Research article

Brendon L. Higgins*, Jean-Philippe Bourgoin and Thomas Jennewein

Numeric estimation of resource requirements for a practical polarization-frame alignment scheme for quantum key distribution (QKD)

https://doi.org/10.1515/aot-2020-0016
Received May 13, 2020; accepted July 7, 2020; published online August 12, 2020

Abstract: Owing to physical orientations and birefringence effects, practical quantum information protocols utilizing optical polarization need to handle misalignment between preparation and measurement reference frames. For any such capable system, an important question is how many resources – for example, measured single photons – are needed to reliably achieve alignment precision sufficient for the desired quantum protocol. Here, we study the performance of a polarization-frame alignment scheme used in prior laboratory and field quantum key distribution (QKD) experiments by performing Monte Carlo numerical simulations. The scheme utilizes, to the extent possible, the same single-photon-level signals and measurements as for the QKD protocol being supported. Even with detector noise and imperfect sources, our analysis shows that only a small fraction of resources from the overall signal – a few hundred photon detections, in total – are required for good performance, restoring the state to better than 99% of its original quality.

Keywords: optical communication; quantum key distribution; reference frames.

1 Introduction

Quantum communication technologies promise to be exciting new avenues for disseminating, processing, and controlling information. The most commercially ready of these technologies, quantum key distribution (QKD), distills a secure encryption key from the measurement results of quantum states sent from one party, Alice, to another, Bob, via a quantum channel [1, 2]. In particular, BB84 [3] and related QKD protocols utilize the no-cloning theorem on qubit states to guarantee that an eavesdropper cannot ascertain any bits of the key without introducing detectable noise into the measurement statistics.

Optical platforms are an obvious choice for communicating quantum information, and one common information carrier is the electromagnetic-field polarization of photonic states. However, optical polarization denotes a direction in space, and for many quantum communications protocols, such as polarization-encoded BB84, the relative alignment of Alice's and Bob's polarization reference frames is crucial to the protocol's serviceability. Furthermore, the phase of each transmitted state must also be preserved, posing a problem beyond spatial frame alignment for birefringent media such as optical fibers (see also Ref. [4]).

Since 2009, our group at the Institute for Quantum Computing, University of Waterloo, has been developing long-distance QKD technology with the goal of achieving Earth-orbiting platforms that service an ecosystem of quantum-secured communications. This work is presently culminating in the QEYSSat quantum satellite mission being spearheaded by the Canadian Space Agency, announced in 2017 [5]. Prior, we and our colleagues conducted a number of proof-of-principle experiments demonstrating polarization-encoded BB84 in closely related contexts, including over high-loss channels [6], and moving platforms both terrestrial [7] and airborne [8].

In support of this work, we developed a practical polarization alignment scheme which uses single-photon-counting tomographic characterization and optimized compensation to correct arbitrary polarization rotations and birefringence of the transmission channel. Here we describe the core quantum-mechanical operation of the scheme in detail and analyze the scheme's performance to

***Corresponding author: Brendon L. Higgins**, Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo N2L 3G1, Ontario, Canada,
E-mail: brendon.higgins@uwaterloo.ca
Jean-Philippe Bourgoin, Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, N2L 3G1, Ontario, Canada; Aegis Quantum, Waterloo, ON, Canada
Thomas Jennewein, Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, N2L 3G1, Ontario, Canada

quantify the single-photon resources required for high-fidelity correction of the transmission channel's effect. Using Monte Carlo simulations, we show that excellent correction can be achieved using only a small fraction of the received photon detections, even in a realistic environment possessing noise and imperfect visibility intrinsic to the source.

2 Polarization alignment

Several frame-alignment schemes for quantum systems have been investigated with the aim of achieving the highest possible fidelity under particular constraints by using multiphoton collectively entangled states and/or measurements – see, e.g., Refs. [9–14]. Implementing these is difficult in practice, and such schemes tend to scale poorly with distance because of losses acting independently on photons within these collective systems. A more practical approach is to augment quantum communications protocols to be reference-frame independent (RFI), such that they utilize polarization subspaces in a way that is insensitive to specific effects – e.g., utilizing the invariance of the circular polarization basis under physical rotations around the beam path (although not birefringence-induced phase effects) for QKD [15–18]. Another approach applies a compensation based on measurements of a correlated side-channel, such as polarimetry of a strong, classical signal multiplexed into the fiber at times or wavelengths near (but distinguishable from) the quantum signal [19, 20].

When creating the polarization alignment scheme described here, our desire was to avoid additional complexities by using the transmitted states and measurements that must already be present for BB84 QKD, to the extent possible. This amounts to single-photon states (or "weak" coherent states with photon numbers $\lesssim 1$, as a good approximation) with polarizations selected from one of four options evenly spaced around the equator of the Poincaré sphere. This approach naturally assures correspondence between the probing states used for characterization and the states being used by the communication protocol, assuming the time variance of the channel's effect is relatively slow.

We first used this alignment scheme in the context of high-loss QKD experiments using a weak coherent pulse (WCP) source emitting at 532 nm wavelength [6]. There it was used so that gradual state deviations caused by temperature fluctuations in the source and optical fibers could be eliminated at the press of a button.

