 doi:10.20944/preprints201803.0228.v1

Article

Quantification of the Impact of Photon Distinguishability on Measurement-Device-Independent Quantum Key Distribution

Garrett K. Simon [1], Blake K. Huff [1], William M. Meier [1], Logan O. Mailloux [2] and Lee E. Harrell [1]*

[1] Department of Physics and Nuclear Engineering, United States Military Academy, West Point, NY 10996, United States

[2] Department of Systems Engineering, Center for Cyberspace Research, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, United States

* Correspondence: lee.harrell@usma.edu; Tel.: +1-845-938-5012

Abstract: Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) is a two-photon protocol devised to eliminate eavesdropping attacks that interrogate or control the detector in realized quantum key distribution systems. In MDI-QKD, the measurements are carried out by an untrusted third party, and the measurement results are announced openly. Knowledge or control of the measurement results gives the third party no information about the secret key. Error-free implementation of the MDI-QKD protocol requires the crypto-communicating parties, Alice and Bob, to independently prepare and transmit single photons that are physically indistinguishable, with the possible exception of their polarization states. In this paper, we apply the formalism of quantum optics and Monte Carlo simulations to quantify the impact of small errors in wavelength, bandwidth, polarization and timing between Alice's photons and Bob's photons on the MDI-QKD quantum bit error rate (QBER). Using published single-photon source characteristics from two-photon interference experiments as a test case, our simulations predict that the finite tolerances of these sources contribute $(4.04 \pm 20/\sqrt{N_{\text{sifted}}})\%$ to the QBER in an MDI-QKD implementation generating an N_{sifted}-bit sifted key.

Keywords: Measurement-Device-Independent Quantum Key Distribution; Quantum Optics; Two-Photon Interference

1. Introduction

Quantum Key Distribution (QKD) is an application of quantum cryptography—the process of exploiting quantum effects to establish secure communications between two authorized users, Alice and Bob, in the presence of an unwanted third party, Eve. QKD protocols promise unconditionally secure communications through exchange of encoded photons, which, due to their quantum nature, are altered in a detectable way if they are observed by an unauthorized eavesdropper [1].

In conventional QKD protocols such as BB84 [2], the original QKD protocol, a photon is randomly encoded in one of a pre-determined set of quantum states by Alice. Alice transmits the photon to Bob who obtains partial information on Alice's encoding by performing a randomly selected projective measurement on the photon. Subsequently Alice reveals partial information on her encoding over an open classical channel. Along with the measurement results, this additional information allows Bob to identify the original encoding state of a subset of the transmitted photons with certainty. The encoding of this subset constitutes the raw shared secret key that Alice and Bob use for encrypted

 doi:10.20944/preprints201803.0228.v1

communications [3]. Because Eve does not have access to the results of Bob's measurements, she lacks the necessary information to infer the secret bits.

Since 1984, other protocols have been proposed to address security vulnerabilities in implementations of BB84 [4–7]. One such protocol is Measurement-Device-Independent QKD (MDI-QKD), depicted in Figure 1, which addresses the vulnerability of Bob's measurement to malicious signals introduced on the quantum channel by Eve. MDI-QKD moves the act of photon measurement from Bob to an untrusted third party, Charlie (shown in red). Alice and Bob each send one polarization-encoded photon to Charlie, who subjects them to two-photon interference in a symmetric 50:50 beam splitter, followed by polarization-sensitive detection via a pair of polarizing beam splitters and four single-photon detectors, each corresponding to a polarization and beam splitter output port (d_V, d_H, c_V, c_H). Charlie publicly announces which detectors registered photons. Subsequently, Alice and Bob publicly announce which polarization basis (horizontal-vertical or antidiagonal-diagonal) they used for encoding. From this information and their private knowledge of their own photon encodings, Alice and Bob can infer one bit of shared secret key in 25% of the exchanges under ideal circumstances. Figure 2 demonstrates these steps explicitly for two key attempts—one in the horizontal-vertical basis and one in the antidiagonal-diagonal basis. The blue and green arrows denote communication on a sensitive quantum channel, while red arrows denote communication on an open classical channel visible to Charlie. Similarly, Table 1 displays all possible same-basis input states, Charlie's potential detection states for each input, and the shared bit value associated with a given input state. When Alice and Bob choose opposite encoding bases for a trial, that trial is discarded, and no key is generated. The same-basis inputs $|V\rangle|V\rangle$ and $|H\rangle|H\rangle$ cannot be used to generate a key bit because Charlie can infer the bit from his measurement and knowledge of the encoding basis. There are also some detected states for antidiagonal-diagonal basis encodings that can occur for multiple input states, making them unusable for key generation.

