Detection of Eavesdropping in Quantum Key Distribution using Bell’s Theorem and Error Rate Calculations

David Gaharia
Joel Wibron

under the direction of
Prof. Mohamed Bourennane
Quantum Information & Quantum Optics
Department of Physics
Stockholm University

Research Academy for Young Scientists
July 6, 2011
Abstract

Quantum key distribution claims to be an unconditionally secure way of communication. In this paper we investigate the possibility of eavesdropping upon a quantum key distribution using the BB84 protocol by the intercept-resend method. To determine if an eavesdropper was present, both the Bell inequality and the error rate was calculated. Without any eavesdropper present the Bell value was determined to $|S| = 2.62 \pm 0.08$ and the error rate to 4.4%. With the eavesdropper present the Bell value was determined to $|S| = 1.40 \pm 0.07$ and the error rate to 31%. This data strongly indicates that an eavesdropper using this method of attack will be detected.
1 Introduction

People have always wanted to keep some information hidden or secret from each other. To prevent eavesdropping in communication of such secret information different means of encryption have been invented. The security of all modern communication rests on the assumptions that the eavesdropper does not have the knowledge or technology required to break the encryption within a time span that makes the effort profitable. As technology advances it becomes an easier task to break classical means of encryption. Quantum cryptography rests on none of these assumptions and promises the two communicating parties total and unconditional privacy, no matter how technologically advanced or well-funded the eavesdropper might be.

The purpose of this paper is to investigate the possibility of eavesdropping upon a quantum channel by using the intercept-resend method without being detected.

2 Theory

2.1 Classical Cryptography

Deriving from the Greek words κρυπτς and γραϕη meaning 'hidden' and 'to write', cryptography is the art of making a message unintelligible without specific knowledge. There are many ways of encrypting a message to meet these ends and one can divide almost all ciphers into two distinct groups: substitution and transposition ciphers. In substitution cipher each letter is replaced by another determined by a pattern, based on the key. Transposition ciphers simply switch the order of the letters in the message in accordance with a predetermined pattern, also based on a key. The principle of all of them is that a sender, Alice, encrypts the plaintext with the help of a key. She then sends the ciphertext to the receiver, Bob, who also has the key, which he can use to decrypt the ciphertext into plaintext. All of this must be done with a key that is common between Alice and Bob, but secret to all other parties. Otherwise an eavesdropper, Eve, can gain full access to the information.

In this report we will focus on one distinct form of encryption: the one-time pad. This is a symmetric substitution cipher were Alice and Bob shares a common key which is completely random, unique and as long as the plaintext. Because of these three properties all outcomes are equally probable. This means that the one-time pad offers complete and perfect secrecy [1].

The most efficient way of creating a cipher for a binary code is by a method called the XOR cipher. Basically it can be described with four simple steps:

1. Alice has a plaintext, for example 01001100 01110011, and a key, 00110111 01111000.
2. By putting the plaintext and the key as two rows under each other and adding the columns together: 0 and 2 both make 0, while 1 makes 1. Thus 0+0 and 1+1 both equal 0, while 0+1 and 1+0 equal 1. Thereby the ciphertext, 01111011 00001011, is generated.
3. Alice then sends the ciphertext to Bob through a classical channel.
4. Bob uses the key that he shares with Alice to reverse the procedure done by Alice. This is possible by putting the ciphertext above the key and repeating the process done in step 2.

The encryption process is simply addition of the columns modulo 2. The strength of this encryption is that there is no way for an eavesdropper to know if there is a 0 or 1 in the plaintext or the key if the only known fact about a bit is that it is represented by a '1' in the ciphertext. The direct consequence of this is that all outcomes are equally probable, thus making the cipher impossible to break [2]. The procedure might also be demonstrated by table 1 and 2.

To use the one-time pad by classical cryptographic means has proven to be quite a challenge. One of the major drawbacks of the one-time pad is the key distribution. Since each key has to be unique one cannot use a single key twice, because of the critical drawback a ciphertext might have is that it is repetitive in one way or another. This means that for every plaintext sent from Alice to Bob, they must share a common key of the same length as the plaintext. There are no completely secure, or even very efficient, ways of classical key distribution. If the key somehow falls into the hands of Eve between the time that Alice and Bob share it and the time when they send the message, Eve will have complete access to the information. Quantum mechanics does however offer a solution to this problem [1].
2.2 Basics of Quantum Mechanics

2.2.1 The qubit - encoding bits to physical states

All information needs to be encoded in some kind of physical state. In the field of quantum information, digital information is encoded onto the physical states of particles such as photons. These states can be described as a qubit - a quantum bit, which exists in a two-dimensional Hilbert space and can be represented by a Bloch sphere, which is a unit sphere. Since it is a generalization of a classical bit, the qubit can be in one of two arbitrary orthogonal basis states \(|0\rangle\) or \(|1\rangle\), and take on any superposition of these states. This superposition of states can be written as

\[
|\psi\rangle = \alpha |0\rangle \pm \beta |1\rangle
\]  

where \(\alpha^2\) is the probability that a measurement would find the particle in state \(|0\rangle\), while \(\beta^2\) being the probability that a measurement would find it in state \(|1\rangle\).

