thus more unique and semi-unique CRPs exist.

Alice sends to Bob. Since the protocol can be generalized to be q qubits (photons), the state-space becomes $|\psi^{challenge}\rangle^{\otimes q}$, where the attacker's per-qubit success probability is upper-bounded by $\frac{q+1}{q+d}$ [50].

3.2.5 Optical Authentication of Classical and Quantum Information

Traditionally, PUFs are only used for device authentication and not for message authentication. Our device is fully optical and can accept quantum states 'at-once' unlike the original readout protocol [47]. The modified protocol described can also have the additional benefit of being reconfigurable, or the ability to act as many PUFs within a single device due to the tunability of the MZI's relative phases. The major difference is in the density matrix and projected measurements showing the additional ω_p parameter. The value for ω_p changes with each distinct challenge possible within the device, such that the solution space increases not only by $|\psi^{challenge}\rangle^{\otimes q}$ but, by an additional factor of:

$$\sum_{i=0}^{CRP_{max}} \|\omega_{p,\,i}\|\,, \tag{3.8}$$

where the value for CRP_{max} can be determined by a maximal upper bound by following the Catalan numbers [51], C_n. It is then possible to count the number of *distinguishable* settings within the optical PUF by analyzing the MZI structure as a fully-rooted binary tree with $n+1$ leaves. A rooted binary tree may be applied since the PUF is pumped from a single input and can calculate an upper bound given by:

$$C_n = \frac{(2n)!}{(n+1)!n!}. \tag{3.9}$$

This maximal upper limit is unfortunately still too large, due to the number of configurations of MZIs that are not possible within the architecture. The limit of

the architecture where pure Catalan numbering cannot apply is due to the limited number of columns in the device. The limit in number of columns means that the Catalan numbering scheme will count combinations in a light-cone pattern that are impossible. To overcome the configuration limit set by the standard Catalan numbers, a lesser-known combinatorics counting method for binary trees can be utilized, as described by F. Qi and B. Guo [52], the method of counting by integral representation of the Catalan numbers. The method of integral counting can be directly applied to the planar tree variation of counting, similar to the work by P. Flajolet and A. Odlyzko in [53].

If for a forest composed of a set of trees, $\mathcal{F} = \{t_0, t_1, \ldots, t_k\}$, a single tree is examined, $t_i(n, h)$: this tree can represent any binary tree with or without a shared child of height h with n nodes. Simply, $\sum_h t_i(n, h) = C_n$, for the n-th Catalan number. By analysis, the Catalan recurrence for a planar tree gives the recurrence formula for $t_i(n, h)$[8]:

$$t_i(n+1, h+1) = 2 \sum_{m=h+1}^{n} t_i(m, h) \sum_{j=0}^{h-1} t_i(n-m, j) + \sum_{m=h+1}^{n-h-1} t_i(m, h)\, t_i(n-m, h)\,. \tag{3.10}$$

The formula in Equation 3.10 utilizes the double summation to count the number of combinations to build a binary tree on $n+1$ vertices whose left sub-tree has a height h_0, and whose right sub-tree has height $h < h_0$. Doubling this value by a factor of 2 adds all trees whose right sub-tree have height h_0', and whose left sub-trees have height $h' < h_0'$. The final term of Equation 3.10 serves to count the planar trees

[8]This formula requires the following definitions $t_i(0, 0) = 1$ and $\forall\, t_i(0, -) = 0$.

on $n+1$ vertices whose left and right sub-trees are of height h.

Following the modified quantum readout, a simple extension can be made where authentication of classical data, and quantum messages can be completed. In the classical case, Bob receives the optical PUF used in this work that acts as several distinct devices labeled $0, \ldots, CRP_{max} - 1$. Bob wants to send an authenticated classical random variable $x \in \mathbf{X}$ or message vector $\mathbf{x}$ to Alice. Bob's message vector of length n is decomposed into $\mathbf{x}_i = \{0, \ldots, n-1\} \in \mathbf{x}$, where $x = (p_j)_{j=1}^{N}$, $p_j \in \{0, \ldots, CRP_{max} - 1\}$, for some PUF p_j with selected CRP, j, and is subsequently sent to Alice. Alice and Bob perform the following:

1. Bob sends x to Alice over a public and non-authenticated channel.

2. For $j \in \{0, \ldots, CRP_{max} - 1\}$ Alice and Bob both perform the modified quantum readout protocol using the PUF's CRP number p_j.

During each of the CRP tests in p_j, Alice slowly gains confidence that Bob's PUF is returning the responses to her issued challenges. Since there is a response to the challenges it can be assumed that the holder of Bob's PUF agrees with the variable x sent over the non-authenticated channel.

The quantum message authentication variant of the modified quantum readout protocol operates significantly different with respect to the initial design. Consider a PUF design where $CRP_{max} = 3$. Alice sends a random challenge state $|\psi^{challenge}\rangle$ to Bob. Bob then routes the challenge to CRP_0 with probability amplitude α, CRP_1 with probability amplitude β, and CRP_2 with probability amplitude γ. The probability amplitudes are sent to satisfy $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$ since the total

probabilities cannot sum to be greater than one. Bob's response state sent back would then be:

$$|\psi^{response}\rangle = \underbrace{\alpha\hat{R}_0}_{\alpha R_0 U_0^{arb}} |\psi^{challenge}\rangle + \underbrace{\beta\hat{R}_1}_{\beta R_1 U_1^{arb}} |\psi^{challenge}\rangle + \underbrace{\gamma\hat{R}_2}_{\gamma R_2 U_2^{arb}} |\psi^{challenge}\rangle \,, \tag{3.11}$$

which is subsequently sent to Alice. Alice is then able to verify even though she doesn't know the probability amplitudes (α, β, γ) since she does know the components of $\hat{R}_i$ from the initial registration of the optical PUF. This means that when Alice verifies Bob's response, that she will need to rely on the initial PUF weight constant, ω_p, to have a 'best guess' of what the probability assignment for the PUF's CRPs would be when assigned by Bob. Alice then knows that:

$$\left|\omega_p^{CRP_0}\right|^2 + \left|\omega_p^{CRP_1}\right|^2 + \left|\omega_p^{CRP_2}\right|^2 \propto |\alpha|^2 + |\beta|^2 + |\gamma|^2 \,, \tag{3.12}$$

where she will then be able to determine that the responses and probabilities match those that were originally registered from the PUF – assumed to be – held by Bob. Alice also knows from receiving the modified state that the sender *has* to be holding Bob's PUF, through successive state readouts; thus achieving an optical, reconfigurable, PUF-based authentication of a quantum state.

3.2.5.1 Secrecy of Modified Readout for Reconfigurable PUF

From a security standpoint of the quantum message authentication using an all-optical PUF with reconfigurable CRPs, the data could still be considered confidential. Assuming a challenge-estimation attack on a q-qubit system where $q < d$, an initial state $\psi^{challenge}$ would be chosen uniformly at random. An attacker could know

$\psi^{response}$ but would not posses the PUF. Additionally, assuming the attacker does not have access to a quantum machine, or any device that can compute arbitrary unitary transformations losslessly, only a generic measurement could be completed with a biased estimator. The adversary would then only be able to compute an estimation of a response $\hat{\mathbb{E}}_{|\psi^{response}\rangle} = \hat{R}\hat{\mathbb{E}}_{|\psi^{challenge}\rangle}$.

If an adversary challenged Bob's PUF, the response would not necessarily reveal the probability amplitudes (α, β, γ) of the proper CRP because, to an adversary, this information could plausibly be from a different reconfigurable PUF or could relate to a different reconfiguration setting. In addition, an adversary that could determine the probability amplitudes sent for different CRPs would not know the original registered parameter, ω_p, that contains the true suggested probability amplitudes for each of the CRPs within the reconfigurable PUF.

Thus, the modified quantum readout scheme for a reconfigurable all optical PUF verifies the authenticity of the PUF and can be used to authenticate both classical messages and quantum states.

3.3 Strict Photon Authentication

Although the idea of a hardware authentication such as that described in Section 3.2 is good for devices that have a known 'owner,' there are other times when a more mobile authentication type is needed. A more mobile variant of a quantum authentication protocol and quantum identity authentication (QIA) can be shown where simple, non-entangled, photons are used to form a special key-sequence[9] that proves the identity of either a prover or verifier in a two-party system. The major

[9]This key-sequence is not to be confused with a standard encryption or decryption key!

difference is that the QIA protocol is able to be mobile across platforms due to the non-requirement of advanced quantum resources, and can also be used to prove the identity of *multiple* provers or verifiers in a multi-party communication system.

A recent work by C. Hong et al. describes a simple protocol to accomplish QIA with a single photon [54], briefly described where an idealized set of quantum devices are used with user-specific authentication keys that are coded through encoding bases of photon polarization. The protocol requires relatively few resources, with security based on the average eavesdropper's information gained through each protocol run; similar to the way that the optical PUF authentication protocol works for classical information presented in Section 3.2.4. There are two major flaws in the original protocol: *a*) Not a single portion of the secret can be revealed, even accidentally, otherwise Eve is able to collect subsequent portions of the secret during the repeated protocol runs, and *b*) there is no proper adaptation to use the protocol as described to authenticate classical data in a quantum manner. The work pioneered by M. Curty and D. Santos in QIA schemes is a simple building block that has had much work expanded upon it since its inception in 2001 [55]. Similarly to the optical PUF authentication, there is some pre-assigned secret information that each party holds, the security of the protocol requires that there is no leakage of private information during the exchange process and that the execution does not reveal additional information to an eavesdropper through subsequent runs of the protocol.

3.3.1 Photon Identity Authentication Protocol

The general requirements for a non-hardware approach to identity authentication are quite stringent since there is no physical device that is registered then transferred

to the appropriate parties. For the QIA protocol to be secure, the following must be true:

1. *No* portions of the shared secret between communicating parties can be exposed to an eavesdropper,

2. the shared secret must remain unchanged between subsequent reruns from an unsuccessful QIA attempt,

3. and no prior means of authentication of the underlying channel shared between communicating parties can be assumed.

The original QIA protocol based on single photons in the work by C. Hong et al. is based on a pre-shared secret authentication key, $SK = (Sk_1, \ldots, Sk_n)$, where the combination of Sk_i represents a two-bit combination of $\{0, 1\}$. The original protocol also operates in two sets of bases: A rectilinear basis $B_r = \{|0\rangle, |1\rangle\}$, and a diagonal basis $B_d = \{|+\rangle, |-\rangle\}$, used for specific sets of encodings, shown in Table 3.1.

Table 3.1: QIA encoding rules used by Alice and Bob when using a single photon for authentication within an untrusted environment or establishing communication.

Basis	B_r	B_r	B_d	B_d
$Sk_i(k_n, k_{n+1})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
Q State	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$

The protocol between Alice and Bob then continues as shown in Appendix E, as Protocol E.1. The protocol works as expected, but there are potential problems, described below, when it comes to the same MITM attack that the optical PUF is susceptible to.

If Eve is impersonating Alice, then Eve is able to measure the photons coming from Alice and forward fake photons to Bob on the same basis derived from Eve's

measurement. There are three scenarios in this case, where Eve will either be successful in passing the counterfeit data to Bob or she will be detected:

1. Eve's outcome and passing of data agrees with Alice's encoding, where nothing will be detected,

2. the reconstructed photon from Eve is in the correct state but the data may not match what was originally sent by Alice,

3. or the bit decoded by Bob in reception was the result of an incorrect basis selection by Eve, where Bob's decoding will fail.

All options are possible, independent of the mode selected by Alice. If Eve gets a basis selection wrong, Bob will have the incorrect encoding. Since the protocol is designed to be run again, Eve will gain subsequent knowledge from each of the rounds accomplished; she will slowly figure out the information sent and have a higher probability of correctly choosing the basis set by Alice. It is then obvious that for each protocol abort sent, Eve will learn an additional portion of the secret shared between Alice and Bob.

Interestingly, the possibility for a MITM attack to happen on the protocol described by C. Hong et al. means that this work should also be susceptible to similar attacks as were present in the original Bennett-Brassard 1984 (BB84) quantum public key distribution protocol; the foundation of QKD [56]. The protocol described by C. Hong et al. matches the same four-basis state encoding that is present in the original BB84 QKD scheme. Indeed, this is the case, as is shown by H. E. Brandt [57], whereby a probing setup, a 'Brandt probe,' can be constructed for the BB84 QKD scheme such that three separate classes of unitary transformation can be applied to the probe to carry out an entanglement discrimination attack. The simplest method of probing

that H. E. Brandt devised, relies upon the implementation of a single controlled-NOT (CNOT) gate where the control qubit consists of two polarization-basis states of the signal, the target qubit consists of two probe-basis states, and the initial state of the probe is set by the error rate.

The CNOT approach by Brandt to probe a BB84-like protocol, *i.e.* the protocol devised by C. Hong et al., can be applied to make the protocol more secure. Assuming that a modified basis used between Alice and Bob is $B_u = \{|u\rangle, |\bar{u}\rangle\}$ and $B_v = \{|v\rangle, |\bar{v}\rangle\}$, plus an arbitrary $\pm\pi/n$ relative to the computational basis used by Eve. The bases are then related by

$$|0\rangle = cos\left(\frac{\pi}{n}\right)|u\rangle + sin\left(\frac{\pi}{n}\right)|\bar{u}\rangle \qquad |1\rangle = -sin\left(\frac{\pi}{n}\right)|u\rangle + cos\left(\frac{\pi}{n}\right)|\bar{u}\rangle \tag{3.13}$$

$$|0\rangle = cos\left(\frac{\pi}{n}\right)|v\rangle - sin\left(\frac{\pi}{n}\right)|\bar{v}\rangle \qquad |1\rangle = sin\left(\frac{\pi}{n}\right)|v\rangle + cos\left(\frac{\pi}{n}\right)|\bar{v}\rangle\ . \tag{3.14}$$

From the encoding above, Eve can then attempt to reconcile the information sent between Alice and Bob by entangling a travel qubit with a probe register using a CNOT gate,

$$CNOT = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_X\,, \tag{3.15}$$

where I is an identity operation and $\sigma_X = |1\rangle\langle 0| + |0\rangle\langle 1|$ or a Pauli-X bit-flip applied to the target register. Since Eve has the freedom to choose her basis of an initial state ψ_E, she will have four basis operations to chose from, where Bob can observe relative errors induced during communication. Eve then can produce the following possible states through using her own state, the bases B_u and B_v, and her σ_X operation:

$$|u\rangle|\psi_E\rangle \xrightarrow{CNOT} |u\rangle\left(cos^2\left(\frac{\pi}{n}\right)I + sin^2\left(\frac{\pi}{n}\right)\sigma_X\right)|\psi_E\rangle \tag{3.16}$$

$$+ |\bar{u}\rangle \, sin\left(\frac{\pi}{n}\right) cos\left(\frac{\pi}{n}\right)\left(I - \sigma_X\right)|\psi_E\rangle$$

$$|v\rangle\,|\psi_E\rangle \xrightarrow{CNOT} |v\rangle\left(cos^2\left(\frac{\pi}{n}\right)I + sin^2\left(\frac{\pi}{n}\right)\sigma_X\right)|\psi_E\rangle \tag{3.17}$$

$$+ |\bar{v}\rangle \, sin\left(\frac{\pi}{n}\right) cos\left(\frac{\pi}{n}\right)\left(I - \sigma_X\right)|\psi_E\rangle$$

$$|\bar{u}\rangle\,|\psi_E\rangle \xrightarrow{CNOT} |\bar{u}\rangle\left(sin^2\left(\frac{\pi}{n}\right)I + cos^2\left(\frac{\pi}{n}\right)\sigma_X\right)|\psi_E\rangle \tag{3.18}$$

$$+ |u\rangle \, sin\left(\frac{\pi}{n}\right) cos\left(\frac{\pi}{n}\right)\left(I - \sigma_X\right)|\psi_E\rangle$$

$$|\bar{v}\rangle\,|\psi_E\rangle \xrightarrow{CNOT} |\bar{v}\rangle\left(sin^2\left(\frac{\pi}{n}\right)I + cos^2\left(\frac{\pi}{n}\right)\sigma_X\right)|\psi_E\rangle \tag{3.19}$$

$$+ |v\rangle \, sin\left(\frac{\pi}{n}\right) cos\left(\frac{\pi}{n}\right)\left(I - \sigma_X\right)|\psi_E\rangle$$

If Bob measures correctly, then Eve's register must exist in two possible states due to the basis selected, where Eve's state she initially chose for the probing register only provides her a 50% advantage over a random guess. For the 50% of states where Eve cannot decipher the incoming message, her minimum error discrimination between her (non-orthogonal) basis states then leads to the rate of inconclusive measurement to equal her overlap between the discriminated states; thus Eve only can conclusively determine the transmitted symbol only a $(1 - q)$ fraction of the cycles completed between Alice and Bob.

3.3.2 Result of the Modified Strict Photon Authentication Protocol

Since Eve can deploy a Brandt probe constructed according to the maximum performance metric described by J. Shapiro [58] to the described authentication between Alice and Bob, and thus gain further information from the communication that takes place, a classical side-channel can easily be added to further increase the security of the identity authentication protocol. The classical side-channel serves as

a format to send data publicly, where the public information has no value by itself. An eavesdropper will therefore not be able to construct any meaningful information from the information transmitted in the classical side-channel.

The value of the compared secret and the sequential processing of the secret is the downfall of the original single photon identity authentication protocol. By applying a simple hashing mechanism to the protocol, and removing the originally described control mode, the classical/quantum photon identity protocol can be made secure. The change reveals that Eve would then be tasked with finding the specific pseudorandom hash-value and will then be faced with solving the secure identity authentication protocol in an all-or-nothing manner. The probability of solving the pseudorandom hash generator is then nearly zero, depending on the strength of the classical hashing function.

For some alphabet, $\mathscr{A}$, Alice and Bob can share some sequence length $i \pmod 2 = 0$ such that $\exists\, x_i \in X \,\forall\, a \in \mathscr{A}$, there will be a classical hash function $H(\cdot)$ and the standard bases B_r and B_d, which communicate via quantum channel with a classical side-channel. In this instance, a classical (perhaps post-quantum secure) hash function like SHA-3 [59] can be employed, with classical control [60], to help Alice harden her data against Eve, who is using the Brandt probe, by developing a session secret from the hash function with inputs of a random number r and the sequence $x_i \in X$. A modified message mode following this theme would then continue as:

Protocol 3.1 QIA Hash Protocol Between Two Parties

Inputs. Verifier-generated session secret hash value.

Goal. Two parties successfully authenticate each others identity.

The protocol:

1. **Setup.**

   (a) Both parties set individual counters to $n = 0$.

