Pre-Privacy Amplification: A Post-Processing Technique for Quantum Key Distribution with Application to the Simplified Trusted Relay

by

John Burniston

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Masters of Science
in
Physics (Quantum Information)

Waterloo, Ontario, Canada, 2023

Author's Declaration

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

Until quantum repeaters and quantum error correcting codes can be made commercially viable, long distance quantum key distribution (QKD) will continue to rely on trusted relay satellites. Strongly constrained by weight and power efficiency, little room is left for raw computational power, lowering the key rate per second. Efforts to reduce the computational burden on satellites, such as the simplified trusted relay [1] (which does not participate in privacy amplification), come at a significant cost to their key rate per bit sent and maximum tolerable error rate. We construct a post processing technique, that acts as a sort of *pre-privacy amplification* that is performed before the usual error correction and privacy amplification steps. Loosely speaking, it provides a way to scale between the simplified trusted relay and the usual full trusted relay. For the asymptotic qubit six-state protocol, we demonstrate an increase in the maximum tolerable error rate from $\sim 12.62\%$ to $\sim 12.83\%$ for the full trusted relay, and from $\sim 9.05\%$ to $\sim 11.7\%$ for the simplified trusted relay. We also provide several sufficient conditions to determine when unique reduction matrices will yield identical key rates.

Acknowledgements

I would like to thank my supervisor Norbert Lütkenhaus who not only provided insightful input, and also encouraged a strong positive and friendly group dynamic which helped me weather the Pandemic.

I would also like to extend my thanks to Wenyuan Wang, Jie Lin, and Scott Johnstun, for their significant contributions to Optical Quantum Communication Theory Group's Numerical key rate toolbox. The skills I developed and experienced gained working with them offered invaluable insight into QKD and robust computational methods. I would also like to extend this to the rest group. Especially to Lars Kamin, Shlok Nahar, Florian Kanitschar, and Devashish Tupkary for the long discussion on QKD.

I am grateful for the help provide by Scott Johnstun, Lars Kamin, Florian Kanitschar, Devashish Tupkary, and Shlok Nahar who provided feedback on early drafts of my thesis.

Last but not least, I am grateful for my family, whose unending love and support was felt even on the other side of the country.

Table of Contents

List of Figures

Chapter 1

Introduction

Cryptographic protocols govern nearly all private communications. However, current cryptographic systems (referred to as classical cryptography) all operate on strict and unproven assumptions such as the complexity of certain mathematical problems, and computational resources to which an eavesdropper has access. If either assumption is false, then the security is fully compromised. For example, it is well known that a quantum computer running Shor's algorithm can break widely used public key cryptographic protocols like RSA [2]. There are many candidates, called post-quantum cryptographic protocols, to replace these, but they all still require making the same type of assumptions [3]. Thus, there is no guarantee that other quantum, or even classical, algorithms does not render these protocols vulnerable or obsolete. Although sufficient for short term secrets like credit card details that are only relevant for a few years, personal health records and state secrets can require a life time of guaranteed privacy. Quantum key distribution (QKD) overcomes these challenges by using fundamental properties of quantum mechanics to produces true information-theoretic secure key exchange [4, 5, 6]. QKD transforms the assumptions from unproven mathematical statements to the laws of physics and the physical implementation of devices. Therefore, QKD ensures that a secret key generated today cannot be broken by any technological improvement in the future.

QKD requires access to an insecure and untrusted quantum channel, and an authenticated classical channel[1] (the message's integrity and sender's identity are verifiable). QKD

[1]The implementation of the authenticated classical channel is considered a separate, but solvable problem from the security of QKD.

protocols typically operate with a sender, Alice, sending randomly selected signal states and transferring them to a receiver, Bob, over the untrusted quantum channel (which is assumed to be controlled by an eavesdropper, Eve). After Bob measures the signals, both parties split off and announce a random subset of their data. Because of the no-cloning theorem, Eve cannot obtain information about the signals without manipulating them. From this, Alice and Bob can characterize the quantum channel and choose to abort. If they choose to continue, Alice and Bob perform multiple steps of classical post processing, including steps to ensure they share the same secret key (error correction), and to eliminate any correlations Eve shares with them (privacy amplification) [6].

Although mathematically sound and secure, the physical implementation of QKD faces several challenges. For example, QKD done over optical fibre is limited by loss [7, 8]. As distance increases, the number of signals that reach Bob decays exponentially[2]. Coupled with imperfect detectors, the surviving signals are too close to the noise floor from random detectors firing, called dark counts [9]. Because all imperfections in the signal must be attributed to Eve, no secret key can be extracted. This limits point to point fibre optic QKD to short intercity connections [10]. One solution is to use untrusted relays utilizing entanglement swapping or quantum error correcting codes to increase distance. However, these rely on robust quantum memory and high fidelity quantum gates, and are far from commercially viable [9, 11]. The near future solution is trusted relays. Unlike, quantum repeaters and quantum error correcting codes, trusted relays are given enough information such that they can learn part or all of the secret key. For example, a *full trusted relay* performs a complete run of a QKD protocol with Alice, then does the same with Bob. It then announces the parity of the two key strings, effectively using one-time pad [12, 13] to encrypt one secret key with the other. However, each relay must act faithfully and cannot leak any information about the key. If even a single trusted relay in a chain acts in bad faith, then the entire secret key is compromised.

Although both trusted and untrusted relays allow for secret key exchange across arbitrary distances, the noise and loss in optical fibres and the atmosphere heavily increase the number of relays required. One solution is to place relays on satellites. In space, loss and noise are significantly reduced [10], and a satellite can travel from the line of sight from one party, to another. However, satellites are limited in computational power [14], and for trusted relays, steps such as privacy amplification are exceptionally expensive to

[2]Continuous variable QKD protocol operate differently and have other problems to contend with. We do not cover them in this thesis.

perform [1, 15]. Therefore, measures to reduce computational load on the satellite are exceptionally important hurdles that must be overcome.

One proposed solution is the *simplified trusted relay*, which performs error correction, but leaves privacy amplification to Alice and Bob [1, 15]. As a result the simplified trusted relay requires less computational power, but comes with a significant cost to the key rate per bit sent, and a lower maximum error tolerance. Recent analysis from [16] has shown that under low error rates, the simplified trusted relay can be run fast enough to compensate for this.

Drawing inspiration from delayed privacy amplification [17], we construct a novel post processing technique that acts as a sort of pre-privacy amplification step. Several raw key bits (before error correction and privacy amplification) are combined into a vector and a predecided parity check matrix, called a *reduction matrix*, is applied, limiting Eve's information. Loosely speaking, this provides a method to scale computational resource between the simplified trusted relay and the full trusted relay. Due to numerical limitations, we use the tomographically complete qubit six-state protocol [5], and limit our analysis to depolarization (errors indistinguishable from random noise [12]). We show that through careful selection of the reduction matrix, we get a small increase in maximum tolerable error rate for full trusted relays, and major increases for the simplified trusted relay. We also provide several sufficient conditions that result in distinct reduction matrices giving identical key rate.

The thesis is organized as follows: Chapter 2 covers the linear algebra, quantum information, and QKD required to follow this thesis. Chapter 3 introduces reduction matrices and applies them to the relatively simple full trusted relay. We cover multiple techniques to reduce the computational burden to calculate the key rate, and provide methods to reduce the number of reduction matrices that need to be checked. In Chapter 4 we extend our analysis to the simplified trusted relay and demonstrate major improvements to the key rate per bit sent. We summarize all our results in Chapter 5.

Chapter 2

Background

The Background is organized as follows. Section 2.1 covers basic properties of vector spaces that do not require inner products. This includes linear operators and tensor products. Section 2.2 covers the basics of finite dimensional Hilbert spaces and the Basics of quantum mechanics. This includes Special classes of operators, multipartite systems, channels and measurements. Section 2.3 covers the basics of information theory, and covers both classical and quantum entropy. Section 2.4 covers the basics of quantum key distribution, including the basic structure of a protocol, the mathematical format, and the six-state protocol. Section 2.5 covers full and simplified trusted relays, and Section 2.6 briefly outlines delayed privacy amplification, and the concepts borrowed from it.

2.1 Fields and Vector Spaces

Because much of the work in this thesis relies on finite fields, we first provide many properties of vector spaces that do not rely on an inner product structure. This section is primarily based on [18] for finite fields and vector spaces, in conjunction with notation from [19].

A review of basic fields, vector spaces, and groups can be found in Appendix A. Roughly speaking, a field is a set with commutative addition and multiplication. It contains elements analogous to 0 and 1, and every element has additive and multiplicative inverses (except there is no multiplicative inverse for 0). For a field $\mathcal{R}$, when addition and multiplication

operators are unambiguous, we use $\mathcal{R}$ to refer to both the field and the underlying set. We are primary concerned with the fields of real numbers ($\mathbb{R}$), complex numbers ($\mathbb{C}$), and finite fields (fields with only a finite number of elements). The most common finite field used in this thesis is the field $\mathbb{Z}_2$. Here addition and multiplication are done modulo 2 (so $-1 = 1$) and the field only has the elements 0 and 1 [18]. A vector space over a field $\mathcal{R}$ is defined in much the same way as vector spaces over $\mathbb{R}$ and $\mathbb{C}$, except scalar multiplication is done with respect to the field $\mathcal{R}$. Note that many fields do not support an inner product.

A passing familiarity of group theory, although not strictly needed, helps for determining equivalent reduction matrices found in Chapters 3 and 4. From Section A.2, the most important parts are the notation for the general linear group of size n over the field $\mathcal{R}$, $\mathrm{GL}_n(\mathcal{R})$, the notation for the permutation group of n elements, S_n, and the permutation matrices P_π where $\pi \in \mathrm{S}_n$.

Because we make heavy use of finite fields where inner products cannot be defined, we delay anything requiring inner products to Section 2.2. Furthermore, we only focus on finite dimensional vector spaces. For the vector space $\mathcal{R}^n$, we denote elements of the canonical basis as e_i, or $\vec{e}_i$ for $i \in \{1, \ldots, n\}$.

2.1.1 Linear Operators

Definition 2.1.1 (Linear Operator)**.** Let A and B be vector spaces over the field $\mathcal{R}$, and let $F : A \to B$. F is called a *linear operator* if it satisfies for all $\vec{a}, \vec{b} \in A$ and $r \in \mathcal{R}$

$$F(r\vec{a} + \vec{b}) = rF(\vec{a}) + F(\vec{b}). \tag{2.1}$$

Definition 2.1.2 (Space of Linear Operators)**.** Let A and B be vector spaces over the field $\mathcal{R}$. We define the set of all linear operators from A to B as $\mathrm{L}(A, B)$ and all linear operators from A to A as $\mathrm{L}(A)$. $\mathrm{L}(A, B)$ and $\mathrm{L}(A)$ are vector spaces over the field $\mathcal{R}$ [18].

Let A and B be vector spaces over the field $\mathcal{R}$ with dimensions n and m respectively. For any linear operator $F \in \mathrm{L}(A, B)$, we can associate with it a matrix M_F given by the following process. Let $\{e_i\}_{i=1,\ldots,n}$ and $\{e_j\}_{j=1,\ldots,m}$ be the canonical bases of A and B respectively. Also, Let $\{\vec{e}_i\}_{i=1,\ldots,n}$ and $\{\vec{e}_j\}_{j=1,\ldots,m}$ be the canonical bases of $\mathcal{R}^n$ and $\mathcal{R}^m$ respectively. Let $f_i = F(e_i)$, and $\{f_{j,i}\}_{j=1,\ldots,m} \subset \mathcal{R}$ such that $f_i = \sum_{j=1}^{m} f_{i,j} e_j$. We then

define the matrix M_F as

$$M_F = \sum_{i=1}^{n} \sum_{j=1}^{m} f_{j,i} \vec{e}_j \vec{e}_i^{\mathrm{T}}. \tag{2.2}$$

In other words, $\mathrm{L}(A, B) \simeq \mathcal{R}^{m \times n}$. We refer to the linear operator F and its matrix M_F interchangeably.

Definition 2.1.3 (Dual Space)**.** Let A be a vector space over a field $\mathcal{R}$. We call the space $\mathrm{L}(A, \mathcal{R})$ the *dual space* of A and denote it as $A^\dagger$.

Because we work with finite dimensions, $A \simeq A^\dagger$, we often just use A and $(A^\dagger)^\dagger$ interchangeably, and do not explicitly write the double dual.

Theorem 2.1.4 (Dual Basis)**.** *Let A be a vector space over a field $\mathcal{R}$, and $\{v_i\}_{i=1,\ldots,n}$ a basis of A. Then, there exist a basis $\{w_i\}_{i=1,\ldots,n}$ of $A^\dagger$ such that for all $i, j \in \{1, \ldots, n\}$*

$$w_j(v_i) = \delta_{i,j}. \tag{2.3}$$

For the case where $\{V_i\}_{i=1,\ldots,n}$ is the canonical basis, we denote the dual canonical basis as $\{\tilde{e}_i\}_{i=1,\ldots,n}$. Naturally, we associate with this the bilinear form $\langle \cdot, \cdot \rangle : A \times A \to \mathcal{R}$ with

$$\langle e_i, e_j \rangle = \tilde{e}_i(e_j). \tag{2.4}$$

Unless the field is $\mathbb{C}$, or specify other wise, we use this as our bilinear map.

Definition 2.1.5 (Dual Operators)**.** Let A and B be vector spaces and let $\rho \in \mathrm{L}(A, B)$. We uniquely define the *dual operator* $\rho^\dagger \in \mathrm{L}(B, A)$ by

$$\langle \rho^\dagger b_B, a_A \rangle = \langle b_B, \rho a_A \rangle, \tag{2.5}$$

for all $a_A \in A$ and $b_B \in B$.

Some of the most important set and subspaces associated with linear operators are the kernel, image, and pre-image, defined bellow.

Definition 2.1.6 (Kernel)**.** Let A and B be vector spaces over a field $\mathcal{R}$, and $M \in \mathrm{L}(A, B)$. The kernel of M is defined as

$$\ker(M) = \{ \vec{a} \in A | M\vec{a} = 0 \}. \tag{2.6}$$

Definition 2.1.7 (Image)**.** Let A and B be vector spaces over a field $\mathcal{R}$, and $M \in \mathrm{L}(A, B)$. The image of M is defined as

$$\mathrm{Im}(M) = \{M\vec{a} \,|\, \vec{a} \in A\}\,. \tag{2.7}$$

Definition 2.1.8 (Pre-Image)**.** Let A and B be vector spaces over a field $\mathcal{R}$, $M \in \mathrm{L}(A, B)$, and $\vec{b} \in B$. The pre-image of $\vec{b}$ for M is defined as

$$M^{-1}(\vec{b}\,) = \left\{ \vec{a} \in A \middle| M\vec{a} = \vec{b} \right\}. \tag{2.8}$$

Theorem 2.1.9 (Rank-Nullity)**.** *Let A and B be vector spaces over a field $\mathcal{R}$, and $M \in \mathrm{L}(A, B)$, then*

$$\dim(A) = \dim(\ker(M)) + \mathrm{rank}(M) \tag{2.9}$$

Definition 2.1.10 (Reduced Row Echelon Form)**.** Let $\mathcal{R}$ be a field and let $M \in \mathcal{R}^{m\times n}$. M is said to be in reduced row echelon form if it satisfies all of the following [18]:

1. All rows of zeros are at the bottom of the matrix.
2. The first non zero entry of a row (called the pivot) is 1.
3. For any row j the pivot for the row $j+1$ must be further to the right.
4. Every other entry in a column with a pivot must be 0.

Furthermore, let a matrix $N \in \mathcal{R}^{m\times n}$, and a matrix $M \in \mathcal{R}^{m\times n}$ in reduced row echelon form. We say N is the reduced row echelon form of M if and only if there exists a invertible matrix $U \in \mathrm{GL}_m(\mathcal{R})$ such that $M = UN$.

For example, bellow we give a matrix $M \in \mathbb{R}^{4\times 5}$ and its reduced row echelon form N.

$$M = \begin{bmatrix} 1 & 2 & 10 & 3 & 9 \\ 1 & 0 & 4 & 3 & -1 \\ -2 & 1 & -5 & 3 & 25 \\ 1 & 0 & 4 & 0 & -7 \end{bmatrix}, \qquad N = \begin{bmatrix} 1 & 0 & 4 & 0 & -7 \\ 0 & 1 & 3 & 0 & 5 \\ 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{2.10}$$

Every matrix has only one reduced row echelon form, and the reduced row echelon form produces an equivalence class under left multiplication by invertible matrices (row operations).

In addition, for a matrix M and its reduced row echelon form N, $\text{rank}(M) = \text{rank}(N)$. Later in Section 3.4, we use find a new property that is shared between a matrix and its reduced row echelon form.

Because the spaces $\text{L}(A)$ and $\text{L}(B)$ are themselves vector spaces, we can define linear operators that act on them.

Definition 2.1.11 (Operators of Operators)**.** Let A and B be vector spaces over the field $\mathcal{R}$. We define $\text{T}(A, B) = \text{L}(\text{L}(A), \text{L}(B))$. Also we denote $\text{T}(A) = \text{T}(A, A)$.

Like "regular" linear operators, they have dual operators, kernels, images, and pre-images. For clarity, we call the identity operator on $\text{T}(A)$, id_A. One of the most important Operators of Operators is the trace.

Definition 2.1.12 (Trace)**.** Let A be an n dimensional vector space over the field $\mathcal{R}$. The *trace*, is the linear operator denote $\text{tr} \in \text{T}(A, \mathcal{R})$.[1] For all $F \in \text{L}(A)$

$$\text{Tr}[F] = \sum_{i=1}^{n} F_{i,i}. \tag{2.11}$$

2.1.2 Direct and Tensor Products

Definition 2.1.13 (Direct Product)**.** Let A and B be vector spaces over the field $\mathcal{R}$. We define the (external) *direct product* of A and B is denoted as $A \oplus B$. The vector space is over the set $A \times B$ and for all $a, a' \in A$, $b, b' \in B$ and $r \in \mathcal{R}$

$$r(a, b) + (a', b') = (ra + a', rb + b'). \tag{2.12}$$

In essence, the direct product is just the natural way of building a vector space for the Cartesian product. We typically denote the pairs (a, b) as $a \oplus b$. If we let $\{e_i\}_{i=1,\ldots,n}$ and $\{e_j\}_{j=1,\ldots,n}$ be the canonical bases of A and B respectively, then

$$\{e_i \oplus 0\}_{i=1,\ldots,n} \cup \{0 \oplus e_j\}_{j=1,\ldots,m}, \tag{2.13}$$

is a basis for $A \oplus B$.

[1] $\text{T}(\mathcal{R}) \simeq \text{L}(\mathcal{R}) \simeq \mathcal{R}$ and we refer to them interchangeably.

Remark 2.1.14. *Let C be a vector space over the field $\mathcal{R}$. Let $A, B \subset C$ such that $A \cap B = \{0\}$ and $A + B = C$ Then, $A \oplus B \simeq C$ and for all $a \in A$ and $b \in B$, $a \oplus b \simeq a + b$.*

This is particularly useful for breaking down vectors into separate components and is featured heavily in Chapters 3 and 4.

Definition 2.1.15 (Tensor Product)**.** Let A and B be vector spaces over the field $\mathcal{R}$. We define the vector space $A \otimes B$ (or just AB for short) as

$$A \otimes B = \text{span}\left(\{a \otimes b | a \in A, b \in B\}\right), \tag{2.14}$$

where $\otimes : A \times B \to AB$ is a bilinear function such that for any vector space C and any bilinear function $f : A \times B \to C$ there exists a unique linear map $f' : AB \to C$ such that $f' \circ \otimes = f$.

If we let $\{e_i\}_{i=1,\ldots,n}$ and $\{e_j\}_{j=1,\ldots,n}$ be the canonical bases of A and B respectively, then

$$\{e_i \otimes e_j\}_{i=1,\ldots,n,\ j=1,\ldots m}, \tag{2.15}$$

is a basis for $A \otimes B$.

For both the direct and tensor product, strictly speaking $A \oplus B \neq B \oplus A$ and $A \otimes B \neq B \otimes A$, however they are isomorphic, and we can convert from one to the other by linear transformation. As such, when we give a subscripts for the systems we make the slight abuse of notation and say $\vec{a}_A \otimes \vec{b}_B = \vec{b}_B \otimes \vec{a}_A$.

We can now define one of the most useful operators of operators, the partial trace.

Definition 2.1.16. Let A and B be n and m dimensional vector spaces over the field $\mathcal{R}$. Let $\rho_{AB} \in AB$, and the matrix representation

$$\rho_{AB} = \sum_{i,i'=1}^{n} \sum_{j,j'=1}^{m} \rho_{i,j,i',j'} \vec{e}_i \vec{e}_{i'}^{\mathrm{T}}{}_A \otimes \vec{e}_j \vec{e}_{j'}^{\mathrm{T}}{}_B. \tag{2.16}$$

We define the *partial trace*, as the operator $\text{Tr}_A \in \text{T}(AB, B)$ given by[2]

$$\text{Tr}_A[\rho_{AB}] = \sum_{j,j'=1}^{m} \left(\sum_{i,i'=1}^{n} \rho_{i,j,i',j'} \right) \vec{e}_j \vec{e}_{j'}^{\mathrm{T}}{}_B, \tag{2.17}$$

[2]Technically, we have to convert the output back into an operator, but those are just little details.

and define $\rho_B = \mathrm{Tr}_A[\rho_{AB}]$.

2.2 Hilbert Spaces and the Fundamentals of Quantum

With the basics of vector spaces established, we move to inner product and Hilbert spaces, which form the fundamental language of quantum mechanics. Material in this section is primarily based on the introductory quantum information and computing books [12, 19, 20][3].

Definition 2.2.1. Let A be a vector space over the field $\mathbb{C}$. A function $\langle \cdot, \cdot \rangle : A \times A \to \mathbb{C}$ is an *inner product*, if it satisfies for all $a, b, c \in A$ and $\alpha \in \mathbb{C}$:

1. $\langle a, b \rangle = \langle b, a \rangle^*$,
2. $\langle a, \alpha b \rangle = \alpha \langle a, b \rangle$,
3. $\langle a, b + c \rangle = \langle a, b \rangle + \langle b, c \rangle$,
4. $\langle a, a \rangle \geq 0$ with equality if and only if $a = 0$.

A vector space equipped with an inner product is called a *inner product space*. Similarly, it is defined for the reals by swapping $\mathcal{C}$ for $\mathcal{R}$.

Commonly, we use the notation $\langle \phi | \psi \rangle$ from Dirac notation for vectors. The inner product space is automatically given the norm $\|\phi\| := \sqrt{\langle \phi | \phi \rangle}$, and the metric for Euclidean distance $\mathrm{d}(\phi, \psi) = \|\phi - \psi\|$.

Definition 2.2.2. For an inner product space A, a *Cauchy sequence* is a sequence $\{|\phi_x\rangle\} \subset A$ such that for any $\epsilon > 0$, there exists an $n \in \mathbb{N}$ such that for all $a, b > n$,

$$\|\phi_a - \phi_b\| < \epsilon. \tag{2.18}$$

Definition 2.2.3. For an inner product space A, A is a *Hilbert space* if for all Cauchy sequences $\{|\phi_x\rangle\} \subset A$, there exists an $\vec{\phi} \in A$ such that $\lim_{x \to \infty} \| |\phi\rangle - |\phi_x\rangle \| = 0$.

[3] Small amounts of notation are borrowed from a yet unpublished textbook by Dr. Gilad Gour which he generously gave us access to. A sample of the notation can be found in [21].

All finite dimensional inner product spaces are isomorphic to either $\mathbb{R}^n$ or $\mathbb{C}^n$. We use the same symbol to refer to a system and the Hilbert space describing it. For example we call Alice's system and the Hilbert space that describes it as A. For a Hilbert space $A = \mathbb{C}^n$, we denote the vectors using as kets so $\phi \in A$ is written as $|\phi\rangle_A$. Furthermore, we denote the canonical basis vectors not as e_i but as $|i\rangle$. We also start indexing at 0 instead of 1.

Unsurprisingly, the space of linear operators between two Hilbert spaces is also a Hilbert spaces. We also upgrade from the regular dual of operators to the *adjoint* of operators. Which is nearly identical to the dual, except we use the inner product instead of bilinear forms. For every vector $|\phi\rangle \in A = \mathbb{C}^n$, we associate with it the functional from the adjoint space $A^\dagger = \mathrm{L}(A, \mathbb{C})$

$$\langle\phi| = \langle\phi|\,(x) = \langle\phi|x\rangle\,, \tag{2.19}$$

which naturally yields an adjoint canonical basis of $\{\langle i|\}_{i=0,\ldots,n-1}$. Furthermore, in Dirac notation we prefer to write operators in inner products as $\langle\phi|M|\psi\rangle$ instead of $\langle\phi, M\psi\rangle$. We also break down there components into a matrix given by

$$M = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} m_{i,j}\,|i\rangle\langle j|\,, \tag{2.20}$$

with $m_{i,j} = \langle i|M|j\rangle$. Using this, the trace takes on the simple form $\mathrm{Tr}[\rho] = \sum_i \langle i|\rho|i\rangle$.

Definition 2.2.4. Let $M \in \mathrm{L}(A, B)$ the *adjoint* of M, denoted as $M^\dagger$ is the unique operator satisfying for all $a \in A$, and $b \in B$,

$$\langle M^\dagger b, a\rangle = \langle b, Ma\rangle. \tag{2.21}$$

For matrices, $M^\dagger$ is just the complex conjugate transpose. With the adjoint operators, we construct the inner product for $\mathrm{L}(A, B)$ as $\langle M, N\rangle = \mathrm{Tr}\big[M^\dagger N\big]$ for all $M, N \in \mathrm{L}(A, B)$.

With Hilbert spaces, we also have many more useful and interesting types of linear operators.

Definition 2.2.5 (Types of Linear Operators)**.** We define the following special types of Linear operators:

Normal $M \in \mathrm{L}(A)$ is *normal* if $M^\dagger M = MM^\dagger$.

Hermitian $M \in \mathrm{L}(A)$ is *Hermitian* if $M^\dagger = M$. The set of all Hermitian operators is denoted as,

$$\mathrm{Herm}(A) := \left\{ M \in \mathrm{L}(A) \middle| M = M^\dagger \right\}. \tag{2.22}$$

Positive semidefinite $M \in \mathrm{L}(A)$ is *positive semidefinite* if for all $|\psi\rangle \in A$, $\langle\psi|M|\psi\rangle \geq 0$. The set of all Positive semidefinite operators is denoted as,

$$\mathrm{Pos}(A) := \{ M \in \mathrm{L}(A) | \forall\, |\psi\rangle \in A,\, \langle\psi|M|\psi\rangle \geq 0 \}. \tag{2.23}$$

Projection $M \in \mathrm{Pos}(A)$ is a *projection* if $M^2 = M$. The set of projection operators is,

$$\mathrm{Proj}(A) := \left\{ M \in \mathrm{Pos}(A) \middle| M^2 = M \right\}. \tag{2.24}$$

Density operator $\rho \in \mathrm{L}(A)$ is a *density operator* if $\rho \in \mathrm{Pos}(A)$ and $\mathrm{Tr}[\rho] = 1$. The set of density operators is,

$$\mathrm{D}(A) := \{ \rho \in \mathrm{Pos}(A) | \mathrm{Tr}[\rho] = 1 \}. \tag{2.25}$$

Unitary $U \in \mathrm{L}(A)$ is *Unitary* if $UU^\dagger = U^\dagger U = I$ (ie. $U^{-1} = U^\dagger$). The set of unitary operators is thus,

$$\mathrm{U}(A) := \left\{ U \in \mathrm{L}(A) \middle| UU^\dagger = U^\dagger U = I \right\}. \tag{2.26}$$

Isometry $V \in \mathrm{L}(A, B)$ is an *isometry* if $V^\dagger V = I_A$. The set of isometry operators is,

$$\mathrm{U}(A, B) := \left\{ V \in \mathrm{L}(A, B) \middle| V^\dagger V = I_A \right\}. \tag{2.27}$$

Note that Hermitian, positive semidefinite, projection, density, and unitary operators are all sets of normal operators. Therefore, the spectral decomposition theorem is particularly useful.

Theorem 2.2.6 (Spectral Decomposition)**.** *Let $M \in \mathrm{L}(A)$ be a normal operator, then there exists an integer $k \in \mathbb{Z}$, a set of distinct eigenvalues $\{\lambda_i\}_{i=1,\ldots,k}$ and projectors $\{P_i\}_{i=1,\ldots,k}$ with $\sum_i P_i = I$, such that [19]*

$$M = \sum_{i=1}^{k} \lambda_i P_i. \tag{2.28}$$

Each eigenvalue has multiplicity equal to the rank of its projector. This form of the spectral decomposition is unique. Most importantly, it lets us extend complex functions, $f : \mathbb{C} \to \mathbb{C}$, to functions on normal operators. Namely, $f(M) = \sum_{i=1}^{k} f(\lambda_i) P_i$.

Theorem 2.2.7. *Let $U \in \mathrm{U}(A)$, $V \in \mathrm{U}(A, B)$, and $f : \mathcal{C} \to \mathcal{C}$, then [19]*

$$f(UMU^\dagger) = U f(M) U^\dagger. \tag{2.29}$$

If $f(0) = 0$, we extend this to

$$f(VMV^\dagger) = V f(M) V^\dagger. \tag{2.30}$$

From the definition of density operators, we can define quantum states as mathematical objects.

Definition 2.2.8 (States)**.** In quantum mechanics a *state* in a system A is any element from $\mathrm{D}(A)$. Furthermore, a state $\rho_A \in \mathrm{D}(A)$ is *pure* if $\mathrm{rank}(\rho_A) = 1$. Otherwise the state is called *mixed*.

For any state $\rho_A \in \mathrm{D}(A)$, if ρ_A is pure, then there exists a state $|\rho\rangle_A \in A$ such that $\rho_A = |\rho\rangle\langle\rho|_A$. We often also refer to $|\rho\rangle_A$ as the state. When normalization is not a concern, we may relax the normalization and call any positive semidefinite operator, or vector a state. Given a preferred basis (typically just the canonical basis), we call a state *classical* if it is diagonal in the preferred basis.

2.2.1 Multipartite Systems

The tensor product of Hilbert spaces is itself a Hilbert space. If A and B are Hilbert spaces, then we equip AB with the inner product $\langle a_1 \otimes b_1, a_2 \otimes b_2\rangle = \langle a_1, b_1\rangle\langle a_2, b_2\rangle$, where $a_1, a_2 \in A$ and $b_1, b_2 \in B$. In Dirac notation, with $|a\rangle_A \in A$ and $|b\rangle_B \in B$, we shorten $|a\rangle_A \otimes |b\rangle_B$ to $|a\rangle_A |b\rangle_B$ or even $|a, b\rangle_{AB}$.

Definition 2.2.9 (Pure Entangled and Separable States)**.** Let $|\psi\rangle_{AB} \in AB$. $|\psi\rangle_{AB}$ is called *separable* if it can be written as $|\psi\rangle_{AB} = |a, b\rangle_{AB}$ for some $|a\rangle \in A$ and $|b\rangle \in B$. Otherwise, $|\psi\rangle_{AB}$ is called *entangled*.

We can extend this to all positive semidefinite operators on AB.

Definition 2.2.10 (Mixed Entangled and Separable States)**.** Let $\psi_{AB} \in \mathrm{Pos}(AB)$. $\psi_A B$ is called *separable* if it can be written in the form $\psi_{AB} = \sum_i r_i \phi_{A,i} \otimes \varphi_{B,i}$, where $r_i \geq 0$, $\{\phi_{A,i}\}_i \subset \mathrm{Pos}(A)$, and $\{\varphi_{B,i}\}_i \subset \mathrm{Pos}(B)$. Otherwise, ψ_{AB} is called *entangled*.

We also define the canonical (unnormalized) maximally entangled state

$$\left|\phi^+\right\rangle_{A\tilde{A}} = \sum_{i=0}^{|A|-1} |i,i\rangle_{A\tilde{A}}\,. \tag{2.31}$$

Any mixed state can be viewed as a pure state entangled with some inaccessible system.

Theorem 2.2.11. *Let $|\rho\rangle_{AB} \in \mathrm{L}(AB)$, then there exists a matrix $M \in \mathrm{L}(A,B)$ such that $|\rho\rangle_{AB} = I_A \otimes M \left|\phi^+\right\rangle_{A\tilde{A}}$, and $\tilde{A}$ is a Hilbert space with $\dim(A) = \dim(\tilde{A})$. Furthermore, $|\rho\rangle_{AB} = M^T \otimes I_B \left|\phi^+\right\rangle_{\tilde{B}B}$.*

Definition 2.2.12. Let $\rho_A \in \mathrm{D}(A)$. A state $|\psi\rangle_{AE} \in AE$, is called a *purification* of ρ_A if,

$$\mathrm{Tr}_E[|\psi\rangle\langle\psi|_{AE}] = \rho_A. \tag{2.32}$$

Note that if a state is pure if and only if its purification is separable.

Theorem 2.2.13. *For any $\rho_A \in \mathrm{Pos}(A)$, there is the purification*

$$|\rho\rangle_{A\tilde{A}} = \sqrt{\rho_A} \otimes I_{\tilde{A}} \left|\phi^+\right\rangle_{A\tilde{A}} \tag{2.33}$$

and all other purifications with a system B can be written in the form

$$|\rho\rangle_{AB} = \sqrt{\rho_A} \otimes V \left|\phi^+\right\rangle_{A\tilde{A}}, \tag{2.34}$$

for any isometry $V \in \mathrm{U}(\tilde{A}, B)$.

Often we require a system A to be broken into n smaller identically sized systems. We refer to these systems as $A_1, A_2, \ldots, A_n$. When we need to specify a subset of these starting from system i to system j we denote $A_i^j = A_i A_{i+i} \ldots A_j$. For example, $A = A_1^n$.

Furthermore, given an alphabet $\mathcal{R}$, with $|\mathcal{R}| = \dim(A)$, and $\vec{l} \in \mathcal{R}^n$, we define

$$\left|\vec{l}\right\rangle_A = \bigotimes_{i=1}^{n} |l_i\rangle_{A_i} . \tag{2.35}$$

If the alphabet $\mathcal{R}$ represents a finite field, then for any operator (given in matrix form) $M \in \mathcal{R}^{m\times n}$ we give the m tensored state $\left|M\vec{l}\right\rangle$. From this we get a special case for invertable matrices in the following definition.

Definition 2.2.14. Let $\mathcal{R}$ be a finite field and A_1 a Hilbert space with orthonormal basis $\{|l\rangle\}|_{l\in\mathcal{R}}$. Let $M \in \mathrm{GL}_n(\mathcal{R})$. We define the permutation matrix $U_{A,M} \in \mathrm{U}(A_1^n)$ as

$$U_{A,M} = \sum_{\vec{l}\in\mathcal{R}^n} \left|M\vec{l}\right\rangle\left\langle\vec{l}\right|_A . \tag{2.36}$$

We extend this for multiple spaces of the same size as $U_{AB,M} = U_{A,M} \otimes U_{B,M}$.

Of particular importance are multipartite states where each subsystem is an exact copy of the same state. We call these states *independent and identically distributed* or I.I.D. for short.

Definition 2.2.15. Let $A = A_1^n$ and $\rho_{\mathrm{single}A_1} \in \mathrm{D}(A_1)$. We call the state

$$\rho_A = \bigotimes_{i=1}^{n} \rho_{\mathrm{single}A_i} \tag{2.37}$$

an *independent and identically distributed state* (I.I.D.).

Furthermore, purifications for I.I.D. states are as simple as repeating the purification for the original state.

Theorem 2.2.16. *For $\rho_{singleA_1} \in \mathrm{Pos}(A_1)$, then a purification of the I.I.D. state $\rho_{singleA}^{\otimes n} \in \mathrm{Pos}(A_1^n)$ is the I.I.D. state*

$$\left(\sqrt{\rho_{singleA}} \otimes I_{\tilde{A}} \left|\phi^+\right\rangle_{A\tilde{A}}\right)^{\otimes n} . \tag{2.38}$$

2.2.2 Measurement and Channels

We have established states as density matrices. Now, we establish measurements and actions on states.

The most basic type of measurement is the *projective measurement*. As its name implies, for a state $\rho_A \in A$, a projective measurement projects ρ_A onto subspaces of A. Typically this involves projecting onto a basis of A, but it can be more complex than that. For example, measuring energy levels could have degeneracy. We summarize in the following definition.

Definition 2.2.17. Let $\{P_i\}_{i=1,\dots,n} \subset \mathrm{Proj}(A)$. The set $\{P_i\}_{i=1,\dots,n}$ is called a *projective measurement* if $\langle P_i, P_j \rangle = \delta_{i,j}$ and $\sum_i P_i = I$.

Measuring a state $\rho_A \in \mathrm{D}(A)$ with the projective measurement $\{P_i\}_{i=1,\dots,n}$ produces the outcome i with probability $p_i = \langle P_1, \rho_A \rangle$. With outcome i the state is transformed to $\rho_A^{(i)} = P_i \rho_A P_i / p_i$. Furthermore,we may describe the outcome with a *classical-quantum* state ρ_{XA}, where we have added a register X to store the classical information. The projective measurement is thus[4]

$$\begin{aligned} \rho_{XA} &= \sum_{i=1}^{n} p_i \left|i\right\rangle\!\left\langle i\right|_X \otimes \rho_A^{(i)} \\ &= \sum_{i=1}^{n} \left|i\right\rangle\!\left\langle i\right|_X \otimes P_i \rho_A P_i. \end{aligned} \tag{2.39}$$

A *positive operator valued measure* (POVM) only cares about the classical outcomes, and not the post measurement state. For example, a photon striking a photo detector produces a click signal while the photon is absorbed. A POVM is formally described by:

Definition 2.2.18. Let $\{E_i\}_{i=1,\dots,n} \subset \mathrm{Pos}(A)$. $\{E_i\}_{i=1,\dots,n}$ is a *POVM* if $\sum_{i=1}^{n} E_i = I$.

When measuring a state $\rho_A \in \mathrm{D}(A)$, with a POVM $\{E_i\}_{i=1,\dots,n}$, the classical outcome i

[4]Sometimes, the projection refers to only the classical register X, or only the quantum register A. In those situations, trace out other register.

occurs with probability $p_i = \langle E_i, \rho_A \rangle$. We can describe the post measurement state ρ_X as

$$\begin{aligned} \rho_X &= \sum_{i=1}^{n} p_i \left|i\right\rangle\!\left\langle i\right|_X \\ &= \sum_{i=1}^{n} \mathrm{Tr}[E_i \rho_A] \left|i\right\rangle\!\left\langle i\right|_X . \end{aligned} \tag{2.40}$$

Granted a large supply set of the same state ρ_A, applying the same POVM to each copy will build a set of statistics that give some information on ρ_A. However, not all POVMs will give enough information to fully reconstruct ρ_A. For a system A, $\mathrm{Herm}(A)$ is a Hilbert space over the field $\mathbb{R}$, with $\dim_{\mathbb{R}}(\mathrm{Herm}(A)) = \dim(A)^2$. Now $\mathrm{D}(A)$ is a subset of $\mathrm{Pos}(A)$ and $\mathrm{span}_{\mathbb{R}}(\mathrm{Pos}(A)) = \mathrm{Herm}(A)$. Therefore, we can fully describe any $\rho_A \in \mathrm{D}(A)$ by using a POVM that spans all Hermitian operators. More formally:

Definition 2.2.19. A POVM $\{E_i\}_{i=1,\ldots,n} \subset \mathrm{Pos}(A)$ is called *informationally complete* if [22]

$$\mathrm{span}_{\mathbb{R}}(\{E_i\}_{i=1,\ldots,n}) = \mathrm{Herm}(A). \tag{2.41}$$

We would now like a way to describe all physical evolution of states. To do so we work with operators of operators. For example, a projective and POVM measurements on the system A can be viewed as elements from $\mathrm{T}(A, AX)$ and $\mathrm{T}(A, X)$ respectively. In order to determine what elements of $\mathrm{T}(A, B)$ represent physical processes, we first need to define some special properties elements of $\mathrm{T}(A, B)$ can have.