In our case, the particle and state in question is the photon and its polarization. If one describes light as a wave, the polarization can be seen as the way it is rotated. The basis vectors \(|0\rangle\) and \(|1\rangle\) are then in this case horizontal, \(|H\rangle\), and vertical, \(|V\rangle\), polarization, respectively. The basis vectors can also be changed by rotating the polarization, for example to \(|+\rangle\) and \(|-\rangle\) by a rotation of 45°.

2.2.2 Indistinguishability

One of the fundamental principles of quantum mechanics is the impossibility of distinguishing between non-orthogonal states. To explain this one needs to look into the properties of the diagonal state, \(|+\rangle\). When a photon in the \(|+\rangle\) state is going through an optical instrument such as a polarization beam splitter (PBS), it is either reflected or transmitted randomly. A photon in the \(|H\rangle\) state would however always be transmitted, and one in the \(|V\rangle\) state always reflected. Hence the instrument’s name; it splits the beam according to the polarization of the photons. This can also more generally be described as that the \(|V\rangle\) state has equal probabilities to collapse either into the \(|H\rangle\) or \(|V\rangle\) state when measured.

If then the polarization was to be turned diagonally with an instrument such as a half-wave plate, one would also shift the basis vectors. As such, the results for the \(|H\rangle\) and \(|V\rangle\) states would now be random, and the \(|+\rangle\) and \(|-\rangle\) states would always be transmitted and reflected respectively. This demonstrates that the measurement of states other than the basis vectors will always render a random result, and because of this there is no way of knowing the state of a particle before it was measured. The conclusion that must be drawn from this is that there is no quantum measurement that is capable of deterministically distinguishing between non-orthogonal states.

2.2.3 No-Cloning Theorem

Not only does the nature of quantum mechanics prevent us from distinguishing non-orthogonal states, it also forbids perfect cloning of an unknown state. That the state is unknown is crucial.
since one could for example easily create a second photon with $|H\rangle$ polarization if one knows that
this is the polarization of the first photon. To prove that this is not possible for an unknown state,
let us imagine a unitary transformer $U$ which is able to perfectly clone the state $|\psi\rangle$ onto a second
photon

\[ |\psi\rangle = \alpha |H\rangle + \beta |V\rangle \]  

(2)

\[ U |\psi\rangle |0\rangle = U (\alpha |H\rangle + \beta |V\rangle) |0\rangle = \alpha |H\rangle |H\rangle + \beta |V\rangle |V\rangle \]  

(3)

The resulting composite state should now be equal to the state $|\psi\rangle \langle \psi|$, however

\[ |\psi\rangle \langle \psi| = \alpha^2 |H\rangle |H\rangle + \alpha \beta |H\rangle |V\rangle + \alpha \beta |V\rangle |H\rangle + \beta^2 |V\rangle |V\rangle \]  

(4)

\[ \Rightarrow |\psi\rangle \langle \psi| \neq U |\psi\rangle |0\rangle \]  

(5)

### 2.2.4 Entanglement

Entanglement is when two or more particles can only be described by one single quantum state,
which cannot be separated into product states. If then two particles are entangled and the state of
the first particle is measured, one will immediately ascertain the state of the second particle. The
relation between particles can be either correlated - the states are identical - or anti-correlated - the
states are orthogonal. Eq. (6) is a correlated entangled state, while eq. (7) is an anti-correlated
entangled state. Entanglement does not depend on the distance between the entangled states; it
has been observed experimentally between two photons at a distance of 144 km [3].

\[ |\Psi^\pm\rangle = \frac{1}{\sqrt{2}} (|H_1 H_2\rangle \pm |V_1 V_2\rangle) \]  

(6)

\[ |\Phi^\pm\rangle = \frac{1}{\sqrt{2}} (|H_1 V_2\rangle \pm |V_1 H_2\rangle) \]  

(7)

Entangled photons can be created in many ways, e.g. spontaneous parametric down-conversion in
a non-linear BBO (beta-barium borate) crystal, which is the case in this experiment.

