Studies on the readability and on the detection rate in a Mach-Zehnder interferometer-based implementation for high-rate, long-distance QKD protocols

Christos Papapanos1, Dimitris Zavitsanos1, Adam Raptakis1, Giannis Giannoulis1, Christos Kouloumentas1 and Hercules Avramopoulos1
1Photonics Communication Research Laboratory, School of Electrical and Computer Engineering, National Technical University of Athens, Iroon Polytechniou Street 15773 Greece

Abstract. We study the way that chromatic dispersion affects the error detection probability and the synchronization on Quantum Key Distribution (QKD) protocols in a widely-used setup based on the use of two fiber-based Mach-Zehnder (MZ) interferometers at transmitter/receiver stations. We identify the necessary conditions for the path length difference between the two arms of the interferometers for achieving the desired error detection probability given the transmission distance- where the form of the detector’s window can be considered. We also associate the above limitations with the maximum detection rate that can be recorded in our setup, including the quantum non-linearity phenomenon, and to the maximum time window of the detector’s gate. We then apply our theoretical outcomes in a more realistic QKD deployment, considering the case of phase-encoding BB84 QKD protocol, which is widely used. At the end, exploiting our results we provide two methods to perform the chromatic dispersion compensation of our setup for keeping the correct order of the transmitted signal. Our proposed methods, depending on the transmission distance and on the photon emission rate at transmitter station, can be easily generalized to every fiber-optic QKD protocol, for which the discrimination of each symbol is crucial.

1 Introduction

New technological achievements have provided the Quantum Key Distribution (QKD) systems to constantly expand to unprecedented transmission distances [1,2,3,4]; exploiting practical and simple synchronization techniques at kHz-scale rates [1], advanced detection units together with novel finite-key security analysis [3] and superconducting nanowires combined with ultra-low loss fibers and cold filters to suppress the background noise [4], successful QKD protocol implementation can be realized through hundreds of kilometers of fiber optics. Moving towards noiseless setup implementations, the authors claim BB84 protocols with fiber distances of 600km [4]. Apart from the BB84-based QKD implementations, the new era of emerged protocols such as twin-QKD [5], promise to overcome the rate-distance limitations by greatly extending the range of secure quantum communications. In this context, other physical limitations that were previously ignored should now be revisited in order to provide a practical implementation framework for this new ultra-long fiber transmission QKD ecosystem.

In QKD protocols, not only the kind of the components that constitute the QKD setup are responsible for the kind and the efficiency of the protocol created, but the values of the parameters involved too. For example, the phase encoding BB84 and its decoy-state modification QKD protocols have the same configuration; the synchronization and the value of parameters involved are the only difference between them. Hence, the study of the phenomena that take place in optical fibers for the specific setup is crucial for maximizing the efficiency of each protocol.

Many QKD protocols- including the aforementioned ones- use time bin encoding for the creation and the reception of the qubit. This method is advantageous for long-distance quantum communication [6]. The setup used for time-slot implementation of prepare and measure protocols is depicted in Fig. 1: the incoming pulse at the input is divided into three pulses at the output. The components with more details are presented in Fig. 2. We will later prove that the exterior pulses do not contain any information for the transmitted states and so they should be distinguished from the middle pulse to avoid the temporal overlapping. As a result, the correct synchronization is important for reading the middle pulse (indicated by time slot $t_2$). It is evident that the temporal width of the pulse plays a crucial role to prevent the temporal overlapping as well as to obtain the proper synchronization. For these two reasons, chromatic dispersion of the fiber medium has a major impact on the protocol’s efficiency, especially as the communication distance is significantly increased.

The added value of our contribution is the definition and the theoretical establishment of a complete bottom-up approach to the natural limitations created by chromatic dispersion and the countermeasures that should be taken
Chromatic dispersion causes the widening of the transmitted pulses with a temporal intensity profile of Gaussian shape. In [7], the results of the transmission of a gaussian pulse through two MZ interferometers, connected in series as indicated in Fig. 2, have been studied. We make use of the mathematical formalism presented in [7], which is true for the general case regarding the possible parameters that characterize the interferometers, as a tool to provide "plug and play" formulas. As a result, we have chosen to use the same symbols, see Fig. 2, for our formalism.

In our paper, it is proved that the proper choice of the phase shift values of the two Mach-Zehnder (MZ) interferometers is sufficient and necessary to provide the output with the required readability, despite the effect of chromatic dispersion, for performing decoding and synchronization. During this process, an alternative approach for establishing the values of the phase shifters, necessary for creating the two bases of phase encoding BB84 QKD protocol, is presented in appendix A, where we have used a mathematically original quantum approach.

More specifically, the condition (lower bound) that needs to be satisfied between the phase shifters of the two interferometers for a given fiber distance between Alice (transmitter) and Bob (receiver) stations in order to attain a specific error detection probability is extracted. Furthermore, the form of the detector's reading window is taken into consideration, leading to a more realistic model.

The maximum theoretical detection rate (raw key rate) that can be generated is related to these setup parameters and, thus we are also able to identify an upper bound.

At longer fiber distances, the widening of each pulse may cause some symbols to be detected in different order than the way they were sent, because of the chromatic dispersion effect. As a result, the final part of this research is devoted to the definition of a mitigation strategy to overcome the impact of fiber dispersion in our setup. More specifically, we use the estimated maximum detection rate to obtain the minimum required compensation length to preserve the correct arrival order. Two methods are presented depending on the systems pulse repetition rate at Alice station, which can be easily expanded out of this specific two MZ interferometers setup.

**2 Definition of our model for QKD protocols**

In our paper, we consider the case that is true for most QKD protocols, which uses two MZ interferometers (ex. phase encoding BB84 QKD, decoy-state phase encoding QKD). In these protocols, the setup uses two symmetric MZ interferometers with the only difference being the phase factors in their long paths, \( \Delta_d \neq \Delta_m \). The difference between these values is, almost always, of the order of wavelength; more specifically \((0, \frac{\lambda_0}{4}, \frac{3\lambda_0}{2}, \frac{3\lambda_0}{4})\) which correspond to phase shift values \((0, \pi, \pi/2, 3\pi/2)\). However, our model is true for the general case where \( \Delta_d - \Delta_m \) can take any value. Furthermore, in most QKD protocols gaussian pulses are transmitted through the fiber link be-
tween Alice and Bob without considering any phase factor through this link ($\Delta_{g} = 0$).

