Finite Key analysis of Semi Quantum Key Distribution

1st Calvin Roth
Department of Computer Science
University of Minnesota
Minneapolis, United States
rothx195@umn.edu

2nd Dr. Walter Krawec
Computer Science and Engineering Department
University of Connecticut
Storrs, United States
walter.krawec@uconn.edu

***Abstract*—An important problem in bounding the security and limitations of Semi Quantum Key distribution protocols is the Key Rate and the case of a finite key has not properly been studied now. The Key rate determines the worst case ratio of qubits sent to length of our final key that is still secure. A low key rate means our protocol would be fragile to noisy environments and more limited in terms of when it can be used. We found the key rate of a known semi quantum key distribution protocol to be 11% and 7.9 % under two different set of environments. Later we will use these techniques to analyze the finite key case as opposed to the asymptotic case.**

I. Introduction

In this work, we find the key rate of multiple quantum and semi quantum key distribution(SQKD) protocols by using mismatch statistics. In particular, we will find the key rate of the SQKD protocol in the concrete case. In the quantum and semi quantum setting of this problem we assume the two parties Alice and Bob have previously established a authenticated classical channel in addition to a quantum channel they can use. We make very modest restrictions on Eve namely, that she follow the laws of physics. These are much easier assumptions to satisfy than what is needed to securely share a key classically. In addition, as quantum computers are steadily getting better and cheaper as well increasing demands for security the relevance of this work will also increase.

The semi quantum protocol suggested by Boyer et. al [2] is the protocol that we will study closely. This protocol has the advantage over previously well studied protocols due to it being a semi quantum protocol which means only Alice needs a quantum computer; Bob gets by with only a classical computer. We will find the key rate of this protocol protocol by using mismatch statistics to bound the information that Eve has. A mismatch is when Alice sends something and different errors occur throughout the protocol. These statistics are the probabilities of these certain actions occurring.

The concrete case that we are studying is harder to consider than the previously considered asymptotic case. In the asymptotic case we consider the key rate as the number of qubits goes to infinity. This is a nice relaxation of the problem and it simplifies a lot of the math needed to mdoel the interactions for deriving the key rate. This is because certain factors such as error correction are perfect and costs and arbitrarily small fraction of the bits sent in the asymptotic case. But needing to send infinite bits isn't very practical. In the concrete case, we can't send an unlimited number of bits but instead are capped at sending a finite amount of bits on the order of 10^8 bits. This complicates the math as we well show in the results but is more realistic.

The other contribution of this paper is in re demonstrating the usefulness of mismatch statistics to derive the key rate. Mismatch statistics have been shown to be a good tool in the asymptotic case already by Krawec [4]. But they have not be fully utilized in the concrete case we are considering. This combination of studying the concrete case of semi quantum distribution protocols is what makes this work stand out as an important extension of previous work

The remainder of this paper is structured as follows. First, we will discover relevant background info on semi quantum key distribution as well as related works. Then we will move into the techniques that this work uses to obtain our results. Finally we will discuss the results.

II. Related Works

There have been multiple papers that have explored the uses of mismatched statistics in bounding the key rate, in 1990 Boyer et. al [1] which explored attacks where Eve intercepted and resent and Krawec [4] where the semi-quantum key distribution protocol as well as a few other protocols were analyzed but only in the asymptotic manner whereas we are concerned with the concrete case. Renner et al. [5] and Winter [3] have both proven the important bound on the key rate that we use. The semi quantum key distribution protocol that we are studying was first described by Boyer et. al [2]. The paper we rely on to then we move to the finite case is Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way post processing by Scarani and Renner [6]. They combined results from probability theory from other works to get equations that will serve as useful tools for us. In their paper, aside from creating these tools they also analyzed the finite case of BB84.

Special thanks to the National Science Foundation for funding this research

III. Background

In a quantum key distribution protocol, two parties, Alice and Bob, wish to derive a shared secret key in the presence of an adversary, Eve. The assumptions that are needed to achieve information-theoretic security are very modest compared to what is needed to achieve the same security with classical computation. We allow Alice and Bob to have 2 channels, a quantum channel and an unecrypted but authenticated classical channel. As we will see shortly any attacks that Eve can do on the quantum channel will induce errors that are detectable by Alice and Bob. We allow Eve to be a very strong adversary with the only limitation being that her actions are limited by the laws of physics. She has as much computational power and memory as she wants including being capable quantum computation and sending her own qubits. In the semi quantum case, the focus of this paper, Alice can do quantum computation but Bob can not. In particular when given a qubit the operations that Bob can perform are limited to: measure it in a fixed basis, reflect the qubit unmeasured to Alice, send a qubit in his fixed basis. This is useful because with it only one part needs a full quantum computer. It should be pointed out that although not the focus of this paper, many of the techniques and underlying mathematics here transfer well to fully quantum protocols.