Definition 2.2.20. Let $\Phi_{A\to B} \in \mathrm{T}(A, B)$. $\Phi_{A\to B}$ is called *trace non-increasing* (TNI) if for all $\rho_A \in \mathrm{Herm}(A)$,

$$\mathrm{Tr}[\Phi_{A\to B}(\rho_A)] \leq \mathrm{Tr}[\rho_A], \tag{2.42}$$

and *trace preserving* (TP) for equality.

For a process to be physical, it must take in density matrices and return density matrices. Therefore, it must be trace preserving.

Definition 2.2.21. Let $\Phi_{A\to B} \in \mathrm{T}(A, B)$. $\Phi_{A\to B}$ is called *positive*, if for all $\rho_A \in \mathrm{Pos}(A)$, $\Phi(\rho_A) \in \mathrm{Pos}(B)$.

This means that the process takes in positive semidefinite operators, and returns positive semidefinite operators, *but*, because of entanglement this is not guaranteed to hold if $\Phi_{A\to B}$ only acts on a sub system. To capture this, we define the *completely positive* operators.

Definition 2.2.22. Let $\Phi_{A\to B} \in \mathrm{T}(A, B)$, and $\tilde{A}$ a system the same size as A. $\Phi_{A\to B}$ is called *completely positive* (CP) if for all $\rho_{A\tilde{A}} \in \mathrm{Pos}(A\tilde{A})$, $(\mathrm{id}_A \otimes \Phi_{\tilde{A}\to B})(\rho_{A\tilde{A}}) \in \mathrm{Pos}(AB)$.

We bring these together to define describe physical processes.

Definition 2.2.23. A process $\Phi_{A\to B} \in \mathrm{T}(A, B)$ is called a *quantum channel* and represents a physical process if $\Phi_{A\to B}$ if it is CP and TP.[5]

Theorem 2.2.24 (Stinespring Representations)**.** *For every channel $\Phi_{A\to B} \in \mathrm{T}(A, B)$ there exists an ancillary system E and a unitary matrix $U \in \mathrm{U}(A, BE)$ such that*

$$\Phi_{A\to B}(\rho_A) = \mathrm{Tr}_E[U\rho_A U^\dagger]. \tag{2.43}$$

In this way quantum channels can be thought of as interactions between the system and the environment, followed by loosing access to information in the environment. Note that in the Stinespring representation, every isometry U defines a channel, but U is not unique.

Alternatively, we can use the Kraus operator representation for quantum channels.

Definition 2.2.25 (Kraus Operators)**.** Let $\Phi_{A\to B} \in \mathrm{T}(A, B)$. There exists a set of operators $\{K_i\}_{i=1,\ldots,n} \subset \mathrm{L}(A, B)$ called *Kraus operators* such that $\sum_{i=1}^n K_i^\dagger K_i = I_A$ and

$$\Phi_{A\to B}(\rho_A) = \sum_{i=1}^n K_i \rho_A K_i^\dagger. \tag{2.44}$$

Just like the Stinespring representation, every set of Kraus operators represents a channel, but they are not unique. Furthermore, given a channel in its Stinespring representation with the isometry $U \in \mathrm{U}(A, BE)$, then we can construct a Kraus representation for it using Kraus operators of the form $K_i = (I_B \otimes \langle i|_E)U$.

[5]For a fast way to determine if a process is CPTP map, use the Choi-Jamiolkowski isomorphism [19].

2.3 Information Theory

Here we briefly describe entropic quantities used to quantify the information between multiple parties. We start with classical information, then move to quantum information. This section is primarily based on [12, 13, 19].

2.3.1 Classical information and Shannon Entropy

Shannon entropy measures the average uncertainty of an event drawn from a predefined distribution. Events that are more likely contain little information and contribute little uncertainty [13, 19]. Let $\mathbb{R}_{\geq 0}$ be the set of non negative real numbers. We start by defining the following simple function.

Definition 2.3.1. Let $x \in \mathbb{R}_{\geq 0}$, then

$$\mathrm{Q}(x) = -x \log(x). \tag{2.45}$$

Here the logarithm is taken as base 2 to measure information in bits, and $0 \log(0)$ is taken as 0.

Definition 2.3.2 (Shannon entropy)**.** Let X be a random variable on the finite alphabet $\mathcal{X}$ with probabilities $\{p_x\}_{x \in \mathcal{X}}$. The *Shannon entropy* of X is,

$$\mathrm{H}(X) := -\sum_{x \in \mathcal{X}} p_x \log(p_x). \tag{2.46}$$

Here the logarithm is taken as base 2 to measure information in bits, and $0 \log(0)$ is taken as 0.

Often we need to break down entropy calculations and split them into unnormalized distributions. For this purpose we extend Shannon entropy as follows:

Definition 2.3.3. Let $\mathcal{X}$ be a finite alphabet and $X \subset \mathbb{R}_{\geq 0}$ with $X = \{q_x\}_{x \in \mathcal{X}}$. We define the Shannon entropy of X as

$$\mathrm{H}(X) := -\sum_{x \in \mathcal{X}} q_x \log(q_x). \tag{2.47}$$

Definition 2.3.4 (Joint entropy)**.** Let X and Y be random variables on finite alphabets $\mathcal{X}$ and $\mathcal{Y}$, with a joint probability distribution $\{p_{x,y}\}_{x\in\mathcal{X},y\in\mathcal{Y}}$, the joint entropy is

$$\mathrm{H}(X,Y) := -\sum_{x\in\mathcal{X},y\in\mathcal{Y}} p_{x,y}\log(p_{x,y}). \tag{2.48}$$

Definition 2.3.5 (Conditional entropy)**.** Let X and Y be random variables, the condition entropy of X given Y is

$$\mathrm{H}\left(X|Y\right) := \mathrm{H}(X,Y) - \mathrm{H}(Y), \tag{2.49}$$

We adopt the same formulation for joint and conditional entropy for unnormalized distributions.

A few properties of the Shannon entropy can be derived by using properties of logarithms.

Theorem 2.3.6 (Common properties of entropy)**.** *Let $X, Y \subset \mathbb{R}_{\geq 0}$ with finite number of elements. Then for the Cartesian product the following holds*

$$\mathrm{H}(X\times Y) = \left(\sum_{x\in X} x\right)\mathrm{H}(Y) + \left(\sum_{y\in Y} y\right)\mathrm{H}(X), \tag{2.50}$$

$$\mathrm{H}\left(X^n\right) = n\left(\sum_{x\in X} x\right)^{n-1}\mathrm{H}(X). \tag{2.51}$$

Furthermore, let $\pi \in \mathrm{S}_{|X|}$ be a permutation of the set X, then

$$\mathrm{H}(\pi(X)) = \mathrm{H}(X). \tag{2.52}$$

Definition 2.3.7 (Binary entropy)**.** For a probability $0 \leq p \leq 1$ the binary entropy of p is

$$\mathrm{h}(p) := \mathrm{H}(\{p, 1-p\}). \tag{2.53}$$

Classical Error Correction

Here we give an overview of classical linear error correcting codes. A basic familiarity of classical linear error correcting codes is useful for building intuition for reduction matrices

studied in Chapters 3 and 4, which are related to parity check matrices. This section draws heavily from Section 10.4.1 of [12]. Here we give error correcting codes for the field $\mathbb{Z}_2$, but it is possible to generalize this for other finite fields with only a few tweaks.

An error correcting code seeks to take a message $\vec{x} \in \mathbb{Z}_2^k$ and encode it in n bits in such a way that if a small number of error occur, they can be detected and corrected. A code that achieves this is called an $[n, k]$ linear error correcting code and is represented by a matrix $G \in \mathbb{Z}_2^{n\times k}$ and the code word is thus $G\vec{x}$. For the most basic example, the $[3, 1]$ error correcting code given by

$$G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \tag{2.54}$$

takes in a single bit and repeats it 3 times. If a single error occurs, then it can be corrected by checking if the majority of the bits are 0 or 1. We assume that G is full rank and has no rows of all zeros. For more complex codes, it is difficult to easily pick out where error likely occurred. To do so, we use what is called a *parity check matrix*.

Definition 2.3.8. Let $G \in \mathbb{Z}_2^{n\times k}$ be the generator matrix of a $[n, k]$ code. The *parity check matrix* $H \in \mathbb{Z}_2^{n-k\times n}$ is the matrix such that $HG = 0$. In other words, the rows of H are a basis for $\ker(G)$.[6]

If Alice sends an encoded message $G\vec{x}$, and the i^{th} bit flips, then the Bob receives $G\vec{x} + \vec{e}_i$. When Bob applies the parity check matrix, he gets

$$H(G\vec{x} + \vec{e}_i) = H\vec{e}_i, \tag{2.55}$$

called the *syndrome*, which uniquely identifies the single error. Bob then corrects his message to the closest code word. Typically, generator matrices are given in the standard form

$$G = \begin{bmatrix} G' \\ I_k \end{bmatrix}, \tag{2.56}$$

where $G' \in \mathbb{Z}_2^{n-k\times k}$. The corresponding parity check matrix is then simply given by

$$H = \begin{bmatrix} I_{n-k} & -G' \end{bmatrix}. \tag{2.57}$$

[6]Later in Chapters 3 and 4, we will modify parity matrices and use them as the basis for our pre-privacy amplification.

There are still two outstanding questions:

1. What is the "closest" code word?
2. How many errors can a code tolerate?

To construct a notion of distance, we use the *Hamming weight* defined bellow.

Definition 2.3.9 (Hamming weight)**.** Let $\mathcal{A}$ be an alphabet with an element called zero, and let $\vec{a} \in \mathcal{A}^n$. The *Hamming weight* of $\vec{a}$ is the number of non-zero entries in $\vec{a}$. We denote it as $\mathrm{d}(\vec{a})$.

The distance between two strings $\vec{a}$ and $\vec{b}$ is thus $\mathrm{d}(\vec{a} - \vec{b})$, which counts the number of entries the two strings differ. To determine how many error a generator matrix can correct, we need to know the minimum distance between code words.

Definition 2.3.10. Let $G \in \mathbb{Z}_2^{n\times k}$ be a generator matrix. The code distance of G is defined as

$$\mathrm{d}(G) = \min_{\vec{x}\in\mathbb{Z}_2^k, \vec{x}\neq 0} \mathrm{d}(G\vec{x}). \tag{2.58}$$

With this, an error correcting code can only correct errors that are up to half the distance between separate code words, and we formally state this with the the following theorem.

Theorem 2.3.11. *Let $G \in \mathbb{Z}_2^{n\times k}$ be a generator matrix. Then the code given by G can always correct up to $\lfloor \frac{\mathrm{d}(G)-1}{2} \rfloor$ errors.*

2.3.2 Von Neumann Entropy

The Shannon entropy is extended to quantum states via the von Neumann Entropy defined as:

Definition 2.3.12. Let $\rho_A \in \mathrm{D}(A)$, the von Neumann entropy of ρ_A is

$$\mathrm{H}(A) = \mathrm{H}(\rho_A) := -\operatorname{Tr}[\rho_A \log(\rho_A)]. \tag{2.59}$$

This naturally extends to all $\rho_A \in \mathrm{Pos}(A)$ for unnormalized states [19].

The intuition for this is as follows. A pure state is fully determined, and given a measurement in a suitable basis, the result will always be the same. Therefore, the state should have 0 entropy. Density matrices can be viewed as classical mixtures (convex combinations) of pure states. So naturally, the maximally mixed state, which produces a uniform distribution no mater what projection is used, should have the highest entropy. applying the function $Q(x) = -x\log(x)$ at the heart of Shannon entropy to density matrices is a fitting extension. Taking the trace provides the sum seen in the original Shannon entropy. This leads to the following theorem.

Theorem 2.3.13. *Let $\rho_A \in \mathrm{Pos}(A)$, with eigenvalues $\{\rho_i\}_{i=1,\dots,n}$, then the von Neumann Entropy of ρ_A reduces to*

$$\mathrm{H}(\rho_A) = \mathrm{H}\left(\{\rho_i\}_{i=1,\dots,n}\right). \tag{2.60}$$

Theorem 2.3.14. *Let $\rho_A \in \mathrm{Pos}(A)$, $\sigma_B \in \mathrm{Pos}(B)$, and $V \in \mathrm{U}(A,C)$ then the following hold:*

$$\mathrm{H}(\rho_A \otimes \sigma_B) = \mathrm{Tr}[\rho_A]\,\mathrm{H}(\sigma_B) + \mathrm{Tr}[\sigma_B]\,\mathrm{H}(\rho_A), \tag{2.61}$$

$$\mathrm{H}(\rho_A^{\otimes n}) = n\,\mathrm{Tr}[\rho_A]^{n-1}\,\mathrm{H}(\rho_A), \tag{2.62}$$

$$\mathrm{H}(V\rho_A V^\dagger) = \mathrm{H}(\rho_A). \tag{2.63}$$

Proof. The first two are just simple extensions of the properties from Theorem 2.3.6. The third property can be derived in two ways:

1. Eigenvalues are invariant under isometries,[7] and by Theorem 2.3.13 the entropy must be the same.
2. Use Theorem 2.2.7 on $Q(x) = -x\log(x)$, so $\mathrm{Tr}\left[Q(V\rho V^\dagger)\right] = \mathrm{Tr}\left[VQ(\rho)V^\dagger\right] = \mathrm{H}(\rho)$.

□

Theorem 2.3.15. *Let $\rho_A \in \mathrm{Pos}(A)$ with a block diagonal decomposition given by $\rho_A = \bigoplus_i \rho_i$, then the von Neumann entropy is given by*

$$\mathrm{H}(\rho_A) = \sum_i \mathrm{H}(\rho_i). \tag{2.64}$$

[7] The multiplicity of the eigenvalue 0 may change, but $\mathrm{Q}(0) = 0$ so it does not mater how large of space we embed the state in.

One of the most used cases for this theorem is when ρ_A has the form $\rho_A = \sum_i \rho_i \otimes |i\rangle\langle i|$, then we get the entropy

$$\mathrm{H}\left(\sum_i \rho_i \otimes |i\rangle\langle i|\right) = \sum_i \mathrm{H}(\rho_i). \tag{2.65}$$

Definition 2.3.16. Let $\rho_A \in \mathrm{Pos}(A)$, $\{\rho_i\}|_{i=1}^n \subset \mathrm{Pos}(A)$, and $Z = \{z_i\}_{i=1}^n \in \mathbb{R}$ be non-negative numbers, such that $\rho_A = \sum_i z_i \rho_i$, then the *Holevo quanity* of ρ_A is given by

$$\begin{aligned} \chi(Z : A) &:= \mathrm{H}(\rho_A) - \sum_i z_i \, \mathrm{H}(\rho_i) \\ &= \mathrm{H}(\rho_A) + \mathrm{H}(Z) - \sum_i \mathrm{H}(z_i \rho_i). \end{aligned} \tag{2.66}$$

2.4 Basics of QKD

A quantum key distribution (QKD) protocol is a method for constructing a secret key between two parties [4, 5, 6]. The sender (Alice) and the receiver (Bob) use an imperfect quantum channel and an authenticated classical channel to grow and construct secret keys. For a well designed protocol, the no-cloning theorem ensures that an eavesdropper (Eve) cannot learn information about exchanges over the quantum channel without altering the signals sent.[8] Alice and Bob can detect this interference and choose to abort the protocol or use techniques like privacy amplification to reduce Eve's information.

QKD protocols are typically split into prepare and measure based schemes and entanglement based schemes. The outline of both schemes is relatively similar so we give the steps for an entanglement based scheme and show how to reduce prepare and measure based to entanglement based. For an entanglement based scheme, A QKD protocol typically operates as follows:[9]

Prepare and transmit signal An untrusted 3$^{\text{rd}}$ party prepares entangled pairs from a predefined list of signals. Half of each pair is sent to Alice, and the other half is sent to Bob.

[8] For finite size key lengths this becomes a chance of failure. See [6] for more details.

[9] This outline only applies to the asymptotic limit. Finite size security proofs have significantly stricter layouts and must be closely adhered to [23].

Measurement Alice and Bob measures the transmitted signals with POVMs and records their outcome.

Parameter estimation Alice and Bob split off a random set of their data and announce their measurement outcomes. From this they can estimate the shared random state they hold.[10]

Sifting Alice and Bob bin their data based on public announcements made. Alice and Bob remove bins based on a predetermined list. For example, results measured in different basis choices are likely to have little to no correlation and a protocol would place them on a list for removal.

Key mapping For each bin, Alice maps her outcomes to a raw key based on a predefined function. Alternative approaches which require additional communication between Alice and Bob are not covered in this thesis.

Error correction From parameter estimation, Alice prepares and sends information for a one-way, linear error correcting code so Bob can correct for errors in transmission. This leaks information to Eve and additional privacy amplification is required. Two-way error correction and/or non linear error correcting codes are not covered in this thesis.

Privacy amplification Alice and Bob apply a randomly selected function from a family of two-universal hash functions to their key. In the asymptotic limit, Eve's correlation with the final key can be completely removed.

2.4.1 Prepare and Measure and the Source Replacement Scheme

For a prepare and measure protocol, Alice controls the source of their quantum states. In this case, Alice randomly selects a state to transmit to Bob from a predefined list, and records her choice. Alice randomly selects a state $|\psi_i\rangle \in A'$ from a pre-selected list of states,

[10] This only applies for asymptotic protocols. For finite size protocols Alice and Bob must check if their results fit within a predefined post-selection set. If not, Alice and Bob abort the protocol. See [23] for more details.

with probability p_i. She prepares the state and records her choice, effectively creating a classical quantum source,

$$\rho_{AA'} = \sum_i |i\rangle\langle i|_A \otimes |\psi_i\rangle\langle\psi_i|_{A'} \,. \tag{2.67}$$

When Alice sends the signal in register A' to Bob, it is assumed that a third party Eve is monitoring the line, and all information lost to the environment is gathered by her [24]. Effectively, for any state $|\psi\rangle\langle\psi|_{A'}$ Alice sends to Bob, Eve performs an isometry $V \in \mathrm{L}(A', B)$, producing a pure state $|\psi'\rangle_{EB} = V|\psi\rangle_{A'}$. Therefore, just before measurement, the three parties share the state

$$\rho_{ABE} = \sum_i |i\rangle\langle i|_A \otimes |\psi_i'\rangle\langle\psi_i'|_{BE} \,. \tag{2.68}$$

All analysis could be performed on this state, but any prepare and measure based protocol can be formulated as an equivalent entanglement based protocol, simplifying the analysis [25]. For the equivalent entanglement based protocol, Alice acting as the 3$^{\text{rd}}$ party prepares the entangled state

$$|\rho\rangle_{AA'} = \sum_i \sqrt{p_i}\,|i\rangle_A \otimes |\psi_i\rangle_{A'} \,. \tag{2.69}$$

When Alice measures with the POVM $\{|i\rangle\langle i|_A\}|_i$, she effectively prepares $|\psi_i'\rangle_{A'}$ for Bob with probability p_i. Because Alice controls the state preparation, Eve cannot change Alice's marginal distribution on her system A. Alice's marginal distribution ρ_A can then be used in parameter estimation. For system A', Eve performs the same isometry as before, producing the shared pure state

$$|\rho\rangle_{ABE} = \sum_i \sqrt{p_i}\,|i\rangle_A \otimes |\psi_i'\rangle_{BE} \,. \tag{2.70}$$

For simplicity, we combine Alice's measurement result with her announcements in the POVM $\{M_{A,x,a}\}|_{x\in\mathcal{X},\alpha\in\mathcal{A}}$ for her outcome $x \in \mathcal{X}$ and announcement $\alpha \in \mathcal{A}$. Furthermore, Schmidt decomposition is often used to reduce the dimensions of Equations (2.69), (2.70), and Alice's measurements.

It is important to note that we always assume that Eve attacks with an isometry as it is the strongest attack she can perform [24]. As such, we assume Eve then holds a

purification. Thankfully, we do not need to specify which purification Eve holds because any purification is related by an isometry, so Eve can freely change her purification at any time. This leads to the fundamental theorem:

Theorem 2.4.1. *The key rate of entanglement based, and prepare and measure schemes are independent of the purification held by Eve. Therefore, any purification can be used in the analysis*[11].

2.4.2 Key Rate format

We now formalize this to produce the key rate formula. Let $\mathcal{X}, \mathcal{A}, \mathcal{Y}, \mathcal{B}$, and $\mathcal{R}$ be finite alphabets where:

- $\mathcal{X}$ and $\mathcal{Y}$ represent Alice and Bob's private measurement information.
- $\mathcal{A}$ and $\mathcal{B}$ represent Alice and Bob's announcements.
- $\mathcal{R}$ are the values the key can take.

Let $\{M_{A,x,\alpha}\}|_{x\in\mathcal{X},\alpha\in\mathcal{A}}$, and $\{M_{B,y,\beta}\}|_{y\in\mathcal{Y},\beta\in\mathcal{B}}$ be Alice and Bob's POVM measurements respectively. The quantum to classical channels are given by:

$$\begin{aligned}\mathcal{E}'_{A\to XC_A}(\rho_A) &= \sum_{x\in\mathcal{X}}\sum_{\alpha\in\mathcal{A}} |x\alpha\rangle\langle x\alpha|_{XC_A} \operatorname{Tr}[M_{A,x,\alpha}\rho_A],\\ \mathcal{E}'_{B\to YC_B}(\rho_B) &= \sum_{y\in\mathcal{Y}}\sum_{\beta\in\mathcal{B}} |y\beta\rangle\langle y\beta|_{YC_B} \operatorname{Tr}[M_{B,y,\beta}\rho_B],\end{aligned} \tag{2.71}$$

for Alice and Bob respectively. After transmission, Alice, Bob and Eve share a pure state described by Equation (2.70). Alice and Bob perform their measurements producing the classical quantum state,

$$\rho_{XYEC} = (\mathcal{E}'_{A\to XC_A}\otimes\mathcal{E}'_{B\to YC_B})(\rho_{ABE}), \tag{2.72}$$

[11] A more formal proof and statement requires analysis of Equation (2.77), but it can be summarized as a result of applying Theorem 2.3.14 to Eve's system.

where $C = C_A C_B$. In the asymptotic limit, the data Alice and Bob reveal for parameter estimation let them construct the observed probability of all outcomes $p(x, y, \alpha, \beta)$. In addition, for prepare and measure protocols, Eve cannot interfere with Alice's measurement, therefore $\mathrm{Tr}_B[\rho_{AB}] = \mathrm{Tr}_{A'}[\rho_{AA'}]$. Alice and Bob bound the possible states they share (and thus any purification Eve holds) to the set

$$\begin{aligned}\Gamma = \big\{\rho_{AB} \in \mathrm{D}(AB) \big|\, & \mathrm{Tr}_B[\rho_{AB}] = \mathrm{Tr}_{A'}[|\rho\rangle\langle\rho|_{AA'}], \\ & p(x, y, \alpha, \beta) = \mathrm{Tr}[(M_{A,x,\alpha} \otimes M_{B,y,\beta})\rho_{AB}], \forall (x, y, \alpha, \beta) \in (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B})\big\}. \quad (2.73)\end{aligned}$$

Let $g : \mathcal{X} \times \mathcal{A} \times \mathcal{B} \to \mathcal{R}$ be the key map Alice uses on her secret data and announcements to set the key. The corresponding channel is

$$\begin{aligned}\mathcal{E}_{XC\to RC}(\rho_{XC}) = \sum_{x\in\mathcal{X}} \sum_{\alpha\in\mathcal{A}} \sum_{\beta\in\mathcal{B}} & |g(x, \alpha, \beta)\rangle\langle g(x, \alpha, \beta)|_R \\ & \otimes |\alpha\beta\rangle\langle\alpha\beta|_C \,\mathrm{Tr}[|x\alpha\beta\rangle\langle x\alpha\beta|_{XC}\, \rho_{XC}]. \quad (2.74)\end{aligned}$$

Given any purification, Alice Bob and Eve share the state

$$\rho_{RYEC} = \mathcal{E}_{XC\to RC} \circ (\mathcal{E}'_{A\to XC_A} \otimes \mathcal{E}'_{B\to YC_B})(\rho_{ABE}). \quad (2.75)$$

Let $\mathcal{S} \subseteq \mathcal{A} \times \mathcal{B}$ be the set of announcements Alice and Bob accept during sifting. For each pair $(\alpha, \beta) \in \mathcal{S}$, Alice and Bob perform error correction on that bin of data, conditioning on the pair of announcements leaking

$$\begin{aligned}\delta^{(\alpha,\beta)}_{\mathrm{leak}} &= f\,\mathrm{H}\left(R|Y, \alpha, \beta\right) \\ &= f\left(\mathrm{H}(R, Y|\alpha, \beta) - \mathrm{H}(Y|\alpha, \beta)\right),\end{aligned} \quad (2.76)$$

using the distribution $p(x, y, \alpha, \beta)$, and where f is the efficiency of error correction compared to the Shannon limit. Here $f = 1$ means that the the error correction scheme is operating at the Shannon limit. For $f > 1$, the error correction has inefficiencies and for every 1 bit required in the Shannon limit, it requires f bits for this error correcting code.

The key rate is then lower bounded by the Devetak-Winter formula[12] [26]

$$\begin{aligned} R &\geq \sum_{(\alpha,\beta)\in\mathcal{S}} p(\alpha,\beta)\left(\mathrm{H}\left(R|\alpha,\beta\right) - \max_{\rho_{AB}\in\Gamma}\chi(R:E|\alpha,\beta) - \delta_{\text{leak}}^{(\alpha,\beta)}\right) \\ &= \sum_{(\alpha,\beta)\in\mathcal{S}} p(\alpha,\beta)\left(\min_{\rho_{AB}\in\Gamma}\left(\sum_{r\in\mathcal{R}}\mathrm{H}\left(p(r|\alpha,\beta)\rho_E^{(r,\alpha,\beta)}\right) - \mathrm{H}\left(\rho_E^{(\alpha,\beta)}\right)\right) - \delta_{\text{leak}}^{(\alpha,\beta)}\right), \end{aligned} \tag{2.77}$$

where, $|\rho\rangle_{ABE}$ is any purification of ρ_{AB}, $\rho_E^{(r,\alpha,\beta)}$ and $\rho_E^{(\alpha,\beta)}$ are the marginal states for Eve conditioned on the announcements and key map results. Here, the second form is constructed by swapping to the second form of Definition 2.3.16 for the Holevo quantity. Alternative, but equivalent formulations include the relative entropy approach often used in numerical key rate calculations [23, 27].

2.4.3 Six-State Protocol

Originally designed by Bruss in 1998 [5], the six-state uses 3 mutually unbiased bases to exchange keys. As a highly symmetric and tomographically complete protocol, it lends itself well to analytic key rate calculations [28], such as the ones in this thesis. Here we provide a description for the six-state protocol with source replacement and Schmidt decomposition to reduce Alice's dimensions.

Prepare and transmit signal Alice prepares many copies of the Bell state $|\Phi^+\rangle_{AA'}$ and sends half of each pair to Bob.

Measurement Alice and Bob each randomly selects a basis from among Z, X, and Y enumerated as 0, 1, and 2. The choices are given with probabilities $\{p(\alpha)\}_{\alpha=0}^{2}$.

Parameter estimation Alice and Bob perform parameter estimation as usual.

Sifting Alice and Bob announce their basis choices and bin their data based on it. They throw away all bins where they measured in different bases.

[12] Stripping back the notation, the Devetak-Winter formula is $R \geq \min_{\rho\in\Gamma}\mathrm{H}\left(R|EC\right) - \mathrm{H}\left(R|YC\right)$. The first term is the worst case senario where Eve has the most information about the key, and the second term is the cost of correcting Bob's raw key.

Key mapping For each bin Alice maps her outcomes 0, +, and L to a raw key bit of 0, and 1, −, and R to a raw key bit of 1.

Error correction Alice and Bob perform the usual error correction.

Privacy amplification Alice and Bob perform the usual privacy amplification.

More formally, Alice starts with the source replacement state

$$|\rho_{\text{single}}\rangle_{AA'} = \left|\Phi^+\right\rangle_{AA'}. \tag{2.78}$$

Here we model the situation when Eve uses a depolarizing channel on the signal transmitted to Bob. Because the six-state protocol is tomographically complete, in the asymptotic limit Alice and Bob can completely characterize Eve's attack and the set Γ becomes a single point. The channel depolarizes by $\xi \in [0,1]$ and is described as

$$\Phi(\rho_{A'}) = (1-\xi)\rho_{A'} + \xi\frac{I_{A'}}{|A'|}. \tag{2.79}$$

Applying this to Alice and Bob's state gives

$$\begin{aligned}\rho_{\text{single}AB} &= (\text{id}_A \otimes \Phi_{A'\to B})(\Phi^+_{AA'}) \\ &= (1-\xi)\Phi^+_{AB} + \xi\frac{I_{AB}}{|AB|} \\ &= \left(1-\frac{3\xi}{4}\right)\Phi^+_{AB} + \frac{\xi}{4}\left(\Phi^-_{AB} + \Psi^+_{AB} + \Psi^-_{AB}\right),\end{aligned} \tag{2.80}$$

and is purified by

$$|\rho_{\text{single}}\rangle_{ABE} = \sqrt{1-\frac{3\xi}{4}}\left|\Phi^+\right\rangle_{AB}|00\rangle_E + \sqrt{\frac{\xi}{4}}\left(\left|\Phi^-\right\rangle_{AB}|01\rangle_E + \left|\Psi^+\right\rangle_{AB}|10\rangle_E + \left|\Psi^-\right\rangle_{AB}|11\rangle_E\right). \tag{2.81}$$

After transmission, Alice and Bob apply their POVM measurements with the quantum to classical channels described in Equation (2.71) with the POVMs

$$\begin{aligned}&M_{A,0,0} = p(\alpha=0)\,|0\rangle\langle 0|_A, \quad M_{A,0,1} = p(\alpha=1)\,|+\rangle\langle +|_A, \quad M_{A,0,2} = p(\alpha=2)\,|L\rangle\langle L|_A, \\ &M_{A,1,0} = p(\alpha=0)\,|1\rangle\langle 1|_A, \quad M_{A,1,1} = p(\alpha=1)\,|-\rangle\langle -|_A, \quad M_{A,1,2} = p(\alpha=2)\,|R\rangle\langle R|_A,\end{aligned} \tag{2.82}$$

and

$$\begin{aligned} M_{B,0,0} &= p(\beta=0)\,|0\rangle\langle 0|_B\,, \quad M_{B,0,1} = p(\beta=1)\,|+\rangle\langle +|_B\,, \quad M_{B,0,2} = p(\beta=2)\,|R\rangle\langle R|_B\,, \\ M_{B,1,0} &= p(\beta=0)\,|1\rangle\langle 1|_B\,, \quad M_{B,1,1} = p(\beta=1)\,|-\rangle\langle -|_B\,, \quad M_{B,1,2} = p(\beta=2)\,|L\rangle\langle L|_B\,. \end{aligned} \tag{2.83}$$

Note that when Alice measures $|L\rangle_A$ she prepares $|R\rangle_{A'}$ for Bob. As such, Alice and Bob's POVM elements for the Y basis are the opposite of each other. Most importantly, Alice and Bob's measurements are tomographically complete, therefore they can determine the exact state they share in the asymptotic limit. Therefore, $\Gamma = \{\rho_{\text{single}AB}\}$ and no convex optimization is needed to determine the key rate. The post-processing set is given by $\mathcal{S} = \{(0,0),(1,1),(2,2)\}$, which is all events where Alice and Bob used the same basis. Alice then Applies the key map $g(x,\alpha,\beta) = x$, effectively relabelling her system X as the key register R.

The symmetry of both the six-state protocol and Eve's attack allows for a significant simplification, which we state in the following theorem.

Theorem 2.4.2. *Let ρ_{AB} be the shared state from Equation (2.80) (depolarized by ξ) and $\alpha \in \mathcal{A}$, then for the six-state protocol*

$$\sum_{r\in\mathcal{R}} \mathrm{H}\left(p(r|\alpha,\alpha)\rho_E^{(r,\alpha,\alpha)}\right) - \mathrm{H}\left(\rho_E^{(\alpha,\alpha)}\right) = \sum_{r\in\mathcal{R}} \mathrm{H}\left(p(r|0,0)\rho_E^{(r,0,0)}\right) - \mathrm{H}\left(\rho_E^{(0,0)}\right), \tag{2.84}$$

and

$$\delta_{leak}^{(\alpha,\alpha)} = \delta_{leak}^{(0,0)}. \tag{2.85}$$

Proof. A simple outline of the proof is as follows. We start by looking at the Alice and Bob's POVMs conditioned on their announcements. We can write them in the form

$$M_{A,x|\alpha} = U_\alpha\,|x\rangle\langle x|\,U_\alpha^\dagger, \quad M_{B,y|\beta} = U'_\beta\,|y\rangle\langle y|\,U'^\dagger_\beta, \tag{2.86}$$

where

$$\begin{aligned} U_0 = U'_0 &= I, \\ U_1 = U'_1 &= |+\rangle\langle 0| + |-\rangle\langle 0|\,, \\ U_2 = |L\rangle\langle 0| + |R\rangle\langle 1|\,,\ U'_2 &= |R\rangle\langle 0| + |L\rangle\langle 1|\,. \end{aligned} \tag{2.87}$$

Now, Alice and Bob share the initial state $\rho_{AB} = (1-\xi)\phi^+_{AB} + \xi\frac{I_{AB}}{|AB|}$, and with little effort

one can show

$$\rho_{AB} = U_\alpha \otimes U'_\alpha \rho_{AB} U_\alpha^\dagger \otimes U_\alpha'^\dagger. \tag{2.88}$$

Therefore, post measurement, Alice and Bob share the exact same statistics as when they both measured in the Z-basis. □

With this theorem, we only need to solve the terms in the Z-basis, then repeat the result for each other basis. With some effort, one can show

$$\sum_{r\in\mathcal{R}} \mathrm{H}\left(p(r|0,0)\rho_E^{(r,0,0)}\right) - \mathrm{H}\left(\rho_E^{(0,0)}\right) = 1 + \mathrm{h}\left(\frac{\xi}{2}\right) - \mathrm{Q}\left(1 - \frac{3\xi}{4}\right) - 3\,\mathrm{Q}\left(\frac{\xi}{4}\right), \tag{2.89}$$

and

$$\delta_{\text{leak}}^{(0,0)} = f\,\mathrm{h}\left(\frac{\xi}{2}\right). \tag{2.90}$$

Overall, the key rate is then given by

$$R \geq \left(\sum_{\alpha\in\mathcal{A}} p(\alpha,\alpha)\right)\left(1 + \mathrm{h}\left(\frac{\xi}{2}\right) - \mathrm{Q}\left(1 - \frac{3\xi}{4}\right) - 3\,\mathrm{Q}\left(\frac{\xi}{4}\right) - f\,\mathrm{h}\left(\frac{\xi}{2}\right)\right). \tag{2.91}$$

2.5 Full and Simplified Trusted Relays

All quantum channels in QKD are vulnerable to noise and loss. For all practical QKD protocols, the noise and loss typically scale with distance. For example, most commercially available optical fibres experience a loss between 0.18dB/km to 0.143dB/km [10]. Furthermore, dark counts, which are caused by a detector randomly clicking when no signal is present, introduce a base level of noise to QKD protocols. Over long distances, loss grows large enough such that the signal to noise ratio from dark counts makes it impossible to extract a secret key [9]. To increase key rate at long distances requires the use of quantum repeaters and relays. Untrusted quantum repeaters and relays require a combination of fault tolerant quantum memory and gates to operate [9]. As such, there are no commercially viable quantum repeaters and relays [10, 11].

Currently, the near future solution is to use a trusted 3$^{\text{rd}}$ party to mediate exchange between Alice and Bob. Multiple trusted 3$^{\text{rd}}$ parties allows for unlimited distance. Because

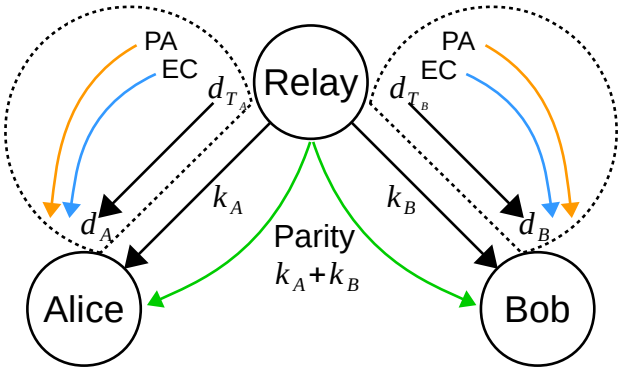


Figure 2.1: Diagram of a full trusted relay.

the relays must be trusted, if even a single relay acts in bad faith, then the entire secret key is compromised. Additionally, high loss and noise still requires many relays to link distant parties, which can quickly grow in cost and complexity. This can be mitigated with trusted relays on satellites as atmospheric loss scales at around 0.07dB/km[13] [10]. Satellites are also visible to large areas at once, allowing for connection to be established without laying down additional optical fibre. Furthermore, low earth orbit satellites allow distant parties to establish a secret key by letting the satellite communicate with one party, then travel and communicate with the other party [10]. Therefore, trusted satellite relays allow for secret key exchange at arbitrary distance with significantly less relays.

In this section we cover two implementations of trusted relays, the common full trusted relay [10, 29, 30], and the proposed simplified trusted relay [1, 15, 16], and focus on the scenario where only a single relay is required.

2.5.1 Full Trusted Relay

For a full trusted relay, the relay performs a full quantum key exchange between itself and Alice, then between itself and Bob, as seen in Figure 2.1. This includes all the privacy amplification and error correction needed between the relay and each party. After the key exchanges, Alice and the relay hold a shared secret key k_A, while Bob and the relay hold a shared secret key k_B. The relay now publicly announces the parity of keys, $k_A + k_B$. Bob then decodes $k_B + (k_A + k_B) = k_A$, giving him Alice's secret key. Effectively the relay used

[13] Though other sources of loss such as beam diffraction mitigate some of the advantage.

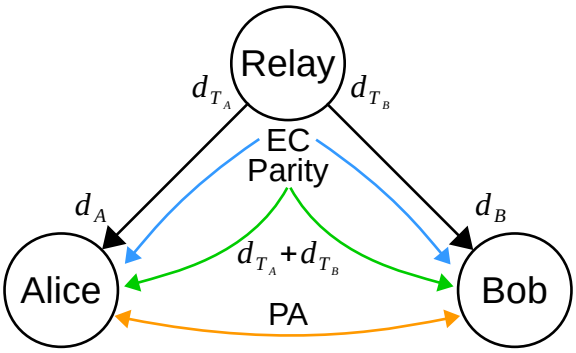


Figure 2.2: Diagram of a simplified trusted relay.

Bob's key k_B to encrypt Alice's key k_A with the one time pad. Equivalently, Alice could decode Bob's key $k_A + (k_A + k_B) = k_B$. By composability of secret keys, Alice and Bob now share an epsilon secure secret key. The overall key rate is then given by whichever link had the worst key rate.

For a cost-effective implementation, the satellite should be exchanging keys continuously between trusted parties. This comes with the major drawbacks of requiring the satellite to have enough computational power and memory to continuously perform two full instances of a quantum key distribution protocol [1, 15]. For ground stations, this cost is trivial, but satellites must be lightweight, power efficient and built to survive the hostile conditions of space, leaving little room for powerful computational devices [14].

