Quantum Key Distribution: Theory, implementations, contributions

Arnav Metrani
ms21254@iisermohali.ac.in
Indian Insitute of Science Education and Research, Mohali

May 6, 2024 - July 31, 2024

Abstract

In this report I detail my readings and contributions to the ongoing experiments at the laboratory of Prof. Varun Raghunathan at the Indian Institute of Science (IISc). This includes analysis of the BB84 protocol, T12 protocol, MDI-QKD protocol, introduction into beamsplitters, and detailing the physical implementations of these protocols.

Contents

1 Introduction

Quantum Key Distribution is still a nascent field, originating from the fear of quantum computers cracking existing cryptographic protocols in the near future, as well as protecting oneself against enemies following the "store now, decrypt later" strategy for encrypted data.
Post Quantum Cryptography (PQC) attempts to answer the problem posed by quantum computers via classical cryptography, but PQC and QKD aren't really answering the same question…
The purpose of QKD itself can be easily summed up: to allow the distribution of a secret key between two or more parties st. even an infinitely powerful entity could not crack it as long as the postulates of Quantum Mechanics hold true. Such an entity would not be affected by mortal problems such as time, money, resources, P vs NP, etc.

Some parts of the problem have been solved, such as:

- What to do once a key has been distributed: see one-time pad.
- How to do it atleast theoretically: see BB-84 protocol for the simplest protocol (so far).
- Building the components to do it: see components.

Several issues have yet to be addressed:

- Implementable protocols that deal with active eavesdroppers.
- Practical implementations of device-independent protocols (where even if we cannot trust any of our instruments, the protocol can be executed).
- Implementations that can be conducted over distances comparable to classical communication.
- Key generation speeds relative to classical communication.
- Cost-effective implementations.

and so on… (kelalaka 2021)

Nevertheless, one can argue that the scope doesn't necessarily have to extend beyond transmitting extremely sensitive codes. With this in mind, this field may prove to be of paramount importance in the far future.

2 Code, References, and Miscellaneous Points

The report serves to document all that I have done and read over the project. All references have been linked in the bibliography. Codes and raw data can be found here. To make the report as self-contained as possible, a glossary has been added along with an appendix. References can be navigated to by clicking on the authors in the brackets enclosed in the text, and vice versa. All analysis regarding attacker detection has been done under the assumption that the attacker follows a naïve intercept-resend strategy. For further information please reach out via email.

3 Protocols

3.1 BB84 Protocol

Devised by Charles Bennett and Gilles Brassard and presented in 1984, the protocol (Bennett and Brassard 2014) utilises the no-cloning theorem, the indistinguishability of non-orthogonal states through measurement, and the disturbance of state when distinguishing non-orthogonal states to establish a secure one-way communication line.

The main intention of the protocol is for Alice (A) to securely transmit to Bob (B) a random bitstring, after which the bitstring is utilised as a one-time pad for communication.

3.1.1 Procedure:

The protocol's steps are as follows:

1. Alice (A) has access to two random bitstrings where 0 and 1 are equiprobable. Alice uses the bit from the first bitstring to determine the basis of encoding the photon (either in $\{H, V\}$ or $\{A, D\}$, where $A = \frac{|H\rangle + |V\rangle}{\sqrt{2}}$, $D = \frac{|H\rangle - |V\rangle}{\sqrt{2}}$) and uses the bit from the second bit string to determine which state to encode. In the rectilinear basis, $0 = |H\rangle, 1 = |V\rangle$, and in the diagonal basis $0 = |A\rangle, 1 = |D\rangle$.[1]
2. Alice transmits the state to Bob.
3. Bob has access to an independent random bitstring. If the bit is 0, Bob measures in the rectilinear basis, and if the bit is 1 then Bob measures in the diagonal basis.[2]
4. Bob records the detection made in the basis chosen by him.
5. Steps 1 to 4 are repeated several times.
6. After Alice has transmitted the intended number of photons (seen in step 5), Alice publically declares the basis she used for encoding for each of the photons, followed by Bob declaring the basis he used for "guessing" the basis for each photon. The classical channel is used for this purpose.
7. Alice and Bob only keep the bits in which their basis match.
8. *Assuming no error*, Alice and Bob's bits should match perfectly. To identify any eavesdropper (Eve), Alice and Bob publically declare some of their "private" bits to check if there is any discrepancy. If any discrepancy is detected, the protocol is aborted. If not, the string can be used as a one-time pad.

[1] Henceforth rectilinear basis is taken to mean the Z basis, and the diagonal basis is taken to mean the X basis.

[2] *Why should Bob measure in the first place? Once Bob receives the collection of qubits from Alice, Bob could simply store them until Alice declares the basis used for encoding, after which Bob can make the measurements. This way we could potentially have a much higher key rate.* The issue with this approach is that we assume Eve to be infinitely powerful. Eve can simply trap and store the qubits. When Alice sends the basis encoding through the classical channel, Eve can read it immediately, apply the measurement along the correct basis, generate the desired photons and send them to Bob st. he receives both with no indiscernible time delay b/w both channels. Bob will not know if he has "stored" the photons in the right time bin without measuring them.

QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↖	↔	↕	↕	↔	↔	↖	↗	↕	↖	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Figure 1: Sample run taken from (Bennett and Brassard 2014)

3.1.2 Discussion:

The protocol prevents the existence of 'passive' eavesdroppers (Appendix A3) provided single photon sources are utilised.

For weak coherent states, the decoy state technique can be utilised.

Let us assume that the attacker Eve decides to intercept and measure each photon[3]. It is undetected for 75% of the cases: The probability of guessing the right basis is $\frac{1}{2}$, and the probability that Eve guesses the wrong basis but the prepared photon resolves to the intended state ($|A\rangle \rightarrow |H\rangle$ due to wrong basis, $|H\rangle \rightarrow |A\rangle$ in Bob's measuring device) is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. However, the probability that Eve "wins" for a bitstring of length N is 0.75^N, which does not scale well as N increases.

Research into the upper bounds for QBER that allows secure key transmission under different conditions is still ongoing (Bocquet, Alléaume, and Leverrier 2011).

[3]This may seem as a haphazard strategy, but for MUBs such an attack scheme seems to be the most optimal so far.

3.2 T-12 Protocol

3.2.1 Summary:

Given: Alice and Bob are connected by a classical channel and a quantum channel. Bob has access to 2 detectors that are not photon number resolving.

1. Alice sends Bob two pulses whose relative phase shift is either in the set $\{0, \pi\}$ to encode as $\{|0_Z\rangle, |1_Z\rangle\}$, or is in the set $\left\{\frac{3\pi}{2}, \frac{\pi}{2}\right\}$ which is mapped to $\{|0_X\rangle, |1_X\rangle\}$.[4]
2. This pulse is attenuated st. if the pulses is not absorbed before reaching Bob, then it will contain one photon with a very high probability.
3. Bob "guesses" the basis by applying either a phase shift of 0 (corresponding to Z basis) or $\frac{\pi}{2}$ (corresponding to X basis) before overlapping the pulses with a delay line interferometer (DLI) and recording the interference effects at the detectors.
4. The detectors are calibrated st. one detector clicks at constructive interference and the other clicks at destructive interference.[5]
5. From this, at the declaration of their bases if Bob's guess matches Alice's encoding for a pulse/qubit then Bob is able to map the detector outcome to the encoding set by Bob.

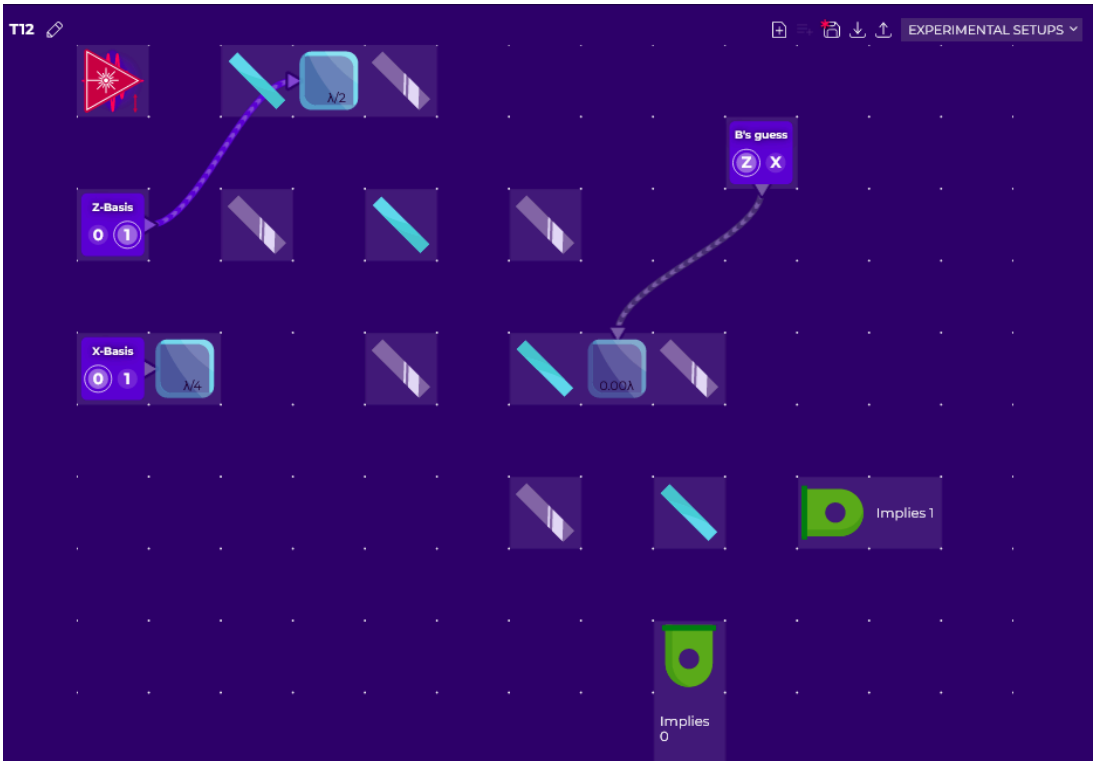


Figure 2: Pedagogical representation of T-12 protocol.

(See footnote[6] for explanation.)

[4]This is a modification from the original protocol for convenience, will be made clear later.

[5]No energy/photons are being lost in destructive interference. Quantum mechanically, it is easy to see through the beamsplitter equations that the photons must leave through either port. Classically, energy is conserved over the entire region, ie. we must consider the regions of constructive interference (and everything between) as well. For slit experiments with single photons, the photon is still measured, just its position of detection is dictated by wave interference.

[6]This is an optical setup created on Quantum Flytrap, a simulation application which lets you simulate quantum optics experiments. To simulate X axis, Z and X axis blocks can be swapped. For phase encoding, we are using blocks that perform instantaneous phase shifts. File is available here.

For reasons discussed in BB84 and through decoy state protocol, Eve's information about the state as well as the detection of Eve is bounded by the QBER of the process.

3.2.2 Details and analysis: (Reworked from (Lucamarini et al. 2013))

We start with Alice having a source that produces phase-randomised coherent states. The phase is randomised since we create a very tight bound on the uncertainty regarding the mean photon number. Phase randomisation is necessary as it removes any possible information that the eavesdropper could extract from the correlation of concurrent pulses (along with any other grouping).
If our source produces coherent states, the number of photons in the pulse produced will follow a poissonian distribution (knzhou 2016).

$$p(\text{k photons in pulse}) = \frac{e^{-\mu}\mu^k}{k!} \tag{1}$$

We overcome the attacks on weak coherent sources by utilising decoy states. To implement it, Alice chooses one out of the three intensities randomly: u, v, w out of which the latter two are used for decoy. Let us assume that in one key session Alice sends N pulses to Bob. Due to losses, let us assume that only $C \leq N$ pulses are registered by Bob.[7] In error correction, E more bits are eliminated, and in the Privacy Amplification step bits_{PA} are eliminated.[8]

No. of bits with μ_j as intensity source: N_{μ_j}
No. of bits with μ_j as intensity source and A's and B's bases: $\left\{N_{\mu_{jZZ}}, ...\right\}$
No. of registered/detected bits with μ_j as intensity source and A's and B's bases: $\left\{C_{\mu_{jZZ}}, ...\right\}$
No. of errors in detected bits with μ_j as intensity source: $\left\{E_{\mu_{jZZ}}, ...\right\}$

Secure key rate (SKR): Number of secure bits generated in a key session.

One key session involves the production of N coherent pulses, which is equivalent to the preparation of N states where the substates are entangled, denoted as $\rho_{A^N B^N}$.

$$1 \text{ state} = 1 \text{ pulse} \tag{2}$$

This is followed by Alice measuring its own subspace. Through deferred measurement principle (glS 2021) this measurement can be done at the end.

Where

$$\rho_{AB} = |\phi_D^k\rangle\langle\phi_D^k|, D = \{Z, X\}, \text{and } |\phi_D^k\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0_D\rangle_A|0_D^k\rangle_B + |1_D\rangle_A\ |1_D^k\rangle_B\right) \tag{3}$$

This slightly unusual description works as Alice *decides* what to send to Bob, and its measurement result collapses the state into one of the two sub-states. To simplify calculations, we assume that Bob's detectors work at equal efficiency, and the measurement outcomes of Bob are orthogonal to avoid indistinguishability.

Continuing with the analysis of the protocol, our goal would be to determine the secure bits after privacy amplification:

[7] We assume that the entire pulse is missed, not individual photons in a pulse. This is a fair assumption to make since (1) here we are only concerned with detections, not the number of photons detected and (2) we set the photon number to 0.5^9 so the probability of a multi photon pulse is close to zero.

[9] This number arises from linear optimization problems when evaluating the secure key rate. Informally, when looking at the probability function $\mu = 0.5$ is roughly around the region where the probability of multi-photon pulses starts to rise appreciably.

[8] Privacy Amplification is the process of completely removing any information held by Eve of the key after error correction. I did not cover it in my readings, refer to (Bennett, Brassard, and Robert 1988)

$$r' = \frac{\text{Secure bits}}{\text{Detected pulses}} \tag{4}$$

Since distillation of secret bits for X is the same as for Z basis due to symmetry, we only show it for Z basis here.

Deviation: Determination of r' *(Reworked from (Scarani and Renner 2008a))*

The security of a key can be parametrised by ε: its deviation from a uniformly random distribution of symbols which is completely unknown to Eve.

We say a key is ε-*secure* if:

$$D(\rho_{KE}, \tau_K \otimes \rho_E) \leq \varepsilon \tag{5}$$

Here we use the trace norm as it gives us a measure of the extent to which the attacker is coupled with the key's state τ_K. We consider σ_E instead $|0\rangle\langle 0|_{ENV}$ since the attacker's qubits can be in any other state as well.

τ_K is the maximally mixed state.

$$\tau_k = \frac{\mathbb{I}}{d}, \text{d= \# of dimensions} \tag{6}$$

We assume that Alice and Bob share $\rho_{A^N B^N}$ and measure their respective subspaces to obtain data. To determine the presence of an active eavesdropper, Alice and Bob reveal a few secret bits (say m bits) and calculate the frequency of bit runs and errors. We later parametrise this as $\lambda_{(A,B)}$ (parameter estimation). This leaves them with $n \leq N - m$ bits that have not been revealed.

Let these "raw" keys be X^n and Y^n for Alice and Bob respectively. Our aim is to determine the lower bound of the information about the "raw" keys that leaks out to Eve through the parameter estimation process. We assign the variable E^n to this (even though it is not a bitstring itself).

Once this is done, we can perform error correction to ensure that Alice and Bob's strings are perfectly correlated. A simple procedure is as follows:

> *With the simplest error correction protocol, Alice randomly chooses pairs of bits and announces their XOR value (i.e. their sum modulo 2). Bob replies either "accept" if he has the same XOR value for his corresponding bits, or "reject" if not. In the first case, Alice and Bob keep the first bit of the pair and eliminate the second one, while in the second case they eliminate both bits.*
>
> — (Gisin et al. 2002)

After this, we need to reduce Eve's information regarding the secret bits, and this is done by privacy amplification protocols:

> *Alice again randomly chooses pairs of bits and computes their XOR value. But, contrary to error correction she does not announce this XOR value. She only announces which bits she chose (e.g. bit number 103 and 537). Alice and Bob then replace (sic) the two bits by their XOR value. In this way they shorten their key while keeping it error free, but if Eve has only partial information on the two bits, her information on the XOR value is even lower. Consider for example that Eve knows only the value of the first bit, and nothing about the second one. Then she has no information at all on the XOR value. Also, if Eve knows the value of both bits with 60% probability, then the probability*

that she guesses correctly the value of the XOR is only of 0.62 + 0.42 = 52%. This process would have to be repeated several times; more efficient algorithms use larger blocks…

— (Gisin et al. 2002)

Asymptotic analysis: As earlier, we define r' as:

$$r' = \lim_{n\to\infty} \frac{l(n)}{n} \tag{7}$$

$l(n)$ is the number of generated secret bits, while n is the length of the raw key. Renner (Renner 2005) defines the following relation:

$$r' = H(X|E) - H(X|Y) \tag{8}$$

(Since this is done for $n \to \infty$, instead of defining $X^\infty, Y^\infty, E^\infty$ we define X, Y, E)
Informally, $H(X|E)$ is the uncertainty Eve has regarding Alice's bitstring X *given* its own intercepted data.
$H(X|Y)$ is the uncertainty Bob has about Alice's Bitstring when taking into account the information Bob has of his bitstring.
Now, we see that the part of the raw key data of Alice that Eve *does not* know about minus the effect of noise (else through the protocol $H(X|Y)$ should be zero) is precisely the sifted key rate.
Here, we see that $r' \simeq r$ (where $r = \frac{l(N)}{N}$) since the number of sacrificed bits does not compare to infinity[10].