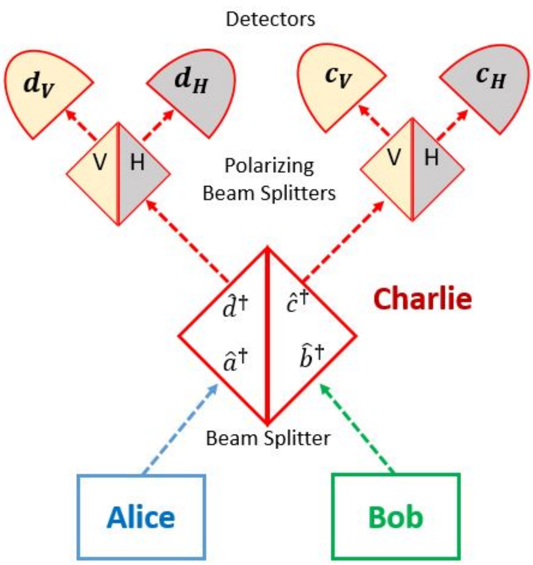


Figure 1. Diagram of MDI-QKD instrumentation.

Despite its immunity from eavesdropping attacks on the detector, MDI-QKD is susceptible to physical non-idealities that can limit the key generation rate by introducing quantum bit errors, which are physically indistinguishable from perturbations caused by Eve's measurements [8]. In addition to detector inefficiencies, dark count rates [9] and polarization errors, MDI-QKD is also susceptible to bit errors caused by timing differences [7] and photon distinguishability in pulse envelope, bandwidth and wavelength [10]. Prior research has addressed polarization and timing errors [9], as well as the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 March 2018 doi:10.20944/preprints201803.0228.v1

feasibility of implementing the protocol utilizing weak coherent pulses from independent laser sources [10], but significant assumptions about photon source characteristics remain unexplored.

In this paper, we analyze the impact of error tolerances in photon polarization encoding, timing, wavelength and bandwidth on the quantum bit error rate (QBER) of an otherwise ideal MDI-QKD implementation using single photon sources with Gaussian pulse envelopes. In section 2 we specify the photon temporal wave functions and apply the formalism of quantum optics to calculate probabilities for Charlie's measurement outcomes as a function of Alice's and Bob's encoding choices and the tolerances of their photon sources. In section 3 we describe our Monte Carlo simulation of the MDI-QKD protocol based on these probabilities to determine the associated Quantum Bit Error Rate (QBER). In section 4 we present the results of our simulations and discuss the sensitivity of MDI-QKD to various contributions to photon distinguishability. We conclude the paper in section 5 with a discussion of the implications of our results for studying practical implementations of MDI-QKD and identify possible extensions to our work.

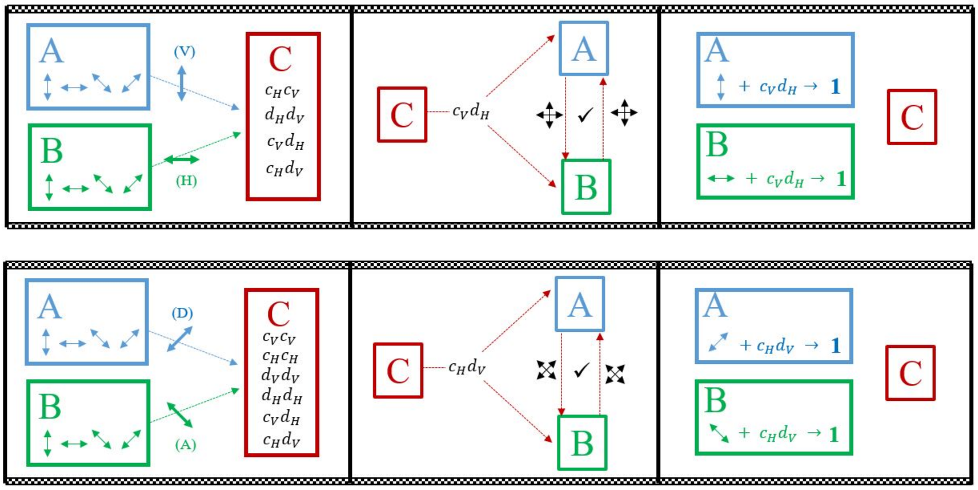


Figure 2. Representative sequences of events for the MDI-QKD protocol for two particular input states.

Table 1. Nominal probability of generating a key bit and the shared secret bit value for all eight same-basis photon polarization encodings and associated measurement outcomes.