Following experiments used this WCP source to perform QKD from a transmitter on the roof of a building to a receiver in the bed of a moving truck [7]. There, the source was located in a temperature-controlled laboratory, producing states that were guided by ≈85 m of single-mode optical fiber through the core of the building to a motorized pointing platform. By contrast, the receiver side consisted of free-space polarization analysis optics, mounted on a truck that remained essentially level throughout. Thus, Alice's laboratory-to-roof fiber was the biggest contributor to state deviation owing to optical fiber temperature fluctuation and the motion of the pointing platform. For practicality, focus was put on compensating the fiber channel, by characterizing the light arriving at the transmitter telescope via a pick-off and immediate "Bob" measurement – the free-space channel and truck receiver orientation effects were omitted (notably, because only the optical power exiting the transmitter telescope is relevant for QKD security, with this approach any power lost to the pick-off may be compensated by increasing the WCP source power). The polarization alignment scheme itself was automated to operate once per second throughout the experiment.

With upgraded hardware – including larger telescopes, integrated receiver optics, and a faster, higher-quality source at 785 nm wavelength – a similar approach to polarization alignment was used to support a demonstration of QKD transmitted from the ground to an aircraft in flight [8]. Most recently, that source was used in a long-distance demonstration of time-bin encoded QKD [21], where the polarization alignment scheme was used to stabilize polarization states for conversion into time-bin states.

In the following description of the scheme, a key assumption is that there are no significant polarization-sensitive nonunitary effects within the quantum channel. This is generally true of both atmospheric and fiber transmission, and any significant polarization-sensitive nonunitary effect would be inherently detrimental to QKD performance, regardless of frame alignment. For photons that successfully traverse the channel, the most significant effects on polarization – owing to birefringence and physical orientation – can then be characterized as SU(2) rotations of the polarization-encoded qubit state. Any number of these effects can together be described as a quantum channel which applies a single SU(2) unitary $\widehat{U}$ to any state sent through the channel. The alignment scheme is then conceptually separated into two main tasks: (a) characterize the action of the channel such that it has sufficient information about $\widehat{U}$ to then (b) determine, and

subsequently implement, a compensation operation $\hat{V}$ such that the combined action of $\hat{U}$ and $\hat{V}$ closely approximates identity.

2.1 Characterization

The effect of the quantum channel is characterized by transmitting a predefined set of states through the channel and analyzing measurement outcomes. Let $|\psi_{a,n}\rangle$ be one such transmitted state, with $|\psi_{b,n}\rangle = \hat{U}|\psi_{a,n}\rangle$ being the corresponding state measured at the receiver. Given a measurement eigenstate $|\phi_m\rangle$, the fidelity after applying the unknown unitary, $F(\phi_m|\psi_{b,n}) = |\langle \phi_m|\psi_{b,n}\rangle|^2$, quantifies the probability of obtaining that measurement outcome. We note that, in most practical situations, this is limited by an intrinsic signal fidelity, F_S, owing to imperfections of source, channel, and measurement apparatuses leading to real or apparent depolarization. We can encompass these into an effective state $\hat{\rho}_n = (2F_S - 1)|\psi_{b,n}\rangle\langle\psi_{b,n}| + (1 - F_S)\hat{I}$ being measured at the receiver after the unknown unitary of the channel is applied, with $\hat{I}$ being the identity operator.

To completely determine the action of $\hat{U}$, it is sufficient to accurately characterize the direction of one post-$\hat{U}$ state vector and the residual angular rotation about that vector. In practice, we can satisfy this by transmitting ensembles of (at least) two different, nonorthogonal states (say, $|\psi_{a,1}\rangle$ and $|\psi_{a,2}\rangle$), followed by single-qubit state tomography (i.e., single-photon polarimetry) of these states at the receiver.

We focus our attention on the $|H\rangle$, $|V\rangle$, $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, and $|A\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ states prepared as part of the BB84 QKD protocol. If Bob's apparatus is sufficient to perform single-qubit state tomography, Alice may simply continue transmitting the same random sequence of states in $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$, defining $|\psi_{a,n}\rangle$ with $n \in \{1, 2, 3, 4\}$, respectively (alternately, if Alice has an entangled photon source, as for the BBM92 protocol, she may measure her photon to project Bob's photon onto the $|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$ states – again just as she would do for the QKD protocol). Temporal correlation of photon measurement events to the corresponding input states (i.e., particular values of n) can be performed using the same procedures Alice and Bob must already utilize for QKD. This allows photon measurement counts for each n to be collected even though these states are sent in random order.

The four BB84 input states are more than necessary for complete characterization of $\hat{U}$ – for example, the states $|H\rangle$ and $|D\rangle$ alone would be sufficient. The detection counts corresponding to the extra states orthogonal to each of these could be simply discarded, but in practice, the measurement results are easily included in analysis and compensation (see the following), and doing so improves the efficiency of the polarization alignment scheme with an unchanged QKD source.