A quantum bit or qubit for short is the basic unit of information of quantum computing. Unlike classical bits which are deterministic qubits are probabilistic until measured. That if we have an unmeasured qubit originally encoded as a 0 there is a chance, which depends on how we measure it, that we will read a 1. We represent a qubit as 2d complex vector such as $|\psi\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ where $a, b \in \mathbb{C}^2$ and $|a|^2 + |b|^2 = 1$. The reason why $|a|^2, |b|^2$ should sum to 1 is these represent the probabilities of measuring a 1 or a 0. We can send a qubit in any orthonrmal basis we wish. There are two particularly important bases of $\mathbb{C}^2$ that we will talk about. First, the computational or Z basis:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

and the Hadamard or X basis:

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, |-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$

. These two basis can be converted to each other by noticing that $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle$ This notation of $|\cdot\rangle$ to represent a vector that we've been using is called a ket and we represent the conjugate transpose as a bra $\langle\cdot|$. This notation called bra-ket(a pun for bracket) is useful since it concisely allows us to write $\langle x||y\rangle$ to be the inner product of x and y and $|x\rangle\langle y|$ to be the outer product of x and y in notation that looks like their traditional forms. There is a third operation that we will mention is the tensor product $\otimes$. If $|x\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$ and C is any matrix then $|x\rangle \otimes C = \begin{bmatrix} aC \\ bC \end{bmatrix}$. Some properties of tensor products are useful to state. Let A,B,C be matrices and d be a scalar for the following properties.

1) Tensor products are associative: $A \otimes (B \otimes C) = (A \otimes B) \otimes C$.
2) They distribute over addition $A \otimes (B + C) = (A \otimes B) + (A \otimes C)$.
3) With respect to scalars the following relations hold $(dA) \otimes B = A \otimes (dB) = d(A \otimes B)$

We sometimes will write $|ab\rangle := |a\rangle \otimes |b\rangle$ which is a commonly used notation. Three qubits $|a\rangle, |b\rangle, |c\rangle$ also follow the fact that $\langle a||b\rangle|c\rangle = |c\rangle\langle a||b\rangle$ If we want to measure in a different basis than the basis that was prepared, mathematically we do a change of basis operation on $|\psi\rangle\langle\psi|$ to the basis we want to measure in. When we measure a qubit that was prepared in the basis we measure, for instance $|0\rangle$ in the Z basis, we will always measure that result correctly. For incorrect measurements in the wrong basis with respect to our 2 important bases take note that measuring an X basis qubit, say $|+\rangle$ will be measured a 0 with probability 0.5 and a 1 with probability 0.5.

We can use our bra ket notation to define density matrices. A density matrix represents the probabilities of measuring different outcomes an unknown quantum state. The density operator of $|\psi\rangle = |\psi\rangle\langle\psi|$. The terms along the diagonal represent the probability of that outcome and therefore the trace must be 1. An additional property is that all density operators are positive semi-definite. A positive semi-definite matrix A satisfies the properties that $i) A = A^t$ where t is conjugate transpose and $ii)$ all the eigenvalues of A are greater than or equal to zero.

The next thing to discuss is the partial trace which corresponds to 'forgetting' part of a quantum system. The partial trace of Y a system $Tr_y(X \otimes Y) = Tr(Y)X$ and can be defined as an operation

$$Tr_Y(X \otimes Y) = \sum_{a \in S} (I \otimes \langle a|)(X \otimes Y)(I \otimes |a\rangle)$$

where S is the set of states of system Y.

Measuring a qubit will make this probabilistic system collapse into the state we observed it in. Coupled with the no cloning theorem, a quantum mechanics theorem that shows it is impossible to copy a quantum state, is what put limitations on Eve's actions. Additionally, we model the ways we can change a density operator p as a class of operators called admissible operators. An admissible operator Φ is defined as

$$\Phi(p) = \sum_{i=0}^{k} A_i p A_i^t$$

such that the matrices $A_1 \cdots A_k$ satisfy:

$$\sum_{i=0}^{k} A_i A_i^t = I$$

where I is the identity matrix. These operators have the property that they preserve the trace of p which is what we what since the total probability of events should be invariant.