Finite analysis:
Renner uses the smooth min-entropy to analyse the case for finite bitstring lengths:
For a given bipartite density matrix ρ_{AB} we first generate the set of all density matrices that are ε-close to ρ_{AB}. This we denote as $\left\{\overline{\rho}_{AB}\right\}$ Then we calculate the $H_{min}(A|B)$ for all the elements in the set and choose the maximum value.[11]

$$\text{Smooth min-entropy} = H^{\varepsilon}_{min}(A|B) = \max_{\left\{\overline{\rho}_{AB}\right\}} \left(H_{min}(A|B)\right) \tag{9}$$

Given that

$$H_{min}(A|B) = -\lg \lambda_{min} \tag{10}$$

λ_{min} is the smallest positive value of λ for which there exists σ_B that satisfies $\overline{\rho}_{AB} \leq \lambda_{min}(\mathbb{I}_A \otimes \sigma_B)$[12]
One possible motivation for this formalism- we want to quantify the maximum information that we can extract from the ε-secure states. This becomes clear when we take $A = K, B = E$. Let ρ_1 be more "random/secure" than ρ_2, then if we take $\lambda_1 > \lambda_2$ then $H_{\rho_1}(K|E) < H_{\rho_2}(K|E)$, thus through this process we choose ρ_2 to be more "leaky" than ρ_1.[13]

As stated by Renner, a protocol generates ε-secure keys if

$$l(n) < H^{\overline{\varepsilon}}_{min}(X^n|Y^n) - \text{leak}_{EC} - 2\lg\left[\frac{1}{2(\varepsilon - \overline{\varepsilon} - \varepsilon_{EC})}\right] \tag{11}$$

[10]N was the total number of transmitted pulses.

[11]The issue of maximising vs minimising over all sets seems to require a better understanding of the work. My reasoning for minimising over all sets was to ensure that we start of from the worst-case scenario and analyse from there on. In this approach it seems that we are choosing the most optimistic case of maximum information leakage and analysing it.

[12]It seems that τ_A would be more correct than $\mathbb{I}_A$. Understanding why trace distance is used instead of another function will require a closer reading of Renner's work.

[13]An explicit example could not be shown as calculating the smooth min-entropy proved to be computationally problematic. Even determining lambdas for specific cases proves to be intensive.

leak_{EC} is the number of bits sacrificed for error correction.
Another inequality which he derives is

$$H_{min}^{\overline{\varepsilon}}(X^n|EC^n) \geq H_{min}^{\overline{\varepsilon}}(X^n|E^n) - \text{leak}_{EC} \tag{12}$$

Where EC^n is the bitstring sent for error correction.
We are defining $\overline{\varepsilon}$ to give us some leeway in the analysis: $\overline{\varepsilon} \leq \varepsilon - \varepsilon_{EC}$ by definition, so choosing a smaller $\overline{\varepsilon}$ reduces the states that we are considering and would give a lower and more accurate bound, while choosing a higher value allows us to analyse more possible outcome state, but gives a "looser" bound.[14]

Here we are checking for collective attacks only: The attacker intercepts and "stores" the information of the qubits individually, but can operate on them collectively. To represent this, we can use the fact that the individual pulses sent by Alice have no correlation with each other to say $\rho_{A^nB^n} = (\sigma_{\overline{AB}})^{\otimes n}$. Next, let us say that Eve's action on this joint system of AB couples Eve's subspace with their system as well. To define the coupling of Alice and Eve's system, we can simply take our state $\rho_{A^nB^nE^n}$ and trace out Bob's subspace. This will give us $\rho_{X^nE^n} = (\sigma_{\overline{XE}})^{\otimes n}$

As stated earlier we use the parameter estimation procedure to determine the presence of an active eavesdropper. We do not concern ourselves with *how* it is done, just that it is possible. Now, we posit that this is what has taken place for a subset of states, which we denote as Γ' or $\overline{\varepsilon}'$ states. Another constraint defined in the paper is $\overline{\varepsilon}' < \overline{\varepsilon}$. We can interpret this as the probability of states with active eavesdropping being lesser than that of obtaining a successful case, but for now we can justify the inequality in the following manner:
Let us characterise Eve's operation as some CPTP mapping $\mathcal{E}(\rho)$.
Using the following inequality:

$$D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma) \tag{13}$$

We can substitute $\rho = \rho_{X^nY^n} \otimes \sigma_E$ and $\sigma = (\tau_K \otimes \sigma_E)$ so see how it relates Eve's operation to the trace distance inequalities. Let Eve's operation result in the following transformation:

$$\mathcal{E}(\rho_{X^nY^n} \otimes \sigma_E) = \rho_{X^nY^nE^n} \tag{14}$$

We know that for any two quantum states ρ and σ, the triangle inequality holds:

$$D(\mathcal{E}(\rho), \sigma) \leq D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) + D(\mathcal{E}(\sigma), \sigma) \tag{15}$$

We also know that $D(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq D(\rho, \sigma)$ Furthermore, $D(\mathcal{E}(\sigma), \sigma) \geq 0$, equality if the process maps to the same state.

Thus we can safely say that $D(\mathcal{E}(\rho), \sigma) \leq D(\rho, \sigma)$ which gives us

$$D(\mathcal{E}(\rho_{X^nY^n} \otimes \sigma_E), \tau_K \otimes \sigma_E) \leq D(\rho_{X^nY^n} \otimes \sigma_E, \tau_K \otimes \sigma_E) \tag{16}$$

Since the LHS is $\overline{\varepsilon}'$ and the RHS is $\overline{\varepsilon}$, the inequality is justified.

With this in mind, Renner proves the following inequality:

$$H_{min}^{\overline{\varepsilon}'}(X^n|E^n) \geq n\Big(\min_{\sigma_{\overline{XE}} \in \Gamma}\big[H(\overline{X}|\overline{E}) - \delta\big]\Big), \delta = 7\sqrt{\frac{\lg\left(\frac{2}{\overline{\varepsilon} - \overline{\varepsilon}'}\right)}{n}} \tag{17}$$

[14] ε_{EC} has a dual definition, its conventional definition is the probability that the protocol fails in the error correction stage due to errors above the threshold correctable by the EC procedure. see dual use.

Next, Renner assumes that the parameter estimation has been done for m pairs of bits[15] (λ_m). He also states a previously proved proposition, namely:
Given a state σ, if λ_m is calculated by using a POVM with d outcomes and if $\overline{\varepsilon}'$ is positive, then σ is in the set Γ_ξ with probability $1-\overline{\varepsilon}'$ provided the following holds:

$$\|\lambda_m - \lambda(\infty)\| \leq \xi, \text{where } \xi = \sqrt{\frac{2\ln\left(\frac{1}{\overline{\varepsilon}'}\right) + d\ln(m+1)}{m}} \tag{18}$$

λ_∞ is the probability distribution we would obtain for the measurement results if the POVM is applied onto σ (ie. an infinitely accurate probability distribution since we obtain the frequency of symbols for an infinite bitstring).
He provides a simple setting in the paper which utilises these formalisms later, but it seems that we can interpret this step as the parameter estimation process itself, while the POVM is simply the measurement of the single bit at a time.

Using all the above constructions, Renner develops the following inequality:

$$r' = H_\xi(X|E) - \frac{\text{leak}_{EC} + \Delta}{n} \tag{19}$$

$$\text{Where } \Delta = 2\lg\left(\frac{1}{2[\varepsilon - \overline{\varepsilon} - \varepsilon_{EC}]}\right) + 7\sqrt{n\lg\left(\frac{2}{\overline{\varepsilon} - \overline{\varepsilon}'}\right)} \text{ and } H_\xi(X|E) = \min_{\sigma_{\overline{XE}} \in \Gamma_\xi} H\big(\overline{X}|\overline{E}\big) \tag{20}$$

To summarise, Renner starts off by obtaining an expression for r' which contains $H(X|E)$. To bound this expression, he uses the smooth-min entropy as it has a parameter λ that he co-opts to express the frequency of symbols in the parameter estimation process. If it's too low, the protocol must be abandoned. Once this is done, he considers only collective attacks, which now require the quantification of $H\big(\overline{X}|\overline{E}\big)$. Also, after considering the set of states unaffected by active eavesdropping we develop a bound for λ through the parameter estimation process by linking it to measuring bits via some projective measurement operators and making the information public. Since this is the only information made public in the entire protocol (other than the basis reconciliation section), Eve can only extract information regarding the secret bits by analysing the distribution of data made public in the parameter estimation process. Having done this, he obtains an expression for r'. Lastly, from the paper itself:

> *We recall that* $(N, \varepsilon, \text{leak}_{EC}, \varepsilon_{EC})$ *are parameters of the protocol implementation, while* $(n, m, \overline{\varepsilon}, \overline{\varepsilon}')$ *must be chosen as to maximise* $r = \left(\frac{n}{N}\right)r'$ *under the constraint* $n + m \leq N$ *and* $\varepsilon - \varepsilon_{EC} > \overline{\varepsilon} > \overline{\varepsilon}' \geq 0$.
>
> — (Scarani and Renner 2008a)

[15] ie. for m ordered pairs, (A_i, B_i)

Eg. Asymmetric BB84 bound:

Let us assume that Alice and Bob choose basis B_0 with probability p_0 and basis B_1 with probability p_1 and we use let us say we use only matching B_1 basis bits for parameter estimation, which would mean say using only the matching XX cases for parameter estimation, the ZZ bits are kept secret. Then we see $n = N(p_0)^2, m = N(p_1)^2$ and $2Np_0p_1$ bits are discarded due to non-matching bases. Renner argues that the only factor that needs to be considered in the finite key analysis (for the calculation of $H_\xi(X|E)$) is the error in the basis B_1 (since we are only using B_1 for parameter estimation). The asymptotic value of $H(\overline{X}|\overline{E}) = 1 - h(\overline{e}_1)$, where $\overline{e_1}$ is the error rate in the basis B_1. By substituting the necessary sections into the expressions above and setting the POVM with two outcomes (same bits VS flipped bits), Renner obtains the expression $H_\xi(X|E) = 1 - h(\overline{e}_1)$.

Using this, the rest can be obtained.

Issue of dual-use:

We initially define ε as a trace distance quantity through our definitions of epsilon-secure keys, and $\overline{\varepsilon}$ as a parameter bounded by ε. It seems that ε has a dual definition: as a trace distance and as an error probability. This is seen for example in the interpretation of ε_{EC}. However, when we define $\varepsilon > \varepsilon_{EC}$, what exactly is being implied here? One obvious implication is that the error probability of EC cannot be greater than the total error probability of the protocol (if it is then the protocol is rendered useless), but how do we reconcile this with their trace distance definitions? Especially in the case that Γ is the set of states for which the parameter estimation shows that there is enough correlation to continue with the rest of the steps, what does it mean when we say $\overline{\varepsilon} > \overline{\varepsilon}'$? Does it imply that the states on which PE shows bad correlation 'must' be closer to the perfect key, or is there something else? We have justified why the inequality should hold without providing any conceptual justification that is in line with the dual definition.

The authors attempt to clarify this in a later paper (Scarani and Renner 2008b).

Return to T-12: The authors define $\overline{X}$ as a single bit, X^n, E^n as X, E.

We now have an explicit expression for r':

$$r' = H_\xi(X|E) - \frac{\text{leak}_{EC} + \Delta}{n} \tag{21}$$

$$\text{Where } \Delta = 2\lg\left(\frac{1}{2[\varepsilon - \overline{\varepsilon} - \varepsilon_{EC}]}\right) + 7\sqrt{n\lg\left(\frac{2}{\overline{\varepsilon} - \overline{\varepsilon'}}\right)} \tag{22}$$

$$H_\xi(X|E) = \min_{\sigma_{\overline{XE}} \in \Gamma_\xi} H(\overline{X}|\overline{E}) \tag{23}$$

The next step is to account for the effect of noise on the secure key rate.

$$\text{leak}_{EC} = nf_{EC}h_{BIN}(e_z) \tag{24}$$

Here, e_Z is the error in the Z-basis pulses (it is the error per pulse), h_{BIN} gives an estimate on the number of bits required to correct each error[16] and f_{EC} is some adjustable parameter to account for the inefficiency of the error correction procedure.

[16]Although not stated in the paper, it seems that we can treat entropy as a parameter. $h_{BIN} = 0$ implies 0 bits to correct an error, $h_{BIN} = 0.5$ implies 1 secure bit is extractable from 2 bits from the raw key after error correction.

For the T-12 procedure, we now need to determine $H(X|E)$:

Diversion: Calculation of $H(X|E)$ (Reworked from (Koashi 2006)):
Let's construct a framework: Alice sends weak coherent pulses: $|a_W^{(n)}\rangle = |n, \theta_{W,a}\rangle$ where $A = \{0, 1\}$ and $W = \{X, Z\}$.
This is just a way of compressing the protocol's explanation itself, for example Alice could send one photon pulse of 1_Z which corresponds to $|1, \pi\rangle$ since for T-12 we take 1_Z to be encoded as π relative phase shift (the original paper by Koashi interprets θ as polarisation).

Using the same formalism as described here, we can say that Alice prepares $|\Phi_W^{(n)}\rangle$.

$$|\Phi_W^{(n)}\rangle = \frac{|0_W\rangle_A \ |0_W^n\rangle_B + |1_W\rangle_A \ |1_W^n\rangle_B}{\sqrt{2}} \tag{25}$$

For the vacuum state case (where Bob does not detect anything because Alice sends an "empty" pulse) we define $a_W^0\rangle_B = |\text{vac}\rangle_B$. Next, for the case where $n = 0$ for a transmitted pulse:

$$|\Phi_Z^0\rangle_{AB} = \frac{[\ |0_Z^0\rangle_A + |1_Z^0\rangle_A]|\text{vac}\rangle_B}{\sqrt{2}} = |0_X\rangle_A|\text{vac}\rangle_B \tag{26}$$

Similarly, $|\Phi_X^0\rangle_{AB} = |0_Z\rangle_A|\text{vac}\rangle_B$.

In this slightly unconventional formalism, we see that if Alice "sends" a vacuum state, Bob knows with 100% probability that he will measure 0 regardless of the basis encoding. This seems to be a forced way to posit that vacuum states have no contribution to the error.

For $n = 1$ for a transmitted pulse:

$|\Phi_Z^1\rangle_{AB} = |\Phi_X^1\rangle_{AB}$. This is identical to what we see in the BB84 protocol, and the only way the bits do not match for matching bases is due to error.

For $n \geq 2$ for a transmitted pulse, the author argues that there is no correlation between the measurements of Alice and Bob.

My partial reasoning:
For any state prepared, if Alice and Bob have matching bases then the outputs must be correlated. We see this for $n = 1$ itself. If Alice prepares one of the basis states at random (say $|\Phi_Z^1\rangle_{AB}$) and *both* measure in the other basis, then if Alice measures "0", then Bob will measure "0" as well, we see this from the calculations itself. For $n = 2$, we see

$$\begin{aligned} |\Phi_X^2\rangle_{AB} &= \frac{1}{\sqrt{2}}[\ |0_X\rangle_A \ |0_X 0_X\rangle_B + |1_X\rangle_A \ |1_X 1_X\rangle_B] \\ \Rightarrow \frac{1}{2}[\ |0_Z\rangle_A|0_Z 0_Z\rangle_B &+ |0_Z\rangle_A|1_Z 1_Z\rangle_B + |1_Z\rangle_A|0_Z 1_Z\rangle_B + |1_Z\rangle_A|1_Z 0_Z\rangle_B] \end{aligned} \tag{27}$$

We see that if Alice randomly ends up preparing this state and both measure in Z, then if Alice measures "0" Bob will measure "00", and similarly for the other case. However if both measure in the X basis, then even if Alice measures "0" Bob could measure "00" or "11" with equal probability, which is as bad as having no correlation.

Although it seems that Alice measuring 1 would give some correlation with Bob's measurement, this correlation disappears when we consider that $|\Phi_Z^2\rangle_{AB}$ could be prepared as well since in that case we see

$$\begin{aligned} |\Phi_Z^2\rangle_{AB} &= \frac{1}{\sqrt{2}}[\ |0_Z\rangle_A\ |0_Z 0_Z\rangle_B + |1_Z\rangle_A\ |1_Z 1_Z\rangle_B] \\ \Rightarrow \frac{1}{2}[\ |0_X\rangle_A |0_X 0_X\rangle_B &+ |0_X\rangle_A |1_X 1_X\rangle_B + |1_X\rangle_A |0_X 1_X\rangle_B + |1_X\rangle_A |1_X 0_X\rangle_B] \end{aligned} \tag{28}$$

Next point: it seems that if both the detectors of Bob click then Alice *must* have sent a 1 regardless of the original basis preparation. This seems to hold even if we cannot distinguish between the $1_B 0_B$ and the $0_B 1_B$ case.
This is however not considered in the paper, as the author assumes earlier that any case where both the detectors click must be randomly allotted as a "0" detection or a "1" detection. It seems that the author does this to mitigate the case for $n = 1$ where we may have a valid click at one detector and a dark count click at the other detector simultaneously, which would make it impossible to tell what the initial information sent was. However the exact reasoning is not made explicit. The author also states[17] that the parameter estimation process used for $n = 1$ will not work for higher cases.

Here it seems that the author assumes neither has any information of the actual state prepared, and they simply choose the basis and apply measurement operators corresponding to that basis. This could be explained by having an MDI-esque setup where a neutral source prepares the state $|\Phi_Z^n\rangle_{AB}$ or $|\Phi_X^n\rangle_{AB}$ and send the first qubit to Alice and the rest to Bob, after which the basis reconciliation and other steps can take place. Such an interpretation is mathematically indistinguishable from our current setup.

