Optimisation of the two-state protocol

Zican Wang

***Abstract*—Quantum key distribution protocols requires post-processing works that alters the distributed keys for both parties. In this project we investigate the cause of the reduction of the key length and calculate the secret key rate of the two-state protocol as a function of the disturbance (channel noise) and the angle between the two states. The aim of the project is to find the optimal angle for each value of the disturbance. We will first look at the analysis of protocol for which we want to optimise. Related researches outlines a general area where the maximum disturbance tolerance lies, using this we can then maximize the key rate within a narrower range.**

I. Introduction

A. Overview

There are several phases that forms a quantum key distribution protocol, including the distribution phase, error correction phase and the privacy amplification phase[1]. The distribution phase works on transferring qubits as keys from one end to another while preventing any possibilities of an eavesdropper. This is often achieved by the sender having an basis that has some angle to the receiver's basis. The error correction makes sure both parties have the same key with minimal information leaked, while the privacy amplification phase alters the part of the key that might be leaked out during the first two phases. The last two phases often introduce dropping parts of the received keys for purposes such as estimating the success rate. This research focuses on finding a suitable expression for the final key length, optimizing the angle between two bases for each value of disturbance and looking for the relationship between the angle, disturbance and the final key rate. We would want the reduced length to be longer for the final key so that higher efficiency can be achieved. There are many different quantum key distribution protocols that are proposed since 1984[1], here we want to optimise for the two state protocol[2]. described in section III. We first look at the variables and constants that would affect the key rate in section III and try to find the optimal value for the highest key rate in section IV. The most general form of attack is simulated by using unitary gates and the disturbance is represented in terms of the coefficients of each element in the state vector, and we optimise according to the entropy value of the attacker for each disturbance. Constraints on the coefficients can be calculated from the disturbance and the unitary property so that we can optimise in a limited set of possible values.

B. Related work

One research shows that although the BB84 protocol and the two-state protocol are secure in terms of eavesdropping, the former protocol is more popular because it has a higher tolerance to channel noise(disturbance in later sections)[3]. They further proposed that considering a finite number of qubits transferred, the maximal tolerable depolarizing rate can be improved. They also recommended using software such as Mathematica to perform convex optimisation. Their results shows that the final key rate decreases almost linearly as the disturbance raises. A related research shows that the disturbance would be around 6% for the final key rate to be greater than zero[4].

Another report shows focuses on deriving expressions for key rates for the extended two-state protocol[5] where the key rates were generally higher than the previous paper with the same level of disturbance[3]. Their result also shows a slightly curved relationship between the disturbance and the key rate.

II. Mathematical preliminaries

A. Quantum measurements

In contrast to measurements in the classical physic world, where it does not have a noticeable effect on the object being measured, quantum measurements can change the state of the quantum particle or qubit[6].

In brief, the original state of some qubits can be superpositions – each string has a probability of being the measurement outcome, shown by the square of the corresponding element in the state vector. Thus, the probability of getting a string x (computational basis) when measuring ψ is calculated by $\langle x| \times |\psi\rangle$ or $\langle x|\psi\rangle$ in short. The state of those qubits after measuring collapses to the outcome we get with fix probability 1. This is often referred to as the measurement postulate or Born's rule.

For example, the state $|\psi\rangle = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}$, when being measured in the computational basis, has probability $(1/\sqrt{2})^2 = 50\%$ of getting the outcome 0 or 1. After the measurement, the state of ψ becomes 1 if the outcome is 1, and becomes 0 otherwise (Figure 1). Also note that $|\psi\rangle$ can be a linear combination of the two basis vectors, which infers that a state vector can be represented by a linear combination of the vectors in another non-orthogonal basis. Thus, linear combinations can be comprehended as superpositions and in this example, $|\psi\rangle$ is a superposition of 0(1,0) and 1(0,1). $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

From this, we can see that measuring a state using a basis non-orthogonal to the state's basis will give more than one possible outcome and result in a change of the state.

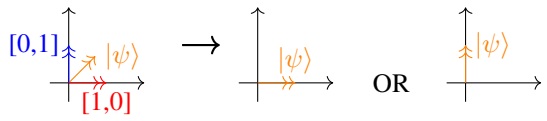


Fig. 1: measuring $|\psi\rangle$

B. Entropy

The Shannon entropy is used here to determine the uncertainty, measured in bits, one has regarding a set of strings X[7]. It is defined as:

$$H(X) = -\sum_{x \in X} p(x) \log_2(p(x)) \tag{1}$$

where p(x) is the probability distribution of each string x in the set X. Here we always use capital letters for sets and lowercase letters for elements in a set.

The binary entropy is defined as

$$h(p) = -p \log_2 p - (1-p) \log_2 (1-p) \tag{2}$$

C. Factors of disturbance

Both channel noise and the presence of an attack can introduce disturbance. In section IV we consider both of them as the most general interaction so that specific forms of attack or noise are included in consideration. We treat both the noise and the errors induced by an eavesdropped as a total disturbance D which will be derived in section III.