   (b) If $n > Sk_n$, authentication is successful, else proceed.

   (c) Alice chooses the hash-based secure message mode.

2. **Hash Secured Message Mode.**

   (a) Alice generates her modified session secret from the hash of a random number and sequence.

   (b) Bob listens on the classical channel for Alice to send her random number. Bob takes the received random number and calculates a session secret, then starts to listen on the quantum channel.

   (c) Alice then encodes her qubits according to the previous table and sends them individually, not necessitating a secure channel, to Bob.

   (d) Bob expects a sequenced set of qubits and is able to decode them based on the settings agreed in the session secret.

   (e) Bob then can estimate the number of lost or incorrect qubits based on his reception and can form a biased estimation to decide if the message should be kept.

Interestingly, the simple modification necessary to make the originally described scheme secure is only the inclusion of time-slotting and a shared hash function between the two parties. The result is that each authentication appears different from the

previous authentication runs and provides no basis for an eavesdropper to get a full key, shared secret, encoding table, or the hash function itself.

From the previous possible MITM attack described, Eve would measure incoming qubits but would obtain outcomes that are only local operations happening on the strings being sent between Alice and Bob. The hash function guarantees that Eve is unable to deduce the correct measurement basis from knowledge of the randomly generated number alone.

The designed protocol here describes the variation in a random coefficient that is immune to a Brandt probe style attack and makes a non-genuine authentication impossible between the two communicating parties.

CHAPTER 4

QUANTUM SIMULTANEOUS MESSAGE PASSING SECURE COMMUNICATION

As a continuation to the ideas about hash functions and state extension of polynomially mapped quantum messages presented in Chapter 2, it is possible to build a secure message-passing model based on quantum hash functions and their arbitrary length extensions. Specifically, the simultaneous message passing (SMP) model [61] is the best to follow for this work, because it allows a third, trusted, party to handle the direct passing of information between users. The protocol would be fairly complex to realize in a physical system at this time due to limitations in the experimental setup. The major limitation for this protocol would be the implementation of a dual quantum SWAP-test, similar to the implementation for dual signing introduced by J. Liu et al. [62] in 2016. To start understanding how the quantum hash-based SMP protocol would work, a quick refresher on how the SMP model operates is necessary.

4.1 Classical SMP Model

A. C.–C. Yao developed the original basis for the SMP model in 1979 [61] through a question about a communication game. If there is a Boolean function $f : X \times Y \mapsto \{0, 1\}$ where two players, Alice and Bob, wish to collaboratively compute the value of f for an input $(x, y) \in X \times Y$, how can they do so if Alice can only see input x

and Bob can only see input y? The seemingly obvious answer would be what Yao proposed: A model called *simultaneous messages* whereby a referee handles the two variables that Alice and Bob each hold, and computes on behalf of the two parties the evaluation of $f(x, y)$. The evaluation of $f(x, y)$ is, however, not standard since both Alice and Bob *simultaneously* pass their messages of fixed length to the referee, after which the referee announces the function value. Interestingly, each party in the SMP model is a function of the arguments, that each party knows, respectively.

Given two parties and a referee, it should be simple to examine a topological space of tightly interconnected nodes to simulate the message space in which a SMP model could fit. Indeed, the older work by L. Babi and P. Kimmel [63] discusses in their Section 4 how related problems in graph theory regarding the complexity of communication in SMP models apply. The results of the work by L. Babi and P. Kimmel prove that one-sided error randomized simultaneous message complexity is of equality under a restricted set of protocols, namely, those where the function f is symmetric through the equal actions of Alice and Bob.

Suppose that Alice and Bob receive inputs x and y, respectively. If $x = y$, then Alice and Bob send vertices from independent complexity sets, a referee can output 1. If $x \neq y$ then the probability that the referee outputs a 0 is exactly the density of the graph space between the independent complexity sets of X and Y [63]. Looking at the error in this operating scheme shows that as long as x and y are close enough, the result from the referee will be $1 + \epsilon$; there are plenty of options for recovery from a small error introduced by a referee.

4.2 Building a Quantum Hash SMP Model

The work described in Chapter 2 can be applied to the work in this section, as the quantum sponge function can be built into a SMP model. To begin, a simple one-sided Boolean model is constructed and evaluated with respect to a polynomial representation of a message to be passed.

4.2.1 One-Sided Boolean SMP Model

In a model where Alice performs calculations and evaluates data to be sent to Bob, she will ultimately send Bob information with the complexity determined by the number of qubits sent. Bob, in return, computes the portion of the protocol and provides an output. Assuming a function $f(x_1, \ldots, x_{n_1}, y_1, \ldots, y_{n_2})$ with $n = n_1 + n_2$ variables, Alice will handle the sequence of values in x and Bob will handle the sequence of values in y. Since the SMP model has both Alice and Bob handling different information, it is necessary to exploit $f(\cdot)$ to decompose any input polynomial into the sum of two polynomials of equal degree, with one distributed to each communicating member.

Thus, assuming that $f(x, y)$ is a simplified Boolean polynomial function with $n = n_1 + n_2$ variables, there exists a characteristic polynomial $g(x, y)$ for $f(x, y)$ over $\mathbb{Z}_q$. If $g(\cdot)$ can be decomposed such that $g(x, y) = g_1(x) + g_2(y)$, then an arbitrary function $\delta(\cdot)$ can be decomposed and computed by $f(\cdot)$ in a one-way protocol with $log\, d + 1 = \mathcal{O}(log\, log\, q + log(1/\delta))$ qubits of information, following from Equation 2.9.

The communicating parties give a combined input (x, y) and want to know if $f(x, y) = 1$. This is similar to the equation $g(x, y) = 0$ or if $g_1(x) = -g_2(y)$; an equality that a protocol would check based on this simplified scheme, a comparison

of Boolean hash values through a quantum swap-test. If the returned value is not exactly 1, then an intermediate value between 0 and 1 must be considered, since that difference represents similarity in information transmitted.

4.2.2 Swap Test and Quantum Information

The swap-test, as originally described by D. Gottesman and I. Chuang in their 2001 paper on quantum digital signatures [64], details how to determine with certainty whether two unknown quantum states are different in a pass-fail method. The swap-test involves a Fredkin gate [65]; representative for a multi-qubit gate with one control qubit and two target qubits to compare with each other.

Two forms of swap-test gates have been proposed in literature: First, the original, and destructive, Hong-Ou-Mandel (HOM) interference swap using a MZI [66] without an ancillary qubit and second, the non-destructive [67, 68] swap-test that utilizes an ancillary qubit for measurements. The non-destructive swap-test is directly applicable, from a modified Fredkin gate construction [69, 65], used to perform the swap operation. The Fredkin-based swap-test additionally has the advantage of being able to determine the difference between two unknown states, not just to determine if the two states are the same. Since the difference in states is important to the quantum SMP model for information regarding messages, the non-destructive swap-test is the preferred method for this work.

Assuming that there are two prepared quantum states between Alice and Bob for their polynomials, x and y, respectively, then $|x\rangle, |y\rangle \in \mathbb{C}^{2^n}$ will be two quantum states prepared by unitary transition operators U_x and U_y. Or, in individual terms:

$$|x\rangle = U_x |0\rangle^{\otimes n} \quad and \quad |y\rangle = U_y |0\rangle^{\otimes n} . \tag{4.1}$$

The swap-test can be applied to estimate the similarity (or difference) through the calculation of inner product $\langle x|y\rangle$.

The initial state prepared is a controlled unitary phase state,

$$|\phi_r\rangle = \frac{1}{\sqrt{2}}(|+\rangle |x\rangle + |-\rangle |y\rangle)\,. \tag{4.2}$$

The constructed state then is transformed by unitary transformation into U_R as

$$\begin{aligned} U_R &= (I^{\otimes(n+1)} - 2\,|\phi_r\rangle\,\langle\phi_r|)(\sigma_Z \otimes I^{\otimes n}) \\ &= U_{\phi_r}(I^{\otimes(n+1)} - 2\,|0\rangle^{\otimes(n+1)}\,\langle 0|^{\otimes(n+1)})U_{\phi_r}^{\dagger}(\sigma_Z \otimes I^{\otimes n})\,, \end{aligned} \tag{4.3}$$

where $\sigma_Z = |0\rangle\,\langle 0| - |1\rangle\,\langle 1|$ is the Pauli-Z matrix.

The state after transformation is then easily written as

$$|\phi_r\rangle = \frac{1}{2}(|0\rangle\,(|x\rangle + |y\rangle) + |1\rangle\,(|x\rangle - |y\rangle))\,. \tag{4.4}$$

The formula in Equation 4.4 here represents the non-normalized superposition state, through simplification, between the data that Alice and Bob hold, where the density matrix is $|\phi_r\rangle\,\langle\phi_r|$, holding the probabilistic outcome of the swap-test.

Taking the amplitude of the states is done to normalize $|x\rangle$ and $|y\rangle$ where

$$||0\rangle|^2 = \frac{\sqrt{1 + \mathbf{Re}\,\langle x|y\rangle}}{\sqrt{2}} \tag{4.5}$$

$$||1\rangle|^2 = \frac{\sqrt{1 - \mathbf{Re}\,\langle x|y\rangle}}{\sqrt{2}}\,, \tag{4.6}$$

and there exists a real-valued phase that satisfies the amplitudes where $\theta_r \in [0, \pi/2]$. The normalized states between Alice and Bob can be denoted as

$$|u\rangle = |x\rangle + |y\rangle \quad and \quad |v\rangle = |x\rangle - |y\rangle \ , \tag{4.7}$$

where θ_r satisfies the oscillatory amplitude function

$$|\phi_r\rangle = sin\,\theta_r\,|0\rangle\,|u\rangle + cos\,\theta_r\,|1\rangle\,|v\rangle \ . \tag{4.8}$$

Applying the Schmidt decomposition [70] to the state $|\phi_r\rangle$ decomposes the state to

$$|\phi_r\rangle = \frac{-j}{\sqrt{2}}(e^{j\theta_r}\,|y_+\rangle - e^{-j\theta_r}\,|y_-\rangle)\,, \quad \text{where} \quad |y_\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|u\rangle \pm j\,|1\rangle\,|v\rangle)\,. \tag{4.9}$$

The values of $|y_\pm\rangle$ thus represent the eigenstates of U_R, where the information about phases θ_r are contained in the eigenvalues.

From Equation 4.9, the output of a quantum phase estimation [71, 72, 73] will be the approximate state represented as

$$|\psi_r\rangle = \frac{-j}{\sqrt{2}}(e^{j\theta_r}\,|\gamma_r\rangle\,|y_+\rangle - e^{-j\theta_r}\,|2^t - \gamma_r\rangle\,|y_-\rangle)\,, \tag{4.10}$$

where t is a precision parameter derived from the dimension of the referees state-space, and where $\gamma_r \in [0, 2^{t-1}]$ for an approximate value $2\theta_r \approx \gamma_r\pi/2^{t-1}$, since from Equation 4.6, θ_r can be used to satisfy $cos\,\theta_r =$ Equation 4.6, or in other words

$$\mathbf{Re}\,\langle x|y\rangle = -2cos\,\theta_r\,. \tag{4.11}$$

By Equation 4.6 and Equation 4.11, then, it is clear that

$$\mathbf{Re}\,\langle x|y\rangle \approx -cos\left(\frac{\pi\gamma_r}{2^{t-1}}\right). \tag{4.12}$$

The approximate equality here represents the measure of similar information shared between two parties Alice and Bob when transferred and computed in a swap-test and is also suitable for the imaginary component of the information compared, necessary to compare information shared between polynomial strings of phase-encoded data, as developed in Chapter 2.

4.2.3 General Application of Swap Test on Quantum SMP Method

To compile the quantum hashing function component into a SMP model, the swap-test must be applied. For the Boolean function $f(\cdot)$ and the data to be sent, a characteristic polynomial should be considered, χ_f^q on $\mathbb{Z}_q$. For two sets between Alice and Bob, $\Gamma = \{\gamma_1, \ldots, \gamma_{n_1}\}$ and $\Lambda = \{\lambda_1, \ldots, \lambda_{n_2}\}$, of polynomials on $\mathbb{Z}_q$ such that the set $\chi_f^q = \{\gamma_1 + \lambda_1, \ldots, \gamma_{n_1} + \lambda_{n_2}\}$ is characteristic of $f(\cdot)$ over $\mathbb{Z}_q$, there will be a subset of distinct polynomials representing the individual's data. The polynomials from Γ will depend on Alice's input $X = \{x_1, \ldots, x_{n_1}\}$ and the polynomials from Λ will rely on Alice's input in conjunction with Bob's input $Y = \{y_1, \ldots, y_{n_2}\}$ through an intermediate (referee) polynomial set $Z = \{z_1, \ldots, z_i\}$.

4.2.3.1 Alice's SMP Information Transfer

The beginning of the SMP model begins when Alice receives an input $\bar{\alpha} = \{\alpha_1, \ldots, \alpha_{n_1}\}$ and applies the values to $\Gamma(\cdot)$ as $\Gamma(\bar{\alpha}) = \{\gamma_1(\alpha_1), \ldots, \gamma_{n_1}(\alpha_{n_1})\}$ into the following general hash, derived from Equation 2.9, in $log\, d + 1$ qubits as

$$|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \left(cos\, \frac{2\pi b_i(\gamma_1(\alpha_1))}{q} |0\rangle + sin\, \frac{2\pi b_i(\gamma_1(\alpha_1))}{q} |1\rangle \right) \times \\ \ldots \times \left(cos\, \frac{2\pi b_i(\gamma_{n_1}(\alpha_{n_1}))}{q} |0\rangle + sin\, \frac{2\pi b_i(\gamma_{n_1}(\alpha_{n_1}))}{q} |1\rangle \right). \tag{4.13}$$

The state is then sent to Bob, along with information concerning the referee, $Z = \{z_1, \ldots, z_i\}$, that can contain specific information related to the processing of the SMP transfer.

4.2.3.2 Bob's SMP Addition and Conveyance to Referee

Bob then receives the information and prepares his information, $\bar{\beta} = \{\beta_1, \ldots, \beta_{n_2}\}$, the quantum hash $|\psi_{q,\vec{B}}(\cdot)\rangle$, and the values $z_1, \ldots, z_i$. In the absence of a referee, it is possible for Bob to complete the SMP protocol at this point, but it is not suggested, since a referee will have absolute authority over the swap-test function. Bob can compute his respective hash for $\Lambda(\bar{\beta}) = \{-\lambda_1(\beta_1), \ldots, -\lambda_{n_2}(\beta_{n_2})\}$ as

$$|\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \left(cos\, \frac{2\pi b_i(\lambda_1(\beta_1))}{q} |0\rangle + sin\, \frac{2\pi b_i(\lambda_1(\beta_1))}{q} |1\rangle \right) \times \\ \ldots \times \left(cos\, \frac{2\pi b_i(\lambda_{n_2}(\beta_{n_2}))}{q} |0\rangle + sin\, \frac{2\pi b_i(\lambda_{n_2}(\beta_{n_2}))}{q} |1\rangle \right). \tag{4.14}$$

Bob then forwards the result of the functions to a referee to perform the final swap-test, and the information extraction, according to the method defined in Section 4.2.2.

4.2.3.3 Referee's Swap-Test and Information Comparison

The referee takes the set of states from Alice and Bob, $|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle$ and $|\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle$, respectively, and computes the set of phase values θ_r for each of the polynomials $z_i \in Z$. The phase difference values are then calculated following the method from Section 4.2.2. The values utilized by the referee come out to

$$|\theta_r\rangle = sin\,\theta_r\,|0\rangle\,(|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle + |\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle) + cos\,\theta_r(|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle - |\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle)\,, \tag{4.15}$$

following the expected result when applying Equation 4.8. Applying the Schmidt decomposition leads to the eigenstates

$$\begin{aligned} |y_{\pm}\rangle = \frac{1}{\sqrt{2}}(&|0\rangle\,(|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle + |\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle) \\ &\pm j\,|1\rangle\,(|\psi_{q,\vec{B}}(\Gamma(\bar{\alpha}))\rangle - |\psi_{q,\vec{B}}(\Lambda(\bar{\beta}))\rangle))\,. \end{aligned} \tag{4.16}$$

Even though the eigenstates now contain the information related to the originally sent polynomial, a vector of difference values will become apparent. The following section describes a simplified method of handling the similarity between states.

4.2.4 Similarity in Information Outcome from SMP Referee

The referee's outcome of the non-destructive swap-test is ultimately a measure of information similarity, on a scale of 0 to 1, where a 0 represents no similarity in the density operator ($|\phi_r\rangle\,\langle\phi_r|$) and a 1 represents a complete match in information. Any other state between 0 and 1 can be calculated by the referee to determine the differences in data sent from the communicating parties. The differentiation in information is easily completed by following the process starting at Equation 4.9.

The two eigenvalues of the state are the following

$$\lambda_1 = \frac{-je^{j\theta_r}}{\sqrt{2}} \quad \text{and} \quad \lambda_2 = \frac{je^{-j\theta_r}}{\sqrt{2}}\,. \tag{4.17}$$

To find the similarity, the referee's interpretation of the state ϕ_r will be ψ_r, where the two density operators for comparison will be $\rho = |\psi_r\rangle\langle\psi_r|$ and $\sigma = |\phi_r\rangle\langle\phi_r|$. Applying the 1-norm defined for some matrix $A = \sqrt{\rho}\sqrt{\sigma}$ as

$$\|A\|_1^2 = Tr[A^\dagger A] \quad \text{where} \quad A^\dagger A = \sqrt{\sigma}\rho\sqrt{\sigma} = \tau\,, \tag{4.18}$$

and the 2-norm defined as

$$\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_2^2 = Tr[\sqrt{\sigma}\rho\sqrt{\sigma}] = Tr[\sqrt{\sigma}\sqrt{\sigma}\rho] \tag{4.19}$$

$$= Tr[\sigma\rho]\,, \tag{4.20}$$

according to the method employed by M. Wilde to find information similarity [74], then the results can be analyzed according to the decomposed value of τ.

Decomposing the value of τ will be the simple singular value decomposition where

$$\tau = XDX^{-1} \tag{4.21}$$

for a diagonal matrix D. Exchanging the value of $Tr[\sigma\rho]$ for $Tr[D]$ is then allowed since the matrix represents the Hilbert-Schmidt inner product.