To re-iterate from earlier, we are using the matching Z bases cases for the secret key generation and the matching X basis cases for parameter estimation. Since the parameter estimation statistics $\lambda_{A,B}$ is made public, it invariably would reveal some information regarding the pattern/frequency distribution of the secret bits since the distribution of bits and bitruns in the Z basis is equivalent to that of the X basis. Thus, if we wanted to quantify the entropy per secret bit given the parameter estimation information is made public, it would come to:

$$\begin{aligned} H = q_Z^0 \times 0 + q_Z^1 \times H_{BIN}(e_X^1) + \left(1 - q_Z^0 - q_Z^1\right) \times 1 \\ \Rightarrow 1 - q_Z^0 - q_Z^1[1 - H_{BIN}(e_X^1)] \end{aligned} \tag{29}$$

(It should be e_Z^n but here we are assuming the error in the Z basis due to the channel to be the same as in the X basis.)

$$\text{Where } q_Z^n = \frac{Q_Z^n}{Q_Z} \text{ and } Q_Z = \text{Rate of detected pulses} = \frac{\text{Pulses detected by Bob in Z}}{\text{Pulses sent by Alice in Z}} \tag{30}$$

[17] Personal correspondence.

Experimental implementation

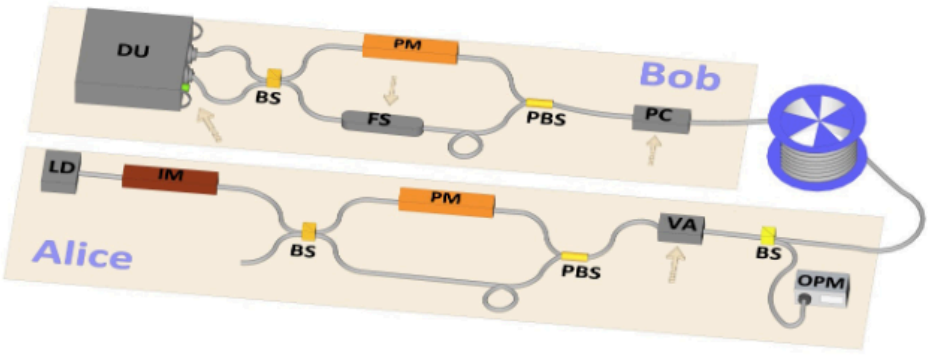


Fig. 1. Experimental setup for the T12 protocol. In Alice's layout, light pulses are emitted by a 1550 nm laser diode (LD), pulsed at 1 GHz, and transmitted through an intensity modulator (IM) and an unbalanced Mach-Zehnder interferometer. This is composed by a fibre-integrated beam-splitter (BS), a phase modulator (PM) and a final polarising BS (PBS). A variable attenuator (VA) is used to set the intensity of the pulses at the desired level. An optical power meter (OPM) measures the total flux in the fibre and adjust the VA in real-time in order to keep it constant. After a fibre spool of different lengths, the light passes through a polarization control (PC) and a second interferometer that matches Alice's. In one arm, a fibre-stretcher (FS) is used to match the arms length between the two distant interferometers, thus generating interference at the final BS. Pulses are eventually measured by a detection unit (DU).

Figure 3: T12 Schematic (from the original paper).

The mapping stated in the summary is now seen quite clearly: if Alice and Bob choose the Z basis, then $0 \to 0$ and $\pi \to \pi$. Outputs can be directly mapped. In the same manner, if both choose X basis, then $\frac{3\pi}{2} \to 2\pi$ and $\frac{\pi}{2} \to \pi$, easily mapped again. This explains why the swapping of 0_X and 1_X phase shifts is convenient since we now have ones detector for zeroes, and one for ones.

Instrumentation for T12 is covered here.

Alice uses a CW laser as the photon source. The continuous pulse[18] is then passed through the intensity modulator, which not only periodically creates two distinct pulses, but also is used for modulating the number of photons in the generated pulse. The polarization is stabilized using the polarization controller.

[18] A 15 dBm 1550 nm laser will give roughly 31.6 mW output, which translates to 2.47*10^14 photons/sec. Since a photon is emitted on the order of picoseconds, for our purposes it is continuous.

The intensity modulator "carves" out light pulses. Directly pulsing the laser is not ideal. When the current is turned on, the increase in carrier density produces photons faster than the electron-hole pairs can be depleted by stimulated emission. As a result the intensity of the laser pulse overshoots the expected intensity. It settles back to the desired intensity in a decaying manner, giving "ringing" artifacts.

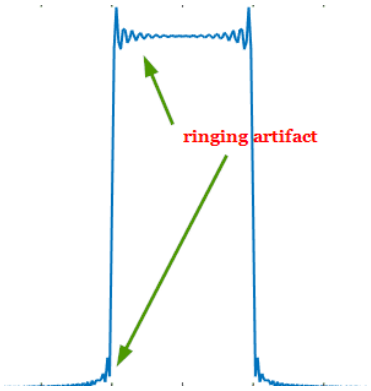


Figure 4: Visualisation of ringing artifacts.

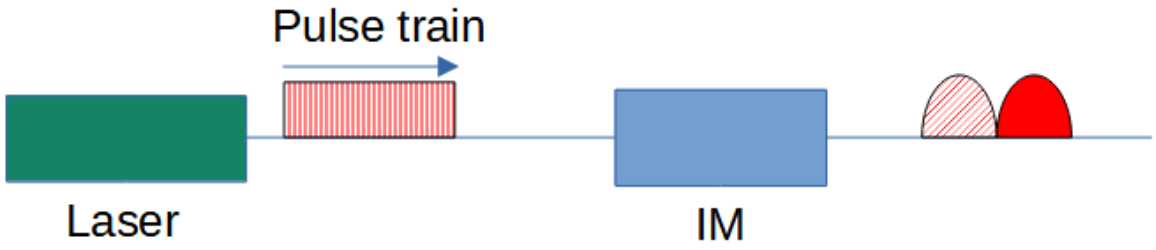


Figure 5: Action of intensity modulator.

Square pulses shown as elliptical for illustration purposes.
Shaded pulse is the late pulse, filled pulse is the early pulse.

The EOPM then is used to encode a phase shift between the pulses randomly (either $0, \pi$ or Z basis, or $3\frac{\pi}{2}, \frac{\pi}{2}$ for X basis).

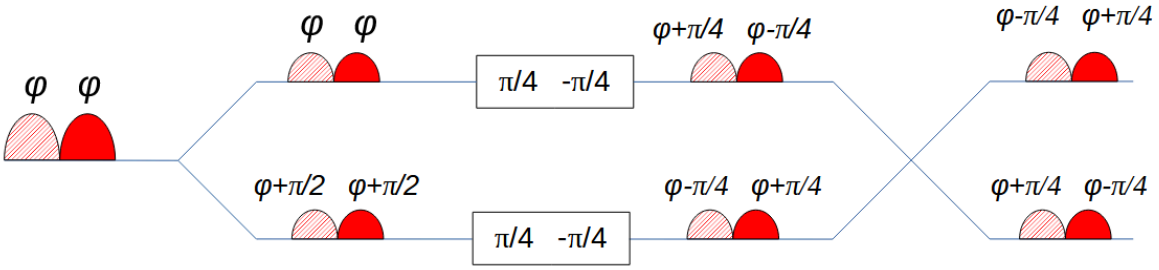


Figure 6: Action of EOPM for pi/2 shift. Any one arm can be chosen to serve as optical pulse.

Next, the attenuators are used at Alice's side to ensure that the pulse that arrives at Bob's side has a high probability of being a single photon pulse (losses through the quantum channel are accounted for).

Phase randomisation of the pulses takes place in this step. Before attenuation, the "carved" pulses will have a very high number of photons ($\sim 10^6$) so there is only a loose bound on Δn. Through the attenuators the mean photon number is set to 0.5 photons. Since coherent sources follow a poissonian distribution, $\Delta n = \sqrt{\mu}$, this is a tight enough bound st. the wavefunction is highly localised over the $|0\rangle$ and $|1\rangle$ state. Due to the number state-phase uncertainty principle, the phase is effectively randomised.

At Bob's side, the same EOPM operation is applied in accordance with Bob's guess (0 or Z basis, $\frac{\pi}{2}$ or X basis), and the EOPM is fitted into a delay line interferometer st. the early and late pulses are made to overlap.

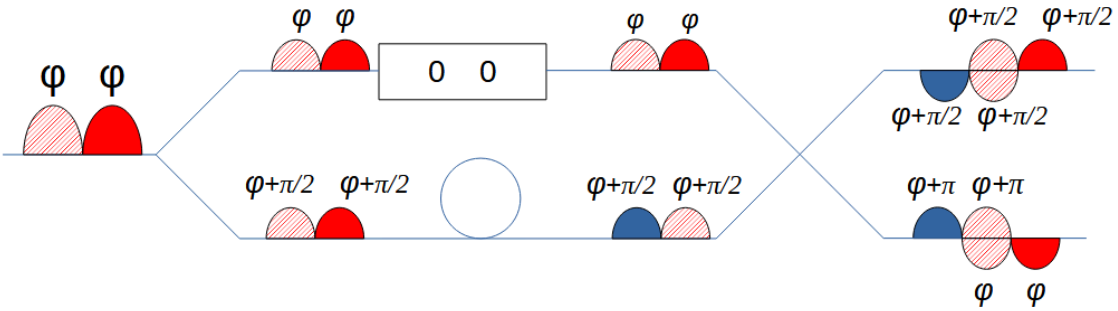


Figure 7: Action of DLI coupled with EOPM for Z-basis guess. Input state is 0Z.

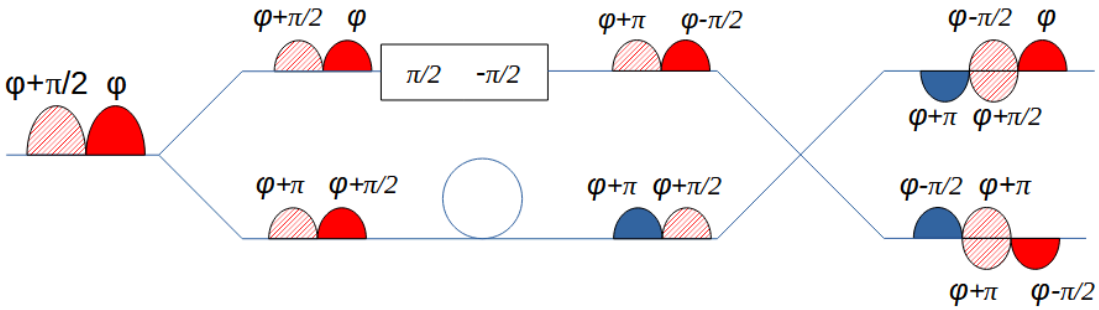


Figure 8: Action of DLI coupled with EOPM for X-basis guess. Input state is 1X.

The blue timebin refers to the "latest" timebin.

We set one of the detectors at constructive interference and the other at destructive interference. From this we obtain a set of detector counts.

A classical channel is then used to correlate the detector clicks with the encoding at Alice's end. After the post-processing, Alice and Bob have access to the same private key.

Electrical pulses are provided through an AWG at each end, which have their clocks synced through an additional channel.

3.2.3 Contributions

LabVIEW

Since the TCSPC's (detector's time controller/CPU) software is interfaced with the AWG (Arbitrary Waveform Generator) using LabVIEW, I covered the basics of this programming language. A couple of sub-programs have been added to highlight my understanding of the language.

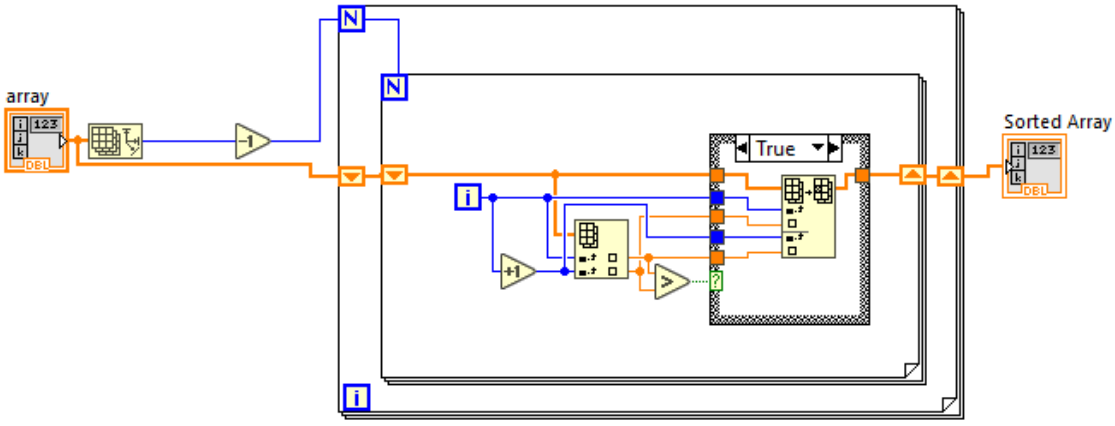


Figure 9: Bubble sort in LabVIEW

To explicitly highlight the working of this sub-program:

- The unsorted array is fed into the shift register.
- Array size -1 is fed into the iteration number of the for loop (external and internal).
- Using the iterator of the inner loop, the i^{th} and $i+1^{th}$ terms of the array are compared and swapped if the i^{th} term is bigger.
- The modified array is stored in the shift register and re-used for every iteration until the process is complete.

To simulate the interaction between a Python script and LabVIEW program, a simple script was written for the addition of numbers: Two inputs will be sent from the LabVIEW program to a Python script which will add and return them, and the result will be sent back to the LabVIEW program:

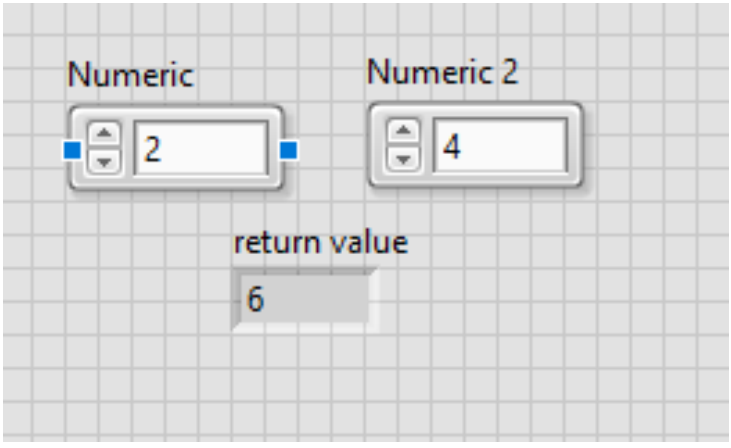


Figure 10: Front panel.

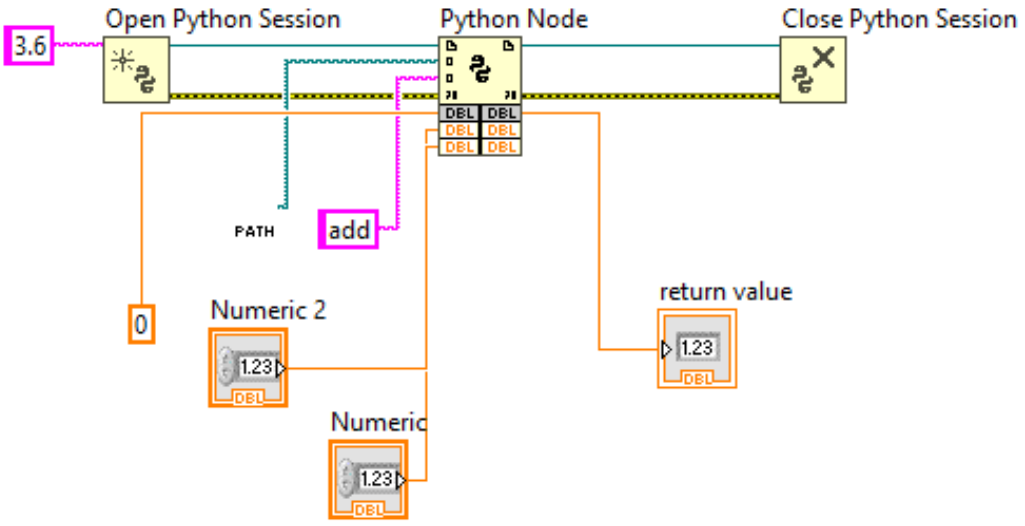


Figure 11: Block diagram.

See here for files.

Since LabVIEW 2022 supports only up to Python 3.6.0, the packages that can be utilised are very limited. As a result, a more comprehensive implementation did not utilise packages such as Numpy.

An implementation was developed for determining the central peak in the raw detector timestamps.

The code allows the user to input the file path of the first calibration file, which is sent to Python to determine the central peak, and these values are returned to the LabVIEW program (after which the rest of the analysis can be done using these values.) The code also records the execution time of the interfaced code.

The intention was to automate the process of determining the voltages at which the EOPM applies a relative phase shift of $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ to the pulse pair.

I rewrote the Python script to identify the central peak and construct the necessary photon count vs voltage graph.

Need for PM calibration

The EOPM must be calibrated since the RF output from the AWG is not plugged in directly to the EOPM. AWGs generally reach a maximum V_{pp} of 650 mV. On the other hand, the operating voltage for the EOPMs is around 5-8 volts. As a result, RF amplifiers are required. Even if the amplifier gain does not drift, if the effective applied phase is even off by a few degrees to the intended voltage it will show up as increased QBER which is detrimental to real-time communication. As a result, calibration of the EOPM is required before every experiment.[19]

PM Waveform generation

Once this is done, the waveform can be generated depending on whether we want to perform further testing of the basis separately or to perform the experiment. I wrote a Python script that generates the necessary waveform.

[19] As an add-on, every instrument has attacks associated with it. (Gnanapandithan, Qian, and Lo 2024) investigates the drop in SKR due to the imperfect temporal profile of the optical pulse due to the non-linear response of the amplifier beyond a certain point. (In the paper, at 5.6 V onwards.) At a high enough encoding rate. This is modelled as a side-channel in the paper.