Considering these restrictions from paper [7], we can extract the following result for the position spectra at the exits o,p:

$$|\psi_{o,p}|^2 = \frac{T_{g}}{32 \pi^{2} \sqrt{2 \pi} (\delta k)} (|J_{dm}(x)|^2 + |J_{cm}(x)|^2 + |J_{dc}(x)|^2 + 2|J_{o,p}(x)|^2) \right \}
\tag{1}
$$

where

$$II_{o,p}(x) = -\Re[|J_{dm}(x)|^2] + |J_{cm}(x)|^2 + |J_{dc}(x)|^2 \right \}
\tag{2}
$$

where in both Eqs. 1 and 2 we used $c = n$ because of our restrictions (c,n represent the short legs of each MZ as shown in Fig. 2).

We have chosen the squared absolute value of the position wave function, $\psi_{o,p}(x)$, as it represents the position spectrum and has the desired meaning of the probability that we will later use.

In Eqs. 1 and 2 we use:

$$|J_{ij}(x)|^2 = 4\pi (\delta k)^2 \sqrt{\frac{1}{\gamma_{ij}}} T_{i} T_{j} \times \exp\{-2(\delta k)^2[x'_{ij} - 2\delta_{ij}k_{0}]^2/\gamma_{ij}\},$$

$$\Re[J_{ij}(x)J_{kl}(x)] = c'_{ij} c'_{kl} \cos[z_{ij}(x) - z_{kl}(x)],$$

$$c'_{ij} = 2(\delta k) \sqrt{\frac{T_{i} T_{j}}{\gamma_{ij}}} \right \}
\tag{3}
$$

In paper [7], it is defined:

$$\delta_{ij} = B_{i} + B_{i} + B_{j} \right \}
\tag{4}
$$

where $B_{i} = \kappa_{i} l_{i} t_{i}$ is a constant which depends on the central wavelength of our pulse ($\lambda_{0}$). We can see that because of our restrictions, every possible combination of i,j gives $\delta_{ij}$ the same value. Therefore, from now on we will call every pair $\delta_{ij} \equiv \delta_{i}$ (not to be confused with $\delta k$).

We also have:

$$\gamma_{ij} = 1 + 16(\delta k)^4 \delta_{ij}^2 = 1 + 16(\delta k)^4 \delta_{i}^2 \right \}
\tag{5}
$$

where $(\delta k)^2$ is the mean square deviation of wave numbers of the input Gaussian pulse/function and it holds $\delta k = 2\pi(\delta \lambda)/\lambda_{0}^2$. In the same way, we find that the parameter $\gamma_{ij}$ has the same value for every combination of i,j and, thereby we will call it $\gamma$.

It is defined:

$$x'_{ij} = x - A_{i} - A_{j} \right \}
\tag{6}
$$

where x is the total distance that the input pulse has propagated until the outputs of the MZ interferometer and $A_{i} = \Delta_{i} + N_{0} l_{i}$, where $N_{0} = N(\lambda_{0})$ is the group index for the mean wavelength $\lambda_{0}$. As mentioned in [7], x is the (hypothetical) distance as if the photons have the vacuum speed of light. Furthermore, using the same logic the parameters $T_{i}, l_{i}$ can be expressed uniquely as $T_{i}, l_{i}$ respectively.

### 3 Interpretation of our model

In order to interpret our previously established model, we define the parameter:

$$\mu_{ij} = N_{0} l_{i} + \Delta_{i} + \Delta_{j} + 2N_{0} l_{i} + 2\delta_{i} k_{0} \right \}
\tag{7}
$$

One important observation worth mentioning at this point is that although $\mu_{ij}$ differs for every pair ij, the difference of the values is very small due to the fact that $l_{i} \gg \Delta_{i}$ for every i and for long transmission distances.

Finally, we can express more clearly the Eqs. 3 in the following form:

$$|J_{ij}(x)|^2 = 4\pi (\delta k)^2 T_{i} T_{j} \times \exp\{-2(\delta k)^2[x'_{ij} - 2\delta_{ij}k_{0}]^2/\gamma_{ij}\},$$

$$\Re[J_{ij}(x)J^{*}_{kl}(x)] = c'_{ij} c'_{kl} \cos[z_{ij}(x) - z_{kl}(x)],$$

$$c'_{ij} = 2(\delta k) \gamma^{-1/4} T_{i} T_{j} \times \exp\{-2(\delta k)^2[x'_{ij} - 2\delta_{ij}k_{0}]^2/\gamma_{ij}\},$$

$$z_{ij}(x) = \frac{1}{\sqrt{\gamma}} \arctan[4\delta_{ij}(\delta k)^2] + \frac{1}{\gamma_{ij}} [k_{0}^2 \delta_{ij} - k_{0} x'_{ij} - 4(\delta k)^4 \delta_{ij} x'_{ij}^2] \right \}
\tag{8}
$$

As can be now seen, $|J_{ij}(x)|^2$, $\Re[J_{ij}(x)J^{*}_{kl}(x)]$ are gaussian distributions with a mean value given by:

$$\mu_{1} = \mu_{ij} \right \}
\tag{9}
$$

$$\begin{align*}
\mu_{2} &= \frac{\mu_{1} + \mu_{kl}}{2} \\
\sigma &= \frac{\sqrt{\gamma}}{2(\delta k)} \right \}
\tag{10}
\end{align*}
$$

for both distributions. Obviously, the cosine term on Eq. 8 changes the amplitudes of each gaussian distribution.
For computing the mean value and the standard deviation of the second term \(\langle R[J_{ij}(x)J_{ij}(x)]\rangle\), the formulas of the product of two gaussian distributions with arbitrary means \(\mu_f, \mu_g\) and standard deviations \(\sigma_f, \sigma_g\) have been used.

Now, we are in position to express the full width half maximum (FWHM) value of each pulse. The FWHM is the same for every pulse since it depends on the variance and not on the mean value. So:

\[
FWHM = \sqrt{8\ln 2} \cdot \sigma
\] (11)

In conclusion, the signal at the MZ interferometer outputs set prior to the photon detectors, is a sum of gaussian distributions with the same standard deviation and slightly different mean values.

4 Results and Discussion

The range of the derived FWHM is not a sufficient metric for QKD protocols, as we will later see; neither is the wider one, where the energy of the pulse falls to the \(1/e\) of its maximum value. The half width of the latter value is often used in classical description of Gaussian pulses and is symbolized \(T_0\). As a result, a wider metric is needed.

For determining the proper width of this metric, we need to define the new parameter \(X_\kappa\) which is the half width of the pulse where its energy falls to \(1/e^2\).

\[
X_\kappa = \kappa \cdot \frac{FWHM}{2\sqrt{\ln 2}}
\] (12)

As expected for \(\kappa = \sqrt{\ln 2}\) we have \(X_{\kappa_{\ln 2}} = \frac{FWHM}{2}\) and for \(\kappa = 1\) we have \(X_1 = T_0\). Here, the constant \(\kappa\) is different from the previous constant \(\kappa\) mentioned in \(B_1\).