2.5.2 Simplified Trusted Relay

Developed by Stacey, et al. [15], the simplified trusted relay (abbreviated STR) aims to reduce the computational burden placed on the satellite at the cost of key rate per bit sent. Unlike the fully trusted relay, the simplified trusted relay passes the computationally expensive task of privacy amplification to Alice and Bob. As depicted in Figure 2.2, the simplified trusted relay performs the quantum phase of the QKD protocol with both parties. Parameter estimation is performed between all parties to characterize all correlations they share. The relay holds the raw keys d_{T_A} and d_{T_B}, while Alice and Bob respectively hold imperfect copies d_A and d_B. The relay then publicly announces the parities of the two raw keys $d_{T_A} + d_{T_B}$. Then based on whichever party has the worst quantum bit error rate, the relay prepares one way linear error correction information which it sends to both

parties.[14] With the error correction information, Alice and Bob correct their raw keys to d_{T_A} and d_{T_B}. Furthermore, the parity announcements let Bob reconstruct the raw secret key $d_{T_B} + (d_{T_A} + d_{T_B}) = d_{T_A}$. Alice and Bob then perform privacy amplification to virtually eliminate Eve's knowledge of the final secret key.

Unlike the full trusted relay, the simplified trusted relay cannot be separated into two distinct key exchanges. This allows Eve multiple attempts to harvest information about the key bits, as well as a joint attack on both links. Furthermore, unlike the full trusted relay's announcement $k_A + k_B$, the simplified trusted relay's announcement $d_{T_A} + d_{T_B}$ uses information already correlated with Eve, giving her more power. As such, Alice and Bob must perform more privacy amplification to protect their final secret key. Although the key rate per *bit* sent is lower, this does not necessarily imply that a simplified trusted relay is slower than a full trusted relay; With significantly less computational burden placed on the relay, practical satellite implementations may run the simplified trusted relay significantly faster than the full trusted relay. For low error rate conditions, Guerrini et al. [16] estimate that for a low earth orbit satellite where Alice and Bob have limited time to communicate with the satellite, a simplified trusted relay which does not participate in error correction, privacy amplification and parameter estimation could produce 40% more key per *second* compared to the full trusted relay.[15]

We now adapt the simplified trusted relay to the key rate format given in Section 2.4.2. In the simplified trusted relay, the relay takes on the role of the sender for receivers Alice and Bob. Up to the parity announcement, the simplified trusted relay is equivalent to running the same protocol twice except on an initial state ρ_{TAB}, shared between each link.[16] Here, the relay acts on system $T \equiv T_{AB} \equiv T_A T_B$, where T_A and T_B is the relay's initial systems on Alice and Bob's links respectively. Alice and Bob keep their system's original labels A and B. It is assumed Eve holds a purification $|\rho\rangle_{TABE}$.

The relay measures each half with the POVMs $\{M_{T_A,x,\alpha}\}|_{x\in\mathcal{X},\alpha\in\mathcal{A}}$ and $\{M_{T_B,x',\alpha'}\}|_{x'\in\mathcal{X},\alpha'\in\mathcal{A}}$, then records its private data in registers X_A and X_B, and its public announcements in registers C_{T_A} and C_{T_B}. Alice and Bob measure their systems with POVMs $\{M_{A,y,\beta}\}|_{y\in\mathcal{Y},\beta\in\mathcal{B}}$

[14] This is a simplification which is expanded upon later in this section.

[15] The comparison was done for qubit based BB84 with loss and a ratio between the quantum signals transmitted and received per second, and th classical signals transmitted and received per second on the order of 10^{-2}.

[16] This is the easiest form for a simplified trusted relay. More exotic forms can allow the relay to act on each link in a more joint manner, though the relay's POVMs, measurements, source replacement, etc. would no longer be separable.

and $\{M_{B,y',\beta'}\}|_{y'\in\mathcal{Y},\beta'\in\mathcal{B}}$, then record private data and public announcements in registers Y_A, Y_B, C_A, and C_B respectively. For short hand we may refer to combinations of these registers as $C_T \equiv C_{T_A T_B}$, $X \equiv X_A X_B$, and $Y \equiv Y_A Y_B$. Just like in Equation (2.71), we associate these POVMs with the quantum to classical channels:

$$\begin{aligned}
\mathcal{E}'_{T_A\to X_A C_{T_A}}(\rho_{T_A}) &= \sum_{x\in\mathcal{X}}\sum_{\alpha\in\mathcal{A}} |x\alpha\rangle\langle x\alpha|_{X_A C_{T_A}} \operatorname{Tr}[M_{T_A,x,\alpha}\rho_{T_A}],\\
\mathcal{E}'_{T_B\to X_B C_{T_B}}(\rho_{T_B}) &= \sum_{x'\in\mathcal{X}}\sum_{\alpha'\in\mathcal{A}} |x'\alpha'\rangle\langle x'\alpha'|_{X_B C_{T_B}} \operatorname{Tr}[M_{t_B,x',\alpha'}\rho_{T_B}],\\
\mathcal{E}'_{A\to Y_A C_A}(\rho_A) &= \sum_{y\in\mathcal{Y}}\sum_{\beta\in\mathcal{B}} |y\beta\rangle\langle y\beta|_{Y_A C_A} \operatorname{Tr}[M_{A,y,\beta}\rho_A],\\
\mathcal{E}'_{B\to Y_B C_B}(\rho_B) &= \sum_{y'\in\mathcal{Y}}\sum_{\beta'\in\mathcal{B}} |y'\beta'\rangle\langle y'\beta'|_{Y_B C_B} \operatorname{Tr}[M_{A,y',\beta'}\rho_B].
\end{aligned} \tag{2.92}$$

We compress these to the measurements on each link,

$$\begin{aligned}
\mathcal{E}'_{T_A A\to X_A Y_A C_{T_A A}} &= \mathcal{E}'_{T_A\to X_A C_{T_A}} \otimes \mathcal{E}'_{A\to Y_A C_A},\\
\mathcal{E}'_{T_B B\to X_B Y_B C_{T_B B}} &= \mathcal{E}'_{T_B\to X_B C_{T_B}} \otimes \mathcal{E}'_{B\to Y_B C_B},
\end{aligned} \tag{2.93}$$

and further to the channel for all quantum to classical measurements,

$$\mathcal{E}'_{TAB\to XYC_{TAB}} = \mathcal{E}'_{T_A A\to X_A Y_A C_{T_A A}} \otimes \mathcal{E}'_{T_B B\to X_B Y_B C_{T_B B}}. \tag{2.94}$$

Parameter estimation is carried out by determining the observed joint probabilities between *all* measurements, $p(x,x',y,y',\alpha,\alpha',\beta,\beta')$. Furthermore, for prepare and measure protocols, we also add constraints to reflect that Eve cannot manipulate the relay's measurements. From the source replacement scheme, the relay holds a state of the form

$$|\rho\rangle_{TT'} = \sum_l \sqrt{p_l}\,|l\rangle_{T_A} \otimes |\psi_l\rangle_{T'_A} \otimes \sum_{l'} \sqrt{p_{l'}}\,|l'\rangle_{T_B} \otimes |\psi_{l'}\rangle_{T'_B}. \tag{2.95}$$

The constraint then takes on the form $\operatorname{Tr}_{AB}[\rho_{TAB}] = \operatorname{Tr}_{T'}[\rho_{TT'}]$. All together, the constraint

set for the simplified trusted relay is given by

$$\Gamma = \Big\{ \rho_{TAB} \in \mathrm{D}(TAB) \Big| \operatorname{Tr}_{AB}[\rho_{TAB}] = \operatorname{Tr}_{T'}[\rho_{TT'}],\ p(x,x',y,y',\alpha,\alpha',\beta,\beta') \\ = \operatorname{Tr}[(M_{T_A,x,\alpha} \otimes M_{T_B,x',\alpha'} \otimes M_{A,y,\beta} \otimes M_{B,y',\beta'})\, \rho_{TAB}], \\ \forall (x,x',y,y',\alpha,\alpha',\beta,\beta') \in (\mathcal{X},\mathcal{X},\mathcal{Y},\mathcal{Y},\mathcal{A},\mathcal{A},\mathcal{B},\mathcal{B}) \Big\}. \tag{2.96}$$

To get the key and parity announcement the relay applies the original key map $\mathcal{E}$ to both sides, then announces the parity of the result. We compress the original key maps to

$$\mathcal{E}_{XC_{TAB} \to RC_{TAB}} := \mathcal{E}_{X_A C_{T_A A} \to R_A C_{T_A A}} \otimes \mathcal{E}_{X_B C_{T_B B} \to R_B C_{T_B B}}, \tag{2.97}$$

then apply

$$\mathcal{E}_{\mathrm{STR},R \to R_A C_R}(\rho_R) = \sum_{r,r'=0}^{1} |r\ r+r'\rangle\langle r\ r+r'|_{R_A C_R} \operatorname{Tr}_R[|r\ r'\rangle\langle r\ r'|_R\, \rho_R], \tag{2.98}$$

where C_R stores the parity announcement. The net result gives the simplified trusted relay a key map of

$$\mathcal{E}_{\mathrm{STR},R \to R_A C_R} \circ \mathcal{E}_{XC_{TAB} \to RC_{TAB}}. \tag{2.99}$$

For the post-selection set, both sides of the link must accept. This usually manifests as Alice and the relay pick the same basis choice, and for the other link, Bob and the relay choose the same basis choice. Typically, the additional parity announcement is unused for post-selection, and all protocols we study here accept every parity announcement. Therefore, for an original post-selection set $\mathcal{S}$, and parity announcements drawn from the alphabet $\mathcal{R}$, the post-selection set for the simplified trusted relay is

$$\mathcal{S}_{\mathrm{STR}} = \mathcal{S} \times \mathcal{S} \times \mathcal{R}. \tag{2.100}$$

Error correction for the simplified trusted relay is significantly more complex than in two party protocols. Because Alice and Bob are separated from each other, (ignoring announcements for now) we cannot simply take the error correction cost as $\delta_{\mathrm{leak}} = f\,\mathrm{H}\,(R_A|Y)$. Doing so would imply that Alice and Bob could exchange information without notifying Eve. Taking $\delta_{\mathrm{leak}} = f(\mathrm{H}\,(R_A|Y_A) + \mathrm{H}\,(R_A|Y_B))$ (the cost to correct each party's raw keys

separately) typically overestimates the cost of performing error correction, as Alice's joint distribution with the key can be similar to Bob's joint distribution with the key. In other words, we expect the error correction cost to be bounded by

$$f\,\mathrm{H}\left(R_A|Y_A\right) \leq \delta_{\mathrm{leak}} \leq f(\mathrm{H}\left(R_A|Y_A\right) + \mathrm{H}\left(R_A|Y_B\right)). \tag{2.101}$$

Furthermore, two way error correction can leak additional information from both Alice and Bob back to Eve, and tracking any overlap in information leaked by Alice and Bob becomes exceptionally complex.

For simplicity, we only consider protocols that perform a single one way error correction announcement from the relay to both Alice and Bob. There are many scenarios where $f\,\mathrm{H}\left(R_A|Y_A\right)$ is the correct error correction cost. For example, if there exists a post processing map g such that $g(Y_B) = Y_A$, then error correction information generated for Alice is also sufficient for Bob.[17] If the map g does not exists, then error correction fails, and the protocol aborts. As such, the secrecy of the key is not compromised. Taking into account the alternative scenario where Alice can apply a map g such that $g(Y_A) = Y_B$, we take the error correction cost as

$$\delta_{\mathrm{leak}} = f \max\{\mathrm{H}\left(R_A|Y_A\right), \mathrm{H}\left(R_A|Y_B\right)\}. \tag{2.102}$$

We then add the conditions for the announcements of the basis choices α, α', β and β', and the parity r'. For the protocols and channels studied in this thesis, every announcement that is part of the post-processing set $\mathcal{S}_{\mathrm{STR}}$ has[18]

$$\mathrm{H}\left(R_A|Y_A, \alpha, \alpha', \beta, \beta', r'\right) = \mathrm{H}\left(R_A|Y_B, \alpha, \alpha', \beta, \beta', r'\right). \tag{2.103}$$

The error correction cost simplifies to

$$\delta_{\mathrm{leak}}^{(\alpha,\alpha',\beta,\beta',r')} = f\,\mathrm{H}\left(R_A|Y_A, \alpha, \alpha', \beta, \beta', r'\right). \tag{2.104}$$

Finally, like in Equation (2.77), we can write the key rate for the simplified trusted

[17] For example, if Alice and Bob are using a qubit six-state based relay, and Alice receives more depolarization than Bob, Bob can apply a binary symmetric error channel to his data to get the same distribution as Alice.

[18] For protocols where different basis announcements could have vastly different distributions, sifting techniques discussed later in Section 3.1.3 should also be considered.

relay

$$
\begin{aligned}
R \geq & \sum_{(\alpha,\alpha',\beta,\beta',r')\in\mathcal{S}_{\mathrm{STR}}} p(\alpha,\alpha',\beta,\beta',r') \Bigg[\mathrm{H}\left(R_A|\alpha,\alpha',\beta,\beta',r'\right) \\
& \qquad - \max_{\rho_{TAB}\in\Gamma} \chi(R_A:E|\alpha,\alpha',\beta,\beta',r') - \delta_{\mathrm{leak}}^{(\alpha,\alpha',\beta,\beta',r')} \Bigg] \\
= & \sum_{(\alpha,\alpha',\beta,\beta',r')\in\mathcal{S}_{\mathrm{STR}}} p(\alpha,\alpha',\beta,\beta',r') \\
& \times \Bigg[\min_{\rho_{TAB}\in\Gamma} \left(\sum_{r\in\mathcal{R}} \mathrm{H}\left(p(r|\alpha,\alpha',\beta,\beta',r') \rho_E^{(r,\alpha,\alpha',\beta,\beta',r')} \right) - \mathrm{H}\left(\rho_E^{(\alpha,\alpha',\beta,\beta',r')} \right) \right) \\
& \qquad - \delta_{\mathrm{leak}}^{(\alpha,\alpha',\beta,\beta',r')} \Bigg].
\end{aligned}
\tag{2.105}
$$

When solved for the qubit six-state protocol, under the same conditions as in Section 2.4.3, yields a key rate of[19]

$$
\begin{aligned}
R \geq & \left(\sum_{\alpha\in\mathcal{A}} p(\alpha,\alpha) \right) \Bigg(2 \Bigg[1 + \mathrm{h}\left(\frac{\xi}{2}\right) - \mathrm{Q}\left(\frac{1}{2} \left(\left(1-\frac{3\xi}{4}\right)^2 + \left(\frac{\xi}{4}\right)^2 \right) \right) \\
& - \mathrm{Q}\left(\left(1-\frac{3\xi}{4}\right)\frac{\xi}{4} \right) - 4\,\mathrm{Q}\left(\frac{1}{2}\left(1-\frac{\xi}{2}\right)\frac{\xi}{4} \right) - 2\,\mathrm{Q}\left(\left(\frac{\xi}{4}\right)^2 \right) \Bigg] - f\,\mathrm{h}\left(\frac{\xi}{2}\right) \Bigg).
\end{aligned}
\tag{2.106}
$$

In [1, 15], the simplified trusted relay was tested on the qubit BB84 protocol [4]. Here, we demonstrate similar effects on the qubit six-state protocol with depolarization and no loss. The effect on the key rate can clearly be seen in Figure 2.3 where the simplified trusted relay has a lower error tolerance than the full trusted relay. In this scenario both links are subjected to the same amount of depolarizing noise ξ. For the no relay case, Alice and Bob are effectively applying the depolarization twice, totalling to a depolarization of $\xi(2-\xi)$. With no relay, Alice and Bob can only tolerate $\sim 13\%$ depolarization. The simplified trusted relay drastically improves on this for a tolerance of $\sim 18\%$, but still lags behind the full trusted relay at $\sim 25\%$.

[19] Calculating this by hand takes some considerable time. We recommend coming back to this after deriving the general case in Chapter 4, specifically using Theorem 4.2.3.

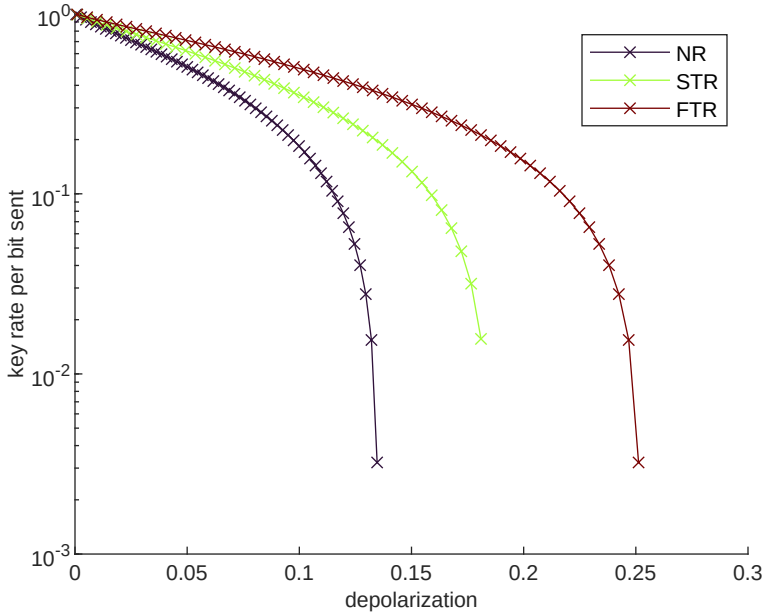


Figure 2.3: Qubit six-state protocol with depolarization ξ per each link and no loss. Error correction performed at the Shannon limit ($f = 1$). NR: no relay, STR: simplified trusted relay, FTR: full trusted relay. QBER is equivalent to $\frac{\xi}{2}$.

2.6 Delayed Privacy Amplification

One solution to boost the key rate of the simplified trusted relay is to borrow concepts from delayed privacy amplification [17]. For regular (linear) privacy amplification, once Alice and Bob have completed error correction (and error verification), with high probability, they both share the same insecure key $\vec{k}$. Alice randomly selects a linear hashing function F from a family of two universal hash function and announces her selection. Alice and Bob then apply the function to their shared, insecure key generating $F\vec{k}$. If the protocol didn't abort, Alice and Bob share an ϵ-secure key. Alice can then take a secret message $\vec{m}$ and send $\vec{m} + \vec{k}$ to Bob using one time pad encryption.

Delayed privacy amplification flips the order of hashing and the one time pad encryption. After Alice announces the hashing function F, she randomly selects a vector $\overrightarrow{m'}$ from the preimage $F^{-1}(\vec{m})$. Alice then uses the one time pad to encrypt $\overrightarrow{m'}$ with the insecure key $\vec{k}$. Bob receives $\overrightarrow{m'} + \vec{k}$, and calculates $\overrightarrow{m'}$. Applying the hashing function F, Bob recovers $\vec{m} = F\overrightarrow{m'}$. In [17], Fung et al. proved that delayed privacy amplification has equivalent security to regular privacy amplification.

Although not directly applicable to the simplified trusted relay, delayed privacy amplification highlights a critical property often overlooked when discussing privacy amplification and post processing. When choosing a random message $\overrightarrow{m'} \in F^{-1}(\vec{m})$, delayed privacy amplification is embedding the message $\vec{m}$ in a higher dimensional space, then adding a random element from $\ker(F)$ to obscure it. When Bob applies F, the additional element from $\ker(F)$ is removed.

Chapter 3

Pre-Privacy Amplification and the Six-State Protocol

From delayed privacy amplification, a fixed linear code is used to perform privacy amplification of the secret key after a one-time pad was used. Although not directly useful, a core observation was that a message could be obscured by embedding it in a higher dimensional space, then adding a random element from the kernel of the privacy amplification matrix. In this chapter we use this same concept to define a post processing map to perform a sort of *pre-privacy amplification*. This pre-privacy amplification is done just after the original raw key mapping, and is followed by the usual application of error correction and privacy amplification. As the core concept is to take a large number of raw key bits and concentrate their secrecy into a few bits, we call the matrices that perform it, *reduction matrices*.

In this chapter we define pre-privacy amplification and construct it for the framework set out in Section 2.4. We then apply it to the qubit six-state protocol with depolarization. We also show multiple techniques to increase the computational performance as well as symmetries to reduce the search for finding optimal reduction matrices. Finally, we show that reduction matrices slightly increase the maximum tolerable depolarization of the six-state protocol. The application to the simplified trusted relay is delayed to Chapter 4.

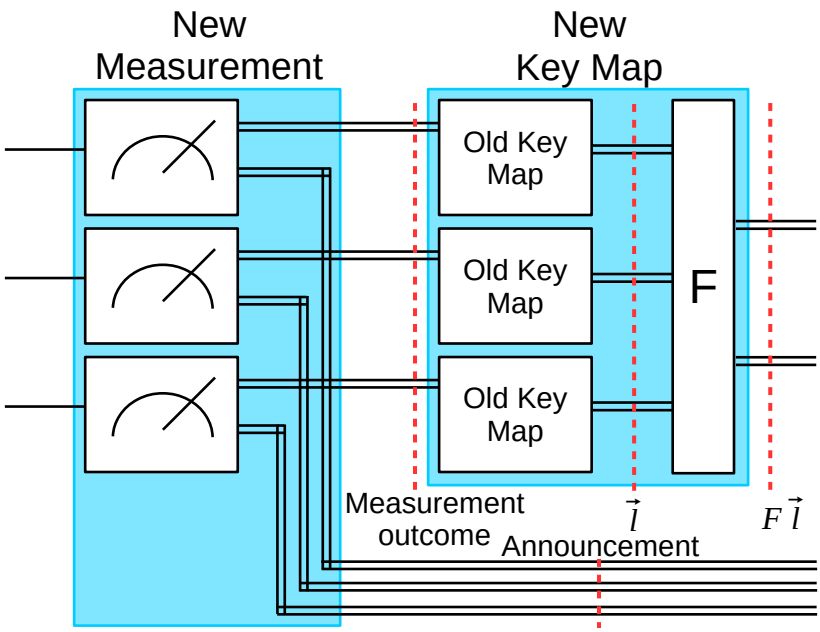


Figure 3.1: Overview for converting a regular protocol into a pre-privacy amplification protocol. We group, n copies of the original protocol together.

3.1 Pre-Privacy Amplification and Reduction Matrices

Suppose Alice and Bob have a QKD protocol that fits into the description of Section 2.4. Alice and Bob perform measurements and announcements on multiple rounds. For rounds not used in parameter estimation, each round either produces a single raw key-dit $l \in \mathcal{R}$ (where $\mathcal{R}$ is a finite field) or the round is sifted out during post-processing. In the pre-privacy amplification post processing step, we gather n of these rounds together and treat them as a single round on a much larger Hilbert space. As depicted in Figure 3.1, we combine our measurements into a new single measurement over n systems, and then do the same for announcements and key mappings. With this, we now have a single raw key-dit $\vec{l} \in \mathcal{R}^n$. We then apply pre-privacy amplification to reduce the size of the raw key and limit Eve's knowledge. We achieve this by applying a publicly agreed upon full rank matrix $F \in \mathcal{R}^{m \times n}$ $(m \leq n)$ to $\vec{l}$. Afterwards, the usual steps of error correction and privacy amplification are performed. It is important to note that if even a single one of

the sub rounds is sifted out, then the entire group must be thrown out.[1] We then formally define a reduction matrix as

Definition 3.1.1. Let $m \leq n$ and $\mathcal{R}$ a finite field. We call a full rank matrix $F \in \mathcal{R}^{m \times n}$ a *reduction matrix*.

3.1.1 General Procedure and Notation

In essence, Alice and Bob turn a $|\mathcal{R}|$-qudit protocol into a $|\mathcal{R}|^n$-qudit protocol. With this in mind we extend a few other steps in the QKD protocol. To construct the protocol, the natural first step is to combine n rounds of the initial protocol with tensor products. The only major difference is the new key map using pre-privacy amplification. As such, the majority of the section is just constructing a clear book keeping method. Alice and Bob's measurements were originally defined by POVMs $\{M_{A,x,\alpha}\}|_{x\in\mathcal{X},\alpha\in\mathcal{A}}$, and $\{M_{B,y,\beta}\}|_{y\in\mathcal{Y},\beta\in\mathcal{B}}$. We extend these to the new POVMs,

$$\left\{M_{A,\vec{x},\vec{\alpha}}\right\}_{\vec{x}\in\mathcal{X}^n,\vec{\alpha}\in\mathcal{A}^n}, \tag{3.1}$$

$$\left\{M_{B,\vec{y},\vec{\beta}}\right\}_{\vec{y}\in\mathcal{Y}^n,\vec{\beta}\in\mathcal{B}^n}, \tag{3.2}$$

where,

$$M_{A,\vec{x},\vec{\alpha}} := \bigotimes_{i=0}^{n} M_{A,x_i,\alpha_i}, \tag{3.3}$$

$$M_{B,\vec{y},\vec{\beta}} := \bigotimes_{i=0}^{n} M_{B,y_i,\beta_i}. \tag{3.4}$$

During parameter estimation, Alice and Bob perform n uses of their original POVM measurement $\mathcal{E}^{\otimes n}_{AB\to XYC}$,

$$\mathcal{E}'^{\otimes n}_{AB\to XYC}(\rho_{AB}) = \sum_{\vec{x}\in\mathcal{X}^n}\sum_{\vec{y}\in\mathcal{Y}^n}\sum_{\vec{\alpha}\in\mathcal{A}^n}\sum_{\vec{\beta}\in\mathcal{B}^n} |\vec{x}\,\vec{y}\rangle\langle\vec{x}\,\vec{y}|_{XY} \otimes \left|\vec{\alpha}\,\vec{\beta}\right\rangle\!\left\langle\vec{\alpha}\,\vec{\beta}\right|_C \mathrm{tr}\left[(M_{A,\vec{x},\vec{\alpha}}\otimes M_{B,\vec{y},\vec{\beta}})\rho_{AB}\right], \tag{3.5}$$

[1] There are a few ways around this, discussed later in Section 3.1.3.

and the initial key mapping (before pre-privacy amplification),

$$\mathcal{E}_{XC\to RC}^{\otimes n}(\rho_{XC}) = \sum_{\vec{x}\in\mathcal{X}^n}\sum_{\vec{\alpha}\in\mathcal{A}^n}\sum_{\vec{\beta}\in\mathcal{B}^n}\left|g(\vec{x},\vec{\alpha},\vec{\beta})\right\rangle\!\left\langle g(\vec{x},\vec{\alpha},\vec{\beta})\right|_R \otimes \left|\vec{\alpha}\,\vec{\beta}\right\rangle\!\left\langle\vec{\alpha}\,\vec{\beta}\right|_C \mathrm{Tr}\left[\left|\vec{x}\,\vec{\alpha}\,\vec{\beta}\right\rangle\!\left\langle\vec{x}\,\vec{\alpha}\,\vec{\beta}\right|_{XC}\rho_{XC}\right], \quad (3.6)$$

where $g : \mathcal{X}\times\mathcal{A}\times\mathcal{B}\to\mathcal{R}$ is the key map on the alphabets of Alice's private information and announcements. Here, it is extended to vectors by simply applying the map g to each triplet. Formally, we write this as

$$g(\vec{x},\vec{\alpha},\vec{\beta}) := \sum_{i=1}^{n} g(x_i,\alpha_i,\beta_i)\,\vec{e}_i. \quad (3.7)$$

For simplicity, we require the output alphabet $\mathcal{R}$ of the key map g to be a finite field. This way we can use linear algebra on finite fields for easy analysis of the key rate. After the original key mapping is applied to all n systems, the reduction matrix, $F\in\mathcal{R}^{m\times n}$, is applied by the classical channel

$$\mathcal{E}_{\mathrm{PPA},R\to R'}(\rho_R) := \sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\!\langle F\vec{r}|_{R'}\,\mathrm{Tr}[|\vec{r}\rangle\!\langle\vec{r}|_R\,\rho_R]. \quad (3.8)$$

Functionally, the pre-privacy amplification map constructs a new key dit in $\mathcal{R}^m$ from the old key dits in $\mathcal{R}^n$. Without this mapping, the process would degenerate into n separate runs of the original protocol.

The post-selection set of announcements, $\mathcal{S}$, from 2.73 is extended similarly to $\mathcal{S}^n$, and the error correction leakage for a given announcement is

$$\begin{aligned}\delta_{\mathrm{leak}}^{(\vec{\alpha},\vec{\beta})} &= f\,\mathrm{H}\left(R'\middle|Y,\vec{\alpha},\vec{\beta}\right)\\ &= f\left(\mathrm{H}\left(R',Y\middle|\vec{\alpha},\vec{\beta}\right)-\mathrm{H}\left(Y\middle|\vec{\alpha},\vec{\beta}\right)\right).\end{aligned} \quad (3.9)$$

The constraint set Γ takes on a similar form to Equation (2.73), except with several cross

terms of constraints from each of the individual copies collected together.

$$\Gamma = \Big\{ \rho_{AB} \in \mathrm{D}(AB) \Big| \operatorname{tr}_B[\rho_{AB}] = \operatorname{tr}_{A'}[\rho_{AA'}], \\ p(\vec{x}, \vec{y}, \vec{\alpha}, \vec{\beta}) = \operatorname{Tr}\Big[(M_{A,\vec{x},\vec{\alpha}} \otimes M_{B,\vec{y},\vec{\beta}}) \rho_{AB} \Big], \forall (\vec{x}, \vec{y}, \vec{\alpha}, \vec{\beta}) \in (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B})^n \Big\}. \tag{3.10}$$

Finally, placing each of these into the general key rate equation from Equation 2.77 (remembering that we are now using a key register R'), the full key rate per *block* is bounded by

$$\begin{aligned} R &\geq \sum_{(\vec{\alpha},\vec{\beta}) \in \mathcal{S}^n} p(\vec{\alpha}, \vec{\beta}) \left(\mathrm{H}\left(R' \middle| \vec{\alpha}, \vec{\beta} \right) - \max_{\rho_{AB} \in \Gamma} \chi(R' : E | \vec{\alpha}, \vec{\beta}) - \delta_{\text{leak}}^{(\vec{\alpha},\vec{\beta})} \right) \\ &= \sum_{(\vec{\alpha},\vec{\beta}) \in \mathcal{S}^n} p(\vec{\alpha}, \vec{\beta}) \left(\min_{\rho_{AB} \in \Gamma} \left(\sum_{\vec{r} \in \mathcal{R}^m} \mathrm{H}\left(p(\vec{r} | \vec{\alpha}, \vec{\beta}) \rho_E^{(\vec{r},\vec{\alpha},\vec{\beta})} \right) - \mathrm{H}\left(\rho_E^{(\vec{\alpha},\vec{\beta})} \right) \right) - \delta_{\text{leak}}^{(\vec{\alpha},\vec{\beta})} \right). \end{aligned} \tag{3.11}$$

It is important to note that this is the key rate per a block and not per qudit sent because we gathered the n qudits together and treat them as a single massive qudit. The key rate formula from Equation 2.77 cannot distinguish this. For example, if we use identity for the reduction matrix F, then the protocol degenerates into n runs of the original protocol done at once for n times the original key rate. With the key rate formula we can upgrade any protocol from Section 2.4 with pre-privacy amplification in a straight forward manor.

3.1.2 Splitting the Pre-Privacy Amplification Map

Currently, the form of the pre-privacy amplification map $\mathcal{E}_{\mathrm{PPA},R\to R'}$ from Equation (3.8) obscures the underlying mechanism for enhancing privacy and simplifications to the key rate calculation. Multiple vectors $\vec{r} \in \mathcal{R}^n$ all map to the same value when we apply the reduction matrix F. In other words, for any $\vec{r} \in \mathcal{R}^n$ and $\vec{r'} \in \ker(F)$, $F(\vec{r} + \vec{r'}) = F\vec{r}$. Removing the redundancy from the key register would simplify key rate calculations. If F was an operator over $\mathbb{R}$, then we could split $\mathcal{R}^n$ into the subspaces $\ker(F)$ and $(\ker(F))^\perp$. Unfortunately for finite fields, we do not have an inner product, so the perpendicular space is not well defined. However we can still break apart elements of $\mathcal{R}^n$ into the sum from vectors in $\ker(F)$ and another subspace. For this purpose we define *representative spaces*.

Definition 3.1.2 (representative space)**.** Let $F \in \mathcal{R}^{m\times n}$, we call a vector space $\mathcal{V}$ subspace of $\mathcal{R}^n$ a *representative space* of F if $\mathcal{V}$ satisfies

1. $\mathcal{V} + \ker(F) = \mathcal{R}^n$, and
2. $\mathcal{V} \cap \ker(F) = \{\vec{0}\}$.

By the rank-nullity theorem (Theorem 2.1.9), $\dim(\mathcal{V}) = n - \dim(\ker(F)) = \text{rank}(F)$, and for any vector $\vec{r} \in \mathcal{R}^n$, there exists vectors $\vec{a} \in \mathcal{V}$ and $\vec{b} \in \ker(F)$ such that $\vec{r} = \vec{a} + \vec{b}$. In Equation (3.8) we could then replace $F\vec{r}$ with $F(\vec{a} + \vec{b}) = F\vec{a}$, therefore we do not need to consider anything from the $\ker(F)$ in the key register. Furthermore, as the name suggests, the elements of $\mathcal{V}$ are representatives for each pre-image of F. In other words, $\mathcal{V}$ is isomorphic to the quotient space $F|\ker(F)$, and $F(\mathcal{V}) = \text{Im}(F)$. Also, for $c = \text{rank}(F)$, we know that $\mathcal{V} \simeq \mathcal{R}^c$, and $\ker(F) \simeq \mathcal{R}^{n-c}$. It is more convenient to work with $\mathcal{R}^c$ and $\mathcal{R}^{n-c}$ than $\mathcal{V}$ and $\ker(F)$, so we set up isomorphisms between them with a few matrices. We summarize this with the theorem,

Theorem 3.1.3. *Let $\mathcal{V}$ be a representative space of $F \in \mathcal{R}^{m\times n}$. Also let $c = \dim(\text{Im}(F))$, so $\mathcal{V} \simeq \mathcal{R}^c$ and $\ker(F) \simeq \mathcal{R}^{n-c}$. Then there exists full rank matrices $V \in \mathcal{R}^{n\times c}$ and $\tilde{V} \in \mathcal{R}^{n\times n-c}$ such that $\text{Im}(V) = \mathcal{V}$ and $\text{Im}(\tilde{V}) = \ker(F)$.*

Note that $\ker(FV) = \{\vec{0}\}$, so no vector in $\mathcal{R}^c$ is "wasted". Also, for any $\vec{r} \in \mathcal{R}^n$ there exists unique $\vec{a} \in \mathcal{R}^c$, $\vec{b} \in \mathcal{R}^{n-c}$ such that $\vec{r} = V\vec{a} + \tilde{V}\vec{b}$, and $F\vec{r} = FV\vec{a}$.

Definition 3.1.2 and Theorem 3.1.3 are extremely useful and will feature in many areas of this thesis. As such, they were written for any matrix $F \in \mathcal{R}^{m\times n}$. However, in the context of the pre-privacy amplification map from Equation (3.8) we can limit our analysis to when F is a reduction matrix. For this, we give the following theorems:

Theorem 3.1.4. *Let $n \geq m$, $F \in \mathcal{R}^{m\times n}$ be a reduction matrix (F is full rank), and let $\mathcal{V}$ be a representative space of F. Then, $\dim(\mathcal{V}) = m$ and for any $V \in \mathcal{R}^{n\times m}$ such that $\text{Im}(V) = \mathcal{V}$, the matrix FV is invertable.*

Proof. Let $\mathcal{V}$ be representative space of F, and $V \in \mathcal{R}^{n\times m}$ such that $\text{Im}(V) = \mathcal{V}$. We already know that $\text{Im}(FV) = \text{Im}(F) = \mathcal{R}^m$, and $FV \in \mathcal{R}^{m\times m}$ therefore the $\ker(FV) = \{\vec{0}\}$ and the square matrix FV must be invertable. □

Theorem 3.1.5. *Let $F \in \mathcal{R}^{m\times n}$ be a reduction matrix, and $\mathcal{V}$ a representative space of F. Then for any invertable matrix $U \in \mathcal{R}^{m\times m}$, there exists a $V \in \mathcal{R}^{n\times m}$ such that* $\mathrm{Im}(V) = \mathcal{V}$ *and $FV = U$.*

Proof. Let $\mathcal{V}$ be a representative space of F, $U, E \in \mathcal{R}^{m\times m}$ be invertable matrices, and $V \in \mathcal{R}^{n\times m}$ such that $\mathrm{Im}(V) = \mathcal{V}$. $\mathrm{Im}(VE) = \mathrm{Im}(V) = \mathcal{V}$, and FV is invertable. Therefore, pick $E = (FV)^{-1}U$. We get $V' = V(FV)^{-1}U$ such that $\mathrm{Im}(V') = \mathcal{V}$ and $FV' = U$. □

Naturally, for any given representative space $\mathcal{V}$ of F, we choose a V from Theorem 3.1.5 such that $FV = I_m$. Therefore, for any $\vec{l} \in \mathcal{R}^n$, there exists $\vec{a} \in \mathcal{R}^m$ and $\vec{b} \in \mathcal{R}^{n-m}$ such that $\vec{r} = V\vec{a} + \tilde{V}\vec{b}$ and $F\vec{r} = \vec{a}$. Applying this to the pre-privacy amplification map from Equation (3.8) gives

$$\mathcal{E}_{\mathrm{PPA},R\to R'}(\rho_R) := \sum_{\vec{a}\in\mathcal{R}^m} |\vec{a}\rangle\langle\vec{a}|_{R'} \sum_{\vec{b}\in\mathcal{R}^{n-m}} \mathrm{Tr}\left[\left|V\vec{a} + \tilde{V}\vec{b}\right\rangle\left\langle V\vec{a} + \tilde{V}\vec{b}\right|_R \rho_R\right]. \tag{3.12}$$

In this form, the interpretation of pre-privacy amplification is similar to delayed privacy amplification [17]. Note that F is the parity check matrix for the linear error correcting code generated by $\tilde{V}$. Essentially, we are constructing a secret key from the syndromes associated with a linear error correcting code and using the kernel to obscure them during transmission. Broadly speaking, the worse an error correcting code the matrix $\tilde{V}$ generates, the better the reduction matrix F is at pre-privacy amplification.[2]

3.1.3 Sifting and maintaining key rate

We run into an immediate problem with sifting and the post-selection set. For a single copy and measurement in the original protocol, if its announcements had probability p_{pass} of falling into $\mathcal{S}$, then n copies have probability p_{pass}^n of falling into $\mathcal{S}^n$. This can easily reduce the key rate to nearly nothing. Here are a few solutions to help prevent or mitigate this.

1. If Alice and Bob have some degree of control over which announcement is made, then they can manipulate their measurements to bias one announcement over others. For

[2] With the caveat that pre-privacy amplification also amplifies the errors that Bob must correct.

example, in BB84 Alice and Bob each randomly choose whether to measure in the X or Z-basis, then announce their choices after all signals are measured. For equal basis choice probability, they have $p_{\text{pass}} = \frac{1}{2}$, and a vanishingly low chance of passing sifting for n copies. However, if they bias their measurements so that the Z-basis occurs with probability ≈ 1, then p_{pass}^n can still be kept close to 1. At this point, the most important factor is just getting enough measurements in the X-basis so that Alice and Bob can complete parameter estimation.

2. The first approach is not always possible. For example, an announcement by Bob that a signal was lost is typically out of Alice and Bob's control. Alternatively, if Alice and Bob cannot bias their basis choice, or cannot bias it enough,[3]then for large values of n, this will become an issue again. In these cases reblocking is necessary. In reblocking, the signals are first filtered by their announcements, then organized into blocks of n for the key rate analysis (Section 4.6.1 of [1]). However this breaks permutation symmetries used to generalize from I.I.D. attacks to general attacks used in post selection techniques such as in [31]. Techniques for handling this for the simplified trusted relay are discussed in Section 4.6.1 of [1] which could be applied to protocols with pre-privacy amplification.

