PPLN-waveguide-based polarization entangled QKD simulator

John Gariano, Ivan B. Djordjevic

John Gariano, Ivan B. Djordjevic, "PPLN-waveguide-based polarization entangled QKD simulator," Proc. SPIE 10409, Quantum Communications and Quantum Imaging XV, 104090A (30 August 2017); doi: 10.1117/12.2272449

SPIE.

Event: SPIE Optical Engineering + Applications, 2017, San Diego, California, United States

PPLN-waveguide-based polarization entangled QKD simulator

John Gariano[a*] and Ivan B. Djordjevic[a]

[a]The University of Arizona, Tucson, AZ

ABSTRACT

We have developed a comprehensive simulator to study the polarization entangled quantum key distribution (QKD) system, which takes various imperfections into account. We assume that a type-II SPDC source using a PPLN-based nonlinear optical waveguide is used to generate entangled photon pairs and implements the BB84 protocol, using two mutually unbiased basis with two orthogonal polarizations in each basis. The entangled photon pairs are then simulated to be transmitted to both parties; Alice and Bob, through the optical channel, imperfect optical elements and onto the imperfect detector. It is assumed that Eve has no control over the detectors, and can only gain information from the public channel and the intercept resend attack. The secure key rate (SKR) is calculated using an upper bound and by using actual code rates of LDPC codes implementable in FPGA hardware. After the verification of the simulation results, such as the pair generation rate and the number of error due to multiple pairs, for the ideal scenario, available in the literature, we then introduce various imperfections. Then, the results are compared to previously reported experimental results where a BBO nonlinear crystal is used, and the improvements in SKRs are determined for when a PPLN-waveguide is used instead.

Keywords: Quantum Key Distribution, Quantum cryptography, Polarization entanglement

1. INTRODUCTION

The need to generate a secure key between two parties at a distance has increased as communication systems transmit faster and sned larger chunks of data. One solution to generating this secret key is quantum key distribution (QKD), which was presented by Bennett and Brassad in 1984.[1] Ekert then presented the E91 protocol,[2] which was simplified by Bennett, Brassad, and Mermin in 1992, and has become known as the BB92 protocol.[3]

Current QKD systems are implemented using weak coherent sources[4–6] and entangled photon sources.[7,8] Some of the advantages to using an entangled photon source are: lower information leakage from multiple-pair photon signals,[9] and channels with higher losses are usable;[10] however, the generation rate of photon pairs is much lower than using a weak coherent source. To generate entangled photons, a spontaneous-parametric-down-conversion (SPDC) source is used, where a pump laser interacts with a non-linear medium, allowing for entangled photons to be generated. The SPDC source can be a Type I or Type II, where polarization of the photons in a pair are parallel or orthogonal. These sources can be made by using β-barium borate (BBO) or periodically poled $LiNbO_3$ (PPLN) nonlinear crystals. A PPLN crystal has a much higher coupling efficiency than a BBO crystal.[11]

In our previous work,[12] a trade study of a QKD system over a maritime channel using a weak coherent source was performed. Here, a simulation is presented for a QKD system implementing the BB84 protocol using entangled photons. An eavesdropper is included in the simulation, with attacks that are limited to the intercept resend attack and access to all communications over the public channel. This simulation is then compared to analytical equations as well as to previously published results. Then, using a theoretical upper bound and practical LDPC codes, the secure key rates of our simulation are compared to experimental results.

*E-mail: Jagariano@email.arizona.edu

Quantum Communications and Quantum Imaging XV, edited by Ronald E. Meyers, Yanhua Shih, Keith S. Deacon, Proc. of SPIE Vol. 10409, 104090A · © 2017 SPIE
CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2272449

2. SYSTEM DESIGN

When using a SPDC source, it can be controlled by a third party at any location in the channel,[10] as seen in Figure 1. In our system, it is assumed that Eve is only located in the channel going to Bob. The SPDC source generates pairs of entangled photon, along two different paths. The first photon of the pair is transmitted to Alice, through a lossy channel and then through the detection apparatus. The second photon of the pair is transmitted to Bob and Eve, first transitioning through a channel to Eve, then on to Bob, and finally through the detection apparatus. Eve will perform the intercept resend attack on each photon that reaches her, with a probability of $P_{E.I.R}$. The detection apparatus is designed to implement the BB84 protocol, using a beam splitter to randomly sort photons into two mutually unbiased basis (HV or AD), then using a polarizing beam splitter to sort into orthogonal polarizations, symbolizing the binary data. If a detection occurs in both the HV and AD basis or in the orthogonal polarizations, the system will randomly select the basis or polarization.