4.1 Lower bound - Low error detection probability

Succeeding low error detection probability demands the complete knowledge of the signal at the MZ interferometer outputs. Since every pulse at the output of the fiber setup exhibits the same spreading, as a next step we need to find the longest distance between any two gaussian distributions at the output of the setup produced by one incoming pulse.

From Eqs. 8 and 9 we derive that the maximum possible distance between two gaussian distributions of Eq. 1 depends only on the values of the phase shifters, \(\Delta\). The longest distance between the gaussian distributions is between the part of the pulse that propagates through the short-short legs of the two MZ interferometers \(|J_{cc}(x)|^2\) term and the part of the pulse that propagates through the long-long legs of the two MZ interferometers \(|J_{dd}(x)|^2\) term. It is evident that this distance is the same for both \(|\psi_a|^2\) and \(|\psi_b|^2\) because the aforementioned terms exhibit the same dependence on the exterior gaussian distributions.

Subtracting the distances that the mean value of the aforementioned two pulses have propagated along the entire fiber link (meaning \(\mu_{cc}, \mu_{dd}\)), we find the maximum width of the exterior gaussian distributions. If we remove the standard deviation (\(\sigma\)) of each gaussian distribution, the final width of the symbol because of chromatic dispersion effect is shown in Fig. 3. Recalling that \(\mu_{dm} > \mu_{cc}\), this width is equal to:

\[
(x - \mu_{cc}) - (x - \mu_{dm}) = \Delta_d + \Delta_m - 2\Delta_c
\] (13)

where we replaced \(\Delta_c = 0\), a consideration that most of the similar setups meet or consider it as a benchmark.

Figure 3 shows an overview of the different values of \(X_\kappa\). It is worth mentioning that these values are identical for each pulse, including the middle one and the two exterior ones. Since the exterior pulses are present in every case, they do not provide us any information about the basis of the signal; as a result we need to separate them from the middle pulse. We can see that as the width (Eq. 13 decreases, a critical point will be approached. Beyond this point, the 3 pulses will interfere and, thus we will not be able to decode the information. We are then able to extract the necessary condition to achieve this separation, given the error detection probability that we want to succeed:
\[ \Delta_d + \Delta_m \geq 4X_\kappa = \frac{2\kappa \text{FWHM}}{\sqrt{\ln 2}} = \kappa \cdot 4\sqrt{2}\sigma \] (14)

where \( \kappa \) expresses the error detection probability in the way that will be mentioned in the next paragraph.

As stated above, each pulse is a gaussian distribution and it is also the position spectrum of the particle that the symbol contains. Hence, we are able to interpret it as the probability of detecting the particle in each position, so by transforming the gaussian distributions of the pulses to standard normal distributions we can estimate the detection probability in each pulse in relevance with the parameter \( \kappa \). A similar approach could be used for other than Gaussian pulses as the input pulse.

Table 1 summarizes the main results that can be provided from Eq. (13). We have considered only the equality of this condition and furthermore we can conclude that there is no point of selecting values of \( \kappa \) higher than 3 for the below reasons:

1. We accomplish the maximum probability for correct distinction which equals to 1.
2. As \( \kappa \) increases, the length of transmission increases too. Leading to higher losses and, thus to lower raw key rate.
3. A more important factor is the maximum raw key rate which is restricted from the intersymbol interferences. We will analyze this factor in detail in the next subsection.

| \( \kappa \) | \( \Delta_d + \Delta_m \) | Correct detection probability |
|------------|-----------------|-----------------------------|
| 1          | 2.402 \( \cdot \) \text{FWHM} | 84.26% (1.414\( \sigma \))   |
| 2          | 4.804 \( \cdot \) \text{FWHM} | 99.54% (2.828\( \sigma \))   |
| 3          | 7.206 \( \cdot \) \text{FWHM} | 100% (4.243\( \sigma \))     |

Table 1: Correct detection probability of the signal, depending on the path difference of the two Mach-Zehnder interferometers.

The probabilities which are presented in table 1 in the case of the ideal configuration (except, of course, for the chromatic dispersion), are the values of the interference Visibility of the setup. Visibility is an important parameter since it is directly connected with the Quantum Bit Error Rate (QBER) performance which in turn assesses the secure key rate that can be distilled [3,9].

In case that there are also other imperfections- for example not perfect alignment- on the setup (referring only on the line between Alice and Bob), the total Visibility of the setup can be estimated as the product of the individual probabilities for the case of independent variables (independent imperfections). In practical QKD installations, the Visibility ranges from 93% to 99.999%. [5]

At this point, we need to mention that the above consideration of the equality (Eq. (13) and Table 1) considers the existence of an ideal detector; meaning the rising and falling times are zero and, thus the shape of the time slot that the detector reads is orthogonal as shown in Fig. 1. Otherwise, these characteristics of the detectors should be taken into consideration by increasing the right term of the condition (14) by the rising and falling times translated into units of length. More specifically, considering that the detectors could read with precision only at the peak of the time slot, we obtain:

\[ \Delta_d + \Delta_m \geq 4X_\kappa + c_0 \cdot (t_{\text{rising}} + t_{\text{falling}}) \]
\[ = 2\kappa \cdot \frac{\text{FWHM}}{\sqrt{\ln 2}} + c_0 \cdot (t_{\text{rising}} + t_{\text{falling}}) \]
\[ = \kappa \cdot 4\sqrt{2}\sigma + c_0 \cdot (t_{\text{rising}} + t_{\text{falling}}) \] (15)

where \( c_0 \) is the speed of light in the vacuum. An effective index of the transmitted mode is not needed because, as we have already mentioned, the initial formulas define \( x \) as if photons had the vacuum speed of light. In general, in condition (14) a safety factor could be considered.

The results that we have extracted can be applied to QKD implementations relying on the use of MZ interferometers-assisted state preparation and measurements stations. Hence, they are universal and in Fig. 1 are presented in the range that this category of QKD protocols operate. As it was originally expected, they appear a linear dependence on distance and the value of the sum of the phase shifters is increased for higher detection rates.

\[ (\Delta_d + \Delta_m) - L \]

Fig. 4: Minimum sum of the values of the phase shifters needed because of chromatic dispersion.

It is worth applying realistic \( t_{\text{rising}} \) and \( t_{\text{falling}} \) times to Eq. (15) in order to define the dominant term of this condition. Although the work in [13] is relatively new, approxi-
mate recovery times can be extracted from it where we are able to see that superconducting nanowire single-photon detectors (SNSPDs) can exhibit recovery time around 50 nsec. Hence, the added term because of the imperfect detector equals to 15 nsec and the first sum as indicated in Fig. 4 with the dotted line is around 1.8 m for 200 km transmission distance; for longer distances the gap between those terms is diminished.

