A public key cryptosystem based on quantum stabilizer codes

Lubjana Beshaj[1], Travis Russell[2,*]

[1]Army Cyber Institute, United States Military Academy
[2]Department of Mathematics, Dartmouth College

Received: 15th June 2022 | Accepted: 15th July 2022

Abstract *We introduce a public key cryptosystem for the transmission of classical data using quantum information. In the protocol, a public key and a private key are chosen corresponding to stabilizer groups, i.e. commutative subgroups of the n-qubit Pauli group not containing the negative identity operator. A quantum state called the "tableau" is prepared by the receiver as a stabilizer state for the private key. The tableau is sent to the sender, who encodes the message by passing the state through a quantum circuit. The encoded state is returned to the receiver who decodes the message by performing a quantum measurement. We study the security properties of this protocol, proving that it is secure against brute force attacks. We also analyze a potential letter frequency attack, showing that such an attack is successful if the receiver reuses the private key too much, and can be thwarted by simply varying the choice of private key.*

Keywords: Quantum Cryptography, Public Key Cryptography, Stabilizer Codes
2010 Mathematics Subject Classification: 68Q12, 81P94, 81P68

1 INTRODUCTION

Cryptography is the art of concealing messages. As soon as people started sending each other messages that were not intended for the public, the need for privacy arose. In the standard cryptography literature, the sender of the message and the receiver are named Alice and Bob. We assume that they are communicating with one another over an insecure channel. In classical cryptography there are two type of cryptography protocols, private key cryptography and public key cryptography. In private key cryptosystems the sender and the receiver use the same key to encrypt and decrypt the message. It is in principle very secure but it requires the sender and the receiver to have a way of exchanging the key without being intercepted by a spy. Moreover, the key must be changed regularly since a set of messages encoded with the same key reveal regularities making it easy to decipher the message. The transmission of the secret key is an expensive and slow process, and for these reasons it is now preferred to use public key cryptography. In these systems there are two keys one which is made public and one which is kept private. The knowledge of one key does not enable us to calculate the second key. To be precise, the requirement is that the computation of the second key from the first should be hard.

The development of public key methods revolutionized cryptography. Before, both parties had to have a private key, which required a completely secure channel in order to exchange it. Imagine if you personally had to have a secure line to every website you wished to make online purchases from so that you could exchange your private keys. This method was suitable when the internet was very small, but at this time it would be nearly impossible to manage. When two individuals want to secretly communicate on a public, insecure network, without privately meeting they must resort to public key cryptography.

However, advances in mathematics, high performance computing, as well as the possibility of building a large scale quantum computing pose a threat to classical cryptography. Companies and governments around the world are in a quantum arms race, the race to build the first usable quantum computer. The technology promises to make some kinds of computing problems much, much easier to solve than with today's classical computers. One of those problems is breaking certain types of encryption. Shor in his paper [8] gives an algorithm showing how a quantum computer can be used to factor a positive odd integer, not a prime power, and to solve the discrete log problem (which is the underlying problem on which the majority of public key cryptosystems are based on). Compared to classical computers, quantum algorithms are exponentially faster than any other known method at solving such problems.

Hence, with the advent of quantum computing, an adversary can efficiently break universally adopted public-key cryptographic schemes (e.g. RSA, DSA and elliptic-curve cryptography). In order to mitigate this imminent threat, cryptographic schemes that are resistant against quantum computers have drawn great attention from academia

*Corresponding Author: travis.b.russell@dartmouth.edu

and industry. These schemes are collectively referred to as post-quantum cryptography (PQC). These types of cryptosystems will be implemented in classical computers. For more details on PQC look at the National Institute of Standards and Technology webpage on PQC [7].

Above we pointed out that the problem of securely transmitting the key in symmetric key cryptography is a serious one. In the 1980's two researchers came up with the clever idea to exploit quantum mechanics. This idea formed the basis of the first quantum key exchange protocol. Charles Bennett and Gilles Brassard in 1984 introduced the first quantum key exchange protocol, BB84 (see [1]). As of now there is no encryption of a message using quantum physics. Quantum key distribution (QKD) is used to ensure that the transmission of a key is not intercepted by an eavesdroper.

Unlike traditional cryptography, which is based on mathematics, quantum cryptography is based on the laws of quantum mechanics. When we send qubits rather than bits over some channel the following are true. First, Eve cannot make perfect copies of qubit stream: the no-cloning theorem prevents this from happening. Hence, the no-cloning theorem hampers Eve's ability to use past messages to conduct her analysis. Second, the very act of measuring the qubit stream alters it. Hence, each time Eve measures the qubit stream, she disturbs it, allowing Alice and Bob to detect her presence along the channel.

In this paper we propose a public-key cryptosystem based on stabilizer codes, quantum error correction codes introduced by Shor in [9] and studied extensively by Gottesman in [5]. Stabilizer codes are defined as subspaces of the n-qubit Hilbert space stabilized by a stabilizer group, a commutative subgroup of the n-qubit Pauli group not containing the negative multiple of the identity operator. Stabilizer codes are convenient classes of vectors to consider, since the stabilizer groups from which they are derived are in one-to-one correspondence with certain rectangular matrices of $\mathbb{Z}_2$ called *check matrices*. By representing stabilizer codes using vectors and matrices over $\mathbb{Z}_2$, it is possible to simplify the analysis of the behavior a stabilizer state when acted upon by unitaries in the n-qubit stabilizer group, or projections onto other stabilizer codes. We rely on this simplified analysis prove our main results.

Our protocol is described as follows. Initially, a public key is published as a rectangular matrix H over $\mathbb{Z}_2$. The matrix H corresponds to a stabilizer group, which the sender can use to construct a quantum circuit for encoding an n-bit message into an n-qubit state. The circuit requires as input a state selected from the stabilizer code of another stabilizer group, which is known only to the receiver (the secret key). The receiver prepares such a state, called the "tableau", and sends the state to the sender. The sender passes the tableau through the circuit and returns the encoded state to the receiver. Finally, the receiver decodes the message by performing a quantum measurement based on the stabilizer group which was used to prepare the state. We prove that the protocol successfully encodes and decodes messages. We then analyze the key space, characterizing the set of possible secret keys which may be used to encode the initial state used in the protocol. Using our analysis of the key space, we consider senarios where an eavesdropper randomly samples the key space to decode an encoded state or a sequence of encoded states. We show that this kind of brute force sampling gives the eavesdropper no valuable information if a single encoded state is captured. However, if the receiver reuses the secret key many times, the eavesdropper may be able to converge on a suitable key using a modified "letter-frequency" attack. This scenario can be avoided by having he receiver randomly vary the secret key at each transmission.

Our protocol is unconventional compared to other public-key cryptosystems in several ways. First, it uses quantum infrastructure to encode classical messages. This is most similar to the "superdense coding" protocol introduced in [2]. In superdense coding, the sender and receiver share a pair of entangled qubits. The sender encodes her qubit using a quantum circuit, then returns the qubit to the receiver who decodes the message using a quantum measurement. The protocol is known to be secure provided that an eavesdropper has access only to one of the two qubits. Generalizations of the protocol to multiple qubits exist (see [4]). Our protocol differs in that we do not require the sender and receiver to share entangled pairs of particles, potentially reducing the amount resources required to carry out the protocol. Another similar quantum cryptosystem is "quantum McEliece", developed by Fujita in [3]. Fujita's quantum McEliece also uses a stabilizer group as a public key, but requires no private key. The sender transmits a quantum state with added noise encoded using the public key, and the message is decrypted using a stabilizer code known to the receiver. The security of this system relies on the computational difficulty of deriving the stabilizer code from the secret key. Our protocol differs in that the private key is not unique and hence cannot be derived from the public key regardless of the the computational capabilities of an eavesdropper. Second, while our protocol relies on public and private keys, it is not fully asymmetric as is the case for must public key cryptosystems. In other public key systems, the sender encodes the message using only the public key, then sends the message to the receiver to decrypt using the secret key. Our protocol requires the receiver to first prepare the "tableau" state and send it to the receiver to be used for encoding. This feature has positive and negative qualities. On the one hand, it introduces the possibility of leakage, as an eavesdropper may be able to capture the tableau and attempt to divine the secret key from it through measurement. This problem is partly alleviated by the no-cloning theorem, which prevents an eavesdropper from making exact copies of quantum states. The situation should also

be helped by having the receiver randomly vary the choice of secret key for each transmission.

The outline of the paper is as follows. First, in Section 2, we go over some preliminaries on asymmetric crytography, quantum mechanics, and stabilizer formalism. For further background on these topics, we refer the interested reader to the textbook [6]. In Section 3, we describe our protocol formally and prove that encryption and decryption can be performed successfully. Then, in Section 4, we study the set of possible secret keys which can be paired with a given public key. In Section 5, we consider several types of attacks and study the security of the protocol. We also identify other potential weak points in our protocol and consider several avenues for future work. Finally, we conclude with Section 6 where we detail potential future avenues of study.