3.1.4 Numerical limitations

Although most prococols that follow the outline in Section 2.4 can have pre-privacy amplification added to them by following the steps in Section 3.1.1, the computational cost to calculate the key rate can easily surpass available resources. For example, numerical techniques such as the ones used in [7, 23, 27] use convex optimization to bound the key rate. Optimizing over all $\rho_{AB} \in \Gamma$ can quickly become infeasible as the number of optimization parameters grows exponentially. Even a simple qubit BB84 protocol with no loss will cause issues. Using the Schmidt decomposition, Alice and Bob would still share a state ρ_{AB} of size $4^n \times 4^n$. Convex optimization problems of $4^n \times 4^n$ hermitian operators can easily surpass any computation limits. Furthermore, numerical techniques such as the ones used in [7, 23, 27] use the relative entropy and require solving the eigenvalues and vectors of the state after applying the G and Z maps from Section 2.4.2. Even if one can exploit some

[3]For example, some of the original squashing maps designed to manage infinite dimensions require equal basis choice [8].

block diagonal structure, the diagonalization will still take an exponential amount of time and resources. As such, we are limited to solving protocols analytically. This limits our analysis to protocols and attacks that are tomographcally complete and highly symmetric.

3.2 Six-State Pre-Privacy Amplification Protocol

In order to avoid the numerical limitations from Section 3.1.4, we apply pre-privacy amplification to the tomographically complete six-state protocol. This way, we skip the numerically costly task of maximizing the Holevo quantity.

For the six-state protocol with pre-privacy amplification, we assume Eve's attack is I.I.D. between separate groups of n qubits. From this, techniques like the de Finetti theorem can lift this from I.I.D. collective to coherent attacks [6]. Furthermore, we focus on the scenario where Eve's attacks leaves each qubit in a group with depolarization ξ. Therefore, Alice and Bob share the initial state

$$\rho_{AB} = \rho_{\text{single}AB}^{\otimes n} = \left((1-\xi)\Phi_{AB}^{+} + \xi\frac{I_{AB}}{\dim(AB)}\right)^{\otimes n}, \tag{3.13}$$

which is just the n tensored version of Equation (2.80) from the orginal six-state protocol.

Before we determine the purification and measured state held by Alice, Bob and Eve, we make the following assumption to reduce redundant work for the key rate. The key rate Equation (3.11) for pre-privacy amplification asks us to calculate the key rate for every pair of post-selection announcements $(\vec{\alpha}, \vec{\beta}) \in \mathcal{S}^n$. However, recall from Theorem 2.4.2, the key rate for the six-state protocol in the asymptotic limit conditioned on the basis choice was the same whenever Alice and Bob both choose basis $\alpha \in \mathcal{A}$. As such, we only needed to calculate the key rate conditioning on the Z-basis, and multiply by a factor of $\sum_{\alpha\in\mathcal{A}} p(\alpha,\alpha)$ to account for post-selection, as seen in Equation (2.91). Similarly when we apply pre-privacy amplification to the six-state protocol, whenever Alice and Bob choose the same sequence of Basis choices $\vec{\alpha} \in \mathcal{A}^n$, the key rate conditioned on $\vec{\alpha}$ is identical regardless of the choice of $\vec{\alpha}$. Therefore, we only need to calculate the key rate for the case where Alice and Bob measured each of the n qubits in the Z-basis, and apply a factor of $\sum_{\vec{\alpha}\in\mathcal{A}^n} p(\vec{\alpha},\vec{\alpha})$ to account for post-selection.

In this Section 3.2.1 we construct the purification Eve holds, the measurement op-

erators, and the state the three parties share after measurements and the key map. In Section 3.2.2 we use the previously calculated state to determine the error correction cost δ_{leak} as well as the Holevo Quantity. We then combine these to give the key rate and provide an example where pre-privacy amplification outperforms the original protocol.

3.2.1 State, Purification, and Measurement

In order to calculate terms associated with the Holevo quantity and error correction cost, we need to know the density matrix shared by Alice, Bob and Eve after the measurements and post processing are applied. Furthermore, we highlight the block diagonal structure in the shared state, which will simplify the entropy calculations for the Holevo quantity and error correction cost.

Just as Alice and Bob now share the n copies of Equation (2.80), with $\rho_{AB} = \rho_{\text{single}AB}^{\otimes n}$, Eve holds n I.I.D. purifications, one for each system. Overall, Alice, Bob and Eve share the purified state $|\rho\rangle_{ABE} = |\rho_{\text{single}}\rangle_{ABE}^{\otimes n}$ using $|\rho_{\text{single}}\rangle_{ABE}$ from Equation (2.81).

Applying all the measurement and post-processing maps to $|\rho\rangle_{ABE}$ would be particularly difficult to work with. Thankfully, the cost of error correction δ_{leak} only depends on Alice and Bob's registers. Therefore we can trace out Eve's system (which gives the original ρ_{AB}). Similarly, with some careful manipulation Bob's system is not needed when determining the Holevo quantity in (2.4.2), so we can trace over B. Therefore, we construct the marginal shared by Alice and Eve without Bob, ρ_{AE}, then apply measurements and post processing to get the shared state between Eve and the key register $\rho_{R'E}$, then do the same for Bob and the key register $\rho_{R'Y}$.

Alice and Eve's Marginal

From Equation (3.13) we already have Alice and Bob's shared state, but we still need Alice and Eve's marginal. We work with a single copy, then expand to a tensor product of n copies. Starting from the purification of a single state for the six-state protocol in

Equation (2.81), we trace out Bob and get

$$\rho_{\text{single}AE} = \frac{1}{2}\Bigg[\left(\sqrt{1-\frac{3\xi}{4}}\,|0\rangle_A\,|00\rangle_E + \sqrt{\frac{\xi}{4}}\,(|0\rangle_A\,|01\rangle_E + |1\rangle_A\,|10\rangle_E - |1\rangle_A\,|11\rangle_E)\right)\langle\text{c.c.}| \\ + \left(\sqrt{1-\frac{3\xi}{4}}\,|1\rangle_A\,|00\rangle_E + \sqrt{\frac{\xi}{4}}\,(|1\rangle_A\,|01\rangle_E + |0\rangle_A\,|10\rangle_E - |0\rangle_A\,|11\rangle_E)\right)\langle\text{c.c.}|\Bigg]. \quad (3.14)$$

In this form, the correlations between Alice and Eve are too hard to see, and it does not lend itself well to taking large tensors of subsystems like in Equation 2.35. For notational simplicity, we use

$$\begin{aligned} |e_{i,j}\rangle_E &= |i\rangle_{E_1} \otimes Z^j\,|\tau_i\rangle_{E_2}\,, \\ |\tau_0\rangle &= \frac{1}{\sqrt{2}}\left(\sqrt{1-\frac{3\xi}{4}}\,|0\rangle + \sqrt{\frac{\xi}{4}}\,|1\rangle\right), \\ |\tau_1\rangle &= \sqrt{\frac{\xi}{4}}\,|+\rangle\,, \end{aligned} \quad (3.15)$$

and simplify $\rho_{\text{single}AE}$ to

$$\begin{aligned} \rho_{\text{single}AE} &= (|0\rangle_A\,|e_{00}\rangle_E + |1\rangle_A\,|e_{11}\rangle_E)\langle\text{c.c.}| + (|1\rangle_A\,|e_{10}\rangle_E + |0\rangle_A\,|e_{01}\rangle_E)\langle\text{c.c.}| \\ &= \sum_{l,l',k\in\mathbb{Z}_2} |l,\ l+k\rangle\langle l',\ l'+k|_{AE_1} \otimes Z^l_{E_2}\,|\tau_{l+k}\rangle\langle\tau_{l'+k}|_{E_2}\,Z^{l'}_{E_2}. \end{aligned} \quad (3.16)$$

Right away one can see that when Alice measures her state in the Z-basis, she constructs a block diagonal state. Furthermore, we also get block diagonal structure between the two parts of Eve's system E_1 and E_2. For ρ_{AE}, we combine n copies of $\rho_{\text{single}AE}$ and write it using vector notation as

$$\begin{aligned} \rho_{AE} &= \rho_{\text{single}AE}^{\otimes n} \\ &= \sum_{\vec{l},\vec{l'},\vec{k}\in\mathbb{Z}_2^n} \left|\vec{l},\ \vec{l}+\vec{k}\right\rangle\!\left\langle\vec{l'}\ \ \vec{l'}+\vec{k}\right|_{AE_1} \otimes Z^{\vec{l}}_{E_2}\,|\tau_{\vec{l}+\vec{k}}\rangle\langle\tau_{\vec{l'}+\vec{k}}|_{E_2}\,Z^{\vec{l'}}_{E_2}, \end{aligned} \quad (3.17)$$

where we define

$$|\tau_{\vec{l}}\rangle = \bigotimes_{i=1}^{n} |\tau_{l_i}\rangle\,, \tag{3.18}$$

which are n tensored copies of $|\tau_l\rangle$ from Equation (3.15) and,

$$Z^{\vec{l}} = \bigotimes_{i=1}^{n} Z^{l_i}. \tag{3.19}$$

With Equations (3.13) and (3.17), we can now apply Alice and Bob's measurements along with the pre-privacy amplification key mapping.

Measurement and Post Processing Maps

Because we are working with measurements conditioned on using the Z basis, Alice's private measurement outcomes (0 and 1) are identical to the key map (before pre-privacy amplification). Therefore, we skip the intermediate step of storing Alice's measurement outcome in a register X, and directly store her result in register R. Alice's measurement combined with her initial key map is then

$$\mathcal{E}^{\otimes n}_{A\to R}(\rho_A) = \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_R \otimes \mathrm{Tr}\left[\left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_A \rho_A\right]. \tag{3.20}$$

For the pre-privacy amplification map, we use the form from Equation 3.12 which splits the reduction matrix $F \in \mathbb{Z}_2^{m\times n}$ into matrices V and $\tilde{V}$ such that $FV = I_m$ and $\mathrm{Im}(\tilde{V}) = \ker(F)$. The six-state pre-privacy amplification map for a reduction matrix $F \in \mathbb{Z}_2^{m\times n}$ is given by

$$\mathcal{E}_{\mathrm{PPA},R\to R'}(\rho_R) = \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|F\vec{l}\right\rangle\!\left\langle F\vec{l}\right|_{R'} \mathrm{Tr}\left[\left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_R \rho_R\right]. \tag{3.21}$$

Combining the pre-privacy amplification map with Alice's initial measurement and key map gives,

$$\mathcal{E}_{\mathrm{PPA},R\to R'} \circ \mathcal{E}^{\otimes n}_{A\to R}(\rho_A) = \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} |\vec{\gamma}\rangle\!\langle\vec{\gamma}|_{R'} \,\mathrm{Tr}\left[\left|V\vec{\gamma} + \tilde{V}\vec{\beta}\right\rangle\!\left\langle V\vec{\gamma} + \tilde{V}\vec{\beta}\right|_A \rho_A\right]. \tag{3.22}$$

By contrast Bob's new measurement is simply a repeated version of his original measurement giving,

$$\mathcal{E}'^{\otimes n}_{B\to Y}(\rho_B) = \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_{\mathcal{Y}} \mathrm{Tr}\left[\left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_B \rho_B\right]. \tag{3.23}$$

With these maps we can write out the marginals $\rho_{R'E}$ and ρ_E needed for the Holevo quantity, and the marginals $\rho_{R'Y}$ and ρ_Y needed for the error correction cost.

Post Processed Marginals

For the Holevo based term, we simply apply Alice's pre-privacy amplification and measurement to her and Eve's joint state from Equation (3.17). With some effort, the key and Eve's registers $\rho_{R'E}$ reduce to,

$$\begin{aligned}
\rho_{R'E} &= \mathcal{E}_{\mathrm{PPA},R\to R'} \circ \mathcal{E}^{\otimes n}_{A\to R}(\rho^{\otimes n}_{\mathrm{single}AE}) \\
&= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} |\vec{\gamma}\rangle\langle\vec{\gamma}|_{R'} \otimes \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \mathrm{Tr}_A\left[\left(\left|V\vec{\gamma}+\tilde{V}\vec{\beta}\right\rangle\!\left\langle V\vec{\gamma}+\tilde{V}\vec{\beta}\right|_A \otimes I_E\right)\rho^{\otimes n}_{\mathrm{single}AE}\right] \\
&= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{\gamma},\vec{l}\right\rangle\!\left\langle\vec{\gamma},\vec{l}\right|_{R'E_1} \otimes \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}.
\end{aligned} \tag{3.24}$$

Furthermore, ρ_E is required for the Holevo quantity, so it can be quickly calculated giving

$$\rho_E = \sum_{\vec{l},\vec{k}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_{E_1} \otimes Z^{\vec{k}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{\vec{k}}. \tag{3.25}$$

Note that in Equations (3.24) and (3.25) the density matrices each have a large block diagonal structure that drastically reduces the computational cost of determining the eigenvalues for the entropy.

In a similar manner, for the error correction cost we apply Alice's pre-privacy amplification and measurement along side Bob's measurement to get their joint state $\rho_{R'Y}$,

$$\begin{aligned}
\rho_{R'Y} &= \left(\mathcal{E}_{\mathrm{PPA},R\to R'} \circ \mathcal{E}^{\otimes n}_{A\to R} \otimes \mathcal{E}'^{\otimes n}_{B\to Y}\right)\left(\rho^{\otimes n}_{\mathrm{single}AB}\right) \\
&= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}}\sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{\gamma},\vec{l}\right\rangle\!\left\langle\vec{\gamma},\vec{l}\right|_{R'Y} \left\langle V\vec{\gamma}+\tilde{V}\vec{\beta},\ \vec{l}\right|\rho^{\otimes n}_{\mathrm{single}AB}\left|V\vec{\gamma}+\tilde{V}\vec{\beta},\ \vec{l}\right\rangle.
\end{aligned} \tag{3.26}$$

Furthermore, for $\rho_{\text{single}AB}$ given in Equation (2.80), we can employ Theorem 2.2.11, $|l\rangle = X^l|0\rangle$, and reshuffling the summations variables to reduce $\rho_{R'Y}$. Ultimately, we are left with the state

$$\rho_{R'Y} = \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \sum_{\vec{l}\in\mathbb{Z}_2^n} |\vec{\gamma}\rangle\langle\vec{\gamma}|_{R'} \otimes X_Y^{V\vec{\gamma}} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_Y X_Y^{V\vec{\gamma}} \left\langle \vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right| \rho_{\text{single}AB}^{\otimes n} \left|\vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right\rangle, \tag{3.27}$$

where $X^{\vec{l}}$ is defined similarly to $Z^{\vec{l}}$ as $\bigotimes_{i=1}^n X^{l_i}$. Note that Equation (3.27) is fully diagonal, (and classical) therefore the entropy calculations will not require any costly eigenvalue calculations.

Instead of trying to calculate Bob's marginal ρ_Y from $\rho_{R'Y}$, we can simply determine it from tracing out Alice from $\rho_{\text{single}AB}^{\otimes n}$ from Equation (2.80) and applying Bob's measurement channel $\mathcal{E}'_{B\to Y}$. The result is simply the maximally mixed state $\rho_Y = 2^{-n} I_Y$. With the marginals $\rho_{R'E}, \rho_E, \rho_{R'Y}$, and ρ_Y, it is possible to construct the error correction leakage and the Holevo quantity.

3.2.2 Error Correction, Holevo Quantity, and Key Rate

With the marginals we can now calculate each of the entropic quantities for the key rate per block.

Error Correction and Leakage

The easiest of the terms, the error correction is given by the following theorem.

Theorem 3.2.1. *For a reduction matrix $F \in \mathbb{Z}_2^{m\times n}$, acting on n copies of Equation (2.80), for identical basis choices of Alice and Bob $\vec{\alpha}$, the error correction cost with efficiency f is given by*

$$\delta_{leak}^{(\vec{\alpha},\vec{\alpha})} = f \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \right), \tag{3.28}$$

where $\mathrm{d}(\cdot)$ *is the hamming distance, $V \in \mathbb{Z}_2^{n\times m}$ such that $FV = I_m$, and $\tilde{V} \in \mathbb{Z}_2^{n\times n-m}$ such that* $\mathrm{Im}(\tilde{V}) = \ker(F)$.

A full proof can be found in Appendix B.1 but the general gist is as follows:

The error correction cost (up to the efficiency f) is given by $\mathrm{H}(R', Y) - \mathrm{H}(Y)$. We know that ρ_Y is maximally mixed so the term $\mathrm{H}(Y) = n$. The other term $\mathrm{H}(R', Y) = \mathrm{H}(\rho_{R',Y})$ for $\rho_{R'Y}$ from Equation (3.27) uses the block diagonal structure along with Theorem 2.3.14 to remove global unitary transformations. After some rearrangement we are left with

$$\mathrm{H}(R', Y) = 2^n \sum_{\vec{\gamma} \in \mathbb{Z}_2^m} \mathrm{Q} \left(\sum_{\vec{\beta} \in \mathbb{Z}_2^{n-m}} \left\langle \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right| \rho_{\text{single}AB}^{\otimes n} \left| \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right\rangle \right). \tag{3.29}$$

At first glance the product $\left\langle \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right| \rho_{\text{single}AB}^{\otimes n} \left| \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right\rangle$, seems to require evaluating the diagonal entries of a large matrix, but this can be reduced. Note that for $\rho_{\text{single}AB}$ defined in Equation (2.80),

$$(\langle 0|_A \otimes I_B) \rho_{\text{single}AB} (|0\rangle_A \otimes I_B) = \frac{1}{2} \left(\left(1 - \frac{\xi}{2} \right) |0\rangle\langle 0|_B + \frac{\xi}{2} |1\rangle\langle 1|_B \right). \tag{3.30}$$

Therefore, the product $\left\langle \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right| \rho_{\text{single}AB}^{\otimes n} \left| \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right\rangle$ reduces to counting the number of entries in $V\vec{\gamma} + \tilde{V}\vec{\beta}$ that are 0 (which select $\frac{1}{2}\left(1 - \frac{\xi}{2}\right)$) and the number of entries in $V\vec{\gamma} + \tilde{V}\vec{\beta}$ that are 1 (which select $\frac{1}{2}\frac{\xi}{2}$).[4] With the Hamming weight, we use the substitution

$$\left\langle \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right| \rho_{\text{single}AB}^{\otimes n} \left| \vec{0},\ V\vec{\gamma} + \tilde{V}\vec{\beta} \right\rangle = 2^{-n} \left(1 - \frac{\xi}{2} \right)^{n - \mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta})} \left(\frac{\xi}{2} \right)^{\mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta})}, \tag{3.31}$$

and the rest of the proof follows with some algebraic manipulation.

The Holevo Quantity

The Holevo quantity is by far the hardest part to solve. In this section we focus on using the block diagonal structure. Later in Section 3.3 we determine the eigenvalues. From Equation (3.11), the goal is to determine the privacy of the secret key $\mathrm{H}\left(R' \middle| \vec{\alpha}, \vec{\beta}\right) -$

[4] Recall that for the quantum bit error rate is $\frac{\xi}{2}$. So these are half the probability of getting no error, and an error respectively.

$\max_{\rho_{AB}\in\Gamma}\chi(R' : E|\vec{\alpha},\vec{\beta})$ for each pair of announcements $(\vec{\alpha},\vec{\beta})\in\mathcal{S}^n$. Just as for the error correction, we only need to solve the case that Alice and Bob measure all the states in the Z-basis. As such, we drop the notation for conditioning on the announcements. Furthermore, the quantum part of the six-state protocol was left unchanged (just grouped together). Therefore, adding pre-privacy amplification to six-state still leaves the protocol tomographically complete. This eliminates the minimization as there is only 1 state that satisfies all the constraints. Just as in Equation (2.77), we combine $\mathrm{H}(R')$ with the Holevo quantity and solve them together. Overall, the goal is to determine the following two terms:

1. Determine $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\mathrm{H}\left(p(\vec{\gamma})\rho_E^{(\vec{\gamma})}\right)$.
2. Determine $\mathrm{H}\left(\rho_E\right)$.

Lemma 3.2.2. *For a reduction matrix $F\in\mathbb{Z}_2^{m\times n}$, operating on n copies of Equation (2.80),*

$$\sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\mathrm{H}\left(p(\vec{\gamma})\rho_E^{(\vec{\gamma})}\right)=2^m\sum_{\vec{l}\in\mathbb{Z}_2^n}\mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}}Z^{\tilde{V}\vec{\beta}}\left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right|Z^{\tilde{V}\vec{\beta}}\right),\tag{3.32}$$

where $\tilde{V}\in\mathbb{Z}_2^{n\times n-m}$ and $\mathrm{Im}(\tilde{V})=\ker(F)$.

Proof. Without loss of generality we prove the statement for all measurements in the Z-basis (and drop writing $\vec{\alpha}$). We already showed in Section 3.2.1 that after a purification of n copies of Equation (2.80), Alice's key register and Eve hold the joint state $\rho_{R'E}$ from Equation (3.24). Measuring the key register in Equation (3.24) produces

$$p(\vec{\gamma})\rho_E^{(\vec{\gamma})}=\left|\vec{\gamma}\right\rangle\!\left\langle\vec{\gamma}\right|_{R'}\otimes\sum_{\vec{l}\in\mathbb{Z}_2^n}\left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_{E_1}\otimes\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}}Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}\left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right|_{E_2}Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}},\tag{3.33}$$

where $V\in\mathbb{Z}_2^{n\times m}$ such that $FV=I_m$, and $\tilde{V}\in\mathbb{Z}_2^{n\times n-m}$ such that $\mathrm{Im}(\tilde{V})=\ker(F)$ from

the theorem. We then simplify the expression using the block diagonal structure

$$\begin{aligned}\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_E^{(\vec{\gamma})}\right) &= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\Bigg(|\vec{\gamma}\rangle\langle\vec{\gamma}|_{R'} \otimes \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\left\langle\vec{l}\right|_{E_1} \\ &\qquad \otimes \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}} \Bigg) \\ &= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}\right) \\ &= 2^m \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{\tilde{V}\vec{\beta}}\right),\end{aligned} \tag{3.34}$$

where we removed the global unitary $Z^{V\vec{\gamma}}$. □

The term $\mathrm{H}(\rho_E)$ is solved for simply by using the marginal of $\rho_{R'E}$ found in Equation (3.25). We then get

$$\begin{aligned}\mathrm{H}(\rho_E) &= \mathrm{H}\left(\sum_{\vec{l},\vec{k}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\left\langle\vec{l}\right|_{E_1} \otimes Z^{\vec{k}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{\vec{k}}\right) \\ &= \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{k}\in\mathbb{Z}_2^n} Z^{\vec{k}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}| Z^{\vec{k}}\right).\end{aligned} \tag{3.35}$$

Combining these gives the Holevo term for a *block* of n qubits on identical basis choices $\vec{\alpha}$ for Alice and Bob

$$\begin{aligned}\mathrm{H}(R'|\vec{\alpha},\vec{\alpha}) - \max_{\rho_{AB}\in\Gamma} \chi(R':E|\vec{\alpha},\vec{\alpha}) = 2^m &\sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|_{E_2} Z^{\tilde{V}\vec{\beta}}\right) \\ &- \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{k}\in\mathbb{Z}_2^n} Z^{\vec{k}} |\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}| Z^{\vec{k}}\right).\end{aligned} \tag{3.36}$$

Key Rate

We combine the sifting, error correction, and Holevo quantity together to give the key rate for a *block* of n qubits as stated in the following theorem.

Theorem 3.2.3. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, acting on n copies of the shared state $\rho_{singleAB}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). The key rate per* block *of the six-state protocol with pre-privacy amplification is lower bounded by*

$$R_{blk}(F) \geq \left(\sum_{\vec{\alpha}\in\mathcal{A}^n} p(\vec{\alpha},\vec{\alpha})\right)\left[2^m \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}} \left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right| Z^{\tilde{V}\vec{\beta}}\right)\right. \tag{3.37}$$
$$- \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{k}\in\mathbb{Z}_2^n} Z^{\vec{k}} \left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right| Z^{\vec{k}}\right)$$
$$\left. - f\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})}\right)\right],$$

where the post-selection set of basis announcements is $\mathcal{S} = \{(\vec{\alpha},\vec{\alpha})|\vec{\alpha}\in\mathcal{A}^n\}$, the efficiency of error correction is $f \in [1,\infty)$, $V \in \mathbb{Z}_2^{n\times m}$ such that $FV = I_m$, and $\tilde{V} \in \mathbb{Z}_2^{n\times n-m}$ such that $\mathrm{Im}(\tilde{V}) = \ker(F)$.

Now that we have the key rate per block, it would be best to compare it with the key rate for the usual six-state protocol. However, in its current form, the six-state protocol with pre-privacy amplification gives the key rate for a block of n qubits, compared to the original six-state protocol which gives the key rate per qubit. The simple solution is to just divide the key rate per block by the number of qubits used to make it. Thus the key rate per qubit is given by,

$$R(F) = \frac{R_{\mathrm{blk}}(F)}{n}. \tag{3.38}$$

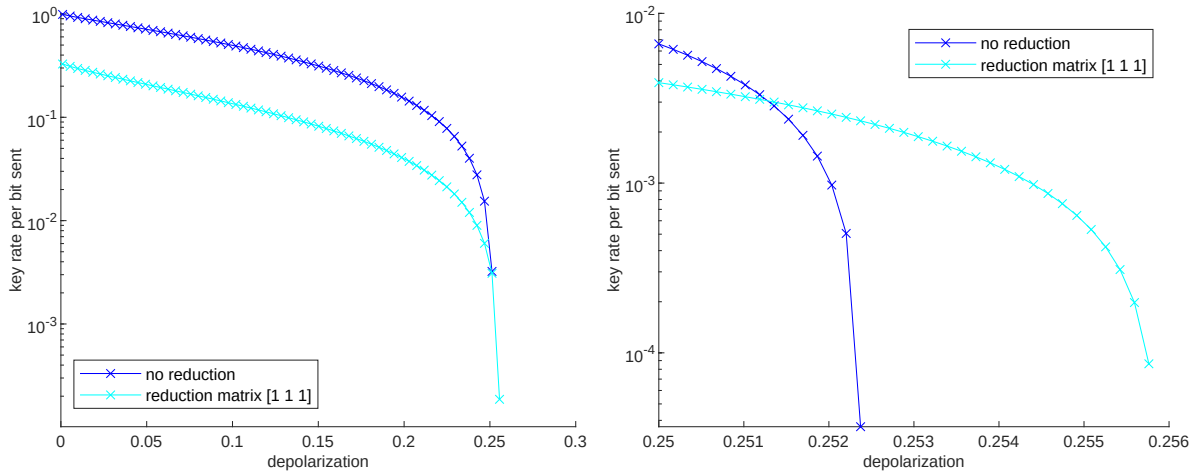
The reduction matrix $F = \big[1\big]$, is equivalent to performing no pre-privacy amplification on the six-state protocol, which we can quickly check. For basis choice biased heavily towards

Z, and substituting $F = \begin{bmatrix} 1 \end{bmatrix}$ into Equation (3.37), we get

$$\begin{aligned} \frac{R([1])}{\sum_{\vec{\alpha} \in \mathcal{A}^n} p(\vec{\alpha}, \vec{\alpha})} &\geq 2 \sum_{l \in \mathbb{Z}_2} \mathrm{H}\left(|\tau_l\rangle\langle\tau_l| \right) - \sum_{l \in \mathbb{Z}_2} \mathrm{H}\left(\sum_{k \in \mathbb{Z}_2} Z^k \, |\tau_l\rangle\langle\tau_l| \, Z^k \right) - f \sum_{\gamma \in \mathbb{Z}_2} \mathrm{Q}\left(\left(1 - \frac{\xi}{2}\right)^{\gamma} \left(\frac{\xi}{2}\right)^{1-\gamma} \right) \\ &= 1 + \mathrm{h}\left(\frac{\xi}{2}\right) - \mathrm{Q}\left(1 - \frac{3\xi}{4}\right) - 3\,\mathrm{Q}\left(\frac{\xi}{4}\right) - f\,\mathrm{h}\left(\frac{\xi}{2}\right), \end{aligned} \tag{3.39}$$

which matches the original biased basis choice key rate formula for the six-state protocol from Equation (2.91).

Before we continue, in Figure 3.2 we give a sneak preview of a single example of a reduction matrix on the six-state protocol that provides a small improvement to the key rate near the maximum tolerable depolarization.



(a) Coarse grained detail across full depolarization spectrum.

(b) Fine grained detail near maximum tolerable depolarization.

Figure 3.2: Comparison of the qubit six-state protocol to the qubit six-state protocol with reduction matrix $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ for a depolarizing channel. Error correction performed at the Shannon limit.

3.3 Determining the Eigenvalues

Although the key rate for a reduction matrix can be computed from Equation (3.37), it requires on the order of 2^n matrix diagonalizations to retrieve the eigenvalues for the entropy calculation. Compounding this, the dimension of $|\tau_{\vec{l}}\rangle$ is size 2^n and for a square matrix of size $a \times a$, diagonalization takes on the order of a^3 time. Furthermore, the space required to store and process these matrices also grows exponentially. For example, later in Chapter 4, the key rate formulation will have a similar form but will require diagonalizing matrices of size $4^n \times 4^n$. Each entry uses a double precision floating point number, which requires 8 bytes of memory. For pre-privacy amplification on 7 copies, a single matrix requires 2GB of Memory, and 8 copies require 32GB. [5] In this format, the density matrices must be stored as sparse arrays and clever eigenvalue solving algorithms must be employed. Fortunately, this can be avoided by analytically determining the eigenvalues.

To determine the eigenvalues we will rewrite terms from Equation (3.37) with CPTP maps of the form $\Phi_W(\rho) = \sum_{\vec{l} \in \mathbb{Z}_2^{n-m}} Z^{W\vec{l}} \rho Z^{W\vec{l}}$. We then show that these maps can be rewritten as orthonormal projections in the Z-basis, then determine the eigen values of the map acting on a pure (rank 1) state. Then, we show how to drastically speed up the final calculation with a few algebraic tricks.

3.3.1 Rewriting the Sum

From Equation (3.37), up to a constant the summations inside the entropy function have the form

$$\Phi_W(\rho) := 2^{-b} \sum_{\vec{l} \in \mathbb{Z}_2^b} Z^{W\vec{l}} \rho Z^{W\vec{l}}, \tag{3.40}$$

where $W \in \mathbb{Z}_2^{a \times b}$ and $a \geq b$. Analytically determining the eigenvalues of $\Phi_W(\rho)$ would drastically improve the speed of key rate calculations.

[5] Early in development, a naive implementation using the relative entropy was done. For the simplified trusted relay, it required 4 qubits, and 18 possible announcements. Using n copies would produce $288^n \times 288^n$ sized matrices. With double precision complex numbers requiring 16 bytes each, 2 copies alone would produce a matrix using over 110GB of RAM. Even when splitting off the announcements, the matrix was still $16^n \times 16^n$, and 4 copies would push the size to 68GB. In some sense the project was to compress dimensions, find symmetries, and push towards an analytic solution.

Theorem 3.3.1. *Let $W \in \mathbb{Z}_2^{a\times b}$ with $a \geq b$. The CPTP map $\Phi_W(\rho)$ can be rewritten as*

$$\Phi_W(\rho) = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{R}_W(\vec{\phi})\rho\,\mathrm{R}_W(\vec{\phi}), \tag{3.41}$$

where

$$\mathrm{R}_W(\vec{\phi}) := \sum_{\vec{k}\in\mathbb{Z}_2^a} \delta_{\vec{\phi},W^T\vec{k}} \left|\vec{k}\right\rangle\!\left\langle\vec{k}\right|, \tag{3.42}$$

and $\delta_{\vec{\phi},W^T\vec{k}}$ is the Kronecker delta comparing the vectors $\vec{\phi}$ and $W^T\vec{k}$.

A full proof can be found in Appendix B.2. Overall, the proof is given by acting Φ_W on the basis $\left\{\left|\vec{k}\right\rangle\!\left\langle\vec{k'}\right|\right\}_{\vec{k},\vec{k'}\in\mathbb{Z}_2^a}$ which gives

$$\Phi_W\left(\left|\vec{k}\right\rangle\!\left\langle\vec{k'}\right|\right) = \delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}} \left|\vec{k}\right\rangle\!\left\langle\vec{k'}\right|. \tag{3.43}$$

Therefore,

$$\Phi_W(\rho) = \sum_{\vec{k},\vec{k'}\in\mathbb{Z}_2^a} \delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}} \left|\vec{k}\right\rangle\!\left\langle\vec{k}\right| \rho \left|\vec{k'}\right\rangle\!\left\langle\vec{k'}\right|. \tag{3.44}$$

Rewriting the delta function using $\delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}} = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k'}}$ and rearranging completes the proof.

It is simple to show that

$$\mathrm{R}_W(\vec{\phi})\,\mathrm{R}_W(\vec{\varphi}) = \delta_{\vec{\phi},\vec{\varphi}}\,\mathrm{R}_W(\vec{\phi}), \tag{3.45}$$

thus, $\mathrm{R}_W(\vec{\phi})$ and $\mathrm{R}_W(\vec{\varphi})$ are orthogonal projections. This implies that Φ_W projects ρ into the subspaces characterized by solutions to $\vec{\phi} = W^{\mathrm{T}}\vec{k}$.[6] Because Φ_W uses 2^b Kraus operators and $|\psi\rangle\langle\psi|$ is rank 1, the rank of $\Phi_W(|\psi\rangle\langle\psi|)$ is at most 2^b. Therefore, $\Phi_W(|\psi\rangle\langle\psi|)$ must have the eigenvalue 0 with multiplicity at least 2^{a-b}. The rest of the eigenvalues constructed from

$$(\Phi_W(|\psi\rangle\langle\psi|))\left(\mathrm{R}_W(\vec{\phi})\,|\psi\rangle\right) = \langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle\left(\mathrm{R}_W(\vec{\phi})\,|\psi\rangle\right), \tag{3.46}$$

[6] If there is no $\vec{k}\in\mathbb{Z}_2^a$ such that $\vec{\phi} = W^{\mathrm{T}}\vec{k}$, then $\mathrm{R}_W(\vec{\phi}) = 0$ and it can be safely dropped.

which are orthogonal.[7] Using this, we remove the need to diagonalize $\Phi_W(|\psi\rangle\langle\psi|)$ for the entropy calculation. With a few extra steps, we get the following theorem.

Theorem 3.3.2. *Let $W \in \mathbb{Z}_2^{a\times b}$ with $a \geq b$, and $|\psi\rangle \in \mathbb{C}^{2^n}$, then*

$$\mathrm{H}\left(\Phi_W(|\psi\rangle\langle\psi|)\right) = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^a} \delta_{\vec{\phi},W^T\vec{k}} \left|\left\langle \vec{k}\middle|\psi\right\rangle\right|^2\right). \tag{3.47}$$

Furthermore, let $c = \mathrm{rank}(W^T)$, $\mathcal{W}$ a representative space of W^T, $W_1 \in \mathbb{Z}_2^{a\times c}$ such that $\mathrm{Im}(W_1) = \mathcal{W}$, $W_2 \in \mathbb{Z}_2^{a\times a-c}$ such that $\mathrm{Im}(W_2) = \ker(W^T)$, then

$$\mathrm{H}\left(\Phi_W(|\psi\rangle\langle\psi|)\right) = \sum_{\vec{k}_1\in\mathbb{Z}_2^c} \mathrm{Q}\left(\sum_{\vec{k}_2\in\mathbb{Z}_2^{a-c}} \left|\left\langle W_1\vec{k}_1 + W_2\vec{k}_2\middle|\psi\right\rangle\right|^2\right). \tag{3.48}$$

A full proof can be found in Appendix B.3. The first part of Theorem 3.3.2 is the result of rewriting the eigenvalues $\langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle$ with the definition of $\mathrm{R}_W(\vec{\psi})$ from Equation (3.42). With this, we have removed the need to diagonalize a $2^a \times 2^a$ matrix built from 2^b summations, and replaced them with calculating 2^{a+b} terms of the form $\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\left|\left\langle \vec{k}\middle|\psi\right\rangle\right|^2$. But, we can still do better. Like how we used Theorem 3.1.3, to break down reduction matrices into elements from a representative space and kernel, we can use Theorem 3.1.3 to break down W^{T}. In fact, doing so reduces the number of sums from 2^{a+b} to just 2^a sums of the terms $\left|\left\langle W_1\vec{k}_1 + W_2\vec{k}_2\middle|\psi\right\rangle\right|^2$.

We have one final note before we use this theorem to rewrite the Holevo quantity terms in Equation (3.37). When W^{T} is a reduction matrix, then in Equation (3.48), $c := \mathrm{rank}(W^{\mathrm{T}}) = b$ and the dimensions of W_1 and W_2 are simply derived from the dimensions of W. Furthermore, following from Theorem 3.1.5, we choose $W_1 \in \mathbb{Z}_2^{a\times b}$ such that $W^{\mathrm{T}}W_1 = I_b$. Applying applying the theorem and observation to the Holevo terms in the key rate

[7] There is a slight caveat, if $\mathrm{R}_W(\vec{\phi})\,|\psi\rangle = 0$, then it obviously can't be an eigenvector. However, this also reduces the rank of $\Phi(|\psi\rangle\langle\psi|)$ garunteeing that there is just another eigenvalue of 0.

Equation (3.37) gives:

$$2^m \sum_{\vec{l} \in \mathbb{Z}_2^n} \mathrm{H}\left(\Phi_{\tilde{V}}\left(|\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|\right)\right) = 2^m \sum_{\vec{l} \in \mathbb{Z}_2^n} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m}} \mathrm{Q}\left(2^{n-m} \sum_{\vec{k} \in \mathbb{Z}_2^m} \left|\left\langle W_1 \vec{\phi} + W_2 \vec{k} \middle| \tau_{\vec{l}} \right\rangle\right|^2\right), \tag{3.49}$$

$$\sum_{\vec{l} \in \mathbb{Z}_2^n} \mathrm{H}\left(\Phi_{I_n}\left(|\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|\right)\right) = \sum_{\vec{l}, \vec{\phi} \in \mathbb{Z}_2^n} \mathrm{Q}\left(2^n \left|\left\langle \vec{\phi} \middle| \tau_{\vec{l}} \right\rangle\right|^2\right), \tag{3.50}$$

where $W_1 \in \mathbb{Z}_2^{n \times n-m}$ such that $\tilde{V}^{\mathrm{T}} W_1 = I_{n-m}$ and $W_2 \in \mathbb{Z}_2^{n \times m}$ such that $\mathrm{Im}(W_2) = \ker(\tilde{V})$. Furthermore, with Theorem 3.3.3, we can replace W_2 with F^{T}, where F is the original reduction matrix.