Tomographic reconstruction of each state $|\psi_{b,n}\rangle = \hat{U}|\psi_{a,n}\rangle$ is then based on time-correlated photon detection statistics. Like the transmitted states, for practicality, it makes most sense to utilize the measurement outcome eigenstates Bob already utilizes to implement BB84 ($|H\rangle$, $|V\rangle$, $|D\rangle$, and $|A\rangle$). Thus, for tomography, we use the tomographically complete set of measurements defined by the three Pauli matrices $\hat{Z}$ (projecting into $|H\rangle/|V\rangle$), $\hat{X}$ (projecting into $|D\rangle/|A\rangle$), and $\hat{Y}$ (projecting into $|R\rangle/|L\rangle$, where $|R\rangle = (|H\rangle + i|V\rangle)/\sqrt{2}$, and $|L\rangle = (|H\rangle - i|V\rangle)/\sqrt{2}$). In fact, this set of measurements is tomographically overcomplete, in the sense that they are more than necessary to extract full state information. Even so, measurements in the circular polarization basis, $|R\rangle/|L\rangle$, are necessary – states lying only on a great circle of the Poincaré sphere, such as BB84 states, are not tomographically complete. This places an additional requirement on Bob's apparatus beyond BB84 QKD. As we see in the following, the compensation mechanism can itself be utilized to achieve a change of basis necessary to implement these projections without further modifications to Bob's receiver.

The overcomplete basis set provides additional experimental robustness when compared with a complete basis set [22] and, because most of these bases are also the BB84 measurement bases, can be practically implemented at the receiver. For each n, we tomographically reconstruct the density matrix $\hat{\rho}_n'$ from measured counts in these bases using maximum likelihood estimation [23]. With these density matrices, an appropriate compensation can then be determined.

2.2 Compensation

We consider a compensation of the unitary $\hat{U}$ taking place at the receiver just before the measurement. Any SU(2) operation can be implemented in polarization optics by a quarter-, half-, quarter-wave plate arrangement, the operation being parametrized by the physical rotation of the three wave plates from their optic axes around the beam path. Determining the optimal

compensation is thus a matter of optimizing the three wave plate orientation angles $\vec{\theta} = (\theta_1, \theta_2, \theta_3)$ such that each in the set of characterized states (each $|\psi_{\mathrm{b},n}\rangle$) matches the corresponding transmitted state ($|\psi_{\mathrm{a},n}\rangle$) with high fidelity.

For our implementation, we utilize the common Nelder-Mead simplex optimization algorithm. First, we construct a theoretical compensation unitary $\hat{V}(\vec{\theta}) = \hat{Q}(\theta_3)\hat{H}(\theta_2)\hat{Q}(\theta_1)$ encompassing the operation of the three wave plates given the parameter $\vec{\theta}$. The cost function of the algorithm, C, is then defined as the negative sum of fidelities between each state predicted after applying the compensation operation and the corresponding initial state – i.e.,

$$C = -\sum_n \langle \psi_{\mathrm{a},n}|\hat{V}\left(\vec{\theta}\right)\hat{\rho}_n{}'\,\hat{V}^{\dagger}\left(\vec{\theta}\right)|\psi_{\mathrm{a},n}\rangle, \tag{1}$$

here, using a more general form of fidelity to accommodate the density matrix $\hat{\rho}_n{}'$, which may not be a pure state.

If the reconstructed states $\hat{\rho}_n{}'$ accurately characterize the measured states $|\psi_{\mathrm{b},n}\rangle$ (i.e., if $\hat{\rho}_n{}' \approx \hat{U}|\psi_{\mathrm{a},n}\rangle\langle\psi_{\mathrm{a},n}|\hat{U}^{\dagger}$), then the cost function C will be minimized when $\hat{V}(\vec{\theta})\hat{U} = \hat{I}$. Minimizing C by varying $\vec{\theta}$ thus optimizes the compensation operation. Applying the optimized theoretical wave plate orientations $\vec{\theta}$ to actual wave plates at the receiver implements the compensation and completes the alignment scheme, as pictured in Figure 1 (although we do not directly reconstruct $\hat{U}$, in principle the inverse of $\hat{V}(\vec{\theta})$ will be a close approximation).

Note that in the aforementioned formalism, we have assumed, for simplicity, that while photon counting for characterization of $\hat{U}$ is taking place, the compensation wave plates are set such that they implement the identity $\hat{I}$ (e.g., by moving back to their optic axes). However, the effect of the wave plates not being at their optic axes during this phase, assuming their positions are known, can be straightforwardly incorporated. In addition, they could also be used for a secondary purpose if Bob's apparatus is only capable of photon counting in the $\hat{Z}$ and $\hat{X}$ bases. There, the compensation wave plates can be utilized to implement a change of basis before the state projection, and thereby achieve projections onto circular polarizations. (This could be done by, e.g., setting the second quarter-wave plate to an angle 45° from its optic axis, effectively transforming $\hat{Z}$ into $\hat{Y}$ for the remaining measurement time. This was done for the study by Bourgoin et al [6].)

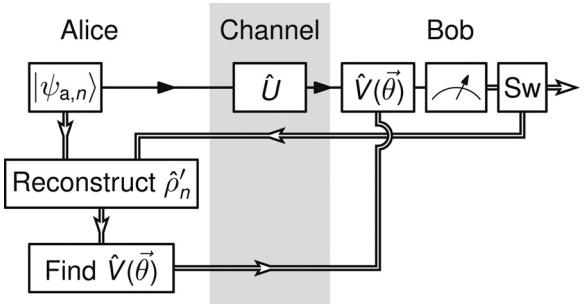

Figure 1: Schematic overview of the polarization alignment scheme as considered here. In this "forward" configuration, Alice prepares states $|\psi_{\mathrm{a},n}\rangle$ and transmits them to a receiver, Bob, with the channel imparting an unknown unitary rotation $\hat{U}$. For characterization, Bob measures the states in a tomographically complete basis set – potentially making use of the controllable unitary $\hat{V}(\vec{\theta})$ to do so – and a logical data path switch (Sw) directs the results to Alice (a switch could alternatively be placed before measurement, allowing unmeasured qubits to pass downstream, as in Refs. [7, 8, 21]). The detection coincidence counts are used to reconstruct the received states $\hat{\rho}_n{}'$ for each n. $\vec{\theta}$ are then optimized in a numerical model of compensation optics, $\hat{V}(\vec{\theta})$, and finally applied to the real apparatus for compensation of subsequent transmissions. A "reversed" configuration can be similarly constructed where $\hat{V}(\vec{\theta})$ is applied before the qubit traverses the quantum channel.

