# INFORMATION VS. DISTURBANCE IN DIMENSION D

P. Oscar Boykin

*Department of Electrical and Computer Engineering, University of Florida*
*Gainesville, Florida 32611, USA*

Vwani P. Roychowdhury

*Department of Electrical Engineering, University of California, Los Angeles*
*Los Angeles, California 90024, USA*

We show that for Eve to get information in one basis about a state, she must cause errors in *all* bases that are mutually unbiased to that basis. Our result holds in any dimension. We also show that this result holds for *all functions of messages* that are encrypted with a key.

*Keywords*: Quantum Cryptography, QKD, MUB

## 1 Introduction

Ideal quantum key distribution (QKD) *with qubits*[1] is known to be secure[2, 3, 4, 5, 6], and the security proofs are based on what are called information-vs.-disturbance results. The basic QKD protocol involves the following steps: Alice transmits one of four possible states randomly chosen from $|0\rangle_X, |1\rangle_X, |0\rangle_Z$, and $|1\rangle_Z$, i.e., the basis vectors in the $X$ and $Z$ bases. The basic information-vs.-disturbance result states that if the eavesdropper, Eve, obtains information about which basis vector was sent in for example, the $X$ basis, then she must introduce disturbance in the $Z$ basis. By disturbance, it is meant that if Bob made measurements to distinguish between the two states sent in the $Z$ basis, then he will observe errors. Thus Alice and Bob can test a random subset of a transmitted block of qubits in the $Z$ basis and estimate the information that Eve has about those in the $X$ basis. If the error rate is small enough in the tested qubits (hence, Eve's information about the qubits in the $X$ basis is small enough), then Alice and Bob can use classical error correcting and amplification schemes to distill an informationally secure key from the qubits sent in the $X$ basis.

In this paper, we consider a general setup involving $D$ dimensional quantum states, instead of the 2-dimensional systems considered in the QKD literature. The basic setup is as follows: Alice sends states chosen randomly from among the basis vectors of a particular basis of the $D$ dimensional Hilbert space. She intends these states to act as the information states, i.e., the $\log D$ bits per transmitted state will be used to distill a final key. The natural questions that arise are (i) which set of states should the "test" states come from, and (ii) what is the corresponding information-vs.-disturbance result for a $D$-dimensional space.

We first extend some basic distinguishability bounds found for qubits[7] to $D$-level systems. That is, if a source $S$ outputs one of $n$ $D$-dimensional quantum states randomly, then we derive bounds on the mutual information between $S$ and any measurement output $E$, only in terms of the properties of the quantum states generated by $S$. In other words, we bound the mutual information between the random variable representing which state was generated by $S$ and the random variable representing the output from a generalized measurement of the states output by $S$. These results are powerful because they only depend on the source and not on any measurement done. We next apply these bounds on distinguishability to relate the

amount of information eavesdroppers can obtain to the disturbance they cause in the quantum state. In particular, we prove a generalized information-vs.-disturbance result: if Eve gets information about which basis vector (from the chosen basis in $D$ dimensions) was sent by Alice, then she must introduce *disturbance in any basis that is mutually unbiased to the basis chosen by Alice.*

In terms of previous work, our results generalize those in [4, 8]. We would also like to note that QKD in dimension 3 was studied in [9, 10]. Security bounds for individual cloning attacks in dimension $D$ have been reported[11]. More recently, qubit QKD techniques[3, 5] have been generalized to prime dimensions[12]. By contrast, our bounds *apply to any attack in any dimension.* Also, this work further illuminates the relationship of mutually unbiased bases (MUBs)[13] to quantum cryptography. Previously, it was shown that the eigenvectors of maximally commuting quantum encryption operators form MUBs[14]. Here we show that when Eve tries to get information in one basis, she disturbs *all* MUBs. Our result may be viewed as form of an uncertainty principle: the more Eve knows about one basis, the more she disturbs *all* conjugate bases.

In addition to applying the above bounds and techniques to the security of quantum keys, we also consider *functions of messages encrypted with those keys.* If Alice and Bob share a key $k$, it may be that Eve learns only exponentially little information about $k$, but she may be able to learn a lot about some function of a message $f(M)$, given the encrypted version of that message $m + k$. In particular, consider the following setup: Alice sends a random basis vector $|k\rangle$ belonging to a chosen basis to Bob. Alice next publicly announces she sent basis vector $|k \oplus m\rangle$, where $\oplus$ is the bitwise exclusive or (XOR) operation. Bob could then recover the encrypted message $m$. Now, we know that information of Eve about $k$ is bounded by the error she causes in any basis that is mutually unbiased to the chosen basis. How about a function $f(M)$ of the message? For example, Eve might be interested in only learning whether $m = 0$ or not. In a previous work[8], it was shown that given the encrypted message, $m + k$, the information that Eve gets about any function of an encrypted n-bit message $f(m)$, is bounded by the square root of the error Eve's attack causes in the Hadamard transformed basis. More recently, alternative and more general solutions to this problem have been given [15, 16]. In this work we extend previous results[8] beyond qubits to $d$-dimensional systems. Also, we show that Eve's information is bounded by the error she causes is *any* MUB.

This paper is structured as follows: Section 2 gives various new bounds on distinguishability and classical information accessible from quantum states; Section 3 applies these results to obtain "information-vs-disturbance" results for QKD; finally in Section 4 we show these results also hold for *functions of encrypted messages* and not just for the keys themselves.

## 2 Bound On Information For Any Source

In [7], many bounds are given on the distinguishability of two quantum states. In this section we generalize some of those to the distinguishability of $n$ quantum states. Our setting is the following: A source outputs one of $n$ quantum states. The random variable representing the source is $S$ i.e., it is the identifier of the particular quantum state made available at the output and can be generated by purely classical means, such as flipping coins or spinning wheels. A general measurement is made on the state, which results in one of several measurement outcomes represented by the random variable $E$. We consider bounds on the mutual information

$I(S;E)$ valid for any measurement, which is to say, the bound will only be a function of the quantum states emitted by the source.

The bounds here address the same problem as the well known Holevo bound[17], which is:

$$I(S;E) \leq H(\rho) - \sum_s p_s H(\rho_s) \tag{1}$$

where $H(\rho)$ is the Von-Neumann entropy of the density matrix $\rho$. The main difference between the results of this section and the Holevo bound is that these results deal explicitly with a distance metric, namely the trace norm distance, between two density matrices. Using a simple distance metric allows a certain ease in proving the results in Section 3*

In the appendix, we review certain previously published [7, 8] bounds on distinguishability of quantum states. As we will see later in the paper, this allows us to derive the fundamental information vs. disturbance results that are at work in quantum security protocols. Additionally, these results give an important insight into the robustness of the trace norm as a metric bound for information.

