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

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

[1] Department of Physics and Nuclear Engineering, United States Military Academy, West Point, NY 10996, USA; Garrett.Simon@usma.edu (G.K.S.); Blake.Huff@usma.edu (B.K.H.); william.meier@usma.edu (W.M.M.)

[2] Department of Systems Engineering, Center for Cyberspace Research, Air Force Institute of Technology, Wright-Patterson Air Force Base, OH 45433, USA; Logan.Mailloux@afit.edu

* 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 communications [3]. As 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 [4–8]. 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 announced 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.
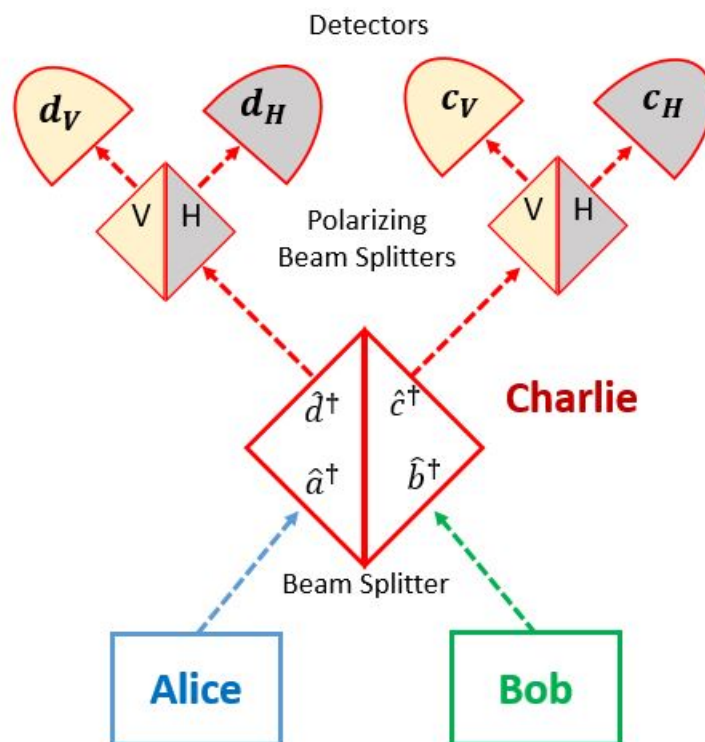

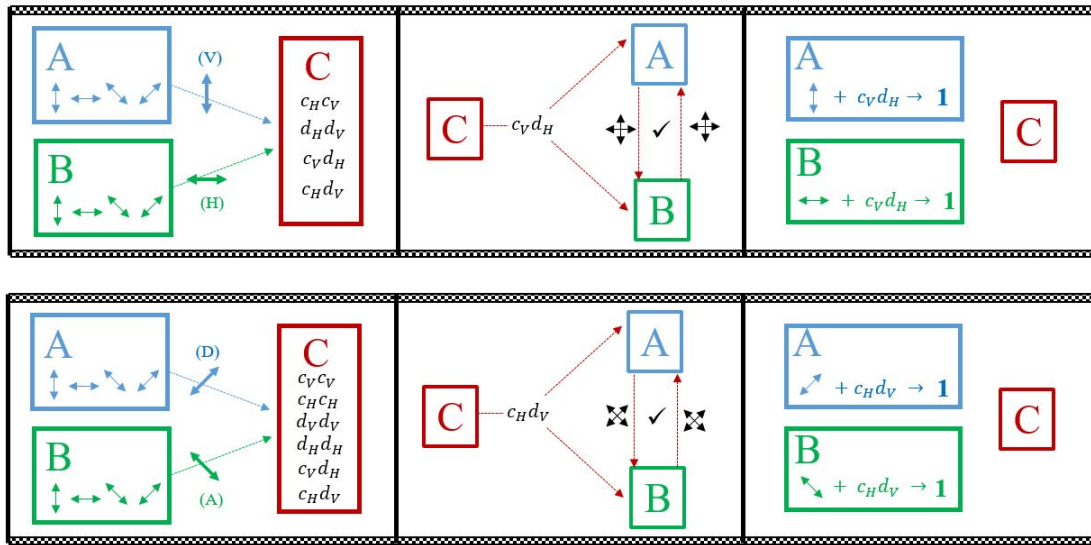**Figure 1.** Diagram of MDI-QKD instrumentation.