As a result, technology establishes the second term as dominant leading to higher phase shift values. It is evident that a few nanoseconds of recovery time will reverse the dominant role but this is not feasible yet.

Finally, practical conditions for high quality readability have been defined and the proper metric for QKD systems that we were looking for is $X_3$. This metric can be used beyond this two MZ interferometers setup.

As a next step, we will analyze the third important aforementioned factor that prevents the intersymbol interference and maintains the correct arrival order of each symbol (this interpretation is presented in Sec. 5).  

4.2 Upper bound - Theoretical maximum raw key rate

At the output of the setup, owing to the chromatic dispersion each symbol has its widest pulsewidth and then, after a very short distance (from the MZ’s output to the detector), it will be detected. We will symbolize this distance as MZ-D. Each symbol, as we have mentioned, is consisted of three pulses. The pulses which come from the short-short travel, the short-long/long-short travel and the long-long travel of the symbol will be from now on referred as right one, middle one and left one respectively, where we have considered, without loss of generality, that the symbol propagates along the right axis. Considering two consecutive pulses, there is a distance threshold above which these two consecutive symbols will start to interact. The parts of the symbols that will firstly interact are the left pulse of the first symbol and the right pulse of the second symbol.

As already mentioned, the information is hidden in the middle pulse of each symbol and, thus we need to find a condition that will prevent the interaction of the two consecutive symbols being able to affect the middle pulse/window altering the order and/or the value of the symbol read.

When the two symbols start to temporally overlap, the quantum non-linearity phenomenon could possibly arise. In this case, single photons at new frequencies can be generated and due to chromatic dispersion they will then propagate along fiber with different velocities. Hence, during the distance MZ-D, if the new frequencies are sufficiently fast to cover the adjacent temporal window set prior to the detectors, a part of energy of the interacting pulses could probabilistically leak into the middle pulse, degrading thereby the readability of our setup. However, as can be derived from [11][12], this is quite impossible to happen at these energy levels and in the conventional telecom fibers testbeds which are currently used in long-distance deployments. Through the literature, there are limited works demonstrating photon-to-photon non-linear interaction using specialty fiber setups where one can probe this quantum non-linear domain [13].

Having this in mind and targeting to keep our results as general as possible in support of the future experimental realizations, we have studied both cases; considering and ignoring the quantum non-linearity effect. To this end, we also derive the modified condition for the case where non-linear photon-to-photon interaction can be obtained between the symbols in our model which leads to lower detection rates.

In case where quantum non-linearity phenomenon cannot affect, as previously described, the middle pulses of these two consecutive symbols, we can extract the condition [10]. As shown in Fig. 5a, the distance between two successive symbols needs to be equal to two times the value of the width of the pulse, meaning $4X_\kappa$, in order to not have intersymbol interference. This straightforwardly leads to:

$$ R \leq \frac{c}{4X_\kappa} \quad (16) $$

so an increase of $\kappa$ leads to a decrease of the maximum possible raw key rate. This is the mechanism behind the obtained trade-off between the error detection probability and the maximum raw key rate, as it has been already emphasized in the introduction. Certainly, the values of the maximum raw key rate are higher than those that most protocols have succeed because of the low energy of the pulse and the speed of the electronic systems that the setup uses.

In case where the quantum non-linearity phenomenon could affect the middle pulse, we modified our condition as follows:

$$ R \leq \frac{c}{6X_\kappa} \quad (17) $$

so that each symbol has no shared part with any of the consecutive pulses (see [11]). As expected from Figs 5a and 5b, the maximum theoretical detection rate is smaller when quantum non-linearity has an effect than when it has not. The exact ratio is three times smaller as indicated in Eq. 17.

All figures below represent the case that quantum non-linearity has no effect on the middle pulse but using Eq. 17 someone can easily represent the opposite case.

It is worth mentioning that in order to keep the maximum possible raw key rate, we should not consider, as in classical channels, the range of the pulse where its power reaches the $\frac{1}{e}$ of the maximum value but instead the point that its power reaches the $\frac{1}{e^2}$ of the maximum value. Therefore, the definition of the dispersion length ($L_D$), as defined in [14], for the quantum setup implementations studied for most QKD protocols, representing the maximum optical fiber length so that the chromatic dispersion will not affect the signal decoding needs to be re-considered and/or re-expressed by future works.

The condition [10] leads to an upper bound for the raw key rate that can be obtained, if no countermeasures are
Below we present some results which indicate the maximum raw key rate creation that can be accomplished at Bob station without using any dispersion compensating fiber which increases the distance and, thus, the photon losses (Fig. 4). In all of our simulations, we have considered wavelength equal to \( \lambda_0 = 1550\,\text{nm} \) and divergence from the central wavelength equal to \( \delta \lambda = 0.31\,\text{nm} \), meaning \( \frac{\delta \lambda}{\lambda_0} = 2 \times 10^{-4} \). Our results are true for both deterministic single-photon sources where an ideal emitter can produce one photon at a time and also for probabilistic sources realized through an attenuated laser source. The only characteristics of the source which we have considered are the central wavelength and the divergence from it.

Our simulations have shown that the maximum theoretical raw key rate (upper bound) that can be generated at Bobs site is far beyond the rates that the current technological level can provide. In more detail, due to the hardness of engineering on-demand single-photon sources, most QKD implementations and experiments rely on the use of highly attenuated laser sources which emit probabilistically photons, including also multi-photon pulses. In order to not compromise security, because of the presence of these multi-photon pulses, the attenuation required is such that the average photon number is set much smaller than one, leading thereby to lower detection rates. Furthermore, other restrictions of our nowadays technology is the maximum detection rate and the maximum clock rate of the pulses produced by the source; both are much lower than the frequencies indicated in Fig. 6. However, when technology overcome these problems, the upper bound will be important to be known. Some serious steps have already been done towards this direction, see the works \([10, 17]\) and future needs in \([18]\). This upper bound, for maintaining the correct reading order of the symbols sent, could be reached only by the use of single-photon sources in a lossless channel. In case of the probabilistic sources, it cannot be achieved but even in that case this upper bound needs to be fulfilled and the practical use of this theoretical maximum detection rate is presented in Sec. 5.

In practical systems, there are single-photon detectors (SPDs) with detection rate in the range of 100MHz to 200MHz \([19]\) so in Fig. 7 we have chosen to present the maximum achievable distance allowed by chromatic dispersion for the aforementioned detection rate range. In order to achieve longer distances, countermeasures should be taken, some of which we have previously mentioned.