IM Waveform generation

- **Two-dimensional case:** The intensity pulse pair waveform consists of two square waves in consecutive time bins. I wrote a Python script which generates this waveform.
- **Multi-dimensional case:**

For the multi-dimensional case, we have chosen to encode and send our information in the form of "nits" (nit= information carrying entity with 'n' possible values). Each nit is encoded in a 100 ns window.

Although the ideal encoding protocol is straightforward:

nit	Encoding
0	0 ns, 1 ns
1	0 ns, 1 ns with π relative phase
2	2 ns, 3 ns
3	2 ns, 3 ns with π relative phase

Table 1: ... until nit=100.

Even if Eve intercepts the photon which is encoded in the 60-62 ns time window, if Eve guesses the wrong basis then she cannot tell if a 30 or 80 was encoded.

So we can generate 50 different types of intensity pulse pairs.

However, this does not work out in practice due to side peaks and detector after-pulsing. Since side peak counts of one time bin would erroneously count as valid data points for the adjacent timebins. Similarly, to ignore the after-pulsing effects of the detector we need to intentionally create "dead air" time slots so that the after-pulsing counts do not show up as counts in another timebin.

I wrote a Python script which generated waveforms based on a pre-defined scheme used for previous experiments in the lab.

SKR and QBER calculation

After the run has concluded, for analysis and calibration purposes we calculate SKR and the QBER. The analysis is conducted in the following manner:

- After the acquisition time is completed, we extract the timestamps corresponding to the central peak for both of the detectors via histogram analysis.
- After this, we extract the clock indexes of the photon detections at each of the detectors. Since we have set one detector as constructive interference and the other as destructive interference, basis reconciliation and detector click correspond to Alice sending 0 or 1. (ie. D_1 clicks when the phase shift is 0, D_2 clicks when the phase shift is π. For cases of phase shift $\frac{\pi}{2}$ and $\frac{3\pi}{2}$ the detectors can click with equiprobability.)
- The QRNG bits corresponding to the clock indexes for each of the detectors are extracted and matched with the expected string of all zeroes in D_1 and all ones in D_2.

$$\text{SKR}= \frac{\text{Total correct entries from } D_1 \text{ and } D_2}{\text{Total acquisition time}} \tag{31}$$

$$\text{QBER}= \frac{\text{Total correct entries from } D_1 \text{ and } D_2}{\text{Total registered photon counts}} \times 100 \tag{32}$$

Hands-on experience:

Gained some rudimentary experience in handling optic fibre connections, AWG, and TCSPC software. Performed PM calibration, waveform generation and data analysis.

3.3 MDI-QKD Protocol

3.3.1 Details

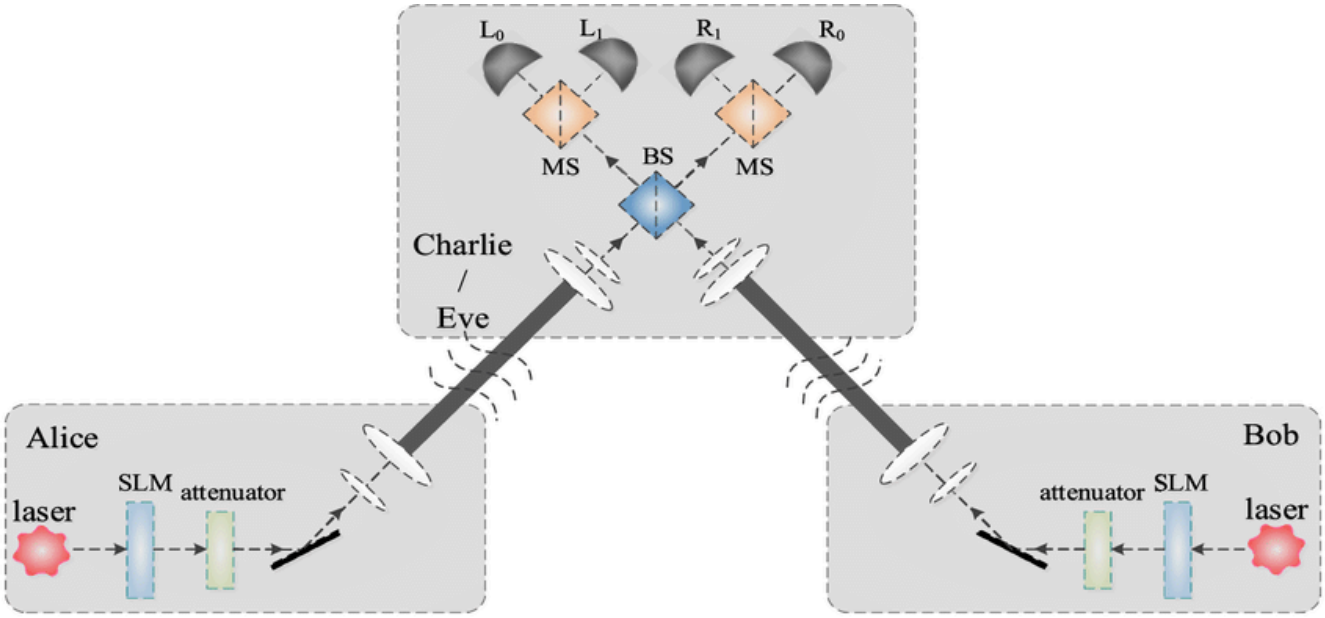


Figure 12: MDI setup.

The protocol relies on the HOM effect indirectly to generate detection results which Charlie cannot use to determine the initial inputs by Alice and Bob.

The protocol proceeds as follows (in its current implementation):

1. Alice and Bob independently encode a state into their pulse.
2. The pulses of both parties are passed through a beamsplitter.
3. Charlie announces the measurement result.
4. If Charlie announces a singlet state (one click at each detector and at different timebins), both parties disclose their basis.
5. If their basis match and their matching basis is Z, Bob flips the bit corresponding to his encoding and stores it, while Alice stores her encoding bit as it is.

Similar to the T12 protocol, the protocol utilises the relative phase between pulses as well as timebin encoding to parametrise the states. The Z basis is defined as $\{|e\rangle,|l\rangle\}$, where $|e\rangle, |l\rangle$ correspond to a photon sent in the early and late timebin respectively (1 ns windows in experimental implementation), while the X-basis is $\{\frac{|e\rangle+|l\rangle}{\sqrt{2}}, \frac{|e\rangle-|l\rangle}{\sqrt{2}}\}$.

The states prepared are indistinguishable, ie. 0_Z by Alice and Bob are indistinguishable.

Considering for matching Z basis case:

If Alice sends a 0 and Bob sends 0, then $|e\rangle_A|e\rangle_B$ arrives at the beamsplitter, giving rise to the photon bunching HOM effect, and a click is registered at either detector C or D (which corresponds to two photons arriving). Now if Alice and Bob *decide* to use this case, then since the protocol must be made public for Alice and Bob to agree on the rules, on their basis declaration Charlie will know both their states.

On the other hand, if Alice sends 0_Z and Bob sends 1_Z, then on the declaration of a singlet state Bob simply needs to flip his state to match Alice, while Charlie gains no information on their state.

Considering Alice encoding in X and Bob in Z:

For any detection event, since the other party's state encoding itself isn't known, even if a singlet state is announced it is impossible to extract any information; Alice does not know what time bin her photon resolves to, Bob does not know the relative phase in the state sent by Alice.

If both encode in X, then we see standard interference effects taking place.

If parties send flipped states then Charlie cannot extract information and Bob needs to simply flip his state.

If Charlie announces two clicks for the same detector, then Alice and Bob have sent the same state, no flipping is required. Unfortunately, this state will not be detected with current technological capabilities. This is because the time gap between the detection is too small for the detector to resolve. Here the time gap is 2 ns. Superconductor wire detectors currently have a dead time of ~20 ns. The SKR gain in including this state by increasing the time gap between the two pulses that make up the $|0_X\rangle$ and $|1_X\rangle$ states will be outweighed by the decrease in the rate of information transmission. Thus, having a photon number resolving detector is not sufficient. As a result, this case is discarded.

The spacing of the pulses that make up the states in MDI is not a factor as they resemble orthogonal states. $\langle e|l\rangle = 0$.

Since Alice and Bob randomly choose their basis, probability of success is $\frac{1}{8}$, which goes to $\frac{1}{4}$ if we take ideal detectors. Here, I assume that Eve utilises an intercept-resend strategy on Alice. For attacker detection, both parties declare the state they have sent, and correlate it with Charlie's announcement. In such a setup, it is seen that when matching Z base states are declared by Alice and Bob, and the resultant announcement is not two clicks for the same timebin in a detector, the attacker is caught. This happens with probability $\frac{1}{4}$.

$$\begin{aligned}
[0_Z, 0_Z] &\rightarrow E_E, F_E \\
[0_X, 0_Z] &\rightarrow \underbrace{E_E E_L}_{(\times)}, \underbrace{E_E F_L}_{(\times)}, E_E, \underbrace{E_L F_E}_{(\times)}, \underbrace{F_E F_L}_{(\times)}, F_E \\
[1_X, 0_Z] &\rightarrow \underbrace{E_E E_L}_{(\times)}, \underbrace{E_E F_L}_{(\times)}, E_E, \underbrace{E_L F_E}_{(\times)}, \underbrace{F_E F_L}_{(\times)}, F_E
\end{aligned} \tag{33}$$

If matching X-base states are declared y Alice and Bob and the resultant announcement by Charlie is a click in each detector, the attacker is caught. This happens with probability $\frac{1}{8}$.

$$\begin{aligned}
[0_X, 0_X] &\rightarrow E_E E_L, E_E, E_L, F_E F_L, F_E, F_L \\
[0_Z, 0_X] &\rightarrow E_E E_L, \underbrace{E_E F_L}_{(\times)}, E_E, \underbrace{E_L F_E}_{(\times)}, F_E F_L, F_E \\
[1_Z, 0_X] &\rightarrow E_E E_L, \underbrace{E_E F_L}_{(\times)}, E_L, \underbrace{E_L F_E}_{(\times)}, F_E F_L, F_L
\end{aligned} \tag{34}$$

This is for ideal detectors. For those which cannot resolve two clicks in the same detector, for X-basis case it remains $\frac{1}{8}$ while for Z-basis it becomes $\frac{1}{8}$ as well.

The above analysis is done assuming single photon sources. In more realistic settings there are several other factors involved, most significant being visibility.

When determining the distinguishability of the pulses produced by both parties, the visibility parameter is utilised.

$$\text{Visibility} = \frac{\text{counts}_{\text{max}} - \text{counts}_{\text{min}}}{\text{counts}_{\text{max}}} \tag{35}$$

$\text{counts}_{\text{max}}$ *is obtained for completely distinguishable pulses, and* $\text{counts}_{\text{max}}$ *for the best possible indistinguishable pulses that can be prepared by the physical setup.*

Weak coherent pulses have a theoretical maximum of 50% visibility (Rarity, Tapster, and Loudon 1997). Furthermore, the matching X-basis pulses are usually not utilised for communication, as they are utilsed to measure the relative phase drift in the X-basis states of the two sources.[20]

Now when it comes to the interpretation of the states in the X-basis, from the wave perspective there is no issue, as there is just a pulse composed of two pulses with some relative phase shift between them. After the attenuation process there is only one photon in the pulse composed of early and late timebins.

3.3.2 Physical implementation

The protocol is implemented in the following manner:

Both parties have access to an independent laser source. The AWGs of the parties have their clocks synchronized via an additional channel. The lasers' wavelengths are determined and matched via an external instrument that takes in the inputs from the raw laser output via beamsplitters. Just as in T12, pulses are "carved" using an intensity modulator, and phase encoding is carried out by EOPMs. Polarization controllers are placed before the attenuator and an electrically controlled polarization controller is used after the attenuators for the pulses from both parties (to ensure perfect polarization overlap). To ensure temporal overlap, optical delay lines are utilised before the attenuation process.

3.3.3 Contributions

Analysis of possible scenarios

Using the generalised code for beamsplitter calculations, we can alter the code to suit the MDI-QKD protocol. On brute-forcing through all the cases, we can easily see the cases where the bit must be discarded and where communication is possible.

Hands-on experience

Gained rudimentary experience in handling optic fiber connections and TCSPC software. Performed mean photon number determination and visibility determination.

Mean photon number determination To determine μ, we need to characterize the effect of the electro-optic attenuators on it as a function of their voltage. This was done by by cycling through a fixed range of voltage values for both attenuators and correlating it with the intensity of the pulse after attenuation (via a beamsplitter which is connected to a power meter), and with the counts at the detector (as a direct line of connection, no interference with the other laser's channel).

Visibility determination This was carried out by determining the HOM dip in the temporal region. Counts were taken for a fixed time period while changing the delay through the optical delay line.

[20] Why have X-basis pulses at all? It ensures that the input states satisfy the MUB criteria, which is shown to be completely secure.

4 Other work undertaken

4.1 Investigating the non-flipping variant of MDI-QKD protocol

On investigating further into the results obtained at Supplementary S1, we see that Bob flips its bit on receiving a singlet state to ensure that both have the same bits. If Bob does not perform the flipping of his bits, then the protocol serves as a lossy two-way simultaneous communication line.
If Alice wanted to send Bob the state 0 and Bob wanted to send the state 1 (the states which they want to send are flipped), then they could randomly choose their basis and be able to transmit to the other party 50% of the time. If their intended states to send were the same then it drops to 25% of the time.
All that the attacker knows is which bit indexes of $A \rightarrow B$ and $B \rightarrow A$ are the same and which are flipped, it does not know the contents themselves.

However as seen in Appendix A4, this alone leaks an uncomfortable amount of information.

Let the keys Alice transmits to Bob be $\{K_A\}$ and Bob transmits to Alice be $\{K_B\}$. Now, given that $\forall i$ Eve knows the values of $K_{A_i} \oplus K_{B_i}$, how can we use these pairs of keys? One trivial solution is to utilise only one set of keys generated, but this would defeat the purpose of using both $\{K_A\}$ and $\{K_B\}$.

Another way to utilise the two sets of keys is to use the second set of keys $\{K_B\}$ in a randomised manner, thus making it tougher for the attacker Eve to identify the counterpart of the key in $\{K_A\}$.
As a rough setup, consider the following scheme: Let us say that both parties wish to generate 1024-bit keys in a single key session. Both parties will first conduct 10^{19} key sessions, generating two sets of keys with 10^{27} keys in each. Next, the keys K_{A_1} and K_{B_1} are undisclosed and not used for one-time pad generation.
The rest of the keys in $\{K_A\}$ can be first used for one-time pad generation (say in the order of $K_{A_2}, K_{A_3}, ...$).
Next, we pick up K_{A_1} and convert it into a decimal number. A 1024 binary number will have $\log(2^{1024}) \simeq$ 308 digits as a decimal number. Since this is still a randomised decimal number, the 308 digit number will roughly have on average 30 zeroes, 30 ones,...,30 nines. So if we randomly choose 19 digits from the decimal representation of K_{A_1}, we can use it as a function to choose our one-time pad encoding string from $\{K_B\}$. The choosing of the 19 digits could even be done systematically ie. following a pattern since the digits themselves are randomised and only Alice and Bob knows the value of the function, not Eve. Repeats will occur as $C_{19}^{308} \simeq \times 10^{30}$, but such repeat cases can be easily discarded
The only hope for Eve to obtain information is to find the pair of K_{A_i} in K_B by XORing all ciphertexts $\{C_A\}$ with $\{C_B\}$, which is tough to do for 10^{19} keys.

Another way to utilise the $\{K_B\}$ is to verify the message sent by Alice to Bob and vice versa.
Eg. let us say Alice sends Bob $C_1 = K_{A_1} \oplus M_1$, Bob can verify if the message he has decoded is free of errors by sending Alice $C_2 = C_1 \oplus K_{A_1} \oplus K_{B_1}$, which Alice can then decrypt and verify.

On a similar note, there is ongoing research into the recycling of one-time pads: (Oppenheim and Horodecki 2005),(Damgård, Pedersen, and Salvail 2014).

4.2 Analysis of modified QKD protocols

I devised two variants of an existing MDI-QKD protocol and analysed their properties (not listed).

4.3 Attempts to build protocols using tritters:

A tritter is a 3 input, 3 output beamsplitter. Although they can have a wide range of outputs, the intention here was to keep the transformation matrix st. a single photon through any of the ports can come out of any of the output ports with equal probability.

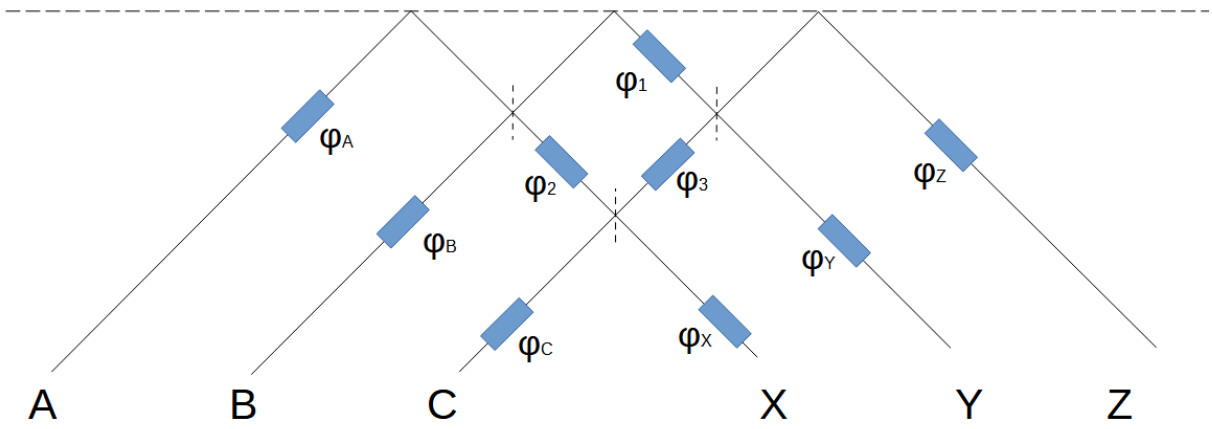


Figure 13: Construction of tritter. Top two BS have reflectivity 1/2, bottom has reflectivity 1/3.