We begin by developing a lower bound on entropy and then applying that bound to the mutual information.

**Lemma 1** *For any random variable $X'$ with each probability $p_i{}' \leq 1/2$:*

$$H(X) \geq H(X') - \sum_i \log(\frac{1}{p_i{}'})|p_i - p_i{}'|$$

**P**roof.$H(X) = -\sum_i p_i \log p_i$, so if we define $f(p_i) \equiv -p_i \log p_i$, we see that $H(X) = \sum_i f(p_i)$. See that $f$ is concave and is zero at $p_i = 0, 1$; thus lemma A.1 applies:

$$f(p_i) \quad \geq \quad f(p_i{}') - \frac{f(p_i{}')}{p_i{}'}|p_i - p_i{}'|$$

Plugging this into the definition of entropy:

$$\begin{aligned} H(X) &= \sum_i f(p_i) \\ &\geq \sum_i (f(p_i{}') - \frac{f(p_i{}')}{p_i{}'}|p_i - p_i{}'|) \\ &= H(X') - \sum_i \log(\frac{1}{p_i{}'})|p_i - p_i{}'| \end{aligned}$$

∎

**Lemma 2** *For any source $S$ that outputs $s$ with probability $p_s$ such that $p_s \leq 1/2$, the mutual information is bounded:*

$$I(S;E) \quad \leq \quad \sum_s p_s \log(\frac{1}{p_s}) \sum_e |p(e|s) - p(e)|$$

*We do believe, however, that it is possible to obtain similar results by applying the purification techniques of Section 3 directly to the Holevo bound.

**P**roof.Make use of lemma 1:

$$\begin{aligned} I(S;E) &= H(S) - H(S|E) \\ &= H(S) - \sum_e p_e H(S|E=e) \\ &\leq H(S) - \sum_e p_e \left( H(S) - \sum_s \log(\frac{1}{p_s}) |p(s|e) - p_s| \right) \\ &= \sum_e p_e \sum_s \log(\frac{1}{p_s}) |p(s|e) - p_s| \\ &= \sum_e \sum_s p_s \log(\frac{1}{p_s}) |\frac{p(e)p(s|e)}{p_s} - p(e)| \\ &= \sum_e \sum_s p_s \log(\frac{1}{p_s}) |p(e|s) - p(e)|. \end{aligned}$$

∎

**Lemma 3** *If a source $S$ outputs quantum states $\rho_i$ with probabilities $p_i$ with $p_i \leq 1/2$, then mutual information between this source and the output of any measuring device $E$ is bounded:*

$$I(S;E) \leq \sum_s p_s \log(\frac{1}{p_s}) Tr|\rho_s - \sum_s p_s \rho_s|.$$

**P**roof.Define the notation $\rho = \sum_s p_s \rho_s$. Starting from lemma 2, we use the definition of a POVM to replace $p(e|s)$ with $Tr(E_e \rho_s)$:

$$\begin{aligned} I(S;E) &\leq \sum_e \sum_s p_s \log(\frac{1}{p_s}) |p(e|s) - p(e)| \\ &= \sum_e \sum_s p_s \log(\frac{1}{p_s}) |Tr(E_e \rho_s) - Tr(E_e \rho)| \\ &= \sum_e \sum_s p_s \log(\frac{1}{p_s}) |Tr(E_e(\rho_s - \rho))| \end{aligned}$$

Using the same facts about POVMs as in lemma A.3, one can show that

$$\sum_e |Tr(E_e(\rho_s - \rho))| \leq Tr|\rho_s - \rho|.$$

Hence, we have:

$$I(S;E) \leq \sum_s p_s \log(\frac{1}{p_s}) Tr|\rho_s - \rho|.$$

∎

**Corollary 1** *If a source $S$ outputs one of $n$ quantum states $\rho_i$ with probability $1/n$, then mutual information between this source and the output of any measuring device $E$ is bounded:* $I(S;E) \leq \log n \sum_s \frac{1}{n} |\rho_s - \rho|$.

**P**roof.For all $n \geq 2$, then $1/n \leq 1/2$, hence lemma 3 applies:

$$\begin{aligned} I(S;E) &\leq \sum_s p_s \log(\frac{1}{p_s}) Tr|\rho_s - \rho| \\ &= \log n \sum_s \frac{1}{n} Tr|\rho_s - \rho| \end{aligned}$$

∎

Now we have a basic lemma in hand which gives an upper bound on the information any measurement device can get from any source, purely in terms of the quantum states emitted from that source. In the next section, we will model the eavesdropping process as a source of quantum states for Eve. Eve is free to measure states in any way, but using the previous lemma, we have an upper bound on how much information she may obtain.

## 3 Security of Quantum Key Distribution

We now have the tools necessary in order to derive an *information theoretic counterpart to the Heisenberg uncertainty principle*. This result is the basis for quantum security results in [4]. Quantum key distribution (QKD) is directly related to the setup we considered in the previous section. In general, in a QKD setup Alice has the source $S$ that outputs one of $n$ quantum states; Alice transmits the output state over a quantum channel to Bob. This quantum channel, however, can belong to the eavesdropper Eve, who can perform any operation that quantum mechanics allows. Figure 3 gives a schematic of the most general attack that Eve might perform. From her perspective, she has access to a source, and she can make any measurement to get information about what was sent. Bob thus receives a state that Eve has already processed and makes his own measurements using a fixed protocol that is known to everyone. Alice and Bob complete a block transmission of several output states of the source $S$, and then use classical communication over an open channel to distill a secret key. Eve can listen in as well on the classical channel, but cannot perform a person-in-the-middle attack on the classical channel, which will make the whole protocol trivially unsecured. Such a classical channel can be easily implemented by message authentication, e.g., via previously shared secret bits between Alice and Bob.

Security of the QKD schemes depend on the amount of mutual information between Alice's source, $S$, and Eve's measurement $E$ (i.e., $I(S;E)$ as considered in the previous section) when measured as a function of the disturbance that she causes to the state received by Bob. The intuition from quantum mechanics is that measurements will disturb the system; hence, Alice and Bob can use a random subset of the transmitted quantum states for testing purposes, and detect the error rate on this subset, and thereby infer how strongly has Eve attacked the whole block. The underlying result and assumption here is that if the error she causes is less than a threshold then so is the mutual information $I(S;E)$. They proceed with key distillation only if the test errors are below a pre-specified threshold. Next, one can use classical privacy amplification schemes to show that as long as $I(S;E)$ is small enough (as implied by the disturbance), then one can make the mutual information between $E$ and a final distilled key as low as possible. These classical techniques involve the use of error correcting codes.