III. Description of the two-state protocol

The following protocol depends on the parameter θ, which is optimised in later sections.

A. Distribution phase

In each round $i \in \{1, 2, \ldots, N\}$ Alice and Bob perform the following two steps.

Preparation.

Alice generates a random number $x_i \in \{0, 1\}$ with probability $P(x_i) = 1/2$, then prepares the state:

$$|\varphi_{x_i}\rangle = \cos\theta\,|0\rangle + (-1)^{x_i} \sin\theta\,|1\rangle \ , \tag{3}$$

and sends it to Bob.

Measurement.

Bob generates a random number $y_i \in \{0, 1\}$ with probability $P(y_i) = 1/2$ and performs a measurement in the basis $\{|\varphi_{y_i}\rangle, |\bar{\varphi}_{y_i}\rangle\}$, where we define

$$|\bar{\varphi}_{y_i}\rangle = \sin\theta\,|0\rangle - (-1)^{y_i} \cos\theta\,|1\rangle \ . \tag{4}$$

- If the outcome is $|\bar{\varphi}_{y_i}\rangle$ then Bob's guess for x_i is $x'_i = 1 - y_i$.
- If the outcome is $|\varphi_{y_i}\rangle$ then Bob tells Alice to discard this round.

The generated data is (x_j, x'_j) for $j = 1, \ldots, N'$.

B. Estimation phase

Alice and Bob randomly select a subset $\mathcal{S} \subseteq \{1, \ldots, N'\}$ of size $|\mathcal{S}| = \lceil \sqrt{N'} \rceil$, publish the pairs (x_j, x'_j) in the subset $j \in \mathcal{S}$, and compute the relative frequency of errors

$$D = \frac{|\{j \in \mathcal{S} : x_j \neq x'_j\}|}{|\mathcal{S}|} \ , \tag{5}$$

also known as the *disturbance*. The raw key (x_k, x'_k) with $k \in \{1, \ldots, N_\mathrm{r}\}$ is obtained after discarding the items in $\mathcal{S}$.

C. Error correction phase[8]

Alice calculates the number

$$M = \lceil N_\mathrm{r}\, h(D) \rceil \ , \tag{6}$$

generates a random hash function
$f : \{0,1\}^{N_\mathrm{r}} \to \{0,1\}^M$,
and publishes f and $f(x_1, \ldots, x_{N_\mathrm{r}})$. Bob uses the information $(x'_1, \ldots, x'_{N_\mathrm{r}})$, the knowledge of f and $f(x_1, \ldots, x_{N_\mathrm{r}})$ to reconstruct $(x_1, \ldots, x_{N_\mathrm{r}})$.

D. Privacy amplification phase[9]

Alice calculates the number

$$N_\mathrm{k} = \lfloor N_\mathrm{r}\, H(X|E) - M \rfloor \ , \tag{7}$$

generates a random hash function $g : \{0,1\}^{N_\mathrm{r}} \to \{0,1\}^{N_\mathrm{k}}$ and publishes it. Both, Alice and Bob, generate the joint secret key by computing $(k_1, \ldots, k_{N_\mathrm{k}}) = g(x_1, \ldots, x_{N_\mathrm{r}})$.

IV. Calculation of $H(X|E)$

N_k would be our final secret key rate for this project. Thus the optimal value of N_k should be the maximum value for each angle. $H(X|E)$ will be affected by different factors in transmission. We assume in the calculation part, that $H(X|E)$ is the minimal value for each angle in order to calculate the minimal optimal key rate. This means that it is the worst case scenario and the key rate generated at the end of the project would be a lower bound to all the other possible key rates.

A. Bob's probability of accepting

For $y_i = 0$, we have the basis:
$\{\sin\theta\,|0\rangle - \cos\theta\,|1\rangle, \cos\theta\,|0\rangle + \sin\theta\,|1\rangle\}$, with the second one being the same as the state Alice prepares when $x_i = 0$ and not orthogonal to when $x_i = 0$ (figure 2). So Bob can be sure Alice prepares $x_i = 1$ when he gets the result $\sin\theta\,|0\rangle - \cos\theta\,|1\rangle$. Bob then only leave the ones he is sure about, by discarding the ones where he gets $|\varphi y_i\rangle$.Same for $y_i = 1$.