Theorem 3.3.3. *For a reduction matrix $F \in \mathbb{Z}_2^{m \times n}$, $V \in \mathbb{Z}_2^{n \times m}$ such that $FV = I_m$, and $\tilde{V} \in \mathbb{Z}_2^{n \times n-m}$ such that $\mathrm{Im}(\tilde{V}) = \ker(F) \simeq \mathbb{Z}_2^{n-m}$, then $V^T F^T = I_m$, and $\mathrm{Im}(F^T) = \ker(\tilde{V}^T)$.*

Proof. The first property is easy, $FV = I_m$ therefore $V^{\mathrm{T}} F^{\mathrm{T}} = I_m$. For the second property, note that F is full rank, thus $m = \mathrm{rank}(F) = \mathrm{rank}(F^{\mathrm{T}})$. Now $\tilde{V}$ was constructed just so that $F\tilde{V} = 0$. Therefore, $\tilde{V}^{\mathrm{T}} F^{\mathrm{T}} = 0$, and $\mathrm{Im}(F^{\mathrm{T}}) \subseteq \ker(\tilde{V}^{\mathrm{T}})$. Because $\tilde{V}$ is injective, $\tilde{V}^{\mathrm{T}}$ is surjective, and $\dim(\mathrm{Im}(\tilde{V}^{\mathrm{T}})) = n - m$. This implies $\dim(\ker(\tilde{V}^{\mathrm{T}})) = m$. This gives us that $\dim(\mathrm{Im}(F^{\mathrm{T}})) = \dim(\ker(\tilde{V}^{\mathrm{T}}))$, therefore $F^{\mathrm{T}} \in \mathbb{Z}_2^{n \times m}$ and $\mathrm{Im}(F^{\mathrm{T}}) = \ker(\tilde{V}^{\mathrm{T}})$. □

This form for the Holevo terms is significantly faster to compute. It contains no eigenvalue calculations, no linear algebra over the real or complex numbers, and it uses vastly less memory. It still takes an exponential amount of time to compute. At this point it requires 4^n summations and an inner product on vectors of size 2^n, but the problems can now be solved for larger values of n and m, and numerical techniques like parallel pools can be used to split up the problem for multiple CPU cores.

3.3.2 Speeding up the Sum

Although the key rate equation using the formulation of Theorem 3.2.3 is significantly faster and less resource intensive when we rewrite the Holevo terms with Equations (3.49) and

(3.50), it still grows exponentially in the number of summations. As such, it is important to find time savings for each sum. Here the obvious target is the inner products of the form $\left|\left\langle W_1\vec{\phi} + W_2\vec{k}\middle|\tau_{\vec{l}}\right\rangle\right|^2$. In this form, each inner product requires us to construct vectors of size 2^n, however, we only need a few of the components each time. Like in Equation (B.9), we aim to turn the inner product of terms like $\left|\left\langle W_1\vec{\phi} + W_2\vec{k}\middle|\tau_{\vec{l}}\right\rangle\right|^2$ into exponentials with exponents using Hamming weights.

Theorem 3.3.4. *Let* $\vec{k}, \vec{l} \in \mathbb{Z}_2^a$*, then*

$$\left|\left\langle \vec{k}\middle|\tau_{\vec{l}}\right\rangle\right|^2 = \frac{1}{2}\left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k},\vec{l})}\left(\frac{\xi}{4}\right)^{a-\tilde{\mathrm{d}}(\vec{k},\vec{l})}, \tag{3.51}$$

where $\tilde{\mathrm{d}}(\vec{k}, \vec{l}) := \mathrm{d}((\vec{k} + \vec{1s}) \odot (\vec{k} + \vec{1s}))$*,* $\odot$ *denotes element-wise multiplication, and* $\vec{1s}$ *is the vector of all ones.*

Proof. Let $\vec{k}, \vec{l} \in \mathbb{Z}_2^a$. We then break down the inner product as

$$\left|\left\langle \vec{k}\middle|\tau_{\vec{l}}\right\rangle\right|^2 = \prod_{i=1}^{n} |\langle k_i|\tau_{l_i}\rangle|^2. \tag{3.52}$$

For a single term note that

$$|\langle i|\tau_j\rangle|^2 = \frac{1}{2}\begin{cases} 1 - \frac{3\xi}{4}, & i = j = 0 \\ \frac{\xi}{4}, & \text{otherwise} \end{cases}. \tag{3.53}$$

So the problem will reduce to counting the number of terms where the entries in $\vec{k}$ and $\vec{l}$ are both 0. Now note that $i = j = 0$ is equivalent to the logical expression NOT i AND NOT j, which we can express in $\mathbb{Z}_2$ as $(i+1)(j+1)$. We can vectorize this by for $\vec{k}$ and $\vec{l}$ by swapping $+1$ with $+\vec{1s}$ and using element wise multiplication, $\odot$. We then count the entries where we get ones with the the Hamming weight. We denote this counting process with the function

$$\tilde{\mathrm{d}}(\vec{k}, \vec{l}) := \mathrm{d}((\vec{k} + \vec{1s}) \odot (\vec{l} + \vec{1s})). \tag{3.54}$$

Applying this counting to the product gives

$$\left|\left\langle \vec{k} \middle| \tau_{\vec{l}} \right\rangle\right|^2 = 2^{-a} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k},\vec{l})} \left(\frac{\xi}{4}\right)^{a-\tilde{\mathrm{d}}(\vec{k},\vec{l})}, \tag{3.55}$$

completing the proof. □

Applying to Equation (3.48) using $|\psi\rangle = |\tau_{\vec{l}}\rangle$ gives the simplified form

$$\begin{aligned} &\mathrm{H}\left(\Phi_W(|\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|)\right) \\ &\quad = \sum_{\vec{k}_1 \in \mathbb{Z}_2^c} \mathrm{Q}\left(2^{-a} \sum_{\vec{k}_2 \in \mathbb{Z}_2^{a-c}} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{k}_1 + W_2\vec{k}_2, \vec{l})} \left(\frac{\xi}{4}\right)^{a-\tilde{\mathrm{d}}(W_1\vec{k}_1 + W_2\vec{k}_2, \vec{l})}\right). \end{aligned} \tag{3.56}$$

We have thus taken the inner product from exponential to polynomial running time. Applying this to the key rate in Theorem 3.2.3 using the rewritten entropy terms from Equations (3.49) and (3.50), and simplifying with Theorem 3.3.3 gives the following lower bound.

Theorem 3.3.5. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, acting on the shared state $\rho_{singleAB}^{\otimes n}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). The key rate per* block *of the six-state*

protocol with pre-privacy amplification is lower bounded by

$$
\begin{aligned}
R_{blk}(F) \geq & \left(\sum_{\vec{\alpha} \in \mathcal{A}^n} p(\vec{\alpha}, \vec{\alpha}) \right) \\
& \left[2^m \sum_{\vec{l} \in \mathbb{Z}_2^n} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m}} \mathrm{Q} \left(2^{-m} \sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1 \vec{\phi} + F^T \vec{k}, \vec{l})} \left(\tfrac{\xi}{4}\right)^{n - \tilde{\mathrm{d}}(W_1 \vec{\phi} + F^T \vec{k}, \vec{l})} \right) \right. \\
& \qquad \left. - \sum_{\vec{l}, \vec{\phi} \in \mathbb{Z}_2^n} \mathrm{Q} \left(\left(1 - \tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{\phi}, \vec{l})} \left(\tfrac{3\xi}{4}\right)^{n - \tilde{\mathrm{d}}(\vec{\phi}, \vec{l})} \right) - \delta_{leak} \right] \\
= & \left(\sum_{\vec{\alpha} \in \mathcal{A}^n} p(\vec{\alpha}, \vec{\alpha}) \right) \\
& \left[m + \sum_{\vec{l} \in \mathbb{Z}_2^n} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m}} \mathrm{Q} \left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1 \vec{\phi} + F^T \vec{k}, \vec{l})} \left(\tfrac{\xi}{4}\right)^{n - \tilde{\mathrm{d}}(W_1 \vec{\phi} + F^T \vec{k}, \vec{l})} \right) \right. \\
& \qquad \left. - n \left(\mathrm{Q} \left(1 - \tfrac{3\xi}{4}\right) + 3\, \mathrm{Q} \left(\tfrac{\xi}{4}\right) \right) - \delta_{leak} \right],
\end{aligned}
\tag{3.57}
$$

where:

- *The post-selection set of basis announcements is* $\mathcal{S} = \{(\vec{\alpha}, \vec{\alpha}) | \vec{\alpha} \in \mathcal{A}^n\}$.
- $\delta_{leak} = f \sum_{\vec{\gamma} \in \mathbb{Z}_2^m} \mathrm{Q} \left(\sum_{\beta \in \mathbb{Z}_2^{n-m}} \left(1 - \frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n - \mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta})} \right)$.
- $f \in [1, \infty)$ *is the efficiency of error correction.*
- $V \in \mathbb{Z}_2^{n \times m}$ *such that* $FV = I_m$.
- $\tilde{V} \in \mathbb{Z}_2^{n \times n-m}$ *such that* $\mathrm{Im}(\tilde{V}) = \ker(F) \simeq \mathbb{Z}_2^{n-m}$.
- $W_1 \in \mathbb{Z}_2^{n \times n-m}$ *such that* $\tilde{V}^T W_1 = I_{n-m}$.
- $|\tau_{\vec{l}}\rangle = \bigotimes_{i=0}^{n} |\tau_{l_i}\rangle$.

- $|\tau_0\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{1-\frac{3\xi}{4}}\,|0\rangle + \sqrt{\frac{\xi}{4}}\,|1\rangle\right)$, *and* $|\tau_1\rangle = \sqrt{\frac{\xi}{4}}\,|+\rangle$.

The final simplifications are the result of applying common properties like the ones in Theorem 2.3.6 along side the binomial theorem. In this form we no longer have any matrices or vectors that require exponential amounts of memory as we increase the number of copies n we start with. The time it takes to evaluate is still exponential and grows roughly at 4^n summations. At this point further speed ups require understanding symmetries with reduction matrices and the key rate equation.

3.4 Equivalence of Reduction Matrices

Now that we can determine the key rate for a single reduction matrix in a (relatively) reasonable time frame, it begs the question: "For a given amount of depolarization ξ, what is the optimal choice of reduction matrix to boost the key rate?". A brute force search checking every possible reduction matrix is infeasible as there are $\prod_{i=0}^{m-1}(|\mathcal{R}|^n - |\mathcal{R}|^i)$ full rank matrices in $\mathcal{R}^{m\times n}$. As such it is imperative to determine when distinct reduction matrices will give identical key rates. In this section, we identify 3 ways to find reduction matrices that give the same key rate and to simplify computation. They are:

1. Equivalence under row operations.
2. Equivalence under column permutations (for permutation invariant states).
3. Exploiting block diagonal structure (for separable states).

Not only do these conditions help us filter our search, but they also highlight symmetries which we can use to improve our calculation's performance.

3.4.1 Equivalence Under Row Operations

The easiest of the 3, applying row operations to a reduction matrix, is an important special case of Theorem 2.3.6 which states that classical entropy is invariant under a permutation of the indices of our probability distribution.

Theorem 3.4.1. *Let $n \geq m$, $\mathcal{R}$ a finite field, a reduction matrix $F \in \mathcal{R}^{m\times n}$, and a invertible matrix $U \in \mathrm{GL}_m(\mathcal{R})$. Then for the reduction matrix $F' = UF$, $R_{blk}(F') = R_{blk}(F)$.*

Proof. Let F, U, and F' be defined as above. From the general procedure in Section 3.1.1, Alice Bob and Eve share the state $|\rho\rangle\langle\rho|_{ABE}$. After applying measurements, and the initial key mapping, they share the state ρ_{RYEC}. Next they apply the pre-privacy amplification with F and their shared state is

$$\begin{aligned}\rho_{R'YEC} &= \mathcal{E}_{\mathrm{PPA},R\to R'}(\rho_{RYEC}) \\ &= \sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_{R'} \otimes \mathrm{Tr}_R\left[(|\vec{r}\rangle\langle\vec{r}|_R \otimes I_{YEC})\rho_{RYEC}\right].\end{aligned} \tag{3.58}$$

Similarly, when they use the new reduction matrix F', their shared state is

$$\rho'_{R'YEC} = \sum_{\vec{r}\in\mathcal{R}^n} |UF\vec{r}\rangle\langle UF\vec{r}|_{R'} \otimes \mathrm{Tr}_R\left[(|\vec{r}\rangle\langle\vec{r}|_R \otimes I_{YEC})\rho_{RYEC}\right]. \tag{3.59}$$

All what we have done is permute the labels for the classical register R'. This is an invertible process so the Holevo quantity and error correction leakage are unchanged. □

Note that the proof used only a general pure state $|\rho\rangle_{ABE}$ and did not require any specific structure. As such, this theorem applies to all protocols with pre-privacy amplification that follow the general procedure in Section 3.1.1. From this proof, only reduction matrices in reduced row echelon form (Definition 2.1.10) need to be considered. This significantly reduces the search space for optimal reduction matrices. For example, for the six-state protocol we are analyzing, the reduction matrices

$$F_1 = \begin{bmatrix}1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\end{bmatrix}, F_2 = \begin{bmatrix}1 & 1 & 0 & 0\\ 0 & 1 & 1 & 1\end{bmatrix}, \tag{3.60}$$

have the same reduced row echelon form and key rate for any choice of depolarization.

3.4.2 Equivalence Under Column Permutation

Unlike Theorem 3.4.1 which worked for any ρ_{AB}. Equivalence of column permutations require ρ_{AB} to be permutation invariant across Alice and Bob's subsystems.[8] For example, when ρ_{AB} is permutationaly invariant, the reduction matrix,

$$F_3 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}, \tag{3.61}$$

has the exact same key rate as the reduction matrices F_1 and F_2 from the previous section, even though it has a different reduced row echelon form. We formalize this with the following theorem:

Theorem 3.4.2. *Let $n \geq m$, $\mathcal{R}$ a finite field, a reduction matrix $F \in \mathcal{R}^{m\times n}$, and $\pi \in \mathrm{S}_n$. If ρ_{AB} is permutation invariant, then for the reduction matrix $F' = FP_\pi$, $R_{blk}(F) = R_{blk}(F')$.*

A full proof can be found in appendix B.4. The general idea of the proof is that our new pre-privacy amplification map $\mathcal{E}^{(F')}_{\mathrm{PPA},R\to R'}$ can be written as a permutation of the original key registers in R followed by the reduction map $\mathcal{E}^{(F')}_{\mathrm{PPA},R\to R'}$, written as $\mathcal{E}^{(F)}_{\mathrm{PPA},R\to R'} \circ U_{R,\pi}$. Roughly speaking, we push the permutation through Alice and Bob's original key map and measurements, $\mathcal{E}^{\otimes n}_{XC\to RC} \circ \mathcal{E}'^{\otimes n}_{AB\to XYC}$, using Theorem A.2.8, then use the permutation invariance of ρ_{AB} to absorb the permutation.

We can combine Theorems 3.4.1 and 3.4.2 to vastly simplify the reduction matrices we must consider and increase the speed to evaluate the protocol over all reduction matrices. For any reduction matrix $F_1 \in \mathcal{R}^{m\times n}$ we can find a reduction matrix F_2 such that F_2 has the form $\begin{bmatrix} I_m & F' \end{bmatrix}$, where $F' \in \mathcal{R}^{m\times n-m}$. This is just the standard form of a parity check matrix, and is obtained by computing the reduced row echelon form of F_1, then permuting the columns so the pivots form block I_m.

In Appendix D, we use this form of the reduction matrix to improve the performance of the key rate calculation in Theorem 3.3.5 from 4^n summations to $4^m 3^{n-m}$ summations (up to a small polynomial contribution). Although numerically useful, it provides little further insight into reduction matrices that produce the same key rate.

[8] In other words we can swap the subsystems A_iB_i with A_jB_j without changing ρ_{AB}.

Combining Row Operations and Column Permutations

Now that we can focus on just matrices in the standard form $\begin{bmatrix} I_m & F' \end{bmatrix}$ with $F' \in \mathcal{R}^{m\times n-m}$, how many reduction matrices do we have to search through? Right away, the possible choices for F' gives us the upper bound of $|\mathcal{R}|^{m(n-m)}$. Though, Theorems 3.4.1 and 3.4.2, produce a stricter equivalence relation for matrices $F_1, F_2 \in \mathcal{R}^{m\times n}$,

$$F_1 \sim F_2 \iff \exists U \in \mathrm{GL}_m(\mathcal{R}), \pi \in \mathrm{S}_n \text{ such that } UF_1P_\pi^{-1} = F_2. \tag{3.62}$$

This leaves the question "How do we enumerate/determine representatives of these equivalence classes?". Unfortunately, this is extremely difficult to determine. To get a sense of the difficulties, we rearrange the equivalence relation to $UF_1 = F_2P_\pi$, which is equivalent to checking if there exists a permutation $\pi \in \mathrm{S}_n$ such that F_1 and F_2P_π have the same reduced row echelon form. However, the reduced row echelon form is not invariant under column permutations. Therefore, we must search through many different permutations. Not to be discouraged, there are still many cases we can efficiently check. For example, if we limit ourselves to permutations or the rows and columns, we can relate the problem to 2-color graphs. Here we focus on the field $\mathbb{Z}_2$.[9]

Definition 3.4.3. For a matrix $F \in \mathbb{Z}_2^{a\times b}$ we define the bijection $\mathcal{G}$ from $\mathbb{Z}_2^{a\times b}$ to the undirected bipartite 2-color graphs with a green "output" vertices and b blue "input" vertices. For the graph $\mathcal{G}(F)$, the edge between the blue vertex j and the green vertex i exists if and only if $\vec{e}_i^{\,\mathrm{T}} F \vec{e}_j = 1$.

In other words, if we lay out the adjacency matrix for $\mathcal{G}(F)$ as the green output vertices followed by the blue input vertices, the adjacency is

$$\begin{bmatrix} 0 & F \\ F^{\mathrm{T}} & 0 \end{bmatrix}. \tag{3.63}$$

An example of Definition 3.4.3 is given in Figure 3.3. At this point, determining if reduction matrices $F_1, F_2 \in \mathbb{Z}_2^{m\times n-m}$ are related by permutation is equivalent to determining if $\mathcal{G}(F_1)$ is isomorphic to $\mathcal{G}(F_2)$ by permuting vertices with the same colour.[10] It is well known that the complexity of this problem is equivalent to the general graph isomorphism problem [32],

[9] Though, many of the results here can be extrapolated to other finite fields.
[10] In other words, the bijection $\mathcal{G}$ is an isomorphism for permutations.

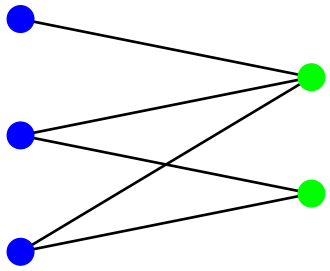


Figure 3.3: Example of the bijection from Definition 3.4.3 applied to the matrix $F = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$. The blue and green nodes represent the input and output systems respectively. Permuting rows and columns of F is equivalent to permuting nodes with the same colour.

which was only recently shown to have an algorithm that solves it in quasi-polynomial time [33].[11] So long as the algorithm used to determine is if $\mathcal{G}(F_1)$ is isomorphic to $\mathcal{G}(F_2)$ is relatively fast compared to calculating the key rate, we can still save a large chunk of time. Furthermore, we can combine this with a few techniques for permutation on matrices in standard form.

Lemma 3.4.4. *Let $F = \begin{bmatrix} I_m & F' \end{bmatrix}$ be a reduction matrix with $F' \in \mathbb{Z}_2^{m \times n-m}$. For all permutations $\tilde{\pi} \in \mathrm{S}_m$, there exists a permutation $\pi \in \mathrm{S}_n$ such that*

$$P_{\tilde{\pi}} F P_{\pi}^{-1} = \begin{bmatrix} I_m & P_{\tilde{\pi}} F' \end{bmatrix}. \tag{3.64}$$

Proof. $P_{\tilde{\pi}} F = \begin{bmatrix} P_{\tilde{\pi}} & P_{\tilde{\pi}} F' \end{bmatrix}$ So we need to transform $P_{\tilde{\pi}}$ back to I_m. To do so, simply choose π such that for all $i \in \{1, \ldots, m\}$, $\pi(i) = \tilde{\pi}(i)$ and for all $i \in \{m+1, \ldots n\}$, $\pi(i) = i$. □

In other words, if a reduction matrix F is given in standard form $\begin{bmatrix} I_m & F' \end{bmatrix}$ (or if we transform it to standard form), then we can limit our row and column permutations of F to just permutations of F'. For example, we can sort the columns of F'. Let $\{\vec{f}_1, \ldots \vec{f}_{n-m}\} \subset \mathcal{R}^m$ be the columns of F'. In other words, $F' = \begin{bmatrix} \vec{f}_1 \ldots \vec{f}_{n-m} \end{bmatrix}$. We then transform $\vec{f}_i$ to an integer f_i by treating $\vec{f}_i$ as a string of of digits for an integer in base $|\mathcal{R}|$. We then permute the columns so that for all $i \leq j$, $f_i \leq f_j$. Therefore, we only need to consider F' whose columns represent integers in ascending order. This can be easily enumerated and

[11] Which is *far* beyond the scope of this project.

there are $\binom{n-m+|\mathcal{R}|^m-1}{n-m}$ reduction matrices of this form.[12] For reduction matrices that take many copies to only a few, this massively cuts down the number of reduction matrices to iterate over. Furthermore, before calculating the key rate for the reduction matrix with augment F', we sort the rows and check if it was already computed. This further cuts down the number of steps needed. For example, sorting the rows of the augments

$$F_1' = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, F_2' = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}, \tag{3.65}$$

both produce

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}. \tag{3.66}$$

Therefore, F_1' and F_2' are related and we only need to calculate one of them.

3.4.3 Decomposing Reduction Matrices

In the previous section, we demonstrated multiple ways to speed up calculation and reduce the number of reduction matrices that need to be checked using a combination of row operations and column permutations. In this section we show that if a reduction matrix can be written in a block diagonal form (and Alice and Bob's shared state shares a similar tensor product structure), then we can break the key rate calculation into separate independent chunks that can be calculated in parallel. Furthermore, we show that any reduction matrix of this form performs no better than a different smaller reduction matrix.

We start with the basic underlying theorem used in this section.

Theorem 3.4.5. *Let $F_1 \in \mathcal{R}^{m_1 \times n_1}$, and $F_2 \in \mathcal{R}^{m_2 \times n_2}$ be reduction matrices on key registers with finite field $\mathcal{R}$. Let $n = n_1 + n_2$ and $m = m_1 + m_2$. If Alice and Bob's shared State has the form $\rho_{AB} = \rho_{A_1^{n_1} B_1^{n_1}} \otimes \rho_{A_{n_1+1}^n B_{n_1+1}^n}$, then the reduction matrix*

$$F = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}, \tag{3.67}$$

[12] It is a simple stars and bars problem with $|\mathcal{R}|^m$ distinguishable bins and $n-m$ indistinguishable items.

has key rate per block $R_{blk}(F) = R_{blk}(F_1) + R_{blk}(F_2)$.

A full proof can be found in Appendix B.5. The overall picture is that if we can break the reduction matrix F down in this manor, then the key register $|F\vec{r}\rangle\langle F\vec{r}|_{R'}$ with $\vec{r} \in \mathcal{R}^n$ from Equation (3.8) can be rewritten in the form

$$\begin{aligned} |F\vec{r}\rangle\langle F\vec{r}|_{R'} &= |F_1\vec{r}_1 \oplus F_2\vec{r}_2\rangle\langle F_1\vec{r}_1 \oplus F_2\vec{r}_2|_{R'} \\ &= |F_1\vec{r}_1,\ F_2\vec{r}_2\rangle\langle F_1\vec{r}_1,\ F_2\vec{r}_2|_{R'}\,, \end{aligned} \tag{3.68}$$

where $\vec{r}_1 \in \mathcal{R}^{n_1}$ and $\vec{r}_2 \in \mathcal{R}^{n_2}$. We then propagate this split through Alice and Bob's measurement and key mapping. We are then left with the tensor product of two completely separate protocols, one on the n_1 subsystems of $\rho_{A_1^{n_1}B_1^{n_1}}$ and the other on the n_2 subsystems of $\rho_{A_{n_1+1}^n B_{n_1+1}^n}$.

Theorem 3.4.5 allows many key rates to be calculated using significantly less time and resources. When we look at the key rate per *qudit* instead of per block, we can see that the key rate is the (convex) weighted average

$$R(F) = \frac{n_1 R(F_1) + n_2 R(F_2)}{n}. \tag{3.69}$$

If Alice and Bob's state is I.I.D., then $R(F) \leq \max\{R(F_1), R(F_2)\}$. Therefore, when searching for an optimal reduction matrix up to dimensions $m \times n$, if Alice and Bob share an I.I.D. state, then any reduction matrix matrix cannot give a higher key rate per qubit than at least one of its components. We can use this to reject reducible reduction matrices without needing to calculate their key rates! In a similar vein, we can remove columns of all zeros from reduction matrices without changing the key rate per block sent.

Theorem 3.4.6. *For the field $\mathcal{R}$ and reduction matrix $F \in \mathcal{R}^{m\times n}$, the reduction matrix $\tilde{F} = \begin{bmatrix} F & 0 \end{bmatrix} \in \mathcal{R}^{m\times n+1}$ has key rate $R_{blk}(\tilde{F}) = R_{blk}(F)$, if Alice and Bob's shared state has the form $\rho_{AB} = \rho_{A_1^n B_1^n} \otimes \rho_{A_{n+1}B_{n+1}}$.*

Proof. The proof is near identical to the proof for Theorem 3.4.5, and it gives $R_{\text{blk}}(\tilde{F}) = R_{\text{blk}}(F) + R_{\text{blk}}(0)$. The matrix that maps everything to zero only has one possible state and contains no information. Therefore, $R_{\text{blk}}(\tilde{F}) = R_{\text{blk}}(F)$. □

Therefore, we can reject any reduction matrix that has one or more columns of all

zeros. We combine Theorems, 3.4.5 and 3.4.6 to define a class of reduction matrices worth calculating the key rate of for n to m reduction of I.I.D. states.

Definition 3.4.7. A reduction matrix $F \in \mathcal{R}^{m\times n}$ is called *reducible* if,

1. it has at least one column of all zeros,
2. or there exists a permutation $\pi \in \mathrm{S}_n$ and a matrix $U \in \mathrm{GL}_m(\mathcal{R})$ such that UFP_π can be written in the form $\begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}$ from Theorem 3.4.5.

Otherwise, F is called *irreducible*.

In other words, a reduction matrix F is reducible if we can apply Theorem 3.4.6 to remove a column of all zeros, or if we can apply Theorem 3.4.5 to split F into separate blocks after applying row operations and/or column permutations. It is thus desirable to only calculate the key rate for irreducible reduction matrices. Determining if a matrix is reducible can be difficult by only applying row operations and column permutations, but we can relate the problem to checking the connectedness of the graph after translating to the standard form $\begin{bmatrix} I_m & F' \end{bmatrix}$.

Theorem 3.4.8. *Let $F \in \mathcal{R}^{m\times n}$ be a reduction matrix, and let $\mathcal{F} := \{\vec{f}_i\}_{i=1,\dots m}$ be the columns of F. Let the reduced row echelon form be* $\mathrm{rref}(F)$*. The following are equivalent:*

1. *F is reducible.*
2. *There exists a proper subset $J \subset \mathcal{F}$ such that $J \neq \emptyset$ and* $\mathrm{span}(J) \cap \mathrm{span}(\mathcal{F}/J) = \{\vec{0}\}$.
3. *The graph $\mathcal{G}(\mathrm{rref}(F))$ is disconnected (ie. there exists a pair of nodes that are not connected by any path).*[13]

A full proof can be found in appendix B.6. The proof is done in a cycle. The case for when F contains a column of all zeros is trivial, but for the other case, more care is needed. Much of the proof relies on the fact that the reduced row echelon form of F is obtained by multiplying an invertible matrix $U \in \mathrm{GL}_m(\mathcal{R})$ and is equivalent to a change of basis. This

[13] When the finite field $\mathcal{R}$ is not $\mathbb{Z}_2$, we modify 3.4.3 by giving the edges labels $\vec{e}_i^{\mathrm{T}} F \vec{e}_j$ (when $\vec{e}_i^{\mathrm{T}} F \vec{e}_j \neq 0$).

way we can analyze the structure of F in a significantly simpler form, then we translate back.

For a small additional optimization, when working with the standard form $\begin{bmatrix} I_m & F' \end{bmatrix}$, we only need to analyze the augment, F'.

Theorem 3.4.9. *Let $F = \begin{bmatrix} I_m & F' \end{bmatrix}$ be a reduction matrix with $F' \in \mathbb{Z}_2^{m \times n-m}$. $\mathcal{G}(F)$ is connected if and only if $\mathcal{G}(F')$ is connected.*

Proof. Adding and removing vertices with only one edge does not change the connectivity of a graph. All the blue input vertices associated with I_m have only one edge. □

Algorithms exist to determine the connectivity of a graph in $\mathcal{O}(V + E)$ where V is the number of vertices and E the number of edges. Therefore, it is easy to remove many reduction matrices in the form $\begin{bmatrix} I_m & F' \end{bmatrix}$ by checking if their graph is not connected.

3.4.4 Final Algorithm for Filtering Reduction Matrices

All together we use the following approach to sort through n to m reduction matrices for the six-state protocol with pre-privacy amplification on I.I.D. states:

1. Iterate over $F \in \mathbb{Z}_2^{m \times n}$, with form $F = \begin{bmatrix} I_m & F' \end{bmatrix}$. Furthermore, F' has the form $F' = \begin{bmatrix} \vec{f}_1 & \dots & \vec{f}_{n-m} \end{bmatrix}$, where if each column $\vec{f}_i$ is treated as the digits of an integer f_i, then $0 < f_1 \leq \cdots \leq f_{n-m}$.
2. Check if $\mathcal{G}(F)$ is connected. If it is not, reject F as better reduction matrices exist.
3. Sort the rows of F' (the same method for columns can be used) and check if it matches a previous reduction matrix. If so, reject F as we have already calculated its key rate.
4. Use the sorted row version of F to calculate the key rate.
5. Record the sorted row version of F and the key rate.

Although this still repeats some equivalence classes for row operations and column permutations, it is significantly less than before.

3.5 Results

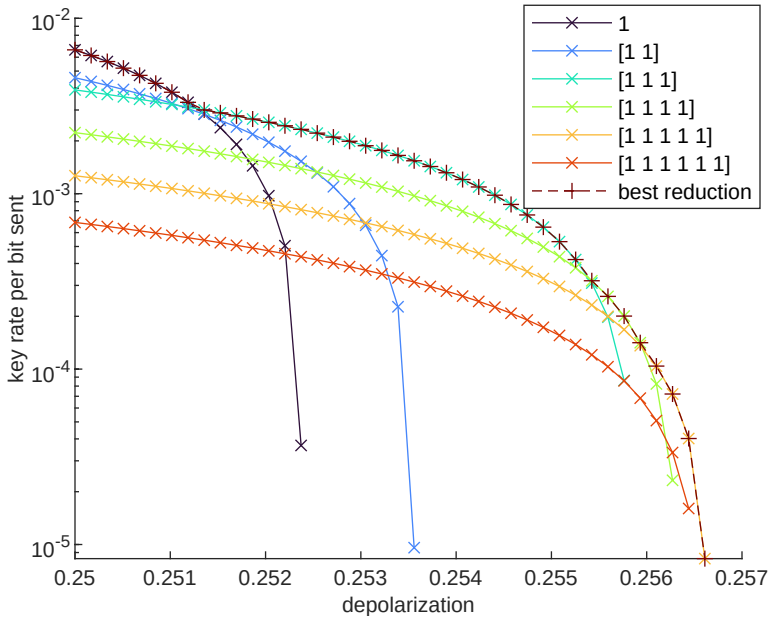


Figure 3.4: Comparison of reduction matrices for the six-state protocol up to a size of 7×7, with depolarization only. Shown near maximum tolerable depolarization. No reduction matrix up to 7×7 outperformed the original six-state protocol (1) below 25% depolarization.

In Figure 3.4, we see that the best reduction matrices, up to size 7×7, increased the maximum depolarization tolerance of the six-state protocol from $\sim 25.23\%$ to $\sim 25.67\%$. Although minimal, this demonstrates that reduction matrices remove some of the looseness in the security proof. Figure 3.4 also highlights two examples of the difficulties in predicting the best reduction matrices up to a certain size, namely:

1. The 2 to 1 reduction shows an improvement over the 1 to 1 reduction (no pre-privacy amplification) for slightly higher depolarization. However, the 2 to 1 curve lies entirely bellow the combination of the 3 to 1 and 1 to 1 curves. Slight increases in the size of the reduction matrix can significantly alter optimal choices.

2. The 6 to 1 reduction matrix gives a strictly lower key rate per bit sent compared to the 5 to 1 reduction matrix. So, although increase the size further limits Eve's

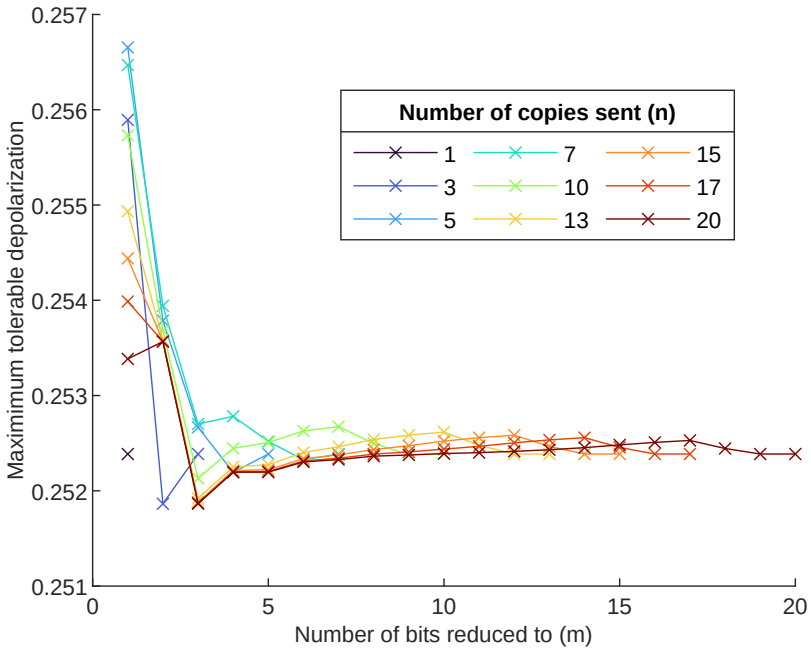


Figure 3.5: Maximum tolerable depolarization for the qubit six-state protocol with reduction matrices $F \in \mathbb{Z}_2^{m\times n}$ of the form $F = \begin{bmatrix} I_m & 1s \end{bmatrix}$, where $1s$ is the block of all ones. Solved with binary search down to a gap of 10^{-6} for the upper and lower bounds.

information, the extra cost to error correction can undo any gain in key rate.

Further numerical simulations where done on all reduction matrices of the form $\begin{bmatrix} I_m & 1s \end{bmatrix}$, (where $1s$ is a block of all ones) up to the size of 50 by 50.[14] From these, the maximum tolerable depolarization peaked at the 5 to 1 reduction. Although this does not represent all reduction matrices, the diminishing returns and the fact that no other reduction matrices up to 7 to 7 surpassed it, suggests the 5 to 1 reduction is close to the maximum tolerable error rate. A selection of the maximum tolerable depolarization for these reduction matrices can be found in Figure 3.5. Furthermore, for each number of copies sent, there is a second peak in the maximum depolarization tolerable beyond reducing to 2 key bits. This second peak also shifts with the number of copies sent. In addition, the key rate for all reduction matrices of the form $F = \begin{bmatrix} I_m & 1s \end{bmatrix}$, where $1s$ was determined from 0% to 26% depolarization for all sizes up to 30 by 30. Beyond the 5 to 1 reduction ma-

[14]This form has enough symmetry to heavily reduce the running time.

trix, very few reduction matrices provided any improvement to the key rate in any regime. For example, the 30 to 29 reduction matrix at 25.017% depolarization only improved the key rate compared by 1.96×10^{-9} bits per signal sent when compared to no pre-privacy amplification. It is likely that broader classes of reduction matrices could demonstrate a better advantage in these regions, however analysis beyond a size of 7×7 would require significantly more computational power. Currently, we recommend using the reduction the 1 to 1 (no reduction), 3 to 1, 4 to 1, and 5 to 1 reduction matrices in the regimes found in Figure 3.4. For more realistic scenarios that have either less symmetric data or are not tomographically complete, the computational burden will likely limit analysis to reduction matrices around 3×3.

Chapter 4

Simplified Trusted Relay for Pre-Privacy Amplification

Recall from Section 2.5.2 and Figure 2.3 that although the simplified trusted relay showed a significant advantage to no relay, it still lagged behind the full trusted relay. In this chapter we combine the simplified trusted relay with pre-privacy amplification to shrink this gap.

Before we get into the mathematical details, it is important to understand the order we wish to compose the simplified trusted relay with pre-privacy amplification. We can do one of two approaches:

1. Apply pre-privacy amplification *after* the STR.
2. Apply pre-privacy amplification *before* the STR.

The outcomes of these protocols are slightly different. To illustrate, suppose we want to combine pre-privacy amplification using a reduction matrix $\begin{bmatrix}1 & 1\end{bmatrix}$ and STR on the six-state protocol. In the first option, the relay sends bits a and b to Alice, and bits c and d to Bob. The relay then announces $a+c$ and $b+d$. The reduction matrix then sets the raw secret key to $a+b$. In the second option, the relay once again sends bits a and b to Alice and bits c and d to Bob. However, this time the reduction matrix is performed and the relay holds $a+b$ and $c+d$, the relay then announces $(a+b)+(c+d)$. This difference

in announcements is critical. In the first scenario, all parties (including Eve) can also construct the announcement in the second scenario, but the reverse is not true. Because more information is leaked to Eve in the first scenario, we choose to focus our analysis on the second scenario. Therefore, for the the rest of this thesis, we focus on applying pre-privacy amplification to our protocols *before* applying the STR.

4.1 General Protocol for a Simplified Trusted Relay with Pre-Privacy Amplification

Much of the mathematical description here is unchanged from Section 2.5.2. Most changes can be summarized as, take any register and make n copies of it. We apply this to

- The POVMs, their quantum to classical channels in Equation (2.92), and their compressed versions in Equations (2.93) and (2.94).
- The initial state prepared by the relay for source replacement in Equation (2.95).
- The constraint set Γ in Equation (2.96).