### 2.2.5 Bell’s Theorem

In 1935 Einstein, Podolsky and Rosen [4] published their famous paper regarding their doubts on
the completeness of quantum mechanics. They were especially doubtful concerning the concept of
entanglement, since according to Einstein’s theory of special relativity nothing can communicate
or interact faster than the speed of light. They considered this principle to be violated if one
could instantaneously determine the state of the other particle in the entangled pair. Instead they
proposed a local hidden variable theory to describe the phenomenon. Opposite to this view was the
that no hidden variable theory could possibly reproduce the predictions of quantum mechanics.
He stated that any hidden variable theory always had to satisfy a Bell inequality, whilst quantum
mechanics could under some circumstances violate it. There was nevertheless no suitable method
of determining which of these was the correct way for describing entanglement until 1969, when
Clauser, Horne, Shimony and Holt [6] proposed a way of doing this. They determined this Bell
inequality to value of $|S| \leq 2$, which is calculated from the correlation functions $E$ as

\[ |S| = E(a,\bar{a}) - E(a,\bar{a}') + E(a',b) + E(a',b') \]  

(8)

where $a$, $a'$, $b$ and $b'$ are the rotation angles of the basis vectors for the two states and $a' = a + 45^\circ$
and $b' = b + 45^\circ$. The maximum violation of the Bell inequality $|S| = 2\sqrt{2}$ is achieved with the Bell
angles $0^\circ$, $22.5^\circ$, $45^\circ$ and $67.5^\circ$ as $a$, $a'$, $b$ and $b'$ respectively. The correlation function $E$ is defined by

\[ E(\alpha,\beta) = P_{HH} - P_{HV} - P_{VH} + P_{VV} \]  

(9)

$P_{HH}$, $P_{HV}$, $P_{VH}$ and $P_{VV}$ are the probabilities for measuring coincidences between $|H\rangle$ and $|V\rangle$ for
the entangled photons.
2.3 Quantum Cryptography

The main focus in this report will be on the BB84 protocol. In this protocol Alice generates a pair of photons which are entangled in polarization in one of two bases, usually $|HV\rangle$ and $|+−\rangle$. The base of polarization is determined completely randomly for each photon. One of the photons is sent to Bob and one to herself. Alice now randomly chooses a base in which to measure, either $|HV\rangle$ or $|+−\rangle$, and depending on the polarization of the photon Alice will get a hit in either a detector representing the bit '0' or the bit '1'. This means that if a photon with the polarization $|H\rangle$ measured in $|HV\rangle$ always goes to the detector for $|H\rangle$, thereby giving the bit '0'. If it is however measured in $|+−\rangle$ there is a 50% probability for it to be detected in $|+\rangle$ and 50% probability for it to be detected in $|−\rangle$. This because of the indistinguishability of non-orthogonal states [7].

Bob must also choose base at random and independent of Alice’s choices. Since the two photons were entangled in polarization, Alice and Bob will have either correlated or anti-correlated results. This only applies if they are measuring in the same base; otherwise the result will be completely random and not correlated at all.

When Bob has received a sufficient amount of bits from Alice he will communicate with her through a classical channel. Now they tell each other in which base they measured each photon. They will save the data where they measured in the same base, and delete the data where they measured in different bases. Then they choose some random photons of which they tell each other the polarization and by so doing they can see how good their results match. When the error rate has been calculated from this information they can know if Eve has been listening. This is called quantum key distribution, since what Alice sent was not the actual message, but a one-time pad key. If no eavesdropper was detected the message can be sent through a classical channel with perfect security [8].

The reason for why Alice and Bob can know if they have been eavesdropped upon by this mean of detection is the fact that no one can eavesdrop without creating errors. By using the intercept-resend method Eve will intercept a photon sent from Alice to Bob and measure it in a randomly chosen base. If this base is not the same as both Alice and Bob measures in, Eve will introduce an error with a probability of 50%. For example, suppose Alice and Bob measures in base $|HV\rangle$ and Alice knows that she sent a photon with $|H\rangle$ polarization. If Eve was to intercept Bob’s photon and measure it in $|+−\rangle$ she would detect that it is either a $|+\rangle$ or $|−\rangle$ photon. She would then generate a photon of the measured polarization. No matter if the polarization is $|+\rangle$ or $|−\rangle$ there would be a 50% probability of Bob detecting it as $|H\rangle$ and 50% probability of detecting it as $|V\rangle$, thus leading to an average 25% error in bits [9].