Alice Polarization	Bob Polarization	Possible Detected States	Probability of generating a usable detection state	Shared Bit Value
$\updownarrow\ \lvert V\rangle$	$\leftrightarrow\ \lvert H\rangle$	Usable: $c_V c_H$, $d_V d_H$, $c_V d_H$, $c_H d_V$ Unusable: *none*	$4 \times 25\% = 100\%$	1
$\leftrightarrow\ \lvert H\rangle$	$\updownarrow\ \lvert V\rangle$		$4 \times 25\% = 100\%$	0
$\updownarrow\ \lvert V\rangle$	$\updownarrow\ \lvert V\rangle$	Unusable: $c_V c_V$, $d_V d_V$ Usable: *none*	0%	---
$\leftrightarrow\ \lvert H\rangle$	$\leftrightarrow\ \lvert H\rangle$	Unusable: $c_H c_H$, $d_H d_H$ Usable: *none*		
$\searrow\ \lvert A\rangle$	$\searrow\ \lvert A\rangle$	Usable: $c_H c_V$, $d_H d_V$ Unusable: $c_H c_H$, $d_H d_H$, $c_V c_V$, $d_V d_V$	$2 \times 25\% = 50\%$	0
$\nearrow\ \lvert D\rangle$	$\nearrow\ \lvert D\rangle$		$2 \times 25\% = 50\%$	1
$\searrow\ \lvert A\rangle$	$\nearrow\ \lvert D\rangle$	Usable: $c_H d_V$, $c_V d_H$ Unusable: $c_H c_H$, $d_H d_H$, $c_V c_V$, $d_V d_V$	$2 \times 25\% = 50\%$	0
$\nearrow\ \lvert D\rangle$	$\searrow\ \lvert A\rangle$		$2 \times 25\% = 50\%$	1

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 March 2018 doi:10.20944/preprints201803.0228.v1

2. Two-Photon Interference in the Polarizing Beam Splitter.

The MDI-QKD protocol relies on quantum interference of two indistinguishable photons incident on a 50:50 beam splitter [9,11]. This interference, known as the Hong-Ou-Mandel (HOM) effect, suppresses the probability that two identical photons simultaneously entering the beam splitter through different ports will be detected exiting the beam splitter through different ports; they must always exit the beam splitter together [12]. Distinguishable photons under the same circumstances show no such correlations. Ideally, photons employed in MDI-QKD are identical in every physical characteristic except (potentially) their polarization angles. Under these conditions, two identically polarized photons will always exhibit HOM interference; however, non-idealities in the photon sources or beam splitter characteristics give rise to partial distinguishability and a non-zero probability of unexpected coincidence events—observation of ostensibly indistinguishable photons exiting different beam splitter ports [10,13,14].

We apply the formalism of quantum optics following the development of Loudon [15] to relate the probabilities of coincidence events, and ultimately the performance limits of MDI-QKD systems, to photon source tolerances. Alice and Bob independently prepare single photon pulses characterized by temporal wave functions $\xi_{\mathrm{a,b}}(t)$ and polarization angles $\theta_{\mathrm{a,b}}$. The input state at the beam splitter is then the product state

$$
\begin{aligned}
|\xi_{\mathrm{a}},\theta_{\mathrm{a}}\rangle \otimes |\xi_{\mathrm{b}},\theta_{\mathrm{b}}\rangle = \int \mathrm{d}t_1 \xi_{\mathrm{a}}(t_1) \left[\hat{a}^\dagger_{\mathrm{H}}(t_1)\cos\theta_{\mathrm{a}} + \hat{a}^\dagger_{\mathrm{V}}(t_1)\sin\theta_{\mathrm{a}}\right] & \\
\int \mathrm{d}t_2 \xi_{\mathrm{b}}(t_2) \left[\hat{b}^\dagger_{\mathrm{H}}(t_2)\cos\theta_{\mathrm{b}} + \hat{b}^\dagger_{\mathrm{V}}(t_2)\sin\theta_{\mathrm{b}}\right]|0\rangle, & \quad (1)
\end{aligned}
$$

where $\hat{a}^\dagger_{\mathrm{H,V}}(t)$ and $\hat{b}^\dagger_{\mathrm{H,V}}(t)$ are the creation operator densities for horizontally and vertically polarized photons at the a and b beam splitter inputs, and $|0\rangle$ is the 4-mode vacuum. Normalization is achieved by requiring

$$
\int \mathrm{d}t \xi^*_{\mathrm{a}}(t)\xi_{\mathrm{a}}(t) = \int \mathrm{d}t \xi^*_{\mathrm{b}}(t)\xi_{\mathrm{b}}(t) = 1. \quad (2)
$$

The beam splitter output state $|\psi_{\mathrm{out}}\rangle$ can be constructed from the input state using the beam splitter transformation,

$$
\begin{aligned}
\hat{a}^\dagger_{\mathrm{H,V}}(t) &\longrightarrow T\hat{c}^\dagger_{\mathrm{H,V}}(t) + R\hat{d}^\dagger_{\mathrm{H,V}}(t) \\
\hat{b}^\dagger_{\mathrm{H,V}}(t) &\longrightarrow R\hat{c}^\dagger_{\mathrm{H,V}}(t) + T\hat{d}^\dagger_{\mathrm{H,V}}(t),
\end{aligned} \quad (3)
$$

where T and R are the transmission and reflection amplitudes of the symmetric beam splitter, subject to the unitarity conditions

$$
\begin{aligned}
|T|^2 + |R|^2 &= 1 \\
TR^* &= -T^*R,
\end{aligned} \quad (4)
$$

and $\hat{c}^\dagger_{\mathrm{H,V}}(t)$ and $\hat{d}^\dagger_{\mathrm{H,V}}(t)$ are the creation operator densities for horizontally and vertically polarized photons at the c and d beam splitter outputs. Applying (3) to (1) we find