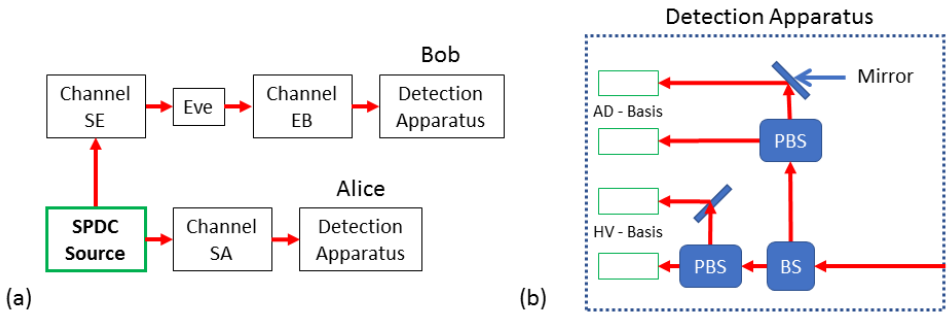

Figure 1. a) QKD System model with an entangled photon source located at an arbitrary position in the channel. b) The detection apparatus used to implement the BB84 protocol, consisting of two mutual unbiased basis, each containing two orthogonal polarizations

The SPDC source can either be Type I or Type II with pair number distributions given by Equation 1 and Equation 2 respectively as functions of μ, the mean number of photon pairs.[10,13,14] It should be noted that the distribution of[14] can be written as Equation 1 by rewriting in terms of the mean number of photons.

$$P_S(n) = \frac{\mu^n}{(1+\mu)^{n+1}} \tag{1}$$

$$P_S(n) = \frac{(n+1)(\mu/2)^n}{(1+(\mu/2))^{n+2}}. \tag{2}$$

The efficiency of the paths from the source to Alice and Bob are defined as η_A and η_B, where η is the product of the efficiencies of all optical elements in that path. A photon passing through the channel can be modeled by a binomial distribution. From this the probability of getting m photons out of the channel given that l photons entered the channel is:

$$P_{Chan}(m|l) = \binom{l}{m}(1-\eta)^{l-m}\eta^m. \tag{3}$$

As the channels going to Alice and Bob are independent of each other, the probability that the source sends l photons, and of them Alice receives α photons and Bob receives β photons is

$$P(l,\alpha,\beta) = P_A(\alpha|l)P_B(\beta|l)P_S(l). \tag{4}$$

The system is also capable of simulating noise from dark counts or background photons. Given the probability of a dark count, P_{Dark}, and probability of receiving a background photon, P_{Back}, the total probability that a single detector clicks due to noise is given by:

$$P_{Noise} = P_{Dark} + P_{Back} - P_{Dark}P_{Back}. \tag{5}$$

As the system implements the BB84 protocol, the probability that Alice (Bob) records a click caused by noise on any of its four detectors, $P_{AN,4}$ ($P_{BN,4}$), is calculated using a binomial distribution, using P_{Noise} for Alice's (Bob's) detection apparatus,

$$P_{AN,4} = \sum_{i=1}^{4} \binom{4}{i} (1 - P_{Noise})^{4-i} P_{Noise}^{i} \tag{6}$$

To calculate the secret key rate (SKR), the security proof given by Koashi and Preskill,[10,15] shown in Equation 7. The bit error rate (BER), δ is assumed to be equal to the phase error rates, $f(\delta)$ is the reconciliation efficiency of the error correction protocol, and $H_2(\delta)$ is the binary entropy function.

$$R_{SKR} = P_{Key} \left[1 - f(\delta) H_2(\delta) - H_2(\delta)\right]. \tag{7}$$

Ideally when $f(\delta) = 1$, however in practice $f(\delta) > 1$. Using the Cascade protocol, proposed by Brassard and Salvail,[16] the values for $f(\delta)$ are given in Table 1.[17] For an LDPC code, the reconciliation efficiency can be calculated for a given rate,R, and threshold error rate,δ_t,[18] as given in Equation 8. The code rates and threshold error rates considered here are given in Table 2.[19]

$$f(\delta) = \frac{1 - R}{H_2(\delta_t)}. \tag{8}$$

Table 1. Reconciliation efficiency of the Cascade protocol for given bit error rate thresholds

δ_t	0.01	0.05	0.1	0.15
$f(\delta)$	1.16	1.16	1.22	1.35

Table 2. LDPC code of length 10^6, Rates and remaining BER is below 1.5×10^{-6}

Rate	0.9	0.85	0.8	0.75	0.70	0.65	0.6	0.55	0.5
δ_t	0.0109	0.0199	0.0298	0.0396	0.0504	0.0633	0.0766	0.0904	0.1071

3. THEORETICAL VALIDATION

Before presenting a theoretical validation of the simulation, it should be noted that the work of Ma *et al* and Waks *et al*,[10,20] have shown a theoretical system as well as the security of QKD using entangled photons. In the work of Ma *et al*, they consider only the case where Alice and Bob both receive the same number of photons. In contrast, this theoretical examination considers the cases where Alice and Bob can receive different number of photons. It is more practical for the channels to be mismatched, causing the number of photons detected by one user will be higher than the other. Similarly, the work of Waks *et al*, assumes that when the source produces multiple photon pairs, they are correlated. This implies that for an ideal system with no loss, all photon pairs will go into the same basis and induce no error. Again, this simulation considers the multiple photon pairs to be independent of each other.