2 PRELIMINARIES

Throughout the paper, let $\mathbb{N}$ denote the set of integers and let $\mathbb{C}$ denote the set of complex numbers. Given any field $\mathbb{F}$ and integer $n \in \mathbb{N}$, let $\mathbb{F}^n$ denote the n-dimensional vector space of $n \times 1$ column matrices with entries in $\mathbb{F}$, and for $m \in \mathbb{N}$ we let $M_{n,m}(\mathbb{F})$ denote the vector space of $n \times m$ matrices with entries in $\mathbb{F}$. Also let $M_n(\mathbb{F})$ represent the matrix algebra $M_{n,n}(\mathbb{F})$ for brevity. For each $n \in \mathbb{N}$, let $\mathbb{Z}_n$ denote the cyclic ring $\{0, 1, \ldots, n-1\}$.

For each complex number λ, let $\overline{\lambda}$ denote its complex conjugate. We regard the vector space $\mathbb{C}^n$ as an n-dimensional Hilbert space with respect to the inner product defined by

$$\langle x, y \rangle = \sum_i \overline{x_i} y_i$$

for $x = (x_i), y = (y_i) \in \mathbb{C}^n$. Linear operators on $\mathbb{C}^n$ correspond to matrices $A = (a_{ij}) \in M_n(\mathbb{C})$, where $a_{ij} = \langle e_i, Ae_j \rangle$, and $\{e_1, \ldots, e_n\}$ denotes the canonical orthonormal basis for $\mathbb{C}^n$. For each $A \in M_n$, let $A^\dagger$ denote the adjoint matrix given by $A^\dagger = (\overline{a_{ji}})_{ij}$, i.e. $A^\dagger$ is the conjugate transpose of A. Let I denote the identity matrix.

2.1 PUBLIC KEY CRYPTOGRAPHY

In this subsection we will give a brief overview of public key cryptography since we will use this idea in our proposed protocol. In this type of cryptographic system we use pairs of keys. Each pair consists of a public key and a private key. The generation of such pairs is based on mathematical functions called one-way-functions, which are functions that are computationally easy to evaluate but computationally difficult to invert. To get a better understanding of how this works precisely we will go over the details of Diffie-Hellman key exchange.

The Diffie-Hellman key exchange algorithm was first published in 1976 and is the first practical key exchange protocol. In the Diffie-Hellman protocol, the communicators must carefully select the information that they send over the channel so that eavesdroppers and adversaries cannot then intercept and understand the secret messages. This cryptosystem is based on the difficulty of solving the discrete logarithm problem (DLP). The Diffie-Hellman key exchange generally follows this algorithm: Alice and Bob agree on a large prime p and a non-zero integer g mod p such that $g \in \mathbb{F}_p$, a finite field. These two values are published in the public channel. Both Alice and Bob select secret integers a and b respectively that they keep private. They use these secret values and the public ones to compute respectively

$$A \equiv g^a \mod p \qquad \text{and} \qquad B \equiv g^b \mod p.$$

They then exchange the values A and B on the public channel and compute the following with the publicly received value and their private integer:

$$A' \equiv B^a \mod p \qquad \text{and} \qquad B' \equiv A^b \mod p$$

These computations actually achieve the same value:

$$A' \equiv B^a \equiv (g^b)^a \equiv (g^a)^b \equiv A^b \equiv B' \mod p,$$

which is the **shared secret key**. The computations that Alice and Bob do are easily carried out (requiring polynomial-time computations). From Eve's perspective, she knows the values of p, g, A, and B, but does not know the secret values a and b. To solve for a and b would require solving the DLP. Thus if she could solve the DLP, then she would know the secret integers and be able to calculate their shared secret key. However, since the DLP is a difficult problem, especially if p is a large enough prime, Eve is not able to solve it in polynomial time.

2.2 QUANTUM INFORMATION

For our purposes, a **quantum system** will be a finite-dimensional Hilbert space over $\mathbb{C}$. The **state** of a quantum system H is given by a unit vector $\varphi \in H$, i.e. a vector $\varphi \in H$ satisfying $\|\varphi\|^2 = \langle \varphi, \varphi \rangle = 1$. A **quantum operation**

is given by a unitary operator U on H, i.e. a matrix $U \in M_n$ satisfying $UU^\dagger = U^\dagger U = I$. If a quantum system has initial state φ, then its state after the quantum operation U is given by $U\varphi$.

By a **projection**, we mean a square matrix $P \in M_n$ satisfying $P = P^2 = P^\dagger$. By a **projection-valued measure**, we mean a set $\{P_1, \ldots, P_k\} \subseteq M_n$ of projections satisfying $\sum_i P_i = I$. Given a projection-valued measure $\{P_1, \ldots, P_k\}$, its associated **quantum measurement** is a process which takes as input the state φ of a quantum system and returns as output an integer $i \in \{1, 2 \ldots, k\}$ with probability $p_i = \langle \varphi, P_i \varphi \rangle$. A quantum measurement of state φ returning value i results in the state of the system changing to

$$\varphi_i = \frac{P_i \varphi}{\langle \varphi, P_i \varphi \rangle^{1/2}}.$$

In particular, if φ is in the range of P_i, then $\varphi_i = \varphi$.

2.3 THE PAULI GROUPS

For the remainder of the paper, we mostly consider quantum systems of n-qubits, i.e. Hilbert spaces of dimension 2^n. An n-qubit Hilbert space may be regarded as the n-fold tensor product Hilbert space $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$, and a vector $\varphi \in \mathbb{C}^2$ is called a **qubit**.

We let X, Y and Z denote the 2×2 Pauli matrices, namely

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

and we let I denote the 2×2 identity matrix. The set $\{I, X, Y, Z\}$ generates a 16 element subgroup of the 2×2 matrices called the *Pauli group*. The 16 elements are given by $\pm\sigma$ and $\pm i\sigma$ where $\sigma \in \{I, X, Y, Z\}$, and the group structure is governed by the relations $X^2 = Y^2 = Z^2 = I$, $XY = iZ$, $XY = -YX$, $XZ = -ZX$, and $YZ = -ZY$. We let P denote the Pauli group.

For each positive integer n, we define the n^{th} Pauli group by

$$P_n = \{\sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n : \sigma_1, \ldots \sigma_n \in P\}.$$

As a group, P_n is isomorphic to the n-fold direct product of P with itself.

It is useful to associate to each element of P_n a corresponding **check vector**. This is done as follows. First, if $g \in P_n$, then g can be expressed uniquely as

$$g = (-1)^c (i)^d (X^{a_1} \otimes \cdots \otimes X^{a_n})(Z^{b_1} \otimes \cdots \otimes Z^{b_n})$$

where $a_1, \ldots, a_n, b_1, \ldots, b_n, c, d \in \{0, 1\}$. Then the check vector associated to g is given by the row vector

$$r(g) = (\vec{a}|\vec{b}), \quad \vec{a}^T, \vec{b}^T \in \mathbb{Z}_2^n.$$

It is easy to verify that if $r(g) = (\vec{a}|\vec{b})$ and $r(g') = (\vec{a}'|\vec{b}')$, then $r(gg') = (\vec{a} + \vec{a}'|\vec{b} + \vec{b}')$, where the addition is in the vector space $M_{1,2n}(\mathbb{Z}_2)$. Therefore many calculations in P_n can be performed in the corresponding transposed vector space $\mathbb{Z}_2^{2n}$.

Check vectors are also useful for determining if two vectors commute or anticommute. It can be verified that if $g, h \in P_n$, then either $gh = hg$ or $gh = -hg$. Whether or not two elements of P_n commute can be determined by computing the **swap product** of the corresponding check vectors. Given check vectors $(\vec{a}|\vec{b}), (\vec{a}'|\vec{b}')$, we define the swap product by

$$(\vec{a}|\vec{b}) * (\vec{a}'|\vec{b}') := \sum_{i=1}^{n} (a_i b_i' + a_i' b_i)$$

where the addition and multiplication all occur in the field $\mathbb{Z}_2$. In other words, the swap product of $(\vec{a}|\vec{b})$ and $(\vec{a}'|\vec{b}')$ is the dot product of $(\vec{a}|\vec{b})$ and $(\vec{b}'|\vec{a}')$ over $\mathbb{Z}_2$. A straightforward calculation shows that $gh = hg$ if and only if $r(g) * r(h) = 0$.

2.4 STABILIZER GROUPS

A **stabilizer group** is a subgroup G of P_n with the following properties:

- G is commutative.
- $-I \notin G$.