$$
\begin{aligned}
|\psi_{\mathrm{out}}\rangle = \int \mathrm{d}t_1 \xi_{\mathrm{a}}(t_1) \left[(T\hat{c}^\dagger_{\mathrm{H}}(t_1) + R\hat{d}^\dagger_{\mathrm{H}}(t_1))\cos\theta_{\mathrm{a}} + (T\hat{c}^\dagger_{\mathrm{V}}(t_1) + R\hat{d}^\dagger_{\mathrm{V}}(t_1))\sin\theta_{\mathrm{a}}\right] & \\
\int \mathrm{d}t_2 \xi_{\mathrm{b}}(t_2) \left[(R\hat{c}^\dagger_{\mathrm{H}}(t_2) + T\hat{d}^\dagger_{\mathrm{H}}(t_2))\cos\theta_{\mathrm{b}} + (R\hat{c}^\dagger_{\mathrm{V}}(t_2) + T\hat{d}^\dagger_{\mathrm{V}}(t_2))\sin\theta_{\mathrm{b}}\right]|0\rangle. & \quad (5)
\end{aligned}
$$

The right hand side of (5) can be written as a summation of terms each contributing amplitudes to one of the ten mutually exclusive experimental outcomes:

$$|\psi_{\text{out}}\rangle = |c_V c_V\rangle + |c_H c_H\rangle + |d_V d_V\rangle + |d_H d_H\rangle + |c_V c_H\rangle + |d_V d_H\rangle + |c_V d_V\rangle + |c_H d_H\rangle + |c_H d_V\rangle + |c_V d_H\rangle, \tag{6}$$

where, for example,

$$|c_V d_V\rangle = \int\int \mathrm{d}t_1 \mathrm{d}t_2 \xi_{\mathrm{a}}(t_1)\xi_{\mathrm{b}}(t_2) \sin\theta_{\mathrm{a}} \sin\theta_{\mathrm{b}} \left(T^2 \hat{c}_V^\dagger(t_1)\hat{d}_V^\dagger(t_2) + R^2 \hat{d}_V^\dagger(t_1)\hat{c}_V^\dagger(t_2)\right)|0\rangle \tag{7}$$

corresponds to the outcome in which one photon is counted in detector c_V and one photon is counted in detector d_V. The probability of the outcome $c_V d_V$ is then

$$P(c_V d_V) = \langle c_V d_V | c_V d_V \rangle. \tag{8}$$

The dependance of the outcome probabilities on the photon wave functions can be expressed in terms of the overlap integral [15]

$$|J|^2 = \left| \int dt \xi_{\mathrm{a}}^*(t)\, \xi_{\mathrm{b}}(t) \right|^2. \tag{9}$$

With $|J|^2$ as defined in (9), the probabilities for each of the detection events are

$$\begin{aligned}
P(c_V c_V) &= P(d_V d_V) = \sin^2\theta_{\mathrm{a}} \sin^2\theta_{\mathrm{b}} |T|^2 |R|^2 \left(1 + |J|^2\right) \\
P(c_H c_H) &= P(d_H d_H) = \cos^2\theta_{\mathrm{a}} \cos^2\theta_{\mathrm{b}} |T|^2 |R|^2 \left(1 + |J|^2\right) \\
P(c_V c_H) &= P(d_V d_H) = |T|^2 |R|^2 \left(\sin^2\theta_{\mathrm{a}} \cos^2\theta_{\mathrm{b}} + \cos^2\theta_{\mathrm{a}} \sin^2\theta_{\mathrm{b}} + 2\sin\theta_{\mathrm{a}} \cos\theta_{\mathrm{a}} \sin\theta_{\mathrm{b}} \cos\theta_{\mathrm{b}} |J|^2\right) \\
P(c_V d_H) &= \sin^2\theta_{\mathrm{a}} \cos^2\theta_{\mathrm{b}} |T|^4 + \cos^2\theta_{\mathrm{a}} \sin^2\theta_{\mathrm{b}} |R|^4 - 2\cos\theta_{\mathrm{a}} \sin\theta_{\mathrm{a}} \cos\theta_{\mathrm{b}} \sin\theta_{\mathrm{b}} |T|^2 |R|^2 |J|^2 \\
P(c_H d_V) &= \sin^2\theta_{\mathrm{a}} \cos^2\theta_{\mathrm{b}} |R|^4 + \cos^2\theta_{\mathrm{a}} \sin^2\theta_{\mathrm{b}} |T|^4 - 2\cos\theta_{\mathrm{a}} \sin\theta_{\mathrm{a}} \cos\theta_{\mathrm{b}} \sin\theta_{\mathrm{b}} |T|^2 |R|^2 |J|^2 \\
P(c_V d_V) &= \sin^2\theta_{\mathrm{a}} \sin^2\theta_{\mathrm{b}} \left(1 - 2|T|^2 |R|^2 \left(1 + |J|^2\right)\right) \\
P(c_H d_H) &= \cos^2\theta_{\mathrm{a}} \cos^2\theta_{\mathrm{b}} \left(1 - 2|T|^2 |R|^2 \left(1 + |J|^2\right)\right).
\end{aligned} \tag{10}$$