Thus, the derivation of an appropriate "information vs. disturbance" result lies at the heart of all security proofs for QKD. While it is clear what we mean by "information," (as

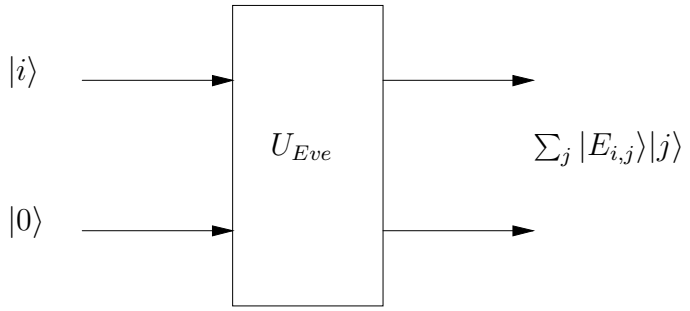


Fig. 3 Most general attack by an eavesdropper.

defined by the quantity $I(S;E)$), we have not yet quantified and defined what we mean by "disturbance." In various security proofs of QKD, researchers have adopted the following strategy: (i) In the protocol, the source $S$ outputs states chosen from the basis vectors belonging to two different bases, e.g., the $X$ and $Z$ bases. (ii) The information vs. disturbance results then refer to the information about which basis vector from one of the bases (e.g., $X$) was sent, and the disturbance caused in the second basis (e.g., $Z$). That is, Eve cannot simultaneously get significant information about which basis vector was sent in one basis, without causing errors in Bob's inference about which basis vector was sent in the other basis. Thus for testing purposes, one could use the states in one of the bases and the observed error rate will put a bound on the information that Eve has about which basis vectors were sent in the other bases.

Specifically, Lo and Chau[3] use an EPR based scheme and show (using the Holevo bound, equation 1) that if the fidelity between Alice and Bob is greater than $1-\delta$ for $R$ singlets, then Eve's information about the final key is bounded by:

$$I \quad \leq \quad -(1-\delta)\log(1-\delta) - \delta \log \frac{\delta}{2^{2R}-1}$$

The above information-vs-disturbance result is used directly by Shor and Preskill in their quantum code based proof[5]. Rather that deal with the fidelity of singlets, Biham et. al.[4] use trace-norm techniques to show that Eve's information on each bit is bounded by the square root of the probability that she would cause more than $\hat{v}/2$ errors had Alice sent the bits in the opposite basis (X replaced with Z and vice-versa), where $\hat{v}$ is the minimum distance between the privacy amplification code and the error correction code. The security of QKD directly depends on the above results: Eve's information is always bounded once Alice and Bob verify that their states have not been greatly disturbed.

In this section, we generalize such information vs. disturbance bounds for states in any dimension $D$, and *also provide a natural choice of the bases* to be used in these results. At this point it is useful to define the concept of Mutually Unbiased Bases:

**Definition.** Let $B_1 = \{|\varphi_1\rangle, \ldots, |\varphi_D\rangle\}$ and $B_2 = \{|\psi_1\rangle, \ldots, |\psi_D\rangle\}$be two orthonormal bases in the $D$ dimensional state space. They are said to be **mutually unbiased bases (MUB)** if and only if $|\langle\varphi_i|\psi_j\rangle| = \frac{1}{\sqrt{D}}$, for every $i,j = 1,\ldots,d$. A set $\{\mathcal{B}_1,\ldots,\mathcal{B}_m\}$ of orthonormal bases in $C^D$ is called a *set of mutually unbiased bases* (a set of MUB) if each pair of bases $\mathcal{B}_i$ and $\mathcal{B}_j$ are mutually unbiased.

Thus, given two MUB $B_1$ and $B_2$, we get $B_1 B_2^\dagger = H$, where $|H_{i,j}| = 1/\sqrt{D}$, and $H$ is a unitary matrix. Hence, *$H$ can be regarded as a generalized Hadamard matrix* in dimension $D$, and the two bases are related by the transformation $B_1 = HB_2$. We next derive a general theorem which shows that whatever the dimension, if Eve gets information in one basis, she disturbs *all* bases which are MUBs of that basis. Since two MUB are related by a generalized Hadamard transformation, the result in Theorem 1 implies that retrieving information in one basis causes disturbances in *all the conjugate bases*.

Finally, it should be emphasized that we only consider a single $D$-dimensional state. This is not a limitation: any product of quantum states can be thought of as a state in a larger dimensional space. Thus, if we consider standard BB84, $n$ 2-dimensional systems (bits) are sent. In our approach we would consider that as one $2^n$ dimensional system. The same applies for any product of quantum states. These results generalize those presented in [8], which proved the following theorem only for dimension $2^n$ and for one pair of bases (the standard $Z$ and $X$ bases).

**Theorem 1** *If Alice sends a randomly selected element from a $D$-dimensional basis (represented by the random variable $A$) to Bob, the information Eve's measurement (represented by $E$) has about Alice's state is bounded by the square root of the probability that Eve would have caused errors in any MUB with respect to Alice's basis:*

$$I(A;E) \quad \leq \quad 4 \log D \sqrt{P_{\widetilde{e}}} \, .$$

**P**roof.We will use lemmas A.6 and A.5 and corollary 1. Starting from corollary 1 we see that: $I(A;E) \leq \log D \sum_i \frac{1}{D} |\rho_i - \rho|$. Our approach will be to bound this by introducing a purification[†]for $\rho_i$ (the state that Eve holds when Alice sends $i$). Using the purification and lemma A.6 we can bound the original trace norm distance.

To attack the state sent to Bob, Eve attaches a probe in a fixed state (say the $|0\rangle$ state) and applies a unitary operator. She then passes Bob his part, and does some generalized measurement on what she still holds. We can characterize this formally:

$$|0\rangle_E |i\rangle_A \stackrel{U}{\rightarrow} \sum_j |E_{i,j}\rangle |j\rangle$$

We represent the MUB as:

$$|\widetilde{i}\rangle \quad \equiv \quad \sum_j H_{ji} |j\rangle$$

With $H$ being a generalized Hadamard matrix on these $D$-dimensional basis: $|H_{ji}| = \frac{1}{\sqrt{D}}$. Applying this to Eve's attack, we obtain:

$$|0\rangle_E |\widetilde{i}\rangle_A \stackrel{U}{\rightarrow} \sum_j |\widetilde{E_{i,j}}\rangle |\widetilde{j}\rangle$$

where $|\widetilde{E_{i,j}}\rangle \equiv \sum_{i',j'} H_{i'i} H^*_{j'j} |E_{i',j'}\rangle$.