This is a modification of the construction provided in Fig.4 of (Marek, Zeilinger, and Horne 1997), with the addition of all possible phase shift components for complete generality. The intention was to obtain a general form of the beamsplitter equation and use it to obtain interesting results. For example, the Discrete Fourier 3X3 matrix:

$$\sqrt{\frac{1}{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^1 & \omega^2 \\ 1 & \omega^2 & \omega^4 \end{pmatrix} \tag{36}$$

Where $\omega = \frac{2\pi}{3}$ It has the interesting property that when applied back to back it behaves as the swap matrix for inputs B and C. Due to the complexity of the equations obtained, numerical analysis was followed with little success in simplification.
Code is available here.

```
Optimization Results:
Success: True
Final error: 4.0974818490729144e-13

Optimized angles:
phi1: 4.745386 rad, 271.8906°, 145/96π
phi2: 3.757365 rad, 215.281145°, 61/51π
phi3: 0.988021 rad, 56.609454°, 28/89π
phiA: 2.789034 rad, 159.799856°, 87/98π
phiB: 1.218237 rad, 69.799856°, 19/49π
phiC: 4.975602 rad, 285.081001°, 19/12π
phiX: 6.019972 rad, 344.918999°, 182/95π
```

```
phiY: 2.937556 rad, 168.309544°, 72/77π
phiZ: 2.413957 rad, 138.309544°, 73/95π

Resulting matrix M1:
[[ 0.57735027-3.23698719e-14j  0.57735027-2.47199799e-14j
   0.57735027+5.02887774e-14j]
 [ 0.57735027+2.20934382e-14j -0.28867513+5.00000000e-01j
  -0.28867513-5.00000000e-01j]
 [ 0.57735027-7.53286322e-14j -0.28867513-5.00000000e-01j
  -0.28867513+5.00000000e-01j]]

Target matrix M2:
[[ 0.57735027+0.j   0.57735027+0.j   0.57735027+0.j ]
 [ 0.57735027+0.j  -0.28867513+0.5j -0.28867513-0.5j]
 [ 0.57735027+0.j  -0.28867513-0.5j -0.28867513+0.5j]]
```

A simpler construction can be considered:

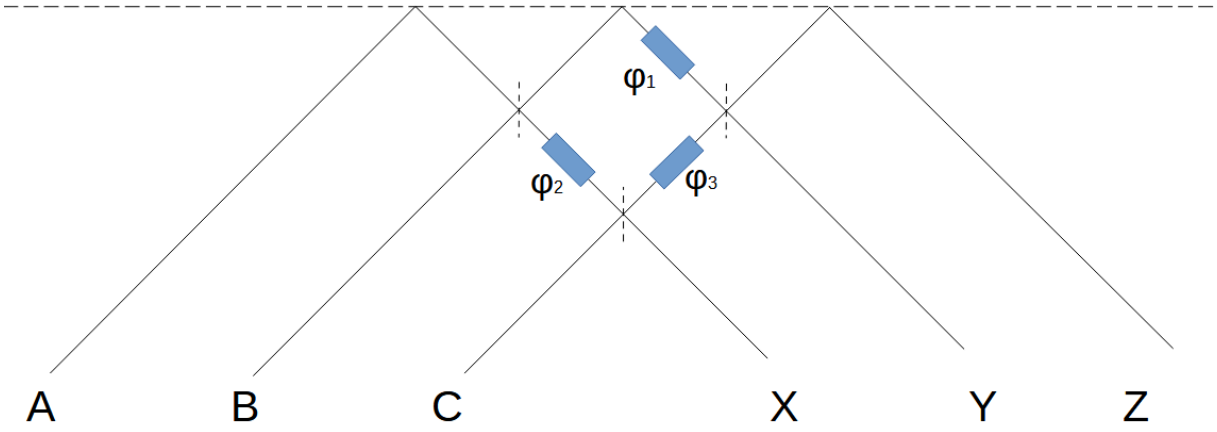


Figure 14: Construction of simplified tritter.

$$\begin{bmatrix} e^{i\phi_2} & ie^{i\phi_2} & i \\ ie^{i\phi_1} - e^{i(\phi_2+\phi_3)} & e^{i\phi_1} - ie^{i(\phi_2+\phi_3)} & ie^{i\phi_3} \\ -e^{i\phi_1} + ie^{i(\phi_2+\phi_3)} & ie^{i\phi_1} - e^{i(\phi_2+\phi_3)} & e^{i\phi_3} \end{bmatrix} \tag{37}$$

It is surprisingly straightforward to determine the transition matrix: M_{11} is the phase picked up from A to X, M_{21} is the phase picked up from A to Y (two terms since two paths) and so on.

An alternative (but arduous) method would be to "follow" the path of the photons through the tritter. In this case, it would be Action of BS on AB → Action of phase shift on AB → Action of bottom BS → Action of phase shift on C → Action of remaining BS, which translates to:

$$\left(\frac{1}{\sqrt{2}}\begin{bmatrix}1&0&0\\0&1&i\\0&i&1\end{bmatrix}\right) \times \left(\begin{bmatrix}1&0&0\\0&1&0\\0&0&e^{i\phi_3}\end{bmatrix}\right) \times \left(\sqrt{\frac{2}{3}}\begin{bmatrix}1&0&i\\0&1&0\\i&0&1\end{bmatrix}\right) \times \left(\begin{bmatrix}e^{i\phi_2}&0&0\\0&e^{i\phi_1}&0\\0&0&1\end{bmatrix}\right) \times \left(\frac{1}{\sqrt{2}}\begin{bmatrix}1&i&0\\i&1&0\\0&0&1\end{bmatrix}\right) \tag{38}$$

Since this is done and there are three variable parameters, I intended to create a protocol where Alice sends a "diffused" photon (photon with equiprobability of measurement on each of the three ports) with some relative phase, Bob uses the tritter and some internal shifts to manipulate the photon in such a way

that when Alice receives the photon back and decrypts, it will be able to extract information through its measurement.

Several other modifications can be thought of, but I did not investigate them during the summer project.

4.4 Further properties of the single photon systems

Adapted from (Gerry and Knight 2004a)

In a 1-D cavity with perfectly conducting walls at $z = 0$ and $z = L$, a single mode field that satisfies the Maxwell equations and boundary conditions is given by:

$$E_{x(z,t)} = \left(\frac{2\omega^2}{V\varepsilon_0}\right) q(t)\sin(kz) \tag{39}$$

V is the effective volume of the cavity and $q(t)$ is a time-dependent factor with dimension $[L]^1$ (eg. $q(t) = Le^{-i\omega t}$) Similarly we have

$$B_{y(z,t)} = \left(\frac{\mu_0\varepsilon_0}{k}\right)\left(\frac{2\omega^2}{V\varepsilon_0}\right)^{\frac{1}{2}} \dot{q}(t)\cos(kz) \tag{40}$$

From this we can define the Poynting vector $\vec{S} = \frac{1}{\mu_o}\vec{E}\times\vec{B}$, giving us

$$\vec{S} = \frac{\omega^2}{Vk}\frac{d}{dx}\Big(q(t)^2\Big) sin(kz)cos(kz)\hat{z} \tag{41}$$

From this, we can define energy density

$$u = \frac{1}{2}\left(\epsilon_0\left|\vec{E}\right|^2 + \frac{1}{\mu_0}\left|\vec{B}\right|^2\right) \tag{42}$$

Which when equated with the expressions above gives us

$$u = \frac{\omega^2}{V}\left[q^2(t)sin^2(kz) + \frac{\mu_0\epsilon_0}{k^2}\dot{q}^2(t)cos^2(kz)\right] \tag{43}$$

We can calculate the total current density using

$$\frac{\partial u}{\partial t} = -\nabla\cdot\vec{S} - \vec{J}\cdot\vec{E} \tag{44}$$

$$\frac{\partial u}{\partial t} = \frac{\omega^2}{V}\left[2\dot{q}(t)q(t)sin^2(kz) + 2\frac{\mu_0\epsilon_0}{k^2}\ddot{q}(t)\dot{q}(t)cos^2(kz)\right] \tag{45}$$

$$\nabla\cdot\vec{S} = \frac{2\omega^2}{V}q(t)\dot{q}(t)cos(2kz) \tag{46}$$

$$-\vec{J}\cdot\vec{E} = \frac{\omega^2}{V}\left[2\dot{q}(t)q(t)cos^2(kz) + 2\frac{\mu_0\epsilon_0}{k^2}\ddot{q}(t)\dot{q}(t)cos^2(kz)\right] \tag{47}$$

$$J_X = -\left(\frac{2\epsilon_0}{V}\right)^{\frac{1}{2}} \times \frac{\omega}{q(t)}cos(kz)tan(kz)\dot{q}(t)\left[q(t) + \frac{\mu_0\epsilon_0}{k^2}\ddot{q}(t)\right] \tag{48}$$

5 Glossary

bipartite system: System that is a composite of two systems. $H' = H_1 \otimes H_2$

bit runs: Sequences of 0′s and 1′s, eg. 0000, 010101, 0011101, etc.

BS: *beamsplitter.*

computational basis: $\{|0\rangle, |1\rangle\}$

gain: $\frac{\text{\# of Bob's detection events where Bob chooses the same basis as Alice}}{\text{\# of emitted signals by Alice for the case where both have matching bases}}$

lg: $\log_2(x)$

Mutually Unbiased Bases (MUBs): *Set of orthonormal bases st.* $|\langle e_i|f_j\rangle|^2 = \frac{1}{d} \forall i, j \in \{1, 2, 3..., d\}$.

passive eavesdropper: *An attacker who intercepts and records the transmissions and does not attempt to alter them to influence the outcomes of the protocol.*

photon number splitting attack: *In this attack, Eve uses a quantum non-demolition measurement of the number state of each pulse. If the pulse is single photon, it is blocked out. If it is a multi-photon pulse, Eve intercepts one of the photons and stores it (see (Simon et al. 2010)) while transmitting the rest. On basis reconciliation it can retrieve the information sent by Alice to Bob.*

positive semi-definite operator: *Operator* M *is positive semi-definite if* $\langle v|M|v\rangle \geq 0 \ \ \forall \ |v\rangle \in \mathbb{V}$.

POVM formalism: *(Limited to Quantum Information) A particular formalism for measurement operators. Given a set of measurement operators* $\{M_m\}$*, since* $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$*, we can define* $E_m = M_m^\dagger M_m$*. Since probabilities are non-negative, all* E_m *must be positive semi-definite. Unlike projective measurement operators, POVM operators can have eigenvalues other than 0 and 1. (See Nielsen and Chuang Pg.92) Further discourse in Nielsen and Chuang, Section 2.2.3 onwards.*

purification: *Given a mixed state* ρ_S*, by coupling with another system* T *we can obtain a pure state in* $\mathcal{H}_S \otimes \mathcal{H}_T$.

Let $\rho_S = \sum_i p_i |i_S\rangle\langle i_S|$*. Then* $|ST\rangle = \sum_i \sqrt{p_i}|i_S\rangle|i_T\rangle$ *will be a pure state. We can obtain the mixed state back by taking the partial trace of system* T $tr_T(|ST\rangle\langle ST|)$.

QBER: $\frac{\text{\# of erronous detection events by Bob when the basis match}}{\text{\# of detection events by Bob for matching bases}}$

quantum non-demolition measurement: Measurements in which the uncertainty of the observable does not increase after measurement or in the time evolution after the measurement.

st.: *such that.*

Stinespring dilation: *Given a quantum operation* $\mathcal{E}(\rho)$ *which need not be unitary, by coupling it with the environment we can define the quantum operation as a unitary operator in the combined space, and since we assume the environment does not interact with the system after the operation we can get the state of the system by tracing out the environment.* $\mathcal{E}(\rho) = tr_{env}\left[U\left(\rho_{system} \otimes \rho_{env}\right)U^\dagger\right]$.

Trace distance: $D(\rho, \sigma) = \frac{1}{2} * \text{tr}(|\rho - \sigma|)$

weak coherent state: Pulse with a low mean photon count wherein all the photons are in phase.

yield: *Probability that a detection event is observed by Bob in the matching basis* given *that a n-photon pulse was emitted by Alice in that matching basis.*

Bibliography

[1] kelalaka, 'Why Quantum Key Distribution (QKD) is impractical'. Accessed: Sep. 01, 2021. [Online]. Available: https://crypto.stackexchange.com/q/93830/110363

[2] C. H. Bennett and G. Brassard, 'Quantum cryptography: Public key distribution and coin tossing', *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014, doi: 10.1016/j.tcs.2014.05.025.

[3] A. Bocquet, R. Alléaume, and A. Leverrier, 'Optimal eavesdropping on quantum key distribution without quantum memory', *Journal of Physics A: Mathematical and Theoretical*, vol. 45, no. 2, p. 25305–25306, Dec. 2011, doi: 10.1088/1751-8113/45/2/025305.

[4] M. Lucamarini *et al.*, 'Efficient decoy-state quantum key distribution with quantified security', *Opt. Express*, vol. 21, no. 21, pp. 24550–24565, Oct. 2013, doi: 10.1364/OE.21.024550.

[5] knzhou, 'Why do coherent states have Poisson number distribution?'. [Online]. Available: https://physics.stackexchange.com/q/296106

[6] C. H. Bennett, G. Brassard, and J.-M. Robert, 'Privacy Amplification by Public Discussion', *SIAM Journal on Computing*, vol. 17, no. 2, pp. 210–229, 1988, doi: 10.1137/0217014.

[7] glS, 'Answer to "What is a proof for the principle of deferred measurement?"'. Accessed: Aug. 31, 2024. [Online]. Available: https://quantumcomputing.stackexchange.com/a/18255

[8] V. Scarani and R. Renner, 'Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing', *Physical Review Letters*, vol. 100, no. 20, May 2008a, doi: 10.1103/physrevlett.100.200501.

[9] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, 'Quantum cryptography', *Reviews of Modern Physics*, vol. 74, no. 1, pp. 145–195, Mar. 2002, doi: 10.1103/revmodphys.74.145.

[10] R. Renner, 'Security of quantum key distribution', in *Ausgezeichnete Informatikdissertationen*, 2005. [Online]. Available: https://api.semanticscholar.org/CorpusID:6888243

[11] V. Scarani and R. Renner, 'Security Bounds for Quantum Cryptography with Finite Resources'. [Online]. Available: https://arxiv.org/abs/0806.0120

[12] M. Koashi, 'Efficient quantum key distribution with practical sources and detectors'. [Online]. Available: https://arxiv.org/abs/quant-ph/0609180

[13] A. Gnanapandithan, L. Qian, and H.-K. Lo, 'Security flaws from time-varying active encoding in high-speed measurement-device-independent quantum key distribution', 2024, [Online]. Available: https://arxiv.org/abs/2404.14216

[14] J. G. Rarity, P. R. Tapster, and R. Loudon, 'Non-classical interference between independent sources', *Journal of Optics B-quantum and Semiclassical Optics*, vol. 7, 1997, [Online]. Available: https://api.semanticscholar.org/CorpusID:119101739

[15] J. Oppenheim and M. Horodecki, 'How to reuse a one-time pad and other notes on authentication, encryption, and protection of quantum information', *Phys. Rev. A*, vol. 72, no. 4, p. 42309–42310, Oct. 2005, doi: 10.1103/PhysRevA.72.042309.

[16] I. Damgård, T. B. Pedersen, and L. Salvail, 'How to re-use a one-time pad safely and almost optimally even if P = NP', *Natural Computing: An International Journal*, vol. 13, no. 4, pp. 469–486, Dec. 2014, doi: 10.1007/s11047-014-9454-5.

[17] Marek, A. Zeilinger, and M. A. Horne, 'Realizable higher-dimensional two-particle entanglements via multiport beam splitters', *Phys. Rev. A*, vol. 55, no. 4, pp. 2564–2579, Apr. 1997, doi: 10.1103/PhysRevA.55.2564.

[18] C. Gerry and P. Knight, 'Field quantization', in *Introductory Quantum Optics*, Cambridge University Press, 2004a, pp. 10–42.

[19] C. Simon *et al.*, 'Quantum Memories. A Review based on the European Integrated Project "Qubit Applications (QAP)"', *The European Physical Journal D*, vol. 58, no. 1, pp. 1–22, May 2010, doi: 10.1140/epjd/e2010-00103-y.

[20] G. M. D'Ariano, C. Macchiavello, and P. Perinotti, 'Superbroadcasting of mixed states', *Physical Review Letters*, vol. 95, no. 6, p. 60503–60504, Aug. 2005, doi: 10.1103/PhysRevLett.95.060503.

[21] aquohn, 'Answer to "Why is the operation in Nielsen and Chuang's Section 8.5 not a quantum operation?"'. Accessed: Jul. 16, 2024. [Online]. Available: https://quantumcomputing.stackexchange.com/a/30267

[22] C. A. Fuchs and A. Peres, 'Quantum State Disturbance vs. Information Gain: Uncertainty Relations for Quantum Information', *Physical Review A*, vol. 53, no. 4, pp. 2038–2045, Apr. 1996, doi: 10.1103/PhysRevA.53.2038.

[23] W. Lawrence, 'Perfect Secrecy of one time pad'. [Online]. Available: https://math.umd.edu/~lcw/OneTimePad.pdf

[24] Rick, 'Stream Cipher Reuse: A Graphic Example'. Accessed: Jul. 17, 2024. [Online]. Available: https://cryptosmith.com/2008/05/31/stream-reuse/

[25] E. Dawson and L. Nielsen, 'Automated Cryptanalysis of XOR Plaintext Strings', *Cryptologia*, vol. 20, pp. 165–181, 1996, [Online]. Available: https://api.semanticscholar.org/CorpusID:19577865

[26] H.-K. Lo, M. Curty, and B. Qi, 'Measurement-Device-Independent Quantum Key Distribution', *Physical Review Letters*, vol. 108, no. 13, Mar. 2012, doi: 10.1103/physrevlett.108.130503.