**4.3 BB84 QKD protocol simulation based on our results**

Before proceeding, we need to highlight the main results of this study, which are presented in Eqs. \([14, 15]\) or \([16, 17]\) and in \([18]\).

To make these results more concrete, we will apply them on the phase encoding BB84 QKD protocol. Obviously, the same procedure applies also on the phase encoding decoy-state QKD protocol, as it uses the same logic.

**Fig. 5:** Minimum distance between two consecutive symbols at the MZ outputs in order for the symbols to not temporally overlap.

(a) Minimum distance in the case that the quantum non-linearity phenomenon can be ignored.

(b) Minimum distance in the case that the quantum non-linearity phenomenon cannot be ignored.

Below we present some results which indicate the maximum raw key rate creation that can be accomplished at Bob station without using any dispersion compensating fiber which increases the distance and, thus, the photon losses (Fig. 4). In all of our simulations, we have considered wavelength equal to \( \lambda_0 = 1550\,\text{nm} \) and divergence from the central wavelength equal to \( \delta \lambda = 0.31\,\text{nm} \), meaning \( \frac{\delta \lambda}{\lambda_0} = 2 \times 10^{-4} \). Our results are true for both deterministic single-photon sources where an ideal emitter can produce one photon at a time and also for probabilistic sources realized through an attenuated laser source. The only characteristics of the source which we have considered are the central wavelength and the divergence from it.

Our simulations have shown that the maximum theoretical raw key rate (upper bound) that can be generated at Bobs site is far beyond the rates that the current technological level can provide. In more detail, due to the hardness of engineering on-demand single-photon sources, most QKD implementations and experiments rely on the use of highly attenuated laser sources which emit probabilistically photons, including also multi-photon pulses. In order to not compromise security, because of the presence of these multi-photon pulses, the attenuation required is such that the average photon number is set much smaller than one, leading thereby to lower detection rates. Furthermore, other restrictions of our nowadays technology is the maximum detection rate and the maximum clock rate of the pulses produced by the source; both are much lower than the frequencies indicated in Fig. 6. However, when technology overcome these problems, the upper bound will be important to be known. Some serious steps have already been done towards this direction, see the works \([10, 17]\) and future needs in \([18]\). This upper bound, for maintaining the correct reading order of the symbols sent, could be reached only by the use of single-photon sources in a lossless channel. In case of the probabilistic sources, it cannot be achieved but even in that case this upper bound needs to be fulfilled and the practical use of this theoretical maximum detection rate is presented in Sec. 5.

In practical systems, there are single-photon detectors (SPDs) with detection rate in the range of 100MHz to 200MHz \([19]\) so in Fig. 7 we have chosen to present the maximum achievable distance allowed by chromatic dispersion for the aforementioned detection rate range. In order to achieve longer distances, countermeasures should be taken, some of which we have previously mentioned.

**4.3 BB84 QKD protocol simulation based on our results**

Before proceeding, we need to highlight the main results of this study, which are presented in Eqs. \([14, 15]\) or \([16, 17]\) and in \([18]\).

To make these results more concrete, we will apply them on the phase encoding BB84 QKD protocol. Obviously, the same procedure applies also on the phase encoding decoy-state QKD protocol, as it uses the same logic.

**Fig. 5:** Minimum distance between two consecutive symbols at the MZ outputs in order for the symbols to not temporally overlap.

(a) Minimum distance in the case that the quantum non-linearity phenomenon can be ignored.

(b) Minimum distance in the case that the quantum non-linearity phenomenon cannot be ignored.

Below we present some results which indicate the maximum raw key rate creation that can be accomplished at Bob station without using any dispersion compensating fiber which increases the distance and, thus, the photon losses (Fig. 4). In all of our simulations, we have considered wavelength equal to \( \lambda_0 = 1550\,\text{nm} \) and divergence from the central wavelength equal to \( \delta \lambda = 0.31\,\text{nm} \), meaning \( \frac{\delta \lambda}{\lambda_0} = 2 \times 10^{-4} \). Our results are true for both deterministic single-photon sources where an ideal emitter can produce one photon at a time and also for probabilistic sources realized through an attenuated laser source. The only characteristics of the source which we have considered are the central wavelength and the divergence from it.
Fig. 6: Maximum detection rate creation because of chromatic dispersion when quantum non-linearity phenomenon has no effects. (y-axis is in logarithmic scale)

Fig. 7: Range of maximum detection rate because of chromatic dispersion for practical devices.

for the construction of the qubits, thereby the results presented in this subsection are true for both protocols.

Here, we assume the same characteristics of the source as mentioned in Sect. 4.2 and we want to accomplish a communication over the 50km distance with as less error detection as possible, meaning $\kappa = 3$ from table 1. We use Eqs. (14) or (15). We will, also, assume that $t_{\text{rising}} = t_{\text{falling}} = 0$, so we obtain:

$$\Delta_d + \Delta_m \geq 0.423 m$$ (19)

In practical designs, the value of 0.5$m$ would be chosen for safety reasons, as it is higher than the limit value, leading to a relatively more robust system to the effects emerging from plausible other imperfections, and also because any divergence from this value will keep us within bounds. This means that whatever choice we have to make in order to create the necessary pair of bases for these protocols, the condition (19) must be always true. Hence, it is reasonable to assume a minimum value equal to $0.5/2 = 0.25m$ for each of the two phase shifters.

Now, we have to assume what phases we should pick for the creation of the bases. Phase encoding make use of two pairs of phases that each signal pulse should be modulated in. There is need to:

1. For the same pair, the phases need to be chosen so that they will lead to orthogonal states creation; maximize the detection probability to different detectors.
2. When read in wrong basis, the result is ambiguous.

In appendix A we extracted a simple way to understand the choice of the value of the two phase shifters:

1. Bob chooses to read randomly between the two bases, by setting $\phi_m = 0$ or $\phi_m = \lambda_0/2$ for basis X and basis Z respectively.
2. Alice modulates in basis X when the values of phase shifters are $\phi_d = 0$ or $\phi_d = \lambda_0/4$ for bits 0 and 1 respectively. Whilst, she modulates in basis Z when the values of phase shifters are $\phi_d = \lambda_0/4$ or $\phi_d = 3\lambda_0/4$ for bits 0 and 1 respectively.

For the meaning of the symbol $\phi_\omega$ where $\omega \in \{d, m\}$ see Eq. A.3 in Appendix A.

