# Simulation of Quantum Key Distribution Using Entangled Photon Pairs Over Free-Space Channels

Daniel E. Jones*, Dashiell L.P. Vitullo*, Trevor Cook*, Lisa M. Scott*, Andrew Toth*, and Brian T. Kirby*†
* DEVCOM Army Research Laboratory, Adelphi, MD, USA
† Tulane University, New Orleans, LA, USA
daniel.e.jones.161.civ@army.mil

2022 IEEE Photonics Conference (IPC) | 978-1-6654-3487-4/22/$31.00 ©2022 IEEE | DOI: 10.1109/IPC53466.2022.9975528

***Abstract*— We develop a quantum network simulation framework designed for integration into tactical simulation tools. It extends the quantum networking tool SQUANCH with realistic fiber and free-space channel models and implements subroutines for simulating entanglement-based QKD. We benchmark our framework using a published free-space QKD experiment.**

***Keywords*— Quantum network simulation, quantum key distribution, quantum information, quantum communication**

## I. Introduction

Quantum networks are unlikely to completely replace classical networks but instead will work in conjunction with them. For simple networks and some specific network configurations, analytical results modeling the behavior of these combined quantum-classical networks are possible. However, in general, simulation is often required to model the combined behavior of quantum and classical components in a quantum network. While several quantum network simulation tools have been developed recently [1], they are generally not applicable to tactical scenarios with severe network resource constraints.

Here, we use our custom framework for quantum network simulation, QuanTACT [2], that can be integrated into existing tactical simulation tools. It uses SQUANCH [3], the Simulator for Quantum Networks and Channels, to model quantum systems. We choose SQUANCH since it utilizes a parallelized agent-based model where each agent runs in its own process. We ultimately plan to integrate QuanTACT with existing tactical network modeling tools such as the Extendable Mobile Ad-hoc Network Emulator (EMANE), so we have designed our framework to allow for a straightforward replacement of SQUANCH's native classical communications with previously developed EMANE classical communication models.

In this paper, we apply our framework to simulate a published quantum key distribution (QKD) experiment using polarization-entangled photons over free-space channels [4]. For a detailed description of the QuanTACT code-base and how it simulates entanglement-based QKD, see [2]. Here, we implement a new channel model for free-space links that includes stray light, detector dark counts, and transient channel degradation, in addition to a new mechanism for simulating imperfect quantum state preparation. The simulation described here also implements the slightly different error correction and privacy amplification processes performed in [4] as opposed to the methods used in the experiments that were previously simulated in [2].

## II. Results

The three sources of loss that we consider in our framework are insertion loss, channel loss, and detection efficiency. See [2] for a description of how loss can be modeled explicitly or included implicitly in the success probability of photon pair generation. In [4], the authors perform QKD with one photon of an entangled pair distributed over a 1.5 km free-space link. The authors specify that the remote coincidence rate is $11\%$ of the locally measured coincidence rate and that the 1.5 km free-space channel accounts for $50\%$ loss of their signal (included in the overall $11\%$). We implement a channel model which explicitly includes the propagation loss, and we implicitly include all other losses (except for detection efficiency) such as loss between the entangled pair source and the sending telescope, loss through telescope optics, and loss through an interference filter. The experimental results also show increased loss throughout the 10 hour experimental duration. These additional losses are not specified in [4]; however, we primarily attribute them to the misalignment of optics over time since no active stabilization is performed during the 10 hour experiment. As such, we implicitly include these losses with a variable insertion loss term in addition to the other implicit losses mentioned above. We use a detector efficiency of 1 since the success probability for photon pair generation and detection is determined from the local coincidence rate, which already accounts for loss due to imperfect detection. That is, the detector efficiency is already included in the definition of the success probability of photon pair generation. These settings accurately reproduce the key rates achieved in [4].

We simulate the entire experimental duration and compare our results to the published results [Fig. 2 of [4]] in Fig. 1. Our simulated raw and sifted key rates prior to 21:30 (when the first obvious additional loss features become apparent) are $2600 \pm 40$ bits/s and $1300 \pm 30$ bits/s, respectively - clearly in agreement with the initial key rates measured in the experiment.

In the experiment, the authors determine an average quantum bit error rate (QBER) of $5.4\%$. The authors state that they do not observe an increase in QBER during propagation through the atmosphere, supporting the hypothesis that polarization disturbance is negligible in most free-space channels. Therefore, the measured QBER is primarily due to the imperfect nature of the state generated by their entangled photon source. As such, we have modeled the errors resulting from the imperfect state