2.3 Reversal using postselection

Typically, the compensation wave plates would be mounted in motorized rotation stages at the receiver, but for some situations, it may be more suitable for these components to be placed at the transmitter. For example, such moving parts on an orbiting satellite platform introduce undesirable complexity and motion noise, making the scheme problematic for a satellite receiver platform [24]. To address this, we exploit the time-symmetric nature of quantum mechanics to construct a "reversed" version of the aforementioned "forward" algorithm. Here, measurements of transmitted states are classified in a manner akin to postselection, allowing us to establish an optimal pre-compensation operation that is applied to the photons immediately before leaving the transmitter.

Compared with the forward version of the scheme, in this reversed version, the sets of input and measured states are swapped – for example, we define $|\psi_{\mathrm{a},n}\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |A\rangle, |R\rangle, |L\rangle\}$, and $|\phi_m\rangle \in \{|H\rangle, |V\rangle, |D\rangle, |A\rangle\}$. As before, measurement count statistics are collected for each combination of input and measured state. Let d_{nm} be the counts for each input state index n and measurement outcome index m. For each m, d_{nm} covers a set of input states that forms a tomographically complete (in fact, overcomplete) basis

set. By selecting the counts d_{nm} for a fixed m and performing tomography using those counts – that is, over all the transmitted states, for each outcome – we reconstruct the effective input state conditional on postselecting $|\phi_m\rangle$. In other words, we thus determine (up to the imprecision of the tomographic reconstruction) what states Alice would have sent Bob in order for them to become $|\phi_m\rangle$ on application of the unknown unitary $\hat{U}$. The compensation is then optimized in the same manner as the forward scheme.

3 Monte Carlo numerical simulations

To determine the performance characteristics of the alignment scheme, we conduct a series of numerical simulations incorporating a Haar-distributed random unitary $\hat{U}$, stochastic count generation, the characterization (tomography) and compensation (optimization) components of the scheme, virtual compensating wave plate operations, and resulting fidelity assessment. Using this, we perform a large number of Monte Carlo simulations of the scheme in both forward and reversed configurations.

For QKD, the primary goal is reducing the quantum bit error ratio (QBER), E, which quantifies the ratio of unexpected measurement outcomes to the total (within each basis relevant for QKD), and is used to determine the security of the channel [2]. A lower QBER allows the bandwidth of key distribution to be increased, while a high QBER can cause the QKD protocol to be aborted with no secure key generated. The QBER is intimately related to the fidelities of the received states – specifically, $E = 1 - \sum_n F_n/4$, where F_n is the measured fidelity of the received state $\hat{\rho}_n$ against the expected $|\phi_n\rangle$. In the context of our compensation algorithm, it is straightforward to show that the QBER E and cost function C are linearly related, with minimal C implying minimal E, so long as $\hat{\rho}_n{}'$ is an accurate estimate of $\hat{\rho}_n$.

We quantify the polarization alignment scheme's performance from our simulation results using the mean predicted QBER, $\bar{E}$, of the nominal (ideal) signal states after the application of the channel unitary $\hat{U}$ followed by the compensation unitary $\hat{V}(\vec{\theta})$. With this definition, this "residual" QBER is zero for perfect compensation, regardless of the actual intrinsic signal fidelity F_S. We independently vary the number of detected photons N and the intrinsic signal fidelity F_S. Our results are calculated from $2^{24} \approx 16.8$ M samples of the Monte Carlo simulation (ensuring thorough convergence) for each of a total 468 configurations. From these results, we obtain very good estimates of the expected mean residual QBERs and their standard deviations.

3.1 Forward scheme

The results for the forward scheme are illustrated in Figure 2a. Given reception of a signal with perfect intrinsic fidelity, the mean residual QBER owing to the application of the polarization alignment scheme is less than 0.5% when at least $N = 400$ photons are measured (an average of 100 photons per input state, the lowest simulated), reducing to less than 0.016% for 12 800 photons (these values are consistent with common understanding that a few