[27] S. Tanzilli *et al.*, 'PPLN waveguide for quantum communication', *The European Physical Journal D - Atomic, Molecular and Optical Physics*, vol. 18, no. 2, pp. 155–160, Feb. 2002, doi: 10.1140/epjd/e20020019.

[28] Avraham, 'Answer to "Probability that a sample comes from one of two distributions"'. Accessed: Sep. 18, 2024. [Online]. Available: https://math.stackexchange.com/a/825514

[29] C. Gerry and P. Knight, 'Beam splitters and interferometers', in *Introductory Quantum Optics*, Cambridge University Press, 2004b, pp. 135–149.

[30] S. M. Barnett and J. A. Vaccaro, Eds., *The Quantum Phase Operator: A Review*, 1st ed. CRC Press, 2007. doi: 10.1201/b16006.

[31] A. M. Brańczyk, 'Hong-Ou-Mandel Interference'. [Online]. Available: https://arxiv.org/abs/1711.00080

[32] C. Gerry and P. Knight, 'Coherent states', in *Introductory Quantum Optics*, Cambridge University Press, 2004c, pp. 43–73.

[33] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, 'Invited Review Article: Single-photon sources and detectors', *Review of Scientific Instruments*, vol. 82, no. 7, p. 71101–71102, 2011, doi: 10.1063/1.3610677.

APPENDIX A

A.1 No cloning theorem

The no-cloning theorem states that it is impossible to create an independent copy of an unknown state. Proofs are as follows:

1. *This proof shows that no such unitary operation exists for a pure state.*
Let there exist a unitary operation s.t. $U|\psi\rangle|E\rangle = |\psi\rangle|\psi\rangle$. Then $U|0\rangle|E\rangle = |0\rangle|0\rangle$, $U|1\rangle|E\rangle = |1\rangle|1\rangle$. Now let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, |\alpha|^2 + |\beta|^2 = 1$.
Applying this unitary cloning operator gives:

$$U(\alpha|0\rangle + \beta|1\rangle)|E\rangle = \alpha|00\rangle + \beta|11\rangle \tag{49}$$

However:

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle \tag{50}$$

If α and β are non-zero, we get a contradiction. Thus proved.

Thus, it is clear to see that we can only clone states which are already known to be in the computational basis (or orthogonal states, since we can always define a unitary operator that transforms these computational basis states to an arbitrary basis), and not for unknown arbitrary states.

We cannot construct workarounds for mixed states as well. One straightforward way to show this is to "purify" the mixed state into a pure state of a composite system. If we assume that there exists a unitary cloning operator for mixed states $U(\rho_{system} \otimes \rho_{env})\, U^\dagger = \rho_{system} \otimes \rho_{system}$, then we should be able to couple the system with another system R to purify it, thus obtaining a universal unitary cloning operator for pure states. But since we have shown it's impossible for pure states, we get a contradiction.

Entangled states are dealt with as well since all states are either pure or mixed.

If we assume that there exists a non-unitary cloning operator, via Stinespring Dilation we can convert the non-unitary operator to a unitary one by coupling a 'dummy' system to our qubit system. After this, the proof by contradiction follows for the mixed states.

As QKD protocols rely on the no-cloning theorem, it is necessary to eliminate all cloning strategies. However the generalised version of this theorem (the no-broadcast theorem) does not hold if we start with multiple copies of the same state (D'Ariano, Macchiavello, and Perinotti 2005). Similar issues may exist for other assumptions (aquohn 2023).

A.2 Indistinguishability of non-orthogonal states on measurement

(*Reworked from Nielsen and Chuang Box 2.3*)

Although this proof uses POVM formalism, it can be done for generalised measurement operators as well.

Let us assume a set of measurement operators exist $\{M_1, M_2\}$ ($\{M_j\}$ for general purposes) which can differentiate $|\psi_1\rangle, |\psi_2\rangle$ ($\{|\psi_i\rangle\}$ for generalisation) by giving a measurement result j when M_j is applied. We assume that once the result is obtained there exists some rule $f(j)$ that allows us to map the result to the state.
For example, if $|\psi_i\rangle$ is prepared then we will get $f(j) = 1$, and never $f(j) = 2$.

A simple setup could be:
Given states $|\psi_1\rangle, |\psi_2\rangle$, we can construct projective measurement operators $P_0 = |\psi_1\rangle\langle\psi_1|, P_1 = |\psi_2\rangle\langle\psi_2|$ and the rule $f(0) = 1, f(1) = 2$.
Now if we naïvely model the P_0 operator with the '0' detector and similarly with P_1, then on measuring state $|\psi_1\rangle$ the probability of the '0' detector clicking will be 1 the obtained state will be $|\psi_1\rangle$.

The proof is as follows:
Given states $|\psi_1\rangle, |\psi_2\rangle$, we have $\{M_j\}$. Constructing $E_i = \sum_{j:f(j)=i} M_j^\dagger M_j$, we can say

$$\langle\psi_1|E_1|\psi_1\rangle = 1, \langle\psi_2|E_2|\psi_2\rangle = 1 \tag{51}$$

Since $\sum_i E_i = \mathbb{I}$,

$$\langle\psi_1|E_2|\psi_1\rangle = 0, \langle\psi_2|E_1|\psi_2\rangle = 0 \tag{52}$$

$\langle\psi_1|E_2|\psi_1\rangle = \langle\psi_1|\sqrt{E_2}\sqrt{E_2}|\psi_1\rangle = \langle\phi|\phi\rangle = 0$, which is only possible if $\sqrt{E_2}|\psi_1\rangle = |\phi\rangle$ is the zero vector.
To make the states non-orthogonal, let $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_{1\perp}\rangle$ and $|\beta|^2 < 1$.

$$\langle\psi_2|E_2|\psi_2\rangle = |\alpha|^2\langle\psi_1|E_2|\psi_1\rangle + |\beta|^2\langle\psi_{1\perp}|E_2|\psi_{1\perp}\rangle = |\beta|^2\langle\psi_{1\perp}|E_2|\psi_{1\perp}\rangle \tag{53}$$

But since $\langle\psi_{1\perp}|E_2|\psi_{1\perp}\rangle \leq \sum_i \langle\psi_{1\perp}|E_i|\psi_{1\perp}\rangle = 1$ (Since the state must resolve to *some* value on measurement/sum of probabilities is 1.), the results we obtain are contradictory, since we get:

$$\langle\psi_2|E_2|\psi_2\rangle = 1 \text{ AND } \langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\langle\psi_{1\perp}|E_2|\psi_{1\perp}\rangle \leq |\beta|^2 < 1 \tag{54}$$

Thus proved.

Although we cannot "one-shot", we can still have "unreliable" distinguishability of non-orthogonal states wherein there is a non-zero probability that our measurement process results in a 'garbage' answer (*See Nielsen and Chuang Pg.92*), however for QKD purposes this process will not be helpful: in the non-zero cases where the interceptor measures a 'garbage' answer, it will be forced to guess the original state and prepare it accordingly, causing the QBER to spike beyond the threshold.

A.3 Non-orthogonal states cannot be distinguished without disturbance

(Reworked from Nielsen and Chuang Proposition 12.18)

Let us assume we want to obtain information regarding the non-orthogonal states $|\psi\rangle$ and $|\varphi\rangle$. We could do this by devising a unitary operator which does the following:

$$U(|\psi\rangle|E\rangle) = |\psi\rangle|v\rangle, U(|\varphi\rangle|E\rangle) = |\varphi\rangle|v'\rangle \tag{55}$$

Where $|E\rangle$ is a pre-defined state from our 'interceptor' system. Since the unitary operator results in different independent states for each of the non-orthogonal states, we can then analyse the states separately. However, if we now take the inner products of the inputs and the outputs:

$$(\langle\varphi|\langle E|)U^\dagger U(|\psi\rangle|E\rangle) = \langle\varphi|\psi\rangle\langle E|E\rangle = \langle\varphi|\psi\rangle\langle v'|v\rangle \tag{56}$$

$$\langle E|E\rangle = \langle v'|v\rangle \tag{57}$$

Which implies $|v\rangle$ and $|v'\rangle$ but be identical, giving us no information.

Just as in Appendix A1, we can use Stinespring dilation to extend this proof to non-unitary quantum operations.
The proof shows that it is impossible to extract information regarding non-orthogonal without disturbing

the state, thus information extraction *implies* disturbance. This works to the benefit of QKD as it forces passive eavesdroppers to disturb the system, which can then be quantified (Fuchs and Peres 1996).

A.4 One-time pad

This is a **provably** perfectly secret method of encryption.

A.4.1 Procedure:

Let us say that A wants to send the message $M \in \{0,1\}^x$ to B.
A and B share a completely random bitstring $K \in \{0,1\}^y$.
Ensuring that x=y, A encodes its message into the cipher text $C = M \oplus K$.
B receives the cipher text and applies the same bitwise XOR operation. Since $C \oplus K = K \oplus M \oplus K = M$, B is able to decode the message.

A.4.2 Proof: *Reworked from Lawrence Washington's notes (Lawrence, n.d.).*

(Note: $\{m\}, \{k\}, \{c\}$ refer to the set of all possible plaintexts, keys, and ciphertexts. m, k, c refers to a particular plaintext m, a particular key k, and a particular ciphertext c.)
This system is perfectly secret if knowing the ciphertext gives out no information about the message. We can quantify this in the following manner:
Let us say that A can transmit any of the plaintexts $\{m\}$ as a message M, and the probability of A transmitting the plaintext m is given by $P(M = m)$. Now, if we wish to transmit a plaintext m and choose a random key k, then the ciphertext will be $c = m \oplus k$ $(C = c)$. We can now restate the earlier statement on perfect security as

$$P(M = m|C = c) = P(M = m) \tag{58}$$

For a message of length n we can construct $N = 2^n$ possible keys (all as results of an n-bit random sequence) each with probability $\frac{1}{N}$, and so there are N such ciphertexts possible with probability $\frac{1}{N}$ as well.
Since our key choice is random and not correlated to the message,

$$P(C = c) = \sum_k P(C = c \cap K = k) \tag{59}$$

Given a plaintext m and a key k, we know that this can give rise to only a unique ciphertext c. Similarly, given a ciphertext c and a key k, due to the bitwise XOR operation it can only give rise to a unique decoded message, plaintext m.
As a result, since $P(C = c \cap K = k)$ is the probability of having generating the key k and the ciphertext c, this *must* be equivalent to the probability of generating the key k and encoding the message m, which is to say:

$$P(C = c \cap K = k) = P(M = c \oplus k \cap K = k) \tag{60}$$

Since the message and key generation are independent,

$$\begin{aligned} P(M = m \cap K = k) &= P(M = c \oplus k)P(K = k) \\ &\Rightarrow P(M = c \oplus k)\left(\frac{1}{N}\right) \end{aligned} \tag{61}$$

$$P(C = c) = \sum_k P(C = c \cap K = k) = \sum_k \frac{1}{N} \times P(M = c \oplus k) = \frac{1}{N} \tag{62}$$

It equates to $\frac{1}{N}$ because fixing the ciphertext c and iterating through all the keys will give you all possible messages, including the plaintext $c \oplus k$.

We can extend the same reasoning used for c and k to c and m. The probability of generating the ciphertext c AND transmitting the message m is equivalent to the probability of generating the key k AND transmitting the message m.

$$P(C = c \cap M = m) = P(K = m \oplus c \cap M = m) \tag{63}$$

Thus, probability of the message being m given that the ciphertext is c is equal to:

$$\begin{gathered} P(M = m|C = c) = \frac{P(C = c \cap M = m)}{P(C = c)} \\ \Rightarrow N \times P(K = m \oplus c \cap M = m) = N \times P(M = m)P(K = c \oplus m) \\ \Rightarrow P(M = m) \end{gathered} \tag{64}$$

$$P(M = m|C = c) = P(M = m) \tag{65}$$

Thus proved.

A.4.3 Properties:

The one-time pad is perfectly secret only for one time uses. For example, if messages m_1 and m_2 are encrypted by the same key k, then the attacker can simply XOR the ciphertexts, giving $c_1 \oplus c_2 = m_1 \oplus k \oplus k \oplus m_2 = m_1 \oplus m_2$. To see why this is a bad idea:

Figure 15: Easy to guess what the two messages were. (Rick 2008)

Automated attacks can be performed based as well (Dawson and Nielsen 1996).

As a result, messages longer than the key will force the reuse of parts of the key as well.

A.5 Decoy state technique

Reworked from (Lo, Curty, and Qi 2012).

The majority of the QKD protocols utilise single photon sources in their original formalism, from BB84 to T-12 and MDI-QKD.

Efficient and reliable single photon sources have so far not been achieved[21]. To utilise the currently available weak coherent sources, we need to make sure that no attacks are possible. We cannot use such sources directly as there are several attacks possible such as the photon number splitting attack.

A consequence of any such attack would be for the gain and yield of single photon pulses to drop to zero, since all counts observed by Bob would only be due to the multi-photon pulses.

We can use this to our advantage: instead of sending photons associated with a fixed laser power/intensity, we can modulate the laser power selectively so as to produce photons associated with a range of different intensities. Out of these, we use only one intensity for key generation, the rest are used as decoys to detect the eavesdropper.

How would this work?

The only difference between these decoy states and the key generation states is that they arise from different intensities; their frequency and periodicity are the same. So given a pulse as it is, it is impossible to deterministically determine the intensity that gave rise to the pulse (for any attacker without information of which intensity was used).[22]

Furthermore, phase-randomised coherent states give rise to poissonian distribution of photon number states (knzhou 2016). As done for T-12 , we can calculate the gain associated with an intensity as the following:

$$Q_\mu = \sum_n^\infty \frac{Y_n p(n)}{\text{prob. of Alice and Bob choosing matching basis}} \tag{66}$$

Y_n is the yield for an n-photon pulse. The sequence can be truncated at will[23].

Since the gain only gives us the probability of detection given that Alice emits a pulse and does not eliminate the cases of erroneous detections due to dark counts, we need to calculate the QBER as well. A simple case of erroneous counts even in matching bases is the following: Alice sends 0_Z and $n = 1$, Bob chooses the Z basis, but the pulse in that channel gets absorbed, while random thermal process gives rise to a photon in the opposite channel, leading Bob to detect 1_Z.)

The QBER would simply be:

$$Q_\mu E_\mu = \sum_n^\infty \frac{Y_n p(n) e(n)}{\text{prob. of Alice and Bob choosing matching basis}} \tag{67}$$

$e(n)$ is the QBER of a n-photon signal.

Now, we can see that for a n-photon pulse, the QBER and yield do not depend on the intensity.

[21] SPDC sources exist but have a pair production rate of 10^{-6} (Tanzilli et al. 2002).

[22] It must be noted that Eve can (obviously) make educated guesses since the probability by which an intensity is chosen is made public along with the intensities being used as well.(Avraham 2014). This causes further complications whose analysis was not covered in my readings.

[23] This is a slight deviation from the paper linked, as I am following the procedure linked in the T-12 paper regarding the calculation of gain. It seems that for the decoy state paper they are only considering the cases where the basis match, leading to the omission of the denominator. Also, the formulation above seems to be more 'rigorous' since we are calculating the conditional probability p((Getting a detection)|Basis match) and the definitions of Y_n incorporates the condition of matching bases.

This stems from our earlier argument of the indistinguishability of decoy and standard states. Thus, given a range of intensities we can calculate their gain and QBER separately during the calibration process.

Now, in the real-time execution of the protocol, if Eve blocks out the single photon pulses, then it is easy to see that this will affect the QBER and gain of the intensities to different extents since each intensity has a different probability of generating a single photon pulse. In the error correction and verification step, for the 'sacrificed' subset of bits we can calculate the observed QBER and gain for the different intensities. Having already done the calibration, if we observe a substantially higher decrease in gain for the lower intensities compared to the higher intensities then we can be fairly confident of tampering having taken place. All that remains is making the proof rigorous.

Now, at most Eve can perform attacks only on the multi-photon pulses. By reducing the mean photon counts/intensities we can reduce the occupances of these pulses. This reduction will lead a to reduction in single-photon pulses as well, but can be worked with using currently available hardware.

A.6 Beamsplitter formalism

Reworked from (Gerry and Knight 2004b)

Why classical formalism ≠ quantum mechanical formalism of beamsplitters

If we follow the classical treatment of a beamsplitter wherein a BS splits the incoming light into two light waves into two light waves of equal intensity for a 50:50 BS, (or some arbitrary ratio depending on the reflectance:transmittance ratio of the BS), then let us take the following setup:

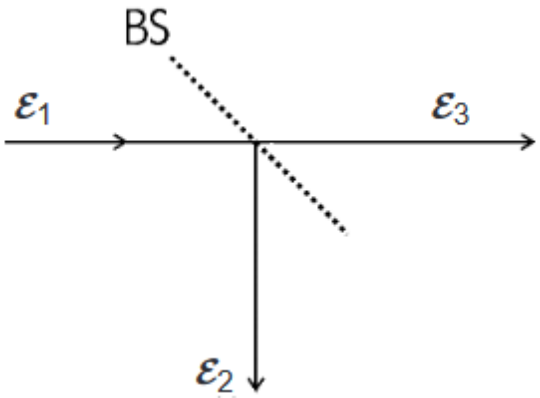


Figure 16: Classical formalism of the BS.

Let a classical light field of amplitude A_1 be incident. Taking the reflectance and transmittance coeffs. as $r, t \in \mathbb{C}$, we see $A_2 = rA_1$ and $A_3 = tA_1$. Through conservation of energy $|A_1|^2 = |A_2|^2 + |A_3|^2$, thus $|r|^2 + |t|^2 = 1$.