Recall that each $g \in P_n$ defines a unique linear map $g : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$ given by matrix-vector multiplication. Moreover, the matrix for g is always Hermitian; if it were not Hermitian, then $g^2 = -I$, which is not possible. Given a stabilizer group G, there exists $k \leq n$ and $g_1, g_2, \ldots, g_k \in G$ which are independent and generate the group G. In this case, $|G| = 2^k$. When independent generators are specified, we write $G = \langle g_1, g_2, \ldots, g_k \rangle$.

Each stabilizer group can be uniquely specified by its **check matrix**, which is a matrix whose rows are (augmented) check vectors for the generators $g_1, \ldots, g_k$. Since the elements of a stabilizer group must be Hermitian, they must have the form

$$(-1)^c i^{\vec{a}\cdot\vec{b}} X(\vec{a}) Z(\vec{b})$$

where $\vec{a}, \vec{b} \in \mathbb{Z}_2^n$, $c \in \{0, 1\}$, and where $X(\vec{a})$ and $Z(\vec{b})$ are given by

$$X(\vec{a}) := X^{a_1} \otimes \cdots \otimes X^{a_n}, \quad Z(\vec{b}) := Z^{b_1} \otimes \cdots \otimes Z^{b_n}.$$

Therefore each element $g \in G$ is uniquely specified by the **augmented check vector** $r'(g) = (\vec{a}|\vec{b}|c)$. Consequently, the entire group is specified by the **augmented check matrix**

$$r(G) = \begin{pmatrix} r'(g_1) \\ r'(g_2) \\ \cdots \\ r'(g_k) \end{pmatrix} = \begin{pmatrix} \vec{a}_1 & \vec{b}_1 & c_1 \\ \vec{a}_2 & \vec{b}_2 & c_2 \\ & \cdots & \\ \vec{a}_k & \vec{b}_k & c_k \end{pmatrix}_{k \times (2n+1)}$$

The check matrix is not unique; however, any two check matrices for the same stabilizer group are row equivalent. Thus, the group G can be uniquely specified with a check matrix in reduced row echelon form.

Note that not all matrices of size $k \times (2n + 1)$ represent a stabilizer group. The independence of the generators forces the rank of the matrix to be k, and the commutativity of the group ensures that the swap product of any two rows is zero. On the other hand, any $k \times (2n + 1)$ matrix of zeroes and ones satisfying these properties specifies a stabilizer group, namely the group generated by the set of operators $\{(-1)^{c_k} i^{\vec{a}_k \cdot \vec{b}_k} X(\vec{a}_k) Z(\vec{b}_k)\}$ (see [6] Section 10.5 for more details on this correspondence).

2.5 STABILIZER CODES

Given a stabilizer group $G \subseteq P_n$, we define the corresponding *stabilizer code* $C(G)$ to be the set of vectors

$$C(G) := \{\varphi \in \mathbb{C}^{2^n} : g\varphi = \varphi \text{ for all } g \in G\}.$$

The space $C(G)$ is a linear subspace of $\mathbb{C}^{2^n}$ of dimension $2^{n-\log|G|} = 2^{n-k}$ (when $|G| = 2^k$).

Corresponding to each stabilizer code $C(G)$ is a projection is given by

$$P_G = \frac{1}{|G|} \sum_{g \in G} g = \frac{1}{|G|} \prod_{i=1}^{k} (I + g_i)$$

where $G = \langle g_1, \ldots, g_k \rangle$. It is also useful to associate to G a measurement $\{P_{\vec{a}}(G)\}_{\vec{a} \in \mathbb{Z}_2^k}$ given by

$$P_{\vec{a}}(G) = \frac{1}{|G|} \prod_{i=1}^{k} (I + (-1)^{a_i} g_i).$$

When φ is an element of $C(G)$, then the measurement $\{P_{\vec{a}}(G)\}_{\vec{a} \in \mathbb{Z}_2^k}$ always yields $\vec{a} = \vec{0}$ and leaves the state φ unchanged.

3 THE PROPOSED CRYPTOSYSTEM

In this section, we will propose a public-key cryptosystem based on stabilizer codes. We will explain how information is encrypted as a quantum state and how that quantum state can be decrypted by quantum measurement.

We first reemphasize that while the protocol requires quantum machinery to be carried out, it is intended for the transfer of classical information (i.e. bit strings) rather than quantum information (i.e. quantum states), and in this way generalizes the super-dense coding protocol of [2]. The protocol does not rely on entanglement in any serious way, although the stabilizer states employed are often entangled. Instead, it relies on superposition to ensure security. For example, if an eavesdropper intercepts a message encrypted in a quantum state, they will have to perform a quantum measurement to obtain classical information from the state. If the wrong measurement

is performed, then the outcome of the measurement will be stochastic in nature, returning different bit strings according to a probability distribution. Decryption is possible because the secret key gives rise to the appropriate measurement for identifying the encoded message from the quantum state without error.

We begin by defining appropriate public and private keys for the protocol.

Definition 1. *Let G and H be stabilizer groups in P_n. We say that G is a **suitable key** for H if for every $h \in H$ there exists $g \in G$ such that $gh = -hg$, or equivalently $r(g) * r(h) = 1$.*

Proposition 1. *Let G and H be stabilizer groups in P_n, and suppose that G is a suitable key for H. If $\varphi \in C(G)$, then*

$$\langle h\varphi, h'\varphi \rangle = \begin{cases} 1 & h = h' \\ 0 & h \neq h' \end{cases}$$

for all $h, h' \in H$.

Proof. If $h = h'$, then $\langle h\varphi, h'\varphi \rangle = \langle h^2\varphi, \varphi \rangle = \langle \varphi, \varphi \rangle = 1$. Suppose that $h \neq h'$. Then there exists $g \in G$ such that hh' anticommutes with g. Hence

$$\begin{aligned} g(hh'\varphi) &= (ghh')\varphi \\ &= -(hh'g)\varphi \\ &= -hh'(g\varphi) \\ &= -hh'\varphi. \end{aligned}$$

Thus $hh'\varphi$ is an eigenvector for g with eigenvalue -1. Since φ is an eigenvector for g with eigenvalue 1 and since g is Hermitian, φ and $hh'\varphi$ are orthogonal. Hence $\langle h\varphi, h'\varphi \rangle = \langle \varphi, hh'\varphi \rangle = 0$. □

Proposition 2. *Let G and H be stabilizer groups in P_n, and suppose that G is a suitable key for H. If $|H| = |G|$, then*

$$\{hP_Gh\}_{h \in H}$$

is a projection-valued measure. Moreover, if $\varphi \in C(G)$, then the quantum measurement associated to $\{hP_Gh\}_{h \in H}$ returns the value h' with certainty when measuring the state $h'\varphi$.

Proof. We first verify that $\{hP_Gh\}_{h \in H}$ is a projection-valued measure. Since P_G is a projection, we have $(hP_Gh)^\dagger = h^\dagger P_G^\dagger h^\dagger = hP_Gh$ and $(hP_Gh)^2 = hP_Gh^2P_Gh = hP_Gh$. So each element hP_Gh is a projection. Suppose that $\rho \in C(G)$. Then by Proposition 1 $\langle h\rho, h'\rho \rangle = 0$ whenever $h \neq h'$. Let $\{\rho_1, \ldots, \rho_k\}$ be an orthonormal basis for $C(G)$. Then

$$\mathrm{Tr}((hP_Gh)(h'P_Gh')) = \mathrm{Tr}(P_G(hh')P_G(hh')) = \sum_{i=1}^{k} \langle \rho_i, (hh')P_G(hh')\rho_i \rangle = 0.$$

This is because $(hh')\rho_i$ is ortogonal to $\rho_i = (I)\rho_i$ whenever $hh' \neq I$, i.e. whenever $h \neq h'$, by Proposition 1. Therefore the set $\{hP_Gh\}_{h \in H}$ consists of mutually orthogonal projections, and hence $\sum_{h \in H} hP_Gh$ is a projection. Now

$$\begin{aligned} \mathrm{Tr}\left(\sum_{h \in H} hP_Gh \right) &= \sum_{h \in H} \mathrm{Tr}(hP_Gh) \\ &= \sum_{h \in H} \mathrm{Tr}(P_G) \\ &= (|H|/|G|)2^n. \end{aligned}$$

Since the rank of a projection is equal to its trace, and since $|H| = |G|$, it must be the case that $\sum_{h \in H} hP_Gh = I$.