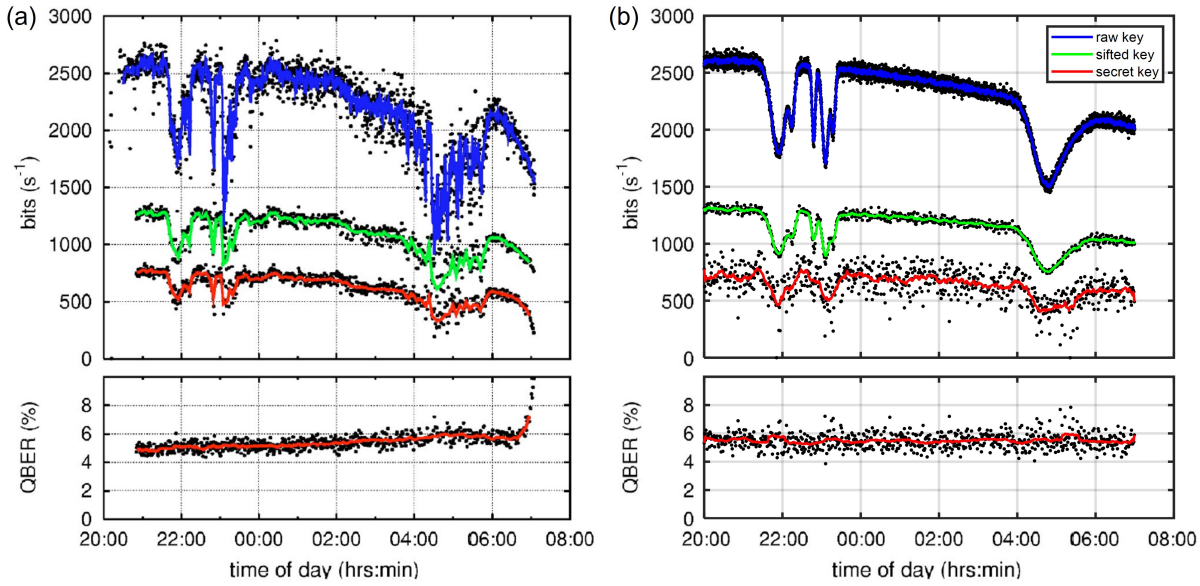


Fig. 1. (a) Results of the free-space QKD experiment performed in [4]. Figure reproduced from [4], with the permission of AIP Publishing. (b) Results of our simulation designed to reproduce the experimental results shown in (a). The key generation rates for the indicated key type are shown.

by probabilistically applying bit-flips to one photon of a perfect Bell-state, resulting in evolution of the single qubit density matrix given by $\rho \rightarrow \rho' = (1 - \frac{p}{2})\rho + \frac{p}{2}\sigma_1\rho\sigma_1$, where $\sigma_1$ is a Pauli matrix and $p$ determines the probability of a bit-flip and, therefore, the quality of the state [5]. Applying these bit-flips with a probability of $5.4\%$ successfully recreates the behavior seen in the experiment, as evident by the average QBER of $5.4 \pm 0.5\%$ determined by our simulation. See [5] for a detailed description of how common types of decoherence affecting polarization-entangled states can be modeled with probabilistic bit-flips.

In agreement with the method stated in [4], we implement a modified version of the Cascade error correction protocol [6]. We also implement a privacy amplification protocol with Toeplitz matrices and the entropy function defined in [4]:

$$e = (r/2)[(1+z)\log_2(1+z) + (1-z)/\log_2(1-z)], \tag{1}$$

where $z = \sqrt{\eta(1-\eta)}$, $\eta$ is the QBER, and $r$ is the raw key length. See [2] for details about how error correction and privacy amplification are implemented in our framework. After error correction and privacy amplification, we achieve a secret key rate of $700 \pm 100$ bits/s prior to 21:30. The simulated secret key rate clearly remains in agreement with the experiment over its entire duration. In the experiment, the authors note that they are left with nonidentical keys after privacy amplification $3.1\%$ of the time. This means that QKD has failed to produce a usable secret key for the users. Our simulation achieves the same result, with nonidentical keys also resulting $3.1\%$ of the time.

## III. Conclusion

We have presented an extension of our custom quantum network simulation framework, QuanTACT, to include channel models for simulating the transmission of polarization-entangled photons in free-space channels. To benchmark the performance of our simulation and its new free-space channel model and error correction and privacy amplification subroutines, we have modeled and successfully reproduced the results of a published experiment where QKD was performed with one photon of an entangled pair traversing a 1.5 km free-space link.

## References

[1] K. Azuma, S. Bäuml, T. Coopmans, D. Elkouss, and B. Li, "Tools for quantum network design," AVS Quantum Science **3**, 014101 (2021).
[2] D.L.P. Vitullo, T. Cook, D.E. Jones, L.M. Scott, A. Toth, and B.T. Kirby, "Simulating Quantum Key Distribution in Fiber-Based Quantum Networks," submitted to J. Def. Model. Simul. (2022).
[3] B. Bartlett, "A distributed simulation framework for quantum networks and channels," arXiv:1808.07047 (2018).
[4] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," Appl. Phys. Lett., **89**, 101122 (2006).
[5] D.E. Jones, B.T. Kirby, G. Riccardi, C. Antonelli, and M. Brodsky, "Exploring classical correlations in noise to recover quantum information using local filtering," New J. Phys., **22**, 073037 (2020).
[6] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol "Cascade"," IEICE Trans. Fundamentals **E83-A**, 1987 (2000).