From the axioms of quantum mechanics, we know that if Alice sends $|i\rangle$ the probability that Bob will measure $|j\rangle$ is $P(j|i) = \langle E_{i,j} | E_{i,j} \rangle$. Similarly, if Alice sends $|\widetilde{i}\rangle$ Bob will measure $|\widetilde{j}\rangle$ with probability $\widetilde{P}(j|i) = \langle \widetilde{E_{i,j}} | \widetilde{E_{i,j}} \rangle$.

[†]see definition A.1

We are now prepared to compute the probability that there are no errors in the MUB:

$$\begin{aligned} P_0 &\equiv \sum_i p(i)\widetilde{P}(i|i) \\ &= \frac{1}{D}\sum_i \langle\widetilde{E_{i,i}}|\widetilde{E_{i,i}}\rangle \\ &= \frac{1}{D}\sum_i \sum_{k,l,k',l'} H^*_{li}H_{ki}H_{l'i}H^*_{k'i}\langle E_{l,k}|E_{l',k'}\rangle \\ &= \frac{1}{D}\sum_{k,l,k',l'} \langle E_{l,k}|E_{l',k'}\rangle \sum_i H^*_{li}H_{ki}H_{l'i}H^*_{k'i} \end{aligned} \tag{2}$$

When Eve's states are considered without Bob, her state will look like $\rho_i = \sum_j |E_{i,j}\rangle\langle E_{i,j}|$. Now we will define a purification for Eve's states that will allow us to compute a bound on $P_0$. We assume that Eve holds

$$|\phi_i\rangle \equiv \sum_j |E_{i,j}\rangle_1 |\psi^i_j\rangle_2 \tag{3}$$

where $|\psi^i_j\rangle$ is an orthonormal basis for each choice of $i$. Due to the orthonormality of $|\psi^i_j\rangle$, $|\phi_i\rangle$ is a purification of $\rho_i$ because $Tr_2|\phi_i\rangle\langle\phi_i| = \rho_i$. We also define the generalized Hadamard transform of these states:

$$|\widetilde{\phi_j}\rangle \equiv \sum_i H^*_{ij}|\phi_i\rangle \ . \tag{4}$$

The Hadamard transform is unitary, so see that $|\phi_i\rangle = \sum_j H_{ij}|\widetilde{\phi_j}\rangle$. It should be noted that our purification $|\phi_i\rangle$ for Eve's states is not orthonormal or normalized. In fact, this is a property of which we will make use in order to get a bound. We now calculate the norm of the $|\widetilde{\phi_0}\rangle$ and see that with the proper choice of $|\psi^i_j\rangle$ that it is proportional to the probability that there was no error, $P_0$:

$$\begin{aligned} \langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle &= \sum_{l,l'} H_{l0}H^*_{l'0}\langle\phi_l|\phi_{l'}\rangle \\ &= \sum_{l,l'}\sum_{k,k'} H_{l0}H^*_{l'0}\langle E_{l,k}|E_{l',k'}\rangle\langle\psi^l_k|\psi^{l'}_{k'}\rangle \end{aligned} \tag{5}$$

At this point we will parameterize $|\psi^l_k\rangle$:

$$|\psi^l_k\rangle = \sum_i \alpha_{lki}|i\rangle$$

with any choice of $\alpha_{lki}$ so long as $\langle\psi^l_{k'}|\psi^l_k\rangle = \delta_{k'k}$. In order to match equation 2 with equation 5, we choose

$$\alpha_{lki} = \frac{H_{li}H^*_{ki}}{H^*_{l0}} \ . \tag{6}$$

To see that our choice of $\alpha_{lki}$ is valid, recall that $|H_{ij}|^2 = 1/D$ and simply compute

$$\langle\psi^l_{k'}|\psi^l_k\rangle = \sum_i \alpha^*_{lk'i}\alpha_{lki}$$

$$
\begin{aligned}
&= \frac{1}{|H_{l0}|^2}\sum_i |H_{li}|^2 H_{k'i}H^*_{ki} \\
&= \sum_i H_{k'i}H^*_{ki} \\
&= \delta_{k'k}
\end{aligned}
$$

which is what we need to show to make equation 3 a valid purification. With the above choice, equation 5 becomes

$$
\begin{aligned}
\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle &= \sum_{l,l'}\sum_{k,k'} H^*_{l0}H_{l'0}\langle E_{l,k}|E_{l',k'}\rangle\langle\psi^l_k|\psi^{l'}_{k'}\rangle \\
&= \sum_{k,l,k',l'}\langle E_{l,k}|E_{l',k'}\rangle\sum_i H^*_{li}H_{ki}H_{l'i}H^*_{k'i} \\
&= DP_0\ .
\end{aligned}
$$

Thus we have related the norm of $|\widetilde{\phi_0}\rangle$ to the probability that there are no errors [‡]in the MUB.

Define ${\rho_i}' \equiv |\phi_i\rangle\langle\phi_i|$ and $\rho' \equiv \frac{1}{D}\sum_i \rho_i$. Now we compute $\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle$:

$$
\begin{aligned}
\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle &= \sum_i \frac{1}{D}|\langle\widetilde{\phi_0}|\phi_i\rangle|^2 \\
&= \sum_i \frac{1}{D}|\langle\widetilde{\phi_0}|\sum_j H_{ij}|\widetilde{\phi_j}\rangle|^2
\end{aligned}
$$

Since $|H^*_{ik}|^2 D = 1$, we can rewrite the above as:

$$
\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle = D\sum_i \frac{1}{D}|H^*_{ik}\langle\widetilde{\phi_0}|\sum_j H_{ij}|\widetilde{\phi_j}\rangle|^2
$$

Since $f(x) = |x|^2$ is convex, then $|\sum_i p_i x_i|^2 \le \sum_i p_i|x_i|^2$.

$$
\begin{aligned}
\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle &= D\sum_i \frac{1}{D}|H^*_{ik}\langle\widetilde{\phi_0}|\sum_j H_{ij}|\widetilde{\phi_j}\rangle|^2 \\
&\ge D|\sum_i \frac{1}{D}H^*_{ik}\langle\widetilde{\phi_0}|\sum_j H_{ij}|\widetilde{\phi_j}\rangle|^2 \\
&= D|\frac{1}{D}\langle\widetilde{\phi_0}|\sum_j\sum_i H^*_{ik}H_{ij}|\widetilde{\phi_j}\rangle|^2 \\
&= D|\frac{1}{D}\langle\widetilde{\phi_0}|\sum_j \delta_{kj}|\widetilde{\phi_j}\rangle|^2 \\
&= D|\frac{1}{D}\langle\widetilde{\phi_0}|\widetilde{\phi_k}\rangle|^2 \\
&= \frac{1}{D}|\langle\widetilde{\phi_0}|\widetilde{\phi_k}\rangle|^2
\end{aligned}
$$