The generated data has length equal to the number of bits that is not discarded by Bob. This can be approximated by calculating the rate of Bob successfully getting $|\bar{\varphi}_{y_i}\rangle$

The probability of Bob getting accepting the bit is:

$$\frac{1}{4}\mathrm{prob}\{|\bar{\varphi}_0\rangle\,|x=1\} + \frac{1}{4}\mathrm{prob}\{|\bar{\varphi}_1\rangle\,|x=0\} \tag{8}$$

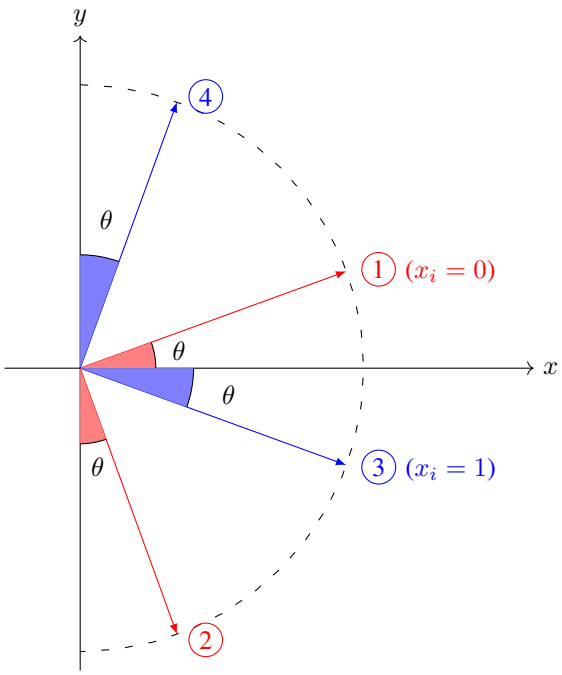


Fig. 2: state vectors, The red basis can only get 3 and the blue basis can only get 1.

y_i	$\|\varphi_{y_i}\rangle$	$\|\bar{\varphi}_{y_i}\rangle$
0	$\cos\theta\|0\rangle + \sin\theta\|1\rangle$ (1)	$\sin\theta\|0\rangle - \cos\theta\|1\rangle$ (2)
1	$\cos\theta\|0\rangle - \sin\theta\|1\rangle$ (3)	$\sin\theta\|0\rangle + \cos\theta\|1\rangle$ (4)

TABLE I: Bob's measuring basis according to y_i

where the fraction $\frac{1}{4}$ is the probability when Alice and Bob both choose the corresponding bit.

According to figure 2 and table I, the angle between x_i and $y_i = 1 - x_i$ is $\frac{\pi}{2} - 2\theta$, thus the probability of getting $|\bar{\varphi}_{y_i}\rangle$ for each pair of prepared state and measuring basis is $\cos^2(\frac{\pi}{2} - 2\theta)$. Bob has a probability of a half of getting the right basis that will produce a valid bit, so the overall rate is $\frac{1}{2}\cos^2(\frac{\pi}{2} - 2\theta)$.

Hence if there are no adversaries and the number of bits in the beginning is N, then afterwards Bob will have $N' = \frac{1}{2}\cos^2(\frac{\pi}{2} - 2\theta) \times N$ bits left.

B. With disturbance

Here we formalise the most general individual attack. In a given round of the protocol, Alice sends qubit B to Bob, in one of the states $|\varphi_x\rangle_B$ with $x \in \{0, 1\}$. Eve's attack is the following:

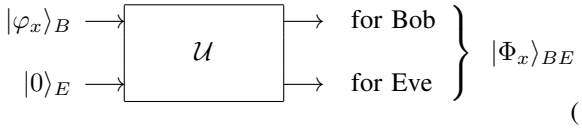
1) Intercept qubit B.
2) Engineer an interaction between systems B and E.
3) Send system B to Bob and keep E (which might be entangled to B).

Without loss of generality, system E is initially in a fixed pure state $|0\rangle_E \in \mathbb{C}^2$ and the interaction is unitary $\mathcal{U}$; since any mixed state and non-unitary interaction can be simulated from a unitarily evolving pure state by disposing part of the system E after the interaction.

We write this general interaction as

$$\mathcal{U}(|0\rangle_E \otimes |\varphi_x\rangle_B) = |\Phi_x\rangle_{EB} = \sum_{r,s=0}^{1} \Gamma_x^{r,s} |r\rangle_E |s\rangle_B \quad . \quad (9)$$

This is summarised in the following picture:



(10)

We only need to consider a two dimensional space because only the first two dimension interacts with Bob's state. With s being only two values, the equation can be simplified as:

$$\sum_{r,s=0}^{1} \Gamma_x^{r,s} |r\rangle_E |s\rangle_B = |0\rangle_B \sum_r \Gamma_x^{r,0} |r\rangle_E + |1\rangle_B \sum_r \Gamma_x^{r,1} |r\rangle_E \quad (11)$$

We also only consider Eve's state being $|0\rangle$ because the unitary function can be seen as a integration of two unitary functions, with the first one changing Eve's state from $|0\rangle$ to an arbitrary state and the second one acting on both Eve's and Bob's state as shown in figure .

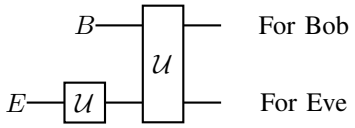


Fig. 3: Secondary unitary gate which can be integrated as one bigger unitary gate shown in gate 10.