By analysis, the following equality will hold true:

$$Tr[\sqrt{D}]^2 = \sum_i \lambda_i^2 + 2(\lambda_1\lambda_2)\,, \tag{4.22}$$

then substituting the necessary eigenvalues leads to

$$\left(\left(\frac{-je^{j\theta_r}}{\sqrt{2}}\right)^2+\left(\frac{je^{j\theta_r}}{\sqrt{2}}\right)^2\right)+2\left(\frac{-je^{j\theta_r}}{\sqrt{2}}\times\frac{je^{-j\theta_r}}{\sqrt{2}}\right), \tag{4.23}$$

with simplification

$$\left(\frac{-e^{j\theta_r}}{2}+\frac{-e^{j\theta_r}}{2}\right)+2\left(\frac{1}{2}\right)=1-e^{j2\theta_r}\,. \tag{4.24}$$

Thus, for some two sets of information from Alice and Bob, the referee in the SMP model will gather that the information similarity can be reduced to solving for θ_r in the following manner

$$e^{j2\theta_r}=cos(2\theta_r)-j\,sin(2\theta_r)\,. \tag{4.25}$$

For this work, the value found for each successive solution for θ_r represents the difference of the information encoded by phase between the two polynomials compared by the referee from Alice and Bob.

4.3 Application of SMP Model and Information Leakage

The SMP model designed for this work is indeed able to be implemented by classical and quantum machines. A classical machine will be able to create a basic classically-mapped function that can be interacted with a purely quantum variant or vice–versa. When analyzing the information difference, the basic state will be considered as a collapsed quantum state and will not contain additional superposition information otherwise required, but is able to be fully mapped into a larger number

of qubits, as described in Section 2.2.2.

The application of the designed SMP model described in this work is secure against classical leakage due to the makeup of the quantum sponge function. This does not mean that a classical machine is not able to compute when in the communication scheme, but that the side information present in this work is secure against an adversary understanding what the information represents. The proofs of quantum hashing being secure against classical leakage are described by C. Huang and Y. Shi [75], whereby a small leakage of classical side information will not ultimately reveal the input of the quantum hash.

Since the referee is the only component of the SMP model with the ability to translate information, the referee becomes the weakest link. Indeed, an adversary with direct access to either of Alice or Bob's messages and the referee's difference polynomial vector could potentially generate a message transformation and find the other party's response. If this process was delegated to several referees, i.e. chaining, then a set of referees may be able to conceal components of state differences, necessitating an adversary to compromise several referees and bases.

CHAPTER 5

PHOTONICS PROCESSOR AND OPTIMIZATION

Photonics research has led into integrated photonic devices to be used for quantum-based processes. Integrated photonics have been used in classical communications for decades, especially in the back-haul fiber communication of our internet today [76]. Integrated quantum photonic applications that promise enhanced security, low loss, low noise, and large computational power are nearly within technological reach. The enabler for this integrated technology is the silicon process that has existed since the turn of the century and promises scalability, integration, and compatibility with CMOS-based microelectronics. The properties of silicon-based integrated quantum nanophotonics circuits enable multiple possibilities of large-scale quantum computation with rapid deployment and ease of manufacturability [77].

5.1 Integrated Silicon Photonics Photon Manipulation

Quantum systems exhibit unique properties and behaviors such as superposition and entanglement. The properties of quantum systems may be used to collect, process, transmit, and encode information, where the field of quantum information science works to revolutionize information technologies. The handling of communication, processing, and collection of information within quantum nanophotonic devices is based on the manipulation of photons; single particles of light [78].

Since silicon has a high third-order nonlinear coefficient $\chi^{(3)}$, the material's refractive index varies with optical intensity, enabling many devices to be fabricated, with varying uses. Devices fabricated in silicon photonics can range from photon sources, photo-optic switches, to transceivers among others. To further understand why a high nonlinear coefficient is valuable for quantum nanophotonics, traditional linear optics must first be understood.

5.1.1 Unitary Decomposition of Photonic Circuits

Without any loss, gains, or parametric processes, any optical system can be simply described by unitary operations. Unitary operations may be considered a special set of operators due to their description as a set of complex rotation matrices or orthogonal matrices. All unitary operations must satisfy the following conditions:

Inverse: $\hat{U}\hat{U}^{\dagger} = \hat{U}^{\dagger}\hat{U} = \mathbb{1}$

Determinant: $|\det \hat{U}| = 1$

Row Normalization: $\sum_i |\hat{U}_{i,j}|^2 = 1$

Column Normalization: $\sum_j |\hat{U}_{i,j}|^2 = 1$

Orthonormality: $\hat{U}_i \cdot \hat{U}_j = \delta_{i,j}$

Decomposition: $\hat{U} = \hat{V}\hat{D}\hat{V}^{\dagger}$

where $\hat{D}$ represents a diagonal matrix and $\hat{U}$ is a unitary matrix. Here it can be said that if $\hat{U}$ is unitary, $\hat{U}\,|v\rangle = \lambda\,|v\rangle$ then $\langle v|\,\hat{U}^{\dagger} = \langle v|\,\lambda^*$. Combining these, the result is $\langle v|v\rangle = \langle v|\hat{U}^{\dagger}U|v\rangle = \langle v|\lambda^*\lambda|v\rangle = |\lambda|^2\,\langle v|v\rangle$. Assuming $\lambda \neq 0$ then $|\lambda|^2 = 1$ is implied, thus all eigenvalues of the unitary matrix are unimodular (having a norm of 1) and can be written easily as $e^{j\alpha}$ for some α. This will help understand the operations of unitary operators within quantum nanophotonic devices.

All linear optical networks may be modeled by unitary operators. These unitary operators need a basis to be physically created to perform computations, with the decomposition of larger circuits into 2×2 matrices outlined by both Reck [79] and Clements [80] using different structures. Both decompositions require an estimated $N(N-1)/2$-many two-port interferometers, able to implement two-dimensional unitary transformations ($U(2)$), to realize an arbitrary N-dimensional unitary matrix. More information on finding the decompositions and proper settings for applying an arbitrary unitary transformation can be found in Chapter 6. A graphical example of the two decompositions mentioned are shown in Figure 5.1.

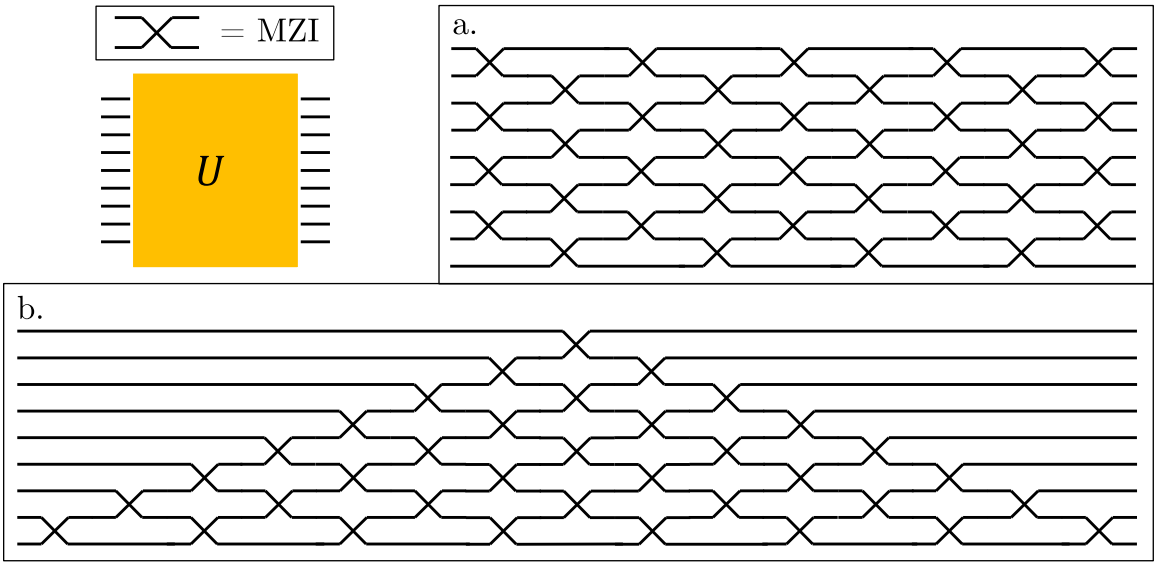


Figure 5.1: Unitary decompositions of a unitary matrix U using both the (a) Clements decomposition [80], and (b) Reck decomposition [79]. Both decompositions use the same number of 2×2 MZIs, with each MZI represented by a 'cross'. Each MZI is composed similarly to the MZI shown in Figure 5.2.

5.1.2 Electric Fields and Photonic Propagation

The unitary matrix is special in that it represents the scattering of the interaction of the electric fields present from photons such that a relation can be made between the waveguides present in the photonics processor and the spatial separation to support an axial propagation coefficient. Examining how the unitary transformation physically interacts with photons, a simple relation for an electric field, $\vec{E}$, can be made:

$$\vec{E}_{out} = U\vec{E}_{in}\,. \tag{5.1}$$

As a first step, Maxwell's equations can be applied where they are expressed in a form of an eigenvalue problem of a Hermitian operator [81, 82]. First, Amperes law is applied such that:

$$\nabla \times \vec{H} = \epsilon(x,y,z)\epsilon_0 \frac{\partial \vec{E}}{\partial t} \tag{5.2}$$

$$= -j\omega\epsilon(x,y,z)\epsilon_0 \vec{E}\,, \tag{5.3}$$

where rewriting for $\vec{E}$ in terms of a traverse field distribution and a traveling wave in the axial direction, $\phi(x,y)e^{-j\omega t + j\beta z}$:

$$\nabla \times \frac{1}{\eta^2(x,y)} \nabla \times \vec{H} = \omega^2 \vec{H}\,. \tag{5.4}$$

The index of refraction, η, is present in Equation 5.4, showing a direct link for this application between Ampere's law and a refraction coefficient. Since the result is a Hermitian operator describing the magnetic field, a relation can be written:

$$(\Theta\psi, \phi) = (\psi, \Theta\phi)\,, \text{ where } \Theta = \nabla \times \frac{1}{\eta^2}\nabla \times \frac{1}{\omega^2}\,, \tag{5.5}$$

for a vector pair (ψ, ϕ) describing the interaction of the magnetic field $\vec{H}$; Θ then being dependent on the distribution of the index of refraction. From the work by A. Hardy and W. Streifer, there is a simple method of describing the coupled mode theory for parallel waveguides [83].

Depending on the length parameter between two waveguides, the Hermitian operator from Equation 5.5 relates directly to a splitting ratio of a directional coupler, controlled by choosing a coupling length. For some splitting ratio η_s, the unitary transformation applied by a directional coupler is:

$$U_{coupler} = \begin{pmatrix} \sqrt{\eta_s} & j\sqrt{1-\eta_s} \\ j\sqrt{1-\eta_s} & \sqrt{\eta_s} \end{pmatrix}\,. \tag{5.6}$$

The single MZI shown in Figure 5.2 details the construction, typically utilized within the field of integrated silicon photonics, where a controlled phase is necessary. Two directional $50:50$ beamsplitters are mated together with electronic control of doped resistive ($850\,\Omega$ typ.) heating elements. The heating elements are adjacent to portions of the waveguide and have the effect of dynamically changing the length of two directional couplers, L_{C1} and L_{C2}.

The values for L_{C1} and L_{C2} are important to the operation of the MZI because they serve to adjust the splitting ratio of each directional coupler. Considering a single 2×2 directional coupler, the length L will be given by

$$L = \frac{3L_\pi}{2} \tag{5.7}$$

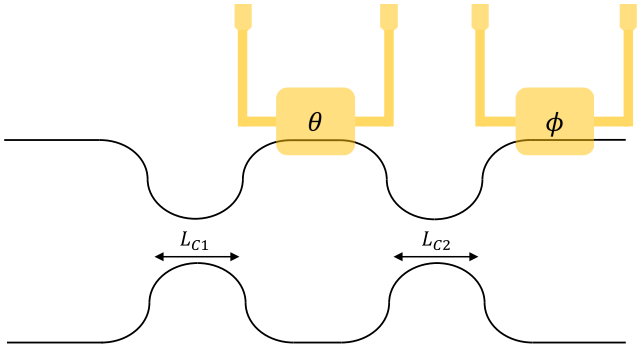


Figure 5.2: Single MZI and control composed of two directional beamsplitters and two integrated resistive heaters. The control covers both the internal and external phases, (θ, ϕ), through the thermo-optic effect, effectively changing the lengths of L_{C1} and L_{C2}.

where L_π is the angular mode propagation, defined as

$$L_\pi = \frac{\pi}{\Delta\beta}\,. \tag{5.8}$$

The value of $\Delta\beta$ is the waveguide mode propagation constant difference, $\Delta\beta = \beta_1 - \beta_2$, which is dependent on the coupling coefficients between the top T and bottom B waveguides, χ_{TB} and χ_{BT}. From coupled mode theory, an amplitude relation is present according to A. Hardy and W. Streifer [83], which states that there is a directionally fixed[1], propagation dependent, amplitude relation:

$$\begin{aligned} \frac{dA_T(z)}{dz} &= -j\,\chi_{BT}\,e^{j\Delta\beta z}A_B(z) \\ \frac{dA_B(z)}{dz} &= -j\,\chi_{TB}\,e^{j\Delta\beta z}A_T(z)\,, \end{aligned} \tag{5.9}$$

for a z-axis propagation direction with amplitudes, A.

The unitary transformation can alternatively be described by the phase relations

[1]Directionally fixed, assuming that a transverse field exists within the waveguide's structure such that there is z-axial dependence generated by the electric and magnetic fields, $\{\vec{E}_t, \vec{H}_t\}$ [83].

in a transfer matrix. A simplified method of phase relation between two waveguides was developed by M. Paiam and R. MacDonald [84]. The method of phase relation, γ, shows that for an input i to output j, for a 2×2 coupler is

$$\gamma_{i,j} = \delta_B - \frac{\pi}{2}(-1)^{i+j+2} + \frac{\pi}{8} \times \left[i + j - i^2 - j^2 + (-1)^{i+j+2} \left(2ij - i - j + \frac{1}{2} \right) \right], \tag{5.10}$$

where δ_B is a constant phase response for the bottom waveguide given by

$$\delta_B = -\beta_T \frac{3L_\pi}{2} + \frac{3\pi}{16}. \tag{5.11}$$

The output amplitude distribution from the 2×2 MZI then is given by

$$\begin{pmatrix} A_T^{out} \\ A_B^{out} \end{pmatrix} = U_{coupler} \begin{pmatrix} A_T^{in} \\ A_B^{in} \end{pmatrix}, \tag{5.12}$$

for a coupler unitary matrix, $U_{coupler}$. The effect of the heaters on phases from Equation 5.10 results in a total transfer matrix T of

$$T = \begin{pmatrix} e^{j(\Delta\gamma_T + \varepsilon\gamma_T)} & 0 \\ 0 & e^{j(\Delta\gamma_B + \varepsilon\gamma_B)} \end{pmatrix},$$

where $\varepsilon\gamma_{(T/B)}$ is the resulting error terms accumulated from the differing portions of the MZI. The resulting output from the waveguides are differences in optical intensity with the base definition stemming from Equation 5.9, calculated as a ratio between $|A_T^{out}|^2$ and $|A_B^{out}|^2$.

5.1.3 Mach-Zehnder Interferometer Unitary Implementation

The major option for the basis of the N-dimensional implementation of a unitary matrix are Mach-Zehnder interferometers (MZIs), mentioned in Section 5.1.2. When using two waveguide-based 50:50 beamsplitters, a phase-shifter may be placed in the path of one of the two legs between the beamsplitters, and the reflectivity of the MZI may be controlled. Assuming some phase of an optical field incident to the input ports can be set, a MZI with an internal phase shifter can implement *any* rotation in $U(2)$ through the addition of a phase shifter in one of the output paths of the MZI. The structure of a photonics processor using multiple MZI unit cells is shown in Figure 5.3.

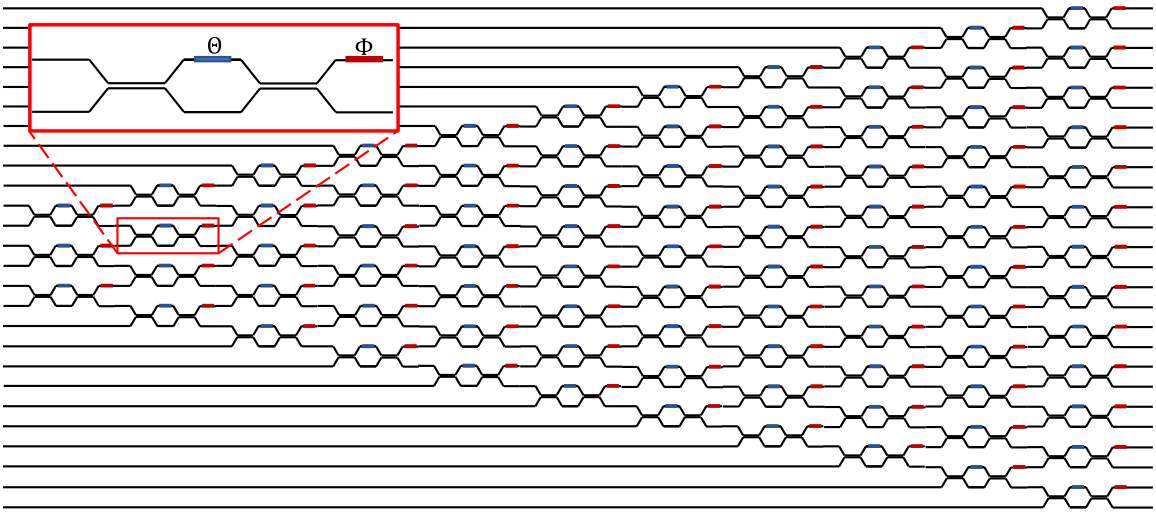


Figure 5.3: QPP architecture showing the structure of MZIs following a modified Reck scheme, shown in Figure 5.1b. This device is designed to be built in a silicon-on-insulator (SOI) process. Waveguides are the horizontal black lines. The internal phase difference θ controls the splitting ratio and the external phase difference ϕ controls the output phase offset. There are 11 layers in total, enabling the implementation of a 26-mode unitary transformation and an 8-mode arbitrary unitary transformation.