Now consider the quantum measurement associated to $\{hP_Gh\}_{h \in H}$. If this measurement is applied to the state $h'\varphi$, then the measurement returns h' with probability

$$\langle h'\varphi, h'P_Gh'(h'\varphi) \rangle = \langle h'\varphi, h'P_G\varphi \rangle = \langle h'\varphi, h'\varphi \rangle = 1.$$

Therefore the measurement returns h' with certainty. □

We now describe the protocol for our public key cryptosystem. The cryptosystem requires a pair of stabilizer groups H and G in P_n, where $|H| = |G|$ and G is a suitible key for H. The public key H is published as a matrix in $M_{k,2n}$ whose rows are given by check vectors $r(h_i)$ corresponding to an ordered list of generators $h_1, h_2, \ldots, h_k \in H$. We let $r(h_1, h_2, \ldots, h_k)$ denote the matrix. Suppose Alice wishes to send Bob the bit string $\vec{\alpha} \in \mathbb{Z}_2^k$. Given the list of generators $h_1, h_2, \ldots, h_k$ in the public key, Alice can then produce a unitary $h(\vec{\alpha}) = h_1^{\alpha_1} h_2^{\alpha_2} \ldots h_k^{\alpha_k}$. This unitary can be encoded into a quantum circuit which takes as input a state φ and produces as output a new state $h(\vec{\alpha})\varphi$. When φ is stabilized by G, Proposition 2 guarentees that the measurement $\{hP_G h\}_{h \in H}$ will identify the element $h(\vec{\alpha}) \in H$ corresponding to Alice's measurement. The entire protocol is described formally in Algorithm 1 below.

Algorithm 1 The protocol

1: Bob publishes $H = \langle h_1, h_2, \ldots, h_k \rangle \subseteq P_n$ as the matrix $r(h_1, h_2, \ldots, h_k) \in M_{k,2n}(\mathbb{Z}_2)$.
2: Alice requests to send a message to Bob.
3: Bob chooses a suitable key $G \subseteq P_n$.
4: Bob prepares a unit vector $\varphi \in C(G)$ (the tableau) and sends it to Alice.
5: To send the bitstring $\vec{\alpha} \in \mathbb{Z}_2^n$, Alice applies the unitary h to the tableau φ, where

$$h = \prod_{i=1}^{k} h_i^{\alpha_i}$$

6: Alice sends $h\varphi$ to Bob.
7: Bob measures the state $h\varphi$ with the measurement $\{hP_g h\}_{h \in H}$, yielding with certainty the element $h \in H$ corresponding to Alice's bit string $\vec{\alpha} \in \mathbb{Z}_2^k$.

4 KEY SPACE ANALYSIS

In this section, we study the set of stabilizer groups G which are suitable keys for a fixed stabilizer group H in P_n representing the public key. We will both count the number of possible keys and also study how different keys are related. To simplify the analysis, we will only consider the case when $H = \langle h_1, \ldots, h_n \rangle$ and hence $|H| = 2^n$. At the end of this section, we will prove that, in this case, the suitable keys for H are described by a family of $2^{n+n(n-1)/2}$ matrices in $M_{n,2n+1}(\mathbb{Z}_2)$. The first $2n$ columns of these matrices correspond to $2^{n(n-1)/2}$ possible choices for generating unitaries $g_1, \ldots, g_n \in P_n$, while the last column can take on arbitrary values corresponding the choice of signs for these generators (so that a final column with entries $c_1, \ldots, c_n$ yields generators $(-1)^{c_1} g_1, \ldots, (-1)^{c_n} g_n$. Our analysis with rely on a careful understanding of the correspondence between check matrices and elements of P_n described in Section 2.

Definition 2. *Let H be a stabilizer group in P_n with independent generators $h_1, \ldots, h_n$. We say that an ordered tuple $(g_1, \ldots, g_n)$ of elements of P_n is **dual** to the ordered tuple $(h_1, \ldots, h_n)$ if for each $i, j \in \{1, \ldots, n\}$ with $i \neq j$, we have $g_i h_i = -h_i g_i$ and $g_i h_j = h_j g_i$.*

Let $C \in M_{k,2n}(\mathbb{F})$ be a matrix over a field $\mathbb{F}$. Then we may identify the first n columns of C as a matrix $A \in M_{k,n}(\mathbb{F})$, last n columns of C as a matrix $B \in M_{k,n}(\mathbb{F})$, and express C as a concatenation of matrices $C = (A|B)$. We now define an operator $\star$ on $M_{k,2n}(\mathbb{Z}_2)$ making use of this observation. For a matrix $(A|B) \in M_{k,2n}(\mathbb{Z}_2)$ (where $A, B \in M_n(\mathbb{Z}_2)$), define $(A|B)^\star := (B|A)$. As in the previous section, given $h_1, \ldots, h_k \in P_n$, we let $r(h_1, \ldots, h_k)$ denote the matrix in $M_{k,2n}$ whose i^{th} row is $r(h_i)$.

Lemma 1. *Let H be a stabilizer group in P_n with independent generators $h_1, \ldots, h_n$. Then $(g_1, \ldots, g_n)$ is dual to $(h_1, \ldots, h_n)$ if and only if*

$$r(h_1, \ldots, h_n)^\star r(g_1, \ldots, g_n)^T = I_n$$

where I_n is the $n \times n$ identity matrix.

Proof. Observe that the i, j entry of $r(h_1, \ldots, h_n)^\star r(g_1, \ldots, g_n)^T$ is precisely $r(h_i) * r(g_j)$. The claim follows, since $h_i g_j = g_j h_i$ if and ony if $r(h_i) * r(g_j) = 0$ and $h_i g_j = -g_j h_i$ if and only if $r(h_i) * r(g_j) = 1$. □

Lemma 2. *Let $g_1, \ldots, g_k \in P_n$ be self-adjoint. Then $G = \langle g_1, \ldots, g_k \rangle$ is a stabilizer group if and only if*

$$r(g_1, \ldots, g_k)^\star r(g_1, \ldots, g_k)^T = 0_k$$

and the rank of $r(g_1, \ldots, g_k) = k$.

Proof. The rank of $r(g_1, \ldots, g_k) = k$ if and only if the elements $g_1, \ldots, g_k$ are independent. Since the ij entry of $r(g_1, \ldots, g_k)^\star r(g_1, \ldots, g_k)^T$ is $r(g_i) * r(g_j)$, the elements $g_1, \ldots g_k$ mutually commute if and only if $r(g_1, \ldots, g_k)^\star r(g_1, \ldots, g_k)^T = 0_k$. Finally if $g_1, \ldots, g_k$ are independent and mutually commuting, then the group they generate cannot contain $-I$, since any non-trivial element of the group generated by $g_1, \ldots, g_k$ must have a check vector which is a non-trivial linear combination of the vectors $r(g_1), \ldots, r(g_k)$, which must be non-trivial, whereas $r(-I) = \vec{0}$. □

Proposition 3. *Let H be a stabilizer group in P_n with independent generators $h_1, \ldots, h_n$. Then another stabilizer group G is a suitable key for H if and only if there exists $g_1, \ldots, g_n \in G$ such that $G = \langle g_1, \ldots, g_n \rangle$ and $(g_1, \ldots, g_n)$ is dual to $(h_1, \ldots, h_n)$.*

Proof. Suppose that G is a sutiable key for H with generators $g_1, \ldots, g_n \subseteq P_n$. Thus, for each $h \in H$ there exists $g \in G$ such that $gh = -hg$. Let $r(h_i) = r_i$, $r(g_i) = s_i$, and let M and N be matrices whose i^{th} row is r_i or s_i, respectively. Then $M^\star M = N^\star N = 0_n$ by Lemma 2. Let V denote the row space of M and let W denote the row space of N. Then $\dim(V) = \dim(W) = n$ and $\ker(M^\star) = V$ and $\ker(N^\star) = W$.

Let K_i denote the kernel, in $\mathbb{Z}_2^{2n}$, of the $(n-1) \times 2n$ matrix whose rows are given by the set of vectors $r_1, \ldots, r_{i-1}, r_{i+1}, \ldots, r_n \in \mathbb{Z}_2^{2n}$. Then

$$\dim(K \cap W) = \dim(K) + \dim(W) - \dim(K + V) = 2n + 1 - \dim(K + W) \geq 1.$$

So there exists a non-zero vector $q_i \in W$ such that $q_i * r_j = 0$ for all $j \neq i$. If $q_i * r_i = 0$, then $q_i \in \ker(M^\star) = V$. However, if that were the case, then there would exist $q \in W$ such that $q_i * q = 1$. That cannot be the case, since $q_i \in W = \ker(N^\star)$. Therefore $q_i * r_i = 1$. This holds for each $i = 1, 2, \ldots, n$. So there exist $q_1, \ldots, q_n \in W$ such that $M^\star q_i = e_i$ for each i.