There are however more efficient ways of eavesdropping, but to counter them there are measures to enhance the security by privacy amplification techniques [10]. This together with the classical error correction that every raw key generated in practice must go through [11] leaves a 10.5% error rate that the transmission between Alice and Bob must be below for perfect security and privacy in communication.

An eavesdropper can also be detected by using Bell’s inequality. By using the Bell angles the maximum theoretical Bell value in quantum mechanics, $2\sqrt{2}$, will be achieved, thus violating the inequality. This only applies to entangled states, meaning that if Eve intercepts the photon and measures it she will break the entanglement and instead create a mixed state. The theoretical value for a mixed state in Bell angles is $\sqrt{2}$.

3 Experiment

The aim of the experiment was to detect the presence of an eavesdropper in quantum key distribution. In this section we will describe the experimental procedure in further detail. As stated in eq. (8) and (9), the probabilities for the different coincidences was obtained in order to calculate the value $|S\rangle$. This is needed to determine whether the Bell inequality has been violated and consequently if an eavesdropper has been present.

This experiment utilized a compact source of polarization-entangled photon pairs at a wavelength of 805 nm using a violet single-mode laser diode as the pump source of type-II spontaneous down-conversion [12]. The two output beams depicted in fig. 1 are in the intersections between two cones consisting of $|H\rangle$ and $|V\rangle$ polarized photons. These two intersection beams contain the entangled photons. In order to correct the phase shift introduced by the first BBO crystal the beams were
Figure 1: A schematic image of the setup. $BBO_1$ and $BBO_2$ stands for beta-barium borate crystal, with $BBO_2$ at half the length of $BBO_1$; $\lambda/2$ stands for half-wave plate; mirrors are grey rectangles and flip mirrors dashed grey rectangles; squares with diagonals are PBS; half circles are measurement stations. The "1" and "0" indicates the bit each detection produces.

directed towards a second BBO crystal with half the length of the first. Then followed a half-wave plate ($\lambda/2$) which was set at a specific angle to change the basis vectors the analysis stations measure in.

In the lower output beam, the ability to introduce an eavesdropper Eve was included through flip mirrors (dashed) set at a 45° angle to the incoming beam. It is crucial that the beam continues as if it was a straight line after going through Eve to Alice, as if Eve never intercepted it. In this setup Eve is more correctly described as a simulated eavesdropper, who will introduce errors by shifting the phase of the photons. The phase shift is a result of the difference in distance between path of the original and the intercepted beam. If Eve would have used real detectors this phase shift would have been introduced because of the impossibility of generating photons at a desired phase.

The measurement stations of Alice and Bob each include a PBS and two output ports connected to a coincidence counter unit through optical fibers, which was in turn connected to a computer which records the coincidence data. The experiment consisted of measuring these coincidences for the Bell angles, which were set at the half-wave plates. The coincidences were then measured over a period of 20 seconds for each angle of which an average was taken for each coincidence.

Additionally, measurements were made for the bases of $|HV\rangle$ and $|+\rangle |−\rangle$ for both an absent and a present Eve. This in order to calculate the error rate $e$, which was later used to calculate the binary entropy $h(e)$. Eq. (12) represents the number of useful bits left after both error correction and privacy amplification.

$$e = \frac{N_{HH} + N_{VV}}{N_{tot}} = \frac{N_{HH} + N_{VV}}{N_{HH} + N_{HV} + N_{VH} + N_{VV}}$$

$$h(e) = -e \log_2 e - (1 - e) \log_2 (1 - e)$$

$$K = N_{tot}(1 - 2h(e))$$

If the number of usable bits $K$ is less than or equal to 0 it is certain that Eve has acquired the whole key which consequently renders it unsecure.
4 Results

4.1 Detection of eavesdropper by Bell’s inequality

The collected data on coincidences was used to calculate the Bell inequality with eq. (8) and (9). Table 3 represents the values of $E(\alpha, \beta)$ for all Bell angles determined for the setup without Eve.

<table>
<thead>
<tr>
<th>Angle $\alpha$</th>
<th>Angle $\beta$</th>
<th>$E(\alpha, \beta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0^\circ$</td>
<td>$22.5^\circ$</td>
<td>$0.67 \pm 0.04$</td>
</tr>
<tr>
<td>$0^\circ$</td>
<td>$67.5^\circ$</td>
<td>$-0.65 \pm 0.04$</td>
</tr>
<tr>
<td>$45^\circ$</td>
<td>$22.5^\circ$</td>
<td>$0.71 \pm 0.04$</td>
</tr>
<tr>
<td>$45^\circ$</td>
<td>$67.5^\circ$</td>
<td>$0.59 \pm 0.04$</td>
</tr>
</tbody>
</table>

Table 3: $\alpha$ angle represents the base chosen by Alice and angle $\beta$ the one chosen by Bob. $E(\alpha, \beta)$ is determined by eq. (9).

