Entangled quantum key distribution with a biased basis choice

Chris Erven\textsuperscript{1,4}, Xiongfeng Ma\textsuperscript{1}, Raymond Laflamme\textsuperscript{1,2} and Gregor Weihs\textsuperscript{1,3}

\textsuperscript{1} Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, ON, N2L 3G1, Canada
\textsuperscript{2} Perimeter Institute, 31 Caroline Street North, Waterloo, ON, N2L 2Y5, Canada
\textsuperscript{3} Institut für Experimentalphysik, Universität Innsbruck, Technikerstrasse 25, 6020 Innsbruck, Austria
E-mail: cerven@iqc.ca

New Journal of Physics\textsuperscript{1} 11 (2009) 045025 (15pp)
Received 11 December 2008
Published 30 April 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/4/045025

Abstract. We investigate a quantum key distribution (QKD) scheme that utilizes a biased basis choice in order to increase the efficiency of the scheme. The optimal bias between the two measurement bases, a more refined error analysis and finite key size effects are all studied in order to assure the security of the final key generated with the system. We then implement the scheme in a local entangled QKD system that uses polarization entangled photon pairs to securely distribute the key. A 50/50 non-polarizing beamsplitter (BS) with different optical attenuators is used to simulate a variable BS in order to allow us to study the operation of the system for different biases. Over 6 h of continuous operation with a total bias of 0.9837/0.0163 ($Z/X$), we were able to generate 0.4567 secure key bits per raw key bit as compared to 0.2550 secure key bits per raw key bit for the unbiased case. This represents an increase in the efficiency of the key generation rate by 79%.

\textsuperscript{4} Author to whom any correspondence should be addressed.
1. Introduction

Quantum key distribution (QKD) allows two distant parties, Alice and Bob, to create a random secret key even when the quantum channel they share is accessible to an eavesdropper, Eve, so long as they also have an authenticated public classical channel. The security of QKD is built on the fundamental laws of physics in contrast to existing classical public key cryptography whose security is based on unproven computational assumptions.

There are mainly two types of QKD schemes: prepare-and-measure schemes, the best known of which is the original BB84 protocol proposed by Bennett and Brassard [1] in 1984; and entanglement-based schemes, the simplest of which is the BBM92 scheme developed by Bennett et al [2] in 1992. The BBM92 scheme essentially symmetrizes the BB84 protocol by distributing entangled pairs of qubits to Alice and Bob and having them both measure their half of each pair in one of two complementary bases. For a more complete overview of both QKD theory and experiments, please refer to the recent review articles by Gisin et al [3], Dušek et al [4] and Scarani et al [5].

A key feature of the BB84 protocol and many others is that the bases used are chosen randomly, independently and uniformly. Most security proofs, including the seminal work by Shor and Preskill [6], rely heavily on the symmetry, which uniformity of basis choice provides. For example, it allows the sifted data from both bases to be grouped together and a simple error correction algorithm to be performed on the grouped data producing a single error rate. However, uniformly chosen bases have the consequence that on average half of the raw data is rejected leading to an efficiency limited to at most 50%. This is the reason for the curious factor of $\frac{1}{2}$ that appears in the key rates of many security proofs [7, 8].

This symmetry requirement was removed by Lo et al [9] in 2004 when they proposed a simple modification to the BB84 scheme that could in principle allow one to asymptotically approach an efficiency of 100%. Their scheme relies on two changes to the BB84 protocol: non-uniformity in the choice of bases and a refined data analysis. The first change of non-uniformity allowed Alice and Bob to achieve much higher efficiencies with their raw data. In fact, Lo et al showed that this efficiency could be made arbitrarily close to 100% in the long key limit. The second change of a refined data analysis allowed Alice and Bob to maintain the security of their system since a simple error analysis was no longer sufficient. Acín et al [10] have also studied this protocol in 2006 using a CHSH test for security under the conditions of no-signalling eavesdroppers.

In this article, we detail the experimental implementation of the biased basis choice protocol with a simulated variable non-polarizing beamsplitter (BS) and a local entangled QKD
system. We begin by first reviewing the theory for the biased protocol. We study the optimal bias ratio and the important parameters necessary to maintain security. We then follow with a description of the experimental set-up for the implementation of the biased scheme. Lastly, we report on the results of the experiment and compare the efficiency of the biased protocol with those of an unbiased protocol.