Entropy plays a large role in bounding the key rate of key distribution protocols. Entropy in computer science is a

measure of how much information is gained by observing certain events or how much disorder is in a system. The most important variants are Shannon entropy which for n events with the probability of observing event i denoted by p_i is defined as $H(p_1, p_2, \cdots, p_n) = -\sum_{i=1}^{n} p_i \log(p_i)$. As a short hand notation, when there are only two possible outcomes we denote $h(x) = H(x, 1-x)$. We also have von Neumann entropy $S(A)$ where A is a probability matrix. $S(A) = -Tr(A\log(A)) = -\sum_{i=1}^{n} \lambda_i \log(\lambda_i)$ where λ_i is the ith eigenvalue of the density matrix. The goal of this work is to find the key rate of certain protocols. Formally the key rate r is $\frac{l(N)}{N}$ where $l(N)$ is the length of the final key and N is the number of qubits sent in total by Alice. An important equation that helps us bound the key rate when Eve does collective attacks, she applies the same attack to each iteration of the protocol independently of previous iterations, the key is then $r = inf(S(A|E) - H(A|B))$ where $S(A|E)$ [5] [3] is the Von Neumann entropy of the Alice's density matrix conditioned on Eve's density matrix and $H(A|E)$ is the Shannon entropy of of Alice conditioned on Bob. For the most part in this domain finding $H(A|B)$ is easy and $S(A|E)$ is the difficult part. The The SQKD protocol central to this paper was first put forward by Boyer et al [2]. Assuming we want the pre-shorted key to be N bits this protocol consists of the following steps:

1) Alice sends $8n + \delta$ qubits to Bob each a random bit encoded in either the computational of Hadamard matrix randomly.
2) For each qubit Bob chooses either to measure it in the computational basis and send to Alice the qubit he observed or reflect the unmeasured qubit to Alice.
3) Alice measures all the qubits that she receives
4) Alice announces each qubits were in the Z basis and Bob announces which he choose to measure

We will find the key rate to the SQKD protocol described above using mismatched statistics. The actions that Eve can take can be modelled as a applying a unitary matrix to the state between her and Alice. WLOG, we can assume that Eve's memory is initialized to be in the state 0. Denote Eve's attack on the transmission from Alice to Bob as U_F and the transmission from Bob back to Alice as U_R. This operators can be modelled as the following:

$$U_F|0,0\rangle = |0e_0\rangle + |1e_1\rangle \tag{1}$$
$$U_F|1,0\rangle = |0e_2\rangle + |1e_3\rangle \tag{2}$$
$$U_R|i,e_j\rangle = |0e^0_{ij}\rangle + |1e^1_{ij}\rangle \tag{3}$$

Where the first component represents the transit qubit and the second is representative of some internal memory Eve is keeping.

Suppose that Bob chooses to measure and that Alice sent a random bit in the computational basis with probability $\frac{1}{2}$ each and Bob choices to measure. The resulting state after Bob's measurement but before Eve's reverse attack is

$$\begin{aligned}&\frac{1}{2}(|0\rangle\langle 0|_B \otimes (|0,e_0\rangle\langle 0,e_0|_{TE} + |0,e_2\rangle\langle 0,e_2|)_{TE}\\ &+\frac{1}{2}(|1\rangle\langle 1|_B \otimes (|1,e_1\rangle\langle 1,e_1|_{TE} + |1,e_3\rangle\langle 1,e_3|_{TE}))\end{aligned} \tag{4}$$

Bob then forwards this to back to Alice but along the way Eve attacks with her second matrix U_r to this state. Alice will get the following state:

$$\begin{aligned}&\frac{1}{2}(|0\rangle\langle 0|_{BA} \otimes (|0,e^0_{0,0}\rangle\langle 0,e^0_{0,0}| + |0,e^0_{0,2}\rangle\langle 0,e^0_{0,2}|)\\ &+\frac{1}{2}(|1\rangle\langle 1|_{BA} \otimes (|1,e^1_{1,1}\rangle\langle 1,e^1_{1,1}| + |1,e^1_{1,3}\rangle\langle 1,e^1_{1,3}|))\\ &+\frac{1}{2}|0,1\rangle\langle 0,1|_{BA} \otimes (|0,e^1_{0,2}\rangle\langle 0e^1_{0,2}||0e^1_{00}\rangle\langle 0e^1_{00}|)\\ &+\frac{1}{2}|1,0\rangle\langle 1,0|_{BA} \otimes (|1e^0_{1,1}\rangle\langle 1e^0_{1,1}||1e^0_{13}\rangle\langle 1e^0_{13}|)\end{aligned} \tag{5}$$