Now with Eve's interaction, error will be introduced. Thus Bob may accept $|\bar{\varphi}_y\rangle$ as he believes that x will always be $1-y$ in this case. Bob and Alice now need to do error correction and Privacy amplification to ensure as little information lost as possible.

With Eve being involved in the bit transfer, the probability of Bob accepting the bit will also change.

$$\begin{aligned} \text{prob}\{\bar{\varphi}\} =& \frac{1}{4} \times \| \langle\bar{\varphi}_0|\Phi_0\rangle \|^2 + \frac{1}{4} \times \| \langle\bar{\varphi}_0|\Phi_1\rangle \|^2 + \\ & \frac{1}{4} \times \| \langle\bar{\varphi}_1|\Phi_0\rangle \|^2 + \frac{1}{4} \times \| \langle\bar{\varphi}_1|\Phi_1\rangle \|^2 \\ =& \frac{1}{4} \sum_{x,y} \| \langle\bar{\varphi}_y|\Phi_x\rangle \|^2 \end{aligned} \quad (12)$$

Bob and Alice will discard all the checking bits. The size of that is $|\mathcal{S}| = \lceil\sqrt{N'}\rceil$, then we have the number of bits left $N_r = N' - \sqrt{N'}$. However, as we are looking for key rates in percentage, the N_k in the later calculation would be normalized and so is N' and N_r. Thus the rate would be a function of $\frac{N'-\sqrt{N'}}{N}$ instead. Since $N' < N$, then

$\frac{\sqrt{N'}}{N} < \frac{\sqrt{N'}}{N'}$. With big quantity of N bits that Alice sends N_r reduces to 0 thus we ignore the negligible $\sqrt{N'}$ in the following process.

D is the rate of Bob getting a wrong outcome from Alice's actual preparation (given that Bob has already accepted the bit).

With no disturbances, Alice and Bob's scenarios can only be the "accept and correct" cells from table II. This is because Bob will always get $y = 1-x = x'$ when he measures $|\bar{\varphi}_y\rangle$ according to Figure 2. Hence no disturbance at all.

However, There are two more scenarios when there is some disturbance: when Alice chooses 1 $(x = 1)$ and Bob measured 1 $(y = 1, x' = 1 - y = 0)$ and the opposite.

The approximated disturbance is the probability of Bob getting the wrong state given that he already accepted the bit since he measures $|\bar{\varphi}_y\rangle$.

Let us define Eve's (normalised) conditional states $|\mu_{x',x}\rangle_E$ as

$$\sqrt{q(x'|x)}\,|\mu_{x',x}\rangle_E = {}_B\langle\bar{\varphi}_{1-x'}|\Phi_x\rangle_{EB} \ , \tag{13}$$

for $x', x \in \{0,1\}$, where $q(x'|x), x' = 1 - y$ is the probability of Bob measuring y when Alice actually prepares x.

With Alice choosing randomly, we can get the approximation of D:

$$\begin{aligned} D &= \frac{\text{prob}\{\textbf{accepted and correct}\}}{\text{prob}\{\textbf{accepted}\}} && (14)\\ &= \text{prob}\{x' = x|\bar{\varphi}\} && (15)\\ &= \frac{q(0|1) + q(1|0)}{q(0|0) + q(0|1) + q(1|0) + q(1|1)} && (16)\\ &= \frac{q(0|1) + q(1|0)}{\sum_{x',x} q(x'|x)} && (17) \end{aligned}$$

C. Components

In equation 13 and gate 10 shows the most general form of attack, which involves unitary gates. Unitary implies:

$$\langle\Phi_x\,|\Phi_x\rangle = 1 \ , \tag{18}$$

$$\langle\Phi_0\,|\Phi_1\rangle = \cos 2\theta \ . \tag{19}$$

$$|\Phi_x\rangle = \mathcal{U}(|0\rangle_E \otimes |\varphi_x\rangle_B) \tag{20}$$

So,

$$\begin{aligned} \langle\Phi_0|\Phi_1\rangle &= \left(\langle\varphi_0|_B \otimes \langle 0|_E\right)\mathcal{U}^\dagger\mathcal{U}(|0\rangle_E \otimes |\varphi_1\rangle_B) \\ &= \langle\varphi_0|_B\,|\varphi_1\rangle_B \\ &= \cos 2\theta \end{aligned} \tag{21}$$