In order to make specific predictions, we model the photon wave functions $\xi(t)_{\mathrm{a,b}}$ as Gaussian wave packets with center angular frequency $\omega_{\mathrm{a,b}}$, bandwidth $\Delta\omega_{\mathrm{a,b}}$, and beam splitter arrival time $t_{\mathrm{a,b}}$. Using the normalized wave functions

$$\xi_{\mathrm{a,b}}(t) = \left(\frac{2\Delta\omega_{\mathrm{a,b}}^2}{\pi}\right)^{1/4} e^{-i\omega_{\mathrm{a,b}}t - \Delta\omega_{\mathrm{a,b}}^2 (t - t_{\mathrm{a,b}})^2}, \tag{11}$$

the overlap integral evaluates to

$$|J|^2 = \frac{2\Delta\omega_{\mathrm{a}}\Delta\omega_{\mathrm{b}}}{\Delta\omega_{\mathrm{a}}^2 + \Delta\omega_{\mathrm{b}}^2} \exp\left(-\frac{(\omega_{\mathrm{a}} - \omega_{\mathrm{b}})^2}{2\left(\Delta\omega_{\mathrm{a}}^2 + \Delta\omega_{\mathrm{b}}^2\right)}\right) \exp\left(-\frac{4\Delta\omega_{\mathrm{a}}^2 \Delta\omega_{\mathrm{b}}^2 (t_{\mathrm{a}} - t_{\mathrm{b}})^2}{2\left(\Delta\omega_{\mathrm{a}}^2 + \Delta\omega_{\mathrm{b}}^2\right)}\right). \tag{12}$$

Combining (10) and (12) we model the HOM effect, as in Figure 3, where the incomplete suppression of coincidence events as a result of photon wavelength and pulse bandwidth differences is

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 March 2018 doi:10.20944/preprints201803.0228.v1

apparent. We also use these results in Monte Carlo simulations of the MDI-QKD protocol, as discussed in section 3, to determine the associated QBER.

3. Monte Carlo Simulation Methodology

To determine the MDI-QKD QBER for achievable single photon source tolerances, we perform Monte Carlo simulations utilizing the probabilities of (10) and the overlap integral of (12). The single photon source parameters (wavelength $\lambda = 788$ nm, wavelength tolerance $\sigma_\lambda = 0.17$ nm, pulse bandwidth $\Delta\omega = 1.18 \times 10^{12}$ rad/s, pulse bandwidth tolerance $\sigma_{\Delta\omega} = 1.18 \times 10^{10}$ rad/s, synchronization tolerance $\sigma_t = 0.26$ ps, and polarization angle tolerance $\sigma_\theta = 1°$) are selected consistently with those described by Kaltenbaek et al. [16], who report a $(96 \pm 1)\%$ HOM-interference visibility using independent single photon sources in an entanglement swapping experiment that is functionally identical to a MDI-QKD implementation. They report the standard deviation of their pulse synchronization and the full-width-at-half-maximum of the filters used to limit fluctuations in the photon wavelengths. We estimate the bandwidth of their pulses on the basis of the width of their HOM-dips and assume a 1% relative fluctuation. The assumed polarization standard deviation is typical of laboratory optics [17]. The results of [16] are particularly relevant because the two photon sources used are completely independent, communicating only via an electronic synchronization signal, just as required for MDI-QKD. The simulation procedure is outlined below, and the code is available in the online supplement.