If we take the partial trace of A's part of the system we are left with

$$\begin{aligned}\rho_{BE} = &\frac{1}{2}(|0\rangle\langle 0|_B \otimes (|e^0_{00}\rangle\langle e^0_{00}| + |e^0_{02}\rangle\langle e^0_{02}|\\ &+ |e^1_{00}\rangle\langle e^1_{00}| + |e^1_{02}\rangle\langle e^1_{02}|)\\ &+ (|1\rangle\langle 1|_B \otimes (|e^1_{11}\rangle\langle e^1_{11}| + |e^0_{11}\rangle\langle e^0_{11}|\\ &+ |e^1_{13}\rangle\langle e^1_{13}| + |e^0_{13}\rangle\langle e^0_{13}|\end{aligned} \tag{6}$$

We can learn some of these parameters by observed error rates in the channel. Specifically, we can easily learn $\langle e_i||e_i\rangle$ and $\langle g^j_i||g^j_i\rangle$. As seen in Krawec [4] if we have a noise rate of Q_F in the forward channel and Q_R in the reverse we can determine the following inner products from channel statistics:

$$Q_R Q_F = \langle e^1_{02}||e^1_{02}\rangle = \langle e^1_{11}||e^1_{11}\rangle \tag{7}$$
$$(1-Q_R)Q_F = \langle e^0_{02}||e^0_{02}\rangle = \langle e^0_{11}||e^0_{11}\rangle \tag{8}$$
$$Q_R(1-Q_F) = \langle e^1_{00}||e^1_{00}\rangle = \langle e^0_{13}||e^0_{13}\rangle \tag{9}$$
$$(1-Q_R)(1-Q_F) = \langle e^0_{00}||e^0_{00}\rangle = \langle e^1_{13}||e^1_{13}\rangle \tag{10}$$

What we are missing to find the key rate is 'cross terms' of the form $\langle g^0_i||g^1_i\rangle$. We can get expressions for these values that depend on the previously found values by considering other probabilities. For instance, what is the probability of Alice measuring a $|+\rangle$ in the end of the protocol conditioned on if She originally sent a $|+\rangle$ and Bob measured a $|1\rangle$. Let us work through the probability of Alice measuring a 1 conditioned on Bob measuring a $|0\rangle$ and Alice initially sending $|+\rangle$:

1) Alice sends $|+\rangle$ to Bob
2) Bob receives $U_F|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle(|e_0\rangle + |e_2\rangle) + |1\rangle(|e_1\rangle + |e_3\rangle))$ and Bob measures a $|0\rangle$. The conditioned probability is $\frac{(|0\rangle(|e_0\rangle+|e_2\rangle)}{\sqrt{2p_{+0}}}$
3) Bob sends this back to Alice which after Eve applies U_R is $\frac{(|0\rangle(|e^0_{00}\rangle+|e^0_{02}\rangle)+|1\rangle(|e^1_{00}\rangle+|e^1_{02}\rangle}{\sqrt{2p_{+0}}}$
4) Alice measures a $|+\rangle$ with probability $\frac{1}{\sqrt{4p_{+0}}}^2(|e^0_{00}\rangle + |e^1_{00}\rangle + |e^0_{02}\rangle + |e^1_{02}\rangle)$
5) Simplification

$$\begin{aligned}&\frac{1}{4p_{+0}}(p_{0,0} + p_{10} + 2Re(\langle e^0_{00}||e^1_{00}\rangle\\ &+ \langle e^0_{02}||e^1_{02}\rangle + \langle e^0_{00}||e^1_{02}\rangle\\ &+ \langle e^1_{00}||e^0_{02}\rangle + \langle e^1_{00}||e^1_{02}\rangle + \langle e^0_{02}||e^1_{02}\rangle)\end{aligned} \tag{11}$$

Working through the similar problems we find the following:

$$p_{0,0,|+\rangle} = \frac{1}{2} + \frac{Re(\langle e^0_{00}||e^1_{00}\rangle}{p_{0,0}} \tag{12}$$

$$p_{0,1,|+\rangle} = \frac{1}{2} + \frac{Re(\langle e^0_{02}||e^1_{02}\rangle}{p_{1,0}} \tag{13}$$

$$p_{1,0,|+\rangle} = \frac{1}{2} + \frac{Re(\langle e^0_{11}||e^1_{11}\rangle}{p_{0,1}} \tag{14}$$

$$p_{1,1,|+\rangle} = \frac{1}{2} + \frac{Re(\langle e^0_{13}||e^1_{13}\rangle}{p_{1,1}} \tag{15}$$