$H(X|E)$ is given by:

$$H(X|E) = H(E|X) + H(X) - H(E) \tag{22}$$

Eve's state (density matrix) conditioned on Alice preparing $|\varphi_x\rangle$ and Bob accepting the bit is

$$\sigma_{E|x} = \frac{\frac{1}{2}\sum_{x'=0}^{1} q(x'|x)\,|\mu_{x',x}\rangle\langle\mu_{x',x}|}{\text{prob}\{\bar{\varphi}|x\}} \tag{23}$$

where $\text{prob}\{\bar{\varphi}|x\}$ is $\frac{1}{2}q(0|x) + \frac{1}{2}q(1|x)$ according to table II, and Eve's averaged state is

$$\sigma_E = \sum_{x=0}^{1} P(x)\,\sigma_{E|x} \ . \tag{24}$$

To derive $\sigma_{E|x}$ and σ_E we can first calculate the $q(x'|x)\,|\mu_{x',x}\rangle\langle\mu_{x',x}|$ for different values of x' and x.

$$\begin{aligned} &q(x'|x)\,|\mu_{x',x}\rangle\langle\mu_{x',x}| \\ &= \sqrt{q(x'|x)}\,|\mu_{x',x}\rangle\,\sqrt{q(x'|x)}\,\langle\mu_{x',x}| \\ &= \langle\bar{\varphi}_{1-x'}|\Phi_x\rangle\,\langle\Phi_x|\bar{\varphi}_{1-x'}\rangle \end{aligned} \tag{25}$$

According to table I and equation 9, we can get: for $x' = 0, x = 0$:

$$\begin{aligned} &\sqrt{q(0|0)}\,|\mu_{0,0}\rangle \\ &= \langle\bar{\varphi}_1|\Phi_0\rangle \\ &= (\sin\theta\,\langle 0| + \cos\theta\,\langle 1|)\left(\sum_{r,s=0}^{1}\Gamma_0^{r,s}\,|r\rangle_E\,|s\rangle_B\right) \\ &= \sin\theta\Gamma_0^{0,0}\,\langle 0|0\rangle_B\,|0\rangle_E + \sin\theta\Gamma_0^{1,0}\,\langle 0|0\rangle_B\,|1\rangle_E \\ &+ \cos\theta\Gamma_0^{0,1}\,\langle 1|1\rangle_B\,|0\rangle_E + \cos\theta\Gamma_0^{1,1}\,\langle 1|1\rangle_B\,|1\rangle_E \\ &= \left(\sin\theta\Gamma_0^{0,0} + \cos\theta\Gamma_0^{0,1}\right)|0\rangle_E \\ &+ \left(\sin\theta\Gamma_0^{1,0} + \cos\theta\Gamma_0^{1,1}\right)|1\rangle_E \\ &= \begin{pmatrix}\sin\theta\Gamma_0^{0,0} + \cos\theta\Gamma_0^{0,1} \\ \sin\theta\Gamma_0^{1,0} + \cos\theta\Gamma_0^{1,1}\end{pmatrix} \\ &= \begin{pmatrix}A_0 + B_0 \\ C_0 + D_0\end{pmatrix} \end{aligned} \tag{26}$$

For representation purposes, we let $A_x = \sin\theta\Gamma_x^{0,0}$, $B_x = \sin\theta\Gamma_x^{0,1}$, $C_x = \sin\theta\Gamma_x^{1,0}$, $D_x = \sin\theta\Gamma_x^{1,1}$.

$$q(0|0)\,|\mu_{0,0}\rangle\langle\mu_{0,0}| = \begin{pmatrix}(A_0 + B_0)^2 & \cdots \\ \cdots & (C_0 + D_0)^2\end{pmatrix} \tag{27}$$

Alice's basis	Bob's receiving basis			
	y = 0		y = 1	
	Bob's receiving state		Bob's receiving state	
	$\|\varphi_{y_0}\rangle$	$\|\bar{\varphi}_{y_0}\rangle$	$\|\varphi_{y_1}\rangle$	$\|\bar{\varphi}_{y_1}\rangle$
x = 0	reject	accepted but wrong	reject	accept and correct
x = 1	reject	accepted but correct	reject	accept but wrong

TABLE II: Bob's measured bits corresponding to Alice's and Bob's basis. Alice has an uniform distribution of choosing x, and so does Bob when choosing basis number y. Bob will not accept any bits when he gets the state $|\varphi_y\rangle$, and he will accept all bits with state $|\bar{\varphi}_y\rangle$. Notice that when Bob receives $|\bar{\varphi}_y\rangle$, he calculates the bit $x' = 1 - y$. Thus so when $y = x$, Bob will get the wrong state as what Alice has prepared.