The first aspect to consider is the rate of both Alice and Bob's detectors recording a click. This happens in one of four ways; both Alice and Bob receive at least one photon that was transmitted, Alice (Bob) receives at least one photon that was transmitted while Bob (Alice) records a click due to noise, and both Alice and Bob record clicks due to noise. From these observations the probability that both Alice and Bob's detectors' recording a click is given by:

$$\begin{aligned} P_{Rec} &= P(A\ Click \cap B\ Click) \\ &= P(l > 0, \alpha > 0, \beta > 0) + P(l > 0, \alpha = 0, \beta > 0) P_{AN,4} \\ &\quad + P(l > 0, \alpha > 0, \beta = 0) P_{BN,4} + P_{AN,4} P_{BN,4} \end{aligned} \tag{9}$$

Since two mutually unbiased basis are used, there is a probability of $\frac{1}{2}$ that a timeslot is used after basis reconciliation. Thus the probability that a bit is recorded and used in the key is:

$$P_{Key} = \frac{1}{2} P_{Rec}. \tag{10}$$

The next step of the protocol is privacy amplifying any information that Eve may have of the received key bits, which is dependent of the measured BER. As Alice and Bob have two detectors,('0' and '1') there are two possible ways to disagree. This implies that the BER is equal to half the probability that a bit is received in error. To calculate the BER however, the probability that Alice and Bob agree on the same bit will be considered.

$$\delta = \frac{1}{2} P_{Err} = \frac{1}{2}(1 - P_{Cor}). \tag{11}$$

The probability that Alice and Bob's detectors agree is given by, P_{Cor}, is defined as follows:

$$\begin{aligned} P_{Cor} &= P(A = B|Key) \\ &= \frac{2P(A = B, Key)}{P_{Rec}} \end{aligned} \tag{12}$$

where $P(A = B, Key)$ is dependent upon the signal, noise, and if Eve has performed the intercept resend attack (E.I.R.),

$$\begin{aligned} P(A = B, Key) = \frac{1}{2} P(A = B, Signal) + P(A = B, Noise) \\ - \frac{1}{2} P(A = B, Signal, Noise) - \frac{1}{2} P(A = B, Signal, E.I.R.). \end{aligned} \tag{13}$$

The above expression comes from using the union of probabilities, where the $\frac{1}{2}$ term is applied to applying basis reconciliation. The first term is the probability that Alice and Bob's bits agree given that the detectors detect photons that had been transmitted. More formally this is given as

$$\begin{aligned} P(A = B, Signal) &= P(A = B, l > 0, 0 < \alpha \leq l, 0 < \beta \leq l) \\ &= \sum_{l=1}^{\infty} \sum_{\alpha,\beta=1}^{l} P(A = B|l, \alpha, \beta) P(l, \alpha, \beta) \end{aligned} \quad , \tag{14}$$

where

$$P(A = B|l, \alpha, \beta) = \begin{cases} (\frac{1}{2})^{l-1} & l = \alpha, l = \beta \\ (\frac{1}{2})^{\beta} & l = \alpha, l \neq \beta \\ (\frac{1}{2})^{\alpha} & l \neq \alpha, l = \beta \\ (\frac{1}{2})^{\alpha+\beta} & l \neq \alpha, l \neq \beta \end{cases} . \tag{15}$$

In Equation 15, the first case is where Alice and Bob both receive all of the photons that were transmitted. In this case, the photons remain entangled, and will land on the correct detectors of the same basis. If there is only a single photon, the bits are always correct; however as more photons are transmitted, error is introduced. In the second and third cases, one of the parties receives all of the photons, while the other party does not, implying all photons reaching the second user will still be entangled. Letting the first user select its bit, each photon has a probability of being detected correctly of $\frac{1}{2}$. Finally, the last case is where both Alice and Bob do not receive the same number of photons that were transmitted. In this case, the photons may or may not still be entangled, thus the photons at each have a probability of being selected of $\frac{1}{2}$.

Lets us now consider the case when Alice and Bob both choose the correct detector when the clicks are only generated by noise, $P(A = B, Noise)$,

$$P(A = B \cap Noise) = \frac{P_{AN,4}}{4}\frac{P_{BN,4}}{4}. \tag{16}$$

Where the factor of $\frac{1}{4}$ comes from the probability of choosing the correct detector in a basis and the probability of choosing the correct basis.