2. Theory

Lo et al [9] proposed their protocol as a modification to the original BB84 protocol, which is a prepare-and-measure scheme. Here, we make the simple extension to the entanglement-based BBM92 scheme developed by Bennett et al [2] in 1992. In the original scheme, a source of polarization entangled photon pairs in the singlet Bell state is placed in between Alice and Bob, and one photon from each pair is sent to Alice and Bob. Alice and Bob then randomly, independently and uniformly choose to measure in either the rectilinear ($H/V$) basis or the diagonal ($+45°/−45°$) basis. Now we extend this scheme to remove the uniformity in the basis choices just as Lo et al did for the BB84 protocol. We are allowed to do so without violating the security of the scheme because the proof by Lo et al already relies on expanding the BB84 scheme into an imagined entanglement-based scheme. Thus, their proof of security holds for performing the actual biased entanglement-based scheme as well as performing the biased BB84 scheme. Additionally, we use the recently developed squashing model [11]–[13] which allows us to assume that we are dealing with qubits so that the proof by Lo et al holds (double clicks are assumed to be rare and ignored).

The biased basis scheme has two main changes: first, Alice and Bob now choose their measurement bases randomly and independently but now non-uniformly with substantially different probabilities. This allows for a much higher probability of Alice and Bob using the same basis and thus allows them to achieve much higher efficiencies with their raw data. With uniformity removed, the second change necessary is a refined error analysis since an eavesdropper could now easily break a system that performed a simple error analysis on the lumped data by eavesdropping primarily along the predominant basis. To ensure security, it is crucial for Alice and Bob to divide their data into two subsets according to the bases used and compute an error rate for each subset separately. It is only with this second addition that one can ensure the security of this biased scheme.

First, we define the necessary quantities that we will use in our security analysis. Define $e_{bx}$ ($\delta_{px}$) and $e_{bz}$ ($\delta_{pz}$) to be the bit (phase) error rates in the $X$ (diagonal) and $Z$ (rectilinear) bases, respectively, where an $e$ is used to denote a measurable quantity and a $\delta$ is used to denote a quantity that has to be inferred. Note that the bit error rates, $e_{bx}$ and $e_{bz}$, are known exactly by Alice and Bob once they perform error correction since they can count the number of errors found during error correction. However, the phase error rates, $\delta_{px}$ and $\delta_{pz}$, need to be estimated from the bit error rates since they are not directly accessible from Alice and Bob’s measurement data.

In order to estimate the phase error rates, we define the quantities $p_{bx}$ ($p_{px}$) and $p_{bz}$ ($p_{pz}$) to be the bit (phase) error probabilities in the $X$ and $Z$ bases, respectively. Since a basis independent source is assumed, we know that

$$p_{pz} = p_{bx}, \quad p_{px} = p_{bz}. \quad (1)$$
Now in the long key limit $e_{bx}$ converges to $p_{bx}$, whereas $\delta_{pz}$ converges to $p_{pz}$. Using equation (1) now allows us to say that

\[
\delta_{px} = e_{hz}, \quad \delta_{pz} = e_{bx}
\]

in the long key limit. Obviously for finite key lengths this equality will not hold exactly and we will have to consider statistical fluctuations. We will address the finite key size effects in a moment, but for now assume that equation (2) holds.

The key point of the security analysis rests in the privacy amplification part [14]. Privacy amplification is usually performed via the two-universal hash functions discovered by Wegman and Carter [15] and that is what is done in the experimental implementation detailed in this paper. Alice and Bob need to take care of the bits exposed during error correction, which they can directly count during the error correction process since an eavesdropper can learn this information listening in to the classical channel. They also need to estimate the phase error rates for the two bases in order to estimate the amount of an eavesdropper’s information on the quantum signals that were distributed. Privacy amplification then needs to be applied to reduce the information of the eavesdropper from these two sources to an arbitrarily small amount. This leads to the following key generation rate according to [8], expressed in terms of secure bits per raw bit, using equation (2) above

\[
R \geq (1 - q)^2 [1 - f(e_{bx})h_2(e_{bx}) - h_2(\delta_{px})] + q^2 [1 - f(e_{bx})h_2(e_{bx}) - h_2(\delta_{pz})] \geq (1 - q)^2 [1 - f(e_{bx})h_2(e_{bx}) - h_2(e_{bx})] + q^2 [1 - f(e_{bx})h_2(e_{bx}) - h_2(e_{bx})],
\]

where $q$ is defined to be Alice’s or Bob’s bias probability of measuring in the $Z$ basis and $(1 - q)$ is their probability of measuring in the $X$ basis, $f(x)$ is the error correction inefficiency as a function of the error rate, normally $f(x) \geq 1$ with $f(x) = 1$ at the Shannon limit and $h_2(x) = -x \log_2 x - (1 - x)\log_2(1 - x)$ is the binary entropy function. For this initial analysis, the key rate formula assumes that Alice and Bob each pick the same identical bias.