Each MZI is able to be thermally tuned by an integrated resistive heating element acting as a phase shifter. The phase shifters, $\theta = \Delta\gamma_T$ and $\phi = \Delta\gamma_B$, which map to

the internal phase setting and output phase offset, respectively, since each MZI can be described by two different transfer matrices:

$$\begin{pmatrix} e^{j\theta} & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} e^{j\phi} & 0 \\ 0 & 1 \end{pmatrix} . \tag{5.13}$$

The phase shifting matrices can be combined with the unitary transformation for the directional couplers in Equation 5.6 to create an equation describing the MZI with respect to the phase applied and the splitting ratios for two sequential couplers, η_{s1} and η_{s2},

$$U_{MZI} = \begin{pmatrix} e^{j\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{\eta_{s2}} & j\sqrt{1-\eta_{s2}} \\ j\sqrt{1-\eta_{s2}} & \sqrt{\eta_{s2}} \end{pmatrix} \begin{pmatrix} e^{j\theta} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{\eta_{s1}} & j\sqrt{1-\eta_{s1}} \\ j\sqrt{1-\eta_{s1}} & \sqrt{\eta_{s1}} \end{pmatrix} . \tag{5.14}$$

Each MZI is able to apply an ideal 2×2 unitary transformation shown in Equation 5.15 with respect to only phase settings, assuming ideal splitting ratios.

$$U_{MZI}(\theta,\phi) = \frac{1}{2} \begin{pmatrix} e^{j\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \begin{pmatrix} e^{j\phi} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & j \\ j & 1 \end{pmatrix} \tag{5.15}$$

A $v2\pi$ voltage range, described further in Section 5.2, is required for a complete response from a typical MZI; with expanded definition of the sinusoidal response from Equation 5.15, simply modified into a sine or cosine format, shown in Equation 5.16.

$$U_{MZI}(\theta,\phi) = \frac{1}{2}\begin{pmatrix} e^{j\phi}(e^{j\theta}-1) & je^{j\phi}(e^{j\theta}+1) \\ j(e^{j\theta}+1) & -(e^{j\theta}-1) \end{pmatrix} = je^{\frac{j\theta}{2}}\begin{pmatrix} e^{j\phi}\sin\left(\frac{\theta}{2}\right) & e^{j\phi}\cos\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \tag{5.16}$$

Since these devices have an ability to be arbitrarily programmed and controlled, it is possible to implement quantum gates out of sets of properly adjusted MZIs to manipulate single photons (qubits). Properly adjusted and controlled MZIs can then be used to carry out protocol or experimental design and simulation.

5.2 Quantum Photonic Processor Optimization

Optimization of networks and graphs are well-known problems since the advent of advanced computing methods and techniques; starting with the rise of parallel computing for optimization in the 1960s [85]. Finding the solutions to large and complex networks and graphs has become simplified to a point where researchers expect solutions to their complex problems within time-frames spanning from hours to a few days, instead of days to a few weeks as became common in the 1980s [86]. Graph and networking theory grew rapidly, with two distinct directions spawning from advances in molecular and electrical theories between the late 19th to 20th centuries; forming two core parts of graph theory, algebraic graph theory and optimization theory.

Today, the optimization portion of both graph and networking theories has an application in all fields, from science and medicine to economics and finance. For this work, following the points of research and development listed in Section 1.2.2, there is reason to research how graph and networking optimization can be applied to

photonics and optics. The work by N. Lagali et al. [87] serves as one of the first analytical approaches to optimizing switching characteristics in generalized Mach-Zehnder inferferometers (GMZIs) by employing multimode interference (MMI) couplers and examining their deviations in phase relations and power splitting ratios through transfer matrices.

A large component of accurately controlling a photonics processor is the optimization and careful characterization of such large MZI structures. There are several forms of optimization that can be used for an array of MZIs. The most common of these currently seek to optimize either in a swap-iterative format [88] or in a recursive search method. For this work, a new method of arrayed MZI optimization is described through the utilization of previously unused global optimizers. The work of this dissertation builds on the theoretical framework by N. Lagali et al. [87] by examining a working system of integrated phase shifters operating on a linear interferometer network with the purpose of single-photon manipulation and control [88, 89]. Such networks are known to be able to perform small quantum circuits [90]. The development work completed here additionally serves to showcase a set of 'best' optimization techniques for handling a large linear interferometer array to achieve full control of the device without necessitating total calibration prior to application.

5.2.1 Global Optimization

Due to the general design of the QPP, and to the sources of error previously mentioned in Section 3.2.1, following an iterative approach to the characterization and optimization of the device is quite challenging due to the degrees of freedom present in the design. Recent work by B. Bartlett and S. Fan, in November 2019, shows a prime example of the complexity of a generic photonic processor for quantum

manipulation tasks [91] which is similar to the notation in Section 5.1.3 but certainly notes that the theoretical framework of photonic architecture usage for quantum information processing is done without error and assumes ideal quantum gates.

In this work, looking at the simple iterative approach towards optimization is a very resource-intensive task and creates overhead in the setup of the device that results in slowed operation. The general optimization approach of simplicial homology is an excellent resource for the photonic device due to its general integer coefficients, representing degrees of freedom, of simplicial complexes where reduction can result in sparse matrices. The sparse matrices are representative of the general combinational topology present on-device and can generally be approximated into homomorphic boundaries between the MZIs present on the device, as previously described in Section 5.1.3.

The work by S. Endres et al. [92] discusses a simplicial homology global optimization for Lipschitz optimization but, the algorithm assumes that the function being optimized has Lipschitz continuity or, given two metric spaces with their metrics, (X, d_X) and (Y, d_Y), a function $f : X \mapsto Y$ would be considered Lipschitz continuous if there exists a real constant $K \geq 0$ such that $\forall x_1, x_2 \in X$,

$$d_Y(f(x_1), f(x_2)) \leq K d_X(x_1, x_2)\,. \tag{5.17}$$

Since any K would be the Lipschitz constant for $f(\cdot)$, it is possible for $0 \leq K \leq 1$ where $f(\cdot)$ may map a metric space to itself, a contraction. This contractive response[2] is what harms a potentially great optimization method and forces one to move to a different simplicial homology global optimizer.

[2]Assuming that there are imperfections in the MZIs and that the system is relatively imperfect, as represented in Equation 5.14, the MZI will need to be handled as non-Lipschitz continuous.

A topographical global optimization method, then, is the best contender to handle the optimization of a large number of degrees of freedom on the photonic processor. A. Törn and S. Viitanen came up with a simple method [93] to attack this problem. The essence of the work by A. Törn and S. Viitanen starts with the mapping of the objective function, in this case a function similar to Equation 5.16, into a topography matrix and then finds starting points to the function i.e. local minimizers. The topology matrix is then searched via the initial minimizers and each new minimum is found and operates towards the calculation of the global minimum required.

For the work in this dissertation, a mathematical 'structure' is provided to an algorithm[3] that represents the MZIs, their adjustable parameters, and the expected ideal response. From the initial parameters, a uniform random sampling occurs where the generation of N points is created within the search space. The points generated are then used to form a topograph of the photonic processor, specifically, a directed graph where each sampled point is a vertex to k nearest neighbors. The nearest neighbor vertices then form the basis for the direction of a path towards points of larger function values. The constructed topograph is then locally minimized, contributing to a larger global maximum.

5.2.1.1 Generation of Sampling Points

Generating the sampling points within the function set is easily achieved through a grey-code implementation defined by I. Antonov and V. Saleev [94] from their 1979 paper detailing single XOR operations for each dimension. Since the dimensions used for the current photonics architecture are generally low, up to an 8×8 matrix, the

[3]Keep in mind that the structure will represent the largest unitary that can fit on the device, in this case an 8×8, where each composite 2×2 unitary made possible by the MZI has matching θ and ϕ parameters.

resulting number of computations to chose N sampling points is low. From a vertex v_i to the next sampling point x_i, the only computation necessary to find the following sampling point is $x_{n,i} = x_{n-1,i} \oplus v_{k,i}$. The implementation of the method to find sampling points is a component of the UQToolkit maintained by Sandia National Lab [95].

5.2.1.2 Construction of the Topograph from MZIs

The topograph for the photonics processor can be directly calculated from the resulting components and intermediate points after the sampling point generation derived from a Clements decomposition [80], as previously discussed in Section 5.1.1. The image shown in Figure 5.4 highlights three stages of point decomposition for a 2-qubit gate.

The 2-qubit gate decomposition into the topograph works similarly to the Clements decomposition, although the topograph is constructed from the generated sampling points within the function space. The function space for the construction is made from probabilities of paths and points, representing the final required distribution of laser-light to be seen on the output ports of the photonic processor. From the simple 2-qubit set of MZIs shown in Figure 5.4, the initial step is to examine the paths possible for alternate routes and their resulting regions within the Clements representation of decomposition. The result will be a set of matrices with distinct probabilities for a given pathing. The second step is to move to the following stage of MZIs to determine what specific modes are interfered and how the paths may change. Following this procedure for the depth of the circuit will result in the topograph's set of initial global minimizer functions, $f(\cdot)$.

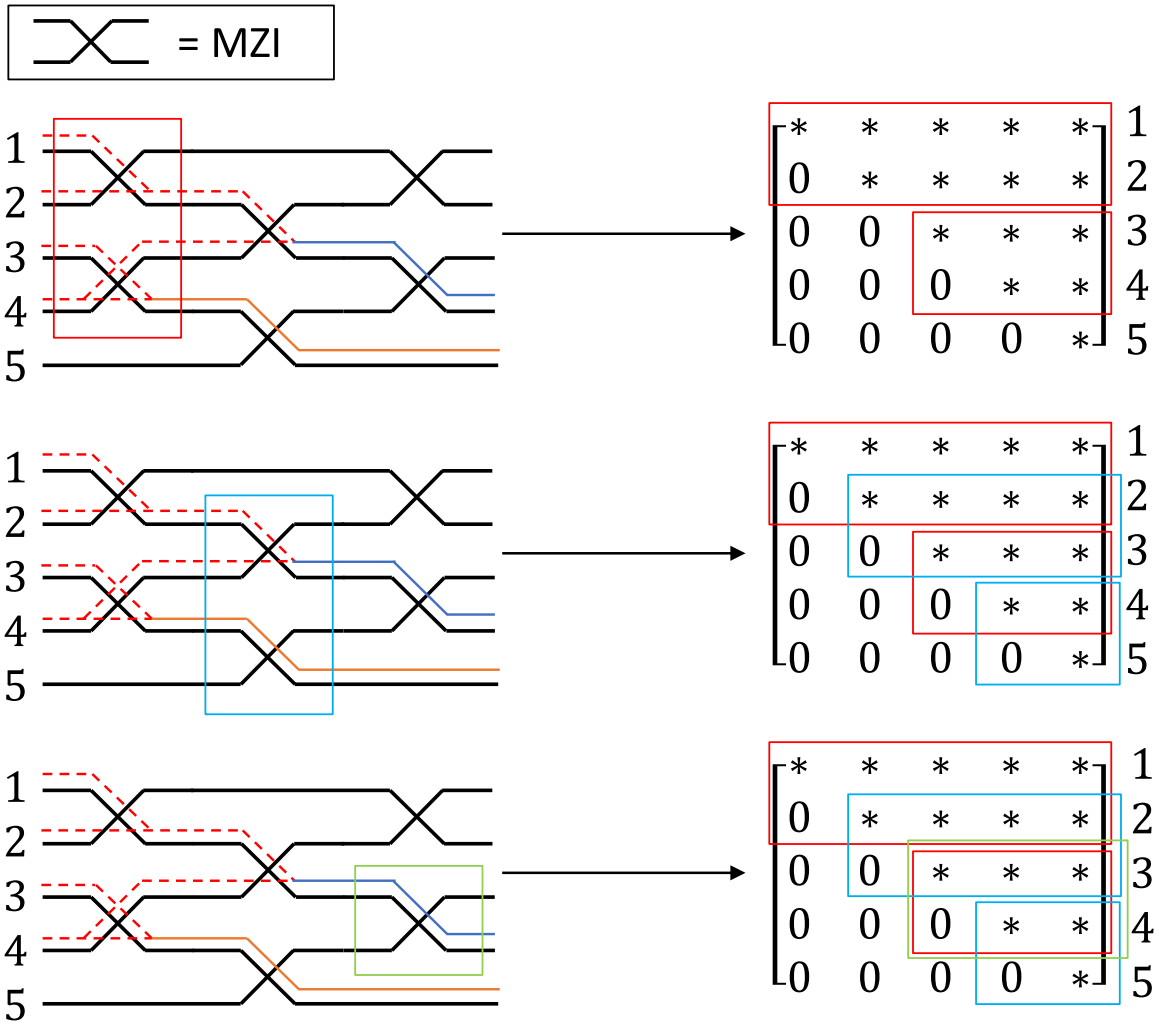


Figure 5.4: Multipath Clements decomposition showing the three stages of a simple 2-qubit gate being decomposed with varying pathing (red, dashed) into the architecture. The matrices to the right of each of the three steps shows where the points are affected after each pathing operation. The topograph points are selected to be intermediately between MZIs but along the respective paths based on wanted output distributions.

The first points within the matrix are effectively selected from the previous uniformly generated sequence of points within a feasible domain, a subset of the real-space operators. Any points that lie outside of this constraint can be ignored since they will not have an effect on the final pathing required for a specific distribution of laser-light on the output ports. The points remaining after eliminating outliers can be ordered by their Euclidean distances. The final ordered list contributes to the final rows of the topograph.

5.2.1.3 Minimization of Functions for MZI Pathing

Each functional minimizer within the topograph, generated as described in Section 5.2.1.2, is used as a starting point for local minimization. The resulting local minima are then used to find a global minimum. The method to find the direction of interior points for pathing though MZIs follows the method set by N. Henderson et al. to find all solutions of nonlinear systems with constraints [96]. The method employed for minimization and local search of functions applies a functional map gradient to the points selected to minimize to the selected pathing required. Assuming that $\nabla f(\cdot)_i \in \mathbb{R}^{n\times m}$ where $f(\cdot) : \mathbb{R}^n \mapsto \mathbb{R}^m$, the function to be minimized will result in a matrix of partial derivatives of $f(\cdot)$. If there is a local minimizer that exists, then first-order optimality will be satisfied, i.e. there will exist a vector of Lagrange multipliers where the elements of the vector are real sets of diagonalizeable integers.

5.2.2 Implementation of Global Optimizer

To implement the optimizer, the method followed was as used by W. Sacco et al. [97] regarding topographical clearing functions for point generation. The original function implemented by W. Sacco et al. was implemented in C++, however, the

method utilized for this work was based in Python 3.x and was adapted to change the method of stochastic number generation by following the output of a previously developed hash-based number generator [98]. The adapted number generation by Sacco was originally based on the Mersenne Twister [99] but was replaced by a standard SHA-2-based hash function, due to issues with large-order patterning, a recurring problem for Mersenne Twister-based generators [100].

The remainder of the function implemented followed the method previously described by N. Henderson et al. [96] to find the solutions of nonlinear solutions, also implemented in Python 3.x.

To run the optimizer, first the pattern of the QPP's architecture was taken into account. A single waveguide was then pumped with classical laser-light and the output intensities were measured. The program then collects samples of the affected MZIs in the light-cone and their relative outputs. The outputs are the upper and lower legs of the MZIs affected by the laser-light input, where the estimated end-points are where the ideal output profile dictates light should travel.

From the first measurement, the topology matrix is constructed with the current positions of light in the waveguides to the output ports and compared against the requested output profile, similar to the measured output profiles described in Section 3.2.4. From this point, the topology matrix is solved for the MZIs and optimized by the routine described previously. The optimized matrix is then converted into the MZI voltage settings and iterated until a steady-state point is reached.

The optimizer developed successfully takes an input source of laser-light from either a single, or multiple, waveguide(s) with the matching initial characterization map, and applies the topographical global optimization scheme with constraints. The constraints on the topographical global optimizer routine determine the method of

pathing within the photonics processor, and determine the final output profile that matches the pathing, according to the constraints initially provided. The application of the optimizer to the photonics processor serves as a large step towards quick and efficient optimization for large linear MZI arrays, enabling other researchers the ability to successfully construct and experiment on large sets of MZIs with high fidelity.

CHAPTER 6

QUANTUM PHOTONICS PROCESSOR HARDWARE/SOFTWARE CO-SIMULATOR

An important portion of this work was the development of a method to simulate not only quantum information processors, but the optical device that was available during the course of writing this dissertation [14]. To complete this task, the early version of Xanadu's software, Strawberry Fields, was used as inspiration [101]. The Strawberry Fields software was originally designed as a full-stack quantum software platform to design, optimize, and simulate photonic quantum circuits. The Strawberry Fields suite, however, does not have a method to handle hardware photonic chips, their architectures, and proper co-simulation[1].

6.1 Quantum Circuit Back- and Front-end

The back-end for the quantum simulator developed is simply created in Python 3.x, first with a focus on the generation of quantum circuits. The back-end was designed as a 'noisy' quantum simulator, where operational and integer noise could be modeled to get a fuller picture of the operation of quantum circuits in a realistic setting. The errors modeled include fidelity errors of the quantum logic gates as well as timing

[1]The co-simulation functionality still has not been implemented in Strawberry Fields at the time of defense - April 2020.

errors. The simulator designed for this work has many tunable parameters designed to fully encapsulate errors seen in typical gate implementations.

The errors modeled to the specific architecture used in experimentation, i.e. the experiments shown in Chapter 3, relate to variances in the total optimization of the photonic chip, after following the method outlined in Section 5.2 and the implemented circuits.

Since the simulator and the controlling software for the photonics processor is written with a Python back-end, there is a simple extension to the simulator where any modeled circuit that is able to be implemented on-chip can be co-simulated. First, the desired quantum circuit is designed using a custom command-console. Second, the unitary transformation is generated, along with MZI phase settings that are then translated to voltages based on the $v2\pi$ response range of the device. Third, the settings are uploaded to the device and the states are prepared for operation. Fourth, the simulator simulates an idealized circuit without error and then simulates a version of the circuit with variational errors derived from device-specific tolerances. After the simulation is complete, the photonic circuit is then run and the response histograms are created, based on real-valued responses from a superconducting nanowire single photon detector array.

6.2 Quantum Photonics Simulator

There are, overall, three primary components that are related to the simulator itself. The first is the circuit composer, used to construct circuits that are to be run on a photonics processor. Second is the circuit decomposition technique; a set of techniques derived from the work by Reck and Clements, previously described in

Section 5.1.1 and visualized in Figure 5.1. Finally is the photonic simulation itself including all errors. The decomposition output is piped into the simulator, simulations are run, and the results recorded.

The quantum gates that can be applied within the simulator are all standard Clifford gates, and arbitrary unitary gates. The gates supported fully by the simulator are:

- Identity Gate: I
- Hadamard Gate: H
- Not Gate: X
- Phase-Shift Gate (π): Z
- Phase-Shift Gate ($\pi/4$): T
- Controlled-Phase Gate: TC
- Controlled Not Gate: CX
- Controlled Rotation Gate: CR

where any of the 'control' gates are able to be expanded to an arbitrary number of qubits, up to the limit for the number of run-time configurations for standard dual-rail qubits or spatial qubits.