[‡]If the Hadamard transform is isomorphic to a group such that $H_{ik}H_{jk} = H_{i+j,k}\frac{1}{\sqrt{D}}$ and $H_{ik}H^*_{jk} = H_{i-j,k}\frac{1}{\sqrt{D}}$ we can show that the probability of an error $e$ in the Hadamard transformed basis (i.e. Alice sends $i$ but Bob receives $i+e$ averaged over all $i$), is $P_e = \langle\widetilde{\phi_e}|\widetilde{\phi_e}\rangle/D$. In this case, $|\psi^i_j\rangle = |\widetilde{i-j}\rangle$. Indeed, this is the case for the standard Sylvester type Hadamard matrices.

We can set $k$ to any value we like, in particular $k = 0$. We have previously shown that $\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle = DP_0$, putting this together:

$$\begin{aligned}
\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle &\geq \frac{1}{D}|\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle|^2 \\
&= \langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle P_0 \\
\frac{\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} &\geq P_0
\end{aligned}$$

We are now ready to prove the theorem. Since $Tr_2(\rho_i') = \rho_i$ and $Tr_2(\rho') = \rho$ we may apply lemma A.6. We will see that we may introduce an intermediate pure state to make the bounding of the information easier. The pure state we will use is $\frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}$. Starting with corollary 1:

$$\begin{aligned}
I(A;E) &\leq \log D \sum_i \frac{1}{D}|\rho_i - \rho| \\
&\leq \log D \sum_i \frac{1}{D}|\rho_i{}' - \rho'| \\
&= \log D \sum_i \frac{1}{D}|\rho_i{}' - \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} + \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} - \rho'| \\
&\leq \log D \sum_i \frac{1}{D}(|\rho_i{}' - \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}| + |\frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} - \rho'|) \\
&\leq \log D \sum_i \frac{1}{D}\left(2\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho_i{}'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} + 2\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}}\right) \\
&= 2\log D\left(\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} + \sum_i \frac{1}{D}\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho_i{}'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}}\right) \\
&\leq 2\log D\left(\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} + \sqrt{1 - \frac{\langle\widetilde{\phi_0}|(\sum_i \frac{1}{D}\rho_i{}')|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}}\right) \\
&= 4\log D\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho'|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} \\
&\leq 4\log D\sqrt{1 - P_0}
\end{aligned}$$

Where $1 - P_0 = P_{\widetilde{e}}$ is the probability that there is an error in the MUB, which proves the theorem. ∎

The previous theorem is what gives security to quantum key distribution schemes; however, we have only shown that QKD schemes are secure if the errors caused in any MUB are extremely small. Using quantum coding based approaches[5], we believe it is possible to use the above theorem to get a simple unconditional security proof that applies in dimension $D$.

In the following section, we will apply these same techniques to show that Eve also cannot learn functions of messages.

## 4 Security of Functions of Messages

According to theorem 1, if the fidelity Bob would have had in any MUB is exponentially close to unity, then Eve's information is exponentially low about which of the basis vectors in the chosen basis was sent. We will refer to the identifier of the basis vector sent by Alice as the *key*, and *Alice can use the key to encrypt a classical message*. For example, after sending a basis vector $|k\rangle$ to Bob, Alice could publicly announce she sent basis vector $|k \oplus m\rangle$, where $\oplus$ is the bitwise exclusive or (XOR) operation. Bob could then recover the encrypted message $m$.

The above mentioned information vs. disturbance result does not address the question of what information Eve might get about a *function* of a message encrypted with that key. Suppose Eve only wants to know if the message has a particular value, i.e., she wants to learn the indicator function: $f(m) = 1$ if $m = m_1$, else $f(m) = 0$. This function only has exponentially little information about the message itself. To see this, suppose each of $d$ messages are equally likely, then

$$\begin{aligned} H(M) &= \log d \\ H(f(M)) &= \frac{1}{d}\log d - (1-\frac{1}{d})\log(1-\frac{1}{d}) \\ H(f(M)|M) &= 0 \\ I(f(M);M) &= H(f(M)) \ . \end{aligned}$$

If $d$ is large, then $H(f(M)) \approx \frac{1}{d}\log d$, but, $d = 2^{H(M)}$, so $H(f(M)) \approx 2^{-H(M)}H(M)$. Hence, in this case, Eve only has to learn exponentially little information. Since QKD security proofs[2, 3, 4, 5, 6] only give exponentially strong security, it is not clear a priori that QKD will be sufficient to prevent Eve from learning any function of the message.

The next theorem will show that Eve must cause errors to *learn any function of the message*, even if it has exponentially little information with the message itself[§].

Throughout this section we work with some group operator + and all operations are in that group. In dimension $2^n$ the + operator will usually be bitwise exclusive or (XOR).

**Theorem 2** *Alice sends the $D$ dimensional state $|k\rangle$ to Bob, with $k$ chosen uniformly at random, and after Bob has received the state Alice announces $a = m + k$ (represented by the random variable $A$). Denote $f(M)$ as the function $f$ of the random variable $M$, and $f(K)$ is the function $f$ of the random variable $K$. The information Eve can get about any function of $m$, $f(m)$, is bounded by the square root of the probability that Eve would have caused errors in any MUB:*

$$I(f(M);E|A) \leq H(f(K))4\sqrt{P_e^{\sim}}$$

**P**roof.This proof will follow closely the proof of theorem 1 and use the same tools. If $a = m+k$,

[§]It should be noted that this result is *not* true for the key itself. If Eve only wants to learn if the key was a particular value $k_0$, she may do so without disturbing the state very much

then $f(m) = f(a-k)$. The state consistent with a function value $i$ is:

$$\sigma_i{}^a \equiv \frac{1}{q_i} \sum_{k:f(a-k)=i} p_k \rho_k$$

with $q_i \equiv \sum_{k:f(a-k)=i} p_k$. Note that since $p_k = \frac{1}{d}$, then the probability of an announcement $a = m + k$ is also $\frac{1}{d}$. As such, $q_i$ does not depend on $m$ and is only related to the number of inputs to the function $f$ which have a given output. The averaged state is:

$$\begin{aligned} \sigma^a &\equiv \sum_i q_i \sigma_i{}^a \\ &= \sum_i \sum_{k:f(a-k)=i} p_k \rho_k \end{aligned}$$