Since the detectors can be triggered by noise when no signal is present or when one user's detector clicks due to signal while the other user's detector is triggered by noise, the probability of receiving a click from signal and from noise, $P(A = B \cap Signal \cap Noise)$, is defined by Equation 17. Using the union of events, Equation 17 must be subtracted.

$$\begin{aligned} P(A = B \cap Signal \cap Noise) &= P(A = B, l > 0, 0 < \alpha \leq l, 0 < \beta \leq l, Noise) \\ &\quad + P(A = B, l > 0, 0 < \alpha \leq l, \beta = 0, Noise) \\ &\quad + P(A = B, l > 0, alpha = 0, 0 < \beta \leq l, Noise) \\ &= \sum_{l=1}^{\infty}\Bigg[\sum_{\alpha,\beta=1}^{l} P(A = B|l, \alpha, \beta, Noise)P(l, \alpha, \beta) \\ &+ \sum_{\beta=1}^{l} P(A = B|l, \alpha = 0, \beta, Noise)P(l, \alpha, \beta) \\ &+ \sum_{\alpha=1}^{l} P(A = B|l, \alpha, \beta = 0, Noise)P(l, \alpha, \beta)\Bigg] \end{aligned}, \tag{17}$$

where

$$P(A = B|l, \alpha, \beta, Noise) = \begin{cases} (P_{AN,4} + P_{BN,4})(\frac{1}{2})^{l+2} & l = \alpha, l = \beta \\ (P_{AN,4} + P_{BN,4})(\frac{1}{2})^{\beta+2} & l = \alpha, l \neq \beta \\ (P_{AN,4} + P_{BN,4})(\frac{1}{2})^{\alpha+2} & l \neq \alpha, l = \beta \\ (P_{AN,4} + P_{BN,4})(\frac{1}{2})^{\beta+\alpha+2} & l \neq \alpha, l \neq \beta \\ P_{BN,4}(\frac{1}{2})^{\alpha+2} & \alpha > 0, \beta = 0 \\ P_{AN,4}(\frac{1}{2})^{\beta+2} & \alpha = 0, \beta > 0 \end{cases}. \tag{18}$$

Examining Equation 18, the factor of $\frac{1}{4}$ comes from selecting the correct basis and detector. In the first four cases, the cases are similar to those described above when no noise is present, with the exception that Alice and Bob both receive photons transmitted, and either Alice or Bob have a detector click due to noise. In the last two cases, we assume that only one of the users has a detector click due to the transmitted photons, and the other user's detector clicks due to noise.

Finally, to define the last term of Equation 13, the probability that Alice and Bob's detectors choose the correct basis and that Eve has performed the intercept resend attack, $P(A = B \cap Signal \cap E.I.R.)$. It is important to note that unlike the case where Alice and Bob both receive a click only due to the dark count rate, a photon must reach Alice and Bob for the detectors to trigger when Eve performs the intercept resend attack.

$$\begin{aligned} P(A = B \cap Signal \cap E.I.R.) &= P(A = B, l > 0, 0 < \alpha \leq l, 0 < \beta \leq l, E.I.R) \\ &= \sum_{l=1}^{\infty}\sum_{\alpha,\beta=1}^{l} P(A = B|l, \alpha, \beta)P(l, \alpha, \beta)P_{E.I.R|\beta} \end{aligned}, \tag{19}$$

where

$$P_{E.I.R|\beta} = \sum_{i=1}^{\beta}\binom{\beta}{i}(1 - P_{E.I.R})^{\beta-i}P_{E.I.R}^{i} \quad . \tag{20}$$

Here $P_{E.I.R|\beta}$ is the probability that Eve has performed the intercept resend attack given that β photons have reached Bob. When Eve performs the intercept resend attack the photon is no longer entangled, thus Alice and Bob's bits have a lower probability of agreement.

Using the equations above that model our system, a comparison of the analytical equations to the simulated results using both type I and type II sources. The simulated results were generated by averaging 100 trials, using a minimum of 40k bits from the generated key to sample the BER. In the following figures, a positive error, indicated that the analytical value is larger than the simulated value, and the percentage error is relative to simulated value.

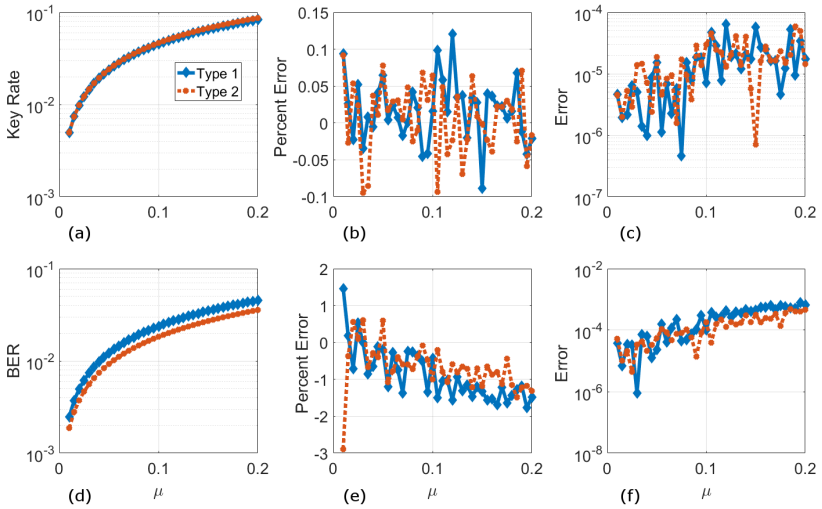

Figure 2. Ideal system: a) Analytic key generation rate for Type I and Type II SPDC source. b) Percentage error between simulated and analytic key generation rate. c) Absolute error between simulated and analytic key generation rate. d) Analytic BER for Type I and Type II SPDC source. e) Percentage error between simulated and analytic BER. f) Absolute error between simulated and analytic BER.