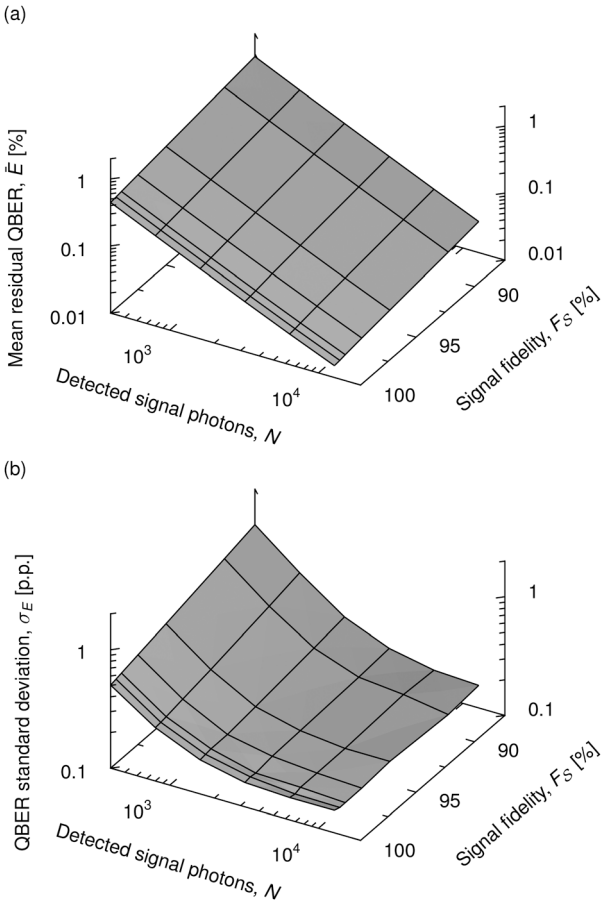

Figure 2: Performance of the forward polarization alignment scheme. (a) Mean residual QBER of nominal signal states after optimized compensation based on characterization analysis of N detected signal photons with intrinsic signal fidelity F_S at the receiver. Only a few hundred photons are required to achieve low mean QBER. (b) Standard deviation of the mean residual QBER. Low photon counts and low intrinsic signal fidelities significantly increase the variation of performance between applications of the scheme. QBER, quantum bit error ratio.

thousand copies are sufficient for producing good qubit state estimates via tomography [25]). In other words, in this condition, as few as four hundred detections are sufficient to recover over 99.5% fidelity when an unknown unitary is acting on the channel.

The expected detection rate for a WCP source is $R[1 - (1 - Y_0)e^{-\eta\mu}]$, where R is the source pulsing rate, μ is the coherent-state mean photon number, η is the transmission of the channel, and Y_0 is the vacuum yield (per pulse) at the receiver. Neglecting the vacuum yield, for typical WCP source parameters $\mu = 0.5$ at $R = 300$ MHz, the expected detection rate over a channel with a significant 40 dB loss will be ≈15 kHz. Of this, 400 detections would be less than 3% of 1 s of data collection. This is less than some QKD implementations reveal publicly for the purpose of parameter estimation – such revealed outcomes could in fact be utilized also for polarization characterization (contrast this to correction techniques based on classical polarimetry, which utilize many orders of magnitude more photons).

In the more realistic condition where the measured signal has imperfect intrinsic fidelity, the mean residual QBER increases – for example, for $F_S = 95\%$, 400 detections leads to 0.59% mean residual QBER, resulting from the inherent statistical uncertainty. A signal with at least $F_S \approx 87.5\%$ is necessary to maintain less than 1% mean residual QBER for 400 photons. Note that this intrinsic signal fidelity corresponds to an intrinsic signal QBER of at least 12.5% – too high to perform successful QKD, but evidently enough for good correction of $\hat{U}$. For comparison, good sources for QKD produce signals with fidelities in the vicinity of 99%. In the context of a satellite receiver, background and detector dark counts are expected to be the largest contributor to the imperfect intrinsic fidelity of the measured signal [24].

We perform a least-squared-error fit of the results of the simulation to a function of the form $\bar{E}(F_S, N) = \alpha(2F_S - 1)^\beta N^\gamma$. The optimized values, $\alpha \approx 2.93$, $\beta \approx -2.23$, and $\gamma \approx -1.07$, yield a coefficient of determination of 0.9999, in excellent agreement with the data. In addition, the value of γ corresponds quite well with the expected $1/N$ precision scaling of the tomographic reconstruction, suggesting that the tomography – necessary for characterizing the unitary – may be the limiting factor in the precision of the polarization alignment scheme.

Figure 2b shows the standard deviation of the residual QBER after compensation, illustrating the variability in the outcomes of each run. Given low numbers of photon detections, a drop in the intrinsic signal fidelity results in significant variations, exceeding one percentage point (p.p.) for $F_S = 87.5\%$ (and worse for lower F_S values not shown). With high intrinsic signal fidelity, however, the scheme behaves consistently, with standard deviations no more than about one-half of a percentage point.