6.2.1 Circuit Composition

The underlying composition of the circuits within the simulator is built so that the initialization of a circuit is started only when given a size, in a number of qubits, that should be operated upon.

```
n_qubits = 3
circuit = Circuit(n_qubits)
```

Next, a gate should be added to the circuit following a special method, add_gate( ), that creates a gate object. As an example, a not gate (X) can be added to the 0th qubit. Note that the qubit the gate is to be assigned to is passed to the gate object.

```
circuit.add_gate(X(0))
```

Additionally, multiple gates may be added in a single statement as follows

```
circuit.add_gate(X(0), X(1))
```

Chained function calls also work when multiple gates are needed in succession.

```
circuit.add_gate(X(0)).add_gate(X(1))
```

For controlled gates, the gate object should be provided the control qubit(s) first, followed by the target(s).

```
circuit.add_gate(CX([0,1], [2,3]))
```

A representation of the circuit can be printed to the console as follows

```
circuit.apply()
print(circuit.draw())
```

which provides the following output:

```
|0> ———X———X———————CX———
|0> ——————————X———@———
|0> ———————————————————
```

Following the work by the IBM team behind a general simulator for their quantum architecture, Qiskit [102], the circuit simulator designed may also add ‘moments’ to

the quantum circuit. Each moment simply represents a slice of a quantum circuit that may have multiple operations happening across multiple qubits simultaneously. To create the moment, it must be specified that gates are to occur in the same moment by creating a moment object, adding gates, then adding the moment to the circuit; enabling better control over how a circuit is run.

First, the moment is created by providing the number of qubits in a circuit.

```
moment = Moment(circuit.n_qubits)
```

Next, the gates are added to the moment. Both the multiple-gate method and chained-gate method may be employed when adding to a moment, similarly to adding individual gates to a circuit.

```
moment.add_gate(H(0), H(1))
```

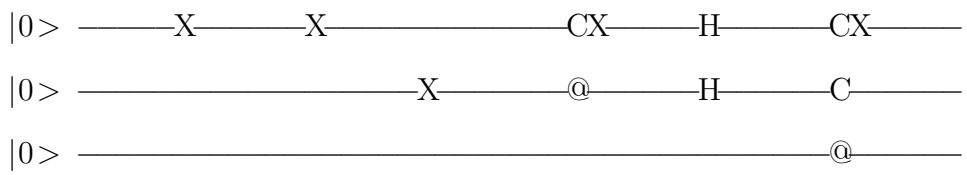
Lastly, the moment is added to the circuit.

```
circuit.add_moment(moment)
```

To see the results, the circuit can be printed again, similarly to the previous example, utilizing single gates, except the output will now predictably change based on moments.

```
|0> ———X———X———————CX———H———
|0> ——————————X———@———H———
|0> ———————————————————————
```

Suppose an additional gate is added with multiple control, circuit .add_gate(CX(0, 1, 2)), and the circuit reprinted. The resulting output will then change.



There is also additional information that can be gathered, including the unitary matrix generated, a flag indicating whether the operations are unitary, and the possible output states.

```
Unitary:
  0.5   0.0  -0.5   0.0   0.5   0.0   0.0  -0.5
  0.0   0.5   0.0  -0.5   0.0   0.5  -0.5   0.0
  0.5   0.0   0.5   0.0   0.5   0.0   0.0   0.5
  0.0   0.5   0.0   0.5   0.0   0.5   0.5   0.0
  0.5   0.0   0.5   0.0  -0.5   0.0   0.0  -0.5
  0.0   0.5   0.0   0.5   0.0  -0.5  -0.5   0.0
  0.5   0.0  -0.5   0.0  -0.5   0.0   0.0   0.5
  0.0   0.5   0.0  -0.5   0.0  -0.5   0.5   0.0

Is unitary really unitary? True.

States:
  0.5|000>
  -0.5|010>
  0.5|100>
  -0.5|111>
```

6.2.2 The Circuit and The Unitary Decomposition

The circuit and generated unitary transformation are then able to be decomposed following either the Reck or Clements transform, described in Section 5.1.1. To complete the decomposition, the following can be run.

```
mzi_settings, output_phases = reck_decomp(circuit.unitary)
```

The output of printing both variables, for the circuit previously generated, will result in the following set of phase settings and output phase adjustment necessary to implement the circuit. The format for the MZI settings is $[waveguide_1, waveguide_2, \theta, \phi, size]$ and the format for the phase adjustments is a vector of required rotations.

```
[[6, 7, 0.0, 3.141592653589793, 8],
[5, 6, 1.5707963267948966, 0, 8],
[4, 5, 0.7853981633974483, 3.141592653589793, 8],
[3, 4, 1.5707963267948966, 0, 8],
[2, 3, 0.9553166181245092, 3.141592653589793, 8],
[1, 2, 1.5707963267948966, 0, 8],
[0, 1, 1.0471975511965979, 3.141592653589793, 8],
[6, 7, 0.7853981633974483, 3.141592653589793, 8],
[5, 6, 1.5707963267948966, -6.123233995736766e-17, 8],
[4, 5, 0.9553166181245092, 3.141592653589793, 8],
[3, 4, 1.5707963267948966, -8.164311994315688e-17, 8],
[2, 3, 1.0471975511965979, 3.141592653589793, 8],
[1, 2, 1.5707963267948966, -9.184850993605148e-17, 8],
[6, 7, 3.061616997868383e-17, 3.141592653589793, 8],
[5, 6, 1.5707963267948966, -1.8369701987210304e-16, 8],
```

```
[4, 5, 1.0471975511965976, -1.0205389992894612e-16, 8],
[3, 4, 1.5707963267948966, -1.103539415828288e-16, 8],
[2, 3, 0.9553166181245093, 3.141592653589793, 8],
[6, 7, 1.0471975511965976, 3.0616169978683836e-16, 8],
[5, 6, 1.5707963267948966, -3.141592653589793, 8],
[4, 5, 0.9553166181245093, -3.141592653589793, 8],
[3, 4, 1.5707963267948966, -5.3674054655673156e-17, 8],
[6, 7, 4.329780281177466e-17, 1.7934537145593042e-17, 8],
[5, 6, 1.5707963267948966, 3.141592653589793, 8],
[4, 5, 0.7853981633974483, 2.144840517017907e-16, 8],
[6, 7, 0.7853981633974483, -3.141592653589793, 8],
[5, 6, 1.5707963267948966, 9.013958510555925e-17, 8],
[6, 7, 1.0330811926697055e-17, -2.8127958890487004e-16, 8]]

[-1.-1.22464680e-16j
1.+9.18485099e-17j
1.+3.16367090e-16j
-1.-6.74008172e-17j
1.+1.65762483e-16j
-1.-6.16847722e-18j
1.+3.56902487e-16j
1.+6.74008172e-17j]
```

The resulting set of values are then piped into the processor optimizer as a set of parameters, required to be met to implement certain circuits, in a method other than

those generated by the global optimizer.

6.3 Theoretical Gate Error and Fidelity Model

To aid in conditioning the results from the photonic processor, there is the necessity for simulation of gate error and simulation of fidelity measure. Classical computers have obvious benchmarking possible on CPUs, GPUs, memory, hard drives, etc. but there is no universal quantum benchmark. Upcoming benchmarking by industry leaders include qubit quality, qubits' fidelity, coherence times, and connectivity. Since the platform utilized for this work is photonic, there is not the same error induced as would typically be seen on an industry superconducting-qubit quantum computer.

Previously mentioned in Section 5.1.3, Equation 5.14, there are limited mathematical models related to MZI error, but none for total quantum gate error in relation to the photonic processing platform. When looking at gate fidelity, $\mathcal{F}$, a parameter for fidelity may be associated with each quantum gate. The fidelity then represents a measure of how close a particular quantum gate is applied versus the idealized quantum state that the gate intended to apply. Mathematically, the fidelity can be computed between an idealized state output, $|\Phi\rangle$, and the actual state of the system $|\hat{\Phi}\rangle$, where U is the ideal unitary transform occurring, and $\hat{U}$ is the imperfect transformation taking place.

$$U\,|\Psi\rangle = |\Phi\rangle \tag{6.1}$$

$$\hat{U}\,|\Psi\rangle = |\hat{\Phi}\rangle \tag{6.2}$$

When analyzing the resulting fidelity, the measure would be calculated as

$$\mathcal{F} = \left|\langle\Phi|\hat{\Phi}\rangle\right|^2. \tag{6.3}$$

For simulation, the imperfect difference generated by the gate application can be modeled as a unitary transform purely composed of errors, U_ϵ. The error generated here is a coherent error where there is no distinct loss in coherence of the quantum state, only a loss or unwanted transformation of information happening to the output of the quantum state after the application of a gate transformation.

Experimentally, measurement of fidelity is not as straightforward, and can ultimately be simulated with varying probabilities based on errors inherent to the qubit's platform. The errors may be measured experimentally by first applying a gate (unitary transformation) to a qubit such that the ending measurement of the qubit is targeted to return the basis state. The application of the unitary and its inverse would be a simple $UU^\dagger$ but, there is a distinct possibility that instead of a basis state, an orthogonal state may be returned. If an orthogonal state is returned, then that implies that the operation $UU^\dagger$ did not transform the state as intended, and it can be completed several more times to determine an average fidelity $\langle\mathcal{F}\rangle$.

6.3.1 Photonic Intensity (Amplitude) Errors

There are several possible reasons for one to measure an incorrect state. In photonics especially, there are two major sources of error *a*) amplitude errors, and *b*) phase errors. The amplitude errors culminate as intensity errors, where laser-light is not of the expected intensity in a classical sense, or where a detector experiences far more registrations than would be expected. Amplitude errors are some of the most difficult errors to quantify and track within a system, where the qubit interactions present can be from other gates, other qubits, or even the environmental noise present.

Being able to quantify intensity errors is extremely important in understanding how a quantum circuit operates in a real-world environment, outside of the laboratory.

For a single qubit gate, an error parameter ϵ can be used to denote total intensity error culminated in the final state output for the system. The error can be described by a unitary-error transformation as

$$U_\epsilon \left|\Psi\right\rangle = \epsilon \left|\Psi_\perp\right\rangle + \sqrt{1-\epsilon^2}\left|\bar{\Psi}\right\rangle \ . \tag{6.4}$$

The transformation is representative of the error seen by the state perpendicular to the operational state ($\left|\Psi_\perp\right\rangle$), plus the error seen by the intended operational state ($\left|\bar{\Psi}\right\rangle$).

As a simple example, a not gate σ_X, with parameters $\left|\Psi\right\rangle = \left|0\right\rangle$ and $\left|\bar{\Psi}\right\rangle = \left|1\right\rangle$, will return a relation for gate fidelity, notated as

$$\mathcal{F} = 1 - \epsilon^2 \, . \tag{6.5}$$

Thus, for an error $\epsilon = 0$, the σ_X gate will return without error, where the unitary transform will also have no error, i.e. fidelity is 1.

The error for a gate operation can be extended to create intensity error unitaries for each of the major gates ran, with the most common shown below.

$$\hat{\sigma}_{X_\epsilon} = \begin{bmatrix} \epsilon & \sqrt{1-\epsilon^2} \\ \sqrt{1-\epsilon^2} & \epsilon \end{bmatrix} \tag{6.6}$$

$$\hat{H}_\epsilon = \begin{bmatrix} \epsilon + \sqrt{1-\epsilon^2} & -\epsilon + \sqrt{1-\epsilon^2} \\ -\epsilon + \sqrt{1-\epsilon^2} & -\epsilon - \sqrt{1-\epsilon^2} \end{bmatrix} \tag{6.7}$$

$$\hat{CNOT}_{\epsilon} = \begin{bmatrix} \sqrt{1-\epsilon_1^2}\sqrt{1-\epsilon_2^2} & -\epsilon_2\sqrt{1-\epsilon_1^2} & -\epsilon_1\epsilon_2 & -\epsilon_1\sqrt{1-\epsilon_2^2} \\ \epsilon_2\sqrt{1-\epsilon_1^2} & \sqrt{1-\epsilon_1^2}\sqrt{1-\epsilon_2^2} & -\epsilon_1\sqrt{1-\epsilon_2^2} & \epsilon_1\epsilon_2 \\ \epsilon_1\sqrt{1-\epsilon_2^2} & -\epsilon_1\epsilon_2 & \epsilon_2\sqrt{1-\epsilon_1^2} & \sqrt{1-\epsilon_1^2}\sqrt{1-\epsilon_2^2} \\ \epsilon_1\epsilon_2 & \epsilon_1\sqrt{1-\epsilon_2^2} & \sqrt{1-\epsilon_1^2}\sqrt{1-\epsilon_2^2} & -\epsilon_2\sqrt{1-\epsilon_1^2} \end{bmatrix} \tag{6.8}$$

From Equation 6.8 it is noted that the errors are in terms of two qubits. Similarly, if written for a three qubit gate such as a controlled-controlled-not (CCNOT), there would be three separate error terms, one related to each qubit in operation. Thus, the following fidelities can be assigned for one- and two-qubit gate operations:

$$\mathcal{F}_{one-qubit} = 1 - \epsilon^2 \tag{6.9}$$

$$\mathcal{F}_{two-qubit} = (1-\epsilon_1^2)(1-\epsilon_2^2)\,. \tag{6.10}$$

Since the gate errors are not identical for each run, averages must be taken for each gate error fidelity. Assuming repeated uses of a gate do not result in the same intensity error, the average fidelity then can be calculated for the same one- and two-qubit gate operations:

$$\langle \mathcal{F}_{one-qubit} \rangle = 1 - \langle \epsilon^2 \rangle \tag{6.11}$$

$$\langle \mathcal{F}_{two-qubit} \rangle = 1 - \langle \epsilon_1^2 \rangle - \langle \epsilon_2^2 \rangle + \langle \epsilon_1^2 \epsilon_2^2 \rangle \ . \tag{6.12}$$

The fidelity averages can then be generalized for n-qubit operations as

$$\langle \mathcal{F}_q^n \rangle = 1 - (\langle \epsilon_1^2 \rangle - \langle \epsilon_2^2 \rangle - \ldots - \langle \epsilon_n^2 \rangle) + (\langle \epsilon_1^2 \epsilon_2^2 \ldots \epsilon_n^2 \rangle)\,. \tag{6.13}$$

From the equations for average fidelity, as long as a matching probability distribu-

tion for any gate's error completely reflects the nature of the gate's error forms, there will be an accurate model for error for every gate implemented by the co-simulation suite.

6.4 Co-Simulation of the Photonic Processor

The co-simulation of the photonic processor is accomplished by a Python 3.x hook to the optimizer and control code. First, the initial calibration data is fetched from a SQLite database for a static pathing similar to the estimated circuit implementation. Second, the optimizer is applied to the circuit when activated with laser-light to implement the expected circuit and pathing model required. Finally, when the optimizer is finished applying the finalized circuit and phase settings, a comparison versus the probabilistic simulated outcome is completed. When the circuit is near to an 'ideal' simulation, sets of scores are given to the simulator to show the user the most likely simulation matching real-world output results.

The continued development of the co-simulator is ongoing and remains a topic for future research.

CHAPTER 7

CONCLUSION, RECOMMENDATIONS, AND FUTURE WORK

Quantum computing is ultimately an interdisciplinary field, melding several concepts and techniques from engineering, computer science, and physics. The applications of quantum computing are still few, but span a broad range; from factorizing, Hamiltonian simulation, and black-box search optimization. Each of the basic tools available to quantum computers; superposition, entanglement and interference, play an important role in several fields to solve problems from 'designer' pharmaceuticals, to quantitative finance, to complex engineering problems. Each field, however, necessitates communication and has present security threats when operating between classical and quantum machines to solve complex tasks.

The research presented in this work set out to answer the question of whether or not secure communication primitives could be designed that would work interchangeably between classical and quantum computers, and if so, how could the primitives designed be used together? The work towards that goal, for this dissertation, is a large step towards the complete interchangeability of hybrid quantum–classical protocols and their underlying algorithms. The general findings, however, lead to the understanding that while quantum technologies are coming to the forefront, they are not displacing existing classical technology that is used in everyone's everyday

life.

7.1 Key Objectives

The key research objectives for this work were: *a*) development of a non–QKD approach towards secure communication, *b*) utilization of a silicon-based quantum photonics processor and the development of high-resolution control, enabling fine-grained phase settings, and an updated design of a photonics processor with a control system, *c*) utilization of quantum teleportation for inter-quantum-processor communication of gates and associated secret information sharing, *d*) and the final development of several components required for a quantum ciphersuite.

The key research objectives all led into a common goal: A ciphersuite developed that is hybrid quantum-classical in the sense that both are required to create a secured method of communication, not necessitating QKD. The contributions towards the field of quantum security that were completed during the course of this research were:

1. Development of the first quantum sponge function, capable of absorbing either quantum or classical information, and producing a keyed, reversible output stream.

2. Development of the first all-optical physically unclonable function based on a linear interferometer array.

3. Development of an embedding mechanism to map a quantum hash onto a polynomial lattice.

4. Development of multiparty single-photon authentication and multi-party keys.

5. Development of a global optimization technique for tunable linear interferometer arrays built on topology graph optimization.

The first key objective was met, and was described in Chapter 2, tying into the second key objective towards a quantum–classical ciphersuite described in Chapter 3. The third key objective was a major component towards the quantum sponge function, from Chapter 2, with the fourth key objective serving to support the single-photon-based authentication scheme shown in Chapter 3. The work in Chapter 5 meets the fifth, and final, key objective which makes it possible to run the experiments from Chapter 3, and opened the pathway towards optimization of the SMP protocol described in Chapter 4.

Methods and application developed 'along-the-way' include the alternate method of the quantum swap-test, supporting a return of information similarity (or difference), to users through a referee, the new form of global optimization subroutines as applied to the requirements in Chapter 6, a method to examine the path transitions described in portions of Chapter 2, and a mechanism to determine the automorphisms of information while being operated within the setting of the quantum random walk. A numerical analysis method based on the Catalan numbers was also developed to help analyze the possible number of CRPs for the given architecture of MZIs in the hardware device shown in Chapter 3.

7.2 Quantum Sponge Relevance

The quantum sponge designed in this work is unique, in that the capability is now present to map either quantum or classical messages into a polynomial space of interconnected nodes. Once the message is mapped into a polynomial-node space, it is

able to be either extended arbitrarily according to a set of rules governed by a quantum random walk, in either constrained or unconstrained space, or may be applied into a message passing model. The messages passes between parties can be deconstructed by a referee where the information contained in the original message is not lost, and is considered secret against an adversary (discussed further in Section 7.4).