We benefit from separating the key rate into contributions from the $X$ and $Z$ bases since the key rate can still be positive for an error rate higher than 11% in one basis so long as the other error rate is low enough. This can be seen in figure 2 of [16] since we use local operations and one way classical communication (1-LOCC) in our post-processing. Note that the cascade error correction algorithm, which we use, is considered 1-LOCC post-processing since the two-way classical communication is not used to perform advantage distillation. Also note that in this treatment of cascade we assume that Eve learns both the positions of the errors and the revealed parity bits.

The last thing to take care of is the finite key size effects since these will be very important in determining how to balance the optimal biasing ratio. For this analysis, we assume the main finite key size effect is due to the parameter estimation; namely, the statistical fluctuations in the phase error rates compared with what is estimated from the bit error rates. The other possible finite key size effects are authentication, the leakage of information during error correction (typically referred to as $\text{leak}_{\text{EC}}$), the probability of failure for error correction and error verification (typically referred to as $\varepsilon_{\text{EC}}$) and the probability of failure of privacy amplification (typically referred to as $\varepsilon_{\text{PA}}$) [17, 18].

For our experiment, the probability of failure for our parameter estimation is of the order of $10^{-6}$ since, as will be discussed below, we choose a safety margin on our phase error estimates so that the probability that the actual phase error rates are outside of this range is less than $10^{-6}$. Also, we do not implement authentication on the classical channel, so we ignore its effect on

\[\text{New Journal of Physics 11 (2009) 045025 (http://www.njp.org/)}\]
our key rate. Note though that the resources required for authentication scale logarithmically in the length of the secret key generated by a QKD session [19]. The information being leaked during error correction does not contribute any finite key size effects since we directly count the number of bits revealed and take care of them in the privacy amplification step [20]. Thus, there are no fluctuations in this contribution since we know it exactly. The error correction and verification algorithm we implement is due to Sugimoto and Yamazaki [21] and allows us to bound the failure probability and thus set its value. For this experiment, we implement the error correction algorithm so that its probability of failure is \( < 10^{-10} \). Lastly, the probability of failure for the privacy amplification step is assumed to be negligible since it depends on the privacy amplification algorithm used and we assume that it is possible to make one with a sufficiently small failure probability. For a strict finite key analysis, one should follow [17, 18, 22, 23].

We need to consider the statistical fluctuations in order to discuss the optimal bias between the two bases. As was stated above, both error rates \( e_{bx} \) and \( \delta_{pz} \) converge to \( p_{bx} = p_{pz} \) in the long key limit. We use standard random sampling theory to determine the following formula given in [8] for the estimates of our phase error rates

\[
P_{\epsilon_x} \equiv \text{Prob}\{\delta_{pz} > e_{bx} + \epsilon_z\} 
\leq \exp\left[-\frac{\epsilon_z^2 n_{xx}}{4e_{bx}(1-e_{bx})}\right],
\]

where \( n_{xx} \) is the number of bits generated from Alice and Bob both measuring in the \( X \) basis and \( \epsilon_z \) is a small deviation from the measured bit error rate. Equation (4) allows us to put a bound on the probability that the phase error rate deviates from our measured bit error rate by more than \( \epsilon_z \). For example, if Alice and Bob measure 10000 qubits in the \( X \) basis \( (n_{xx} = 10000) \), find an error rate of 5\% \( (e_{bx} = 0.05) \) and set their desired deviation to 1\% \( (\epsilon_z = 0.01) \), then equation (4) would allow them to say that the probability that their phase error rate \( (\delta_{pz}) \) deviates by more than \( \epsilon_z \) is less than 0.52\%. In other words, if we use \( \delta_{pz} = 0.06 \) in our key rate formula then we are confident that our key was generated securely with a probability of 99.48\%. So our key rate formula has now become

\[
R \geq (1 - q)^2[1 - f(e_{bx}) h_2(e_{bx}) - h_2(e_{bx} + \epsilon_z)] + q^2[1 - f(e_{bx}) h_2(e_{bx}) - h_2(e_{bx} + \epsilon_z)],
\]

which is the same as before except for the addition of \( \epsilon_x \) and \( \epsilon_z \), which are now necessary to deal with the finite key statistics. We should note that the random sampling formula used in equation (4) is a good approximation in the long key limit.