In the source replacement scheme, the relay now prepares the state,

$$|\rho\rangle_{TT'} = \left(\sum_{\vec{l}} \sqrt{p_{\vec{l}}} \left|\vec{l}\right\rangle_{T_A} \otimes |\psi_{\vec{l}}\rangle_{T'_A}\right) \otimes \left(\sum_{\vec{l'}} \sqrt{p_{\vec{l'}}} \left|\vec{l'}\right\rangle_{T_B} \otimes \left|\psi_{\vec{l'}}\right\rangle_{T'_B}\right). \tag{4.1}$$

After transmission, Alice, Bob and the relay hold the joint state ρ_{TAB} and Eve holds the purification $|\rho\rangle_{TABE}$. From their measurements, Alice, Bob and the relay constrain their shared state ρ_{TAB} to one from the set

$$\begin{aligned}\Gamma = \Big\{\rho_{TAB} \in \mathrm{D}(TAB) \Big| \; & \mathrm{Tr}_{AB}[\rho_{TAB}] = \mathrm{Tr}_{T'}[\rho_{TT'}],\ p(\vec{x}, \vec{x'}, \vec{y}, \vec{y'}, \vec{\alpha}, \vec{\alpha'}, \vec{\beta}, \vec{\beta'}) \\ & = \mathrm{Tr}\Big[\Big(M_{T_A,\vec{x},\vec{\alpha}} \otimes M_{T_B,\vec{x'},\vec{\alpha'}} \otimes M_{A,\vec{y},\vec{\beta}} \otimes M_{B,\vec{y'},\vec{\beta'}}\Big)\rho_{TAB}\Big], \\ & \qquad \forall(\vec{x}, \vec{x'}, \vec{y}, \vec{y'}, \vec{\alpha}, \vec{\alpha'}, \vec{\beta}, \vec{\beta'}) \in (\mathcal{X}, \mathcal{X}, \mathcal{Y}, \mathcal{Y}, \mathcal{A}, \mathcal{A}, \mathcal{B}, \mathcal{B})^n\Big\}.\end{aligned} \tag{4.2}$$

The largest change to the protocol comes from incorporating the pre-privacy amplification key map into the simplified trusted relay's key map. On each side of the relay the pre-privacy amplification map takes the n copies and reduces them to m copies for the key. Each link then uses the key map $\mathcal{E}_{\text{PPA},} \otimes \mathcal{E}^{\otimes n}$, like in Equation (3.22). Combining both links gives the initial key map

$$\begin{aligned}\mathcal{E}_{\text{PPA},R\to R'} \circ \mathcal{E}^{\otimes n}_{XC_{TAB}\to RC_{TAB}} := &\left(\mathcal{E}_{\text{PPA},R_A\to R'_A} \circ \mathcal{E}^{\otimes n}_{X_AC_{T_AA}\to R_AC_{T_AA}}\right) \\ &\otimes \left(\mathcal{E}_{\text{PPA},R_B\to R'_B} \circ \mathcal{E}^{\otimes n}_{X_BC_{T_BB}\to R_BC_{T_BB}}\right).\end{aligned} \tag{4.3}$$

The simplified trusted relay then sets the raw key and generates the parity announcement using its map

$$\mathcal{E}_{\text{STR},R'\to R'_AC_R}(\rho_{R'}) = \sum_{\vec{r},\vec{r'}\in\mathbb{Z}_2^m} \left|\vec{r},\ \vec{r}+\vec{r'}\right\rangle\!\left\langle\vec{r},\ \vec{r}+\vec{r'}\right|_{R'_AC_R} \text{tr}\left[\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle\vec{r},\ \vec{r'}\right|_{R'} \rho_{R'}\right]. \tag{4.4}$$

For a basic simplified trusted relay, the post-selection set from the announcements is extended to

$$\mathcal{S}_{\text{STR}} = \mathcal{S}^n \times \mathcal{S}^n \times \mathcal{R}^m. \tag{4.5}$$

In other words, the parity announcement from $\mathcal{R}^m$ is always accepted, and only the original accepted announcements $\mathcal{S}$ affect the our new acceptance set $\mathcal{S}_{\text{STR}}$. Error correction suffers from the same problems as in the original simplified trusted relay. Once again, we work under the assumption that Alice holds the worst error correction cost, and the information required to correct her copy is also sufficient for Bob to correct his copy. Furthermore, if this fails, then just like the original simplified trusted relay, the protocol aborts and the security remains uncompromised. Therefore, for each announcement the error correction cost is given by

$$\delta^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})}_{\text{leak}} = f\,\text{H}\left(R'_A\middle|Y_A,\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'}\right), \tag{4.6}$$

where f is the error correction efficiency. We can then combine all of these so the key rate per *block* is bounded by

$$R_{\text{blk}} \geq \sum_{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})\in\mathcal{S}_{\text{STR}}} p(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'}) \times \left[\min_{\rho_{TAB}\in\Gamma}\left(\sum_{\vec{r}\in\mathcal{R}^m} \text{H}\left(p(\vec{r}|\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})\rho_E^{(\vec{r},\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})}\right) - \text{H}\left(\rho_E^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})}\right)\right) - \delta_{\text{leak}}^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'},\vec{r'})}\right]. \tag{4.7}$$

Because every parity announcement in classical register C_R is accepted, it is often more convenient to work out the key rate without explicitly conditioning on $\vec{r'}$. We can push it back into the key rate formula by changing our operations to operations on ρ_{EC_R} and $\rho_{R'_A Y_A C_R}$ for the privacy amplification and error correction terms respectively. As such, the key rate formula is equivalently given as

$$R \geq \sum_{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})\in\mathcal{S}^n\times\mathcal{S}^n} p(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'}) \times \left[\min_{\rho_{TAB}\in\Gamma}\left(\sum_{\vec{r}\in\mathcal{R}^m} \text{H}\left(p(\vec{r}|\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})\rho_{EC_R}^{(\vec{r},\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})}\right) - \text{H}\left(\rho_{EC_R}^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})}\right)\right) - \delta_{\text{leak}}^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})}\right], \tag{4.8}$$

with error correction cost

$$\delta_{\text{leak}}^{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})} = f\,\text{H}\left(R'_A\middle|Y_A, C_R, \vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'}\right). \tag{4.9}$$

4.1.1 Equivalence of Reduction Matrices for the Simplified Trusted Relay

Many properties for equivalence of reduction matrices also hold for the simplified trusted relay. Here we give them. Because many of the proofs are not too difficult to lift from their pre-privacy amplification protocol counter parts, we give the proof to the first one

here and the others in Appendix C.1.

Theorem 4.1.1. *Let $n \geq m$, $\mathcal{R}$ a finite field, a reduction matrix $F \in \mathcal{R}^{m\times n}$, and $U \in \mathrm{GL}_m(\mathcal{R})$. Then for reduction matrix $F' = UF$, $R_{blk}(F') = R_{blk}(F)$ for any simplified trusted relay of a pre-privacy amplification based protocol.*

Proof. Let F, U, and F' be defined as above. Alice, Bob, the relay, and Eve share a pure state $|\rho\rangle_{TABE}$. After applying the measurements and original individual key maps to each copy, they share the density matrix $\rho_{RYEC_{TAB}}$. Therefore, the state after the key map is given by[1]

$$\begin{aligned}\rho_{R'_A C_R Y C E} &= \mathcal{E}_{\mathrm{STR},R'\to R'_A C_R} \circ \mathcal{E}_{\mathrm{PPA},F,R\to R'}\left(\rho_{RYC_{TAB}E}\right) \\ &= \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \left|F\vec{r},\ F(\vec{r}+\vec{r'})\right\rangle\!\left\langle F\vec{r},\ F(\vec{r}+\vec{r'})\right|_{R'_A C_R} \\ &\qquad \otimes \mathrm{Tr}_R[(\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle \vec{r},\ \vec{r'}\right| \otimes I_{YEC_{TAB}})\rho_{RYEC_{TAB}}].\end{aligned} \tag{4.10}$$

Similarly, for the reduction matrix F' we get

$$\begin{aligned}\rho'_{R'_A C_R Y C E} &= \mathcal{E}_{\mathrm{STR},R'\to R'_A C_R} \circ \mathcal{E}_{\mathrm{PPA},F',R\to R'}\left(\rho_{RYC_{TAB}E}\right) \\ &= \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \left|UF\vec{r},\ UF(\vec{r}+\vec{r'})\right\rangle\!\left\langle UF\vec{r},\ UF(\vec{r}+\vec{r'})\right|_{R'_A C_R} \\ &\qquad \otimes \mathrm{Tr}_R[(\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle \vec{r},\ \vec{r'}\right| \otimes I_{YEC_{TAB}})\rho_{RYEC_{TAB}}].\end{aligned} \tag{4.11}$$

Just like in the proof of 3.4.1, this is just a permutation of labels on the key register R'_A and the announcements in C_R. Therefore, $R_{\mathrm{blk}}(F') = R_{\mathrm{blk}}(F)$. □

Equivalence of column permutations from Theorem 3.4.2 are generalized for simplified trusted relay as follows.

Theorem 4.1.2. *Let $n \geq m$, $\mathcal{R}$ a finite field, a reduction matrix $F \in \mathcal{R}^{m\times n}$, and $\pi \in \mathrm{S}_n$. If ρ_{TAB} is permutation invariant, then for the reduction matrix $F' = FP_\pi$, $R_{blk}(F) = R_{blk}(F')$.*

[1] This form combines the simplified trusted relay and pre-privacy amplification map into a single step and is used repeatedly for proofs in this section.

Combining Theorems 4.1.1 and 4.1.2, we naturally can restrict our analysis to reduction matrices of the form $F = \begin{bmatrix} I_m & F' \end{bmatrix}$. With this, Lemma D.0.1 and the bijection $\mathcal{G}$ from Definition 3.4.3 are also applicable to simplified trusted relays of pre-privacy amplification based protocols.

Theorem 4.1.3. *Let $F_1 \in \mathcal{R}^{m_1 \times n_1}$ and $F_2 \in \mathcal{R}^{m_2 \times n_2}$ be reduction matrices on key registers with finite field $\mathcal{R}$. Let $n = n_1 + n_2$ and $m = m_1 + m_2$. If Alice, Bob and the relay's shared state has the separable form $\rho_{TAB} = \rho_{T_1^{n_1} A_1^{n_1} B_1^{n_1}} \otimes \rho_{T_{n_1+1}^{n} A_{n_1+1}^{n} B_{n_1+1}^{n}}$, then the simplified trusted relay with reduction matrix*

$$F = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}, \tag{4.12}$$

has a key rate per block *of $R_{blk}(F) = R_{blk}(F_1) + R_{blk}(F_2)$.*

Theorem 4.1.4. *For the finite field $\mathcal{R}$ and reduction matrix $F \in \mathcal{R}^{m \times n}$, the reduction matrix $\tilde{F} = \begin{bmatrix} F & 0 \end{bmatrix} \in \mathcal{R}^{m \times n'}$. If Alice, Bob and the relay's state has the separable form $\rho_{TAB} = \rho_{T_1^n A_1^n B_1^n} \otimes \rho_{T_{n+1}^{n'} A_{n+1}^{n'} B_{n+1}^{n'}}$, then the simplified trusted relay has a key rate per* block *of $R_{blk}(\tilde{F}) = R_{blk}(F)$.*

With Theorems 4.1.1, 4.1.2, 4.1.3, and 4.1.4, all the techniques used to reduce the number of reduction matrices that needed to be checked for pre-privacy amplification protocols also apply for simplified trusted relays of pre-privacy amplification based protocols. This drastically simplifies the problem of finding optimal reduction matrices.

4.2 Simplified Trusted Relay with Pre-Privacy Amplification for Six-State

Once again, the computational demand for solving a general pre-privacy amplification based protocol is too high. Like in Section 3.1.4, minimizing the relative entropy requires convex optimization and diagonalization of a density matrix that exponentially increases in size.[2] Thankfully, the six-state protocol provides enough symmetry to solve analytically. Here each link implements the six-state protocol with pre-privacy amplification, from n

[2] Now at a rate of $16^n \times 16^n$.

to m bits. Until we apply the simplified trusted relay map, each link will look identical to the set up back in Section 3.2. Each link is depolarized by ξ, and is tomographically complete (and so is the complete setup). Therefore, Alice, Bob and the relay share the state $\rho_{\text{single}T_AA}^{\otimes n} \otimes \rho_{\text{single}T_BB}^{\otimes n}$, and Eve holds the purification $|\rho\rangle_{T_{AB}ABE} = |\rho_{\text{single}}\rangle_{T_AAE_A}^{\otimes n} \otimes |\rho_{\text{single}}\rangle_{T_BBE_B}^{\otimes n}$. Here E_A and E_B are Eve's systems split based on which link they are associated with. Each party then performs their measurements and the relay applies the original (pre-reduction) key mapping to each link. Like with Theorem 2.4.2, the symmetry of this protocol under depolarization allows us to ignore the basis announcements and focus on the case where all key measurements are done in the Z-basis. After pre-privacy amplification is applied, each link has a copy of the $\rho_{R'YE}$ (Though it was not explicitly calculated, and the marginals $\rho_{R'E}$ and $\rho_{R'Y}$ were used). The relay, Alice, Bob, and Eve then share the state

$$\rho_{R'YE} = \rho_{R'_AY_AE_A} \otimes \rho_{R'_BY_BE_B}. \tag{4.13}$$

Finally, the simplified trusted relay sets R'_A as the raw key and announces the parity of the two link's keys added together.

$$\begin{aligned}\rho_{R'_AC_RYE} &= \mathcal{E}_{\text{STR},R'\to R'_AC_R}(\rho_{R'YE}) \\ &= \sum_{\vec{r},\vec{r'}\in\mathbb{Z}_2^m} \left|\vec{r},\ \vec{r}+\vec{r'}\right\rangle\!\left\langle\vec{r},\ \vec{r}+\vec{r'}\right|_{R'_AC_R} \\ &\quad \otimes \text{Tr}_{R'}[(\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle\vec{r},\ \vec{r'}\right|_{R'} \otimes I_{YE})\rho_{R'_AY_AE_A} \otimes \rho_{R'_BY_BE_B}].\end{aligned} \tag{4.14}$$

To get the key rate from Equation (4.8), we need the error correction cost and Holevo quantity. We follow a similar procedure to the one used in Section 3.2. $\rho_{R'_AC_RY_A}$, $p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}$, and ρ_{C_RE}.

Error Correction Cost

For the error correction cost, we require the marginal for the key register, Alice, and the parity announcement. As such, we can compute $\rho_{R'_AY_AC_R}$ from $\rho_{R'_AY_A} \otimes \rho_{R'_BY_B}$, which is two copies of Equation (3.27). Applying the simplified trusted relay's map and tracing Bob's

measurement register yields

$$\begin{aligned}\rho_{R'_A C_R Y_A} &= \mathrm{Tr}_{Y_B}[\mathcal{E}_{\mathrm{STR},R'\to R'_A C_R}(\rho_{R'_A Y_A}\otimes \rho_{R'_B Y_B})] \\ &= \mathcal{E}_{\mathrm{STR},R'\to R'_A C_R}(\rho_{R'_A Y_A}\otimes 2^{-m} I_{R'_B}) \\ &= \rho_{R'_A Y_A}\otimes 2^{-m} I_{C_R},\end{aligned} \tag{4.15}$$

As one would expect, the parity announcement for Bob decouples from Alice's half of the link. Therefore, $\mathrm{H}(R'_A|Y_A C_R) = \mathrm{H}(R'_A|Y_A)$ with the same distribution $\rho_{R'_A Y_A}$ from the pre-privacy amplification protocol, and the error correction cost is the same from Theorem 3.2.1.

Holevo Quantity

For the Holevo quantity, we start by constructing $\rho_{R'_A C_R E}$, then get the marginals $p(\vec{\gamma})\rho^{(\vec{\gamma})}_{C_R E}$, and $\rho_{C_R E}$. From Equation (3.24), we know the form of $\rho_{R'_A E_A}$ and $\rho_{R'_B E_B}$, then apply the simplified trusted relay map to get

$$\begin{aligned}\rho_{R'_A C_R E} = &\sum_{\vec{\gamma},\vec{\gamma'}\in\mathbb{Z}_2^m}\sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \left|\vec{\gamma},\ \vec{\gamma'}\right\rangle\!\left\langle\vec{\gamma},\ \vec{\gamma'}\right|_{R'_A C_R}\otimes \left|\vec{l},\ \vec{l'}\right\rangle\!\left\langle\vec{l},\ \vec{l'}\right|_{E_1} \\ \otimes &\sum_{\vec{\beta},\vec{\beta'}\in\mathbb{Z}_2^{n-m}} \left(Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}\otimes Z^{V(\vec{\gamma}+\vec{\gamma'})+\tilde{V}\vec{\beta'}}\right)\left|\tau_{\vec{l}},\ \tau_{\vec{l'}}\right\rangle\!\left\langle\tau_{\vec{l}},\ \tau_{\vec{l'}}\right|_{E_2}\left(Z^{V(\vec{\gamma}+\vec{\gamma'})+\tilde{V}\vec{\beta}}\otimes Z^{V\vec{\gamma}+\tilde{V}\vec{\beta'}}\right).\end{aligned} \tag{4.16}$$

To make this easier to write out, let $\sigma_{\vec{l}} := \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}}\left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right| Z^{\tilde{V}\vec{\beta}}$, then

$$\begin{aligned}\rho_{R'_A C_R E} = &\sum_{\vec{\gamma},\vec{\gamma'}\in\mathbb{Z}_2^m}\sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \left|\vec{\gamma},\ \vec{\gamma'}\right\rangle\!\left\langle\vec{\gamma},\ \vec{\gamma'}\right|_{R'_A C_R}\otimes \left|\vec{l},\ \vec{l'}\right\rangle\!\left\langle\vec{l},\ \vec{l'}\right|_{E_1} \\ &\otimes\left(Z^{V\vec{\gamma}}\otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right)\left(\sigma_{\vec{l}}\otimes\sigma_{\vec{l'}}\right)\left(Z^{V\vec{\gamma}}\otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right).\end{aligned} \tag{4.17}$$

We can then project onto the key register in C_R to find Eve's unnormalized states

conditioned on the key.

$$p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})} = \sum_{\vec{\gamma'}\in\mathbb{Z}_2^m} \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \left|\vec{\gamma'}\right\rangle\!\left\langle\vec{\gamma'}\right|_{C_R} \otimes \left|\vec{l},\ \vec{l'}\right\rangle\!\left\langle\vec{l},\ \vec{l'}\right|_{E_1} \otimes \left(Z^{V\vec{\gamma}} \otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right)\left(\sigma_{\vec{l}} \otimes \sigma_{\vec{l'}}\right)\left(Z^{V\vec{\gamma}} \otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right). \tag{4.18}$$

Furthermore, we can also quickly get ρ_{C_RE} by adding them together,

$$\rho_{C_RE} = \sum_{\vec{\gamma},\vec{\gamma'}\in\mathbb{Z}_2^m} \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \left|\vec{\gamma'}\right\rangle\!\left\langle\vec{\gamma'}\right|_{C_R} \otimes \left|\vec{l},\ \vec{l'}\right\rangle\!\left\langle\vec{l},\ \vec{l'}\right|_{E_1} \otimes \left(Z^{V\vec{\gamma}} \otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right)\left(\sigma_{\vec{l}} \otimes \sigma_{\vec{l'}}\right)\left(Z^{V\vec{\gamma}} \otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right). \tag{4.19}$$

With these marginals, we now solve for the two entropy terms, $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)$ and $\mathrm{H}\left(\rho_{C_RE}\right)$ associated with the Holevo quantity. We start with the term, $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)$.

Lemma 4.2.1. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, acting on n copies of the shared state $\rho_{singleT_AA} \otimes \rho_{singleT_BB}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). Independent of the basis announcement,*

$$\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right) = 2\left(m + \sum_{\vec{l}\in\mathbb{Z}_2^n} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})} \left(\tfrac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})}\right)\right), \tag{4.20}$$

where $\tilde{V} \in \mathbb{Z}_2^{n\times n-m}$ such that $\mathrm{Im}(\tilde{V}) = \ker(F) \simeq \mathbb{Z}_2^{n-m}$, and $W_1 \in \mathbb{Z}_2^{n\times n-m}$ such that $\tilde{V}^T W_1 = I_{n-m}$.

A full proof can be found in Appendix C.2.1. In essence, we start by breaking down $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)$ using the block diagonal structure of Equation (4.18), then remove the global unitaries. Afterwards, we are essentially left with two copies of Equation 3.32. Furthermore, we already computed the eigenvalues of this operator and it just the first term in Theorem 3.3.5.

Now for the other term, $\mathrm{H}(\rho_{C_R E})$. This term is significantly more complex and is the main contributing factor to why simulating the simplified trusted relay is slower than a regular protocol with pre-privacy amplification.

Lemma 4.2.2. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, acting on n copies of the shared state $\rho_{singleT_A A} \otimes \rho_{singleT_B B}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). Independent of the basis announcement,*

$$\mathrm{H}(\rho_{C_R E}) = m + \sum_{\vec{l},\vec{l'},\vec{s}\in\mathbb{Z}_2^n} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})+\tilde{\mathrm{d}}(\vec{s}+F^T\vec{k},\vec{l'})} \left(\frac{\xi}{4}\right)^{2n-\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})-\tilde{\mathrm{d}}(\vec{s}+F^T\vec{k},\vec{l'})} \right), \tag{4.21}$$

where $\tilde{V} \in \mathbb{Z}_2^{n\times n-m}$ such that $\mathrm{Im}(\tilde{V}) = \ker(F) \simeq \mathbb{Z}_2^{n-m}$, and $W_1 \in \mathbb{Z}_2^{n\times n-m}$ such that $\tilde{V}^T W_1 = I_{n-m}$.

A full proof can be found in Appendix C.2.2. The proof starts in the same way as the proof for Lemma 4.2.1, but unlike with Lemma 4.2.1, there is no corresponding term from the six-state pre-privacy amplification protocol we can substitute in. Instead we have to determine the eigenvalues in the same way as we did in Section 3.3. With some effort we can rewrite the term inside the entropy in the form

$$\Phi_{\mathcal{W}}(\rho) := 2^{-(2n-m)} \sum_{\vec{\mathcal{B}}\in\mathbb{Z}_2^{2n-m}} Z^{\mathcal{W}\vec{\mathcal{B}}} \rho Z^{\mathcal{W}\vec{\mathcal{B}}}, \tag{4.22}$$

$$\mathcal{W} = \begin{bmatrix} V & \tilde{V} & 0 \\ V & 0 & \tilde{V} \end{bmatrix}, \tag{4.23}$$

$$\rho = |\tau_{\vec{\mathcal{L}}}\rangle\langle\tau_{\vec{\mathcal{L}}}|, \tag{4.24}$$

$$\vec{L} = \begin{bmatrix} \vec{l} \\ \vec{l'} \end{bmatrix}. \tag{4.25}$$

We then use Equation (3.56) and simplify.

Key rate

All together, the key rate for the simplified trusted relay with pre-privacy amplification on the six-state protocol is given by the following theorem.

Theorem 4.2.3. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, acting on n copies of the shared state $\rho_{singleT_AA} \otimes \rho_{singleT_BB}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). The key rate per* block *of the six-state simplified trusted relay with pre-privacy amplification protocol is lower bounded by*

$$
\begin{aligned}
R_{blk} \geq & \left(\sum_{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})\in\mathcal{S}^n\times\mathcal{S}^n} p(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'}) \right) \\
& \left[2\cdot\left(m + \sum_{\vec{l}\in\mathbb{Z}_2^n}\sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})} \left(\tfrac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})} \right) \right) \right. \\
& \quad - m - \sum_{\vec{l},\vec{l'},\vec{s}\in\mathbb{Z}_2^n}\sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})+\tilde{\mathrm{d}}(\vec{s}+F^T\vec{k},\vec{l'})} \right. \\
& \qquad \left. \left. \times \left(\tfrac{\xi}{4}\right)^{2n-\tilde{\mathrm{d}}(W_1\vec{\phi}+F^T\vec{k},\vec{l})-\tilde{\mathrm{d}}(\vec{s}+F^T\vec{k},\vec{l'})} \right) - \delta_{leak} \right],
\end{aligned}
\tag{4.26}
$$

where:

- *The post-selection set of basis announcements is $\mathcal{S} = \{(\vec{\alpha},\vec{\alpha})|\vec{\alpha}\in\mathcal{A}^n\}$.*
- $\delta_{leak} = f\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})}\right)$.
- *$f \in [1,\infty)$ is the efficiency of error correction.*
- *$V \in \mathbb{Z}_2^{n\times m}$ such that $FV = I_m$.*
- *$\tilde{V} \in \mathbb{Z}_2^{n\times n-m}$ such that $\mathrm{Im}(\tilde{V}) = \ker(F) \simeq \mathbb{Z}_2^{n-m}$.*
- *$W_1 \in \mathbb{Z}_2^{n\times n-m}$ such that $\tilde{V}^T W_1 = I_{n-m}$.*

Like with Theorems 3.4.1, and 3.4.2, we can employ Theorems 4.1.1 and 4.1.2 to further improve the performance of the key rate algorithm. Due to the significant size increase of the problem, the performance gains are critical. A detailed derivation of key rate formula (Theorem D.0.4) is found in Appendix D.

4.3 Results

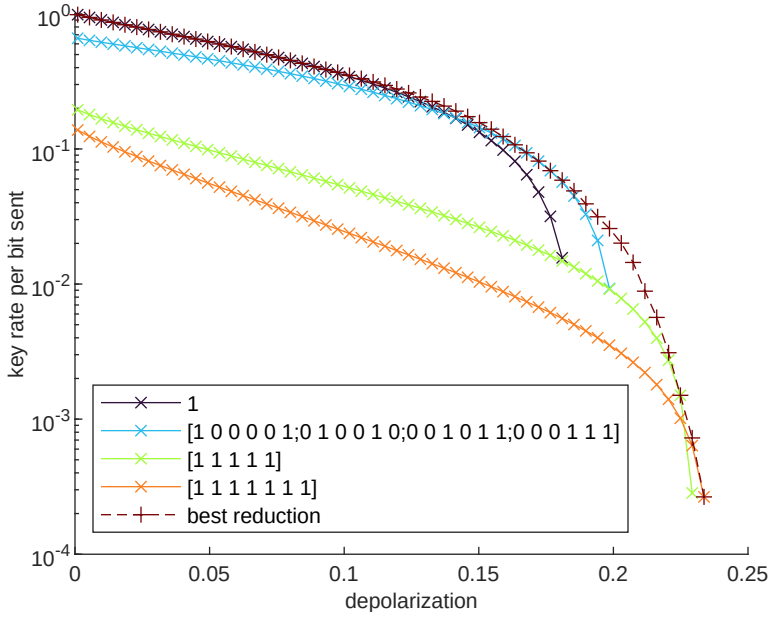


Figure 4.1: Comparison of reduction matrices for the six-state qubit simplified trusted relay protocol, with depolarization only. Best reduction taken from reduction matrices up to a size of 7×7. All reduction matrices shown are the best in some small regime within the size limit.

Due to the extra time requirements to compute the key rates for simplified trusted relays with pre-privacy amplification, only reduction matrices up to a size of 7×7 could be computed. Even then, it is clear that reduction matrices provide a major improvement to key rate and maximum tolerable depolarization. As seen in Figure 4.1, pre-privacy amplification allows the simplified trusted relay to jump from a maximum depolarization tolerance of $\sim 18.1\%$ to $\sim 23.4\%$. Unlike the full trusted relay with pre-privacy amplification, more complex reduction matrices are part of the the best reduction matrix line

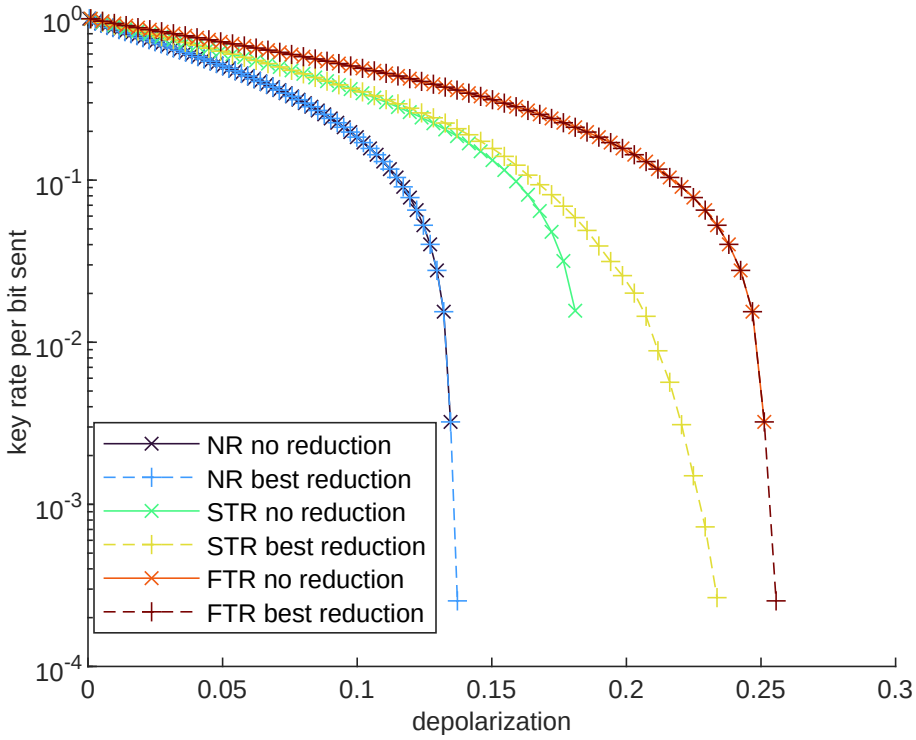


Figure 4.2: Comparison of reduction matrices for the six-state qubit protocol for no relay (NR), simplified trusted relay (STR), and the full trusted relay (FTR). Original simplified trusted relay without pre-privacy amplification is also given. Best reduction taken from reduction matrices up to a size of 7×7.

(within the size constraint of 7×7). From Figure 4.2, although the simplified trusted relay with pre-privacy amplification is still significantly outperformed by the full trusted relay, the gap between both lines is significantly tighter.

Naturally this leads to the question, "How close will the simplified trusted relay and the full trusted relay become for large (and well chosen) reduction matrices?". Although we do not have a definitive answer some numerical simulation seems to suggest that the

difference becomes negligible. Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix, we define the terms

$$T_1(F) = \sum_{\vec{l'},\vec{s}\in\mathbb{Z}_2^n} \mathrm{Q}\left(\left(1-\frac{3\xi}{4}\right)^{\varphi_1}\left(\frac{\xi}{4}\right)^{n-\varphi_1}\right), \tag{4.27}$$

$$T_2(F) = m + \sum_{\vec{l}\in\mathbb{Z}_2^n}\sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m}\left(1-\frac{3\xi}{4}\right)^{\varphi_2}\left(\frac{\xi}{4}\right)^{n-\varphi_2}\right), \tag{4.28}$$

$$T_3(F) = m + \sum_{\vec{l}_1,\vec{l'}_1,\vec{s}_1\in\mathbb{Z}_2^m}\sum_{\vec{l}_2,\vec{l'}_2,\vec{\phi},\vec{s}_2\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m}\left(1-\frac{3\xi}{4}\right)^{\varphi_3}\left(\frac{\xi}{4}\right)^{2n-\varphi_3}\right), \tag{4.29}$$

$$\varphi_1 = \tilde{\mathrm{d}}(\vec{s},\vec{l'}), \tag{4.30}$$

$$\varphi_2 = \tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k},\vec{l}), \tag{4.31}$$

$$\varphi_3 = \tilde{\mathrm{d}}(\vec{s} + F^{\mathrm{T}}\vec{k},\vec{l'}) + \tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k},\vec{l}). \tag{4.32}$$

With these terms, we can rewrite the lower bounds on the key rates for the full and simplified trusted relays as

- Simplified trusted relay:

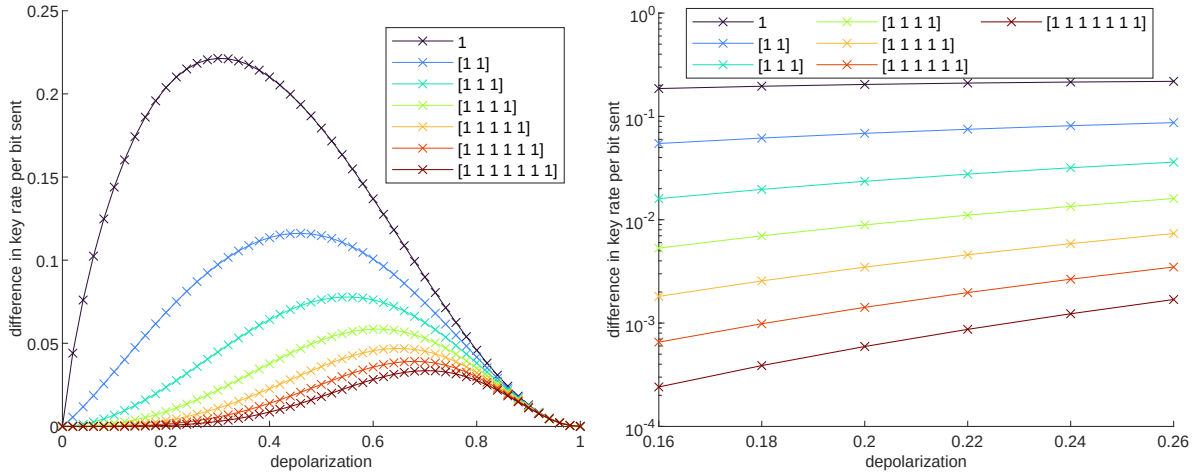
$$R_{\mathrm{blk}}(F) = 2T_2(F) - T_3(F) - \delta_{\mathrm{leak}}, \tag{4.33}$$

- Full trusted relay:

$$\begin{aligned} R_{\mathrm{blk}}(F) &= T_2(F) - T_1(F) - \delta_{\mathrm{leak}} \\ &= 2T_2(F) - (T_2(F) + T_1(F)) - \delta_{\mathrm{leak}}. \end{aligned} \tag{4.34}$$

We already know that δ_{leak} is the same for both the simplified and trusted relays. Therefore, the only factors that mater are $T_3(F)$ from the simplified trusted relay, and $T_1(F)+T_2(F)$ from the full trusted relay. Furthermore, the difference can be reduced by combining $T_1(F) + T_2(F)$ into the single equation

$$T_1(F) + T_2(F) = m + \sum_{\vec{l},\vec{l'},\vec{s}\in\mathbb{Z}_2^n}\sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m}\left(1-\frac{3\xi}{4}\right)^{\varphi_1+\varphi_2}\left(\frac{\xi}{4}\right)^{2n-\varphi_1-\varphi_2}\right). \tag{4.35}$$



(a) Full depolarization range.

(b) Depolarization ranging roughly around the full and simplified trusted relays' maximum tolerable depolarizations for the reductions.

Figure 4.3: Difference in key rate per *bit* sent between the six-state qubit protocol with pre-privacy amplification and the simplified trusted relay of it for a variety of reduction matrices. This is not comparing the difference between the best reduction matrices at each point.

This has nearly the exact same form as $T_3(F)$ with the only difference being the extra $+F^{\mathrm{T}}\vec{k}$ found in φ_3. Therefore, the difference in the key rate between the simplified and full trusted relay, $T_3(F) - T_1(F) - T_2(F)$, amounts to the effect that $+F^{\mathrm{T}}\vec{k}$ has on the entropy. In Figure 4.3 we see that as the fraction of bits reduced increases, the difference in key rates per *bit* shrinks. Naturally near depolarizations of 0 and 1, the values converge, but even in the regime around the maximum tolerable depolarizations, the difference is small. It is still important to note that these are comparing the gap in key rate when both the simplified and full trusted relays are using the same reduction matrix. However the best reductions for each use completely different sets of reduction matrices.

Chapter 5

Conclusion and Outlook

In conclusion, we constructed a post processing technique, that acts as a pre-privacay amplification step. We constructed a method to apply pre-privacy amplification to a wide variety of prepare and measure qudit protocols, and determined a variety of sufficient conditions for when distinct reduction matrices should give identical key rates. With computational complexity in mind, we determined the key rate for the asymptotic qubit six-state protocol and demonstrated a small gain in the maximum tolerable error rate. Furthermore, applying pre-privacy amplification to the simplified trusted relay showed massive gains to key rate and the maximum tolerable error rate.

Currently, work is underway to extend the results for a weak coherent pulse based six-state protocol with infinite decoy intensities. Due to the increased complexity, only very loose lower bounds have been established and the actual effectiveness of the technique must be separated from looseness of the bound.

A natural next step is to move away from tomographically complete protocols. Carefully optimized variations of the techniques found in [7, 23, 27] would allow for computations with small reduction matrices without a trivial constraint set. Tighter bounds could be established for scenarios such as BB84, finite decoy state intensities, and finite size effects. Though it should be noted that a more thorough analysis of error correction cost for the simplified trusted relay may be required.

References

[1] Stacey, William. "The Security of Simplified Trusted Relays". MA thesis. University of Waterloo, 2014.

[2] P.W. Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 35th Annual Symposium on Foundations of Computer Science. Santa Fe, NM, USA: IEEE Comput. Soc. Press, 1994, pp. 124–134. ISBN: 978-0-8186-6580-6. DOI: 10.1109/SFCS.1994.365700.

[3] Daniel J. Bernstein and Tanja Lange. "Post-Quantum Cryptography". In: *Nature* 549.7671 (Sept. 2017), pp. 188–194. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/nature23461.

[4] Charles H. Bennett and Gilles Brassard. "Quantum Cryptography: Public Key Distribution and Coin Tossing". In: *Theoretical Computer Science* 560 (Dec. 2014), pp. 7–11. ISSN: 03043975. DOI: 10.1016/j.tcs.2014.05.025.

[5] Dagmar Bruß. "Optimal Eavesdropping in Quantum Cryptography with Six States". In: *Physical Review Letters* 81.14 (Oct. 5, 1998), pp. 3018–3021. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.81.3018.

[6] Renato Renner. "Security of Quantum Key Distribution". SWISS FEDERAL INSTITUTE OF TECHNOLOGY, Jan. 11, 2006. arXiv: quant-ph/0512258.

[7] Wenyuan Wang and Norbert Lütkenhaus. *Numerical Security Proof for Decoy-State BB84 and Measurement-Device-Independent QKD Resistant against Large Basis Misalignment*. Aug. 25, 2021. arXiv: arXiv:2108.10844. URL: http://arxiv.org/abs/2108.10844 (visited on 12/01/2022). preprint.

[8] O. Gittsovich et al. “Squashing Model for Detectors and Applications to Quantum-Key-Distribution Protocols”. In: *Physical Review A* 89.1 (Jan. 23, 2014), p. 012325. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.89.012325.

[9] Nicolas Gisin et al. “Quantum Cryptography”. In: *Reviews of Modern Physics* 74.1 (Mar. 8, 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145.

[10] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. “Progress in Satellite Quantum Key Distribution”. In: *npj Quantum Information* 3.1 (Dec. 2017), p. 30. ISSN: 2056-6387. DOI: 10.1038/s41534-017-0031-5.

[11] Sheng-Kai Liao et al. “Satellite-to-Ground Quantum Key Distribution”. In: *Nature* 549.7670 (Sept. 7, 2017), pp. 43–47. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/nature23655.

[12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. 10th anniversary ed. Cambridge ; New York: Cambridge University Press, 2010. 676 pp. ISBN: 978-1-107-00217-3.

[13] A. J. Menezes, Paul C. Van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press Series on Discrete Mathematics and Its Applications. Boca Raton: CRC Press, 1997. 780 pp. ISBN: 978-0-8493-8523-0.

[14] Yue Chuan Tan et al. “Radiation Tolerance of Opto-Electronic Components Proposed for Space-Based Quantum Key Distribution”. In: *Journal of Modern Optics* 62.20 (Nov. 28, 2015), pp. 1709–1712. ISSN: 0950-0340, 1362-3044. DOI: 10.1080/09500340.2015.1046519.

[15] William Stacey et al. “Security of Quantum Key Distribution Using a Simplified Trusted Relay”. In: *Physical Review A* 91.1 (Jan. 28, 2015), p. 012338. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.91.012338.

[16] Stefano Guerrini, Marco Chiani, and Andrea Conti. “Secure Key Throughput of Intermittent Trusted-Relay QKD Protocols”. In: *2018 IEEE Globecom Workshops (GC Wkshps)*. 2018 IEEE Globecom Workshops (GC Wkshps). Abu Dhabi, United Arab Emirates: IEEE, Dec. 2018, pp. 1–5. ISBN: 978-1-5386-4920-6. DOI: 10.1109/GLOCOMW.2018.8644402.

[17] Chi-Hang Fred Fung et al. "Quantum Key Distribution with Delayed Privacy Amplification and Its Application to the Security Proof of a Two-Way Deterministic Protocol". In: *Physical Review A* 85.3 (Mar. 9, 2012), p. 032308. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.85.032308.

[18] Seymour Lipschutz and Marc Lipson. *Schaum's Outlines: Linear Algebra*. 4th ed. New York: McGraw Hill Professional, 2011. ISBN: 978-0-07-154353-8.

[19] John Watrous. *The Theory of Quantum Information*. 1st ed. Cambridge University Press, Apr. 26, 2018. ISBN: 978-1-316-84814-2 978-1-107-18056-7. DOI: 10.1017/9781316848142.

[20] Mark Wilde. *Quantum Information Theory*. Second edition. Cambridge, UK ; New York: Cambridge University Press, 2017. 757 pp. ISBN: 978-1-107-17616-4.

[21] Gilad Gour and Andreas Winter. "How to Quantify a Dynamical Quantum Resource". In: *Physical Review Letters* 123.15 (Oct. 8, 2019), p. 150401. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.123.150401.