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
$\updownarrow$ $|V\rangle$	$\leftrightarrow$ $|H\rangle$	Usable: $c_V c_H$, $d_V d_H$, $c_V d_H$, $c_H d_V$	$4 \times 25\% = 100\%$	1
$\leftrightarrow$ $|H\rangle$	$\updownarrow$ $|V\rangle$	Unusable: *none*	$4 \times 25\% = 100\%$	0
$\updownarrow$ $|V\rangle$	$\updownarrow$ $|V\rangle$	Unusable: $c_V c_V$, $d_V d_V$ Usable: *none*	0%	---
$\leftrightarrow$ $|H\rangle$	$\leftrightarrow$ $|H\rangle$	Unusable: $c_H c_H$, $d_H d_H$ Usable: *none*		
$\searrow$ $|A\rangle$	$\searrow$ $|A\rangle$	Usable: $c_H c_V$, $d_H d_V$	$2 \times 25\% = 50\%$	0
$\nearrow$ $|D\rangle$	$\nearrow$ $|D\rangle$	Unusable: $c_H c_H$, $d_H d_H$, $c_V c_V$, $d_V d_V$	$2 \times 25\% = 50\%$	1
$\searrow$ $|A\rangle$	$\nearrow$ $|D\rangle$	Usable: $c_H d_V$, $c_V d_H$	$2 \times 25\% = 50\%$	0
$\nearrow$ $|D\rangle$	$\searrow$ $|A\rangle$	Unusable: $c_H c_H$, $d_H d_H$, $c_V c_V$, $d_V d_V$	$2 \times 25\% = 50\%$	1

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 [9]. In addition to detector inefficiencies, dark count rates [10] 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 [11]. Prior research has addressed polarization and timing errors [10], as well as the feasibility of implementing the protocol utilizing weak coherent pulses from independent laser sources [11], 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.

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 [10,12]. 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 [13]. 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 [11,14,15].

We apply the formalism of quantum optics following the development of Loudon [16] 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 $\xi_{a,b}(t)$ and polarization angles $\theta_{a,b}$. The input state at the beam splitter is then the product state

$$
\begin{aligned}
|\xi_a, \theta_a\rangle \otimes |\xi_b, \theta_b\rangle \;=\; & \int dt_1 \xi_a(t_1) \left[\hat{a}_H^\dagger(t_1)\cos\theta_a + \hat{a}_V^\dagger(t_1)\sin\theta_a \right] \\
& \int dt_2 \xi_b(t_2) \left[\hat{b}_H^\dagger(t_2)\cos\theta_b + \hat{b}_V^\dagger(t_2)\sin\theta_b \right] |0\rangle,
\end{aligned}
\tag{1}
$$

where $\hat{a}_{H,V}^\dagger(t)$ and $\hat{b}_{H,V}^\dagger(t)$ 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

$$
\int dt\, \xi_a^*(t)\xi_a(t) = \int dt\, \xi_b^*(t)\xi_b(t) = 1.
\tag{2}
$$

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

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

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

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

and $\hat{c}_{H,V}^\dagger(t)$ and $\hat{d}_{H,V}^\dagger(t)$ 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

$$
\begin{aligned}
|\psi_{\text{out}}\rangle \;=\; & \int dt_1 \xi_a(t_1) \left[(T\hat{c}_H^\dagger(t_1) + R\hat{d}_H^\dagger(t_1))\cos\theta_a + (T\hat{c}_V^\dagger(t_1) + R\hat{d}_V^\dagger(t_1))\sin\theta_a \right] \\
& \int dt_2 \xi_b(t_2) \left[(R\hat{c}_H^\dagger(t_2) + T\hat{d}_H^\dagger(t_2))\cos\theta_b + (R\hat{c}_V^\dagger(t_2) + T\hat{d}_V^\dagger(t_2))\sin\theta_b \right] |0\rangle.
\end{aligned}
\tag{5}
$$