First, a comparison of an *ideal system*, seen in Figure 2, where it is assumed that there's no loss, noise or eavesdropper present performing the intercept resend attack. Examining Figure 2(a-c), both Type I and Type II SPDC sources generate the key at approximately the same rate. Additionally, the error between the simulated and analytic results is less than 0.2%. Next, examining Figure 2(d-f), the BER is higher for a Type I source than a Type II. This is caused by the Type II source having a lower probability of producing multiple photon pairs than a Type I. Unlike for the key generation rate, the percent error between the analytic and simulated results is now less than 2%. It should be noted that by using a 40k bits to sample the BER, the simulated results have a maximum resolution of 2.5×10^{-5}. Decreasing the average number of photons, the simulated BER will then have a larger standard deviation.

Now when a system with *no loss or eavesdropper*, but each detector has a probability of receiving a click due to noise of $P_N = 1.28 \times 10^{-4}$ is considered, shown in Figure 3. As expected, the key generation rate does not increase as there is such a low probability of noise. There is a slight increase in the BER, however for small μ, the analytic BER is higher than the simulated BER. As μ increases, the error decreases, due to the probability of a click caused by noise becoming of the same order as the key generation rate.

Assuming the system is ideal, with the exception that *Eve is performing the intercept resend attack 10% of the time*, seen in Figure 4. As Eve is measuring the photon and then retransmitting it, the key generation rate is not affected, however the BER is affected, since 10% of the photons that are recorded have been measured by Eve and are no longer entangled. A disentangled photon has an equal probability of being correct given it enters the correct basis, leading to a minimum BER of 5%.

In Figure 5, we consider a system where the source is located at Alice, the detector apparatuses have efficiencies of 18.81%, the channel to Bob has an efficiency of 77.08%, and there is no noise or eavesdropper present. As expected, the key generation rate has decreased, while the percent error has stayed constant. The BER has increased, because with more loss, most of time slots contributing to the key are generated when multi-photon