[22] Isabelle Jianing Geng, Kimberly Golubeva, and Gilad Gour. "What Are the Minimal Conditions Required to Define a Symmetric Informationally Complete Generalized Measurement?" In: *Physical Review Letters* 126.10 (Mar. 8, 2021), p. 100401. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.126.100401.

[23] Ian George, Jie Lin, and Norbert Lütkenhaus. "Numerical Calculations of the Finite Key Rate for General Quantum Key Distribution Protocols". In: *Physical Review Research* 3.1 (Mar. 24, 2021), p. 013274. ISSN: 2643-1564. DOI: 10.1103/PhysRevResearch.3.013274.

[24] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus. "Numerical Approach for Unstructured Quantum Key Distribution". In: *Nature Communications* 7.1 (Sept. 2016), p. 11712. ISSN: 2041-1723. DOI: 10.1038/ncomms11712.

[25] Charles H. Bennett, Gilles Brassard, and N. David Mermin. "Quantum Cryptography without Bell's Theorem". In: *Physical Review Letters* 68.5 (Feb. 3, 1992), pp. 557–559. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.68.557.

[26] Igor Devetak and Andreas Winter. "Distillation of Secret Key and Entanglement from Quantum States". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2053 (Jan. 8, 2005), pp. 207–235. ISSN: 1364-5021, 1471-2946. DOI: 10.1098/rspa.2004.1372.

[27] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. "Reliable Numerical Key Rates for Quantum Key Distribution". In: *Quantum* 2 (July 26, 2018), p. 77. ISSN: 2521-327X. DOI: 10.22331/q-2018-07-26-77. arXiv: 1710.05511 [quant-ph].

[28] Agnes Ferenczi and Norbert Lütkenhaus. "Symmetries in Quantum Key Distribution and the Connection between Optimal Attacks and Optimal Cloning". In: *Physical Review A* 85.5 (May 16, 2012), p. 052310. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.85.052310. arXiv: 1112.3396 [quant-ph].

[29] M Peev et al. "The SECOQC Quantum Key Distribution Network in Vienna". In: *New Journal of Physics* 11.7 (July 2, 2009), p. 075001. ISSN: 1367-2630. DOI: 10.1088/1367-2630/11/7/075001.

[30] M. Sasaki et al. "Field Test of Quantum Key Distribution in the Tokyo QKD Network". In: *Optics Express* 19.11 (May 23, 2011), p. 10387. ISSN: 1094-4087. DOI: 10.1364/OE.19.010387.

[31] Matthias Christandl, Robert König, and Renato Renner. "Postselection Technique for Quantum Channels with Applications to Quantum Cryptography". In: *Physical Review Letters* 102.2 (Jan. 14, 2009), p. 020504. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.102.020504.

[32] V. N. Zemlyachenko, N. M. Korneenko, and R. I. Tyshkevich. "Graph Isomorphism Problem". In: *Journal of Soviet Mathematics* 29.4 (May 1985), pp. 1426–1481. ISSN: 0090-4104, 1573-8795. DOI: 10.1007/BF02104746.

[33] László Babai. *Graph Isomorphism in Quasipolynomial Time*. Jan. 19, 2016. arXiv: arXiv:1512.03547. URL: http://arxiv.org/abs/1512.03547 (visited on 12/06/2022). preprint.

[34] W. Keith Nicholson. *Introduction to Abstract Algebra*. 4th ed. Hoboken: Wiley, 2012. 535 pp. ISBN: 978-1-118-13535-8.

Appendices

Appendix A

Fields, Vector Spaces, and Groups

A.1 Fields and Vector Spaces

For those who need a quick reminder, we provide the definitions for fields, vector spaces and subspaces.

Definition A.1.1 (Field)**.** A *field* $\mathcal{R}$, is a set R with operations $+ : R \times R \to R$, and $\cdot : R \times R \to R$ that obey the following properties. For all $a, b, c \in R$

Commutative $a + b = b + a$ and $a \cdot b = b \cdot a$.

Associative $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

Distributive $a \cdot (b + c) = a \cdot b + a \cdot c$.

Additive Identity There exists an element $0 \in R$ such that for all $d \in R$, $d + 0 = d$.

Multiplicitve Identity There exists and element $1 \in R$ such that for all $d \in R$, $d \cdot 1 = d$.

Addative Inverse There exists an element $-a \in R$ such that $a + -a = 0$.

Multiplicative Inverse If $a \neq 0$, then there exists an element $a^{-1} \in R$ such that $a \cdot a^{-1} = 1$.

Definition A.1.2 (Vector Space)**.** A *vector space* V over the field $\mathcal{R}$ is a set (also denoted as V) and the operations $+ : V \times V \to V$ and $\cdot : \mathcal{R} \times V \to V$ that obey the following properties. For all $a, b, c \in V$ and $r, s \in \mathcal{R}$

Commutative $a + b = b + a$.

Associative $(a + b) + C = a + (b + c)$.

Addative Identity There exists a vector $0 \in V$ such that for all $d \in V$, $d + 0 = d$.

Addative Inverse There exists an element $-a \in V$ such that $a + -a = 0$.

Distributive $r \cdot (a + b) = r \cdot a + r \cdot b$ and $(r + s) \cdot a = r \cdot a + s \cdot a$.

Multiplicative Identity for $1 \in \mathcal{R}$, $1 \cdot a = a$.

Compatibible Scalar Multiplication $(rs) \cdot a = r \cdot (s \cdot a)$.

With this, comes the usual properties one expects for a vector space.

Theorem A.1.3. *Let V be a vector space over the field $\mathcal{R}$. For all $a, b, c \in V$ and $r \in \mathcal{R}$*

- *If $a + b = b + c$, then $a = c$.*
- *$0, -a \in V$ are unique.*
- *$r \cdot 0 = 0$ ($0 \in V$).*
- *$0 \cdot a = 0$ (left $0 \in \mathcal{R}$, right $0 \in V$).*
- *If $r \cdot a = 0$, then $r = 0$ and/or $a = 0$.*
- *$(-r) \cdot a = r \cdot (-a)$.*

Definition A.1.4 (Subspace)**.** Let V be a vector space over a field $\mathcal{R}$. A subset U of V is called a *subspace* (and denoted somewhat ambiguously as $U \subset V$) if it obeys the following. For all $a, b \in V$ and $r \in \mathcal{R}$

1. $0 \in U$.
2. $a + b \in U$.
3. $r \cdot a \in U$.

A.2 Groups and Group Actions

The reader does not need to know much about groups and group actions, but it does help in Chapters 3 and 4. Definitions for groups, group actions, and various groups along with their properties comes from [34].

Definition A.2.1. A *Group* $\mathcal{G}$ consists of a set G and an operation $\cdot : G \times G \to G$ that obeys the following. For all $a, b, c \in G$

Associative $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Identity There exists an element $e \in G$ such that for all $d \in G$, $e \cdot d = d \cdot e = d$.

Inverse There exists an element a^{-1} such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Typically, the group $\mathcal{G}$ and the set G are used interchangeably.

We are primarily concerned with two groups in this thesis.

Definition A.2.2 (Symmetric Group)**.** let $A = \{1, \ldots, n\}$ and S_n the set of all bijective functions $\pi : A \to A$. Under function composition, S_n is the group of permutations called the *symmetric group*.

Definition A.2.3 (General Linear Group)**.** Let V be vector spaces over the field $\mathcal{R}$. The *general linear group* $\mathrm{GL}(V)$ is the set of all invertable operators from $\mathrm{L}(\mathcal{R}^n)$ under composition.

For the vector space $\mathcal{R}^n$ we denote the general linear group as $\mathrm{GL}_n(\mathcal{R})$. Furthermore, for any vector space V over the field $\mathcal{R}$ with $\dim(V) = n$, $\mathrm{GL}(V) \equiv \mathrm{GL}_n(\mathcal{R})$.

Definition A.2.4 (Group Action)**.** Let G be a group, A a non-empty set, and $\star : G \times A \to A$. $\star$ is called a *group action* (or just action) if it obeys the following properties. For all $g_1, g_2 \in G$ and $a \in A$

1. $1 \star a = a$.
2. $(g_1 g_2) \star a = g_1 \star (g_2 \star a)$.

For example, matrix multiplication is a group action between $\mathrm{GL}_n \mathcal{R}$ and $\mathcal{R}^{n \times m}$. Importantly, this represents all row operations on $\mathcal{R}^{n \times m}$.

A.2.1 Useful Permutation Definitions and Theorems

By far the most important group action we use in this thesis is permuting tensor products and the entries of column vectors with S_n. Here we give some notation and a few useful definitions and theorems.

Definition A.2.5. Let $\mathcal{R}$ be a finite field and $\pi \in \mathrm{S}_n$. We define the permutation matrix $P_\pi \in \mathcal{R}^{n\times n}$ as

$$P_\pi = \sum_{i=1}^{n} \vec{e}_{\pi(i)} \vec{e}_i^{\mathrm{T}}, \tag{A.1}$$

and for $\vec{l} \in \mathcal{R}^n$, the mapping π, $\vec{l} \mapsto P_\pi \vec{l}$ is a group action.

For an arbitrary $\vec{l} \in \mathcal{R}^n$ we get[1]

$$P_\pi \vec{l} = \sum_{i=1}^{n} l_i \vec{e}_{\pi(i)} = \sum_{i=1}^{n} l_{\pi^{-1}(i)} \vec{e}_i. \tag{A.2}$$

Combining with Definition 2.2.14 gives a simple way to denote permutations of tensor products. So, for $A = A_1^n$, and $\pi \in \mathrm{S}_n$,U_{A,P_π} permutes the n subsystems of A according to π. With this we can define the permutation invariant states.

Definition A.2.6 (Permutation Invariant States)**.** Let $A = A_1^n$ be a Hilbert space and $\rho_A \in \mathrm{D}(A)$. We say the state ρ_A is *permutation invariant* (for the decomposition A_1^n) if for all $\pi \in \mathrm{S}_n$, $U_{A,\pi}\rho_A U_{A,\pi}^\dagger = \rho_A$.

Here are a few theorems regarding permutations that see use in the proofs of Theorems 3.4.2 and 3.4.2.

The first one lets us shift permutations on permutationally invariant states to a purifying system.

Theorem A.2.7. *Let $\pi \in \mathrm{S}_n$, and let $\rho \in \mathrm{Herm}(A_1^n)$ be a permutation invariant state, then any purification of ρ_A in the form $\sqrt{\rho_A} \otimes V |\phi^+\rangle$ for isometry $V \in \mathrm{L}(\tilde{A}, B)$ obeys*

$$U_{A,P_\pi} \sqrt{\rho_A} \otimes V \left|\phi^+\right\rangle_{A\tilde{A}} = \sqrt{\rho_A} \otimes V U_{\tilde{A},P_\pi}^T \left|\phi^+\right\rangle_{A\tilde{A}}. \tag{A.3}$$

[1]With some finagling, one could use this to write out permutations for any $\mathbb{Z}_m^n$, and not just finite fields.

Furthermore, there exists a unitary $U_B \in \mathrm{U}(B)$ such that

$$U_{A,P_\pi}\sqrt{\rho_A} \otimes V \left|\phi^+\right\rangle_{A\tilde{A}} = \sqrt{\rho_A} \otimes U_B V \left|\phi^+\right\rangle_{A\tilde{A}}. \tag{A.4}$$

In other words, permuting Alice's system by π is just another purification of ρ_A with system B.

Proof. Let π and ρ_A be defined as above, then

$$\begin{aligned} U_{A,P_\pi}\sqrt{\rho_A} \otimes V_{\tilde{A}} \left|\phi^+\right\rangle_{A\tilde{A}} &= U_{A,P_\pi}\sqrt{\rho_A} \otimes V U^{\mathrm{T}}_{\tilde{A},P_\pi} U_{\tilde{A},P_\pi} \left|\phi^+\right\rangle_{A\tilde{A}} \\ &= U_{A,P_\pi}\sqrt{\rho_A} U^{\mathrm{T}}_{A,P_\pi} \otimes V U^{\mathrm{T}}_{\tilde{A},P_\pi} U_{\tilde{A},P_\pi} \left|\phi^+\right\rangle_{A\tilde{A}} \\ &= \sqrt{\rho_A} \otimes V U^{\mathrm{T}}_{\tilde{A},P_\pi} \left|\phi^+\right\rangle_{A\tilde{A}}. \end{aligned} \tag{A.5}$$

Now $VU_{\tilde{A},P_\pi}$ is an isometry from $\tilde{A}$ to B, therefore there exists a unitary transformation from isometry V to VU_{P_π}. □

This proof lets us commute permutations with I.I.D. channels.

Theorem A.2.8. *Let $\mathcal{E}_{A_1\to B_1} \in \mathrm{T}(A_1, B_1)$, and $\pi \in \mathrm{S}_n$. Then for all $\rho_A \in \mathrm{L}(A_1^n)$,*

$$U_{B,P_\pi}(\mathcal{E}^{\otimes n}_{A\to B}(\rho_A))U^\dagger_{B,P_\pi} = \mathcal{E}^{\otimes n}_{A\to B}(U_{A,P_\pi}\rho_A U^\dagger_{A,P_\pi}). \tag{A.6}$$

In other words, for n identical linear maps, permuting the inputs is equivalent to permuting the outputs.

Proof. We prove this for the case that $\dim(A)$ is a prime power so we can represent each dimension with an element from a finite field. When this is not the case, swap the permutation matrix P_π with a function that permutes the entries instead. Let $\mathcal{E}^{\otimes n}_{A\to B}$, and π be defined as above. Let $\mathcal{A}$ be a finite field with $|\mathcal{A}| = \dim(A)$. Then we have for any

$\vec{l}\,, \vec{l'} \in \mathcal{R}^n$ we perform the following

$$
\begin{aligned}
U_{B,P_\pi}\left(\mathcal{E}_{A\to B}^{\otimes n}\left(\left|\vec{l}\right\rangle\!\left\langle\vec{l'}\right|\right)\right)U_{B,P_\pi}^{\dagger} &= \sum_{\vec{k},\vec{k'}\in\mathcal{A}^n}\left|P_\pi\vec{k}\right\rangle\!\left\langle\vec{k}\right|\mathcal{E}_{A\to B}^{\otimes n}\left(\left|\vec{l}\right\rangle\!\left\langle\vec{l'}\right|\right)\left|\vec{k'}\right\rangle\!\left\langle P_\pi\vec{k'}\right| \\
&= \sum_{\vec{k},\vec{k'}\in\mathcal{A}^n}\left|\vec{k}\right\rangle\!\left\langle P_{\pi^{-1}}\vec{k}\right|\mathcal{E}_{A\to B}^{\otimes n}\left(\left|\vec{l}\right\rangle\!\left\langle\vec{l'}\right|\right)\left|P_{\pi^{-1}}\vec{k'}\right\rangle\!\left\langle\vec{k'}\right| \\
&= \sum_{\vec{k},\vec{k'}\in\mathcal{A}^n}\left|\vec{k}\right\rangle\!\left\langle\vec{k'}\right|\prod_{i=1}^{n}\left\langle k_{\pi(i)}\right|\mathcal{E}_{A_i\to B_i}\left(|l_i\rangle\langle l_i'|\right)\left|k'_{\pi(i)}\right\rangle \\
&= \sum_{\vec{k},\vec{k'}\in\mathcal{A}^n}\left|\vec{k}\right\rangle\!\left\langle\vec{k'}\right|\prod_{i=1}^{n}\langle k_i|\mathcal{E}_{A_i\to B_i}\left(\left|l_{\pi^{-1}(i)}\right\rangle\!\left\langle l'_{\pi^{-1}(i)}\right|\right)|k_i'\rangle \\
&= I\left(\bigotimes_{i=0}^{n}\mathcal{E}_{A_i\to B_i}\left(\left|l_{\pi^{-1}(i)}\right\rangle\!\left\langle l'_{\pi^{-1}(i)}\right|\right)\right)I \\
&= \mathcal{E}_{A\to B}^{\otimes n}\left(\left|P_\pi\vec{l}\right\rangle\!\left\langle P_\pi\vec{l'}\right|\right) \\
&= \mathcal{E}_{A\to B}^{\otimes n}(U_{A,P_\pi}\left|\vec{l}\right\rangle\!\left\langle\vec{l'}\right|U_{A,P_\pi}^{\dagger}).
\end{aligned}
\tag{A.7}
$$

Because $\mathcal{E}_{A\to B}^{\otimes n}$ is a linear transformation, we've proven this for any $\rho_A \in \mathrm{L}(A)$. □

Appendix B

Six-State Pre-Privacy Amplification proofs

B.1 Six-State Reduction Error Correction Cost

Proof of Theorem 3.2.1. The error correction cost for a choice of announcements was given in Equation (3.9). Alice and Bob only calculate the key rate for the bins they measured in the same basis choice. The simple term is $\mathrm{H}(Y)$ (reminder that we suppress the notation for conditioning on the Z-basis) which is the entropy of the maximally mixed state $\rho_Y = 2^{-n} I_Y$, and

$$\mathrm{H}(Y) = \mathrm{H}(2^{-n} I_Y) = n. \tag{B.1}$$

For the term $\mathrm{H}(R', Y)$, the joint state is given by Equation (3.27) for n copies of Equation (2.80), resulting in

$$\mathrm{H}(R', Y) = \mathrm{H}\left(\sum_{\vec{\gamma} \in \mathbb{Z}_2^m} \sum_{\vec{\beta} \in \mathbb{Z}_2^{n-m}} \sum_{\vec{l} \in \mathbb{Z}_2^n} |\vec{\gamma}\rangle\langle\vec{\gamma}|_{R'} \otimes X_Y^{V\vec{\gamma}} \left|\vec{l}\right\rangle\left\langle\vec{l}\right|_Y X_Y^{V\vec{\gamma}} \left\langle \vec{0},\ \tilde{V}\vec{\beta} + \vec{l} \right| \rho_{\text{single}AB}^{\otimes n} \left| \vec{0},\ \tilde{V}\vec{\beta} + \vec{l} \right\rangle \right) \tag{B.2}$$

where V and $\tilde{V}$ are chosen the same way as the theorem outlines. Note two very important properties of this. There is block diagonal structure in $|\vec{\gamma}\rangle\langle\vec{\gamma}|$ and a unitary transformation

by $X_Y^{V\vec{\gamma}}$ on system Y. Using Theorems 2.3.14, and 2.3.15, we rewrite $\mathrm{H}(R', Y)$ as

$$\begin{aligned}
\mathrm{H}(R', Y) &= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \sum_{\vec{l}\in\mathbb{Z}_2^n} X_Y^{V\vec{\gamma}} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_Y X_Y^{V\vec{\gamma}} \left\langle \vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right\rangle \right) \\
&= \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_Y \left\langle \vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right\rangle \right) \\
&= 2^m \,\mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \sum_{\vec{l}\in\mathbb{Z}_2^n} \left|\vec{l}\right\rangle\!\left\langle\vec{l}\right|_Y \left\langle \vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right\rangle \right).
\end{aligned} \tag{B.3}$$

Similarly, the block diagonal structure on $\vec{l}$ lets us pull its sum out. We then break down $\vec{l}$ into $\vec{l} = V\vec{\gamma} + \tilde{V}\vec{\phi}$ and follow

$$\begin{aligned}
\mathrm{H}(R', Y) &= 2^m \sum_{\vec{l}\in\mathbb{Z}_2^n} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle \vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ \tilde{V}\vec{\beta}+\vec{l}\right\rangle \right) \\
&= 2^m \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle \vec{0},\ V\vec{\gamma}+\tilde{V}(\vec{\beta}+\vec{\phi})\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ V\vec{\gamma}+\tilde{V}(\vec{\beta}+\vec{\phi})\right\rangle \right) \\
&= 2^m 2^{n-m} \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle \vec{0},\ V\vec{\gamma}+\tilde{V}\vec{\beta}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ V\vec{\gamma}+\tilde{V}\vec{\beta}\right\rangle \right) \\
&= 2^n \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle \vec{0},\ V\vec{\gamma}+\tilde{V}\vec{\beta}\right|\rho_{\mathrm{single}AB}^{\otimes n}\left|\vec{0},\ V\vec{\gamma}+\tilde{V}\vec{\beta}\right\rangle \right).
\end{aligned} \tag{B.4}$$

Now note that for $\rho_{\mathrm{single}AB}$ defined in Equation (2.80),

$$(\langle 0|_A \otimes I_B)\rho_{\mathrm{single}AB}(|0\rangle_A \otimes I_B) = \frac{1}{2}\left(\left(1-\frac{\xi}{2}\right)|0\rangle\!\langle 0|_B + \frac{\xi}{2}|1\rangle\!\langle 1|_B\right). \tag{B.5}$$

This is proportional to a binary symmetric channel with error rate $\frac{\xi}{2}$. Applying this to $\mathrm{H}(R', Y)$ gives

$$\begin{aligned}\mathrm{H}(R', Y) &= 2^n \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(2^{-n} \sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle V\vec{\gamma} + \tilde{V}\vec{\beta}\right| \left(\left(1-\frac{\xi}{2}\right)|0\rangle\langle 0|_B + \frac{\xi}{2}|1\rangle\langle 1|_B\right)^{\otimes n} \left|V\vec{\gamma} + \tilde{V}\vec{\beta}\right\rangle\right) \\ &= n + \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left\langle V\vec{\gamma} + \tilde{V}\vec{\beta}\right| \left(\left(1-\frac{\xi}{2}\right)|0\rangle\langle 0|_B + \frac{\xi}{2}|1\rangle\langle 1|_B\right)^{\otimes n} \left|V\vec{\gamma} + \tilde{V}\vec{\beta}\right\rangle\right).\end{aligned} \tag{B.6}$$

To better understand the inner product, let $\vec{l} = V\vec{\gamma} + \tilde{V}\vec{\beta}$. The inner product can be rewritten as

$$\prod_{i=1}^{n} \langle l_i|\left(\left(1-\tfrac{\xi}{2}\right)|0\rangle\langle 0|_B + \tfrac{\xi}{2}|1\rangle\langle 1|_B\right)|l_i\rangle = \prod_{i=1}^{n} \begin{cases} 1-\frac{\xi}{2}, & l_i = 0 \\ \frac{\xi}{2}, & l_i = 1 \end{cases} \tag{B.7}$$

Therefore, for each entry in $V\vec{\gamma} + \tilde{V}\vec{\beta}$ with a 0, we get factors of $1-\frac{\xi}{2}$, and for each entry of 1, a factor of $\frac{\xi}{2}$. Using the Hamming weight to count the number of ones produces

$$\begin{aligned}\mathrm{H}(R', Y) &= n + \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})}\right), \\ &= n + \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})}\right).\end{aligned} \tag{B.8}$$

Here, we used the fact that for $\vec{l} \in \mathbb{Z}_2^n$, $\mathrm{d}(\vec{l} + \vec{1s}) = n - \mathrm{d}(\vec{l})$, and that there exists a $\vec{\gamma'} \in \mathbb{Z}_2^m$ and a $\vec{\beta'} \in \mathbb{Z}_2^{n-m}$ such that $V\vec{\gamma'} + \tilde{V}\vec{\beta'} = \vec{1s}$. Then we just shift the indexing of $\vec{\gamma}$ and $\vec{\beta}$ by these.

Combining the terms gives

$$\delta_{\mathrm{leak}}^{(\vec{\alpha},\vec{\alpha})} = f \sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(V\vec{\gamma}+\tilde{V}\vec{\beta})}\right), \tag{B.9}$$

for the total cost of correcting a block of n bits. □

B.2 Proof of Φ_W Alternative Form

For Theorem 3.3.1, our goal is to show that we can rewrite $\Phi_W(\rho) := \sum_{\vec{l}\in\mathbb{Z}_2^b} Z^{W\vec{l}}\rho Z^{W\vec{l}}$ as $\Phi_W(\rho) = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{R}_W(\vec{\phi})\rho\,\mathrm{R}_W(\vec{\phi})$, with $\mathrm{R}_W(\vec{\phi}) = 2^{-b}\sum_{\vec{k}\in\mathbb{Z}_2^a}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\left|\vec{k}\right\rangle\!\left\langle\vec{k}\right|$. Before we do so, we prove a few small properties:

Lemma B.2.1. *Let* $\vec{l}, \vec{k} \in \mathbb{Z}_2^a$ *then*

$$Z^{\vec{l}}\left|\vec{k}\right\rangle = (-1)^{\vec{l}^{\,T}\vec{k}}\left|\vec{k}\right\rangle. \tag{B.10}$$

Proof. This follows by expanding the tensor product as follows

$$\begin{aligned} Z^{\vec{l}}\left|\vec{k}\right\rangle &= \bigotimes_{i=1}^{n} Z^{l_i}\left|k_i\right\rangle \\ &= \bigotimes_{i=1}^{n}(-1)^{l_i k_i}\left|k_i\right\rangle \\ &= (-1)^{\sum_{i=1}^{n} l_i k_i}\left|\vec{k}\right\rangle \\ &= (-1)^{\vec{l}^{\,\mathrm{T}}\vec{k}}\left|\vec{k}\right\rangle. \end{aligned} \tag{B.11}$$

□

Lemma B.2.2. *Let* $\vec{k} \in \mathbb{Z}_2^a$ *then*

$$\sum_{\vec{l}\in\mathbb{Z}_2^a}(-1)^{\vec{l}^{\,T}\vec{k}} = \begin{cases} 2^a, & \vec{k} = 0 \\ 0, & \textit{otherwise} \end{cases}. \tag{B.12}$$

Proof. The proof is fairly simple. For $\vec{k} = 0$, $\sum_{\vec{l}\in\mathbb{Z}_2^a}(-1)^{\vec{l}^{\,\mathrm{T}}0} = \sum_{\vec{l}\in\mathbb{Z}_2^a} 1 = 2^a$. For $\vec{k} \neq 0$, we see that $\sum_{\vec{l}\in\mathbb{Z}_2^a}(-1)^{\vec{l}^{\,\mathrm{T}}\vec{k}} = \sum_{\vec{l}\in\mathbb{Z}_2^a}(-1)^{\vec{k}^{\,\mathrm{T}}\vec{l}}$. Now $\dim(\ker(\vec{k}^{\,\mathrm{T}})) = 2^{a-1}$. Therefore, half the terms give $(-1)^0$ and the other half give $(-1)^1$. Adding them all together gives 0. □

With these Lemmas we can prove Theorem 3.3.1.

Proof of Theorem 3.3.1. We start by applying Φ_W to a general element of the basis $\left\{\left|\vec{k}\right\rangle\left\langle\vec{k'}\right|\right\}_{\vec{k},\vec{k'}\in\mathbb{Z}_2^a}$ and apply Lemma B.2.1.

$$\begin{aligned}\Phi_W\left(\left|\vec{k}\right\rangle\left\langle\vec{k'}\right|\right) &= 2^{-b}\sum_{\vec{l}\in\mathbb{Z}_2^b} Z^{W\vec{l}}\left|\vec{k}\right\rangle\left\langle\vec{k'}\right| Z^{W\vec{l}} \\ &= 2^{-b}\sum_{\vec{l}\in\mathbb{Z}_2^b}(-1)^{(\vec{k}+\vec{k'})^{\mathrm{T}}W\vec{l}}\left|\vec{k}\right\rangle\left\langle\vec{k'}\right| \\ &= 2^{-b}\sum_{\vec{l}\in\mathbb{Z}_2^b}(-1)^{\vec{l}^{\mathrm{T}}W^{\mathrm{T}}(\vec{k}+\vec{k'})}\left|\vec{k}\right\rangle\left\langle\vec{k'}\right|\end{aligned} \tag{B.13}$$

Applying Lemma B.2.2 ensures that we get a non-zero result only when $W^{\mathrm{T}}\vec{k} = W^{\mathrm{T}}\vec{k'}$, resulting in $\Phi_W\left(\left|\vec{k}\right\rangle\left\langle\vec{k'}\right|\right) = \delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}}\left|\vec{k}\right\rangle\left\langle\vec{k'}\right|$. Applying this to a general operator ρ, gives

$$\begin{aligned}\Phi_W(\rho) &= \sum_{\vec{k},\vec{k'}\in\mathbb{Z}_2^a}\delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}}\left|\vec{k}\right\rangle\left\langle\vec{k}\right|\rho\left|\vec{k'}\right\rangle\left\langle\vec{k'}\right| \\ &= \sum_{\vec{\phi}\in\mathbb{Z}_2^b}\left(\sum_{\vec{k}\in\mathbb{Z}_2^a}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\left|\vec{k}\right\rangle\left\langle\vec{k}\right|\right)\rho\left(\sum_{\vec{k}\in\mathbb{Z}_2^a}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\left|\vec{k}\right\rangle\left\langle\vec{k}\right|\right) \\ &= \sum_{\vec{\phi}\in\mathbb{Z}_2^b}\mathrm{R}_W(\vec{\phi})\rho\,\mathrm{R}_W(\vec{\phi}),\end{aligned} \tag{B.14}$$

where in the middle step we used $\delta_{W^{\mathrm{T}}\vec{k},W^{\mathrm{T}}\vec{k'}} = \sum_{\vec{\phi}\in\mathbb{Z}_2^b}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}}\delta_{\vec{\phi},W^{\mathrm{T}}\vec{k'}}$. □

B.3 Proof of the Entropy of Φ_W

Proof. From Equation (3.46), the non-zero eigenvalues must have the form $\langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle$, were $\vec{\phi}\in\mathbb{Z}_2^b$. Furthermore, for any $\vec{\phi}$ where $\langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle = 0$, $\mathrm{Q}(0) = 0$ so we can keep

them in the sum. Therefore, the entropy of $\Phi_W(|\psi\rangle\langle\psi|)$ is given by

$$\mathrm{H}(\Phi_W(|\psi\rangle\langle\psi|)) = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{Q}\left(\langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle\right). \tag{B.15}$$

We now rewrite $\mathrm{R}_W(\vec{\phi})$ using its definition from Equation (3.42) and simplify to

$$\langle\psi|\mathrm{R}_W(\vec{\phi})|\psi\rangle = \sum_{\vec{k}\in\mathbb{Z}_2^a} \delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}} \left|\left\langle\vec{k}\middle|\psi\right\rangle\right|^2. \tag{B.16}$$

Placing this back into the function Q gives

$$\mathrm{H}\left(\Phi_W(|\psi\rangle\langle\psi|)\right) = \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^a} \delta_{\vec{\phi},W^{\mathrm{T}}\vec{k}} \left|\left\langle\vec{k}\middle|\psi\right\rangle\right|^2\right), \tag{B.17}$$

completing the first part of the proof.

The second part of the proof revolves around removing the Kronecker delta function to improve the performance. To do so, we use Definition 3.1.2 to construct a representative space, $\mathcal{W}$, of W^{T} and Theorem 3.1.3 to break down W^{T} into parts acting on representative space, and the kernel. Let $c = \mathrm{rank}(W^{\mathrm{T}})$, $W_1 \in \mathbb{Z}_2^{a\times c}$ such that $\mathrm{Im}(W_1) = \mathrm{Im}(W^{\mathrm{T}})$, and $W_2 \in \mathbb{Z}_2^{a\times a-c}$ such that $\mathrm{Im}(W_2) = \ker(W^{\mathrm{T}})$. We then break down $W^{\mathrm{T}}\vec{k}$ into parts $W^{\mathrm{T}}(W_1\vec{k}_1 + W_2\vec{k}_2)$ and substitute this back into the entropy function.

$$\begin{aligned}
\mathrm{H}\left(\Phi_W(|\psi\rangle\langle\psi|)\right) &= \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{Q}\left(\sum_{\vec{k}_1\in\mathbb{Z}_2^c}\sum_{\vec{k}_2\in\mathbb{Z}_2^{a-c}} \delta_{\vec{\phi},W^{\mathrm{T}}(W_1\vec{k}_1+W_2\vec{k}_2)} \left|\left\langle W_1\vec{k}_1 + W_2\vec{k}_2\middle|\psi\right\rangle\right|^2\right) \\
&= \sum_{\vec{\phi}\in\mathbb{Z}_2^b} \mathrm{Q}\left(\sum_{\vec{k}_1\in\mathbb{Z}_2^c}\sum_{\vec{k}_2\in\mathbb{Z}_2^{a-c}} \delta_{\vec{\phi},W^{\mathrm{T}}W_1\vec{k}_1} \left|\left\langle W_1\vec{k}_1 + W_2\vec{k}_2\middle|\psi\right\rangle\right|^2\right).
\end{aligned} \tag{B.18}$$

Note that $W^{\mathrm{T}}W_1$ is injective, so for any value of $\vec{\phi}$ there is either a single solution to

$\vec{\phi} = W^{\mathrm{T}} W_1 \vec{k}_1$ or no solution at all. Going through each combination gives

$$\mathrm{H}\left(\Phi(|\psi\rangle\langle\psi|)\right) = \sum_{\vec{k}_1 \in \mathbb{Z}_2^c} \mathrm{Q}\left(\sum_{\vec{k}_2 \in \mathbb{Z}_2^{a-c}} \left| \left\langle W_1 \vec{k}_1 + W_2 \vec{k}_2 \middle| \psi \right\rangle \right|^2 \right), \tag{B.19}$$

Completing the proof. □

B.4 Equivalence of Column Permutations Proof

Proof for Theorem 3.4.2. Let F, P_π, F' and ρ_{AB} be defined as in Theorem 3.4.2. Eve holds a purification of the state giving $|\rho\rangle_{ABE}$. From the general procedure in Section 3.1.1, after applying measurements, key mapping and pre-privacy amplification, the reduced key register, Bob's registers and Eve share the density matrix

$$\begin{aligned} \rho_{R'YEC} &= \mathcal{E}_{\mathrm{PPA},R\to R'} \circ \mathcal{E}_{XC\to RC}^{\otimes n} \circ \mathcal{E}_{AB\to XYC}^{\prime\otimes n}(|\rho\rangle\langle\rho|_{ABE}) \\ &= \sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_{R'} \otimes \mathrm{Tr}_R\left[(|\vec{r}\rangle\langle\vec{r}|_R \otimes I_{YEC}) \mathcal{E}_{XC\to RC}^{\otimes n} \circ \mathcal{E}_{AB\to XYC}^{\prime\otimes n}(|\rho\rangle\langle\rho|_{ABE}) \right]. \end{aligned} \tag{B.20}$$

Our new state using F' is given by

$$\begin{aligned}
\rho'_{R'YEC} = &\sum_{\vec{r}\in\mathcal{R}^n} |FP_\pi\vec{r}\rangle\langle FP_\pi\vec{r}|_{R'} \\
&\otimes \mathrm{Tr}_R\left[(|\vec{r}\rangle\langle\vec{r}|_R \otimes I_{YEC})\mathcal{E}^{\otimes n}_{XC\to RC}\circ\mathcal{E}'^{\otimes n}_{AB\to XYC}(|\rho\rangle\langle\rho|_{ABE})\right] \\
= &\sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_{R'} \\
&\otimes \mathrm{Tr}_R\left[(|P_{\pi^{-1}}\vec{r}\rangle\langle P_{\pi^{-1}}\vec{r}|_R \otimes I_{YEC})\mathcal{E}^{\otimes n}_{XC\to RC}\circ\mathcal{E}'^{\otimes n}_{AB\to XYC}(|\rho\rangle\langle\rho|_{ABE})\right] \\
= &\sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_{R'} \\
&\times \mathrm{Tr}_R\left[(U_{R,P_{\pi^{-1}}}|\vec{r}\rangle\langle\vec{r}|_R U^\dagger_{R,P_{\pi^{-1}}} \otimes I_{YEC})\mathcal{E}^{\otimes n}_{XC\to RC}\circ\mathcal{E}'^{\otimes n}_{AB\to XYC}(|\rho\rangle\langle\rho|_{ABE})\right] \\
= &\sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_{R'} \otimes (I_E \otimes U^\dagger_{YC,P_\pi}) \\
&\times \mathrm{Tr}_R\left[(|\vec{r}\rangle\langle\vec{r}|_R \otimes I_{YEC})U_{RYC,P_\pi}\mathcal{E}^{\otimes n}_{XC\to RC}\circ\mathcal{E}'^{\otimes n}_{AB\to XYC}(|\rho\rangle\langle\rho|_{ABE})U^\dagger_{RYC,P_\pi}\right] \\
&\times (I_E \otimes U_{YC,P_\pi}).
\end{aligned} \tag{B.21}$$

By Theorem 2.3.14, the permutation of $U^\dagger_{YC,P_\pi}$ on the ends of $\rho'_{R'YEC}$ will not effect any entropy terms and thus not the key rate. Furthermore, $\mathcal{E}^{\otimes n}_{XC\to RC}\circ\mathcal{E}'^{\otimes n}_{AB\to XYC}$ are constructed by applying the same measurement and key mapping channel to each individual copy, therefore we can apply Theorem A.2.8. Thus, we can pull the permutation inside and apply it directly to $|\rho\rangle\langle\rho|_{ABE}$. Because ρ_{AB} is permutation invariant, by Theorem A.2.7 $(U_{P_\pi}\otimes I_E)|\rho\rangle\langle\rho|_{ABE}(U^\dagger_{P_\pi}\otimes I_E)$ is the same purification of ρ_{AB} up to a unitary U_E applied to Eve's system. From Theorem 2.4.1, the choice of purification is arbitrary and the key rate must be identical. □

B.5 Split Reduction Matrices Proof

Proof of Theorem 3.4.5. Let F_1, F_2, F, m, n, m_1, m_2, n_1, n_2, ρ_{AB} and $\mathcal{R}$ be defined as in Theorem 3.4.5. From Section 3.1.1, we know that $\mathcal{E}'^{\otimes n}_{AB\to XYC} = \bigotimes_{i=1}^n \mathcal{E}_{A_iB_i\to X_iY_iC_i}$, and

same for $\mathcal{E}_{XC\to RC}^{\otimes n}$. We partition these into

$$\begin{aligned}\mathcal{E}_{AB\to XYC}'^{\otimes n} &= \bigotimes_{i=1}^{n_1} \mathcal{E}'_{A_iB_i\to X_iY_iC_i} \otimes \bigotimes_{i=n_1+1}^{n} \mathcal{E}'_{A_iB_i\to X_iY_iC_i} \\ &= \mathcal{E}'^{\otimes n_1}_{A_1^{n_1}B_1^{n_1}\to X_1^{n_1}Y_1^{n_1}C_1^{n_1}} \otimes \mathcal{E}'^{\otimes n_2}_{A_{n_1+1}^{n}B_{n_1+1}^{n}\to X_{n_1+1}^{n}Y_{n_1+1}^{n}C_{n_1+1}^{n}},\end{aligned} \tag{B.22}$$

$$\begin{aligned}\mathcal{E}_{XC\to RC}^{\otimes n} &= \bigotimes_{i=1}^{n_1} \mathcal{E}_{X_iC_i\to R_iC_i} \otimes \bigotimes_{i=n_1+1}^{n} \mathcal{E}_{X_IC_i\to R_iC_i} \\ &= \mathcal{E}^{\otimes n_1}_{X_1^{n_1}C_1^{n_1}\to R_1^{n_1}C_1^{n_1}} \otimes \mathcal{E}^{\otimes n_2}_{X_{n_1+1}^{n}C_{n_1+1}^{n}\to R_{n_1+1}^{n}C_{n_1+1}^{n}},\end{aligned} \tag{B.23}$$

which split the calculation into blocks of size n_1 and n_2. Now we split the pre-privacy amplification key map into multiple blocks. We use extra subscripts to denote the reduction matrices.

$$\begin{aligned}\mathcal{E}_{\mathrm{PPA},F,R\to R'}(\rho_R) &= \sum_{\vec{r}\in\mathcal{R}^n} |F\vec{r}\rangle\langle F\vec{r}|_R \operatorname{Tr}_R[|\vec{r}\rangle\langle\vec{r}|_R \rho_R] \\ &= \sum_{\vec{r}_1\in\mathcal{R}^{n_1}} \sum_{\vec{r}_2\in\mathcal{R}^{n_2}} |F_1\vec{r}_1 \oplus F_2\vec{r}_2\rangle\langle F_1\vec{r}_1 \oplus F_2\vec{r}_2|_{R'} \\ &\qquad \times \operatorname{Tr}_R[|\vec{r}_1 \oplus \vec{r}_2\rangle\langle\vec{r}_1 \oplus \vec{r}_2|_R \rho_R] \\ &= \sum_{\vec{r}_1\in\mathcal{R}^{n_1}} \sum_{\vec{r}_2\in\mathcal{R}^{n_2}} |F_1\vec{r}_1\rangle\langle F_1\vec{r}_1|_{R_1'^{m_1}} \otimes |F_2\vec{r}_2\rangle\langle F_2\vec{r}_2|_{R_{m_1+1}'^{m}} \\ &\qquad \times \operatorname{Tr}_R[|\vec{r}_1\rangle\langle\vec{r}_1|_{R_1^{n_1}} \otimes |\vec{r}_2\rangle\langle\vec{r}_2|_{R_{n_1+1}^{n}} \rho_R] \\ &= \mathcal{E}_{\mathrm{PPA},F_1,R_1^{n_1}\to R_1'^{m_1}} \otimes \mathcal{E}_{\mathrm{PPA},F_2,R_{n_1+1}^{n}\to R_{m_1+1}'^{m}}(\rho_R).\end{aligned} \tag{B.24}$$

Therefore we have split the entire measurement, announcement and key mapping into

$$\begin{aligned}&\mathcal{E}_{\mathrm{PPA},F,R\to R'} \circ \mathcal{E}_{XC\to RC}^{\otimes n} \circ \mathcal{E}_{AB\to XYC}'^{\otimes n} \\ &\quad = \left(\mathcal{E}_{\mathrm{PPA},F_1,R_1^{n_1}\to R_1'^{m_1}} \circ \mathcal{E}^{\otimes n_1}_{X_1^{n_1}C_1^{n_1}\to R_1^{n_1}C_1^{n_1}} \circ \mathcal{E}'^{\otimes n_1}_{A_1^{n_1}B_1^{n_1}\to X_1^{n_1}Y_1^{n_1}C_1^{n_1}}\right) \\ &\qquad \otimes \left(\mathcal{E}_{\mathrm{PPA},F_2,R_{n_1+1}^{n}\to R_{m_1+1}'^{m}} \circ \mathcal{E}^{\otimes n_2}_{X_{n_1+1}^{n}C_{n_1+1}^{n}\to R_{n_1+1}^{n}C_{n_1+1}^{n}} \circ \mathcal{E}'^{\otimes n_2}_{A_{n_1+1}^{n}B_{n_1+1}^{n}\to X_{n_1+1}^{n}Y_{n_1+1}^{n}C_{n_1+1}^{n}}\right).\end{aligned} \tag{B.25}$$

Applying this $\rho_{A_1^{n_1}B_1^{n_1}} \otimes \rho_{A_{n_1+1}^{n}B_{n_1+1}^{n}}$ and splitting every entropy term at the tensor product gives the key rate, $R_{\mathrm{blk}}(F) = R_{\mathrm{blk}}(F_1) + R_{\mathrm{blk}}(F_2)$. □

B.6 Reducible Matrices and Disconnected Graphs Proof

Proof of Theorem 3.4.8. If the zero vector $\vec{0} \in \mathcal{F}$, then all three properties are trivially equivalent. We therefore work on the case where $\vec{0} \notin \mathcal{F}$. We prove them in a cycle.