Now we can try to find the optimal bias between the two bases. Given estimates for \( e_{bx} \), \( e_{bz} \) and \( N \) (the total coincidence count), and picking \( P_x = P_{\epsilon_x} + P_{\epsilon_z} \), one can optimize the bias \( q \) and the deviations \( \epsilon_x \) and \( \epsilon_z \) according to equations (5) and (4). For example, with estimates of the parameters we expect to see in our system, we can graph the key rate (normalized in terms of secure key bits per raw key bit) versus the bias ratio \( q \), shown in figure 1. The inset shows the estimates for the parameters needed in order to find the optimum bias: \( N \) is the total number of entangled pairs sent to Alice and Bob over the course of the experiment, \( P_x \) is the confidence probability desired for our phase error statistics, \( e_{bx} \) and \( e_{bz} \) are the observed bit error rates in the \( X \) and \( Z \) bases over the course of the experiment and \( f \) is the observed error correction efficiency. From figure 1 we can see that the key rate is maximized for a bias of \( q = 0.97 \). Once we have found the optimum bias, we can then use it, along with equation (4), to figure out the optimum deviations \( \epsilon_x \) and \( \epsilon_z \) that will still allow us to achieve our desired confidence probability \( P_x \).

New Journal of Physics 11 (2009) 045025 (http://www.njp.org/)
Figure 1. Plot of the key generation rate ($R$) in terms of the bias ratio ($q$).

Examining figure 1, we see that a maximum also occurs around $q = 0.03$ though it is slightly lower than the one at $q = 0.97$. It is obvious that the efficiency curve should be symmetric about the middle point $q = 0.5$ since biasing the protocol towards the $X$ basis should be just as good as biasing it towards the $Z$ basis. However, the curve is not entirely symmetric because the error rates and error correction efficiencies are not identical in the two bases. The error correction efficiency plays the largest part in the overall rate since it costs a fraction of $f(e)h(e)$ in the final key generation rate. Thus, since the error correction efficiency is lower in the $X$ basis than the $Z$ basis ($f_X > f_Z$), the optimum rate is also lower when the bias is skewed towards the $X$ basis.

It is important to understand how the biased protocol utilizes the optimum bias in order to make the most efficient use of the raw key data. The optimum bias, $q$, along with the optimum deviations, $\epsilon_x$ and $\epsilon_z$, are chosen such that only the minimum number of measurements are made in the weak basis in order to achieve the desired confidence probability $P_\epsilon$. This has the consequence that privacy amplification of the measurement results from the strong basis has to be deferred until the end of the entangled photon distribution phase. It is only with the last distributed photon that Alice and Bob gain enough statistics in the weak basis to allow them to privacy amplify all the error corrected keys generated in the strong basis over the course of the experiment. They will obtain small amounts of privacy amplified key from the weak basis over the course of the experiment, but the majority of the key that comes from the strong basis will not be available until after the distribution phase is completed.
3. Experimental implementation

The purpose of this experiment was the experimental investigation of the biased basis QKD protocol and all of the practicalities associated with implementing the protocol; such as, choosing the proper bias, doing a more refined error analysis and worrying about the finite key size effects. In order to focus on these issues, we did not involve the complications of a free-space link and instead chose for Alice and Bob to locally detect each of their halves of the photon pairs while sitting next to the source connected to it with a short optical fibre. Additionally, since we wanted to investigate many different biases, we decided to simulate a variable non-polarizing BS since they do not exist to the best of the author’s knowledge. Indeed, even fixed biased non-polarizing BSs are extremely expensive and difficult to manufacture; therefore, it is worthwhile to study the performance of the system for many different biases with a simulated variable biased BS first. The difficulties associated with biased BSs might suggest one possible reason for employing an active basis selection scheme over a passive one since biasing might be done more easily. However, the active schemes would have their own complications for generating truly random, biased bit strings at a high enough rate for their polarization modulators. We are also currently investigating development of a variable non-polarizing BS to allow the flexible adjustment of the bias in our system without throwing away counts.