In a similar manner, we consider the two cases where Alice sent and measures a $|+\rangle$ and Bob measured a $|0\rangle$,$p_{+,0,+}$, or Bob measured a $|1\rangle$, $p_{+,1,+}$. Suppose that Alice sends a 0 in the Z basis, Bob reflects, and Alice measures a +. Mathematically the state before Alice measures is

$$U_r U_f|0\rangle = U_r(|0e_0\rangle + |1e_1\rangle) \tag{16}$$

$$= |0e^0_{00}\rangle + |1e^1_{00}\rangle + |0e^0_{11}\rangle + |1e^1_{11}\rangle \tag{17}$$

The probability of Alice measuring a plus is

$$P_+ = M(|+\rangle(|e^0_{00}\rangle + |e^1_{00}\rangle + |e^0_{11}\rangle + |e^1_{11}\rangle) \tag{18}$$

$$= \langle e^0_{00}||e^0_{00}\rangle + \langle e^1_{00}||e^1_{00}\rangle + \langle e^0_{11}||e^0_{11}\rangle + \langle e^1_{11}||e^1_{11}\rangle + \tag{19}$$

$$2(\langle e^0_{00}||e^1_{00}\rangle + \langle e^0_{00}||e^0_{11}\rangle + \langle e^0_{00}||e^1_{11}\rangle + \tag{20}$$

$$\langle e^1_{00}||e^0_{11}\rangle + \langle e^1_{00}||e^1_{11}\rangle + \langle e^0_{11}||e^1_{11}\rangle) \tag{21}$$

$$= 1 + \langle e^0_{00}||e^0_{11}\rangle + \langle e^1_{00}||e^1_{11}\rangle \tag{22}$$

Where the last step is achieved by finding the probability Alice measures a minus when she initially sent and observing since both should occur with equal probability we can cancel out terms.

$$\begin{aligned} p_{+,0,+} &= \frac{1}{4p_{+0}}(p_{0,0} + p_{10} + 2Re(\langle e^0_{00}||e^1_{00}\rangle \\ &+ \langle e^0_{02}||e^1_{02}\rangle + \langle e^0_{00}||e^1_{02}\rangle \\ &+ \langle e^1_{00}||e^0_{02}\rangle + \langle e^1_{00}||e^1_{02}\rangle + \langle e^0_{02}||e^1_{02}\rangle) \\ p_{+,1,+} &= \frac{1}{4p_{+1}}(p_{11} + p_{01} + 2Re(\langle e^1_{11}||e^0_{13}\rangle \\ &+ \langle e^0_{11}||e^1_{11}\rangle + \langle e^0_{11}||e^0_{13}\rangle \\ &+ \langle e^0_{11}||e^1_{13}\rangle + \langle e^1_{11}||e^1_{13}\rangle + \langle e^0_{13}||e^1_{13}\rangle) \end{aligned} \tag{23}$$

The case to consider for our collection of values is when Bob reflects. When Bob reflects, it's as if he acted as an identity. We can rewrite the combined actions of Eve's forward attack, Bob's reflection, and Eve's reverse attack on a state $|\phi\rangle$ as $U_R I U_F|\phi\rangle = U_R U_F|\phi\rangle$. Let us denote the combined operator $U_R U_F = V$. In particular V has the following affects:

$$V|0,0\rangle = |0g_0\rangle + |1g_1\rangle \tag{24}$$

$$V|1,0\rangle = |0g_2\rangle + |1g_3\rangle \tag{25}$$

Where the g_is is

$$g_0 = |e^0_{00}\rangle + |e^0_{11}\rangle \tag{26}$$

$$eq2 = |e^1_{00}\rangle + |e^1_{11}\rangle \tag{27}$$

$$eq3 = |e^0_{02}\rangle + |e^0_{13}\rangle \tag{28}$$

$$eq4 = |e^1_{02}\rangle + |e^1_{13}\rangle \tag{29}$$

Using results from Krawec [4] we get that

$$Q_A = \frac{1}{2}(1 - Re(\langle g_0||g_3\rangle + \langle g_1||g_2\rangle + \langle g_0||g_1\rangle + \langle g_2||g_3\rangle) \tag{30}$$