With these values of the correlation function $E(\alpha, \beta)$ the Bell value can be determined to

$$|S| = 2.62 \pm 0.08$$ (13)

Which is a value that violates the bell inequality by 8 standard deviations.

Table 4 represents the values of $E(\alpha, \beta)$ for all Bell angles determined for the setup with Eve.

<table>
<thead>
<tr>
<th>Angle $\alpha$</th>
<th>Angle $\beta$</th>
<th>$E(\alpha, \beta)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$0^\circ$</td>
<td>$22.5^\circ$</td>
<td>$-0.72 \pm 0.04$</td>
</tr>
<tr>
<td>$0^\circ$</td>
<td>$67.5^\circ$</td>
<td>$0.49 \pm 0.04$</td>
</tr>
<tr>
<td>$45^\circ$</td>
<td>$22.5^\circ$</td>
<td>$-0.31 \pm 0.04$</td>
</tr>
<tr>
<td>$45^\circ$</td>
<td>$67.5^\circ$</td>
<td>$0.11 \pm 0.03$</td>
</tr>
</tbody>
</table>

Table 4: $\alpha$ angle represents the base chosen by Alice and angle $\beta$ the one chosen by Bob. The base of Eve, $|HV\rangle$, is constant. $E(\alpha, \beta)$ is determined by eq. (9).

The value of the Bell inequality with a simulated eavesdropper was determined to

$$|S| = 1.40 \pm 0.07$$ (14)

This value of $|S|$ satisfies the inequality and is deviating at its most by 6% from the theoretical value for a mixed state.

4.2 Detection of eavesdropper by error rate

By using the data of coincidences with eq. (10) the average error rate for the test without Eve was determined to 4.4%. According to eq. (12) this will result in 885 bits per second.

With Eve in the setup the average error rate was determined to 31% and according to eq. (12) resulting in a negative amount of bits, meaning that no useful bits can be generated and that Eve has more information about the key than the amount that is shared by Alice and Bob.

4.3 Errors in measurement due to dark current

Dark current in the detectors causes them to detect photons hits even when no photons are being transmitted - a dark count. This dark count was measured by blocking the photon source and minimizing other sources of light present. In the $|V\rangle$ detector of Alice the dark count was approximately 2000 counts per second, while the other detectors had a dark count of approximately 500 counts per second.
5 Discussion

The satisfaction and violation of the Bell inequality for the presence and absence of Eve respectively, rendered by our data strongly indicates that all eavesdropping on a quantum channel by the intercept-resend method will introduce errors to such a degree that it can be detected. This conclusion can be drawn from the fact that a quantum mechanical system cannot be described in a classical sense of physics. Quantum mechanics forbids one to measure something without changing it. The negative and positive usable key rate for the both cases also demonstrates this. The results correctly showed that an eavesdropper will change the original state of entanglement into a mixed state and thereby errors will always be introduced.

The base error rate was determined to 4.4%, which is sufficiently less than the maximum error rate of 10.5%, to make our results credible. The error introduced by Eve should because of this be 29.4%, but the value determined in the experiment was 31%. The difference in error can be credited to misalignment caused by the flip mirrors, but even so the difference was marginal and well above both the 25% and 10.5% limit.

The fact that we did not achieve the theoretical values originates from a number of error sources. These include dark counts in the detectors, which fortunately caused almost no coincidences. Ideally the dark count could have been eliminated by cooling the detectors with e.g. liquid helium. Alas, such equipment was not available for the experiment. The excess amount coincidences were caused by misalignment, especially the one caused when the flip mirrors were turned up and down. After each time they were flipped adjustments had to be made to once more direct the photons into the multi-mode fiber leading to the detector.

6 Conclusion

The data strongly indicates that it is impossible to eavesdrop upon a quantum channel by using the intercept-resend method without causing a sufficiently large amount of errors for the attack to be detected.

7 Acknowledgments

We would like to thank Prof. Mohamed Bourennane from the Quantum Information & Quantum Optics group at the Department of Physics at Stockholm University, whose great mentorship and expertise has been of utmost importance for this research. Many great thanks goes to Ph.D. student Johan Ahrens and Assistant Professor Hannes Hübels for providing help and support when needed. Our final thanks goes to the organizers of the Research Academy for Young Scientists for making this research possible.
References