The experimental set-up consists of a compact spontaneous parametric down-conversion (SPDC) source, two compact passive polarization analysis modules, avalanche photodiode (APD) detectors, time-stampers, GPS time receivers, two laptop computers and custom written software. The SPDC source is comprised of a 1 mm thick $\beta$-BBO crystal pumped with a 50 mW laser that produces entangled photon pairs at a degenerate wavelength of 815 nm. A $\beta$-BBO crystal 0.5 mm thick in each arm compensates for walk-off effects, which can ruin the entanglement. Typically, a total single photon count rate of 100 000 s$^{-1}$ in each arm of the source and a coincident detection rate of 11 000 s$^{-1}$ is measured locally. More details on the setup can be found in our earlier papers [24]–[26].

In order to implement the biased protocol, we simulated a biased BS by placing the appropriate attenuators in the transmission arm of the original 50/50 BS used to perform the basis choice as shown in figure 2. The transmitted arm analyzes the photons in the diagonal basis. Also, in order to directly compare the efficiencies of experiments with different biases, we used the appropriate attenuators ahead of the BS to make the rates of each experiment with

Figure 2. Schematic of the polarization analysis module with a neutral density (ND) filter placed in the transmission arm of the 50/50 BS in order to achieve the desired bias in the measurement results (polarizing beamsplitters (PBS)).
a different bias equal. The attenuators are placed in the transmission arm ($X$, diagonal basis) so that the $Z$ (rectilinear) basis is the one which Alice and Bob predominantly measure in. As was mentioned earlier, we make this choice because error correction costs a factor of $f(e)h(e)$ (with $f(e) > 1$), whereas privacy amplification costs a factor of $h(e)$ in our key generation rate. Thus, since the $Z$ (rectilinear) basis has a much lower intrinsic error rate, we would like to make it the predominant basis since less error correction will be needed than if we chose the $X$ (diagonal) basis to be the predominant one.

Our custom written software needed to be modified in order to analyze the error rates in both bases separately and defer the privacy amplification until the end of the entangled pair distribution phase. Error correction is first performed on the $X$ basis measurements followed by the $Z$ basis measurements, revealing the bit error rates $e_{bx}$ and $e_{bz}$. The number of bits revealed during the error correction of the $X$ and $Z$ measurements are recorded. After the distribution phase, we use the actual experimental results for $N$, $n_{xx}$, $n_{zz}$, $q$, $e_{bx}$, $e_{bz}$, $f(e_{bx})$ and $f(e_{bz})$, along with the desired $P_{\epsilon_x}$ and $P_{\epsilon_z}$ to calculate the optimum $\epsilon_x$ and $\epsilon_z$ according to equation (4). This allows us to distill the maximum amount of key from our raw data. The appropriate privacy amplification factor, according to equation (5), is now calculated for each measurement set. Privacy amplification using a two-universal hash function [14, 15, 27] then takes care of the bits revealed during error correction, the estimated phase error rates, and the additional safety margin needed for the finite key statistics to produce the final secure key.

For this experiment, we improved our error correction algorithm since knowing the bit error rates $e_{bx}$ and $e_{bz}$ as precisely as possible is extremely important. To do this we improved the cascade error correction algorithm [28, 29], which was initially used in a modified form in our system, to the optimized algorithm outlined by Sugimoto and Yamazaki [21]. In previous experiments with our original modified cascade algorithm we achieved a residual bit error rate of $1.92 \times 10^{-3}$ [26], which is clearly insufficient for realistic key sizes especially once finite key size effects have to be taken into account. In order to be secure, it has been shown that privacy amplification needs to work with key lengths of the order of $\sim 10^7$ bits [18]. Consequently, the probability of residual errors needs to be at least two orders of magnitude less than this in order for the privacy amplification to succeed with high probability. With the improved optimized cascade algorithm, we are now able to set a parameter, $s$, which then determines the residual bit error rate according to $P_{\text{residual}} < 2^{-s}$. For this experiment, we chose $s = 40$ which should give us a maximum residual bit error rate of $9.09 \times 10^{-13}$.

4. Results

On the day of the experiment, visibilities of 99.6 and 92.4% are directly measured in the rectilinear and diagonal bases, respectively. This corresponds to baseline error rates in the two bases of $e_{bx} = 0.038$ and $e_{bz} = 0.002$ due to the source. The limited visibility in the diagonal basis (high $e_{bx}$) is likely due to the broad spectral filtering (10 nm) in the polarization detector box that allows some unentangled photon pairs through the filters that still have a strong correlation in the rectilinear basis, but have almost no correlation in the diagonal basis. The limited visibility is also likely due to uncompensated transverse walk-off in the $\beta$-BBO crystal, which is aggravated by the narrow pump beam spot.