Since each input has one and only one output and $p_k = \frac{1}{d}$:

$$\sigma^a = \sum_k \frac{1}{d} \rho_k = \rho$$

The definition of mutual information[18] means that:

$$I(f(M); E|A) = \sum_a p_a I(f(M); E|A = a)$$

Using lemma 3

$$\begin{aligned} &\sum_a p_a I(f(M); E|A = a) \\ &\leq -\sum_a p_a \sum_i q_i \log q_i |\sigma_i{}^a - \sigma^a| \\ &= -\sum_i q_i \log q_i \sum_a p_a |\sigma_i{}^a - \rho| \\ &= -\sum_i q_i \log q_i \sum_a p_a |\sigma_i{}^a - \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} + \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} - \rho| \\ &\leq -\sum_i q_i \log q_i \sum_a p_a \left( |\sigma_i{}^a - \frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}| + |\frac{|\widetilde{\phi_0}\rangle\langle\widetilde{\phi_0}|}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle} - \rho| \right) \\ &= -\sum_i q_i \log q_i \sum_a p_a \left( 2\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\sigma_i{}^a|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} + 2\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} \right) \\ &\leq -\sum_i q_i \log q_i \left( 2\sqrt{1 - \frac{\langle\widetilde{\phi_0}| \sum_a p_a \sigma_i{}^a |\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} + 2\sqrt{1 - \frac{\langle\widetilde{\phi_0}|\rho|\widetilde{\phi_0}\rangle}{\langle\widetilde{\phi_0}|\widetilde{\phi_0}\rangle}} \right) \end{aligned}$$

We can simplify the quantity $\sum_a p_a \sigma_i{}^a$ by remembering that $p_a = 1/d$ and $q_i$ is independent of $a$:

$$\sum_a \frac{1}{d} \sigma_i{}^a = \sum_a \frac{1}{d} \frac{\sum_{k:f(a-k)=i} \frac{1}{d} \rho_k}{q_i}$$

$$
\begin{aligned}
&= \frac{1}{q_i}\sum_a \frac{1}{d} \sum_{m:f(m)=i} \frac{1}{d}\rho_{a+m} \\
&= \frac{1}{q_i} \sum_{m:f(m)=i} \frac{1}{d}\sum_a \frac{1}{d}\rho_{a+m}
\end{aligned}
$$

In the last sum, we sum over all $a$ with equal weight; hence, the $m$ dependence disappears:

$$
\begin{aligned}
\sum_a \frac{1}{d}{\sigma_i}^a &= \frac{1}{q_i} \sum_{m:f(m)=i} \frac{1}{d}\sum_a \frac{1}{d}\rho_{a+m} \\
&= \frac{1}{q_i}(\sum_{m:f(m)=i} \frac{1}{d})\rho \\
&= \rho
\end{aligned}
$$

Putting this back into the information bound:

$$
\begin{aligned}
&\sum_a p_a I(f(M); E|A=a) \\
&\leq -\sum_i q_i \log q_i \left( 2\sqrt{1 - \frac{\widetilde{\langle\phi_0|} \sum_a p_a {\sigma_i}^a |\widetilde{\phi_0}\rangle}{\widetilde{\langle\phi_0}|\widetilde{\phi_0}\rangle}} + 2\sqrt{1 - \frac{\widetilde{\langle\phi_0|}\rho|\widetilde{\phi_0}\rangle}{\widetilde{\langle\phi_0}|\widetilde{\phi_0}\rangle}} \right) \\
&= -\sum_i q_i \log q_i (4\sqrt{1 - \frac{\widetilde{\langle\phi_0|}\rho|\widetilde{\phi_0}\rangle}{\widetilde{\langle\phi_0}|\widetilde{\phi_0}\rangle}}) \\
&= 4H(Q)\sqrt{1 - \frac{\widetilde{\langle\phi_0|}\rho|\widetilde{\phi_0}\rangle}{\widetilde{\langle\phi_0}|\widetilde{\phi_0}\rangle}} \\
&\leq H(f(K))4\sqrt{P_{\widetilde{e}}}
\end{aligned}
$$

Which proves the result. ∎

## 5 Concluding Remarks

By developing bounds on entropy, we are able to bound the amount of information that measurements can get from a quantum source. Modeling eavesdropping in quantum key distribution as a quantum source, we are able to bound information that an eavesdropper can get. Since this bound is a function of the errors that would be caused in any MUB, Alice and Bob can use their measurements to estimate this figure. Therefore, Alice and Bob can bound information that Eve has about the information they share. In addition to showing security of such information, we show that any function of messages encrypted with this secret information is secure. This is a very strong statement about the robustness of quantum security.

## References


1. Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

2. Dominic Mayers. Quantum key distribution and string oblivious transfer in noisy channel. In *Advances in cryptology - CRYPTO'96*, LNCS 1109, pages 343–357. Springer-Verlag, 1996.
3. Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.
4. E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution. In *Proceedings of the 32'nd Ann. ACM Symposium on the Theory of Computing (STOC'00)*, pages 715–724. ACM Press, 2000. quant-ph/9912053.
5. Peter W. Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical Review Letters*, 85:441–444, 2000. quant-ph/0003004.
6. D. Gottesman and H. K. Lo. Proof of security of quantum key distribution with two-way classical communications. *IEEE Trans. Info. Theory*, 49:457–475, 2003. quant-ph/0105121.
7. C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, May 1999. quant-ph/9712042.
8. P. O. Boykin. *Information Security and Quantum Mechanics*. PhD thesis, University of California, Los Angeles, 2002. quant-ph/0210194.
9. D. Bruss and C. Macchiavello. Optimal eavesdropping in cryptography with three-dimensional quantum states. *Physical Review Letters*, 88:127901, 2002. quant-ph/0106126.
10. J. C. Boileau, K. Tamaki, J. Batuwantudawe, and R. Laflamme. Unconditional security of three state quantum key distribution protocols. quant-ph/0408085, 2004.
11. Antonio Acin, Nicolas Gisin, and Valerio Scarani. Security bounds in quantum cryptography using d-level systems. *Quant. Inf. Comp.*, 3(6):563, 2003. quant-ph/0303009.
12. Hoi Fung Chau. Unconditionally secure key distribution in higher dimensions by depolarization. quant-ph/0405016, 2004.
13. I. D. Ivanovic. Geometrical description of quantum state determination. *Journal of Physics A*, 14(12):3241–3245, 1981.
14. S. Bandyopadhyay, P. O. Boykin, V. P. Roychowdhury, and F. Vatan. A new proof of the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2002. quant-ph/0103162.
15. M. Ben-Or, Michal Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. quant-ph/0409078, 2004.
16. Renato Renner and Robert Koenig. Universally composable privacy amplification against quantum adversaries. quant-ph/0403133.
17. A. S. Kholevo. Some estimates of the information transmitted by quantum communication channels. *Problems of Information Transmission*, 9, 1973.
18. Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. John Wiley and Sons, New York, 1991.
19. Asher Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academik Publishers, Dordrecht, 1993.