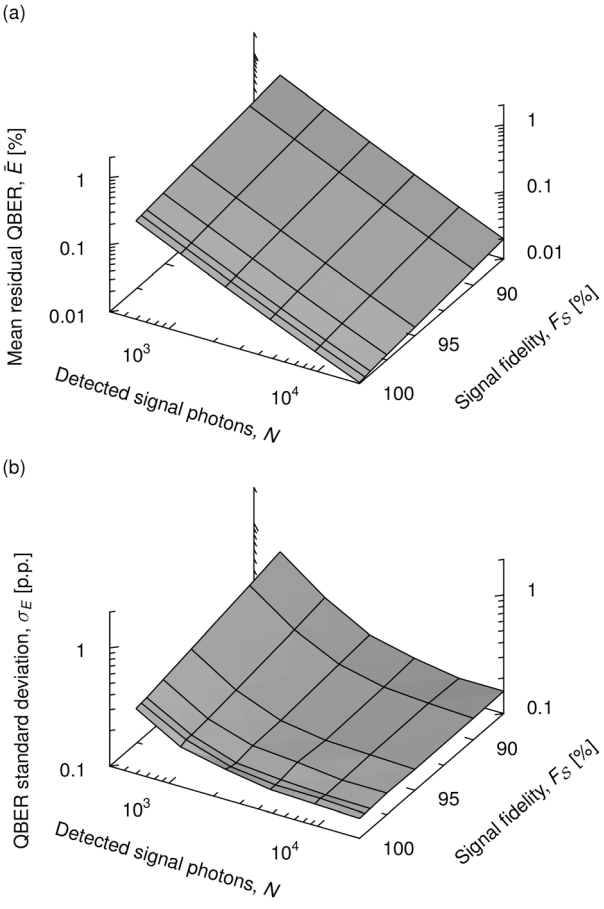

Figure 3: Performance of the reversed polarization alignment scheme. Subfigures a and b are as in Figure 2. QBER, quantum bit error ratio.

3.2 Reversed scheme

The reversed scheme is also simulated, with results plotted in Figure 3. As with the forward scheme, the general trend of better performance (lower mean residual QBER) with better intrinsic signal fidelity and higher numbers of detected photons is maintained. The overall performance, and variability, is very similar to the forward scheme. For example, with $N = 600$ measured photons (again, 100 photons per input state) and an intrinsic signal fidelity F_S of 95%, we find the reversed scheme achieves 0.39% mean residual QBER, comparable with the forward scheme. We again perform a least-squared-error fit to the function $\bar{E}(F_S, N) = \alpha(2F_S - 1)^\beta N^\gamma$, this time resulting in optimized values $\alpha \approx 3.25$, $\beta \approx -2.22$, and $\gamma \approx -1.08$, and yielding a coefficient of determination of 0.9998.

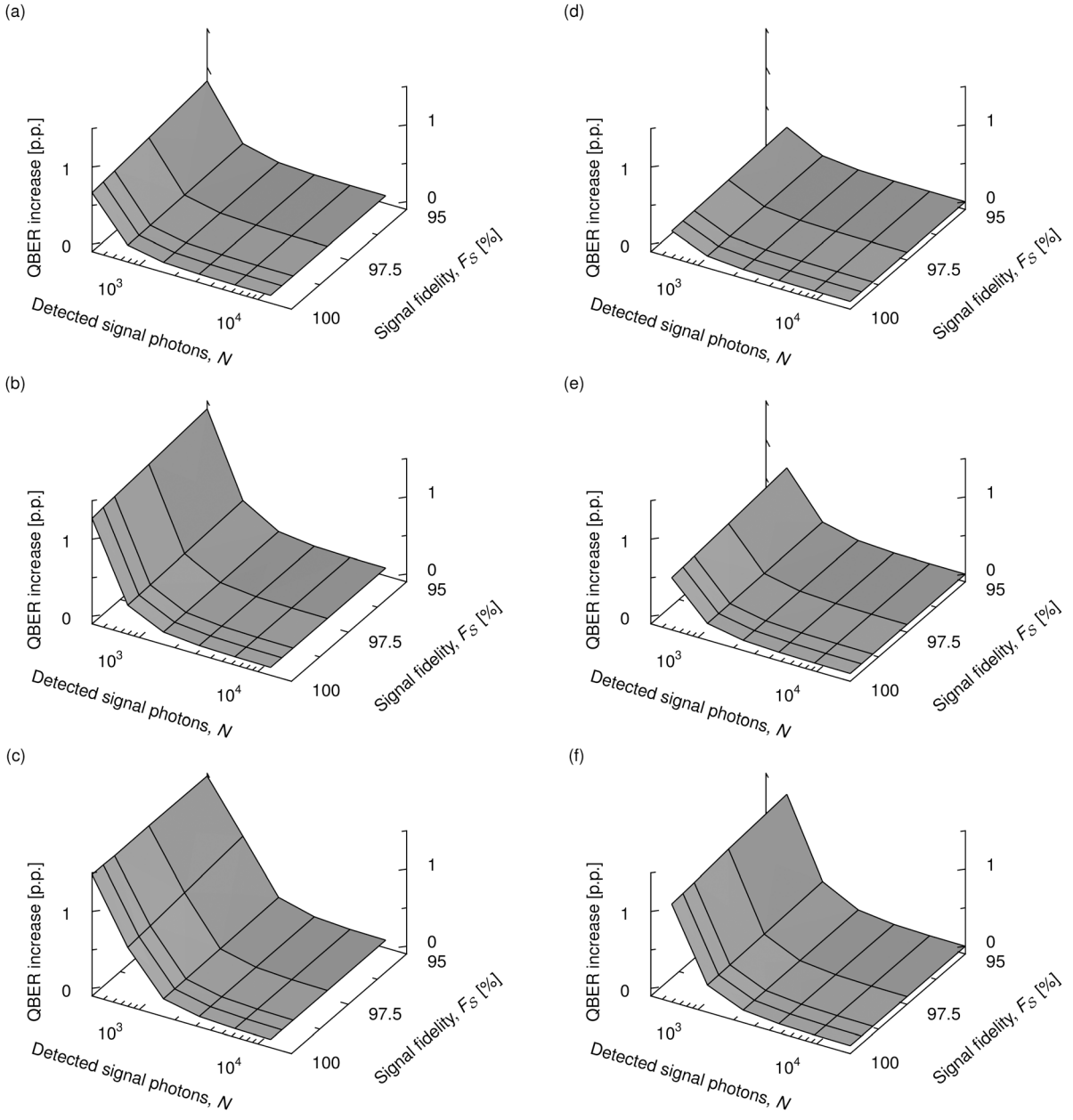

Figure 4: Increase of the mean residual QBER of the scheme when using background subtraction, as compared with not subtracting the background. The left column shows results for the forward case with (a) 100, (b) 200, and (c) 400 mean background counts in each of its six detectors. The right column shows results for the reversed case with (d) 100, (e) 200, and (f) 400 mean background counts in each of its four detectors. Nearly all cases show positive QBER increases, indicating worse outcomes when background is subtracted. QBER, quantum bit error ratio.