We performed four different experiments with the varying biases shown in table 1, each approximately 6 h in duration in order to compare their efficiencies. While the appropriate attenuators were put into the transmission arms of both Alice’s and Bob’s detectors to simulate
Table 1. The observed biases in each of the experiments.

| Exp no. | Alice    | Bob      | Total    |
|---------|----------|----------|----------|
| 1       | 0.4570/0.5430 | 0.4752/0.5248 | 0.4343/0.5657 |
| 2       | 0.5660/0.4340 | 0.6074/0.3926 | 0.6639/0.3361 |
| 3       | 0.7398/0.2602 | 0.7606/0.2394 | 0.8938/0.1062 |
| 4       | 0.8804/0.1196 | 0.9062/0.0938 | 0.9837/0.0163 |

Figure 3. Plot of the key generation rate (R) in terms of Alice’s bias ratio ($q_A$) and Bob’s bias ratio ($q_B$). Alice’s bias is plotted along the left axis, whereas Bob’s is plotted along the right.

The desired bias, differences in coupling efficiencies within the polarization analysis modules produced slightly asymmetric biases between Alice and Bob for the $Z$ basis choice. In order to figure out the optimum $\epsilon$’s needed and the proper privacy amplification factor, the simple uniform bias analysis above had to be expanded into a more complex analysis that allowed Alice and Bob to have non-identical biases. Figure 3 is the generalization of figure 1 and plots the key rate (R) versus Alice’s bias (shown along the left axis) versus Bob’s bias (shown along the right axis). Using this analysis we proceeded to find the optimum $\epsilon$’s, calculate the privacy amplification factors and complete the key generation process.
Figure 4. Plot of the QBERs in the X (blue) and Z (green) bases over the course of the experiments.

Table 2. The QBERs and key rates for each of the experiments.

| Exp no. | QBER  | Key length | Secure bits per raw bit | Inefficiency |
|---------|-------|------------|-------------------------|--------------|
|         | X (%) | Z (%)      | Raw         | Sifted       | Final        |                          |
| 1       | 1.39  | 5.55       | 28 655 075  | 14 779 423  | 7 365 984  | 0.2550  | –                       |
| 2       | 0.90  | 5.76       | 29 705 827  | 15 713 427  | 8 392 528  | 0.2825  | 1.11                     |
| 3       | 0.89  | 5.36       | 29 319 830  | 18 627 251  | 10 568 944 | 0.3605  | 1.41                     |
| 4       | 0.82  | 5.80       | 32 162 313  | 26 154 132  | 14 687 016 | 0.4567  | 1.79                     |

Figure 4 shows the QBERs in the X and Z bases measured over the course of each experiment. The average QBERs in the X and Z bases for each experiment are tabulated in table 2. The increase in the QBER’s from the baseline 3.8 and 0.2% to those observed is attributed to the typical leakage of the polarizing BSs in the polarization analysis modules, the uncompensated birefringence in the single-mode fiber used to transport the photons between the source and the polarization analysis modules and to accidental coincidences.

New Journal of Physics 11 (2009) 045025 (http://www.njp.org/)
Figure 5. Plot of the raw, sifted and average final key rates over the course of each experiment. The rates are grouped by colour with experiment 1 in blue, experiment 2 in green, experiment 3 in red, and experiment 4 in magenta. The upper box holds the raw key rates, the middle box holds the sifted key rates, and the lower box holds the average final key rates.

Figure 5 shows the raw key rate, sifted key rate and average final key rate over the course of each experiment. The statistics for each experiment are grouped by the same color, the upper box holds the raw key rates, the middle box holds the sifted key rates and the lower box holds the average final key rates for each experiment. Note that we can only show an average final key rate since privacy amplification has to be deferred until the end of the entangled photon distribution phase and error correction phase, and then is performed on the ‘entire’ sifted key at once. The results of each experiment are summarized in table 2 along with their efficiencies compared with the first experiment which we take as the ‘unbiased’ experiment. As is clearly shown in table 2, the efficiency of each experiment increases with the bias reaching a value of 0.4567.