To develop a quantum mechanical formalism of BS, we use creation and annihilation operators. $\hat{a}_2 = r\hat{a}_1, \hat{a}_3 = t\hat{a}_1$. We know that $\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij}$ refer to section below),but then $\left[\hat{a}_2, \hat{a}_2^\dagger\right] = |r|^2 \neq \delta_{ij}$ and $\left[\hat{a}_3, \hat{a}_3^\dagger\right] = |t|^2 \neq \delta_{ij}$. If both are satisfied, then $|r|^2 + |t|^2 = 1$ is not, and vice versa.

Thus, the classical formalism does not translate to the quantum mechanical formalism.

Why creation and annihilation operators?

Continuing from the expressions of electric field and magnetic field stated earlier and taking $p(t) = \dot{q}(t)$ via unit mass, we can define the Hamiltonian by integrating the energy density expression over the entire volume ie. $H = \left(\frac{1}{2}\right) \int udV$ we get $H = \left(\frac{1}{2}\right)(p^2 + \omega^2 q^2)$. Since this expression is mathematically equivalent to the quantum harmonic oscillators, the ladder operator formalism can be used here as well, except here

it can be interpreted as the creation and annihilation of photons.
To see this:

$$\hat{a} = \frac{1}{2\hbar\omega}(w\hat{q} + i\hat{p}), \hat{a}^\dagger = \frac{1}{2\hbar\omega}(w\hat{q} - i\hat{p}) \tag{68}$$

$$H = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \tag{69}$$

$\widehat{H}|n\rangle = E_n\ |n\rangle$

Using this, we can use the same procedure as we do for ladder operators:
$H|n\rangle = \hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})|n\rangle$
$H(\hat{a}^\dagger\ |n\rangle) = \hbar\omega(\hat{a}^\dagger\hat{a}\hat{a}^\dagger + \frac{1}{2}\hat{a}^\dagger)\ |n\rangle$
$\hbar\omega[(\hat{a}^\dagger\hat{a} - \hat{a}^\dagger) + \frac{1}{2}\hat{a}^\dagger]|n\rangle = E_n\hat{a}^\dagger|n\rangle$ (Since $[\hat{a}, \hat{a}^\dagger] = \mathbb{I}$)
$\hbar\omega(\hat{a}^\dagger\hat{a} + \frac{1}{2})(\hat{a}^\dagger)|n\rangle = (E_n + \hbar\omega)\hat{a}^\dagger\ |n\rangle$

Furthermore $\hat{a}^\dagger\hat{a} = n|n\rangle$, making it the number operator.

Lastly, the normalization constant of $|n\rangle$ is $\sqrt{n}$.

A.6.2 Number state-phase uncertainty relation

Since $|n\rangle$ is normalized, $\langle n|n\rangle = 1$ and we can find expectation values. Using the results obtained in the single photon section, $\langle E_x\rangle = 0, \langle E_x^2\rangle = 2E_0^2\sin^2(kz) \times \left(n + \frac{1}{2}\right)$, thus $\Delta E_x = \sqrt{2E_0}\sin(kz)\sqrt{n + \frac{1}{2}}$
We see an uncertainty for all values of n, including when n=0. This is expected as the number state operator and E_x do not commute: $\left[\hat{n}, \widehat{E_x}\right] = E_0\sin(kz)(\hat{a}^\dagger - \hat{a})$.
Using the generalized uncertainty relation $\Delta C\Delta D \geq \frac{\langle[C,D]\rangle}{2}$ we get:

$$\Delta n\Delta E_x \geq |\sin(kz)\|\langle\hat{a}^\dagger - \hat{a}\rangle|E_0 \tag{70}$$

.

From this an "informal" uncertainty relationship b/w the phase of the field and the number state, stated as $\Delta n\Delta\phi \geq 1$. Making this formal has proved contentious (Barnett and Vaccaro 2007).

A.6.3 Beamsplitter equations

A valid beamsplitter equation is of the form:

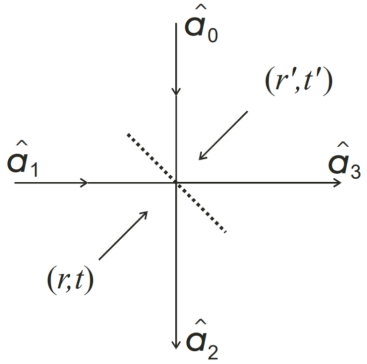


Figure 17: Correct formalism of the BS.

$$\begin{bmatrix} a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} t' & r \\ r' & t \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \tag{71}$$

$$\text{Where } |r'| = |r|, |t'| = |t|, |r|^2 + |t|^2 = 1, r^*t' + r't^* = 0, r^*t + r't'^* = 0 \tag{72}$$

The most commonly used equation is of a 50:50 splitter with $\frac{\pi}{2}$ on reflection:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix}\ |0\rangle_0\ |0\rangle_1 \xrightarrow{\text{BS}} |0\rangle_2\ |0\rangle_3 \tag{73}$$

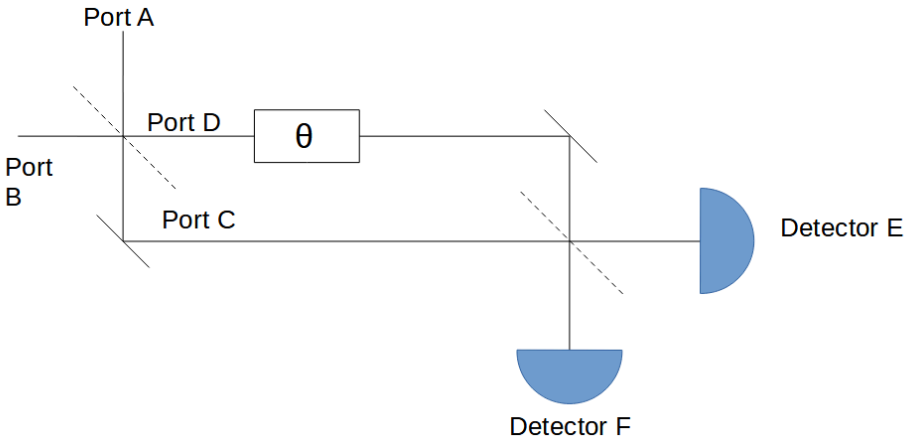


Figure 18: Setup for "self" interference.

Let us take the following setup, with input $|0\rangle_A\ |1\rangle_B$:

$$|0\rangle_A\ |1\rangle_B \xrightarrow{\text{BS}_1} \frac{i\hat{a}_C^\dagger + \hat{a}_D^\dagger}{\sqrt{2}}\ |0\rangle_C\ |0\rangle_D \xrightarrow{\text{EOPM}} \frac{1}{\sqrt{2}}\big(i|1\rangle_C|0\rangle_D + e^{i\theta}|0\rangle_C\ |1\rangle_D\big) \tag{74}$$

$$\xrightarrow{\text{BS}_2} \frac{1}{2}\big[(e^{i\theta}-1)|1\rangle_E\ |0\rangle_F + i(e^{i\theta}+1)|0\rangle_E\ |1\rangle_F\big] \tag{75}$$

We see that back-to-back beamsplitter operations give σ_X.

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix} \times \frac{1}{\sqrt{2}}\begin{bmatrix}1 & i\\ i & 1\end{bmatrix} = i\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} \tag{76}$$

A.6.4 Hong-Ou Mandel effect

From the formulation above, HOM simply becomes a simple case:

$$|1\rangle_A\ |1\rangle_B = \hat{a}_A^\dagger\hat{a}_B^\dagger\ |0\rangle_A\ |0\rangle_B = \frac{1}{2}\big[i\hat{a}_C^\dagger\hat{a}_C^\dagger + \hat{a}_C^\dagger\hat{a}_D^\dagger - \hat{a}_D^\dagger\hat{a}_C^\dagger + i\hat{a}_D^\dagger\hat{a}_D^\dagger\big]|0\rangle_c\ |0\rangle_D \tag{77}$$

$$= \frac{i}{\sqrt{2}}[|2\rangle_c\ |0\rangle_D + |0\rangle_C\ |2\rangle_D] \tag{78}$$

This only holds if the input photons are indistinguishable (polarization, temporally, spatially). For intermediate cases, a thorough analysis needs to be conducted (Brańczyk 2017).

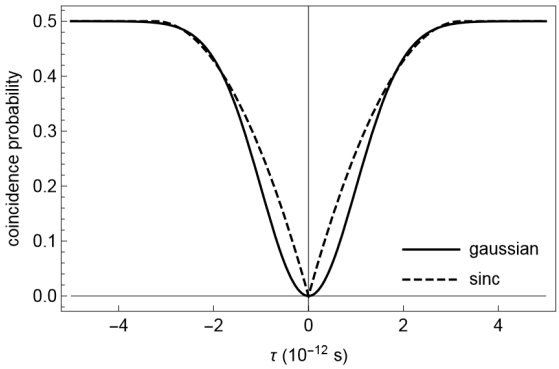


Figure 19: Probability of getting clicks in both ports as a function of temporal shift.

We can utilise this "dip" for calibrating the optical delay to the input pulses from the two different lasers in MDI-QKD.

A.6.5 Impossibility of a passive beam combiner

It seems to be impossible to construct a beam combiner that does not alter the properties of the incoming light pulses. For example, let us say the input to a beam combiner is $|1\rangle_A\ |1\rangle_B$. The output must combine, so we can take it as $|2\rangle_C\ |0\rangle_D$ This is only possible if the matrix is $\begin{bmatrix}1 & 1\\ 0 & 0\end{bmatrix}$ This is not a valid beamsplitter equation as $|r'| \neq |r|$, along with failing other criteria.

It is possible to construct a beam combiner provided that the inputs are polarized. For example, if we take a beamsplitter that reflects $|H\rangle$ and transmits $|V\rangle$, then passing $|H\rangle$ through one port and $|V\rangle$ through another is sufficient.

A.6.6 Coherent states

The definition of coherent states and the derivation of its formalism require further reading. I have only utilised the results here from (Gerry and Knight 2004c).

For a coherent state $|\alpha\rangle$, since it is the eigenstate of the annihilation operator we get $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$. Applying the number state operator gives us $\langle\hat{n}\rangle = \overline{n} = |\alpha|^2$. This is the mean number of photons in the coherent state.

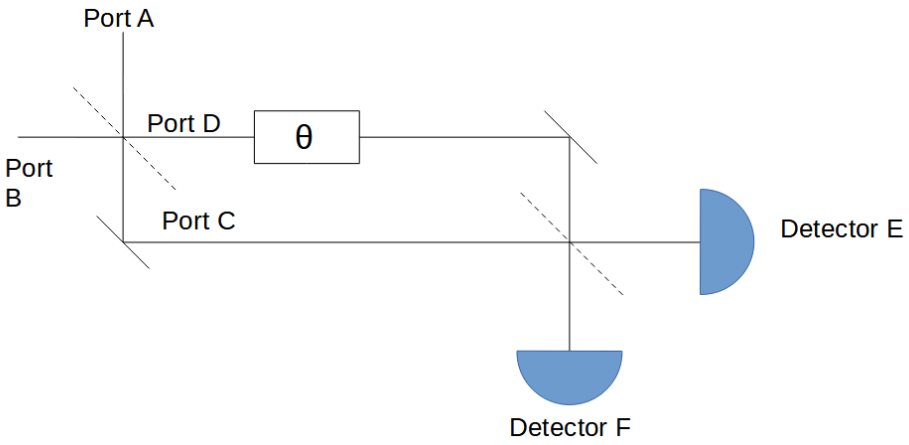
$$\Delta n = \langle\hat{n}^2\rangle - \langle\hat{n}\rangle^2 = \sqrt{n} \tag{79}$$

$$|\alpha\rangle = D(\alpha)|0\rangle, \text{where } D(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right) \tag{80}$$

Thus,

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{81}$$

Using the same setup for single-photon interferometry, we can obtain an expression for coherent states as well:



,

If input of coherent states is from port B:

$$|0\rangle_A\ |\alpha\rangle_B \rightarrow |\frac{i(e^{i\theta}+1)\alpha}{\sqrt{2}}\rangle_E|\frac{(e^{i\theta}-1)\alpha}{\sqrt{2}}\rangle_F \tag{82}$$

A.7 Entropic relations

For a probability distribution X, its entropy is $H(X) = -\sum_i p_i \lg(p_i)$
For two probability distributions X,Y their joint entropy (ie. "uncertainty" of (X,Y)) is $H(X,Y) = -\sum_{i,j} p_{ij} \lg(p_i j)$.
Conditional entropy $H(X|Y) = H(X,Y) - H(Y)$.

Further properties were referred from Chap.8 of *Nielsen and Chuang.*

A.8 Characterisation of quantum operations

Reworked from Chap.8 of Nielsen and Chuang Only what is needed is covered here. Proofs are present in the reference.

We define a mapping from ρ to ρ' by $\mathcal{E}(\rho)$. All such mappings are CPTP maps (complete positive trace-preserving).

As the name suggests:
1. $\mathrm{tr}(\rho) = \mathrm{tr}(\mathcal{E}(\rho))$
2. $\mathcal{E}(\alpha\rho + \beta\sigma) = \alpha\mathcal{E}(\rho) + \beta\mathcal{E}(\sigma)$
3. If $A \geq 0, \mathcal{E}(A) \geq 0$
4. If $A \geq 0, (\mathbb{I}_R \otimes \mathcal{E})(A) \geq 0$ where $\dim(\mathbb{I}_R) = R, R \in \mathbb{Z}^+ - \{0\}$

The results used:
- $D\big(U\rho U^\dagger, U\sigma U^\dagger\big) = D(\rho,\sigma)$
- $D(\rho,\sigma) = \max_{P\in POVM} \mathrm{tr}(P(\rho-\sigma))$
- Triangle inequality holds: $D(\rho,\tau) \leq D(\rho,\sigma) + D(\sigma,\tau)$
- $D(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \leq D(\rho,\sigma)$
- $D\big(\rho^A,\sigma^A\big) \leq D\big(\rho^{AB},\sigma^{AB}\big)$

APPENDIX B : Instrumentation

B.1 Laser

> *Either one chooses a wavelength around 800 nm where efficient photon counters are commercially available, or one chooses a wavelength compatible with today's telecommunication optical fibres, i.e. near 1300 nm or 1550 nm. The first choice requires free space transmission or the use of special fibres, hence the installed telecommunication networks can't be used. The second choice requires the improvement or development of new detectors, not based on silicon semiconductors, which are transparent above 1000 nm wavelength.*
>
> — (Gisin et al. 2002)

Since the short term goal would be incorporating the QKD infrastructure into the current telecommunications infrastructure, the 1550 nm laser is the convention.

B.2 Intensity Modulator

The intensity modulator is a classical MZ interferometer that has an EOPM on one of the arms. The beamsplitter at the end gives two outputs which correspond to two ports; one we use for power monitoring and the other for the optical pulses. Usually set at destructive phase unless for phase generation, at which the number of photons in the initial pulse is modulated by setting some phase; 0 implies all photons in that region pass, pi/2 implies half in that region pass, and so on. Refer to calculations.

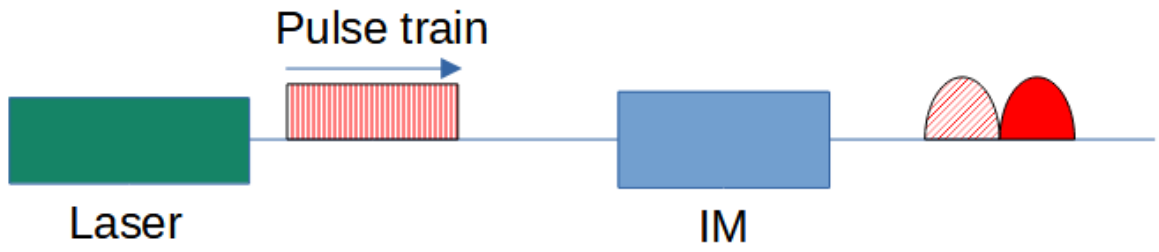


Figure 20: Action of intensity modulator.

Square pulses are shown as elliptical for illustration purposes.
Shaded pulse is the late pulse, the filled pulse is the early pulse.

B.3 Electro-optic Phase Modulator

Reworked from Fundamentals of Photonics by Saleh Section 21.1

An example of EOPM acting for π is illustrated below:

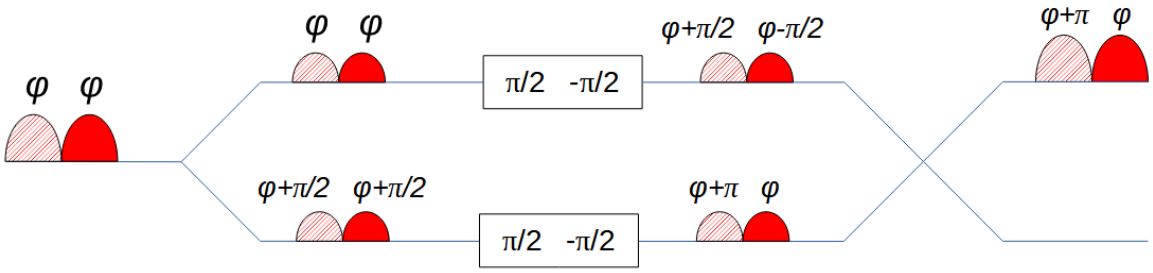


Figure 21: Action of EOPM for pi shift.

The EOPM acts in an unintuitive manner, one would expect it to simply act on one half of the incoming waveform and leave the phase of the other waveform unchanged. However, this would cause the gap b/w the two pulses to increase as the phase modulation will have some operational time. Having such a symmetrical application of phase modulation prevents change in the gap b/w the two pulses.