The right hand side of (5) can be written as a summation of terms each contributing amplitudes to one of the 10 mutually exclusive experimental outcomes:

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

where, for example,

$$
|c_V d_V\rangle = \int\int dt_1 dt_2 \xi_a(t_1)\xi_b(t_2)\sin\theta_a \sin\theta_b \left(T^2 \hat{c}_V^\dagger(t_1)\hat{d}_V^\dagger(t_2) + R^2 \hat{d}_V^\dagger(t_1)\hat{c}_V^\dagger(t_2) \right)|0\rangle
\tag{7}
$$

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 dependence of the outcome probabilities on the photon wave functions can be expressed in terms of the overlap integral [16]

$$
|J|^2 = \left| \int dt \xi_a^*(t)\, \xi_b(t) \right|^2.
\tag{9}
$$

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

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

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

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

the overlap integral evaluates to

$$
|J|^2 = \frac{2\Delta\omega_a \Delta\omega_b}{\Delta\omega_a^2 + \Delta\omega_b^2} \exp\left(-\frac{(\omega_a - \omega_b)^2}{2\left(\Delta\omega_a^2 + \Delta\omega_b^2\right)} \right) \exp\left(-\frac{4\Delta\omega_a^2 \Delta\omega_b^2 (t_a - t_b)^2}{2\left(\Delta\omega_a^2 + \Delta\omega_b^2\right)} \right).
\tag{12}
$$

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 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.
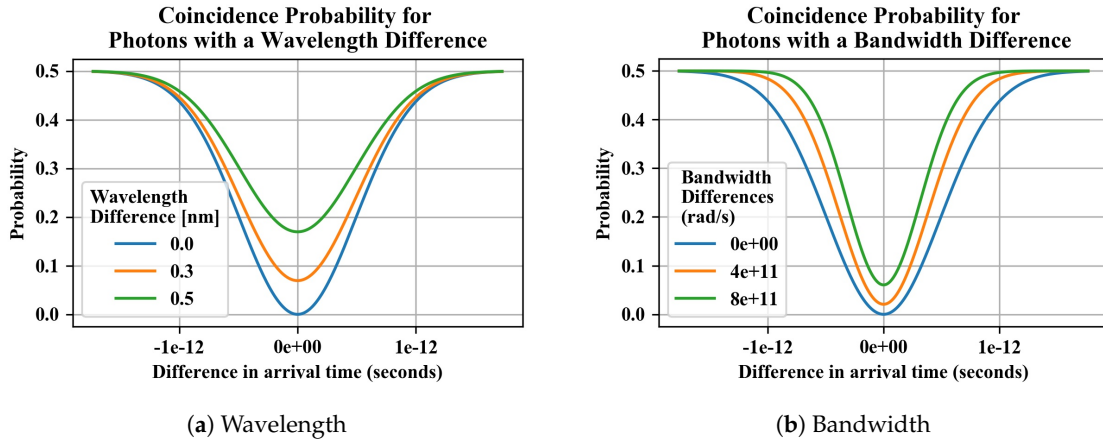
Figure 3. Coincidence probability as a function of beam splitter arrival time difference for photon pairs with varying degrees of distinguishability. The coincidence rate vanishes for perfectly identical photons arriving simultaneously, with the width of the HOM dip determined by the pulse bandwidth. (**a**) displays the coincidence probability curves for two photons with an identical bandwidth $\Delta\omega = 1.18 \times 10^{12}$ rad/s and different wavelengths. (**b**) uses two photons with an identical wavelength $\lambda = 788$ nm and different bandwidths, which center around $\Delta\omega = 1.18 \times 10^{12}$ rad/s. These parameters are chosen consistently with those of the simulations described in Section 4.