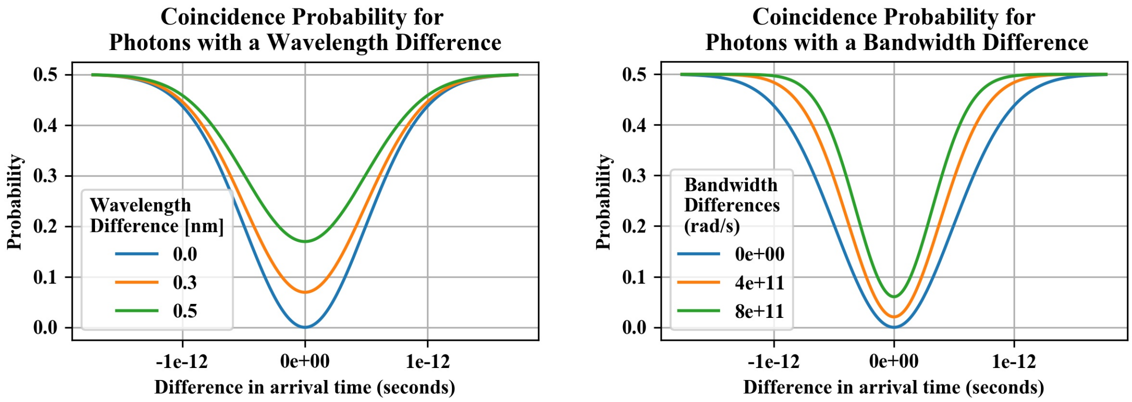
(1) Construct N_{raw}-element arrays of Alice's and Bob's randomly selected basis choices.
(2) Construct N_{raw}-element arrays of Alice's and Bob's randomly selected raw keys bits.
(3) Compare Alice's and Bob's random basis selections and discard trials corresponding to opposite-basis selection from further consideration, retaining $N_{\text{same}} \approx N_{\text{raw}}/2$ trials.
(4) Compute the photon polarization angles for each photon in each trial from the choices of basis, raw key bits, and polarization error tolerances.
(5) Compute the photon wavelength errors for each photon in each trial from the photon wavelength tolerances.
(6) Compute the bandwidth of each photon pulse in each trial from the mean bandwidth and the bandwidth tolerances.
(7) Compute the photon arrival time synchronization error for each trial from the synchronization time tolerance.
(8) Use the results of steps (4) through (7) to calculate the probability of each possible measurement outcome for each trial.
(9) For each trial select a particular measurement outcome in accordance with the probabilities calculated in step (8).
(10) Discard unusable trials and flip Bob's key bit in accordance with the results of step (9), retaining $N_{\text{sifted}} \approx N_{\text{raw}}/4$ bits.
(11) Compare Alice's and Bob's sifted keys to determine the QBER= $N_{\text{error}}/N_{\text{sifted}}$ [18].

4. Simulation Results and Discussion

With the above methodology, averages over repeated simulations using raw keys with lengths $N_{\text{raw}} = 100$ to 1,024,000 bits give QBERs of $(4.04 \pm 20/\sqrt{N_{\text{sifted}}})\%$. These results are consistent with the HOM-interference visibility reported in [16]. The fraction of bits discarded due to opposite basis selection or unusable measurement results are also in line with expectations—approximately 25% of the raw key bits are retained in the sifted key.

Additionally, we explore the consequences of systematically relaxing photon source tolerances to determine the sensitivity of the QBER to fluctuations in wavelength, pulse bandwidth, polarization angle, and source synchronization. The results of these simulations are shown in Figure 4. Each point in the figure represents the average QBER from 100 iterations with $N_{\text{raw}} = 2,500$ for a fixed set of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 March 2018 doi:10.20944/preprints201803.0228.v1



(a) Wavelength **(b)** Bandwidth

Figure 3. Coincidence probability as a function of beam splitter arrival time difference for photon pairs. The coincidence rate vanishes for perfectly identical photons arriving simultaneously, with the width of the HOM dip determined by the pulse bandwidth. The various curves illustrate the effects on the HOM dip of partial photon distinguishability due to differences in **(a)** wavelength, and **(b)** pulse bandwidth.

photon source parameters. The standard deviations of **(a)** photon wavelength, **(b)** pulse bandwidth, **(c)** polarization angle, and **(d)** photon synchronization are varied relative to their nominal values, indicated by orange diamonds, while other photon source parameters are held fixed. As expected, the QBER increases with increasing probability of photon distinguishability due to source fluctuations.

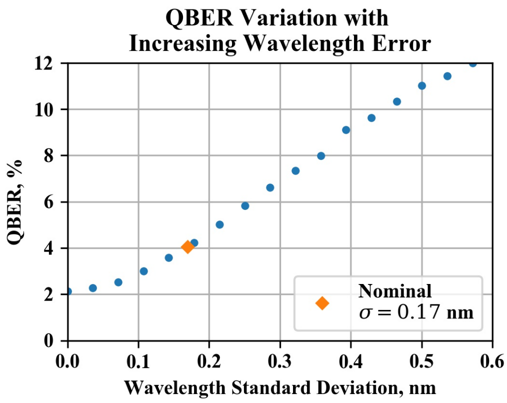
In simulating the MDI-QKD protocol, we have given special attention to the achievable QBER. While the QBER drives the resource impact of error correction protocols on the system's ability to generate key, it also has implications for the ability of the QKD system to generate unconditionally secure keys. The presence of an eavesdropper on the quantum channel generates bit errors that are physically indistinguishable from bit errors arising from finite system tolerances. Consequentially, security analysis of QKD systems attributes all bit errors to information gained through measurements by an eavesdropper [1]. Provided the QBER does not exceed some protocol-dependent limit, it is possible to apply error correction and privacy amplification procedures to resolve bit errors and mitigate privacy concerns [19]. For instance, the theoretically maximum allowable BB84 QBER is 11% [20]. The fundamental QBER limit for MDI-QKD remains a subject for future study.