B.4 Delay Line Interferometer

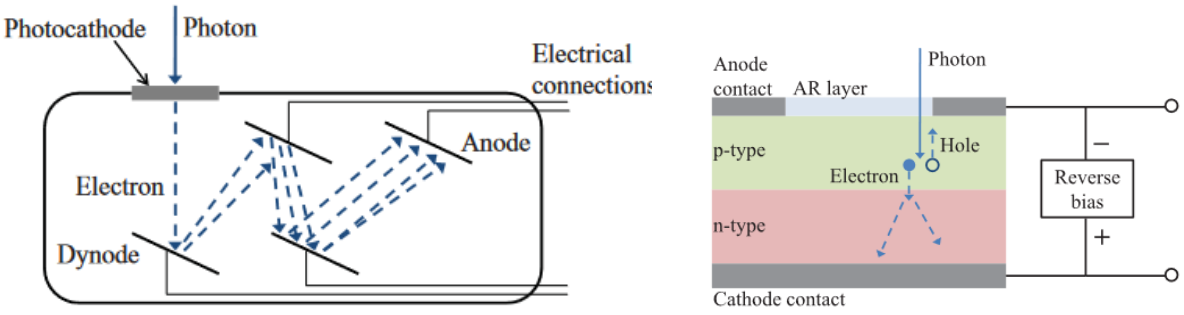
In the original setup, the interferometers used in the encoding on Alice's end and for interference at Bob's end are delay line interferometers (asymmetric MZ). However in our setup the DLI is not required to create separated pulses since we are already doing so through the intensity pulses.

The working of DLI has already been shown earlier. Similar calculations can be done for arbitrary phase shifts.

B.5 Detectors

Reworked from Krister Shalm's tutorial, (Gisin et al. 2002) and (Eisaman et al. 2011)

The conventionally used detectors in QKD currently are SPADs (Single Photon Avalanche Diode). The working of SPADs are analogous to the operation of dynodes:



(a) Photomultiplier tube. (b) SPAD.

Figure 22: Photodetectors.

For photomultipliers: When a single electron strikes the first plate, secondary electron emission takes place and since the first and second plates are set at a potential difference, the emitted electrons accelerate and strike the second plate, repeating the same process. Secondary electron emission can arise through several factors, eg. inelastic scattering.

SPADs work in a similar manner. The diode is set at reverse bias that is above the breakdown voltage. The aperture lets photons pass through. If a photon (of sufficient energy) passes through the aperture, it will with some probability collide with an atom in the semiconductor. Through the photoelectric effect a bound electron is knocked free, causing the production of an electron-hole pair. Due to the reverse bias,

the emitted electron accelerates and knocks out other electrons by way of secondary electron emission, and this avalanche results in the generation of a large enough current to be detected by the detectors' controller. This multiplication process is tougher to model for solid semiconductors, but for pedagogical purposes we can analyse the Townsend discharge mechanism in a Geiger-Muller tube:

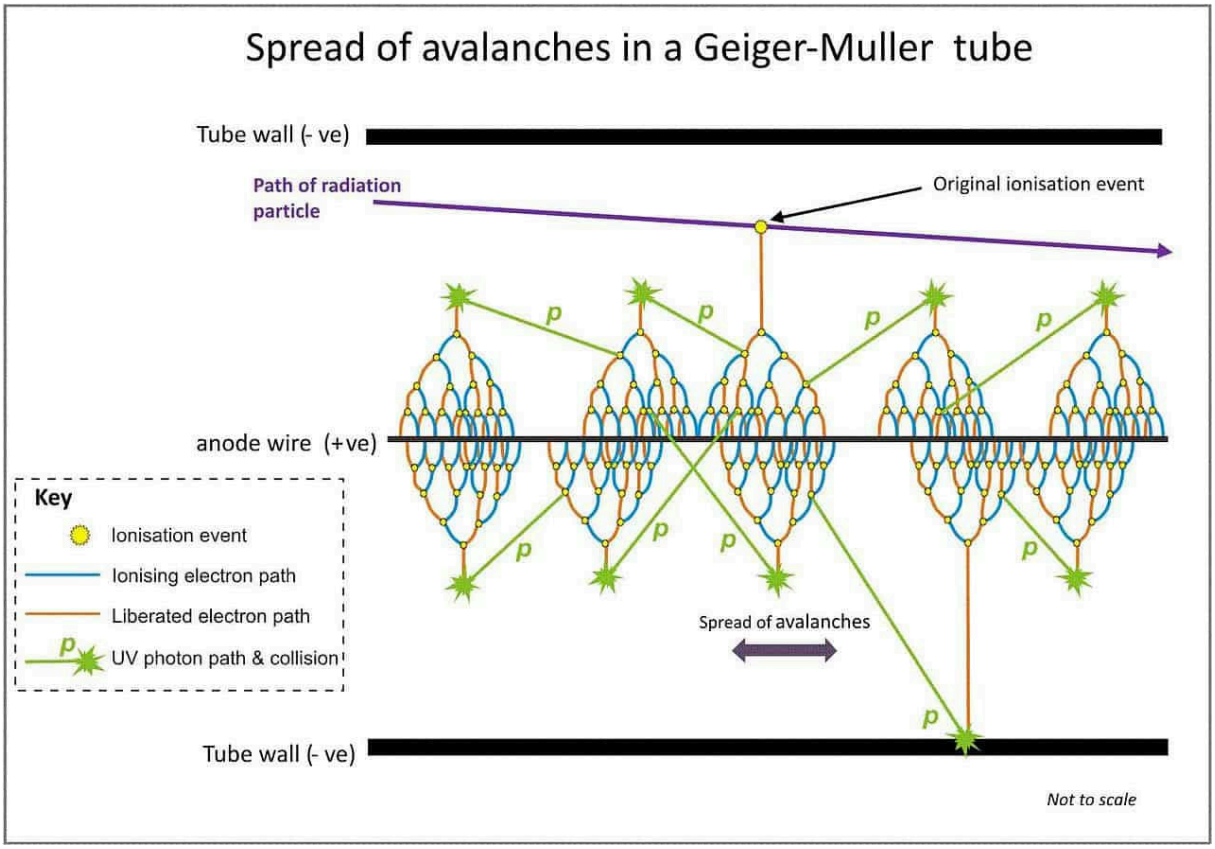


Figure 23: Rough analogy for electron multiplication in SPADs.

The differences arise in the spread of avalanches. In SPADs, there may be photon emission but not necessarily UV, and the avalanche spread is also due to the emission of the knocked-out electron in random directions. Also, since the diode is set in reverse bias, the electrons are accelerated towards the cathode. For our purposes here, this model can be used to explain the other characteristics of SPADs.

Photomultipliers and SPADs are needed because the current associated with a single electron released due to the photoelectric effect is completely insufficient to be registered as a shift in an ammeter. Further, detecting single electrons would give rise to enormous dark counts.

Dark counts: These are false positives that arise due to external conditions or thermal noise. These can be mitigated to some degree by (i) Reducing the temperature of the detector perimeter and isolating it (ii) Analysing the energy spectrum of thermal noise, the semiconductor could be made out of elements whose work function is high enough to prevent avalanche triggering by *most* thermal radiation, and the reverse bias voltage can be set accordingly st. the electron kicked off by stray radiation will not accelerate sufficiently to trigger the avalanche process.

Efficiency: It is the probability of a false negative occurring. This happens if the photon penetrates too deep into the substrate before being detected, giving rise to an avalanche too "close" to the cathode to be amplified sufficiently, or if the photon is simply not absorbed at all.

Quenching: Once the count has been amplified, we need to halt the avalanche process to reset the system for further counts. This is done by reducing the voltage to below breakdown and using a "quenching" process to kill off any spurious electrons or ongoing avalanches. Quenching in SPAD can be carried out in the following manners:

1. Active quenching: The bias voltage is reduced below the breakdown voltage by detecting the rising edge of the avalanche current via electrical circuits. Dead time is of the order of ns.
2. Passive quenching: There is a constant quenching process that takes place in the background.
3. Gated mode: The detector is activated periodically for a specified duration. This drastically reduces the number of dark counts. Usually used as an alternative to active quenching in tandem with passive quenching since it is cheaper.

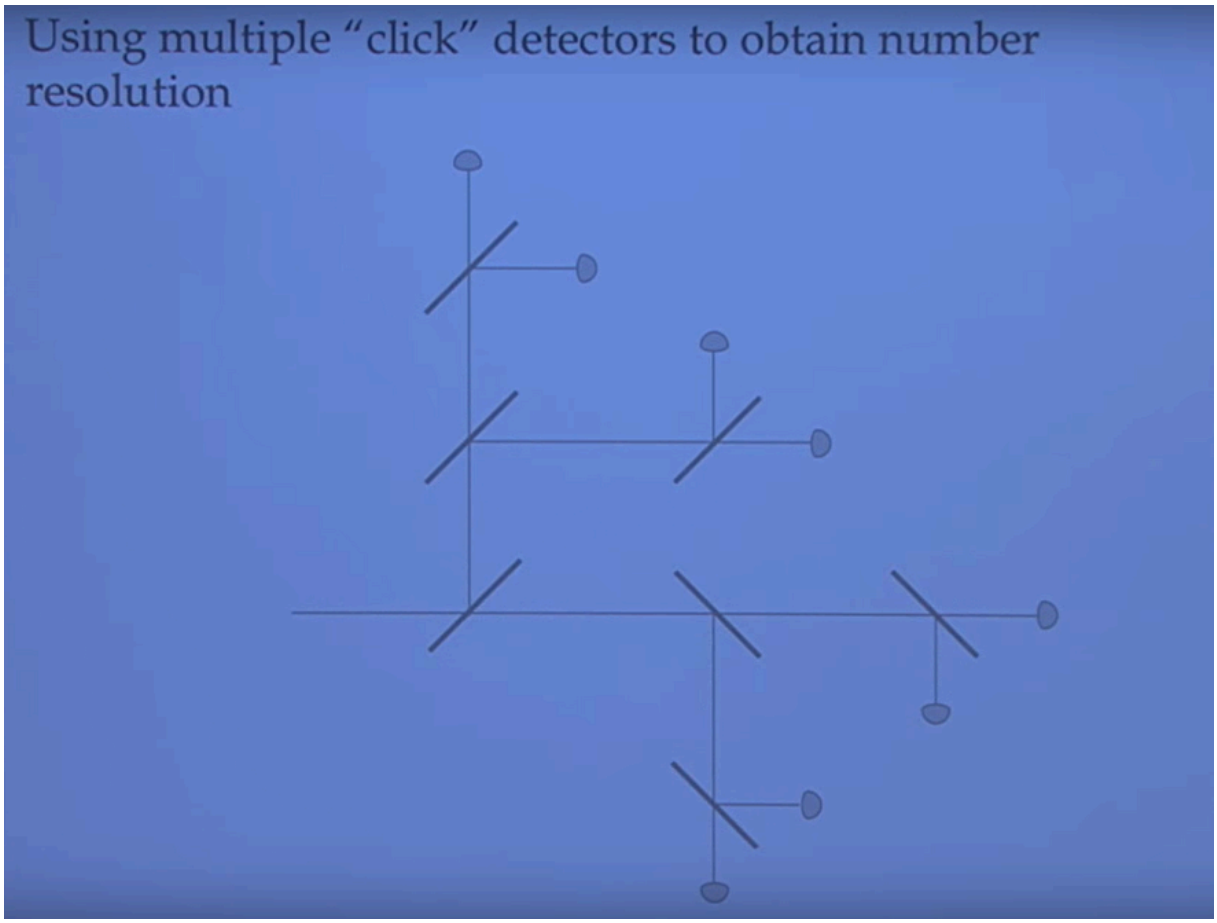
After-pulsing: During the quenching process, it is possible that the avalanche process is not killed off completely despite reducing the bias voltage. This is due to the unsuccessful termination of the lateral avalanches near the cathode, or due to emissions from the populated photon trapping layers which have not depopulated yet. As a result, there is an exponentially decaying probability that the resultant of these processes may give rise to a detection in a timebin after the original detection has been recorded.

Dead-time: To eliminate the afterpulsing effect to a high enough degree, the detector is re-biased only after a certain time period, and all detections in this time period are discarded by the detector's controller.

Jitter: Variation in the detection time of a detector (time duration of amplification process).

Balancing the factors: Increasing the efficiency (eg. by trying to make the detection region "thicker") will increase jitter and dead time. Decreasing the jitter (eg. by making the detection region "thinner") will decrease efficiency. Reducing the dead counts (eg. by cooling the detector) increases the jitter and dead time.

Conversion to number-resolving detector In principle, SPADs can be converted to number resolving in the following manner:



This could potentially be achieved with two detectors by using delay lines as well.

B.6 Beamsplitters

Beamsplitters[24] are used throughout the protocol. Here we use fiber optic based beamsplitters and beam combiners.

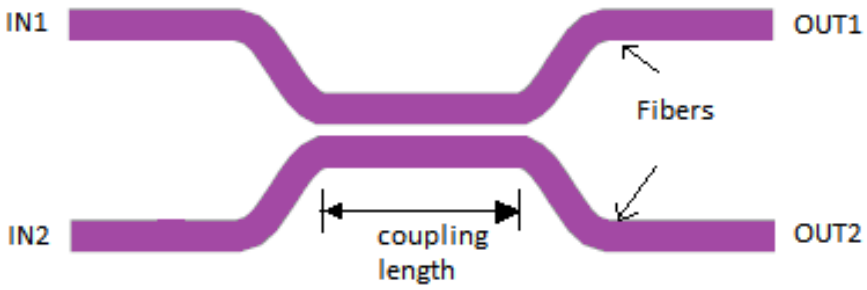


Figure 24: Schematic.

Diagram taken from here.

[24] A full analysis of such beamsplitters was beyond the scope of my project, Section 9.4 of Fundamentals of Photonics by Saleh can be referred to.

B.7 Attenuators

Attenuators can either be mechanical or electrical attenuators. For mechanical attenuators, losses can be induced by changing the aperture opening or by misaligning the input-output fibers.

Electrical attenuators for polarized input can mechanically rotate an internal set of polarizers to obtain the necessary attenuation.

B.8 Quantum channels

We utilise single-mode fibers for transmission. For MDI-QKD polarization maintaining fibers are used. In the propagation of light pulses through a fibre, polarization effects come into place. If a wire is twisted or the starting and ending points of the cable are not on the same horizontal plane, we will observe the polarization at the input and output to be different (easy to visualise the change). This is important due to the possible presence of two different phase velocities for two orthogonal polarization states (birefringence), which would cause issues in high-speed communication. Polarization controllers are used to reduce its effect.

B.9 Polarization controllers

Devices that set the polarization of the light pulses. This can be mechanical (for rough tuning) or electrical (for precise adjustments). It reduces the effect of birefringence and stabilizes the polarization plates. Works by rotation of the cable (for rough tuning) or waveplates (for fine tuning).

B.10 Optical delay line

A device that delays the pulse by elongating the path taken. These can be free space or fibre based.

APPENDIX C : Supplementary material

C.1 All scenarios of the MDI-QKD protocol

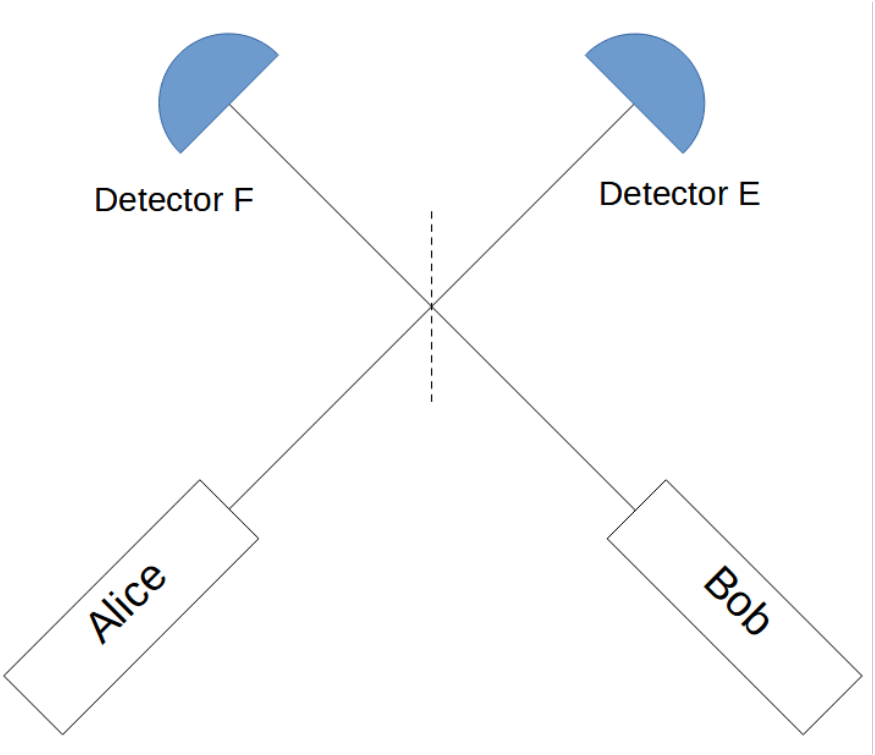


Figure 25: Reference diagram for the case analysis.

The format that I have used: $1A|0B, 0 = 0_Z$ $1A|0B, \pi = 0_X$ $0A|1B, 0 = 1_Z$ $0A|1B, \pi = 1_X$

0_Z implies $|e\rangle$, and so on.

This is for Alice. For Bob the same format is followed, only with `prime` used instead.

For each scenario, Alice and Bob reveal their bases by revealing 0 or π. (This notion was chosen for reasons not related to the protocol.) Through the format chosen it becomes straightforward to follow which party has access to what extent of information.

The final state obtained before measurement is simple to obtain: eg. $1A|0B, 0$ and $1A'|0B', 0$ are initial states. $\hat{a}_E^\dagger \hat{b}_E^\dagger \ |0\rangle_A \ |0\rangle_B \xrightarrow{\text{BS}} \frac{i}{\sqrt{2}}(|2\rangle_E \ |0\rangle_F + |0\rangle_E \ |2\rangle_F)$

The full table of results along with the summarized table (first two cases and for ideal detectors) can be accessed.