Suppose F is reducible. Therefore, there exists a matrix $U \in \mathrm{GL}_m(\mathcal{R})$, permutation $\pi \in \mathrm{S}_n$, and reduction matrices $F_1 \in \mathcal{R}^{m_1 \times n_1}$ and $F_2 \in \mathcal{R}^{m_2 \times n_2}$, such that $n = n_1 + n_2$, $m = m_1 + m_2$ and $UFP_\pi^{-1} = \begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}$. Let $\{\vec{a}_i\}_{i=1\ldots m_1}$ and $\{\vec{b}_j\}_{j=1\ldots m_2}$ be the first m_1, and last m_2 columns of UFP_π^{-1} respectively. Note that:

$$\mathrm{span}(\{\vec{a}_i\}_{i=1\ldots m_1}) = \mathrm{span}(\{\vec{e}_i\}_{i=1\ldots m_1}), \tag{B.26}$$

$$\mathrm{span}(\{\vec{b}_j\}_{j=1\ldots m_2}) = \mathrm{span}(\{\vec{e}_j\}_{j=m_1+1\ldots m}). \tag{B.27}$$

Therefore,

$$\mathrm{span}(\{\vec{a}_i\}_{i=1\ldots m_1}) \cap \mathrm{span}(\{\vec{b}_j\}_{j=1\ldots m_2}) = \{\vec{0}\}. \tag{B.28}$$

Because U is invertible,

$$\{U^{-1}\vec{a}_i\}_{i=1\ldots m_1} \cap \{U^{-1}\vec{b}_j\}_{j=1\ldots m_2} = \{\vec{0}\}, \tag{B.29}$$

$$\{U^{-1}\vec{a}_i\}_{i=1\ldots m_1} \cup \{U^{-1}\vec{b}_j\}_{j=1\ldots m_2} = \mathcal{F}. \tag{B.30}$$

Therefore, the set $J = \{U^{-1}\vec{a}_i\}_{i=1\ldots m_1}$ satisfies all the properties we need, and finishes this part of the proof.

Let J be a proper subset of $\mathcal{F}$ such that $J \neq \emptyset$ and $\mathrm{span}(J) \cap \mathrm{span}(\mathcal{F}/J) = \{\vec{0}\}$. Also, for the reduced row echelon form $\mathrm{rref}(F)$, there exists an invertible matrix $U \in \mathrm{GL}_m(\mathcal{R})$ such that $\mathrm{rref}(F) = UF$. Because U produces the reduced row echelon form of F, it must take m_1 vectors from J and m_2 vectors from $\mathcal{F}/J$ to the canonical basis vectors $\{\vec{e}_i\}_{i=1,\ldots,m}$. Therefore, $U(J)$ and $U(\mathcal{F}/J)$ are spanned by separate subsets of the canonical basis. But, $U(J)$ and $U(\mathcal{F}/J)$ are the columns of $\mathrm{rref}(F)$. Therefore the rows and columns of $\mathrm{rref}(F)$ can be permuted into the form $\begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}$. This implies that the graph $\mathcal{G}(\mathrm{rref}(F))$ has (at least) two connected components, and is thus disconnected.

For the final part of the proof, we assume the graph $\mathcal{G}(\mathrm{rref}(F))$ is disconnected. Immediately, we can permute the green and blue vertices to list one component, followed by

the second one. Therefore, there exists a permutations $\pi \in \mathrm{S}_m$, and $\pi' \in \mathrm{S}_n$ such that $P_\pi \operatorname{rref}(F) P_{\pi'}^{-1}$ has the form $\begin{bmatrix} F_1 & 0 \\ 0 & F_2 \end{bmatrix}$. Furthermore, there exists a $U \in \mathrm{GL}_m(\mathcal{R})$ such that $UF = \operatorname{rref}(F)$. Because $P_\pi U \in \mathrm{GL}_m(\mathcal{R})$, F is reducible. $\square$

Appendix C

Proofs for the Simplified Trusted Relay

C.1 Equivalence of Reduction Matrices for the STR

Here is a compilation of proofs for equivalences of reduction matrices for the simplified trusted relay in Section 4.1.1. Many of these proofs build off of the original ones for protocols with pre-privacy amplification found in Section 3.4. As a quick reminder the simplified trusted relay's key map is given by

$$\mathcal{E}_{\mathrm{STR},R'\to R'_A C_R} \circ \mathcal{E}_{\mathrm{PPA},R\to R'}(\rho_R) = \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \Big|F\vec{r},\ F(\vec{r}+\vec{r'})\Big\rangle\Big\langle F\vec{r},\ F(\vec{r}+\vec{r'})\Big|_{R'_A C_R} \mathrm{Tr}\Big[\Big|\vec{r},\ \vec{r'}\Big\rangle\Big\langle\vec{r},\ \vec{r'}\Big|_R \rho_R\Big]. \quad \text{(C.1)}$$

Proof of Theorem 4.1.2. Let F, P_π, F' and ρ_{TAB} be defined as in Theorem 4.1.2. Eve holds a purification of $|\rho\rangle_{TABE}$. After measurement and the simplified trusted relay's key mapping, Alice, Bob, the relay and Eve share the state

$$\rho_{R'_A YEC} = \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \Big|F\vec{r},\ F(\vec{r}+\vec{r'})\Big\rangle\Big\langle F\vec{r},\ F(\vec{r}+\vec{r'})\Big|_{R'_A C_R} \otimes \mathrm{Tr}_{R'}[(\Big|\vec{r},\ \vec{r'}\Big\rangle\Big\langle\vec{r},\ \vec{r'}\Big|_R \otimes I_{YEC_{TAB}})\rho_{RYEC_{TAB}}]. \quad \text{(C.2)}$$

For the reduction matrix F' we get the state,

$$\begin{aligned}
\rho'_{R'_A YEC} = & \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \left|FP_\pi \vec{r},\ FP_\pi(\vec{r}+\vec{r'})\right\rangle\!\left\langle FP_\pi \vec{r},\ FP_\pi(\vec{r}+\vec{r'})\right|_{R'_A C_R} \\
& \otimes \mathrm{Tr}_{R'}[(\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle \vec{r},\ \vec{r'}\right|_R \otimes I_{YEC_{TAB}})\rho_{RYEC_{TAB}}] \\
= & \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \left|F\vec{r},\ F(\vec{r}+\vec{r'})\right\rangle\!\left\langle F\vec{r},\ F(\vec{r}+\vec{r'})\right|_{R'_A C_R} \\
& \otimes \mathrm{Tr}_{R'}[(\left|P_{\pi^{-1}}\vec{r},\ P_{\pi^{-1}}\vec{r'}\right\rangle\!\left\langle P_{\pi^{-1}}\vec{r},\ P_{\pi^{-1}}\vec{r'}\right|_R \otimes I_{YEC_{TAB}})\rho_{RYEC_{TAB}}] \\
= & \sum_{\vec{r},\vec{r'}\in\mathcal{R}^n} \left|F\vec{r},\ F(\vec{r}+\vec{r'})\right\rangle\!\left\langle F\vec{r},\ F(\vec{r}+\vec{r'})\right|_{R'_A C_R} \otimes \left(U^\dagger_{YC_{TAB},P_\pi}\otimes I_E\right) \\
& \times \mathrm{Tr}_{R'}\left[(\left|\vec{r},\ \vec{r'}\right\rangle\!\left\langle \vec{r},\ \vec{r'}\right|_R \otimes I_{YEC_{TAB}})\left(U_{RYC_{TAB},P_\pi}\otimes I_E\right)\right. \\
& \left. \rho_{RYEC_{TAB}}\left(U^\dagger_{RYC_{TAB},P_\pi}\otimes I_E\right)\right]\left(U_{YC_{TAB},P_\pi}\otimes I_E\right).
\end{aligned} \tag{C.3}$$

The matrix U_{YC_{TAB},P_π} just permutes announcements in classical registers so it has no effect on the key rate. In the middle of the trace we have the term $\rho_{RYEC_{TAB}}$, which is the state after the original key mapping but before the pre-privacy amplification mapping is applied. Writing this in terms of the channels gives

$$\rho_{RYEC_{TAB}} = \mathcal{E}_{XC_{TAB}\to RC_{TAB}} \circ \mathcal{E}'_{TAB\to XYC_{TAB}}(|\rho\rangle\!\langle\rho|_{TABE}), \tag{C.4}$$

which is constructed by applying the measurement and original key map to n individual systems on each side of the link. By Theorem A.2.8, we can pull U_{RYC_{TAB},P_π} through the channel and focus on $(U_{RYC_{TAB},P_\pi}\otimes I_E)\,|\rho\rangle_{TABE}$. ρ_{TAB} is permutation invariant, therefore by Theorem A.2.7, $(U_{RYC_{TAB},P_\pi}\otimes I_E)\,|\rho\rangle_{TABE}$ is equivalent to $|\rho\rangle_{TABE}$ up to a unitary operator on Eve's system. Because the choice of purification on Eve's system is arbitrary (Theorem 2.4.1), The key rate of $R_{\mathrm{blk}}(F') = R_{\mathrm{blk}}(F)$. □

Proof of Theorem 4.1.3. Let F_1, F_2, F, m, n, m_1, m_2, n_1, n_2, ρ_{TAB} and $\mathcal{R}$ as in Theorem 4.1.3. We then split the simplified trusted relay's key map and announcement into

$$\mathcal{E}_{\mathrm{STR},R'\to R'_A C_R} = \mathcal{E}_{\mathrm{STR},R'^{m_1}_1\to R'_{A^{m_1}_1} C_{R^{m_1}_1}} \otimes \mathcal{E}_{\mathrm{STR},R'^{m}_{m_1+1}\to R'_{A^{m}_{m_1+1}} C_{R^{m}_{m_1+1}}}. \tag{C.5}$$

From this point onward. The proof is identical to the proof of Theorem 3.4.5. Each link splits its pre-privacy amplification map, original key map and measurements in the exact same way. The key rate is then given by $R_{\text{blk}}(F) = R_{\text{blk}}(F_1) + R_{\text{blk}}(F_2)$. □

Proof of Theorem 4.1.4. Just as Theorem 3.4.6 is a simple extension of Theorem 3.4.5, so is Theorem 4.1.4 a simple extension of Theorem 4.1.3. The proof is practically identical. □

C.2 Proofs for STR Six-State Pre-Privacy Amplification

C.2.1 STR Six-State Pre-Privacy Amplification Holevo Quantity Part 1

Proof of Lemma 4.2.1. We start by splitting the entropy by using the block diagonal structure in Equation (4.18), then remove the unitary transformations. We also use Theorem 2.3.14 to split the entropy of the tensor product.

$$\begin{aligned}\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_R E}^{(\vec{\gamma})}\right) &= \sum_{\vec{\gamma},\vec{\gamma'}\in\mathbb{Z}_2^m} \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \mathrm{H}\Big(\left(Z^{V\vec{\gamma}}\otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right) \\ &\qquad \times \left(\sigma_{\vec{l}}\otimes\sigma_{\vec{l'}}\right)\left(Z^{V\vec{\gamma}}\otimes Z^{V(\vec{\gamma}+\vec{\gamma'})}\right)\Big) \\ &= 4^m \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sigma_{\vec{l}}\otimes\sigma_{\vec{l'}}\right) \\ &= 2\cdot 4^m \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \mathrm{Tr}\left[\sigma_{\vec{l'}}\right]\mathrm{H}\left(\sigma_{\vec{l}}\right).\end{aligned} \tag{C.6}$$

Expanding $\sigma_{\vec{l}}$ back into $\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}}\left|\tau_{\vec{l}}\right\rangle\!\left\langle\tau_{\vec{l}}\right| Z^{\tilde{V}\vec{\beta}}$, we can evaluate the trace separately giving

$$\sum_{\vec{l'}\in\mathbb{Z}_2^n} \mathrm{Tr}\left[\sigma_{\vec{l'}}\right] = 2^{-m}. \tag{C.7}$$

Subbing this back into $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)$ yields

$$\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right) = 2\cdot 2^m \,\mathrm{H}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} Z^{\tilde{V}\vec{\beta}}\,|\tau_{\vec{l}}\rangle\langle\tau_{\vec{l}}|\,Z^{\tilde{V}\vec{\beta}}\right). \tag{C.8}$$

We already solved this for the six-state protocol with pre-privacy amplification, and it is just the first term in (3.3.5), thus

$$\begin{aligned}&\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)\\ &\quad= 2\cdot\left(m + \sum_{\vec{l}\in\mathbb{Z}_2^n}\sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m}\left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+W_2\vec{k},\vec{l})}\left(\frac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(W_1\vec{\phi}+W_2\vec{k},\vec{l})}\right)\right).\end{aligned} \tag{C.9}$$

Using Theorem 3.3.3, we swap W_2 with F^{T}. □

C.2.2 STR Six-State Pre-Privacy Amplification Holevo Quantity Part 2

Proof of Lemma 4.2.2. We start by splitting the entropy using the block diagonal structure of Equation (4.19), then remove the unitary transformations.

$$\begin{aligned}\mathrm{H}\left(\rho_{C_RE}\right) &= 2^m \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} Z^{V\vec{\gamma}}\sigma_{\vec{l}}Z^{V\vec{\gamma}}\otimes Z^{V\vec{\gamma}}\sigma_{\vec{l'}}Z^{V\vec{\gamma}}\right)\\ &= 2^m \sum_{\vec{l},\vec{l'}\in\mathbb{Z}_2^n} \mathrm{H}\left(\sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\sum_{\vec{\beta},\vec{\beta'}\in\mathbb{Z}_2^{n-m}} \left(Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}\otimes Z^{V\vec{\gamma}+\tilde{V}\vec{\beta'}}\right)\right.\\ &\qquad\left.\times\left|\tau_{\vec{l}},\ \tau_{\vec{l'}}\right\rangle\left\langle\tau_{\vec{l}},\ \tau_{\vec{l'}}\right|\left(Z^{V\vec{\gamma}+\tilde{V}\vec{\beta}}\otimes Z^{V\vec{\gamma}+\tilde{V}\vec{\beta'}}\right)\right).\end{aligned} \tag{C.10}$$

Although at first glance it does not look like it, but this follows the same form as in Section 3.3. To make it clear, we define the following terms:

$$\tilde{\mathcal{V}} = \begin{bmatrix} V & \tilde{V} & 0 \\ V & 0 & \tilde{V} \end{bmatrix}, \qquad \vec{\mathcal{L}} = \begin{bmatrix} \vec{l} \\ \vec{l'} \end{bmatrix}, \qquad \vec{\mathcal{B}} = \begin{bmatrix} \vec{\gamma} \\ \vec{\beta} \\ \vec{\beta'} \end{bmatrix}, \tag{C.11}$$

$$\mathcal{W}_1 = \begin{bmatrix} 0 & W_1 & 0 \\ W_2 & 0 & W_1 \end{bmatrix}, \qquad \mathcal{W}_2 = \begin{bmatrix} W_2 \\ W_2 \end{bmatrix}, \qquad \mathcal{F} = \begin{bmatrix} F & F \end{bmatrix}. \tag{C.12}$$

Using these terms, we rewrite $\mathrm{H}\left(\rho_{C_R E}\right)$ as

$$\mathrm{H}\left(\rho_{C_R E}\right) = 2^m \sum_{\vec{\mathcal{L}} \in \mathbb{Z}_2^{2n}} \mathrm{H}\left(\sum_{\vec{\mathcal{B}} \in \mathbb{Z}_2^{2n-m}} Z^{\tilde{\mathcal{V}}\vec{\mathcal{B}}} \left|\tau_{\vec{\mathcal{L}}}\right\rangle\!\left\langle\tau_{\vec{\mathcal{L}}}\right| Z^{\tilde{\mathcal{V}}\vec{\mathcal{B}}} \right). \tag{C.13}$$

With Equation (3.56), we remove all diagonalizations and are left with

$$\begin{aligned} \mathrm{H}\left(\rho_{C_R E}\right) &= 2^m \sum_{\vec{\mathcal{L}} \in \mathbb{Z}_2^{2n}} \sum_{\vec{\mathcal{K}}_1 \in \mathbb{Z}_2^{2n-m}} \mathrm{Q}\left(2^{2n-m-2n} \sum_{\vec{\mathcal{K}}_2 \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\mathcal{W}_1 \vec{\mathcal{K}}_1 + \mathcal{W}_2 \vec{\mathcal{K}}_2, \vec{\mathcal{L}})} \right. \\ &\qquad \left. \times \left(\frac{\xi}{4}\right)^{2n - \tilde{\mathrm{d}}(\mathcal{W}_1 \vec{\mathcal{K}}_1 + \mathcal{W}_2 \vec{\mathcal{K}}_2, \vec{\mathcal{L}})} \right) \\ &= 2^m \sum_{\vec{\mathcal{L}} \in \mathbb{Z}_2^{2n}} \sum_{\vec{\mathcal{K}}_1 \in \mathbb{Z}_2^{2n-m}} \mathrm{Q}\left(2^{-m} \sum_{\vec{\mathcal{K}}_2 \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\mathcal{W}_1 \vec{\mathcal{K}}_1 + \mathcal{W}_2 \vec{\mathcal{K}}_2, \vec{\mathcal{L}})} \right. \\ &\qquad \left. \times \left(\frac{\xi}{4}\right)^{2n - \tilde{\mathrm{d}}(\mathcal{W}_1 \vec{\mathcal{K}}_1 + \mathcal{W}_2 \vec{\mathcal{K}}_2, \vec{\mathcal{L}})} \right), \end{aligned} \tag{C.14}$$

We then break down $\tilde{\mathrm{d}}(\mathcal{W}_1\vec{\mathcal{K}}_1+\mathcal{W}_2\vec{\mathcal{K}}_2, \vec{\mathcal{L}})$ using the underlying blocks. With Theorem 3.3.3, we swap W_2 to F^{T} and simplify.

$$\mathrm{H}\left(\rho_{C_R E}\right) = m + \sum_{\vec{l},\vec{l'},\vec{s}\in\mathbb{Z}_2^n} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi}+F^{\mathrm{T}}\vec{k},\vec{l})+\tilde{\mathrm{d}}(\vec{s}+F^{\mathrm{T}}\vec{k},\vec{l'})} \left(\frac{\xi}{4}\right)^{2n-\tilde{\mathrm{d}}(W_1\vec{\phi}+F^{\mathrm{T}}\vec{k},\vec{l})-\tilde{\mathrm{d}}(\vec{s}+F^{\mathrm{T}}\vec{k},\vec{l'})} \right). \tag{C.15}$$

□

Appendix D

Further Techniques for Performance

With Theorems 3.4.1, 3.4.2, 4.1.1 and4.1.2, we provide one final way to improve the performance of evaluating the six-state pre-privacy amplification protocol (with and without the simplified trusted relay). Using the listed theorems, we can assume the reduction matrix has the form $\begin{bmatrix} I_m & F' \end{bmatrix}$, for $F' \in \mathbb{Z}_2^{m \times n-m}$. For both protocols, we first rewrite the key rate equations with this form of the reduction matrix, then use a small, hard to spot symmetry to slightly reduce the number of summations that need to be computed.

Both Theorems 3.3.5 and 4.2.3 rely on the same matrices V, $\tilde{V}$, and W_1 in their key rates. With Theorem 3.3.3, we replaced the fourth matrix W_2 with the transpose of the reduction matrix, F^{T}. With the extra structure of $F = \begin{bmatrix} I_m & F' \end{bmatrix}$, we perform a similar process.

Lemma D.0.1. *Let $a \geq b$ and let $F = \begin{bmatrix} I_{a-b} & F' \end{bmatrix}$ be a reduction matrix with $F' \in \mathbb{Z}_2^{a-b \times b}$. Also, let $V, \tilde{V}, W_1$, and W_2 be the matrices:*

$$\begin{aligned} V &= \begin{bmatrix} I_{a-b} \\ 0 \end{bmatrix}, \quad \tilde{V} = \begin{bmatrix} F' \\ I_b \end{bmatrix}, \\ W_1 &= \begin{bmatrix} 0 \\ I_b \end{bmatrix}, \quad W_2 = \begin{bmatrix} I_{a-b} \\ F'^T \end{bmatrix} = F^T, \end{aligned} \tag{D.1}$$

then $FV = I_{a-b}$, $\mathrm{Im}(\tilde{V}) = \ker(F)$, $\tilde{V}^T W_1 = I_b$, and $\mathrm{Im}(W_2) = \ker(\tilde{V}^T)$.

Proof. Proving V, $\tilde{V}$, W_1, and W_2 satisfy the relations is just a matter of placing into the

definitions and checking those properties. □

Shared between both protocols, we apply this to the error correction cost first. Unlike the Holevo terms, the error correction calculation will not gain any speed up, but it will give us a form without needing to compute representative and kernel spaces. In Theorems 3.3.5 and 4.2.3, we calculate the hamming weight $\mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta})$. Applying Lemma D.0.1, we get

$$\begin{aligned} \mathrm{d}(V\vec{\gamma} + \tilde{V}\vec{\beta}) &= \mathrm{d}\left(\begin{bmatrix} \vec{\gamma} + F'\vec{\beta} \\ \vec{\beta} \end{bmatrix}\right) \\ &= \mathrm{d}(\vec{\gamma} + F'\vec{\beta}) + \mathrm{d}(\vec{\beta}), \end{aligned} \tag{D.2}$$

where we split the hamming weight by each block. We then substitute this back into the error correction terms. We perform a similar procedure for the Holevo terms with the function $\tilde{\mathrm{d}}$, then apply a small symmetry argument to slightly reduce the computation cost. The procedure for Theorems 3.3.5 and 4.2.3 are similar, though the later is slightly more complex.

Six-State Pre-privacy Amplification

In Theorem 3.3.5, we have the exponent $\tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k}, \vec{l})$. Applying Lemma D.0.1 and breaking apart $\vec{l}$ into two chunks gives

$$\tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k}, \vec{l}) = \tilde{\mathrm{d}}(\vec{k}, \vec{l}_{\,1}) + \tilde{\mathrm{d}}(\vec{k} + F'^{\mathrm{T}}\vec{k}, \vec{l}_{\,2}), \tag{D.3}$$

where $\vec{l}_{\,1} \in \mathbb{Z}_2^{n-m}$ and $\vec{l}_{\,2} \in \mathbb{Z}_2^m$ such that $\vec{l}^{\,\mathrm{T}} = \begin{bmatrix} \vec{l}_{\,1}^{\,\mathrm{T}} & \vec{l}_{\,2}^{\,\mathrm{T}} \end{bmatrix}$. When we rewrite this term in the entropy calculation, we get

$$\begin{aligned} &\sum_{\vec{l} \in \mathbb{Z}_2^n} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \tfrac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k}, \vec{l})} \left(\tfrac{\xi}{4}\right)^{n - \tilde{\mathrm{d}}(W_1\vec{\phi} + F^{\mathrm{T}}\vec{k}, \vec{l})}\right) \\ &= \sum_{\vec{l}_{\,1} \in \mathbb{Z}_2^m} \sum_{\vec{l}_{\,2} \in \mathbb{Z}_2^{n-m}} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m}} \mathrm{Q}\left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k}, \vec{l}_{\,1}) + \tilde{\mathrm{d}}(\vec{\phi} + F'^{\mathrm{T}}\vec{k}, \vec{l}_{\,2})} \left(\frac{\xi}{4}\right)^{n - \tilde{\mathrm{d}}(\vec{k}, \vec{l}_{\,1}) - \tilde{\mathrm{d}}(\vec{\phi} + F'^{\mathrm{T}}\vec{k}, \vec{l}_{\,2})}\right). \end{aligned} \tag{D.4}$$

Note that whenever a component of $\vec{l}_2$ equals 1, then changing the same component in $\vec{\phi}$ gives the same result. As such, the answer to $\tilde{\mathrm{d}}(\vec{k}, \vec{l}_1) + \tilde{\mathrm{d}}(\vec{\phi} + F'^{\mathrm{T}}\vec{k}, \vec{l}_2)$ is also the answer for $2^{\mathrm{d}(\vec{l}_2)}$ values of $\vec{\phi}$. With this in mind, we can cut down $\vec{\phi}$ from an element in $\mathbb{Z}_2^{n-m}$, to an element in $\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}$, then pad out $\vec{\phi}$ till its entries align with the spaces where $\vec{l}_2$ has elements of 0. To achieve this we define a *spacer matrix*.

Definition D.0.2. Let $\vec{l} \in \mathbb{Z}_2^n$, and the unique bijection $\theta : \{1, \ldots, \mathrm{d}(\vec{l} + \vec{1s})\} \to \{i | l_i = 0\}$ where for all $i < j$, $\theta(i) < \theta(j)$. We define the *spacer* matrix $S_{\vec{l}} \in \mathbb{Z}_2^{n \times \mathrm{d}(\vec{l}+\vec{1s})}$ as

$$S_{\vec{l}} = \sum_{i=1}^{\mathrm{d}(\vec{l}+\vec{1s})} \vec{e}_{\theta(i)} \vec{e}_i^{\mathrm{T}}. \tag{D.5}$$

For example, let $\vec{l}^{\mathrm{T}} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}$ and $\vec{\phi}^{\mathrm{T}} = \begin{bmatrix} \phi_1 & \phi_2 & \phi_3 \end{bmatrix}$ then

$$S_{\vec{l}} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad S_{\vec{l}}\vec{\phi} = \begin{bmatrix} \phi_1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & \phi_2 & 0 \\ 0 & 0 & \phi_3 \end{bmatrix}. \tag{D.6}$$

Applying this to the entropy term gives

$$\sum_{\vec{l}_1 \in \mathbb{Z}_2^m} \sum_{\vec{l}_2 \in \mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \mathrm{Q}\left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k}, \vec{l}_1) + \tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi} + F'^{\mathrm{T}}\vec{k}, \vec{l}_2)} \left(\frac{\xi}{4}\right)^{n - \tilde{\mathrm{d}}(\vec{k}, \vec{l}_1) - \tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi} + F'^{\mathrm{T}}\vec{k}, \vec{l}_2)} \right). \tag{D.7}$$

Overall the key rate for the six-state protocol with pre-privacy amplification from Theorem 3.3.5 is transformed to the following.

Theorem D.0.3. *For a reduction matrix $F = \begin{bmatrix} I_m & F' \end{bmatrix}$ with $F' \in \mathbb{Z}_2^{m \times n-m}$, acting on n copies of the shared state $\rho_{singleAB}^{\otimes n}$ from Equation (2.80) (depolarized by $\xi \in [0, 1]$). The key rate per* block *of the six-state protocol with pre-privacy amplification is lower bounded*

by

$$\frac{R_{blk}(F)}{\sum_{\vec{\alpha}\in\mathcal{A}^n} p(\vec{\alpha},\vec{\alpha})} \geq m + \sum_{\vec{l}_1\in\mathbb{Z}_2^m} \sum_{\vec{l}_2\in\mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \tag{D.8}$$
$$\mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)+\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^T\vec{k},\vec{l}_2)} \left(\frac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)-\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^T\vec{k},\vec{l}_2)}\right)$$
$$- n\left(\mathrm{Q}\left(1-\frac{3\xi}{4}\right)+3\,\mathrm{Q}\left(\frac{\xi}{4}\right)\right) - \delta_{leak},$$

where:

- $\delta_{leak} = f\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(\vec{\beta})+\mathrm{d}(\vec{\gamma}+F'^T\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(\vec{\beta})-\mathrm{d}(\vec{\gamma}+F'^T\vec{\beta})}\right)$.
- $f\in[1,\infty)$ *is the efficiency of error correction.*

Ignoring the poylynomial time it takes to calculate the exponents, we took the key rate calculation from on the order of 4^n operations to 4^m3^{n-m} operations ($4^m3^{n-m} = \sum\vec{l}_1\sum_{\vec{l_2}}\sum_{\vec{\phi}}\sum_{\vec{k}}1$). This is the form of the key rate implemented in the code. The only addition is using parallel pools to split the the sums of $\vec{l}_1$ and $\vec{l}_2$ across multiple cores for a little extra performance gain.

Simplified Trusted Relay for Six-State Pre-privacy Amplification

With Theorems 4.1.1 and 4.1.2, we can reduce to solving only reduction matrices $F\in\mathbb{Z}_2^{m\times n}$ of the form $F=\begin{bmatrix}I_m & F'\end{bmatrix}$. Link in the previous section we remove redundant terms in the summations. The solutions for $\sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right)$ was already solved in the six-sate protocol with pre-privacy amplification and is given by

$$\sum_{\vec{\gamma}\in\mathbb{Z}_2^m}\mathrm{H}\left(p(\vec{\gamma})\rho_{C_RE}^{(\vec{\gamma})}\right) = 2m + 2\sum_{\vec{l}_1\in\mathbb{Z}_2^m}\sum_{\vec{l}_2\in\mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}}$$
$$\mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m}\left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)+\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^{\mathrm{T}}\vec{k},\vec{l}_2)}\left(\frac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)-\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^{\mathrm{T}}\vec{k},\vec{l}_2)}\right), \tag{D.9}$$

where we use spacer matrices from Definition D.0.2. With a similar process to the one used in lemma D.0.1, we break down $\mathrm{H}(\rho_{C_R E})$ from Equation (C.15). We get the very long term

$$\mathrm{H}(\rho_{C_R E}) = m + \sum_{\vec{l}_1, \vec{l'}_1 \in \mathbb{Z}_2^m} 2^{\mathrm{d}(\vec{l'}_1)} \sum_{\vec{s}_1 \in \mathbb{Z}_2^{m-\mathrm{d}(\vec{l'}_1)}} \sum_{\vec{l}_2, \vec{l'}_2 \in \mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)+\mathrm{d}(\vec{l'}_2)} \times \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \sum_{\vec{s}_2 \in \mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l'}_2)}} \mathrm{Q} \left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\varphi} \left(\frac{\xi}{4}\right)^{2n-\varphi} \right), \quad \text{(D.10)}$$

where

$$\varphi = \tilde{\mathrm{d}}(\vec{k}, \vec{l}_1) + \tilde{\mathrm{d}}(S_{\vec{l}_2} \vec{\phi} + F'^{\mathrm{T}} \vec{k}, \vec{l}_2) + \tilde{\mathrm{d}}(S_{\vec{l'}_1} \vec{s}_1 + \vec{k}, \vec{l'}_1) + \tilde{\mathrm{d}}(S_{\vec{l'}_2} \vec{s}_2 + F'^{\mathrm{T}} \vec{k}, \vec{l'}_2). \quad \text{(D.11)}$$

We reorder $\mathrm{H}(\rho_{C_R E})$ into the form

$$\mathrm{H}(\rho_{C_R E}) = m + \sum_{\vec{l}_2, \vec{l'}_2 \in \mathbb{Z}_2^{n-m}} f(\vec{l}_2, \vec{l'}_2), \quad \text{(D.12)}$$

where f is a function containing all the other sums and terms. Notice that $f(\vec{l}_2, \vec{l'}_2) = f(\vec{l'}_2, \vec{l}_2)$. Therefore, anytime we compute $f(\vec{l}_2, \vec{l'}_2)$ we get $f(\vec{l'}_2, \vec{l}_2)$ for free. To save on computational time, we can sum over only the terms where $\vec{l'}_2 \leq \vec{l}_2$.[1] Therefore, whenever $\vec{l'}_2 < \vec{l}_2$, we need to add $f(\vec{l}_2, \vec{l'}_2)$ twice, and only once for equality. This is easily given by a simple factor of $2 - \delta_{\vec{l}_2, \vec{l'}_2}$. The entropy of $\mathrm{H}(\rho_{C_R E})$ is thus given by

$$\mathrm{H}(\rho_{C_R E}) = m + \sum_{\vec{l}_1, \vec{l'}_1 \in \mathbb{Z}_2^m} 2^{\mathrm{d}(\vec{l'}_1)} \sum_{\vec{s}_1 \in \mathbb{Z}_2^{m-\mathrm{d}(\vec{l'}_1)}} \sum_{\vec{l}_2 \in \mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{l'}_2 \leq \vec{l}_2} 2^{\mathrm{d}(\vec{l'}_2)} (2 - \delta_{\vec{l}_2, \vec{l'}_2}) \times \sum_{\vec{\phi} \in \mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \sum_{\vec{s}_2 \in \mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l'}_2)}} \mathrm{Q} \left(\sum_{\vec{k} \in \mathbb{Z}_2^m} \left(1 - \frac{3\xi}{4}\right)^{\varphi} \left(\frac{\xi}{4}\right)^{2n-\varphi} \right). \quad \text{(D.13)}$$

[1] Here we say a vector $\vec{a} \leq \vec{b}$ if and only if $a \leq b$, where a and b are the integers in binary when we read $\vec{a}$ and $\vec{b}$ as binary strings.

This further cuts the computational time by roughly a half. From Theorem D.0.3, we already know the the cost of error correction. Putting it all together gives the following theorem for the key rate.

Theorem D.0.4. *Let $F \in \mathbb{Z}_2^{m\times n}$ be a reduction matrix with the form $F = \begin{bmatrix} I_m & F' \end{bmatrix}$, acting on n copies of the shared state $\rho_{T_AA} \otimes \rho_{T_BB}$ from Equation (2.80) (depolarized by $\xi \in [0,1]$). The key rate per* block *of the six-state simplified trusted relay with pre-privacy amplification protocol is lower bounded by*

$$
\begin{aligned}
R_{blk} \geq \left(\sum_{(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'})\in \mathcal{S}^n\times\mathcal{S}^n} p(\vec{\alpha},\vec{\alpha'},\vec{\beta},\vec{\beta'}) \right) \Bigg[2m + 2 \sum_{\vec{l}_1\in\mathbb{Z}_2^m} \sum_{\vec{l}_2\in\mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \\
\mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\frac{3\xi}{4}\right)^{\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)+\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^T\vec{k},\vec{l}_2)} \left(\frac{\xi}{4}\right)^{n-\tilde{\mathrm{d}}(\vec{k},\vec{l}_1)-\tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^T\vec{k},\vec{l}_2)} \right) \\
- m - \sum_{\vec{l}_1,\vec{l'}_1\in\mathbb{Z}_2^m} 2^{\mathrm{d}(\vec{l'}_1)} \sum_{\vec{s}_1\in\mathbb{Z}_2^{m-\mathrm{d}(\vec{l'}_1)}} \sum_{\vec{l}_2\in\mathbb{Z}_2^{n-m}} 2^{\mathrm{d}(\vec{l}_2)} \sum_{\vec{l'}_2\leq\vec{l}_2} 2^{\mathrm{d}(\vec{l'}_2)}(2-\delta_{\vec{l}_2,\vec{l'}_2}) \\
\times \sum_{\vec{\phi}\in\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l}_2)}} \sum_{\vec{s}_2\in\mathbb{Z}_2^{n-m-\mathrm{d}(\vec{l'}_2)}} \mathrm{Q}\left(\sum_{\vec{k}\in\mathbb{Z}_2^m} \left(1-\frac{3\xi}{4}\right)^{\varphi} \left(\frac{\xi}{4}\right)^{2n-\varphi} \right) - \delta_{leak} \Bigg], \quad \text{(D.14)}
\end{aligned}
$$

where:

- *The post-selection set of basis announcements is* $\mathcal{S} = \{(\vec{\alpha},\vec{\alpha}) | \vec{\alpha} \in \mathcal{A}^n\}$.
- $\varphi = \tilde{\mathrm{d}}(\vec{k},\vec{l}_1) + \tilde{\mathrm{d}}(S_{\vec{l}_2}\vec{\phi}+F'^T\vec{k},\vec{l}_2) + \tilde{\mathrm{d}}(S_{\vec{l'}_1}\vec{s}_1+\vec{k},\vec{l'}_1) + \tilde{\mathrm{d}}(S_{\vec{l'}_2}\vec{s}_2+F'^T\vec{k},\vec{l'}_2)$.
- $\delta_{leak} = f\sum_{\vec{\gamma}\in\mathbb{Z}_2^m} \mathrm{Q}\left(\sum_{\vec{\beta}\in\mathbb{Z}_2^{n-m}} \left(1-\frac{\xi}{2}\right)^{\mathrm{d}(\vec{\beta})+\mathrm{d}(\vec{\gamma}+F'^T\vec{\beta})} \left(\frac{\xi}{2}\right)^{n-\mathrm{d}(\vec{\beta})-\mathrm{d}(\vec{\gamma}+F'^T\vec{\beta})} \right)$.
- $f \in [1,\infty)$ *is the efficiency of error correction.*