We claim $q_1, \ldots, q_n$ is a basis for W. It suffices to show that $q_1, \ldots, q_n$ are linearly independent since $\dim(W) = n$. Suppose $\sum \lambda_i q_i = 0$. Then

$$0 = M^\star(\sum_i \lambda_i q_i) = \sum_i \lambda_i e_i.$$

Since $e_1, \ldots, e_n$ are linearly independent, each $\lambda_i = 0$.

Finally, since $q_i \in W$, the matrix L whose i^{th} row is q_i is row equivalent to N and satisfies both $L^\star L^T = 0_n$ and $M^\star L^T = I_n$. Since L is row equivalent to N, the elements of L correspond to unique elements $g_1', \ldots, g_n' \subseteq P_n$. Since the rank of L equals the rank of N and since $L^\star L^T = 0_n$, the elements $g_1', \ldots, g_n'$ generate G by Lemma 2. Since $M^\star L^T = I_n$, we see that $(g_1', \ldots, g_n')$ is dual to $(h_1, \ldots, h_n)$ by Lemma 1.

On the other hand, suppose that $G = \langle g_1, \ldots, g_n \rangle$ and $(g_1, \ldots, g_n)$ is dual to $(h_1, \ldots, h_n)$. Let h be a nontrivial element of H. Then $h = h_1^{a_1} h_2^{a_2} \ldots h_n^{a_n}$ for some $a_1, \ldots, a_n \in \mathbb{Z}_2$ with $a_i = 1$ for some $i \in \{1, 2, \ldots, n\}$. Then

$$hg_i = h = h_1^{a_1} h_2^{a_2} \ldots h_n^{a_n} g_i = -g_i h = h_1^{a_1} h_2^{a_2} \ldots h_n^{a_n} = -g_i h$$

since g_i commutes with h_j whenever $j \neq i$ and $h_i g_i = -g_i h_i$. It follows that G is a suitable key for H. □

The following theorem characterizes the set of suitable keys for a given public key H.

Theorem 1. *Let H be a stabilizer group with independent generators $h_1, \ldots, h_n \in P_n$. Then G is a suitable key for H if and only if there exist $g_1, \ldots, g_n \in G$ such that*

$$r(g_1, \ldots, g_n)^\star r(g_1, \ldots, g_n)^T = 0_n$$

and

$$r(h_1, \ldots, h_n)^\star r(g_1, \ldots, g_n)^T = I_n.$$

Proof. Observe that since the rank of $r(h_1, \ldots, h_n)^\star$ is n, the condition $r(h_1, \ldots, h_n)^\star r(g_1, \ldots, g_n)^T = I_n$ implies that the rank of $r(g_1, \ldots, g_n)$ is n. The statement now follows from Lemma 1, Lemma 2, and Proposition 3. □

We will use Theorem 1 to describe and enumerate the set of all suitable keys for a given stabilizer H. Suppose $h_1, \ldots, h_n$ are generators for H, and let $M = r(h_1, \ldots, h_n)$. By Theorem 1, we need to count the number of matrices $N \in M_{n,2n}(\mathbb{Z}_2)$ satisfying $N^\star N^T = 0_n$ and $M^\star N^T = I_n$.

Proposition 4. *Let $M \in M_{n,2n}(\mathbb{Z}_2)$ be a rank n matrix satisfying $M^\star M^T = 0_n$, and let r_i denote the i-th row of M for each $i \in \{1, 2, \ldots, n\}$.*

1. There exists $N \in M_{n,2n}(\mathbb{Z}_2)$ such that $N^\star N^T = 0_n$ and $M^\star N^T = I_n$.

2. *If $L \in M_{n,2n}(\mathbb{Z}_2)$ is another matrix satisfying $L^\star L^T = 0_n$ and $M^\star L^T = I_n$, then there exists a unique symmetric matrix $A = (a_{ij}) \in M_n(\mathbb{Z}_2)$ such that*

$$\lambda_i = \eta_i + \sum_{j=1}^{n} a_{ij} r_i$$

where λ_i denotes the i-th row of L and η_i denotes the i-th row of N.

3. *If $A = (a_{ij}), A' = (a'_{ij}) \in M_n(\mathbb{Z}_2)$ are two distinct symmetric matrices, then the matrices L and L' whose i-th rows are given by*

$$\lambda_i = \eta_i + \sum_{j=1}^{n} a_{ij} r_i \quad \textit{and} \quad \lambda'_i = \eta_i + \sum_{j=1}^{n} a'_{ij} r_i,$$

respectively, are distinct, i.e. $L \neq L'$.

Proof. We first consider statement (1). To justify the existence of the matrix N, choose vectors $s_1, \ldots, s_n \in \mathbb{Z}_2^{2n}$ which satisfy $M^\star s_i = e_i$, where $e_1, \ldots, e_n$ are the standard unit vectors in $\mathbb{Z}_2^n$. Such vectors exist since the rank of M is n. Let N' be the matrix whose i^{th} row is s_i. Then $M^\star (N')^T = I_n$. However, it may not be the case that $(N')^\star (N')^T = 0_n$. We will show that we can replace the rows of N' with new rows $\eta_1, \ldots, \eta_n$ to obtain a matrix N which satisfies both $M^\star N^T = I_n$ and $N^\star N^T = 0_n$. We will obtain the vectors $\eta_1, \ldots, \eta_n$ by adding an element of the row space of M to s_i.

We begin with η_1. Define

$$q_1 := \sum_{k=1}^{n} (s_1 * s_k) r_k.$$

Then $q_1 * s_k = 1$ whenever $s_1 * s_k = 1$, and $q_1 * s_k = 0$ whenever $s_1 * s_k = 0$. Set $\eta_1 = s_1 + q_1$. Then $\eta_1 * s_k = 0$ for all $k = 2, \ldots, n$. Similarly, define $\eta_2 = s_2 + q_2$, where

$$q_2 := \sum_{k=2}^{n} (s_2 * s_k) r_k.$$

Then $\eta_2 * s_k = 0$ for all $k \in \{3, 4, \ldots, n\}$. Also,

$$\eta_1 * \eta_2 = \eta_1 * (s_2 + q_2) = \eta_1 * s_2 + \eta_1 * q_2 = 0.$$

This is because $\eta_1 * s_2 = 0$ and $\eta_1 * r_k = 0$ for all $k \in \{2, 3, \ldots, n\}$. Continuing in this manner, we define for each $j = 3, \ldots, n-1$

$$q_j := \sum_{k=j}^{n} (s_j * s_k) r_k$$

and define $\eta_j = s_j + q_j$. We set $\eta_n = s_n$. Then $\eta_i * \eta_j = 0$ for all i and j, and the resulting matrix N satisfies $M^\star N^T = I_n$ and $M^\star N^T = I_n$. This verifies statement (1).

We now consider statement (2). Suppose that L is another matrix which satisfies $M^\star L^T = I_n$ and $L^\star L^T = 0_n$. Let λ_i denote the i^{th} row of L. We calim that $\lambda_i = \eta_i + q_i$ for some element q_i of the row space of M. This is because $\lambda_i - \eta_i$ is an element of the kernel of $M^\star$ and the kernel of $M^\star$ is precisely the row space of M, since

$$\dim(\ker(M^\star)) = 2n - \operatorname{rank}(M^\star) = n$$

and since the n-dimensional row space of M is a subset of the kernel of $M^\star$.

To satisfy the condition $\lambda_i * \lambda_j = 0$ for all i and j, we need

$$\lambda_i * \lambda_j = (\eta_i + q_i) * (\eta_j + q_j) = \eta_i * q_j + q_i * \eta_j = 0.$$

Each vector q_i has a unique decomposition as $\sum_k a_{ik} r_k$. Since $\eta_i * r_i = 1$ and $\eta_i * r_j = 0$ when $i \neq j$, the q_i's must satisfy the following condition: whenever $a_{ji} = 1$, then $a_{ij} = 1$. Thus $A = (a_{ij})$ is symmetric.