The practical implementation of MDI-QKD depends on limiting bit errors due to incomplete HOM interference. By simulating the MDI-QKD protocol using photon source tolerances from a well-characterized two-photon interference study, we demonstrate both good agreement with experiment and the ability to relate the achievable visibility to fluctuations in specific photon properties. From the plots in Figure 4, it is clear that the QBER is sensitive to both photon wavelength and pulse timing. Modest increases in the trial-to-trial fluctuations of photon wavelengths and arrival times lead to significant increases in the QBER, while suppressing either of these fluctuations results in a factor of two improvement. In contrast, the QBER is relatively insensitive to changes in the bandwidth standard deviation and polarization angle standard deviation, even if these fluctuations are suppressed entirely.

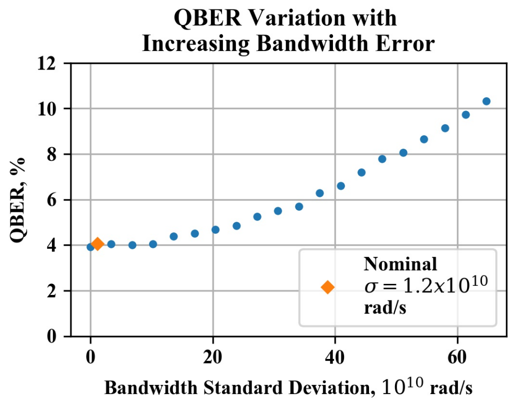
The sensitivity of the QBER to wavelength and timing fluctuations points to the need for design tradeoffs to optimize system performance. In the experiment of [16], wavelength fluctuations are limited by narrow filters that block out-of-tolerance photons from reaching the detectors. While this enhances the HOM visibility, it also reduces the detection rate. As QKD performance is measured on the basis of the rate at which secret key can be generated, there is a point of diminishing returns when the QBER is improved at the the expense of transmission rate. Similar reasoning applies to photon

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 27 March 2018 doi:10.20944/preprints201803.0228.v1

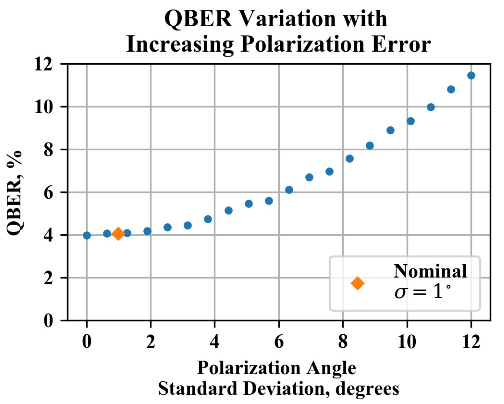
synchronization if improvements in the timing of pulse generation come at the expense of a reduced probability of generating a photon. A reduction in the detection rate could also occur with tighter polarization angle and pulse bandwidth control without improvement in the QBER, thus reducing overall QKD system performance.



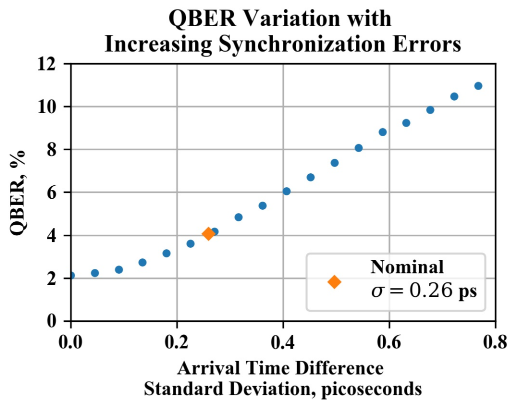
(a) Wavelength



(b) Bandwidth



(c) Polarization



(d) Timing

Figure 4. Dependance of QBER on individual photon source tolerances.

Even though the QBER is not particularly sensitive to bandwidth fluctuations in the region of parameter space under consideration, the sensitivity to pulse synchronization is closely related to the nominal bandwidth. As the bandwidth is inversely proportional to the temporal width of the pulse, larger bandwidth pulses are shorter in duration, thus requiring tighter synchronization tolerances to ensure large wave function overlap, reliable HOM interference, and a low QBER. We also note that the use of very narrow wavelength filters has the potential to complicate the analysis by altering the shape of the photon wave function.

5. Conclusions

These results are significant to the development of physics-based modeling of HOM interference in MDI-QKD. The next logical step in this program is to incorporate our model into a system-level simulation such as the qkdX framework [21] that fully incorporates the effects of photon propagation, transmission losses, detector limitations and security enhancing variations of the MDI-QKD protocol [22,23]. This work could also be extended to consider other types of pulse shapes or probability

 doi:10.20944/preprints201803.0228.v1

distributions, and to account for the effects of optical filters on the shape of the photon wave function envelope. Ultimately, these enhancements will lead to high-fidelity simulations that expedite the development of robust MDI-QKD implementations.

Acknowledgments: This work was funded in part by the United States Military Academy Department of Physics and Nuclear Engineering. We would like to acknowledge the contributions from Jeffrey Morris in familiarizing us with QKD concepts and the MDI-QKD protocol. The conclusions of this work are those of the authors and do not reflect official positions of the Department of the Army or the Department of Defense. As employees of the U.S. Government, the authors' copyright interest are subject to limitations under U.S. copyright law. This manuscript has been cleared for public release.