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 λ = 788 nm, wavelength tolerance σ_λ = 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 σ_t = 0.26 ps, and polarization angle tolerance σ_θ = 1°) are selected consistently with those described by Kaltenbaek et al. [17], 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 [18]. The results of [17] 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.

(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 $= N_{\text{error}}/N_{\text{sifted}}$ [19].

This procedure is implemented in Python 3 [20] and executed with version 4.4.0-Windows-x86_64 of Anaconda3 [21]. Random measurement outcomes are selected by calls to the numpy.random.choice() routine of the numpy package [22]. The code is fully documented and provided in the online supplement.

Given the source parameters and tolerances, the QBER is a well-defined quantity for an infinitely long sifted key, and can be estimated to the desired precision by averaging the QBERs obtained from repeated simulations of finite key length. Random bit errors will obey Poisson statistics, so we expect the sample standard deviation of their rate to scale as $\sqrt{1/N_{\text{sifted}}}$.

4. Simulation Results and Discussion

Employing the procedure described in Section 3, averages over 1000 simulations using raw keys with lengths $N_{\text{raw}} = 100$ to 1,024,000 bits give QBERs of $(4.04 \pm 20/\sqrt{N_{\text{sifted}}})\%$. The observed sample standard deviation of the QBER follows the expected dependence on the length of the sifted key. These results are consistent with the HOM-interference visibility reported in [17]. 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 $N_{\text{raw}} = 2500$ for a fixed set of 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 our simulation of the MDI-QKD protocol, we obtain Alice's and Bob's sifted keys, from which we can identify specific bit errors and calculate the QBER explicitly. In a fielded QKD system, a sifted key that contains errors is not useful for encrypted communication and neither party alone possesses sufficient information to identify and correct these errors. Further, the finite QBER sets a information-theoretic non-zero upper bound on how much information Eve might have obtained about the sifted key by eavesdropping on the quantum channel. All bit errors in our simulated sifted key are attributable to finite source tolerances rather than an eavesdropper. However, in practice, bit errors due to the actions of Eve on the quantum channel are physically indistinguishable from bit errors arising from finite source tolerances (or other system imperfections), and thus, in a rigorous security analysis, bit errors arising from all sources must be attributed to information gained by Eve [1].

The process of removing bit errors and Eve's information from the sifted keys to obtain a shorter secure shared key is called key distillation. The first step of the process is the estimation of the QBER. This can be achieved by publicly comparing a random sample of bits from the sifted key. As the selected bits are revealed on an open channel, they must be discarded, reducing the length of the sifted key. For given key distillation and QKD protocols, the QBER determines the fraction of the remaining key bits that must be consumed to achieve the desired error free and secure key. If the QBER exceeds a protocol-dependent threshold, this fraction is greater than one and the key distillation fails [23]. Even if the QBER does not exceed the threshold, the length of the distilled key can be a tiny fraction of the