With a noise level of Q we are now ready to get our bound from entropy $S(A|E)$ as:

$$\begin{aligned} S(A|E) \geq (1-Q)^2(1-h(\lambda_1)) + Q(1-Q)(1-h(\lambda_2)) + \\ Q(1-Q)(1-h(\lambda_2)) + Q^2(1-h(\lambda_{(4)}))) \end{aligned} \tag{31}$$

where

$$\lambda_1 = \frac{1}{2} + \frac{\langle e^0_{00}||e^1_{13}\rangle}{2(1-Q)^2} \tag{32}$$

$$\lambda_2 = \frac{1}{2} + \frac{\langle e^1_{11}||e^0_{02}\rangle}{2Q(1-Q)} \tag{33}$$

$$\lambda_3 = \frac{1}{2} + \frac{\langle e^1_{00}||e^1_{13}\rangle}{2Q(1-Q)} \tag{34}$$

$$\lambda_4 = \frac{1}{2} + \frac{\langle e^0_{11}||e^1_{02}\rangle}{2Q^2} \tag{35}$$

$$\tag{36}$$

A. The Finite Case

We are now ready to step into the finite case of the semi quantum protocol. Why does this add so much complexity to our analysis of the optimal key rate we can achieve. The reason why this is complicated is to estimate parameters needed in our equations for the key rate, we need to observe the probabilities of 16 different parameters such as the probability that if Alice sent a $|0\rangle$ and Bob measures a $|1\rangle$ Alice remeasures a $|0\rangle$. But we do this by having both parties announce in the public channel what Alice sent originally and measured as well as what Bob measured for a subset of the total rounds. But because we have just revealed these rounds and therefore can't securely use them as part of our key. This adds a balancing act to our analysis: we want to sacrifice some rounds to get good estimation of parameters. Valerio and Renner [6] show how to properly apply statistics to Quantum key distribution protocols. The show their results by analyzing BB84. We will rewrite our statistics that are now imperfectly measured in terms of Q, p_{ij}, p_{ij^k} and p_{iRj}. We also potentially can bound $|\langle e^k_{ij}||e^n_{lm}\rangle|^2 \leq \langle e^k_{ij}||e^k_{ij}\rangle\langle e^n_{lm}||e^n_{lm}\rangle$ via the Cauchy Schwartz inequality. Yet another factor that we will now have to consider in the finite case is bits sacrificed for error correction which like parameter estimation why also can't securely use as part of the key. In the asymptotic case, we didn't have to consider the amount of bits leaked because as N tends to infinity the percentage of bits used for error estimation is arbitrarily small. We will follow Renner's and

Valerio's notation and denote the probability that our protocol fails be ϵ and the number of leaked bits from error correction as $leak_{ec}$. They give us that if we have randomly observed a parameter m times then for any $\overline{\epsilon'} > 0$ the true value, $\lambda(\infty)$ and observed value, $\lambda(m)$, will have the relation that $|\lambda(\infty) - \lambda(m)| < \delta = \sqrt{\frac{2ln(\frac{1}{\epsilon'}+2ln(m+1))}{m}}$ except with probability $\overline{\epsilon'}$

So in our protocol we might observed each statistic anywhere in that range of values. But this brings up the issue that computationally continuous sampling of many independent variables at the same time becomes computationally infeasible. For instance sampling 16 variables independently and concurrently at 10 spots each leads to 10^{16} different optimization problems to solve to find what configuration is the worst case that we could experience as to bound our results. Instead, we conjecture that for each statistic there exists value on the boundary of the error region minimizes the key rate. If true, this leads to 2 options per statistic, +max-error and -max-error, for 2^{16} total considerations as opposed to $10^{16} \approx 2^{53}$ optimization problems to solve. This 2^{16}. Why would this be case. WHY INTUITIVELY WOULD THIS BE THE CASE. Experimentally, we have manually sampled $\binom{16}{1}$ and $\binom{16}{2}$ with constant errors and the results suggest this could be the case. An additional piece of information we can get from numerical sampling is which boundary we should consider for each statistic. For each statistic this is known, the amount of computation is reduced by a factor of 2. This isn't sufficient to prove definitively that optimal values occur on the boundary but it's a good indication. More algebraic as opposed to computational means of verifying this claim will be necessary in future work though. It is currently unclear if algebraic methods will reveal what boundary to select.