Of course, it should be clear by now, that the aforementioned values are added to the value 0.25m that we extracted before by adding in series a constant length (0.25m) to the phase modulator: $\Delta = 0.25 + \phi_\omega$ where $\phi_\omega$ adds the phase modulation which corresponds to 0, $\lambda_0/2$, $\lambda_0/4$ or $3\lambda_0/4$.

Our results can be confirmed by precise simulations, see Figs. 8 and 9. In these figures, we are able to see the importance of the distance between two consecutive symbols and, thus the importance of the results on Sec. 4.2. If we have not considered the maximum transmittance rate, the middle pulse would not be zero in the cases that it has to be (Figs. 8a, 8b, 9c and 9d).

Furthermore, from Eq. (18) or (17) we obtain that the maximum possible raw key rate that can be generated without countermeasures is approximately 710Mbps and 473Mbps respectively. Finally, we are able to find from Eq. (18) the maximum duration of the detector’s window: $\Delta t_{\text{gate}} = 0.962\text{ns}$. 


The next section.

In a similar way, our results can be used for any distance with non-ideal detectors and for any QKD protocol that uses the same two Mach-Zehnder setup; easily can be expanded to other setups as it will be mentioned in the next section.

5 The role of the clock rate on the correct ordering reading for dispersive pulse broadening

Nowadays, the technology of pulsed laser sources can provide very high clock rates. However, these ultra-high speeds cannot be recorded at the detector’s site due to fundamental limitations of their technology (deadtime, jitter) as well the relatively low efficiency and speed of the post-processing error detection algorithms limited to Mbps rates even for channels with low losses [20]. Moving towards longer fiber distances, the photon loss is dramatically increased and is responsible for distilled key rates of few bps even for the Alice pulsed implementations operated on GHz-scale [3].

However, different steps are needed to be considered depending on the frequency of the clocked setup—because of chromatic dispersion— in order to have even more robust implementations.

From Fig. 7 we are able to see the upper limit of the theoretical maximum raw key rate because of chromatic dispersion. Hence, there are two categories:

1. The frequency of the clocked setup is less than the theoretical maximum raw key rate at a given distance. This condition is easily satisfied for short distances with the current technology or for low frequencies of the clocked setup (recording, inevitably, low raw key rate).

2. The frequency of the clocked setup is higher than the theoretical maximum raw key rate at a given distance. This condition will be greatly boosted in future QKD deployments where high frequencies of the clocked setup will be possible as in [4].

For each category, we need to follow different strategies for preserving the high-quality reading:

1. For the first case, we do not need to compensate the signal using Dispersion Compensating Fiber (DCF); we just need to compute the values of the MZ interferometers’ phase-shifters from Eq. 14 (or see Fig. 4). Apart from not using DCF, another advantage of this method is its symmetry; permitting two-way communication whilst pre-compensation does not.

2. The second case requires a completely different treatment. If we were using the first strategy for this case, the order of the qubits sent would be changed leading to wrong qubits being read: during the transmittance of the signal, each symbol will be widened to such extent that a part of it will overrun a part of the next symbol leading to, not only intersymbol interference (ISI), but also changed detection order. Therefore, the use of a dispersion compensation strategy is unavoidable. However, complete compensation of the signal is not necessary. The required steps to identify this minimum compensation length—without the order of the symbols altered—can be found below:

We find the maximum active length from Eq. 16 or Fig. 6 accordingly, which corresponds to the frequency of the clocked setup. Hence, we need to compensate an amount of distance equal to the total...
length subtracted by this active length. This is the minimum compensation length.

Of course, we can fully compensate from the beginning of the deployed fiber link at an increased cost since the DCF is much more expensive compared to the standard telecom fibers (e.g. Standard Single Mode Fibers-SSMFs).

For the needs of studying this second case, we considered the implementation settings reported in [4], where they used a cycled setup at 2.5GHz. Therefore, from Eq. (13) or Fig. [6] accordingly, we find the active length equal to 20km. As a result, instead of performing complete compensation, we need to provide complete compensation for transmission distance equal to \((405 - 20) km = 385km\).

Surely, owing to losses the active length can be higher; as most qubits will be lost, the probability for reading with wrong order is non zero but it can be very close to it. Further study is required to emphasize on the actual relation between the active length, the losses and the wrong order reading probability. However, there are protocols such as the User Datagram Protocol (UDP) in which the wrong reading order is not problem [21].

Although the second case is not symmetrical when pre-compensating, the advantage of not fully compensating the total length can be the cost reduction since the use of longer DCF segments can be prevented.

Overall, we showed two ways- depending on the systems pulse frequency (mentioned as cycled system)- for applying our results and keeping the correct reading order of the transmitted pulses.

These methods can be used not only in this setup with the two MZ interferometers in series but in the general case too; in every fiber optic QKD protocol for which the discrimination of each symbol is important by just changing the Eq. (16) with:

\[
R \leq \frac{c}{2X_n}
\]

(20)

The results of this section provide a different interpretation for the results presented on Sec. [5] in which the theoretical maximum raw key rate is, also, the maximum clock rate that can be used for maintaining the correct symbol order of the signal sent for a specific transmission distance.

6 Conclusions

Maximum readability QKD systems are necessary to reach detection rates as high as possible, where 100% correct detection probability- without any other imperfection other than chromatic dispersion- is needed to achieve that. We have found that in order to achieve this probability the detection window of the detector’s gate should be 7.206 \(\cdot\) FWHM; in case that the detector’s window has non-ideal rising and falling times, a safety factor should be added to the aforementioned value.

Apart from the width of the detector’s window, as a result of chromatic dispersion, the MZ phase shift values should also be appropriately chosen in order to attain high correct detection probability. Lower bound for the sum of the fiber length of phase shifters of the two MZ interferometers has been calculated and, in high precision, it was found to exhibit linear dependence on the fiber transmission length. More specifically, the slope of the dependence is approximately equal to \(0.8454 \cdot \frac{m}{100 km}\) for achieving 100% correct detection probability.

The lower bound restriction of the MZ interferometers phase shifters leads to an upper bound restriction for the maximum raw key rate that can be recorded because of chromatic dispersion in the setup. The upper bound depends on the ISI appeared between two consecutive pulses and it follows an inversely proportional relation with the transmission length. More specifically, the constant of proportionality of this inverse dependence is, approximately, equal to 35.46 Gbps \cdot km for long transmission distances for which we are interested.

In contrast to the ISI effects in classical flows, there is the need to consider the intended error detection probability associated with the setup too and the aforementioned value (35.46 Gbps \cdot km) is for accomplishing 100% correct detection probability. Besides the role of ISI effect, the upper bound can be also affected by the quantum non-linear photon-to-photon interaction and this mechanism should also be considered as part of our study. In this case a constant of proportionality of the aforementioned inverse dependence equal to 11.82 Gbps \cdot km is derived. In this line, our results have taken this into consideration and they are valid either way.