Note that we have one remaining shortcoming in our privacy amplification routines, namely that we work on blocks of 1024 bits. The finite key investigations have shown that privacy amplification has to work on blocks of the order of \( \sim 10^7 \) bits. This ability requires specialized hardware or low level coding which we do not yet have in our experiment.
secure key bits per raw bit for the final experiment, which had a bias of 0.9837/0.0163. Thus, by implementing the biased QKD protocol we were able to increase the secure key generation rate by 79% over the unbiased case. Clearly, the use of a biased protocol for the generation of secure key bits results in a more efficient use of the distributed entangled photon pairs and allows Alice and Bob to distill more secret key from the same number of distributed pairs than what an unbiased protocol would allow. Additionally, as the number of entangled photon pairs is increased, the number of secure final key bits per raw key bit will approach 1.0 as was pointed out earlier.

Since the error correction algorithms were greatly improved during this experiment, we include actual data for their operation during experiment 1. We use the error correction algorithm developed by Sugimoto and Yamazaki [21] as an optimization of the cascade error correction algorithm developed by Brassard et al [29] which was first mentioned in an earlier form in [28]. Table 3 shows the average block sizes used during the error correction of the sifted X and Z keys. Table 4 shows the number of errors corrected during each pass and sequence of cascade. A pass is defined as a new random shuffling of the bits to form blocks of the sizes above which are then error corrected with BINARY [29]. When an error is found, cascade then goes back through all previous sequences of shufflings of bits to correct errors that were missed beforehand. Table 5 shows the average number of errors corrected during the use of the BINARY and BICONF [29] primitives and the corresponding number of bits revealed. Additionally, it shows the average key block lengths and QBERs found during cascade. Knowing these allows the calculation of the error correction efficiencies for our algorithm by first calculating the number of bits which an error correction algorithm operating at the Shannon limit would have revealed via $h_2(\text{QBER}) \times \text{AvgKeyLength}$. These efficiencies are also shown in table 5 relative to an error correction algorithm operating at the Shannon limit.

As was discussed above, the new algorithm allows us to set the desired residual error rate via the parameter $s$ which determines the rate according to $P_{\text{residual}} < 2^{-s}$. However, as

### Table 3. Cascade stats—average block sizes.

| Pass  | Pass 2 | Pass 3 |
|-------|--------|--------|
| X     | 16     | 33     | 65     |
| Z     | 72     | 144    | 289    |

### Table 4. Cascade stats—average number of errors corrected at each step in cascade.

| Totals | Sequence 1 | Sequence 2 | Sequence 3 |
|--------|------------|------------|------------|
| X      |            |            |            |
| Pass 1 | 31.4       | 31.4       | –          | –          |
| Pass 2 | 27.2       | 13.6       | 13.6       | –          |
| Pass 3 | 7.1        | 2.7        | 1.1        | 3.3        |
| Z      |            |            |            |
| Pass 1 | 5.6        | 5.6        | –          | –          |
| Pass 2 | 4.4        | 2.2        | 2.2        | –          |
| Pass 3 | 1.2        | 0.5        | 0.2        | 0.5        |
Table 5. Cascade stats—average number of errors corrected, bits revealed, error correction efficiencies, key block lengths and QBERs.

|                          | BINARY | BICONF | Total |
|--------------------------|--------|--------|-------|
| Average number of errors corrected ($X$) | 65.8   | 1.2    | 67.0  |
| Average number of bits revealed ($X$)    | 437.5  | 53.3   | 490.8 |
| Average number of errors corrected ($Z$) | 11.2   | 1.7    | 12.9  |
| Average number of bits revealed ($Z$)    | 98.2   | 57.6   | 155.8 |
| Average key block length            | $X$    | $Z$    |       |
|                                       | 1207.7 | 927.2  |       |
| Average QBER                       | $X$    | $Z$    |       |
|                                       | 5.4    | 1.2    |       |
| Error correction efficiency ($X$)     | 1.31   |        |       |
| Error correction efficiency ($Z$)     | 1.59   |        |       |

the residual error rate requirements grow more stringent the efficiency of the error correction algorithm relative to the Shannon limit, $f(x)$, will begin to deteriorate. For all experiments there were no residual errors left in the error corrected key after error correction was performed.

5. Conclusions

In conclusion, we have implemented the first experiment to utilize a biased (non-uniform) basis choice in order to increase the efficiency of the number of secure key bits generated from raw key bits. We investigated many of the issues associated with its implementation including choosing the optimal bias, doing a more refined error analysis, and taking care of finite size key effects. We simulated a biased non-polarizing BS in order to study different biases for the system and their resulting efficiencies. All other aspects of the experiment were implemented in their entirety so that our 50/50 BS can be easily exchanged with a new fixed non-polarizing BS with no other changes needed to the system. For the near optimal biases of 0.8804/0.1196 ($Z/X$) for Alice and 0.9062/0.0938 ($Z/X$) for Bob, we were able to generate 0.4567 secure key bits per raw key bit; whereas, the unbiased case generated 0.2550 secure key bits per raw key bit. This represents an increase in the efficiency of the key generation rate by 79% over the unbiased case. An improved error correction algorithm was also implemented and statistics for its operation on actual generated key material were discussed.