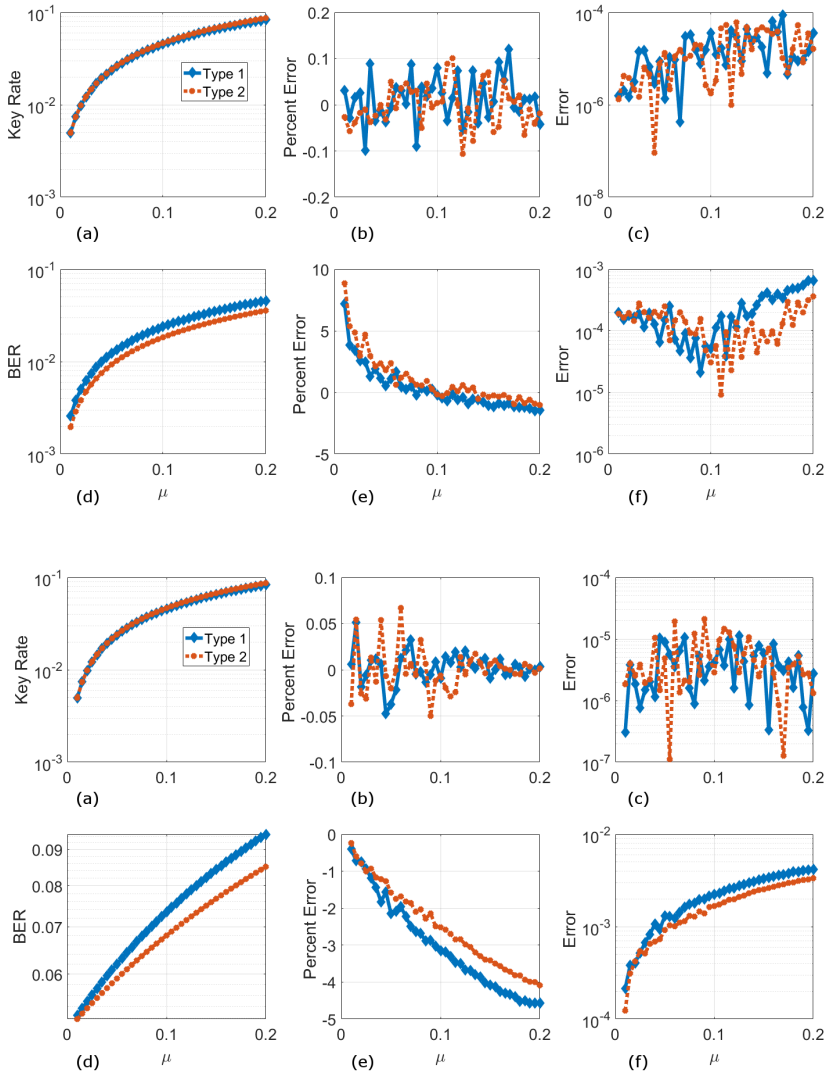

Figure 3. Ideal system with noise: a) Analytic key generation rate for Type I and Type II SPDC source. b) Percentage error between simulated and analytic key generation rate. c) Absolute error between simulated and analytic key generation rate. d) Analytic BER for Type I and Type II SPDC source. e) Percentage error between simulated and analytic BER. f) Absolute error between simulated and analytic BER.

Figure 4. Ideal system with Eve performing the intercept resend attack 10% of the time: a) Analytic key generation rate for Type I and Type II SPDC source. b) Percentage error between simulated and analytic key generation rate. c) Absolute error between simulated and analytic key generation rate. d) Analytic BER for Type I and Type II SPDC source. e) Percentage error between simulated and analytic BER. f) Absolute error between simulated and analytic BER.

pairs that were transmitted. It should be noted that in Figure 5(e), the percent error increase as the average number of photons increases.

In Figure 6, we consider the case above with the losses, and add a probability of receiving a click due to noise of $P_N = 1.28 \times 10^{-4}$. The key generation rate is still tracked with an error on the order of 0.1%. As in the above cases, the BER has increased due to the noise, however the analytic BER is smaller than the simulated BER for small μ, while when μ is larger, the analytic BER is larger than the simulated BER.

4. COMPARISON TO EXPERIMENTAL RESULTS

Now that a mathematical basis has been formed for the simulation, a comparison of the simulated results to the published experimental results of Marcikic *et al.*[8] In their system, the source is a Type II β-barium borate (BBO) nonlinear crystal, located at Alice, detection efficiencies for both detection apparatuses is 20%, and the channel going to Bob has an efficiency of 19.13%. Each detector of their system has an average dark count rate of 1000 s^{-1}. However, the rate the system was operated at was not specified, it is assumed to have be operated at 10 MHz, because they used a maximum detection window of 3.75 ns, with a displacement of 20ns from the main detection window, for maintaining timing synchronization. This implies that the probability of a dark count is given as $P_{Dark} = 10^{-4}$. In Marcikic's experiment, the coincidence rate was 2600 s^{-1}, and after basis