7.3 Multiparty Authentication Component Remarks

The two main components of the multiparty authentication were the development of an all-optical PUF based on linear interferometric device arrays, and the development of a method of using single photons for authentication tasks. Both have interesting applications, but the all-optical PUF has certain limitations, as was found during experimentation.

7.3.1 All-Optical Physically Unclonable Function

The results extrapolated by a planar tree recurrence from Equation 3.10 serve to highlight the optical interferometric PUF's ability to scale exponentially, thus meeting the first criterion for a strong PUF by C. Herder et al. [36]. An additional facet of the design shown is the ability to have quick reconfigurability to assess additional CRPs. Since each of the MZIs are independently tunable, it is observed that the response of a tuned device, and the change of parameters for subsequent CRPs, changes the device's total output and its ability to affect the system. The ability to tune the device at-will enhances application and use-cases to not only the static processing of information but to the processing of streaming information. It is thus possible to

process information streamed through the device or static information where a set of CRPs is dynamically changed depending on the information received.

Unfortunately, there are several negative attributes to using a system of interferometers as a PUF. The greatest negative is the one where nearest-neighbor challenges may give predictable results on smaller PUFs. In addition, the interferometric system is highly structured and fixed, such that a sufficient number of CRPs being calculated could lead to the device being fully characterized. Indeed, the QPP was designed with such characterization in mind, because the original use case was for applications and experimental testing of quantum optical networks [103]. It should be pointed out that the device was not originally intended to act as a PUF and that the operation is based on exploiting its attributes. Since the reconfigurability of the QPP is available, it is possible to make one device clone the function of another device; for purpose of using it as a PUF, it is suggested to utilize this device in an uncalibrated mode. Custom designed interferometric circuits with more complicated interconnections, including variable feedback loops, would be more resistant to characterization and thus act as stronger PUFs.

A second negative attribute of the current prototype is that the operating temperature must be stable within $\pm 1^{\circ}$C. Allowing the temperature to vary may be a route to increasing the number of challenge and response pairs if two devices respond differently to temperature changes. This is an open research question. If temperature variation were not desired, packaging the device may lead to an easy method of stabilization. Alternatively, multiple sets of CRPs can be created for an array of temperatures prior to use. The variation with temperature observed is a direct result of using common SOI and CMOS fabrication. Silicon is a thermo-optic material and was chosen for its ease of integration into existing CMOS processes. However,

the design for an interferometric optical PUF can be trivially transferred to an electro-optically controlled material such as Lithium Niobate to create a more stable standalone device or an application specific integrated circuit. It should be noted, however, that Lithium Niobate will still have a small thermo-optic effect. Conversely each challenge $\bar{C}_i$ could double as an independent bias setting for the device. A variation in other parameters, such as global heating of the device, wavelength inputs, and variance in the number of pumped channels, can allow each challenge to be utilized as an individual, separate, PUF. Here, these parameters have been taken to be constants for simplicity, but if allowed to vary, utilizing more parameters opens an enormous set of possible CRPs theoretically available.

Finally, with the software drivers used in these experiments, it takes approximately 3 seconds to completely set a challenge and measure a response of 1,000 physical measurements on the QPP. This has since been significantly improved with a new driver optimization. The fundamental limit to the speed of the challenge and response is set by the maximum speed that the thermal switching can occur; estimated to be in the $\approx$ 100kHz range [104]. This may appear slow, but it should be stressed that the experimental setup was in no way designed to optimize the speed of the measurements. The system currently runs on several standard Arduino-driven Teensy boards, for ease of development. Hardware integration with an FPGA and implementation in an electro-optical media will result in orders of magnitude speed-ups to gigahertz speeds. If a design were optimized for usage as a PUF with the proper, previously mentioned controls, then the existence of reconfigurable optical PUFs will greatly enhance the security of future optical communications.

7.3.2 PUF-based Identity Authentication

In this work, the use of a reconfigurable all-optical PUF is described as a hardware authentication mechanism. The usage of the optical PUF as an authentication mechanism is carried out by a modified quantum readout protocol. The readout protocol makes the PUF able to authenticate classical and quantum information through the usage of classical light or single-photon-level manipulations. Additionally, the usage of the hardware optical PUF enables one to authenticate that the receiver of information is not adversarial in nature. This work represents the first application of an all-optical reconfigurable PUF for tasks other than object and direct-access user authentication.

7.3.3 Single Photon Authentication

The work to develop a standard single photon authentication mechanism built on top of the recent work by C. Hong et al. [54], whereby a method to utilize a single photon for authentication tasks can be achieved. Since there is a limited quantum resource being utilized for the task, where only the basis is of importance, along with the position characteristics, it is possible for this technique to coexist between quantum and classical computation. To overcome possible probe-style attacks on the scheme, it was modified slightly to employ a classical, post-quantum, technique to obfuscate the selected basis, along with the same position encodings.

The downside to this method, however, is when one may wish to send many more messages in succession than the number of possible basis selections. This situation could lead to possible attack by an eavesdropper with similar power to an oracle operating in a similarly modeled situation.

7.4 Quantum Simultaneous Message Passing

The SMP model developed for this work is based on the mapping of messages to polynomial nodes presented in earlier sections. The major breakthrough in this method is the application of the sponge-based mapping to a model where two (or more) parties may communicate through a referee. Since the referee serves to compare information and relay the differences to the parties, a new form of information criterion applied to a SMP model had to be utilized, based on the Schmidt decomposition. The result is that the referee is able to send a difference measure to the parties, instead of a true or false result.

The inclusion of the information difference between messages then can be further developed into a method for information and key agreement schemes in the future. The key agreement schemes possible from this work, and that will be looked into in the future, would be multi-party key agreements, with the ability to limit access to certain information only meant to be shared with select members of the key agreement.

7.5 Photonics Processor and Optimization

Photonic integrated circuits have become important in the past several years and have been integral to classical optical communication for decades. The attributes that make the photonic integrated circuits ideal for classical communications; compactness, high fidelity, high bandwidth, and the control of a large number of optical modes, make them ideal for use in new applications. Thus, photonic integrated circuits can be used not only for optical classical computing, but for integration of quantum computing with classical optical networks and for quantum acceleration.

The major benefit of the photonics processor is that it is designed around existing CMOS processes, common among foundries world-wide, and that it operates at the same optical wavelengths of current optical telecommunications equipment. The scalability of the photonics processor is also advantageous in that many optical modes, unitary controls, and phase modulators may be implemented on a single chip, not requiring the large amount of space and the stability controls required in bulk optics.

The major future applications of the photonics processor range from self-configuring optical experimental circuits, to quantum information processing, to machine learning and neural network implementation. Specific interest goes to quantum information processing, and entanglement consumption in further quantum applications such as multi-party key agreement schemes, quantum radar, and time-traversal quantum gates.

The setup of a global optimizer for the photonics processor is also relevant, for not only the experimental setup, but for the simulation of specific circuits, to model their operation and the required set-points when it needs to be inclusive of errors that may occur due to imperfections. While the photonic circuits and MZIs are imperfect devices, the goal of the global optimizer is to get rid of imperfections due to the variances in fabrication and to the computer-control of the MZIs integrated resistive heaters. The ability to model and predict the operation of the photonics processor is an important step to enable other researchers to simulate how their quantum circuits and implementations may operate, given the chance to use a similar platform.

The optimizer designed in this work has application where rapid global optimization is necessary, in instances where one might wish to use the photonics processor to model the previously-mentioned Hamiltonian simulations, or for quick switching and optimization of implemented security protocols; a topic for future continued research.

7.6 Photonics Processor Simulation

The application of the quantum photonics co-simulator was originally developed to characterize and simulate the possibilities of implementing portions of the aforementioned hybrid ciphersuite components. The simulation of the photonics processor and contributions made by this work aim to be the foundation of more elaborate simulation systems based on photonic processors, their application in quantum information processing, and their integration into existing optical telecommunication technologies. Since the simulator developed in this work is capable of co-simulation with a physical device, it is of interest to other researchers in similar fields to have access to a simulated version of the photonics processor.

The current state of quantum technologies is fragmented, at best, and shows how unification of written instruction set architectures is necessary at this point in time. As companies and organizations develop their own technologies 'in the dark' a wedge is being driven between researchers who are agnostic to platform. By creating an open platform for others, future research on a given technology will have real weight behind the research.

The photonics simulator thus has multiple attributes to make it a future candidate which would be easily adopted by researchers: The application of a comprehensive decomposition technique for arbitrary unitary transformations, a method of inducing simulated gate errors as applied to the photonic architecture, and an instruction set architecture with simple key words to apply gates and moments to a quantum circuit, with the back-end applying the necessary transformations through transparent methods.

7.7 Final Thoughts and Recommendations

In all, the work presented in this dissertation is not an end-all be-all for a quantum secured hybrid ciphersuite, but represents possible implementations of several ciphersuite components that may operate together cohesively. The representations of information in this work should only serve as a simple foundation to build hybrid ciphersuites. As quantum computing continues, in scale, to become something that classical machines can no longer predict, it will be of utmost importance to secure classical information in a manner considered 'NP'-hard (at a minimum) to the quantum computer.

It is thus a strong recommendation that any base for security developed, with quantum supremacy on the horizon, be one based on physical devices. Software-only approaches will be easily solved in this scenario due to being within the exact nature of the types of problems that quantum computers are good at – black box searches.

7.8 Future Work

Obviously a dissertation is not truly the end of research in a field, but is a small window into a major realm of interest and continued study. Future work stemming from this dissertation is still security-focused and will naturally contribute to the end goal of a full quantum ciphersuite, not merely primitives that work well together, and not merely the processing of data. Continued work that is happening at the time of writing extends into the mathematical mechanisms by which the quantum hash SMP function operates, and the trade-offs that need to be made when considering hybrid algorithms. Some of this work includes the creation of a mathematical tool to allow one to pre-measure a quantum state, then continue operating on it, while achieving the

same result as if the measurement had been done after all operations were completed. Additional work investigates the homomorphic operations on quantum state vertices, and the topology of interconnected states and their related transitions through unitary and non-Clifford gate operations.

Strategies for achieving the goals of future work are actively being worked on, by examining the continuity, differentiation, and quantum state transfer in discrete quantum state structures. The focus of the immediate work is to see how one may traverse continuously, in continuous time, on *just* the vertices of directed graphs, and an application for the transfer of quantum states through a continuous path in a simple quantum network. The work ultimately leads into directed graph homomorphisms of quantum states, and can lead to the development of a more efficient method of quantum homomorphism.

REFERENCES

[1] G. Louie, R. Retter, and J. Slager, "Interface between a microprocessor and a coprocessor," Oct. 15 1985. US Patent 4,547,849.

[2] S. T. Mayer, J. G. Miner, D. G. Neubauer, and J. C. Decuir, "Data processing system with programmable graphics generator," Oct. 20 1981. US Patent 4,296,476.

[3] I. Damgård, V. Pastro, N. Smart, and S. Zakarias, "Multiparty computation from somewhat homomorphic encryption," in *Advances in Cryptology–CRYPTO 2012*, pp. 643–662, Springer, 2012.

[4] A. López-Alt, E. Tromer, and V. Vaikuntanathan, "On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption," in *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pp. 1219–1234, 2012.

[5] C. Peikert and S. Shiehian, "Multi-key fhe from lwe, revisited," in *Theory of Cryptography Conference*, pp. 217–238, Springer, 2016.

[6] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*. US Department of Commerce, National Institute of Standards and Technology, 2016.

[7] G. Alagic, G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, *et al.*, *Status report on the first round of the NIST post-quantum cryptography standardization process*. US Department of Commerce, National Institute of Standards and Technology, 2019.

[8] A. Ambainis, A. Rosmanis, and D. Unruh, "Quantum attacks on classical proof systems: The hardness of quantum rewinding," in *2014 IEEE 55th Annual Symposium on Foundations of Computer Science*, pp. 474–483, IEEE, 2014.

[9] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchangea new hope," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, pp. 327–343, 2016.

[10] R. König, R. Renner, A. Bariska, and U. Maurer, "Small accessible quantum information does not imply security," *Physical Review Letters*, vol. 98, no. 14, p. 140502, 2007.

[11] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New Journal of Physics*, vol. 11, no. 4, p. 045018, 2009.

[12] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, no. 2, p. 441, 2000.

[13] H. P. Yuen, "Universality and the criterion'd'in quantum key generation," *arXiv preprint arXiv:0907.4694*, 2009.

[14] N. C. Harris, J. Carolan, D. Bunandar, M. Prabhu, M. Hochberg, T. Baehr-Jones, M. L. Fanto, A. M. Smith, C. C. Tison, P. M. Alsing, and D. Englund, "Linear programmable nanophotonic processors," *Optica*, vol. 5, no. 12, 2018.

[15] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge functions," in *ECRYPT hash workshop*, vol. 2007, Citeseer, 2007.

[16] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proceedings of the 1st ACM conference on Computer and communications security*, pp. 62–73, ACM, 1993.

[17] B. Guido, D. Joan, P. Michaël, and V. Gilles, "Cryptographic sponge functions," 2011.

[18] R. Rivest, "The md5 message-digest algorithm," tech. rep., 1992.

[19] D. Eastlake III and P. Jones, "Us secure hash algorithm 1 (sha1)," tech. rep., 2001.

[20] D. Eastlake III and T. Hansen, "Rfc 4634-us secure hash algorithms (sha and hmac-sha)," *Motorola Labs and AT &T Labs*, 2006.

[21] R. Merkle, "Secrecy, authentication, and public key systems," *Ph.D. Thesis, Stanford University*, 1979.

[22] I. B. Damgård, "A design principle for hash functions," in *Conference on the Theory and Application of Cryptology*, pp. 416–427, Springer, 1989.

[23] M. Liskov, "Constructing an ideal hash function from weak ideal compression functions," in *International Workshop on Selected Areas in Cryptography*, pp. 358–375, Springer, 2006.

[24] Y.-G. Yang, P. Xu, R. Yang, Y.-H. Zhou, and W.-M. Shi, "Quantum hash function and its application to privacy amplification in quantum key distribution, pseudo-random number generation and image encryption," *Scientific Reports*, vol. 6, p. 19788, 2016.

[25] A. Schreiber, K. N. Cassemiro, V. Potoček, A. Gábris, P. J. Mosley, E. Andersson, I. Jex, and C. Silberhorn, "Photons walking the line: a quantum walk with adjustable coin operations," *Physical Review Letters*, vol. 104, no. 5, p. 050502, 2010.

[26] D. Li, J. Zhang, F.-Z. Guo, W. Huang, Q.-Y. Wen, and H. Chen, "Discrete-time interacting quantum walks and quantum hash schemes," *Quantum Information Processing*, vol. 12, no. 3, pp. 1501–1513, 2013.

[27] F. Ablayev and A. Vasiliev, "Cryptographic quantum hashing," *Laser Physics Letters*, vol. 11, no. 2, p. 025202, 2013.

[28] A. J. Dragt, "Lectures on nonlinear orbit dynamics," in *AIP conference proceedings*, vol. 87, pp. 147–313, AIP, 1982.

[29] A. J. Dragt and J. M. Finn, "Lie series and invariant functions for analytic symplectic maps," *Journal of Mathematical Physics*, vol. 17, no. 12, pp. 2215–2227, 1976.

[30] J. Cornwell, "Group theory in physics, volume i, ii, iii, volume 10 of," *Techniques of Physics*, 1984.

[31] M. Born, W. Heisenberg, and P. Jordan, "Zur quantenmechanik. ii.," *Zeitschrift für Physik*, vol. 35, no. 8-9, pp. 557–615, 1926.

[32] A. Nahum, J. Ruhman, S. Vijay, and J. Haah, "Quantum entanglement growth under random unitary dynamics," *Physical Review X*, vol. 7, no. 3, p. 031016, 2017.

[33] A. Rényi *et al.*, "On measures of entropy and information," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, The Regents of the University of California, 1961.

[34] D. A. Huse and C. L. Henley, "Pinning and roughening of domain walls in ising systems due to random impurities," *Physical Review Letters*, vol. 54, no. 25, p. 2708, 1985.

[35] D. S. Fisher, "Interface fluctuations in disordered systems: 5- ε expansion and failure of dimensional reduction," *Physical Review Letters*, vol. 56, no. 18, p. 1964, 1986.

[36] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014.

[37] T. Xu and M. Potkonjak, "Stable and secure delay-based physical unclonable functions using device aging.," in *ISCAS*, pp. 33–36, 2015.

[38] S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "The butterfly puf protecting ip on every fpga," in *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pp. 67–70, IEEE, 2008.

[39] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "Physical unclonable functions and public-key crypto for fpga ip protection," in *Field Programmable Logic and Applications, 2007. FPL 2007. International Conference on*, pp. 189–195, IEEE, 2007.

[40] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.

[41] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum physical unclonable functions: Possibilities and impossibilities," *arXiv preprint arXiv:1910.02126*, 2019.

[42] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[43] C. Mesaritakis, M. Akriotou, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, and D. Syvridis, "Physical unclonable function based on a multi-mode optical waveguide," *Scientific Reports*, vol. 8, no. 1, p. 9653, 2018.

[44] B. C. Grubel, B. T. Bosworth, M. R. Kossey, H. Sun, A. B. Cooper, M. A. Foster, and A. C. Foster, "Silicon photonic physical unclonable function," *Optics Express*, vol. 25, no. 11, pp. 12710–12721, 2017.

[45] M. Prabhu, "Towards optimal capacity-achieving transceivers with photonic integrated circuits," Master's thesis, Massachusetts Institute of Technology, 2018.

[46] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security*, pp. 3–37, Springer, 2010.

[47] B. Škorić, "Quantum readout of physical unclonable functions," *International Journal of Quantum Information*, vol. 10, no. 01, p. 1250001, 2012.

[48] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[49] D. Bruß and C. Macchiavello, "Optimal state estimation for d-dimensional quantum systems," *Physics Letters A*, vol. 253, no. 5-6, pp. 249–251, 1999.

[50] B. Škorić, "Security analysis of quantum-readout pufs in the case of challenge-estimation attacks," *Quantum Information and Computation*, vol. 16, pp. 0050–0060, 2016.

[51] T. Koshy, *Catalan numbers with applications*. Oxford University Press, 2008.

[52] F. Qi and B.-N. Guo, "Integral representations of the catalan numbers and their applications," *Mathematics*, vol. 5, no. 3, p. 40, 2017.

[53] P. Flajolet and A. Odlyzko, "The average height of binary trees and other simple trees," *Journal of Computer and System Sciences*, vol. 25, no. 2, pp. 171–213, 1982.