for $x' = 1, x = 0$:

$$\begin{aligned}
&\sqrt{q(1|0)}\,|\mu_{1,0}\rangle \\
&= \langle\bar{\varphi}_0|\Phi_0\rangle \\
&= (\sin\theta\,\langle 0| - \cos\theta\,\langle 1|)\left(\sum_{r,s=0}^{1}\Gamma_0^{r,s}\,|r\rangle_E\,|s\rangle_B\right) \\
&= \sin\theta\Gamma_0^{0,0}\,\langle 0|0\rangle_B\,|0\rangle_E + \sin\theta\Gamma_0^{1,0}\,\langle 0|0\rangle_B\,|1\rangle_E \\
&- \cos\theta\Gamma_0^{0,1}\,\langle 1|1\rangle_B\,|0\rangle_E - \cos\theta\Gamma_0^{1,1}\,\langle 1|1\rangle_B\,|1\rangle_E \\
&= \left(\sin\theta\Gamma_0^{0,0} - \cos\theta\Gamma_0^{0,1}\right)|0\rangle_E \\
&+ \left(\sin\theta\Gamma_0^{1,0} - \cos\theta\Gamma_0^{1,1}\right)|1\rangle_E \\
&= \begin{pmatrix}\sin\theta\Gamma_0^{0,0} - \cos\theta\Gamma_0^{0,1}\\ \sin\theta\Gamma_0^{1,0} - \cos\theta\Gamma_0^{1,1}\end{pmatrix} \\
&= \begin{pmatrix}A_0 - B_0\\ C_0 - D_0\end{pmatrix}
\end{aligned} \tag{28}$$

$$q(1|0)\,|\mu_{1,0}\rangle\langle\mu_{1,0}| = \begin{pmatrix}(A_0 - B_0)^2 & \cdots\\ \cdots & (C_0 - D_0)^2\end{pmatrix} \tag{29}$$

Calculation for $x = 1$ will be the same as above. We only care about the diagonal values so the other parts were left out. We can then get the conditional density matrix for Eve:

$$\sigma_{E|x} = \frac{1}{2}\times((27)+(29))\times\frac{1}{\frac{1}{2}q(0|x)+\frac{1}{2}q(1|x)} \tag{30}$$

$$= \frac{\begin{pmatrix}{A_x}^2 + {B_x}^2 & \cdots\\ \cdots & {C_x}^2 + {D_x}^2\end{pmatrix}}{{A_x}^2 + {B_x}^2 + {C_x}^2 + {D_x}^2} \tag{31}$$

We can see that this is valid because the trace of the matrix add up to one, meaning that they are from a probability distribution.

The entropy $H(E)$ of a density matrix σ_E is calculated by (i) finding the eigenvalues of σ_E, which must constitute a probability distribution, and (ii) calculating the entropy of the eigenvalues. The conditional entropy $H(E|X)$ is

$$H(E|X) = \sum_x P(x)\,H(\sigma_{E|x}) \tag{32}$$

$$= \frac{1}{2}H(\sigma_{E|0}) + \frac{1}{2}H(\sigma_{E|1}) \tag{33}$$

where the von Newmann entropy of a density matrix ρ with eigenvalues $\{\lambda, 1-\lambda\}$ is $H(\rho) = h(\lambda)$.

We got $\sigma_{E|x}$ from equation 31, thus the entropy $H(E)$ can be calculated from equation 24:

$$H(E) = H(\frac{1}{2}\sigma_{E|0} + \frac{1}{2}\sigma_{E|1}) \tag{34}$$

$H(X)$ can be calculated with $\mathrm{prob}\{X|\bar{\varphi}\}$, which is the same as $\mathrm{prob}\{X\}$. This is because X is still uniformly distributed after Bob accepts the qubit. Otherwise, Eve's knowledge of X would increase thus decreasing H(X) and H(X—E):

$$H(X) = \frac{1}{2}\log_2\left(\frac{1}{2}\right)\times 2 = 1 \tag{35}$$

Since $\sigma_{E|x}$ can be represented by functions of $\Gamma_x^{r,s}$, we can write $H(E|X)$ and $H(E)$ in terms of $\Gamma_x^{r,s}$ and thus write $H(X|E)$ using $\Gamma_x^{r,s}$. From previous unitary gates and other properties, we can derive some constraints for $\Gamma_x^{r,s}$. We will use the optimized entropy value where all its $\Gamma_x^{r,s}$ values falls in our constraint.

D. Restrictions and constrains

According to equation 17, 18, 19, We can construct constraints for $\Gamma_x^{r,s}$ values. The disturbance is a constant value for difference sessions, thus, we are going to optimise for each discrete disturbance value D in equation 17.

$$(18) \to \left(\sum_{r,s=0}^{1}\Gamma_x^{r,s}\,\langle r|_E\,\langle s|_B\right)\left(\sum_{r,s=0}^{1}\Gamma_x^{r,s}\,|r\rangle_E\,|s\rangle_B\right) \tag{36}$$

$$= \left(\Gamma_x^{0,0}\right)^2 + \left(\Gamma_x^{0,0}\right)^2 + \left(\Gamma_x^{0,0}\right)^2 + \left(\Gamma_x^{0,0}\right)^2 \tag{37}$$