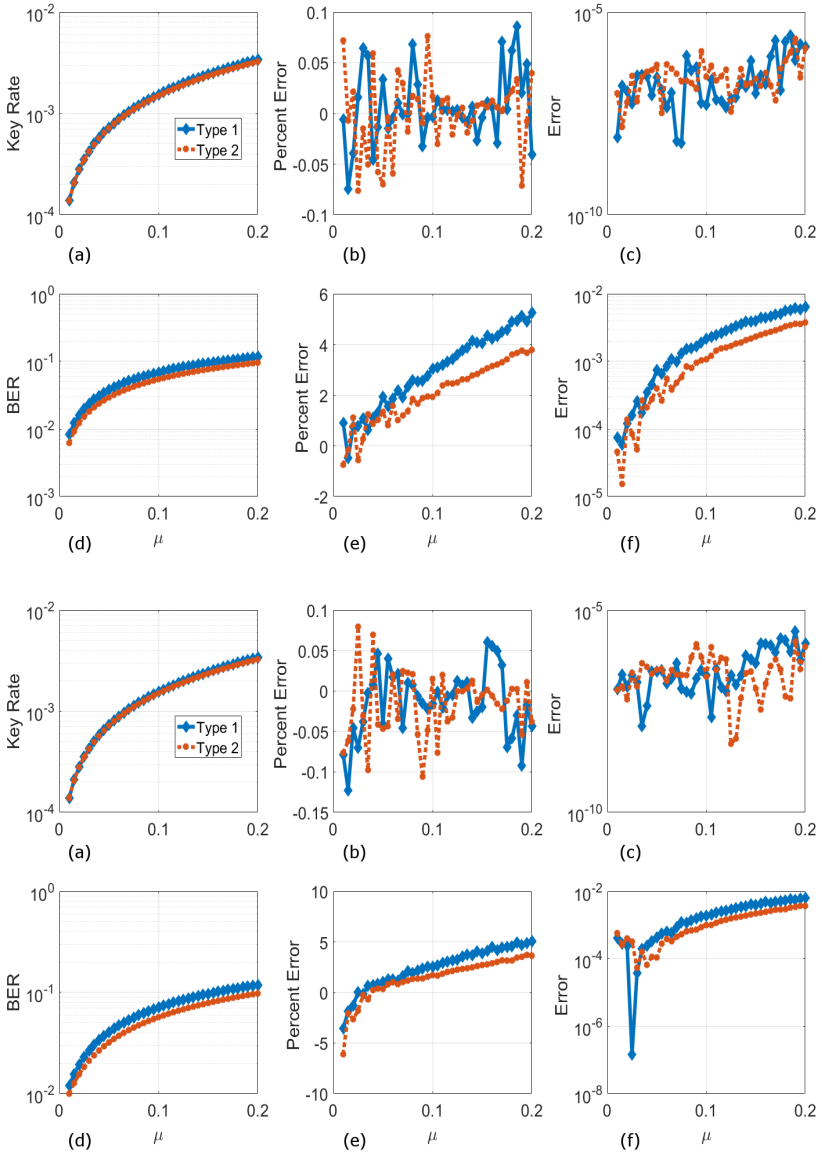

Figure 5. System with loss: a) Analytic key generation rate for Type I and Type II SPDC source. b) Percentage error between simulated and analytic key generation rate. c) Absolute error between simulated and analytic key generation rate. d) Analytic BER for Type I and Type II SPDC source. e) Percentage error between simulated and analytic BER. f) Absolute error between simulated and analytic BER.

Figure 6. System with loss and noise: a) Analytic key generation rate for Type I and Type II SPDC source. b) Percentage error between simulated and analytic key generation rate. c) Absolute error between simulated and analytic key generation rate. d) Analytic BER for Type I and Type II SPDC source. e) Percentage error between simulated and analytic BER. f) Absolute error between simulated and analytic BER.

reconciliation the sifted key bit rate is 1100 s^{-1}. It should be noted that a coincidence is used for key generation if the photons are recorded within a detection window smaller than 1.75 ns. The average BER was found to be 5.4%, and the secure key bit rate was found to be 630 s^{-1}.

In Figure 7, the results of our simulation are presented for a SPDC Type II source with the same channel conditions. Considering only $\mu = 0.085$ when examining Figure 7(a), the key generation rate is found to be 3.6×10^{-4} and the BER is found to be 5.52%. Using the assumption that the system is operating at 10 MHz, the key bit generation rate becomes 3600 s^{-1}. The key generation rate is three times higher than what is presented in Marcikics experiment, but is only slightly higher than the coincidence rate of the system. The BER is also only slightly higher than the value found in Marcikics experiment. Examining Figure 7(b), the secure key rates are presented using the upper bound (UB), cascade protocol, and practical LDPC codes. The simulated results consider using 5k bits for sampling the BER, and adds a statistical error using a confidence interval of 90%. The maximum SKR for the upper bound is found to be located at $\mu = 0.085$, and is 1.07×10^{-4}, while the SKR for the cascade protocol and practical LDPC codes is 8.74×10^{-5} and 1.03×10^{-4} respectively. This implies that

the secure key bit rates are 1070, 874, and 1003 s^{-1} respectively, which is slightly higher than what was reported from the experiment.

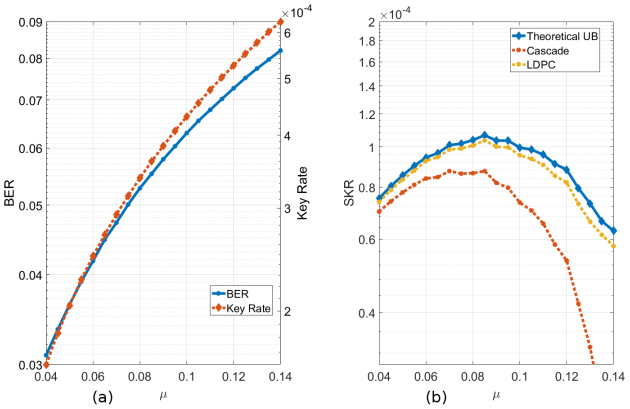

Figure 7. system simulated with the conditions presented in the experiment by Marcikic *et al*:[8] a) Key generation rate and BER. b) SKR for the theoretical upper bound (UB), cascade protocol and practical LDPC codes, assuming 5K bits used to sample the BER.

A second experiment was also performed by Marcikic using the same set up but with a long pass filter. This increased the sifted key bit rate to 1600 s^{-1}, the BER to 5.75% and the secret key bit rate of 850 s^{-1}. There was no information provided regarding the increase in the amount of noise by changing the optical filter, however the results of our simulation provided are also within the proximity of the results for this experiment.