IV. Results

There are 4 variables in this system $\langle e^0_{00}||e^1_{13}\rangle, \langle e^1_{11}||e^0_{02}\rangle, \langle e^1_{00}||e^1_{13}\rangle, \langle e^0_{11}||e^1_{02}\rangle$ subject to the constraints of equation 31 and via the Cauchy Schwartz inequality:

$$\langle e^c_{ab}||e^c_{ab}\rangle \geq \langle e^c_{ab}||e^f_{de}\rangle \leq \langle e^f_{de}||e^f_{de}\rangle$$

The last parameter we have to assign before we optimize of the key rate is Q_A. There are 2 reasonable choices for these. First, we could make the assumption that it is the forward and backwards channel are independent in which case $Q_A = 2Q(1-Q)$. Alternatively, we could assume that are correlated in which case $Q_A = Q$. Under either choice of parameter we can solve this optimization problem for the best minimum of $S(A|E) - H(A|B) =$ key-rate. We get that with the independent assumption, this protocol can tolerate a maximum Q of at most 7.9% and in the the correlated case we can support $Q < 11\%$.

The results that we have gotten at this point are fundamentally re-obtained results from Krawec [4]. That said this is still an okay spot to be at this point because the techniques that will be used moving forward are very similar to what was done to get these results.

TABLE I
KEY RATES FOUND FOR SQKD PROTOCOL IN THE ASYMPTOTIC CASE WITHOUT ANY ERRORS IN THE STATISTICS

Q_A	Maximum Q
$Q_A = Q$	11%
$Q_A = 2Q(1-Q)$	7.9%

The best key-rate of the SQKD protocol found under two different assignments of Q_A

We tested numerically $\binom{16}{1}$ ajd $\binom{16}{2}$ ways to change the error on parameters from what they ideally should be. For each statistic we changed it could be altered additive by $\pm 0.4, \pm 0.3, \pm 0.2, \pm 0.1, 0$. Of course, we keep in mind that these are probabilities and therefore should be strictly in the range the range [0,1] so when we statistic with error would escape this range we bounded it by 0 or 1. For instance, with y as the ideal measurement and y' has our error bounded statistic and $y + 0.4 = 1.05$ then we run the simulation with $y' = 1.0$ because it makes physical sense. In addition, there are families of statistics that together should add to one such as p_{+0}, p_{+1}, the probability that Alice sends a $|+\rangle$ and Bob measures $|0\rangle$ or $|1\rangle$ respectively. In such cases we treat these statistics dependently and if one is given a positive error the other is given a matching negative error. There were 16 different statistics we need to consider which can be partitioned to 3 categories for clarity of explaining what these parameters represent. First is the group of the form p_{ij} which is the probability Alice sends i and Bob measures j which is always in the Z basis. These are $\{p_{+0}, p_{a1}, p_{00}, p_{01}, p_{10}, "p_{11}\}$. The second group is p_{ijk} where Alice sends i, Bob measures j, and Alice measures k. These are $\{p_{00+}, p_{01a}, p_{10+}, p_{11a}, p_{+0+}, p_{+1+}\}$. The finally group of statistics that we need to change is P_{iRj} where Alice sends i, Bob reflects, and Alice measures j. The stats we need from this set is $\{p_{0R0}, p_{0R1}, p_{1R0}, p_{1R1}$. We also considered have no access to certain groups. Specifically we considered 4 cases: We have measurements on all the statistics we want, we have no reflection statistics, we have not statistics of the form p_{ijX} where X indicates ALice measures in the X basis, and when we have neither. The cases we consider 2 from beings correlated or uncorrelated, 4 cases from the above access to, and the $\binom{16}{2} * 9 * 9$ different ways to set the parameters error comes to more than 70,000 optimization problems that need to be run. Without further optimization's to the code or parallelization, which I recommend, this is approaching the edge of what can be searched computationally. As one may suspect this leads to a mass of data to look at in a paper. Here we will highlight the key results from this analysis that one should take away but also mentioned the code and results will be available on github [1]. Running 1 trial of one setting takes 0.08 seconds but to run the whole set of all the trials we consider takes 7700 seconds. From these results we do observe that it is along the boundary of the error ranges is where the key rate is minimized.