length of the original sifted key, making the absolute rate of secure shared key generation prohibitively low. For these reasons, minimizing all sources of bit errors, including those due to finite photon source tolerances, is critical for MDI-QKD system performance.
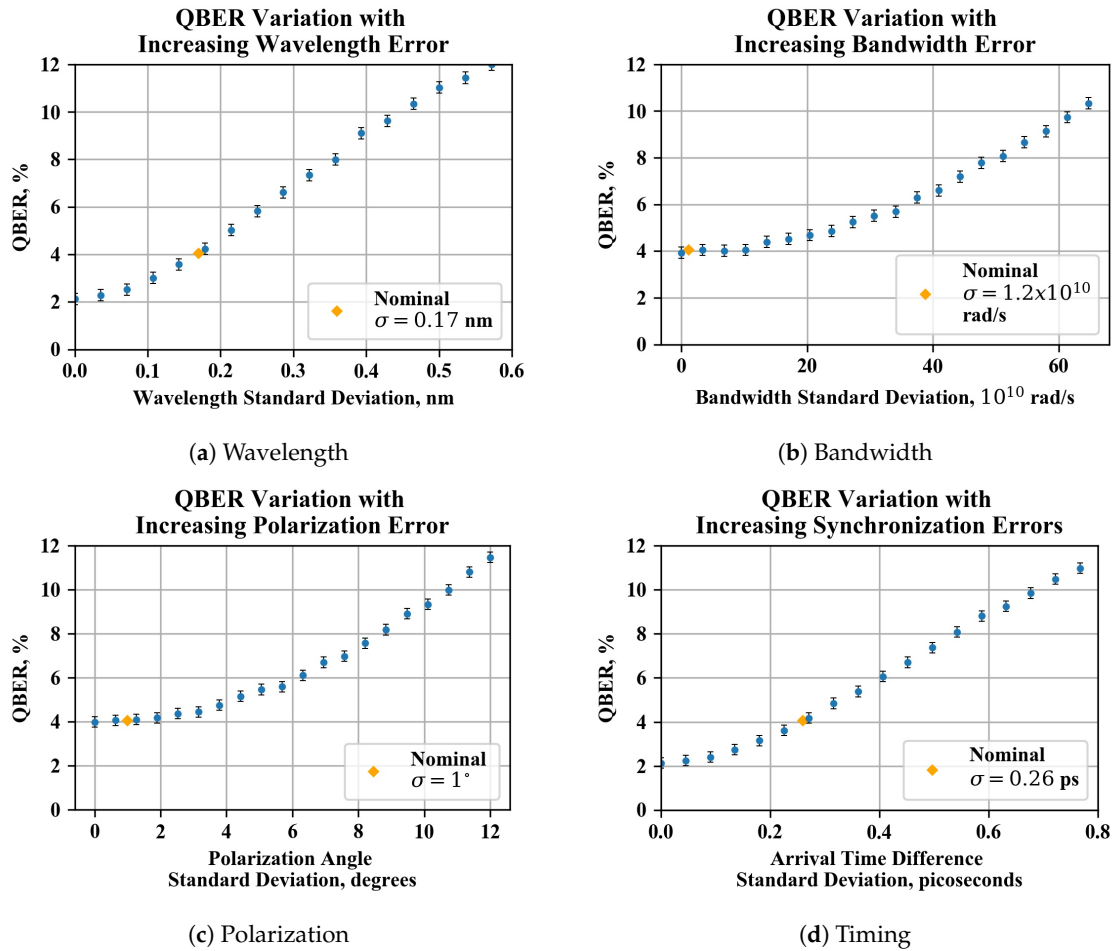

(**a**) Wavelength

(**b**) Bandwidth

(**c**) Polarization

(**d**) Timing

Figure 4. Dependence of the QBER on photon source tolerances for a single variable. The QBER values are averaged over 100 trials of $N_{raw} = 2500$ with uncertainty dominated by shot noise. Error bars represent three times the standard deviation of the mean in either direction.

Assuming the QBER does not exceed the failure threshold, classical error correction and privacy amplification protocols are applied to the remaining sifted key to complete the key distillation. The extensive literature addressing the application of error correction and privacy amplification to QKD protocols is summarized by Nielsen and Chuang . In particular, it is known that effective error correction and privacy amplification protocols exist for the BB84 protocol when the QBER is below 11%, and this threshold is believed to be acceptable for all similar QKD protocols [24,25]. MDI-QKD, as we have formulated it, is not identical to BB84. However, it is similar in that, from the point of view of Alice, MDI-QKD is functionally equivalent to BB84 if she conceptualizes Charlie as an agent of Bob. Accordingly, we expect the threshold QBER for MDI-QKD to be no less than 11%, which is significantly above the QBER we obtained in our simulation of realistic source non-idealities.