5. CONCLUSION

The simulation that has been presented has been shown to implement the BB84 protocol using entangled photons under the assumption that an eavesdropper is limited to only the intercept resend attack and listening to discussion over the public channel. The entangled photons can be from either a Type I or Type II SPDC source, and we have shown analytic expressions that can be used to calculate the feasibility and secure key rate of the system. The analytic equations perform well when the probability of noise is much smaller than the key generation rate and when the average number of photons is much smaller than 1. Finally we have compared the results of simulating the system used in the experiment performed by Marcikic *et al.* Using the parameters of the system that were provided, our simulation was able to generate a secure key rate of the same order as what had been presented for both versions of the experiment performed.

Funding Information

ONR MURI program (N00014-13-1-0627)

REFERENCES

[1] Bennett Ch, H. and Brassard, G., "Quantum cryptography: public key distribution and coin tossing int," in [*Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*], 175–9 (1984).

[2] Ekert, A., "Quantum cryptography based on bell's theorem," *Physical Review Letters* **67**(6), 661–663 (1991).

[3] Bennett, C. H., Brassard, G., and Mermin, N. D., "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.* **68**, 557–559 (Feb 1992).

[4] Marand, C. and Townsend, P. D., "Quantum key distribution over distances as long as 30 km," *Opt. Lett.* **20**, 1695–1697 (Aug 1995).

[5] Bourennane, M., Gibson, F., Karlsson, A., Hening, A., Jonsson, P., Tsegaye, T., Ljunggren, D., and Sundberg, E., "Experiments on long wavelength (1550nm) "plug and play" quantum cryptography systems," *Opt. Express* **4**, 383–387 (May 1999).

[6] Zhang, H.-F., Wang, J., Cui, K., Luo, C.-L., Lin, S.-Z., Zhou, L., Liang, H., Chen, T.-Y., Chen, K., and Pan, J.-W., "A real-time qkd system based on fpga," *Journal of Lightwave Technology* **30**(20), 3226–3234 (2012).

[7] Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H. R., Lorünser, T., Maurhardt, O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T., and Zeilinger, A., "Practical quantum key distribution with polarization entangled photons," *Opt. Express* **12**, 3865–3871 (Aug 2004).

[8] Marcikic, I., Lamas-Linares, A., and Kurtsiefer, C., "Free-space quantum key distribution with entangled photons," *Applied Physics Letters* **89**(10) (2006).

[9] Bettelli, S., Lorunser, T., Peev, M., Querasser, E., Dusek, M., Bartuskova, L., Blauensteiner, B., Huebel, H., Poppe, A., and Zeilinger, A., "Effect of double pair emission to entanglement based qkd," in [*2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference*], 1–1 (June 2007).

[10] Ma, X., Fung, C.-H. F., and Lo, H.-K., "Quantum key distribution with entangled photon sources," *Phys. Rev. A* **76**, 012307 (Jul 2007).

[11] Tanzilli, S., Riedmatten, H. D., Tittel, H., Zbinden, H., Baldi, P., Micheli, M. D., Ostrowsky, D. B., and Gisin, N., "Highly efficient photon-pair source using periodically poled lithium niobate waveguide," *Electronics Letters* **37**, 26–28 (Jan 2001).

[12] Gariano, J., Neifeld, M., and Djordjevic, I., "Engineering trade studies for a quantum key distribution system over a 30km free-space maritime channel," *Appl. Opt.* **56**, 543–557 (Jan 2017).

[13] Lim, H. C., Yoshizawa, A., Tsuchida, H., and Kikuchi, K., "Distribution of polarization-entangled photon-pairs produced via spontaneous parametric down-conversion within a local-area fiber network: Theoretical model and experiment," *Opt. Express* **16**, 14512–14523 (Sep 2008).

[14] Broome, M. A., Almeida, M. P., Fedrizzi, A., and White, A. G., "Reducing multi-photon rates in pulsed down-conversion by temporal multiplexing," *Opt. Express* **19**, 22698–22708 (Nov 2011).

[15] Koashi, M. and Preskill, J., "Secure quantum key distribution with an uncharacterized source," *Phys. Rev. Lett.* **90**, 057902 (Feb 2003).

[16] Brassard, G. and Salvail, L., [*Secret-Key Reconciliation by Public Discussion*], 410–423, Springer Berlin Heidelberg, Berlin, Heidelberg (1994).

[17] Lütkenhaus, N., "Security against individual attacks for realistic quantum key distribution," *Phys. Rev. A* **61**, 052304 (Apr 2000).

[18] Kasai, K., Matsumoto, R., and Sakaniwa, K., "Information reconciliation for qkd with rate-compatible non-binary ldpc codes," in [*2010 International Symposium On Information Theory Its Applications*], 922–927 (Oct 2010).

[19] Elkouss, D., Leverrier, A., Alleaume, R., and Boutros, J. J., "Efficient reconciliation protocol for discrete-variable quantum key distribution," in [*2009 IEEE International Symposium on Information Theory*], 1879–1883 (June 2009).

[20] Waks, E., Zeevi, A., and Yamamoto, Y., "Security of quantum key distribution with entangled photons against individual attacks," *Phys. Rev. A* **65**, 052310 (Apr 2002).