[1] https://github.com/CalvinRoth/finiteKeyAnalysis

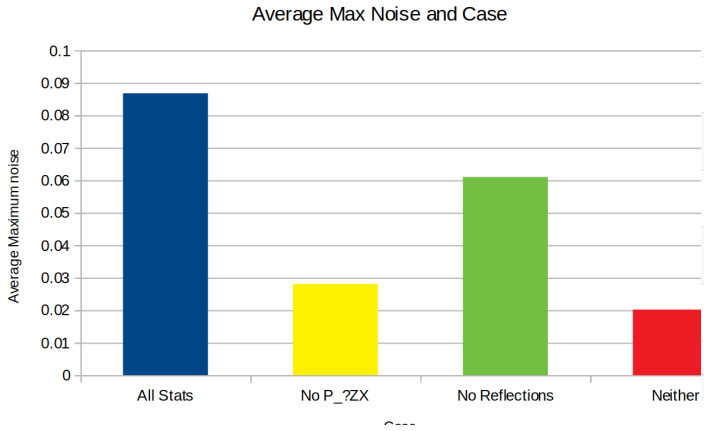

Fig. 1. Average allowed noise over all statistics changed for which of the 4 cases of access to various statistics we can haven

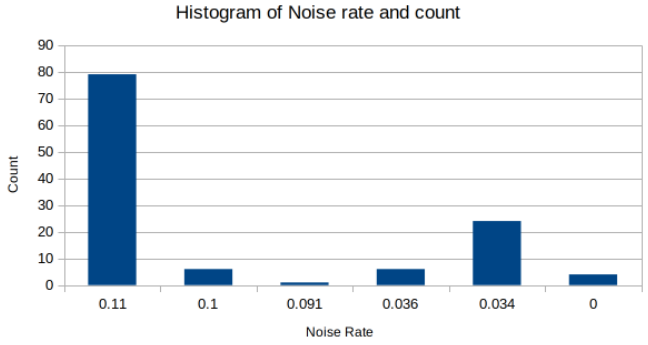

Fig. 2. A histogram of the allowed noised over the statistics in the case where we have access to all statistics

Statistic	All Statistics	No Reflection Statistics	No P_{?ZX}	Neither
p_{00}	Add	Add	Sub	Sub
p_{01}	Add	Add	Sub	Sub
p_{10}	Sub	Sub	Sub	Sub
p_{11}	Sub	Sub	Sub	Sub
p_{a0}	Sub	Sub	Sub	Sub
p_{a1}	Sub	Sub	Sub	Sub
p_{00a}	Sub	Sub	Sub	Sub
p_{10a}	Sub	Sub	Sub	Sub
p_{01a}	Sub	Sub	Sub	Sub
p_{11a}	Add	Add	Sub	Sub
p_{a0a}	Add	Add	Sub	Sub
p_{a1a}	Sub	Sub	Sub	Sub
p_{0R0}	Sub	Sub	Sub	Sub
p_{0R1}	Sub	Add	Sub	Add
p_{1R0}	Sub	Add	Sub	Add
p_{1R1}	Sub	Sub	Sub	Sub

Fig. 3. Table showing for each statistic for each of the 4 cases whether it is the negative or positive side of the confidence range that minimizes the allowed key rate

V. Discussion

We have suggestions for future work. As mentioned earlier, it seems prudent to consider what we can prove about the optimal errors not from sampling but from more general properties of this form of optimization problem. Ideally, we can also get from proving this via mathematics which boundary to pick for at least some statistics. In concern of speed of running tests, we suggest future work looks into more sophisticated optimization techniques that might reduce the run time vs sampling. We would also like to gather which statistics are the most important in terms of how they affect the key rate to obsserve and have the protocol have a bias to get tighter bounds on those and looser on others.

VI. Acknowledgment

This research was made possible through the funding provided by the National Science Foundation.

VII. Conclusion

In this work we have shown how mismatches statistics are utilized in Semi Quantum key distribution protocols to obtain good bounds for the key rate. Establishing these key rates in an important understanding the security and limitations of key distribution protocols. We have developed analysis of these protocols further by considering the finite case. Our results show that there is certainly a notably difference between what statistics are important to collect and have experimentally made a strong claim that it is at the boundaries of the confidence interval by testing this explicitly for changing all sets of

References

[1] Barnett, S. M., Huttner, B., and Phoenix, S. J. Eavesdropping strategies and rejected-data protocols in quantum cryptography. *Journal of Modern Optics 40*, 12 (1993), 2501–2513.

[2] Boyer, M., Kenigsberg, D., and Mor, T. Quantum key distribution with classical bob. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)* (2007), IEEE, pp. 10–10.

[3] Devetak, I., and Winter, A. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences 461*, 2053 (2005), 207–235.

[4] Krawec, W. O. Quantum key distribution with mismatched measurements over arbitrary channels. *arXiv preprint arXiv:1608.07728* (2016).

[5] Renner, R., Gisin, N., and Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A 72*, 1 (2005), 012332.

[6] SCARANI, V., AND RENNER, R. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters 100*, 20 (2008), 200501.