Finally, we consider statement (3). Assume we are given symmetric matrices A and A', and let L and L' be the matrices whose i-th rows are given by

$$\lambda_i = \eta_i + \sum_{j=1}^{n} a_{ij} r_i \quad \text{and} \quad \lambda'_i = \eta_i + \sum_{j=1}^{n} a'_{ij} r_i,$$

respectively. We will check the contrapositive of the statement. Suppose that $L = L'$. Then for every $i \in \{1, \ldots, n\}$ we have

$$\sum_{j=1}^{n} (a_{ij} - a'_{ij}) r_j = \sum_{j=1}^{n} a_{ij} r_i - \sum_{j=1}^{n} a'_{ij} r_i = 0.$$

By the linear independence of $\{r_1, \ldots, r_n\}$, we have $a_{ij} = a'_{ij}$ for all $j \in \{1, \ldots, n\}$. This occurs for every i, so $A = A'$. □

Theorem 2. *Let H be a stabilizer group in P_n with $|H| = 2^n$. Then there are $2^{n+n(n-1)/2}$ distinct suitable keys for H in P_n. These keys are indexed by symmetric matrices $A \in M_n(\mathbb{Z}_2)$ and vectors $\vec{\alpha} \in \mathbb{Z}_2^n$. Specifically, given $H = \langle h_1, \ldots, h_n \rangle$, a symmetric matrix $A = (a_{ij}) \in M_n(\mathbb{Z}_2)$ and a vector $\vec{\alpha} \in \mathbb{Z}_2^n$, the corresponding secret key $G(A, \vec{\alpha})$ is the stabilizer group generated by the elements $g_1, \ldots, g_n$, where*

$$g_k = i^{a_{kj}} (-1)^{\alpha_k} g'_k \prod_{j=1}^{n} h_k^{a_{kj}}$$

and $G_0 = \langle g'_1, \ldots, g'_n \rangle$ is a fixed suitable key for H. Under this correspondence, $G(A, \vec{\alpha}) \neq G(A', \vec{\alpha}')$ if $A \neq A'$ or $\alpha \neq \alpha'$.

Proof. This follows from Theorem 1 and Proposition 4, and the observation that whenever $r(g'_k) = \lambda_k$ and $r(h_k) = r_k$ we have

$$r(g_k) = r(i^{a_{kj}} (-1)^{\alpha_k} g'_k \prod_{j=1}^{n} h_k^{a_{kj}}) = \lambda_i + \sum_{j=1}^{n} a_{ij} r_i.$$

The factor $i^{a_{kj}}$ is needed to ensure that g_k is self-adjoint. The value $2^{n+n(n-1)/2}$ comes from the observation that there are 2^n choices for the vector $\vec{\alpha} \in \mathbb{Z}_2^n$ and $2^{n(n-1)/2}$ possible symmetric matrices in $M_n(\mathbb{Z}_2)$. □

5 ONE-WAY SECURITY ANALYSIS

In this section, we wish to study the security of the protocol introduced above. To do so, we analyze two types of attacks. First, we will consider a brute force attack, where an eavesdropper (Eve) selects a suitable secret key G' at random and attempts to use the key to discern a single bit string $\vec{a}$ by intercepting and measuring the state transferred from Alice to Bob. Second, we will consider a more sophisticated letter frequency attack, where Eve intercepts an unlimited number of states transferred from Alice to Bob under the assumption that Bob always encodes the tableau state using the same secret key G. We will see that the brute force attack is unlikely to yield any significant information, whereas the letter frequency attack may eventually enable Eve to discern Alice's messages. We conclude with a discussion of what precautions can be taken to prevent a successful letter frequency attack.

5.1 THE BRUTE FORCE ATTACK

A brute force attack proceeds as follows. Alice wishes to send a message $h \in H$ to Bob. Bob randomly selects a secret key G, prepares a stabilizer state $\varphi \in C(G)$, and sends φ to Alice. Alice passes φ through a circuit to produce $h\varphi$, which she attempts to send to Bob. However, $h\varphi$ is intercepted by Eve. Eve then attempts to measure $h\varphi$ with a measurement $\{P'_h\}_{h \in H}$ where $P'_h := hP_{G'}h$ and $P_{G'}$ is prepared using another randomly selected suitable secret key G'. We wish to understand what, if anything, Eve can learn by performing this measurement.

Of course, if $G = G'$ (i.e. Eve made a very lucky guess), then the measurement will return h, and Eve will obtain Alice's measurement. In general, the probability that Eve's measurement will return h is given by

$$p(h) = \mathrm{Tr}((hP_{G'}h)(hP_Gh)) = \mathrm{Tr}(P_{G'}P_G).$$

Therefore, we seek to understand quantities of the form $\mathrm{Tr}(P_{G'}P_G)$ where G and G' are suitable secret keys.

To calculate $\mathrm{Tr}(P_GP_{G'})$, we will use the following.

Lemma 3. *Let $n \in \mathbb{N}$. Then for each $g \in P_n$, we have $\mathrm{Tr}(g) \in \{0, \pm 2^n, \pm i2^n\}$. In particular, $\mathrm{Tr}(g) = \lambda 2^n$ if and only if $g = \lambda I$ where $\lambda \in \{1, -1, i, -i\}$.*

Proof. If $g \in P_n$, then $g = \lambda\sigma_1 \otimes \cdots \otimes \sigma_n$, where $\sigma_i \in \{I, X, Y, Z\}$ for each i and $\lambda \in \{1, -1, i, -i\}$. Then

$$\mathrm{Tr}(g) = \lambda \prod_{i=1}^{n} \mathrm{Tr}(\sigma_i).$$

Since $\mathrm{Tr}(X) = \mathrm{Tr}(Y) = \mathrm{Tr}(Z) = 0$, we have $\mathrm{Tr}(g) \neq 0$ if and only if $\sigma_i = I$ for each i. When $\sigma_i = I$ for every i, we get $g = \lambda I$ and $\mathrm{Tr}(g) = \lambda \mathrm{Tr}(I) = \lambda 2^n$. □

Lemma 4. *Let G and G' be stabilizer groups in P_n. Then* $\mathrm{Tr}(P_G P_{G'}) = 0$ *if and only if*

$$|G \cap -G'| \neq 0.$$

Proof. First, suppose that $|G \cap -G'| = 0$. Then there exists $g \in G$ such that $-g \in G'$. Since $-I$ is not an element of G or G', we have $g \neq I$. Now, if $G = \langle g_1, \ldots, g_n \rangle$ and $G' = \langle g'_1, \ldots, g'_n \rangle$, then

$$P_G = \frac{1}{2^n} \prod_{i=1}^{n} (I + g_i) \quad \text{and} \quad P_{G'} = \frac{1}{2^n} \prod_{i=1}^{n} (I + g'_i).$$

Since g and $-g$ are nontrivial elements of G and G', respectively, we may assume that $g_n = g$ and $g'_1 = -g$. Thus

$$P_G P_{G'} = \frac{1}{4^n} (I + g_1) \ldots (I + g_n)(I + g'_1) \ldots (I + g'_n)$$

and

$$(I + g_n)(I + g'_1) = (I + g)(I - g) = I + g - g - g^2 = 0.$$

So $P_G P_{G'} = 0$.

Conversely, suppose that $\mathrm{Tr}(P_G P_{G'}) = 0$. Since

$$P_G = \frac{1}{2^n} \sum_{g \in G} g \quad \text{and} \quad P_{G'} = \frac{1}{2^n} \sum_{g' \in G'} g',$$

we have

$$\mathrm{Tr}(P_G P_{G'}) = \frac{1}{4^n} \sum_{g \in G, g' \in G'} \mathrm{Tr}(g g').$$

By Lemma 3, $\mathrm{Tr}(gg') \in \{0, \pm 2^n, \pm i 2^n\}$ for each $g \in G$ and $g' \in G'$. Since $I \in G \cap G'$ and $\mathrm{Tr}\left(I^2\right) = \mathrm{Tr}(I) = 2^n$, there must be $g \in G$ and $g' \in G'$ such that $\mathrm{Tr}(gg') = -2^n$. By Lemma 3 again, $gg' = -I$. But this implies $g = -g'$. □

Lemma 5. *Let G and G' be stabilizer groups in P_n. Then*

$$\mathrm{Tr}(P_G P_{G'}) = \begin{cases} \frac{1}{2^n} |G \cap G'| & |G \cap -G'| = 0 \\ 0 & \textit{else} \end{cases}$$

Proof. By Lemma 4, $\mathrm{Tr}(P_G P_{G'}) = 0$ if and only if $|G \cap -G'| \neq 0$. Assume $|G \cap G'| = 0$. We claim that for every $g \in G$ and $g' \in G'$, either $\mathrm{Tr}(gg') = 2^n$ or $\mathrm{Tr}(gg') = 0$. To see this, suppose first that $\mathrm{Tr}(gg') = \pm i 2^n$. By Lemma 3, this implies that $gg' = \pm iI$ and hence $g = \pm ig'$. This is not possible because squaring both sides yields $g^2 = -I$ and $-I \notin G$. Next, suppose $\mathrm{Tr}(gg') = -2^n$. Then $gg' = -I$, by Lemma 3. However, this implies $g = -g'$, which is not possible because $|G \cap -G'| = 0$. The claim follows by Lemma 3 again.