[54] C. Ho Hong, J. Heo, J. G. Jang, and D. Kwon, "Quantum identity authentication with single photon," *Quantum Information Processing*, vol. 16, no. 10, p. 236, 2017.

[55] M. Curty and D. J. Santos, "Quantum authentication of classical messages," *Physical Review A*, vol. 64, no. 6, p. 062309, 2001.

[56] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *1984 International Conference on Computers, Systems & Signal Processing*, pp. 175–179, IEEE, 1984.

[57] H. E. Brandt, "Quantum-cryptographic entangling probe," *Physical Review A*, vol. 71, no. 4, p. 042312, 2005.

[58] J. H. Shapiro, "Performance analysis for brandts conclusive entangling probe," *Quantum Information Processing*, vol. 5, no. 1, pp. 11–24, 2006.

[59] "Sha-3 standard: Permutation-based hash and extendable-output functions," U.S. Department of Commerce, NIST Publication, 2014.

[60] H. Jacinto, L. Daoud, and N. Rafla, "High level synthesis using vivado hls for optimizations of sha-3," in *IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 563–566, IEEE, 2017.

[61] A. C.-C. Yao, "Some complexity questions related to distributive computing (preliminary report)," in *Proceedings of the eleventh annual ACM symposium on Theory of computing*, pp. 209–213, 1979.

[62] J.-L. Liu, R.-H. Shi, J.-J. Shi, G.-L. Lv, and Y. Guo, "Quantum dual signature scheme based on coherent states with entanglement swapping," *Chinese Physics B*, vol. 25, no. 8, p. 080306, 2016.

[63] L. Babai and P. G. Kimmel, "Randomized simultaneous messages: Solution of a problem of yao in communication complexity," in *Proceedings of Computational Complexity. Twelfth Annual IEEE Conference*, pp. 239–246, IEEE, 1997.

[64] D. Gottesman and I. Chuang, "Quantum digital signatures," *arXiv preprint quant-ph/0105032*, 2001.

[65] G. J. Milburn, "Quantum optical fredkin gate," *Physical Review Letters*, vol. 62, no. 18, p. 2124, 1989.

[66] J. C. Garcia-Escartin and P. Chamorro-Posada, "Swap test and hong-ou-mandel effect are equivalent," *Physical Review A*, vol. 87, no. 5, p. 052330, 2013.

[67] R. B. Patel, J. Ho, F. Ferreyrol, T. C. Ralph, and G. J. Pryde, "A quantum fredkin gate," *Science Advances*, vol. 2, no. 3, p. e1501531, 2016.

[68] L. Dong, Y.-F. Lin, J.-X. Wang, Q.-Y. Li, H.-Z. Shen, H.-K. Dong, Y.-P. Ren, X.-M. Xiu, Y.-J. Gao, and C. H. Oh, "Nearly deterministic fredkin gate based on weak cross-kerr nonlinearities," *Journal of the Optical Society of America B*, vol. 33, no. 2, pp. 253–260, 2016.

[69] E. Fredkin and T. Toffoli, "Conservative logic," *International Journal of Theoretical Physics*, vol. 21, no. 3-4, pp. 219–253, 1982.

[70] A. Ekert and P. L. Knight, "Entangled quantum systems and the schmidt decomposition," *American Journal of Physics*, vol. 63, no. 5, pp. 415–423, 1995.

[71] B. Sanders and G. Milburn, "Optimal quantum measurements for phase estimation," *Physical Review Letters*, vol. 75, no. 16, p. 2944, 1995.

[72] G. D'Ariano, C. Macchiavello, and M. Sacchi, "On the general problem of quantum phase estimation," *Physics Letters A*, vol. 248, no. 2-4, pp. 103–108, 1998.

[73] R. Demkowicz-Dobrzanski, U. Dorner, B. Smith, J. Lundeen, W. Wasilewski, K. Banaszek, and I. Walmsley, "Quantum phase estimation with lossy interferometers," *Physical Review A*, vol. 80, no. 1, p. 013825, 2009.

[74] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[75] C. Huang and Y. Shi, "Quantum hashing is maximally secure against classical leakage," *arXiv preprint arXiv:1701.01091*, 2017.

[76] J. C. Palais, *Fiber optic communications*. Prentice Hall Englewood Cliffs, 1988.

[77] B. Jalali and S. Fathpour, "Silicon photonics," *Journal of Lightwave Technology*, vol. 24, no. 12, pp. 4600–4615, 2006.

[78] D. A. Miller, "Silicon photonics: Meshing optics with applications," *Nature Photonics*, vol. 11, no. 7, p. 403, 2017.

[79] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Physical Review Letters*, vol. 73, no. 1, p. 58, 1994.

[80] W. R. Clements, P. C. Humphreys, B. J. Metcalf, W. S. Kolthammer, and I. A. Walmsley, "Optimal design for universal multiport interferometers," *Optica*, vol. 3, no. 12, pp. 1460–1465, 2016.

[81] B. Yurke, S. L. McCall, and J. R. Klauder, "Su (2) and su (1, 1) interferometers," *Physical Review A*, vol. 33, no. 6, p. 4033, 1986.

[82] R. Soref and B. Bennett, "Electrooptical effects in silicon," *Journal of Quantum Electronics*, vol. 23, no. 1, pp. 123–129, 1987.

[83] A. Hardy and W. Streifer, "Coupled mode theory of parallel waveguides," *Journal of Lightwave Technology*, vol. 3, no. 5, pp. 1135–1146, 1985.

[84] M. R. Paiam and R. I. MacDonald, "Design of phased-array wavelength division multiplexers using multimode interference couplers," *Applied Optics*, vol. 36, no. 21, pp. 5097–5108, 1997.

[85] G. Rudolph, "Parallel approaches to stochastic global optimization," in *Parallel Computing: From Theory to Sound Practice, Proceedings of the European Workshop on Parallel Computing*, pp. 256–267, Citeseer, 1960.

[86] R. B. Schnabel, "Parallel computing in optimization," in *Computational mathematical programming*, pp. 357–381, Springer, 1985.

[87] N. S. Lagali, M. R. Paiam, R. I. MacDonald, J. Worhoff, and A. Driessen, "Analysis of generalized Mach-Zehnder interferometers for variable-ratio power splitting and optimized switching," *Journal of Lightwave Technology*, vol. 17, no. 12, p. 2542, 1999.

[88] N. C. Harris, J. Carolan, D. Bunandar, M. Prabhu, M. Hochberg, T. Baehr-Jones, M. L. Fanto, A. M. Smith, C. C. Tison, P. M. Alsing, and D. Englund, "Linear programmable nanophotonic processors," *Optica*, vol. 5, no. 12, pp. 1623–1631, 2018.

[89] J. Carolan, C. Harrold, C. Sparrow, E. Martin-Lopez, N. J. Russell, J. W. Silverstone, P. J. Shadbolt, N. Matsuda, M. Oguma, M. Itoh, G. D. Marshall, M. G. Thompson, J. C. F. Matthews, T. Hashimoto, J. L. OBrien, and A. Laing, "Universal linear optics," *Science*, vol. 349, pp. 711–716, 2015.

[90] C. Cerf, ¿+N. J. amd Adami and P. G. Kwiat, "Optical simulation of quantum logic," *Physical Review A*, vol. A57, no. 1477, 1997.

[91] B. Bartlett and S. Fan, "Universal programmable photonic architecture for quantum information processing," *arXiv preprint arXiv:1910.10141*, 2019.

[92] S. C. Endres, C. Sandrock, and W. W. Focke, "A simplicial homology algorithm for lipschitz optimisation," *Journal of Global Optimization*, vol. 72, no. 2, pp. 181–217, 2018.

[93] A. Törn and S. Viitanen, "Topographical global optimization," *Recent Advances in Global Optimization*, pp. 384–398, 1992.

[94] I. A. Antonov and V. Saleev, "An economic method of computing lpτ-sequences," *USSR Computational Mathematics and Mathematical Physics*, vol. 19, no. 1, pp. 252–256, 1979.

[95] K. Sargsyan, C. Safta, K. S. Chowdhary, S. Castorena, S. De Bord, and B. Debusschere, "Uqtk version 3.0 user manual.," tech. rep., Sandia National Lab.(SNL-CA), Livermore, CA (United States), 2016.

[96] N. Henderson, M. de Sá Rêgo, and J. Imbiriba, "Topographical global initialization for finding all solutions of nonlinear systems with constraints," *Applied Numerical Mathematics*, vol. 112, pp. 155–166, 2017.

[97] W. F. Sacco, N. Henderson, and A. C. Rios-Coelho, "Topographical clearing differential evolution: A new method to solve multimodal optimization problems," *Progress in Nuclear Energy*, vol. 71, pp. 269–278, 2014.

[98] H. S. Jacinto, L. Daoud, and N. Rafla, "High level synthesis using vivado hls for optimizations of sha-3," in *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 563–566, IEEE, 2017.

[99] M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Transactions on Modeling and Computer Simulation*, vol. 8, no. 1, pp. 3–30, 1998.

[100] S. Vigna, "It is high time we let go of the mersenne twister," *arXiv preprint arXiv:1910.06437*, 2019.

[101] N. Killoran, J. Izaac, N. Quesada, V. Bergholm, M. Amy, and C. Weedbrook, "Strawberry fields: A software platform for photonic quantum computing," *Quantum*, vol. 3, p. 129, 2019.

[102] H. Abraham, I. Y. Akhalwaya, G. Aleksandrowicz, T. Alexander, G. Alexandrowics, E. Arbel, A. Asfaw, C. Azaustre, A. Ngoueya, P. Barkoutsos, *et al.*, "Qiskit: An open-source framework for quantum computing," 2019.

[103] J. Mower, N. C. Harris, G. R. Steinbrecher, Y. Lahini, and D. Englund, "High-fidelity quantum state evolution in imperfect photonic integrated circuits," *Physical Review A*, vol. 92, no. 3, p. 032322, 2015.

[104] N. C. Harris, Y. Ma, J. Mower, T. Baehr-Jones, D. Englund, M. Hochberg, and C. Galland, "Efficient, compact and low loss thermo-optic phase shifter in silicon," *Optics Express*, vol. 22, no. 9, pp. 10487–10493, 2014.

[105] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," 2000.

[106] N. D. Mermin, *Quantum computer science: an introduction*. Cambridge University Press, 2007.

[107] E. G. Rieffel and W. H. Polak, *Quantum computing: A gentle introduction*. MIT Press, 2011.

[108] C. E. Blair, "The baire category theorem implies the principle of dependent choices," *Bulletin L'Acadmie Polonaise des Science: Srie des Sciences Mathmatiques*, vol. 25, pp. 933–934, 1977.

Appendices

APPENDIX A

QUANTUM COMPUTING

Quantum computing is a relatively new area of computing which holds the potential of significant speedup over classical computers with regard to finding the solution of certain problems. However, the major disadvantage of quantum computers is their fundamental difference in operation versus a classical computer. Literature contains many textbooks which handle the basics of quantum computing, with [105] acting as a comprehensive reference about quantum computing, and [106] and [107] serving to show an accessible alternative for non-physicists. In this section, quantum computing will be viewed from the perspective of someone who does not have a physicist's understanding of quantum mechanics; beginning with basic assumptions and following with the intuitive examples and concepts in an easily conceptualized form.

A.1 Quantum Introduction

In general, a quantum computer is abstractly *similar* to a classical computer in that there is a state for the computer which evolves as each operation takes place. In this work the *state* of the quantum computer is contained in a quantum register, initialized in some predefined way for the desired operation. The state then evolves according to the *operations* which are specified in advance according to the algorithm

necessary for computation. At the finale of computation, information from the state register is obtained through an operation called *measurement*. The measurement, however, must be completed with data stored once computation is finished or else the information produced will be lost due to quantum mechanical effects.

First we must define several key notations to quantum computing:

- *Tensor Product Space* – Given two vector spaces, V and W, over field K with bases $\{e_1, \ldots, e_m\}$ and $\{f_1, \ldots, f_m\}$ respectively, the tensor product, $V \otimes W$, produces another vector space over K of dimension mn. For quantum computing, there is a bi-linear operation in the tensor product space $\otimes : V \times W \to V \otimes W$. The vector space formed by $V \otimes W$ has a basis $e_i \otimes f_j \forall i = \{1, \ldots, m\}, j = \{1, \ldots, m\}$. If the origin vector spaces are complex Hilbert spaces, $\mathbb{H}$, of a type $\mathbb{C}^n$, and a standard basis is chosen where orthonormal vectors have a value of 1 in a single position, 0 elsewhere in the origin vector spaces, then the tensor product is known as the Kronecker product. The Kronecker product in this context is then a generalization of the outer product.

- *Kronecker Product* – To define the Kronecker product, we can consider all operation in this work taking place in the complex Hilbert spaces, $\mathbb{H}$, of form $\mathbb{C}^n$, by using the standard basis. In a loosely defined way, the tensor product can refer to the Kronecker and outer products. Given $A \in \mathbb{C}^{m \times n}, B \in \mathbb{C}^{p \times q}$, the Kronecker product, $A \otimes B$ is the matrix $\mathbb{C}^{mp \times nq}$ defined as:

$$D := A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ a_{21}B & \dots & a_{2n}B \\ \vdots & & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}.$$

If a standard basis is chosen over vector spaces $\mathbb{C}^{m\times n}$ and $\mathbb{C}^{p\times q}$, then the bi-linear operation $\otimes$ of the tensor product $\mathbb{C}^{m\times n}\otimes\mathbb{C}^{p\times q}$ is simply the Kronecker product.

There are fairly broad definitions which the tensor product must satisfy, which are outside of the scope of this work. Other important notations are where A^* is used to denote a conjugate transpose of A, but when given a matrix A, the notation $A^{\otimes n}$ will be used to indicate a tensor product of A with itself n times. The same notation will be used for Hilbert spaces, shown as:

$$\underbrace{A^{\otimes n} := A \otimes A \cdots \otimes A}_{\text{n times}}, \qquad \underbrace{\mathbb{H}^{\otimes n} := \mathbb{H} \otimes \mathbb{H} \cdots \otimes \mathbb{H}}_{\text{n times}}.$$

A.2 Bra-Ket Notation

The final part of notation necessary to understand quantum computing is known as *bra-ket* notation, from quantum mechanics. Given a Hilbert space $\mathbb{H} \equiv \mathbb{C}^n$, a quantity $\psi \in \mathbb{H}$ enclosed in a ket, denoted by $|\psi\rangle$, is a vector which can be envisioned as a classical column vector. A similar quantity, $\phi \in \mathbb{H}^*$, enclosed in a bra is denoted by $\langle\phi|$. The value $\langle\phi|$ represents a vector in the dual space; thought of as a row vector that is the conjugate transpose of $\phi \in \mathbb{H}$. Thus, a resulting expression, $\langle\phi|\psi\rangle$, represents an inner product within the Hilbert space. For this work, the Hilbert spaces will be of the form $(\mathbb{C}^2)^{\otimes q}$, where q is any given integer. Therefore, the basis

elements of the Hilbert spaces must be defined.

The standard basis for $\mathbb{C}^2$ is denoted by:

$$|0\rangle_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} , \qquad \text{and} \qquad |1\rangle_1 = \begin{pmatrix} 0 \\ 1 \end{pmatrix} .$$

A larger standard basis for $(\mathbb{C}^2)^{\otimes q}$, which has q elements is denoted by:

$$|0\rangle_q , |1\rangle_q , \ldots , |2^q - 1\rangle_q .$$

To formally define ket notation for basis vectors, we can abstract without loss of generality by saying that for any q-digit binary string, $x \in \{0,1\}^q, |x\rangle$ is the 2^q-dimensional basis vector in $(\mathbb{C}^2)^{\otimes q}$ which corresponds to the binary string. For example, a 2^q-dimensional basis vector with 1 in position $\sum_{j=0}^{q-1} 2^{q-j-1} x_j$, and 0 elsewhere could be represented by a toy example where $|101\rangle$ is the 8-dimensional basis vector $(00000010)^\intercal$. However, if x is any integer $\leq 2^q - 1$, $|x\rangle_q$ represents the 2^q-dimensional basis vector $|xB_q\rangle \in (\mathbb{C}^2)^{\otimes q}$, or simply, the basis vector in which x is expressed as a binary string on q digits. To simplify notation though, $|x\rangle_q$ is used to note a basis state. For example, $|6\rangle_3 = |101\rangle$ is the 8-dimensional basis vector $(00000010)^\intercal$. Be sure to take note that according to notation, $|0\rangle = |0\rangle_1$ and $|1\rangle = |1\rangle_1$ since sub-scripting a basis state is unnecessary for basis vectors in $\mathbb{C}^2$.

An example for the basis elements of $(\mathbb{C}^2)^{\otimes 2} = \mathbb{C}^2 \otimes \mathbb{C}^2$ can be represented as:

$$|0\rangle_2 = |0\rangle \otimes |0\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |1\rangle_2 = |0\rangle \otimes |1\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|2\rangle_2 = |1\rangle \otimes |0\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \qquad |3\rangle_2 = |1\rangle \otimes |1\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

The index then of a standard basis for $(\mathbb{C}^2)^{\otimes q}$ composed of basis elements corresponding to a tensor product of basis elements of $\mathbb{C}^2$ can be simply noted by the decimal number, which corresponds to a binary string obtained by concatenating the indices of the basis elements of $\mathbb{C}^2$.

A.3 Quantum State and Qubits

By the model developed in this work, a quantum computing device has a state which is stored in a quantum register. Qubits represent the quantum counterpart to a bit found in a classical computer, with the key difference being that a classical computer has registers made of bits versus a quantum computer's usage of a single quantum register composed of qubits. The state of the quantum register, therefore the quantum computer, can be described from the assumption that the state of q-many qubits can be represented as a unitary vector in $(\mathbb{C}^2)^{\otimes q} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. If a standard basis for $\mathbb{C}^2$ is chosen, then a single qubit ($q = 1$) can be represented as:

$$\alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \text{where} \quad \alpha, \beta \in \mathbb{C} \quad \text{and} \quad |\alpha|^2 + |\beta|^2 = 1\,.$$

Following, then if a standard basis is given for each $\mathbb{C}^2$, a basis for $\left(\mathbb{C}^2\right)^{\otimes q}$ is given by:

$$\begin{aligned}
|0\rangle_q &= \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle \otimes |0\rangle}_{\text{q times}} = |0B_q\rangle \\
|1\rangle_q &= \underbrace{|0\rangle \otimes \cdots \otimes |0\rangle \otimes |1\rangle}_{\text{q times}} = |1B_q\rangle \\
&\vdots \\
|2^q - 1\rangle_q &= \underbrace{|1\rangle \otimes \cdots \otimes |1\rangle \otimes |1\rangle}_{\text{q times}} = |(2^q - 1)B_q\rangle\ .
\end{aligned}$$

In general, the state of the qubits can be described by:

$$|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j\,|j\rangle_q \quad \text{where} \quad \alpha_j \in \mathbb{C} \quad \text{and} \quad \sum_{j=0}^{2^q-1} |\alpha_j|^2 = 1\,.$$

It is important to keep in mind that $\left(\mathbb{C}^2\right)^{\otimes q}$ is a 2^q-dimensional space; a sharp contrast with the state of classical bits. For classical bit states, given q-many bits, the state is a binary string in the field $\{0,1\}^q$, which is a q-dimensional space. The major difference in dimensionality is that the dimension of the state space of the quantum register grows *exponentially* by the number of qubits, whereas the dimensionality of the state space for a classical register would grow linearly by the number of bits. In addition, the representation of a quantum state needs complex coefficients since a q-many qubit quantum register will 'store' 2^q complex coefficients: An enormous amount of information compared to what can be stored in a classical q-bit classical

register. However, the quantum state is not able to be accessed directly, thus even if the quantum state contains much information, access is not as easy as with a classical register.