Finally, depending on the pulse generation frequency, the upper bound can be used to select the most efficient compensation scheme to ensure the correct order of the signal and greatly reducing the deployment cost of the fiber-based setup. These methods can be easily expanded to QKD protocol implementations where the discrimination of each symbol is an essential parameter to the best of our knowledge, every known protocol makes use of that; this expansion can happen by changing the constant of proportionality of the inverse dependence from 35.46 Gbps \cdot km to 70.92 Gbps \cdot km.

Welcoming the beyond-500km era for secure distance of QKD in fiber links [22], our work contribute in this topic of ultra-long haul, repeaterless QKD transmission where the role of readability, time synchronization and chromatic dispersion of the QKD implementation should be carefully addressed.

7 Authors contributions

C. Papapanos is the corresponding author of this research. C. Papapanos conceived and comprehended the presented idea and developed the theory as well as the analytical calculations. D. Zavitsanos, A. Raptakis and G. Giannoulis were, also, involved supporting the literature survey and the preparation of the manuscript. All the authors have read and approved the final manuscript.
Appendix A Proper phase shifter choice

In this appendix, we demonstrate an alternative way to find the proper choice of the phase shifters using our quantum-mechanical results. The difference between each MZ output lies in the last term of Eq. 11 so this is where we will try to find some indication for the proper choice of the phase shifters.

On its side, the term \( I_{\omega,x}(x) \) indicates that we can interchange the MZ outputs by changing the sign of its terms; the cosine term is a possible solution for that. Hence, we will try to present the \( z_{ij} - z_{kl} \) term in a more easy to interpret form; from Eq. 11 we have:

\[
\begin{align*}
  z_{ij} - z_{kl} &= \frac{1}{\gamma} \left[ k_0 (x'_{kl} - x'_{ij}) + 4(\delta k)^4 \delta_j (x'_k - x'_l) \right] \\
  &= \frac{x'_{kl} - x'_{ij}}{\gamma} \left[ k_0 + 4(\delta k)^4 \delta_j (x'_k + x'_l) \right] \\
  &= \Delta_i + \Delta_j - \Delta_k - \Delta_l \\
  &= \left[ k_0 + 4(\delta k)^4 \kappa(l_g + 2l) \right] \\
  &\times \left( 2x - 2A_i - A_j - A_k - A_l \right) \\
\end{align*}
\]

where we have substitute \( x'_{ij}, x'_{kl} \) and \( \delta_j \) to find the third line.

Now, we will do a small trick to reveal the desired form. As we said before the parameter \( \mu_{ij} \) is approximately the same for every pair \( ij \) and it represents the distance that the pulse has travelled so far. As a result it would be more convenient to replace the value \( x \) in Eq 10 with the distance that the middle point of the interior pulse will travel. This can be achieved by finding the average

References

1. Yang Liu, Teng-Yun Chen, Jian Wang, Wen-Qi Cai, Xu Wan, Luo-Kan Chen, Jin-Hong Wang, Shu-Bin Liu, Hao Liang, Lin Yang, Cheng-Zhi Peng, Kai Chen, Zeng-Bing Chen, and Jian-Wei Pan, “Decoy-state quantum key distribution with polarized photons over 200 km,” Opt. Express 18, 8587-8594 (2010). (doi: 10.1364/OE.18.008587)

2. Rosenberg, D. et al. Practical long-distance quantum key distribution system using decoy qubits. New Journal of Physics, 11 (4), 045009 (2009). (doi: 10.1088/1367-2630/11/4/045009)

3. Korzh, B., Lim, C., Houlmann, R. et al. Provably secure and practical quantum key distribution over 307km of optical fibre. Nature Photon 9, 163168 (2015). (doi: 10.1038/nphoton.2014.327)

4. Alberto Boaron, Gianluca Bosco, Davide Rusca, Cdric Vuleiz, Claire Autembert, Misaal Caloz, Matthieu Perrenoud, Gatan Gras, Flix Bussires, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden, “Secure Quantum Key Distribution over 421 km of Optical Fiber”, Phys. Rev. Lett., vol. 121, 190502, Published 5 November 2018 (doi: 10.1103/PhysRevLett.121.190502)

5. Lucamarini, M et al. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature vol. 557, 7705 (2018). (doi: 10.1038/s41586-018-0066-6)

6. E. Diamanti, Security and implementation of differential phase shift quantum key distribution systems, Jan 2006.

7. M. Suda, T. Herbst, and A. Poppe, Simulating phase coding in quantum cryptography: Influence of chromatic dispersion, The European Physical Journal D, vol. 42, Jan 2007, 913915. (doi: 10.1140/epjd/e2006-00279-7)

8. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, Physical Review A, vol. 72, no. 3, Sep 2005. (doi: 10.1103/PhysRevA.72.032301)

9. P Eraerds and N Walenta and M Legré and N Gisin and H Zbinden, Quantum key distribution and 1 Gbps data encryption over a single fibre, New Journal of Physics, vol. 12, no. 6, Jun 2010 063027. (doi: 10.1088/1367-2630/12/6/063027)

10. Autembert, Claire & Gras, Gatan & Amri, Enna & Perrenoud, Matthieu & Caloz, Misaal & Zbinden, Hugo & Bussires, Flix. Direct measurement of the recovery time of superconducting nanowire single-photon detectors. (2020)

11. Chang, D., Vuleti, V. & Lukin, M. Quantum nonlinear optics photon by photon. Nature Photon 8, 685694 (2014). (doi: 10.1038/nphoton.2014.192)

12. Reid, M. D. and Walls, D. F., Quantum theory of nondegenerate four-wave mixing, Phys. Rev. A, vol. 34, issue 6, p. 4929-4955, Dec 1986. (doi: 10.1103/PhysRevA.34.4929)

13. Guerreiro, Thiago & Martin, Anthony & Sanguinetti, Bruno & Pelc, Jason & Langrock, C. & Fejer, M. & Gisin, Nicolas & Zbinden, Hugo & Sanguinard, N. & Thew, R.. (2014). Nonlinear Interaction between Single Photons. Physical Review Letters. 113. 173601. (doi: 10.1103/PhysRevLett.113.173601)

14. Bhawna Kairisagar and A. A. Koser, Effect of non linearity on dispersion length, AIP Conference Proceedings, vol. 2100, 1, p. 020200 (2019). (doi: 10.1063/1.5098754)

15. Michal Mlejnek, Nikolay A. Kaltsevskiy, Daniel A. Nolan, "Modeling high quantum bit rate QKD systems over optical fiber," Proc. SPIE 10674, Quantum Technologies 2018, 1067416 (21 May 2018). (doi:10.1117/12.2306875)

16. Dudin, Y. O. & Kuzmich, A. Strongly interacting Rydberg excitations of a cold atomic gas. Science 336, 887889 (2012).