Author Contributions: G.S. extended the MDI-QKD model to arbitrary photon temporal wave functions, ran the simulations, and conducted the analysis. B.H and W.M. developed and validated the MDI-QKD simulations. L.M. proposed the study, conducted background research, identified the critical parameters in need of modeling and simulation, and provided ongoing guidance as the work progressed. L.H. fully incorporated arbitrary source polarizations into the model and provided direct supervision of the project.

Conflicts of Interest: The authors declare no conflict of interest. The founding sponsors had no role in the design of the study; in the collection, analysis, or interpretation of data; in the writing of the manuscript, and in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

QKD	Quantum key distribution
MDI-QKD	Measurement-device-independent quantum key distribution
QBER	Quantum bit error rate
BB84	Bennett and Brassard 1984
HOM	Hong-Ou-Mandel
BS	Beam splitter
PBS	Polarizing beam splitter
HV	Horizontal-vertical
AD	Antidiagonal-diagonal

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Reviews of Modern Physics* **2002**, *74*, 145–195.
2. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. Proceedings of IEEE International Conference on Computers, Systems & Signal Processing (Bangalore, India, December 1984); IEEE: New York, 1984; Vol. 1, pp. 175–179.
3. Liao, Z. Experimental Realization of Decoy State Polarization Encoding Measurement-Device-Independent Quantum Key Distribution. Master's thesis, University of Toronto, Toronto, Canada, 2013.
4. Mailloux, L.O.; Grimaila, M.R.; Engle, R.D.; Mclaughlin, C.V.; Baumgartner, G.B. Using Modeling and Simulation to Study Photon Number Splitting Attacks. *IEEE Access* **2016**, *4*, 2188–2197.
5. Scarani, V.; Kurtsiefer, C. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science* **2014**, *560*, 27–32.
6. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A* **2006**, *74*, 022313.
7. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics* **2015**, *21*, 148–158.
8. Scarini, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Reviews of Modern Physics* **2009**, *81*, 1301–1350.
9. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters* **2012**, *108*, 130503.
10. Lo, H.K.; Curty, M.; Qi, B. Supplemental Information for 'Measurement-device-independent quantum key distribution'. *Physical Review Letters* **2012**, *108*, 130503.

 doi:10.20944/preprints201803.0228.v1

11. Russell, M.; Mailloux, L.; Hodson, D.; Grimaila, M. A Bell State Analyzer Model for Measurement Device Independent Quantum Key Distribution. Proceedings of the 2017 International Conference on Scientific Computing; American Council on Science and Education, CSREA Press: Las Vegas, Nevada, 2017; pp. 127–133.
12. Hong, C.K.; Ou, Z.Y.; Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters* **1987**, *59*, 2044–2046.
13. Mährlein, S.; Oppel, S.; Wiegner, R.; von Zanthier, J. Hong-Ou-Mandel interference without beam splitters. *Journal of Modern Optics* **2017**, *64*, 921–929.
14. Kobayashi, T.; Ikuta, R.; Yasui, S.; Miki, S.; Yamashita, T.; Terai, H.; Yamamoto, T.; Koashi, M.; Imoto, N. Frequency-domain Hong-Ou-Mandel Interference. *Nature Photonics* **2016**, *10*, 441–444.
15. Loudon, R. *The Quantum Theory of Light*, 3 ed.; Oxford University Press, 2000.
16. Kaltenbaek, R.; Prevedel, R.; Aspelmeyer, M.; Zeilinger, A. High-fidelity entanglement swapping with fully independent sources. *Physical Review A* **2009**, *79*, 40302.
17. Barbarow, W.S. Finding the Optimal Polarizer, https://www.meadowlark.com, 2009 (accessed February 18, 2018).
18. Elmabrok, O.; Razavi, M. Wireless quantum key distribution in indoor environments. *Journal of the Optical Society of America B* **2018**, *35*.
19. Kosloski, J.T. QKD Quantum Channel Authentication. *eprint* **2006**, [arXiv:quant-ph/0603101].
20. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters* **2000**, *85*, 441–444.
21. Mailloux, L.O.; Morris, J.D.; Grimaila, M.R.; Hodson, D.D.; Jacques, D.R.; Colombi, J.M.; McLaughlin, C.V.; Holes, J.A. A Modeling Framework for Studying Quantum key Distribution System Implementation Nonidealities. *IEEE Access* **2015**, *3*, 110–130.
22. Wu, C.F.; Du, Y.; Wang, J.D.; Wei, Z.J.; Qin, X.J.; Zhao, F.; Zhang, Z.M. Analysis on performance optimization in measurement-device-independent quantum key distribution using weak coherent states. *Acta Physica Sinica* **2016**, *65*.
23. Zhu, F.; Zhang, C.H.; Liu, A.P.; Wang, Q. Enhancing the performance of the measurement-device-independent quantum key distribution with heralded pair-coherent sources. *Physics Letters A* **2016**, *380*, 1408–1413.