## Appendix A

### 6 Bound on Mutual Information for 1-bit Sources

Suppose there is a classical source $S$ which sends one of two signals; zero or one. Also suppose that $p_{s=1} \leq p_{s=0}$. Following [7], we first come up with a linear bound on $H(p)$:

**Lemma A.1** *For any concave function $H(p)$ with $H(0) = H(1) = 0$ and any $p' \leq 1/2$, $H(p) \geq H(p') - \frac{H(p')}{p'}|p - p'|$*

**P**roof.Consider two regions, $p \leq p'$ and $p > p'$. $H(p)$ is concave, which means that $H(\alpha x + (1-\alpha)y) \geq \alpha H(x) + (1-\alpha)H(y)$. Applying this with $x = p'$, $\alpha = p/p'$ and $y = 0$, we obtain: $H(p) \geq \frac{H(p')}{p'}p$, which is exactly what we need for $p \leq p'$. In the region $p > p'$ we want to show that $H(p) \geq H(p') - \frac{p-p'}{p'}H(p')$. Again using the concavity, set $y = p', x = 1$ and $\alpha = \frac{p-p'}{1-p'}$ We see then that

$$\begin{aligned} H(p) &= H(\frac{p - p' + p' - pp'}{1 - p'}) \\ &= H(\frac{p - p'}{1 - p'} + \frac{1 - p}{1 - p'}p') \\ &\geq \frac{p - p'}{1 - p'}H(1) + \frac{1 - p}{1 - p'}H(p') \\ &= \frac{1 - p}{1 - p'}H(p') \\ &= H(p') - \frac{p - p'}{1 - p'}H(p') \end{aligned}$$

Since $p' \leq 1/2$, this implies that $\frac{1}{1-p'} \leq 2 \leq \frac{1}{p'}$ and $\frac{-1}{1-p'} \geq \frac{-1}{p'}$. We know that $p > p'$ in this region, so $p - p'$ is positive, thus:

$$\begin{aligned} H(p) &\geq H(p') - \frac{p - p'}{1 - p'}H(p') \\ &\geq H(p') - \frac{p - p'}{p'}H(p') \end{aligned}$$

∎

**Lemma A.2** *The mutual information between the random variable $E$ and the random bit $S$ (with $p(s = 0) \geq p(s = 1)$) is bounded:*

$$I(E; S) \leq H(S)p(s = 0)\sum_e |p(e|s = 1) - p(e|s = 0)|$$

**P**roof.Using lemma A.1 as a bound on $H(S|E)$ with $p' = p(s = 1)$, we can obtain the bound on mutual information:

$$\begin{aligned} I(E; S) &= H(S) - H(S|E) \\ &= H(S) - \sum_e p_e H(S|E = e) \end{aligned}$$

$$
\begin{aligned}
&\leq H(S) - \sum_e p_e (H(p(s=1)) - \frac{H(S)}{p(s=1)} |p(s=1|e) - p(s=1)|) \\
&= H(S) \sum_e |p(e|s=1) - p(e)| \\
&= H(S) \sum_e |p(e|s=1) - (p(s=0)p(e|s=0) + p(s=1)p(e|s=1))| \\
&= H(S)p(s=0) \sum_e |p(e|s=1) - p(e|s=0)|
\end{aligned}
$$

∎

**Lemma A.3** *If a source $S$ outputs quantum states $\rho_0$ and $\rho_1$ with probabilities $p_0$ and $p_1$ with $p_0 \geq p_1$, then mutual information between this source and the output of any measuring device $E$ is bounded: $I(E;S) \leq H(S)p(s=0)Tr|\rho_0 - \rho_1|$*

**P**roof.The source sends two states, $\rho_0$ and $\rho_1$. Eve does some POVM[19] on them. The probability that Eve gets outcome $x$ for her measurement given an input $s$ is: $p(e|s) = Tr(E_e \rho_s)$. This gives:

$$
I(E;S) \leq H(S)p(s=0) \sum_e |Tr(E_e(\rho_0 - \rho_1))|
$$

Since $\rho_0 - \rho_1$ is Hermitian, we can diagonalize it as $\sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. Taking this and applying the facts that $E_e$ are positive semi-definite and $\sum_e E_e = I$, we get:

$$
\begin{aligned}
I(E;S) &\leq H(S)p(s=0) \sum_e |Tr(E_e(\rho_0 - \rho_1))| \\
&= H(S)p(s=0) \sum_e |Tr(E_e(\sum_i \lambda_i |\psi_i\rangle\langle\psi_i|))| \\
&= H(S)p(s=0) \sum_e |\sum_i \lambda_i \langle\psi_i|E_e|\psi_i\rangle| \\
&\leq H(S)p(s=0) \sum_e \sum_i |\lambda_i| \langle\psi_i|E_e|\psi_i\rangle \\
&= H(S)p(s=0) \sum_i |\lambda_i| \langle\psi_i| \sum_e E_e |\psi_i\rangle \\
&= H(S)p(s=0) \sum_i |\lambda_i| \\
&= H(S)p(s=0)Tr|\rho_0 - \rho_1|
\end{aligned}
$$

∎

**Corollary A.1** *If a source $S$ outputs quantum states $\rho_0$ and $\rho_1$, then mutual information between this source and the output of any measuring device $E$ is bounded: $I(E;S) \leq H(S)Tr|\rho_0 - \rho_1|$*

**P**roof.Consider two cases, the first where $p_0 \geq p_1$ and the second where $p_1 > p_0$. If $p_0 \geq p_1$, then using lemma A.3 we have that $I(E;S) \leq H(S)p(s=0)Tr|\rho_0 - \rho_1|$. Since $p(s=0) \leq 1$, we get the result. If $p_1 > p_0$ then relabel the $\rho_1$ as $\rho_0$ and vice versa. Hence in the original

labeling, lemma A.3 becomes

$$I(E;S) \leq H(S)p(s=1)Tr|\rho_1 - \rho_0|$$

, and since $p(s=0) \leq 1$ we get the result. ∎

## 7 Bounding the Trace Norm

As we have seen in the previous section, the trace norm distance between quantum states is a powerful tool for bounding mutual information. Now we look at some bounds on trace norm distances.