Next, suppose that $\mathrm{Tr}(gg') = 2^n$ for $g \in G$ and $g' \in G'$. Then $gg' = I$, by Lemma 3. This implies that $g = g'$, and hence $g \in G \cap G'$. On other other hand, if $g = g'$ then $\mathrm{Tr}(gg') = \mathrm{Tr}(I) = 2^n$. Since

$$P_G = \frac{1}{2^n} \sum_{g \in G} g \quad \text{and} \quad P_{G'} = \frac{1}{2^n} \sum_{g' \in G'} g',$$

we have

$$\begin{aligned} \mathrm{Tr}(P_G P_{G'}) &= \frac{1}{4^n} \sum_{g \in G, g' \in G'} \mathrm{Tr}(gg') \\ &= \frac{1}{4^n} \sum_{g \in G} 2^n |\{g' : g' \in G', g = g'\}| \\ &= \frac{1}{4^n} 2^n |G \cap G'| \\ &= \frac{1}{2^n} |G \cap G'|. \end{aligned}$$

□

Theorem 3. *Suppose that $G = \langle g_1, \ldots, g_n \rangle$ and $G' = \langle g'_1, \ldots, g'_n \rangle$ where $r(g'_i) = r(g_i) + r(h_i)$ are suitable secret keys relative to a stabilizer group H and $h_1, \ldots, h_n \in H$. Let $H' = \langle h_1, \ldots, h_n \rangle$, i.e. H' is the subgroup of H generated by $\{h_1, \ldots, h_n\}$. Then*

$$\mathrm{Tr}(P_G P_{G'}) = \begin{cases} \frac{1}{|H'|} & |G \cap -G'| = 0 \\ 0 & \text{else} \end{cases}$$

Proof. By Lemma 5, we know that $\mathrm{Tr}(P_G P_{G'}) = 0$ if and only if $|G \cap G'|$ and otherwise $\mathrm{Tr}(P_G P_{G'}) = \frac{1}{2^n}|G \cap G'|$. Thus we only need to calculate $|G \cap G'|$ in the case when $|G \cap -G'| = 0$.

Assume $|G \cap -G'| = 0$. Let $r(g_i) = r_i \in \mathbb{Z}_2^{2n}$ and let $r(h_i) = s_i \in \mathbb{Z}_2^{2n}$. Let $V = \mathrm{span}\{r_1, \ldots, r_n\}$ and let $W = \mathrm{span}\{r_1 + s_1, \ldots, r_n + s_n\}$. Then $|V| = |G|$, $|W| = |G'|$, and $|V \cap W| = |G \cap G'|$. Now

$$\dim(V \cap W) = \dim(V) + \dim(W) - \dim(V + W) = n + n - (n + k) = n - k$$

where $n + k = \dim(V + W)$. Thus, $n + k$ is equal to the rank of the $2n \times 2n$ matrix

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \\ r_1 + s_1 \\ \vdots \\ r_n + s_n \end{bmatrix}.$$

This matrix is row equivalent to the matrix

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \\ s_1 \\ \vdots \\ s_n \end{bmatrix}$$

and from this it follows that $k = \dim \mathrm{span}\{s_1, \ldots, s_n\}$. Since $|\mathrm{span}\{s_1, \ldots, s_n\}| = |H'|$, we have $|H'| = 2^k$. Thus

$$\mathrm{Tr}(P_G P_{G'}) = \frac{1}{2^n}|G \cap G'| = \frac{1}{2^n} 2^{n-k} = \frac{1}{2^k} = \frac{1}{|H'|}.$$

□

From the above analysis, it follows that the probability of Eve obtaining outcome h when performing the measurement $\{P'_h\}$ on the intercepted state $h\varphi$ is equal to 0 or $\frac{1}{|H'|}$, where $G = \langle g_1, \ldots, g_n \rangle$, $G' = \langle g'_1, \ldots, g'_n \rangle$, and $H' = \langle h_1, \ldots, h_n \rangle \subseteq H$. While we have written H' as the group generated by $h_1, \ldots, h_n$ here, we do not assume that $h_1, \ldots, h_n$ are independent. Hence H' may not equal H and so the probability $1/|H'|$ may be equal to or higher than $1/2^n$.

5.2 THE LETTER FREQUENCY ATTACK

We now consider a more sophisticated letter frequency attack. Consider a classical cryptographic scheme, where a sequence of bit strings are encoded and sent to a receiver in sequence to be decoded using a key. If the sender transmits bit strings according to a fixed known probability distribution (for example, the frequency of letters in the English alphabet), then an eavesdropper over time may be able to decode the intercepted bit strings.

In the context of our quantum protocol, the eavesdropping process becomes non-deterministic. As we saw in the previous subsection, whenever the bitstring $\vec{a}$ is encoded in a quantum state, an eavesdropper must perform a measurement which yields one of several bit strings $\vec{b}_1, \ldots, \vec{b}_n$ according to some probability distribution $\{p_1, \ldots, p_n\}$. This complicates the letter frequency attack, since the eavesdropper will recover a posterior probability distribution $p(\vec{b})$ (the probability of measuring symbol $\vec{b}$) which depends on the unknown prior distribution $q(\vec{a})$ (the probability that the sender encodes bitstring $\vec{a}$). More specifically, if $\pi(\vec{b}|\vec{a})$ is the conditional probability distribution indicating the probability that Eve's measurement yields $\vec{b}$ given that $\vec{a}$ was the encoded string, then

$$q(\vec{b}) = \sum_{\vec{a}} \pi(\vec{b}|\vec{a}) \quad \text{and} \quad p(\vec{a}) = \sum_{\vec{b}} \pi(\vec{b}|\vec{a}).$$

Even if Eve knows the prior distribution $p(\vec{a})$, it may not be possible to learn any information about the channel from only the distribution $q(\vec{b})$. However, we will see that, for our protocol, Eve may be able to at least determine whether or not she has chosen the correct key G' by only analyzing the distribution $q(\vec{b})$. This gives Eve the opportunity to search for a better G' until she has found a key that is good enough to perform a successful letter frequency attack.

We now translate the discussion above into more formal statements. Suppose Alice wishes to send a sequence of bit strings $\vec{a}_1, \ldots, \vec{a}_N \in \mathbb{Z}_2^n$ to Bob, and the bit strings will be transmitted according to the probability distribution $p(\vec{a})$ over $\mathbb{Z}_2^n$. To carry out the transmission, Bob first fixes a suitable key $G = \langle g_1, \ldots, g_n \rangle$ for H and prepares N identical copies of a stabilizer state φ for G. The states are sent to Alice in succession. Alice operates on the states in succession, mapping the i-th copy of φ to $h(\vec{a}_i)\varphi$, where $h(\vec{a}_i) := h_1^{a_1} \ldots h_n^{a_n}$. The states $\varphi_i := h(\vec{a}_i)\varphi$ are sent to Bob in succession. Separately, we assume Eve has fixed another suitable key $G' = \langle g'_1, \ldots, g'_n \rangle$ chosen at random. Eve will then intercept each state φ_i and measure it with the projection valued measure

$$\{P_{G'(\vec{b})}\}_{\vec{b} \in \mathbb{Z}_2^n}$$

where $G'(\vec{b}) := \langle (-1)^{b_1} g'_1, \ldots, (-1)^{b_n} g_n \rangle$. This measurement yields outcome $\vec{b}$ with probability

$$\pi(\vec{b}|\vec{a}_i) = \langle P_{G'(\vec{b})}\varphi_i, \varphi_i \rangle = \langle h(\vec{a}_i) P_{G'(\vec{b})} h(\vec{a}_i)\varphi, \varphi \rangle.$$

Since the rank one projection onto φ is P_G, we have

$$\langle h(\vec{a}_i) P_{G'(\vec{b})} h(\vec{a}_i)\varphi, \varphi \rangle = \mathrm{Tr}\Big(P_{G'(\vec{b})} h(\vec{a}_i) P_G h(\vec{a}_i) \Big).$$

From Proposition 3, we may assume without loss of generality that $(g_1, \ldots, g_n)$ is dual to $(h_1, \ldots, h_n)$ in the sense of Definition 2. Since

$$P_G = \frac{1}{|G|} \prod_{i=1}^{n} (g_i + I)$$

we have

$$h(\vec{a}) P_G h(\vec{a}) = \frac{1}{|G|} \prod_{i=1}^{n} (h(\vec{a}) g_i h(\vec{a}) + I) = \frac{1}{|G|} \prod_{i=1}^{n} (-1)^{a_i} g_i + I) = P_{G(\vec{a})}$$

for any $\vec{a} \in \mathbb{Z}_2^n$. Thus

$$\pi(\vec{b}|\vec{a}_i) = \mathrm{Tr}\Big(P_{G'(\vec{b})} P_{G(\vec{a}_i)} \Big) = \begin{cases} \frac{1}{2^n} |G'(\vec{b}) \cap G(\vec{a}_i)| & |G'(\vec{b}) \cap -G(\vec{a}_i)| = 0 \\ 0 & \text{else} \end{cases}$$

using Lemma 5. Alternatively, if we have $r(g'_i) = r(g_i) + r(h'_i)$ for each $i = 1, \ldots, n$ where $h'_1, \ldots, h'_n \in H$, then we have

$$\pi(\vec{b}|\vec{a}_i) = \begin{cases} \frac{1}{|H'|} & |G'(\vec{b}) \cap -G(\vec{a}_i)| = 0 \\ 0 & \text{else} \end{cases}$$

where $H' = \langle h'_1, \ldots, h'_n \rangle \subseteq H$. Since $r(g) = r(-g)$ for all $g \in P_n$, we see that $|H'|$ does not depend on the choice of $\vec{b}$ and $\vec{a}_i$. Hence $\pi(\vec{b}|\vec{a}_i)$ is uniform on the set $\{\vec{b} : |G'(\vec{b}) \cap -G(\vec{a}_i)| = 0\}$ and zero on its complement in $\mathbb{Z}_2^n$.