17. Wang, H., He, Y., Chung, T. et al. Towards optimal single-photon sources from polarized microwaves. Nat. Photonics 13, 770775 (2019). (doi: 10.1038/s41566-019-04943-3)

18. Reimer, M.E., Cher, C. The quest for a perfect single-photon source. Nat. Photonics 13, 734736 (2019). (doi: 10.1038/s41566-019-0544-x)

19. Chen, X., Ding, C., Pan, H. et al. Temporal and spatial multiplexed infrared single-photon counter based on high-speed avalanche photodiode. Sci Rep 7, 44600 (2017). (doi: 10.1038/srep44600)

20. Z. Yuan et al., "10-Mb/s Quantum Key Distribution," in Journal of Lightwave Technology, vol. 36, no. 16, pp. 3427-3433, 15 Aug.15, 2018. (doi: 10.1109/JLT.2018.2843136)

21. C. Partridge and S. Pink, "A faster UDP (user datagram protocol)," in IEEE/ACM Transactions on Networking, vol. 1, no. 4, pp. 429-440, Aug. 1993. (doi: 10.1109/90.2512895)

22. Chen, Jiu-Peng et al. Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km. Physical review letters 124 7 (2020): 070501. (doi:10.1103/PhysRevLett.124.070501)
value of the minimum and the maximum distance, meaning the short-short travel and the long-long travel of the MZ interferometers. More specifically:

\[
x = \frac{\mu_{xx} + \mu_{dn}}{2} + \delta x
\]

\[= N_0 (l_g + 2l) + 2\delta_x k_0 + \frac{\Delta_j + \Delta_m}{2} + \delta x
\]  \hspace{1cm} (A.2)

where \(\delta x\) has been added to maintain the meaning of \(x\). See Fig. 10 for the visualisation of the meaning of \(\delta x\).

Fig. 10: Overview of the axis new zero point. Symbol viewed at the end of the setup (after second Mach-Zehnder).

Substituting Eq. (A.2) to Eq. (A.1) we get:

\[
z_{ij} - z_{kl} = \frac{\Delta_i + \Delta_j - \Delta_k - \Delta_l}{\gamma}
\]

\[\times \left\{ k_0 + 4(\delta k)^4 n(l_g + 2l) \right. \]

\[\times \left[ 2\delta_x + 4\delta_x k_0 + \Delta_d + \Delta_m \right.
\]

\[\left. - (\Delta_i + \Delta_j + \Delta_k + \Delta_l) \right\} \] \hspace{1cm} (A.3)

Substituting \(\gamma\) and after a few steps we get:

\[
z_{ij} - z_{kl} = \frac{2\pi}{\lambda_0} \left( \frac{\Delta_i + \Delta_j - \Delta_k - \Delta_l}{\gamma} \right)
\]

\[\times \left\{ 1 + \frac{\lambda_0 (1 - \frac{1}{2})}{4\pi n (l_g + 2l)} \right. \]

\[\times \left[ \delta_x + \frac{\Delta_d + \Delta_m - (\Delta_i + \Delta_j + \Delta_k + \Delta_l)}{2} \right] \] \hspace{1cm} (A.4)

We can easily see that the second term is much smaller than the first term for real numeric values \((l_g = 500000 nm, \lambda_0 = 1550 nm)\) and for the point we are interested \(\delta x = 0\) (midle of the received symbol). Therefore, we may say that:

\[
z_{ij} - z_{kl} \simeq \frac{2\pi}{\lambda_0} (\Delta_i + \Delta_j - \Delta_k - \Delta_l)
\]  \hspace{1cm} (A.5)

Equation (A.5) indicates that only the difference between the values of \(\Delta\) affects the result. Hence, we will set:

\[\Delta_\omega = \Delta + \phi_\omega \quad \text{where} \quad \omega \in \{i, j, k, l\} \] \hspace{1cm} (A.6)

where we used the letter \(\phi\), which is normally used for phase values, to keep in mind that we are looking for the phase correspondence.

The middle point that we are interested in is represented by the term \(z_{cm}, z_{dc}\) so the term \(\Delta_i + \Delta_j - \Delta_k - \Delta_l\) becomes \(\Delta_m - \Delta_d\); the sign is not important due to the cosine that follows.

We will start searching by setting for convenience these two values equal to zero; meaning \(\phi_m = \phi_d = 0\), so the cosine term is precisely equal to 1. Now, for this choice we need to change only the \(\phi_d\) so as to invert the outputs. It is easy to find that we can accomplish this by choosing \(\phi_d = \frac{\pi}{2}\), which corresponds to a phase equal to \(\pi\), so, now, the cosine is approximately equal to -1 (instead of 1), indicating that the outputs were inverted.

So far, we have defined the first basis. We also need to find the second one. It must be chosen such that if Bob reads in respect to the second one but Alice has modulated the qubit using the first one, Bob will not be able to decode any information.

A reasonable choice for this to happen is by choosing the second basis to be modulated by adding a phase equal to \(\frac{\pi}{2}\); meaning \(\phi_m = \frac{\lambda_0}{4}\). We can see that in this case if Alice sends a symbol which has been modulated using the first basis \((\phi_d = 0 \text{ or } \phi_d = \frac{\pi}{2})\) and Bob reads this symbol by applying \(\phi_m = \frac{\lambda_0}{4}\), the cosine for both cases are approximately zero, thereby they have the same detection probability to each output.

By the same logic, we can see that Alice needs to modulate applying \(\phi_d = \frac{\lambda_0}{4} \text{ or } \phi_d = \frac{3\lambda_0}{4}\) in order for Bob to be able to read when \(\phi_m = \frac{\lambda_0}{4}\).

At last, we have find the two bases that we wanted and our results can be confirmed by our simulations in the main text. Summing up, we have that Alice creates the qubits by applying:

\[
\phi_d = \begin{cases} 0 \text{ or } \frac{\pi}{2}, & \text{basis X} \\ \frac{\lambda_0}{4} \text{ or } \frac{3\lambda_0}{4}, & \text{basis Z} \end{cases}
\]  \hspace{1cm} (A.7)

where the first value from each row, usually corresponds to bit 0 and the second one to bit 1. Bob reads the qubits by applying:

\[
\phi_m = \begin{cases} 0, & \text{basis X} \\ \frac{\lambda_0}{4}, & \text{basis Z} \end{cases}
\]  \hspace{1cm} (A.8)