A.3.1 Superposition

If both $|x\rangle$ and $|y\rangle$ are in a basis state, either α_0 or α_1 is zero, where, similarly, either β_0 or β_1 is zero while the non-zero coefficients have a modulus of one. We can say that q-many qubits are in a basis state if their state $|\phi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle_q$ is such that for every k: $|\alpha_k| = 1$, $\alpha_j = 0$, $\forall j \neq k$. Otherwise, the qubits are in a *superposition*. Thus, only one of the coefficients in the expression of the state of $|x\rangle \otimes |y\rangle$ is non-zero; in fact the modulus is one, so all other coefficients are zero. It follows that if both $|x\rangle$ and $|y\rangle$ are in a basis state, $|x\rangle \otimes |y\rangle$ represents a basis state as well.

For example, consider two qubits:

$$|x\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$
$$|y\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle \ .$$

The two qubits taken together as a whole will be in state:

$$|x\rangle \otimes |y\rangle = \alpha_0\beta_0 |0\rangle \otimes |0\rangle + \alpha_0\beta_1 |0\rangle \otimes |1\rangle + \alpha_1\beta_0 |1\rangle \otimes |0\rangle + \alpha_1\beta_1 |1\rangle \otimes |1\rangle \ .$$

Now, if we assume that $\alpha_0 = \beta_0 = \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}}$, the qubits $|x\rangle$ and $|y\rangle$ are in a superposition. Following the previous information, the state of $|x\rangle \otimes |y\rangle$ is also in a superposition with a value of:

$$|x\rangle \otimes |y\rangle = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right)$$
$$= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \ .$$

The normalization of coefficients computes correctly, since the tensor product of unitary vectors is unitary. The shown example relates a generalization to an arbitrary number of qubits where for any q, q-many qubits are in a basis state if and only if each of the individual qubits is in a basis state. The realization of multiple basis has no counterpart in classical computing since any q-many classical bits will always be in a basis state since the q-many bits will always correspond to exactly one of the 2^q binary strings possible. Superposition then is a main differentiating feature of quantum computers versus classical computers; the second is the concept of entanglement.

A.3.2 Entanglement

The state of q-many qubits can be represented as a vector in $\left(\mathbb{C}^2\right)^{\otimes q}$, a 2^q-dimensional space. Since the space in which a single qubit exists, a tensor product of $\mathbb{C}^2$, an unanswered question is whether or not moving from the usage of single qubits to multiple qubits brings any inherent gain. To clarify, the question would be whether or not the quantum states which are able to be represented by q-many qubits are simply the tensor product of q-many single qubits. By utilizing prior notation, the state of q-many qubits is a unitary vector in $\left(\mathbb{C}^2\right)^{\otimes q}$, which can be alternately represented as:

$$|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_j |j\rangle_q \ , \quad \sum_{j=0}^{2^q-1} |\alpha_j|^2 = 1 \, .$$

If we consider the tensor product of q-many qubits, the j^{th} of which would be in state $\beta_{j,0}\,|0\rangle + \beta_{j,1}\,|1\rangle$. After taking the tensor product, we obtain the vector:

$$\begin{aligned}|\phi\rangle &= \sum_{j_{q-1}=0}^{1}\sum_{j_{q-2}=0}^{1}\cdots\sum_{j_0=1}^{1}\prod_{k=0}^{q-1}\beta_{k,j_k}\,|j_q j_{q-1}\ldots j_0\rangle \\ &= \sum_{j=0}^{2^q-1}\prod_{k=1}^{q}\beta_{k,(jB_q)_k}\,|jB_q\rangle\,, \quad |\beta_{j,0}|^2 + |\beta_{j,1}|^2 = 1,\ \forall j = 1,\ldots,q\,.\end{aligned}$$

The normalization condition for $|\phi\rangle$ implies:

$$\sum_{j_{q-1}=0}^{1}\sum_{j_{q-2}=0}^{1}\cdots\sum_{j_0=1}^{1}\prod_{k=0}^{q-1}|\beta_{k,j_k}|^2 = 1\,,$$

which is more restrictive that that for $|\psi\rangle$. More plainly, there are values for α_j with:

$$\sum_{j=0}^{2^q-1}|\alpha_j|^2 = 1$$

which cannot be expressed as any coefficient which similarly satisfies the conditions for $|\phi\rangle$.

A.3.3 Entanglement Example

As an example, we can consider two distinct qubits, or two single-qubit states:

$$\begin{aligned}|x\rangle &= \alpha_0\,|0\rangle + \alpha_1\,|1\rangle \\ |y\rangle &= \beta_0\,|0\rangle + \beta_1\,|1\rangle\ .\end{aligned}$$

The two individual qubit states can be taken together by the tensor product, resulting in:

$$|x\rangle \otimes |y\rangle = \alpha_0\beta_0 |00\rangle + \alpha_0\beta_1 |01\rangle + \alpha_1\beta_0 |10\rangle + \alpha_1\beta_1 |11\rangle \ , \tag{A.1}$$

with the normalization conditions of $|\alpha_0|^2 + |\alpha_1|^2 = 1$ and $|\beta_0|^2 + |\beta_1|^2 = 1$. The general state of the quantum two-qubit register $|\psi\rangle$ is:

$$|\psi\rangle = \gamma_{00} |00\rangle + \gamma_{01} |01\rangle + \gamma_{10} |10\rangle + \gamma_{11} |11\rangle \ , \tag{A.2}$$

with a qubit normalization condition of $|\gamma_{00}|^2+|\gamma_{01}|^2+|\gamma_{10}|^2+|\gamma_{11}|^2 = 1$. By comparing Equation A.1 with Equation A.2, it is easily determined that $|\psi\rangle$ is of the form $|x\rangle\otimes|y\rangle$ if and only if it satisfies the relationship:

$$\gamma_{00}\gamma_{11} = \gamma_{01}\gamma_{10} \, . \tag{A.3}$$

At this point it is clear that $|x\rangle \otimes |y\rangle$ will yield coefficients which satisfy the condition set by Equation A.3. To see a mathematically strong converse, let $\theta_{00}, \theta_{01}, \theta_{10}$, and θ_{11} represent the phases of $\gamma_{00}, \gamma_{01}, \gamma_{10}$, and γ_{11}, respectively. By this relation, and by Equation A.3, this implies that:

$$|\gamma_{00}|^2|\gamma_{11}|^2 = |\gamma_{01}|^2|\gamma_{10}|^2$$
$$\theta_{00} + \theta_{11} = \theta_{01} + \theta_{10} \, .$$

We can then rewrite the coefficients as:

$$
\begin{aligned}
|\gamma_{00}| = \sqrt{|\gamma_{00}|^2} &= \sqrt{|\gamma_{00}|^2 \underbrace{\left(|\gamma_{00}|^2 + |\gamma_{01}|^2 + |\gamma_{10}|^2 + |\gamma_{11}|^2\right)}_{\text{normalization condition} = 1}} \\
&= \sqrt{|\gamma_{00}|^4 + |\gamma_{00}|^2|\gamma_{01}|^2 + |\gamma_{00}|^2|\gamma_{10}|^2 + |\gamma_{01}|^2|\gamma_{10}|^2} \\
&= \underbrace{\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}}_{|\alpha_0|} \underbrace{\sqrt{|\gamma_{00}|^2 + |\gamma_{10}|^2}}_{|\beta_0|},
\end{aligned}
$$

which with other coefficients written similarly:

$$
\begin{aligned}
|\gamma_{01}| &= \underbrace{\sqrt{|\gamma_{00}|^2 + |\gamma_{01}|^2}}_{|\alpha_0|} \underbrace{\sqrt{|\gamma_{01}|^2 + |\gamma_{11}|^2}}_{|\beta_1|} \\
|\gamma_{10}| &= \underbrace{\sqrt{|\gamma_{10}|^2 + |\gamma_{11}|^2}}_{|\alpha_1|} \underbrace{\sqrt{|\gamma_{00}|^2 + |\gamma_{10}|^2}}_{|\beta_0|} \\
|\gamma_{11}| &= \underbrace{\sqrt{|\gamma_{10}|^2 + |\gamma_{11}|^2}}_{|\alpha_1|} \underbrace{\sqrt{|\gamma_{01}|^2 + |\gamma_{11}|^2}}_{|\beta_1|}.
\end{aligned}
$$

To finish fully defining the coefficients $\alpha_0, \alpha_1, \beta_0$, and β_1, their phases must be determined. It is easy to assign:

$$
\alpha_0 = e^{i\theta_{00}}|\alpha_0|, \quad \alpha_1 = e^{i\theta_{10}}|\alpha_1|, \quad \beta_0 = |\beta_0|, \quad \beta_1 = e^{i(\theta_{01}-\theta_{00})}|\beta_1|\,. \tag{A.4}
$$

It can be finalized by verification that the state $|\psi\rangle$ in Equation A.2 can be expressed as $|x\rangle \otimes |y\rangle$ in Equation A.1 with the coefficients $\alpha_0, \alpha_1, \beta_0$, and β_1 as given in Equation A.4.

A.3.4 Quantum State Decomposition

The concept of expressing quantum state(s) as a tensor product composed of lower-dimensional quantum states can be described by its decomposed variant. Given

a quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q}$ *is* able to be decomposed if it can be expressed as a tensor product, $|\psi_1\rangle \otimes \cdots \otimes |\psi_k\rangle$ of $k > 2$ quantum states on $(q_1, \ldots, q_k)$ qubits, respectively, with the property that $(q_1 + \ldots + q_k) = q$. The general quantum state $|\psi\rangle$ could be the resulting product of two or more higher-dimensional quantum states, e.g. $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, with $|\psi\rangle_1$ and $|\psi_2\rangle$ being entangled states. In this case, a quantum state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes q}$ is a product state if it can be decomposed into the tensor product of q-many single-qubit quantum states; otherwise it is entangled. In such a situation, $|\psi\rangle$ will still show some entanglement but can be theoretically 'simplified'. By the fact of minor entanglement, a quantum state can be called entangled as long as the state is unable to be fully decomposed.

For example, we can consider the following two-qubit state:

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \ .$$

The state represented is a product state since it is equal to:

$$\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right).$$

Where, by contrast, the following state:

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

is an entangled state since it cannot be expressed as a product of two single-qubit states.

APPENDIX B

CONSTRUCTION OF A QUANTUM HASH FUNCTION BY MODIFYING THE ONE-DIMENSIONAL TWO-PARTICLE DISCRETE-TIME QW ON A CIRCLE

Y. Yang et al. introduce two coin operators [24], the Grover operator $\hat{C}_0^{16}$ and the coin operator $\hat{C}_1^{17}$, in Equation B.1 and Equation B.2, respectively.

$$\hat{C}_0 = \frac{1}{2}\begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix} \tag{B.1}$$

$$\hat{C}_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix} \tag{B.2}$$

B.1 Description of QW Restriction

Taking the construction of a quantum hash function by by D. Li et al. in [26] and expanded by Y. Yang et al. in [24], a one-dimensional two-particle discrete-time

QW on a circle will effectively describe the QW of two walkers whose motions are restricted to a circle. The operators $\hat{S}_1$ and $\hat{S}_2$ of a two-particle QW become:

$$\hat{S}_1 = \begin{cases} |2,0\rangle\langle 1,0| + |n,1\rangle\langle 1,1|\,, & \text{when} \quad x = 1; \\ |1,0\rangle\langle n,0| + |n-1,1\rangle\langle n,1|\,, & \text{when} \quad x = n; \\ |x+1,0\rangle\langle x,0| + |x-1,1\rangle\langle x,1|\,, & \text{when} \quad x \neq 1,n\,. \end{cases} \tag{B.3}$$

It is noted that $\hat{S}_2$ will be similar to $\hat{S}_1$, where the total conditional shift operator $\hat{S}$ is equivalent to $\hat{S} = \hat{S}_1 \otimes \hat{S}_2$. However, when the i-th bit of the message is 0(1), the i-th step of the walk will execute with interaction $\hat{C}_0(\hat{C}_1)$.

B.2 QW Example and State

Example: Given a binary message m = "0 1 0 0 1 1 0", then a final state will evolve to:

$$|\psi\rangle_7 = \hat{U}_0\hat{U}_1\hat{U}_0\hat{U}_0\hat{U}_1\hat{U}_1\hat{U}_0\,|\psi\rangle_0\ , \tag{B.4}$$

where $\hat{U}_0 = \hat{S}\big(\hat{I}\otimes\hat{C}_0\big)$ and $\hat{U}_1 = \hat{S}\big(\hat{I}\otimes\hat{C}_1\big)$. The initial state of the quantum system, $|\psi\rangle_0$ is thus given by:

$$|\psi\rangle_0 = |x,y\rangle \otimes |v_1,v_2\rangle\ . \tag{B.5}$$

Here,

$$|v_1,v_2\rangle = (\alpha\,|00\rangle + \beta\,|01\rangle + \chi\,|10\rangle + \delta\,|11\rangle)\,, \tag{B.6}$$

where $|\alpha|^2 + |\beta|^2 + |\chi|^2 + |\delta|^2 = 1\,.$

APPENDIX C

THE UNIFORM BOUNDEDNESS PRINCIPLE

Let X and Y be Banach spaces, described in Appendix D, and let T_α be a family of bounded linear maps from X into Y. Suppose that the sequence $T_n \in B(X,Y)$ of bounded linear operators has the property that for every $x \in X$, the sequence $T_n(x) \in Y$ is bounded. Then, the sequence of norms $||T_n||$ will be bounded. If we define a larger set: $M_k = \{x \in X : ||T_n(x)|| \leq k \,\forall\, n\}\,, \quad k \geq 1\,.$

Since the T_n's are continuous, the sets are closed, and since for every $x \in X$ the sequence $T_n(x)$ is bounded, we have $x \in M_k$ for a sufficiently large k. Thus

$$X = \bigcup_{k\geq 1} M_k\,.$$

By Baire's category theorem [108], there is a guarantee that one of the closed sets contains an open ball, for example $B(x_0, r) \subset M_{k_0}$. Thus we have

$$||T_n(x)|| \leq k_0 \quad \text{for any} \quad x \in B(x_0, r) \quad \text{and} \quad n \geq 1\,.$$

Letting $x \in X$, $x \neq 0$, then a vector $z = x_0 + \frac{r}{2||x||}x$ belongs to $B(x_0, r)$ and $x = \frac{2||x||}{r}(z - x_0)$. It can thus be calculated that $||T_n|| \leq \frac{4k_0}{r}\,\forall\, n \in \mathbb{N}$.

APPENDIX D

DEFINITION OF BANACH SPACE

A Banach space is a vector space X over field $\mathbb{R}$ or $\mathbb{C}$ that is equipped with a norm and is complete w.r.t. the distance function indiced by the norm. Thus, for all Cauchy sequences $x_n \in X \; \exists \; x \in X$ such that:

$$\lim_{n\to\infty} x_n = x \,, \tag{D.1}$$

or equivalently:

$$\lim_{n\to\infty} ||x_n - x||_X = 0 \,. \tag{D.2}$$

Since the vector space structure allows one to relate directly to Cauchy sequences, a normed space X is a Banach space **iff** each absolutely convergent series in X converges,

$$\sum_{n=1}^{\infty} ||v_n||_X < \infty \quad \text{implies that} \quad \sum_{n=1}^{\infty} v_n \quad \text{converges in} \quad X \,. \tag{D.3}$$

The completeness of a normed space is preserved if the given norm is replaced by an equivalent one, where all norms on a finite dimensional vector space are equivalent. Every finite dimensional normed space over $\mathbb{R}$ or $\mathbb{C}$ is a Banach space.

APPENDIX E

QIA PROTOCOLS BETWEEN TWO PARTIES

Protocol E.1 QIA Protocol Between Two Parties (Original)

Inputs. Pre-established secret key Sk_n.

Goal. Two parties successfully authenticate each others identity.

The protocol:

1. **Setup.**
   (a) Both parties set individual counters to $n = 0$.
   (b) If $n > Sk_n$, authentication is successful, else proceed.
   (c) Alice randomly selects either message or control mode.
2. **Message Mode.**
   (a) Alice takes the shared secret Sk_i and constructs a quantum state according to Table 3.1.
   (b) Alice sends her constructed state to Bob.
   (c) Bob receives the incoming state and measures. He selects the measurement basis using bit k_n of his *own* copy of the shared secret. Bob's measurement outcome will be k'_{n+1}.

(d) Bob publicly announces the reception of the state. Alice then communicates back that they are operating in the 'message' mode.

(e) Bob then compares his received value versus the expected value for the bit. If $k'_{n+1} = k_{n+1}$, the protocol will proceed; waiting to confirm the cycle's success to Alice, $n = n + 2$, then proceed to step 1.b, otherwise abort the protocol.

3. **Control Mode.**

(a) Alice creates the pair (k_n, r), for a random bit r. Then on the agreed basis Alice constructs a state according to Table 3.1.

(b) Alice sends her constructed state to Bob.

(c) Bob receives the incoming state and measures. He selects the measurement basis using bit k_n of his *own* copy of the shared secret. Bob's measurement outcome will be r'.

(d) Bob publicly announces the reception of the state. Alice then communicates back that they are operating in the 'control' mode *and* the value of r.

(e) Bob then compares his received value versus the expected value for the bit. If $r' = r$, the protocol will proceed; waiting to confirm the cycle's success to Alice, $n = n+2$, then proceed to step 1.b, otherwise abort the protocol.