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 [17], 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 expense of transmission rate. Similar reasoning applies to photon 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.

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 [26] that fully incorporates the effects of photon propagation, transmission losses, detector limitations and security enhancing variations of the MDI-QKD protocol [27,28]. This work could also be extended to consider other types of pulse shapes or probability 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.

Author Contributions: G.K.S. extended the MDI-QKD model to arbitrary photon temporal wave functions, ran the simulations, and conducted the analysis. B.K.H. and W.M.M. developed and validated the MDI-QKD simulations. L.O.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.E.H. fully incorporated arbitrary source polarizations into the model and provided direct supervision of the project.

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

References

1. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
2. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, 9–12 December 1984; IEEE: New York, NY, USA, 1984; Volume 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, ON, 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. *Theor. Comput. Sci.* **2014**, *560*, 27–32.
6. Makarov, V.; Anisimov, A.; Skaar, J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A* **2006**, *74*, 022313.
7. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Measurement-device-independent quantum cryptography. *IEEE J. Sel. Top. Quantum Electron.* **2015**, *21*, 148–158.
8. Braunstein, S.L.; Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502.
9. Scarini, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350.
10. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503.
11. Lo, H.K.; Curty, M.; Qi, B. Supplemental Information for 'Measurement-device-independent quantum key distribution'. *Phys. Rev. Lett.* **2012**, *108*, 130503.
12. Russell, M.; Mailloux, L.; Hodson, D.; Grimaila, M. A Bell State Analyzer Model for Measurement Device Independent Quantum Key Distribution. In Proceedings of the 2017 International Conference on Scientific Computing, Bath, UK, 11–15 September 2017; American Council on Science and Education, CSREA Press: Las Vegas, NV, USA, 2017; pp. 127–133.
13. Hong, C.K.; Ou, Z.Y.; Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **1987**, *59*, 2044–2046.
14. Mährlein, S.; Oppel, S.; Wiegner, R.; von Zanthier, J. Hong-Ou-Mandel interference without beam splitters. *J. Mod. Opt.* **2017**, *64*, 921–929.
15. Kobayashi, T.; Ikuta, R.; Yasui, S.; Miki, S.; Yamashita, T.; Terai, H.; Yamamoto, T.; Koashi, M.; Imoto, N. Frequency-domain Hong-Ou-Mandel Interference. *Nat. Photonics* **2016**, *10*, 441–444.
16. Loudon, R. *The Quantum Theory of Light*, 3rd ed.; Oxford University Press: Oxford, UK, 2000.
17. Kaltenbaek, R.; Prevedel, R.; Aspelmeyer, M.; Zeilinger, A. High-fidelity entanglement swapping with fully independent sources. *Phys. Rev. A* **2009**, *79*, 40302.
18. Barbarow, W.S. Finding the Optimal Polarizer. 2009. Available online: https://www.meadowlark.com (accessed on 18 February 2018).
19. Elmabrok, O.; Razavi, M. Wireless quantum key distribution in indoor environments. *J. Opt. Soc. Am. B* **2018**, *35*, 197–207.
20. Python Software Foundation. Available online: https://www.python.org/ (accessed on 11 March 2018).
21. Anaconda, Inc. Available online: https://www.anaconda.com/ (accessed on 11 March 2018).

22. NumPy Developers. Available online: https://www.numpy.org/ (accessed on 11 March 2018).

23. Kosloski, J.T. QKD Quantum Channel Authentication. *arXiv* **2006**, arXiv:quant-ph/0603101.

24. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 10th ed.; Cambridge University Press: Cambridge, UK, 2016.

25. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444.

26. 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.

27. 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 Phys. Sin.* **2016**, *65*, 1–9.

28. 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. *Phys. Lett. A* **2016**, *380*, 1408–1413.