3.3 Impairment from background subtraction

To try to improve the scheme under realistic use cases, we perform some additional simulations exploring the effect of simple background noise subtraction. For these simulations, we add random (Poissonian) background counts to the simulated detected counts and then subtract the mean background (while guarding against unphysical negative counts) before the characterization step. The intent is to examine the effectiveness of subtracting from the measurements a known background level, perhaps determined in a calibration stage, to improve the signal-to-noise ratio.

For various photon detection counts N and intrinsic signal fidelities F_S, we compare the residual QBER of the alignment scheme operating with background subtraction,

$\bar{E}_{\mathrm{BGS}}$, against the alternative case where the background counts are added but the mean not subtracted, $\bar{E}_{\mathrm{BG}}$. The results indicate that background subtraction is not better, and in many conditions clearly worse, than allowing the algorithm to operate using counts with background unaltered. This is illustrated by Figure 4, which shows the increase of the residual QBER found when subtracting background (i.e., $\bar{E}_{\mathrm{BGS}} - \bar{E}_{\mathrm{BG}}$) in both forward and reversed cases.

4 Discussion and conclusion

We have detailed a polarization-frame alignment scheme tailored to BB84 QKD experiments, and theoretically characterized the photonic resources required for it to reliably obtain good alignment. The scheme utilizes only the single-photon-level states of the BB84 protocol itself and state generation or state measurement that is tomographically complete, which can be achieved by making intelligent use of the wave plates necessary to compensate the observed polarization rotation. Given less than a few percent of detection outcomes in a realistic QKD scenario, the residual QBER is below source intrinsic QBER, even over high-loss links – for example, in any context where the signal fidelity is high enough to perform QKD, better than 1% residual QBER is possible with only 400 detections.

As a comparison, by maintaining optimal reference frame alignment, active polarization correction allows BB84 protocols to achieve greater secure key rates than RFI QKD in the general case [17]. Note also that RFI QKD assumes one basis remains well aligned, which is not in general true for SU(2) unitary operations, and which the scheme presented here can naturally accommodate. Also interesting is that RFI QKD requires *random* selection out of three bases for each qubit measurement, as this is a part of the security model, whereas a polarization alignment procedure which does not impact the security model (because it applies identical compensation to all states) can safely perform the *same* measurement on multiple qubits in a row, for each basis. This supports flexibility for practical implementations.

It is clear that our polarization alignment scheme is not quantum-mechanically optimal – for ensembles of identical preparations, optimal approaches must use collective treatments [26]. It is, however, sufficiently efficient and relatively simple to implement as to make it practically useful. Interestingly, there is a trade-off between the number of photons repurposed from QKD key generation to perform the polarization alignment scheme, and the QBER achieved. An optimum must exist, as lower QBER increases the number of secure key bits that can be generated per received photon. However, many outcomes already revealed for parameter estimation could serve a dual role for polarization alignment characterization, mitigating the need for additional resources. This can also translate to other QKD schemes, such as measurement-device-independent QKD, where signals which would otherwise be discarded could instead be used for alignment.

More sophisticated techniques could be incorporated into the scheme to make it more theoretically efficient or practically compact. For example, direct estimation of state fidelities [27] might provide a faster mechanism to assess whether full characterization and compensation is necessary. Or, where feasible, more optimal measurement approaches (e.g., Refs. [25, 28]) or more compact polarimetery technologies (e.g., Ref. [29]) could potentially improve the practicality of the characterization apparatus. Other enhancements, such as estimators optimized for small changes (e.g., Ref. [30]) or online optimum-seeking control mechanisms (e.g., Refs. [31, 32]), with closed-loop control incorporating the compensation elements in the measurement, could be applied when deploying for continuous polarization control. In comparison with the continuous scheme described in the study by Ding et al [32], which shows variable and sometimes very long settling times, such operation using the characterization and optimization approach presented here would compensate the channel effect quickly, accurately, and consistently.