**Lemma A.4** *The trace norm distance between two pure states is:*

$$||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|| = 2\sqrt{1 - |\langle\psi|\phi\rangle|^2}$$

**P**roof.Define $\langle\psi|\phi\rangle = \alpha$. Defining a new orthonormal basis we can write:

$$\begin{aligned} |e_0\rangle &\equiv |\psi\rangle \\ |e_1\rangle &\equiv \frac{1}{\sqrt{1-|\alpha|^2}}(|\phi\rangle - \alpha|\psi\rangle) \end{aligned}$$

Inverting these equations we have:

$$\begin{aligned} |\psi\rangle &= |e_0\rangle \\ |\phi\rangle &= \alpha|e_0\rangle + \sqrt{1-|\alpha|^2}|e_1\rangle \end{aligned}$$

Using this new basis, we find that:

$$\begin{aligned} ||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|| &= |(1-|\alpha|^2)|e_0\rangle\langle e_0| - (1-|\alpha|^2)|e_1\rangle\langle e_1| \\ &\quad -\sqrt{1-|\alpha|^2}(\alpha^*|e_1\rangle\langle e_0| + \alpha|e_0\rangle\langle e_1|)| \end{aligned}$$

This is just a $2 \times 2$ matrix and we can compute the trace norm by taking the absolute value of the eigenvalues, which are:

$$\lambda = \stackrel{+}{-}\sqrt{1-|\alpha|^2}$$

∎

**Lemma A.5** *The trace norm distance between any state and any pure state is bounded:*

$$|\rho - |\psi\rangle\langle\psi|| \leq 2\sqrt{1 - \langle\psi|\rho|\psi\rangle}$$

**P**roof.Let $\rho = \sum_i p_i|\phi_i\rangle\langle\phi_i|$ and apply $\sum_i p_i x_i \leq \sqrt{\sum_i p_i {x_i}^2}$:

$$\begin{aligned} |\rho - |\psi\rangle\langle\psi|| &= |\sum_i p_i|\phi_i\rangle\langle\phi_i| - |\psi\rangle\langle\psi|| \\ &\leq \sum_i p_i||\phi_i\rangle\langle\phi_i| - |\psi\rangle\langle\psi|| \\ &= \sum_i p_i\sqrt{1-|\langle\psi|\phi_i\rangle|^2} \\ &\leq \sqrt{\sum_i p_i(1-|\langle\psi|\phi_i\rangle|^2)} \\ &= 2\sqrt{1-\langle\psi|\rho|\psi\rangle} \end{aligned}$$

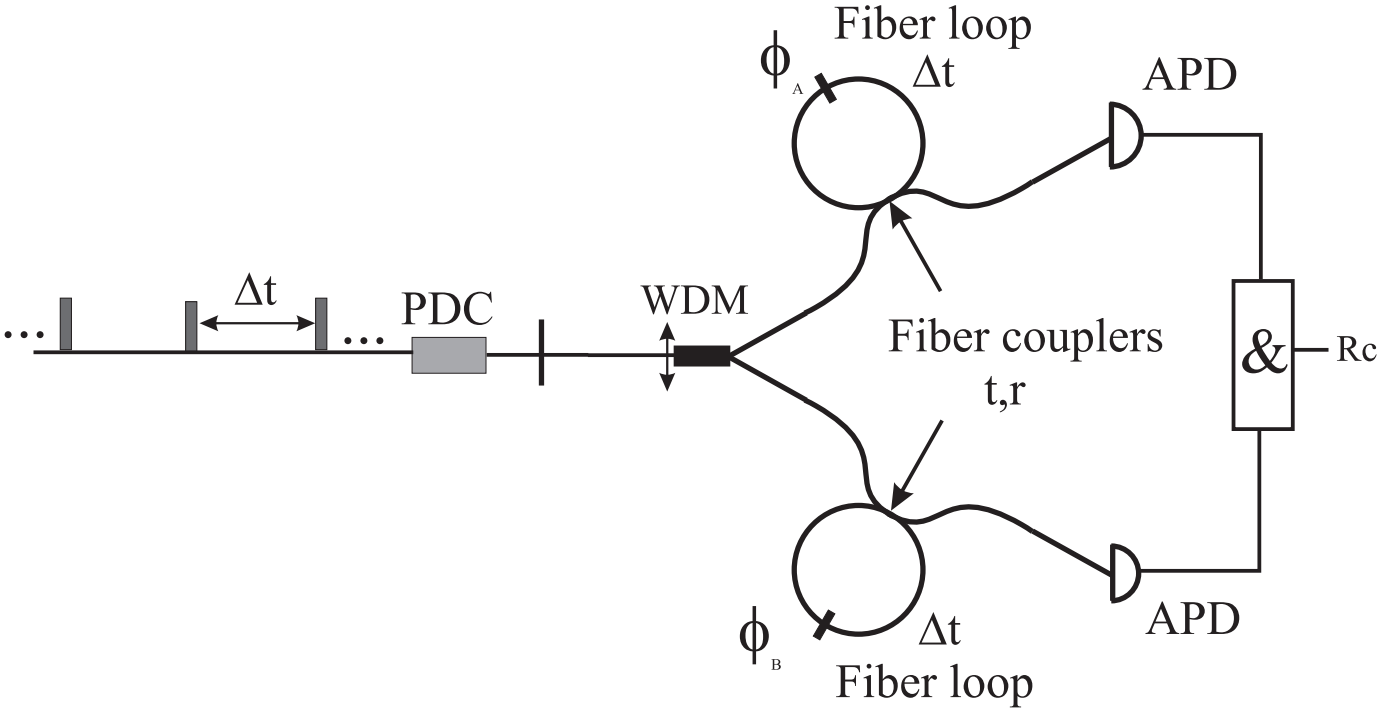
**Definition A.1** *Purification of $\rho$: any pure state $|\psi\rangle$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ such that $Tr_2(|\psi\rangle\langle\psi|) = \rho$*

**Lemma A.6** *The trace norm distance is reduced by partial trace:*

$$|\rho' - \sigma'| \quad \leq \quad |\rho - \sigma|$$

*Where $\rho$ and $\sigma$ are density matrices over states in $\mathcal{H}_1 \otimes \mathcal{H}_2$ and the partial trace is over one of the subsystems: $\rho' = Tr_2(\rho)$ and $\sigma' = Tr_2(\sigma)$.*

**P**roof.See [19].


Fiber loop
$\phi_A$
Δt
APD
Δt
PDC
WDM
Fiber couplers
t,r
&
Rc
$\phi_B$
Δt
Fiber loop
APD