$$= 1 \tag{38}$$

$$(19) \to \left(\sum_{r,s=0}^{1}\Gamma_0^{r,s}\,\langle r|_E\,\langle s|_B\right)\left(\sum_{r,s=0}^{1}\Gamma_1^{r,s}\,|r\rangle_E\,|s\rangle_B\right) \tag{39}$$

$$= \sum_{r,s=0}^{1}\Gamma_0^{r,s}\times\Gamma_1^{r,s} \tag{40}$$

$$= \cos 2\theta \tag{41}$$

E. Calculation

Putting all the components and constrains together:

$$\begin{aligned}
H(X|E) &= H(E|X) + H(X) - H(E) \\
&= \frac{1}{2}H(\sigma_{E|0}) + \frac{1}{2}H(\sigma_{E|1}) + 1 \\
&- H\left(\frac{1}{2}\sigma_{E|0} + \frac{1}{2}\sigma_{E|1}\right)
\end{aligned} \tag{42}$$

The final key rate N_k is then:

$$N_r\left(H(X|E) - h(D)\right) \tag{43}$$

The value of N_r is calculated by the rate of Bob's accepting the qubits in equation 12. Using the Mathematica software, We can try to minimize the new expression for N_k for each value of disturbance D and angle θ. The optimised

angle would then be the highest minimized N_k for each disturbance. We can then look at the angle that produces the best value of N_k with each disturbance values.

V. RESULTS AND LIMITATIONS

Related works in similar topics have shown that the key rate drops to 0 when disturbance D reaches 10%. As a result, the experiment here would limit the span of D from 0 to 20% with an increment of 0.5%. In addition, the the basis will loop around as the angle increases, as shown in figure 2. The value will return in the same path to the start value as the angle passes $\frac{\pi}{4}$. Thus, we set the angle from 0 to $\frac{\pi}{4}$ with an increment of 0.01. The final unedited result is shown in figure 4.

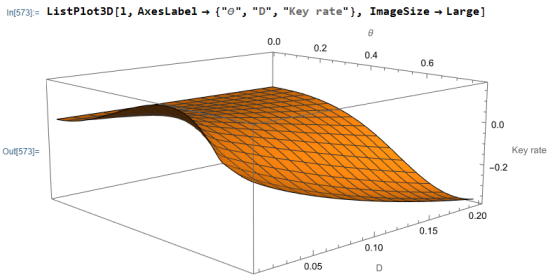


Fig. 4: Non-edited graph of key rate against disturbance against angle

The value of the final key rate is negative for most of the angles with a high disturbance, which indicates that the rate should be zero and the key exchange is ineffective. Changing all the negative values to zero we get figure 5 and 6. The figures show that as the disturbance gets smaller, the angle will have a larger effect on the final key rate value, where the optimal value of best key rate(that is minimized) appears when the disturbance is zero and the angle is about $\frac{\pi}{8}$.

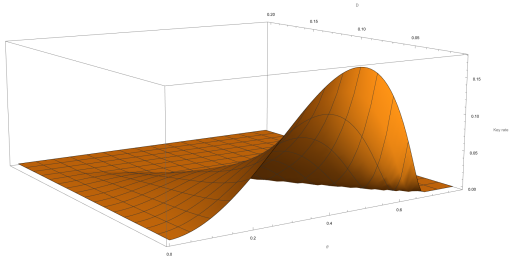


Fig. 5: Non-negative graph of key rate against disturbance against angle

To get a better view of how disturbance affects the optimal key rate, A 2 dimensional graph can be plotted using the optimized values of the key rate for each disturbance value in figure 7. This shows that the optimal key rate declines as the noise increases. The rate of decline slows down the higher D gets, until it reaches zero when D is around 15%. Another graph plotted in figure 8 shows a almost linearly decreasing trend of the angle as the disturbance increases.

Combining both graphs we will get the best angle to choose along with the key rate resulted from the angle