Now, suppose that $G' = G(\vec{b})$ for some $\vec{b} \in \mathbb{Z}_2^n$, i.e. $G' = \langle (-1)^{b_1} g_1, \ldots, (-1)^{b_n} g_n \rangle$. In this case, we have $|G'(\vec{b}) \cap G| = 0$ and $|G'(\vec{b}') \cap G| \neq 0$ for any $\vec{b}' \neq \vec{b}$. In this situation, Eve can carry out a successful letter frequency attack, provided she knows in advance the probability distribution $p(\vec{a})$. This is possible because, in this situation, $\pi(\vec{b}|\vec{a}) \in \{0, 1\}$, meaning that there is a bijective function $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ such that whenever Alice sends bit string $\vec{a}$, Eve's measurement returns $f(\vec{a})$ with certainty. The frequency that Eve observes the value $\vec{b}$ approximates $p(\vec{a}_i)$ for large N. Thus, if Eve selects one of the 2^n random keys of the form $G(\vec{b})$, she can carry out a successful letter frequency attack. As a corollary, if the frequency $q(\vec{b})$ in which Eve observes $\vec{b}$ is not a permutation of the prior distribution $p(\vec{a})$, then Even knows she has not selected a key of the form $G(\vec{b})$, and so she can select another key at random. Over time, if her eavesdropping goes undetected, Eve can converge on a key which can be used for a successful letter frequency attack.

There are at least two flaws that were exploited in the letter frequency attack described above. One flaw is that Alice is sending bit strings according to a probability distribution $p(\vec{a})$ which could be deciphered by an eavesdropper. This may not be helped, since requiring Alice to avoid sending information in certain ways limits the utility and efficiency of the protocol as a means of secure communication. The other flaw is that Bob sends

Alice many copies of the same Tableau φ. This can be remedied by instead sending a sequence of tableau states $\varphi_1, \varphi_2, \ldots$ where each φ_i is a stabilizer state for the stabilizer G_i and G_i is chosen uniformly at random from the set of suitable keys. This kind of randomization would prevent Eve from converging on a key suitable for a letter frequency attack, as described above. This does, however, create a need for synchronization between Alice and Bob, as Bob must know which key G_i to use to measure the i-th state $h(\vec{a}_i)\varphi$ returned by Alice.

6 FUTURE WORK

We conclude with a discussion of other potential vulnerabilities, improvements, or lines of inquiry which may warrant further study.

6.1 LEAKAGE ANALYSIS

As noted in the introduction, the need for the receiver for first transmit the tableau to the sender opens the door to possible leakage of the private key. In other words, an eavesdropper may determine some information about the private key by observing the tableau state and use this information to later decode an encoded message that is intercepted. This kind of leakage is partly prevented by the no-cloing theorem, which states that there does not exist a unitary which takes as input an arbitrary quantum state φ, together with an ancillary state ψ, and produces a pair of identical copies of φ. Thus, an eavesdropper cannot "copy" the tableau φ without changing it and risking detection. However, none of this prevents the eavesdropper from measuring the tableau φ anyway, and it is possible in principle that a viable attack could exist. A detailed analysis of this possibility this therefore warranted.

6.2 "MAN-IN-THE-MIDDLE" ATTACKS

Another attack one could consider against this protocol is a "man in the middle" attack. In this attack, Eve impersonates Bob by preparing her own tableau φ as a stabilzer state for her own chosen suitable key G, and sends the state to Alice. Alice, not realizing she received φ from the eavesdropper, sends Eve the modified state $h(\vec{a}_i)\varphi$. Eve then uses her key to measure the state and obtain $\vec{a}_i$. Preventing such an attack requires some form of authentication between Alice and Bob. One possible means would be for Alice and Bob to first share an entangled state $\widetilde{\varphi}$ and then to use $\widetilde{\varphi}$ to transfer states by quantum teleportation (see [2] for the original algorithm, and [4] for a generalization to multi-qubit states).

6.3 SECURITY AGAINST GENERAL QUANTUM OPERATIONS

In addressing potential brute force and letter frequency attacks, we have assumed that Eve would only use suitable keys, arising from the stabilizer framework, to measure intercepted states. However, there is no reason to assume that an eavesdropper would be so limited in their ability to perform quantum measurements. It is possible, a priori, that by performing measurements other than those which arise from stabilizer codes an eavesdropper may be able to more quickly converge on the correct private key and decipher the message. Understanding these more general attacks requires analysis beyond the stabilizer framework, which is beyond the intent of this paper.

6.4 QUANTUM MCELIECE AS A SUBPROTOCOL

We should also note a potential improvement to the protocol we have described. In [3], a "quantum McEliece" protocol was described, in which Alice endcodes her message, then subjects it to random noise before passing the resulting state to Bob. Bob then uses quantum error correction to reverse the random noise and decipher the message. By using a larger suitable key (i.e. $|G| > |H|$), it is possible to add this quantum McEliece protocol as a subroutine carried out after Alice modifies the tableau sent by Bob. Such a modification could, in principle at least, make the brute force and letter frequency attacks more difficult to carry out, thus increasing the security of the protocol.

6.5 GENERALIZATION BEYOND THE STABILIZER FRAMEWORK

Finally, we remark that one could naturally consider a more general version of the protocol we have described here which does not rely on the stabilizer formalism at all. A general protocol would proceed as follows. First, a generic "tableau" quantum state is prepared by Bob and sent to Alice. Alice then passes the state through a quantum circuit which changes the state to one of n possible mutually orthogonal states, each possible state corresponding to a unique message. The state is then sent back to Bob, who performs an appropriate measurement to obtain Alice's intended message. This protocol does not necessarily require stabilizer groups to be carried out. Thus a study of the possible range of protocols which could be implemented and their security properties would be valuable.

REFERENCES

[1] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing". In: vol. 560. Jan. 1984, pp. 175–179. DOI: 10.1016/j.tcs.2011.08.039.

[2] C. H. Bennett et al. "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels". In: *Phys. Rev. Lett.* 70 (13 Mar. 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

[3] H. Fujita. "Quantum McEliece Public-Key Cryptosystem". In: *Quantum Information and Computation* 12.3–4 (Mar. 2012), pp. 181–202. ISSN: 1533-7146.

[4] L. Gao, S. J. Harris, and M. Junge. "Quantum Teleportation and Super-Dense Coding in Operator Algebras". In: *International Mathematics Research Notices* 2021.12 (June 2019), pp. 9146–9179. ISSN: 1073-7928. DOI: 10.1093/imrn/rnz095. eprint: https://academic.oup.com/imrn/article-pdf/2021/12/9146/38814339/rnz095.pdf. URL: https://doi.org/10.1093/imrn/rnz095.

[5] D. Gottesman. "Class of quantum error-correcting codes saturating the quantum Hamming bound". In: *Phys. Rev. A* 54 (3 Sept. 1996), pp. 1862–1868. DOI: 10.1103/PhysRevA.54.1862. URL: https://link.aps.org/doi/10.1103/PhysRevA.54.1862.

[6] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000, pp. xxvi+676. ISBN: 0-521-63235-8; 0-521-63503-9.

[7] *Post-Quantum Cryptography, NIST*. https://csrc.nist.gov/Projects/post-quantum-cryptography. Accessed: 2022-07-21.

[8] P. W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. Nov. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[9] P. W. Shor. "Scheme for reducing decoherence in quantum computer memory". In: *Phys. Rev. A* 52 (4 Oct. 1995), R2493–R2496. DOI: 10.1103/PhysRevA.52.R2493. URL: https://link.aps.org/doi/10.1103/PhysRevA.52.R2493.