Acknowledgments

Support for this work by NSERC, QuantumWorks, CIFAR, CFI, CIPI, ORF, ORDCF, ERA and the Bell family fund are gratefully acknowledged. We thank N Lütkenhaus, R Kaltenbaek, T Moroder, H Hasseler and O Moussa for their helpful discussions. We also thank R Horn and M Wesolowski for their help with the setup of the experiment. Lastly, we thank the anonymous referees for their many comments, which were very useful in improving the quality of this paper.
References

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore, India) p 175

[2] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell’s theorem Phys. Rev. Lett. 68 557

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys. 74 145–95

[4] Dušek M, Lütkenhaus N and Hendrych M 2006 Quantum cryptography Prog. Opt. 49 381

[5] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2008 A framework for practical quantum cryptography arXiv:0802.4155 [quant-ph]

[6] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol Phys. Rev. Lett. 85 441

[7] Lütkenhaus N 2000 Security against invidual attacks for realistic quantum key distribution Phys. Rev. A 61 052304

[8] Ma X, Fung C H and Lo H K 2007 Quantum key distribution with entangled photon sources Phys. Rev. A 76 012307

[9] Lo H K, Chau H F and Ardehali M 2002 Efficient quantum key distribution scheme and a proof of its unconditional security J. Cryptol. 18 133–65

[10] Acín A, Massar S and Pironio S 2006 Efficient quantum key distribution secure against no-signalling eavesdroppers arXiv:quant-ph/0605246

[11] Beaudry N J, Moroder T and Lütkenhaus N 2008 Squashing models for optical measurements in quantum communication Phys. Rev. Lett. 101 093601

[12] Tsurumaru T and Tamaki K 2008 Security proof for quantum-key-distribution systems with threshold detectors Phys. Rev. A 78 032302

[13] Koashi M, Adachi Y, Yamamoto T and Imoto N N 2008 Security of entanglement-based quantum key distribution with practical detectors arXiv:0804.0891 [quant-ph]

[14] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 Generalized privacy amplification IEEE Trans. Inf. Theory 41 1915

[15] Carter J L and Wegman M N 1979 Universal classes of hash functions J. Comput. Syst. Sci. 18 143

[16] Ma X, Fung F, Dupuis F, Chen K, Tamaki K and Lo H K 2006 Decoy-state quantum key distribution with two-way classical postprocessing Phys. Rev. A 74 032330

[17] Scarani V and Renner R 2008 Security bounds for quantum cryptography with finite resources arXiv:0806.0120v1 [quant-ph]

[18] Cai R Y Q and Scarani V 2009 Finite-key analysis for practical implementations of quantum key distribution New J. Phys. 11 045024

[19] Alléaume R et al 2007 SECOQC white paper on quantum key distribution and cryptography arXiv:quant-ph/0701168

[20] Lütkenhaus N 1999 Estimates for practical quantum cryptography Phys. Rev. A 59 3301

[21] Sugimoto T and Yamazaki K 2000 A study on secret key reconciliation protocol ‘cascade’ IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E83A 1987

[22] Hasegawa J, Hayashi M, Hiroshima T and Tomita A 2007 Security analysis of decoy state quantum key distribution incorporating finite statistics arXiv:0707.3541 [quant-ph]

[23] Scarani V and Renner R 2008 Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way processing Phys. Rev. Lett. 100 200501

[24] Weihs G and Erven C 2007 Entangled free-space quantum key distribution Proc. SPIE 6780 1–9

[25] Erven C, Couteau C, Laflamme R and Weihs G 2008 Entanglement based free-space quantum key distribution Proc. SPIE 7099 709916

[26] Erven C, Couteau C, Laflamme R and Weihs G 2008 Entangled quantum key distribution over two free-space optical links Opt. Express 16 16840–53
[27] Bennett C H, Brassard G and Robert J M 1988 Privacy amplification by public discussion *SIAM J. Comput.* 17 210–29

[28] Bennett C H, Bessette F, Salvail L, Brassard G and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* 5 3–28

[29] Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion *Lect. Notes Comput. Sci.* 765 410