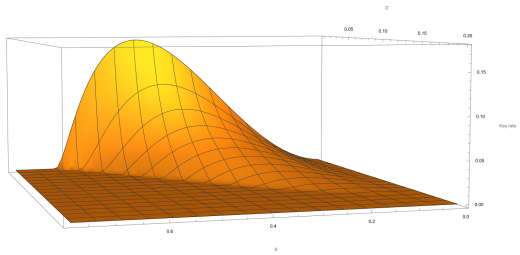


Fig. 6: Disturbance vs the angle that optimises the key rate from the back

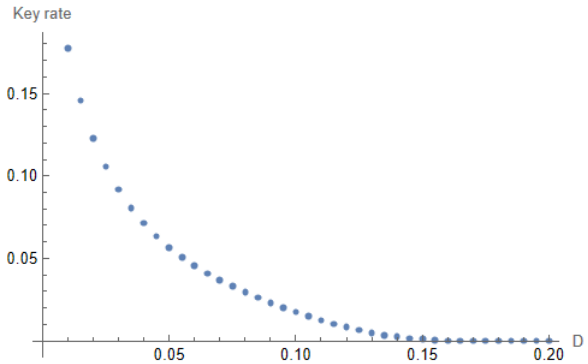


Fig. 7: Disturbance vs most optimal final key rate

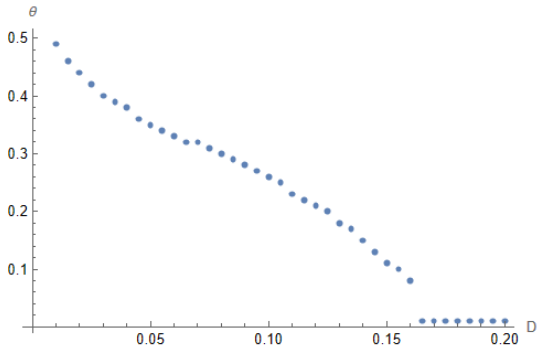


Fig. 8: Disturbance vs the angle that optimises the key rate

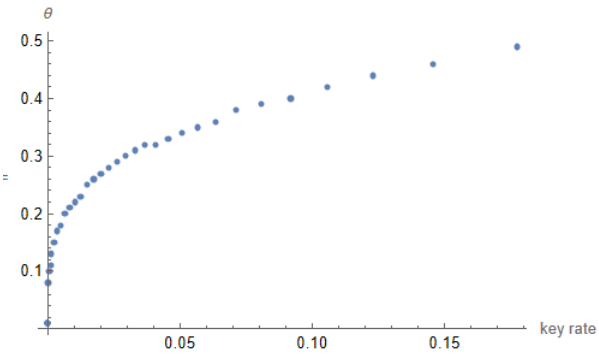


Fig. 9: optimal key rate vs the corresponding angle

This result shows how Alice should prepare the angle according to the disturbance. However, as the angle approaches to 0 which proves the illustration in figure 2.

One limitation of this result is that Alice need to change the angle of the basis constantly according to the calculated disturbance from the previous session of key exchange every session, which results in a new value of disturbance for the new session. With a fixed channel noise, this is no longer a problem because the disturbance will not change. However, if an attacker is involved, and they constantly changes the bit that interacts with Bob, the disturbance will be altered as a consequence. Although this might be necessary to be of concern in the future work, it is unlikely to happen. The reason is that eavesdroppers wants to minimized their value of entropy to they gain a better knowledge of the key. This results in them changing the interacting qubit only after each previous session, so Alice is not the one in the passive situation in this scenario.

VI. CONCLUSIONS AND FUTURE WORK

In this work we have derived an expression for the secret key rate and looked at how angles and disturbances have effects on it. We showed that the entropy is bounded by the coefficients of the elements in the state vector of new entangled qubit. We optimized for discrete values of disturbances, the angle Alice should choose so that the information lost is minimal. We have seen that the angle between both basis need to decrease in order to optimize the key rate for higher disturbances, while the optimal key rate still drops. The change of angle against the change of key rate is non-linear with the rate of increase damps for higher key rates.

For future works, the extended B92 protocol should be investigated, where Alice and Bob utilizes two more basis in addition to the two mention in this research[10]. Researches on this shows that the tolerance of disturbance increased by 5% which might implicate the optimized angle would have a wider range[5]. The analysis of a generalisation of the B92 protocol may also be looked into, where Alice sends more than 2 states to Bob, implying that Alice's state may have a higher dimension that would be affected by Eve's state with a higher dimension[11].

REFERENCES

[1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[2] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[3] Hiroaki Sasaki, Ryutaroh Matsumoto, and Tomohiko Uyematsu. Key rate of the b92 quantum key distribution protocol with finite qubits. In *2015 IEEE International Symposium on Information Theory (ISIT)*, pages 696–699. IEEE, 2015.

[4] Ryutaroh Matsumoto. Improved asymptotic key rate of the b92 protocol. In *2013 IEEE International Symposium on Information Theory*, pages 351–353. IEEE, 2013.

[5] Omar Amer and Walter O Krawec. Finite key analysis of the extended b92 protocol. In *2020 IEEE International Symposium on Information Theory (ISIT)*, pages 1944–1948. IEEE, 2020.

[6] Daniel E Platt. A modern analysis of the stern–gerlach experiment. *American Journal of Physics*, 60(4):306–308, 1992.

[7] John Watrous. *The theory of quantum information*. Cambridge university press, 2018.

[8] Tor Helleseth. *Advances in Cryptology–EUROCRYPT'93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings*, volume 765. Springer, 2003.

[9] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information theory*, 41(6):1915–1923, 1995.

[10] Marco Lucamarini, Giovanni Di Giuseppe, and Kiyoshi Tamaki. Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states. *Physical Review A*, 80(3):032327, 2009.

[11] Hasan Iqbal and Walter O Krawec. Analysis of a high-dimensional extended b92 protocol. *Quantum Information Processing*, 20(10):1–22, 2021.