Acknowledgments: The authors thank Nikolay Gigov for helpful discussions.
Author contributions: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.
Research funding: This work was supported by the NSERC, Canadian Space Agency, CFI, CIFAR, Industry Canada, FedDev Ontario, and Ontario Research Fund (Canada). B.L.H. acknowledges support from NSERC Banting Postdoctoral Fellowships (Canada).
Competing interests: The authors declare no conflicts of interest regarding this article.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.
[3] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
[4] E. R. Jeffrey, J. B. Altepeter, M. Colci, and P. G. Kwiat, "Optical implementation of quantum orienteering," *Phys. Rev. Lett.*, vol. 96, p. 150503, 2006.
[5] Canadian Space Agency, *Quantum encryption and science satellite (QEYSSat)*. Available at: https://asc-csa.gc.ca/eng/sciences/qeyssat.asp [accessed: Apr. 21, 2020].
[6] J.-P. Bourgoin, N. Gigov, B. L. Higgins, et al., "Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations," *Phys. Rev. A*, vol. 92, p. 052339, 2015.
[7] J.-P. Bourgoin, B. L. Higgins, N. Gigov, et al., "Free-space quantum key distribution to a moving receiver," *Opt. Express*, vol. 23, p. 33437, 2015.
[8] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, et al., "Airborne demonstration of a quantum key distribution receiver payload," *Quantum Sci. Technol.*, vol. 2, p. 024009, 2017.
[9] E. Bagan, M. Baig, A. Brey, R. Muñoz-Tapia, and R. Tarrach, "Optimal strategies for sending information through a quantum channel," *Phys. Rev. Lett.*, vol. 85, pp. 5230–5233, 2000.
[10] A. Peres and P. F. Scudo, "Entangled quantum states as direction indicators," *Phys. Rev. Lett.*, vol. 86, pp. 4160–4162, 2001.
[11] E. Bagan, M. Baig, and R. Muñoz-Tapia, "Communication of spin directions with product states and finite measurements," *Phys. Rev. A*, vol. 64, p. 022305, 2001.
[12] E. Bagan, M. Baig, and R. Muñoz-Tapia, "Aligning reference frames with quantum states," *Phys. Rev. Lett.*, vol. 87, p. 257903, 2001.
[13] E. Bagan, M. Baig, and R. Muñoz-Tapia, "Quantum reverse engineering and reference-frame alignment without nonlocal correlations," *Phys. Rev. A*, vol. 70, p. 030301, 2004.
[14] M. A. Ballester, "Estimation of unitary quantum operations," *Phys. Rev. A*, vol. 69, p. 022303, 2004.
[15] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," *Phys. Rev. A*, vol. 82, p. 012304, 2010.
[16] V. D'Ambrosio, E. Nagali, S. P. Walborn, et al., "Complete experimental toolbox for alignment-free quantum communication," *Nat. Commun.*, vol. 3, p. 961, 2012.
[17] J. Wabnig, D. Bitauld, H. W. Li, A. Laing, J. L. O'Brien, A. O. Niskanen, "Demonstration of free-space reference frame independent quantum key distribution," *New J. Phys.*, vol. 15, p. 073001, 2013.
[18] L. Wen-Ye, W. Hao, Y. Zhen-Qiang, et al., "Tomographic approach in three-orthogonal-basis quantum key distribution," *Commun. Theor. Phys.*, vol. 64, p. 295, 2015.
[19] G. B. Xavier, G. Vilela de Faria, T. Ferreira da Silva, G. P. Temporão, and J. P. von der Weid, "Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic," *Micro. Opt. Tech. Lett.*, vol. 53, pp. 2661–2665, 2011.
[20] M. Sasaki, M. Fujiwara, H. Ishizuka, et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Express*, vol. 19, pp. 10387–10409, 2011.
[21] J. Jin, J.-P. Bourgoin, R. Tannous, et al., "Genuine time-bin-encoded quantum key distribution over a turbulent depolarizing free-space channel," *Opt. Express*, vol. 27, pp. 37214–37223, 2019.
[22] W. K. Wootters and B. D. Fields, "A Wigner-function formulation of finite-state quantum mechanics," *Ann. Phys.*, vol. 191, pp. 363–381, 1989.
[23] Z. Hradil, J. Summhammer, G. Badurek, and H. Rauch, "Reconstruction of the spin state," *Phys. Rev. A*, vol. 62, p. 014101, 2000.
[24] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, et al., "A comprehensive design and performance analysis of low Earth orbit satellite quantum communication," *New J. Phys.*, vol. 15, p. 023006, 2013.
[25] J. Řeháček, B.-G. Englert, and D. Kaszlikoski, "Minimal qubit tomography," *Phys. Rev. A*, vol. 70, p. 052321, 2004.
[26] S. Massar and S. Popescu, "Optimal extraction of information from finite quantum ensembles," *Phys. Rev. Lett.*, vol. 74, pp. 1259–1263, 1995.
[27] S. T. Flammia and Y.-K. Liu, "Direct fidelity estimation from few pauli measurements," *Phys. Rev. Lett.*, vol. 106, p. 230501, 2011.
[28] A. Ling, K. P. Soh, A. Lamas-Linares, and C. Kurtsiefer, "An optimal photon counting polarimeter," *J. Mod. Opt.*, vol. 53, pp. 1523–1528, 2006.
[29] S. G. Roy, O. M. Awartani, P. Sen, B. T. O'Connor, and M. W. Kudenov, "Intrinsic coincident linear polarimetry using stacked organic photovoltaics," *Opt. Express*, vol. 24, pp. 14737–14747, 2016.
[30] P. Kolenderski and R. Demkowicz-Dobrzanski, "Optimal state for keeping reference frames aligned and the platonic solids," *Phys. Rev. A*, vol. 78, p. 052333, 2008.
[31] J. Fisher, A. Kodanev, and M. Nazarathy, "Multi-degree-of-freedom stabilization of large-scale photonic-integrated circuits," *J. Lightwave Technol.*, vol. 33, pp. 2146–2166, 2015.
[32] Y.-Y. Ding, W. Chen, H. Chen, et al., "Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits," *Opt. Lett.*, vol. 42, pp. 1023–1026, 2017.