A Model and Simulation Framework for Studying Implementation Non-Idealities in Quantum Key Distribution Systems

L.O. Mailloux, M.R. Grimaila, D.D. Hodson, R.D. Engle, C.V. McLaughlin, and G.B. Baumgartner

***POSTER ABSTRACT*—Quantum Key Distribution (QKD) is an innovative technology which exploits the laws of quantum mechanics to generate and distribute unconditionally secure shared key for use in cryptographic applications. While QKD offers the promise of unconditionally secure key distribution, real world systems are built from non-ideal components which necessitates the need to understand the impact these non-idealities have system performance and security. In this work, we present the QKD modeling framework, *qkdX*, which facilitates the efficient modeling, simulation, and analysis of QKD systems, protocols, and components. The qkdX framework allows developers to more easily study the impact of implementation non-idealities on system performance and security, examine complex interactions between physical phenomenon and system-level behaviors, assess practical design tradeoffs, and experiment with current, future, and notional QKD architectures. Two system-level models are presented to demonstrate the capability of the framework to study QKD systems.**

***Index Terms*—Quantum Key Distribution, Modeling & Simulation, System Performance, System Security**

I. Studying QKD Implementation Non-Idealities

Quantum Key Distribution (QKD) systems offer the promise to generate and distribute unconditionally secure cryptographic keys [1]. However, real world QKD systems are built from non-ideal components and processes which differ greatly from their ideal counterparts [2]. Due to the extensive resources (i.e., time, material, expertise) required to build and analyze physical systems, a more efficient means for studying these systems is warranted. Thus, our research is focused on using Model and Simulation (M&S) as an enabler to understand these complex systems and study their functional dependencies in a cost effective manner. To achieve this objective, we developed a quantum key distribution eXperimentation (*qkdX*) framework to more easily model and analyze QKD realizations [3]. In this paper, we described the qkdX and provide two examples of its usage to study limitations in polarization correction mechanisms and the decoy state protocol's ability to detect eavesdropping.

II. The QKD Modeling Framework

The primary objective of the qkdX framework is to enable the rapid and efficient modeling, simulation, and analysis of current and proposed QKD system implementations using varying levels of abstraction [3]. The qkdX framework is built upon OMNeT++, a communications modeling environment, whose flexible architecture lends itself to a wide variety of application domains [4], [5]. In order to model QKD systems, we extended OMNeT++'s module, message, and channel abstractions to represent optical components, fiber channels, laser pulses, protocols, and processes. This resulted in a "drag-and-drop" library of component and controller models, which can be used to build system-level QKD models.

Figure 1 illustrates the structure between the qkdX, OMNeT++, and various executable simulations, each focused on answering specific research question(s). While OMNeT++ natively supports the efficient modeling of communication networks and embedded controller processes through Discrete Event Simulation (DES), we have extended this capability by adding Continuous Time (CT) simulation necessary for modeling quantum optical phenomenon. Thus, the qkdX provides a hybrid DES/CT modeling paradigm to efficiently and accurately model (to the desired fidelity) a quantum communication system's behavior [6].

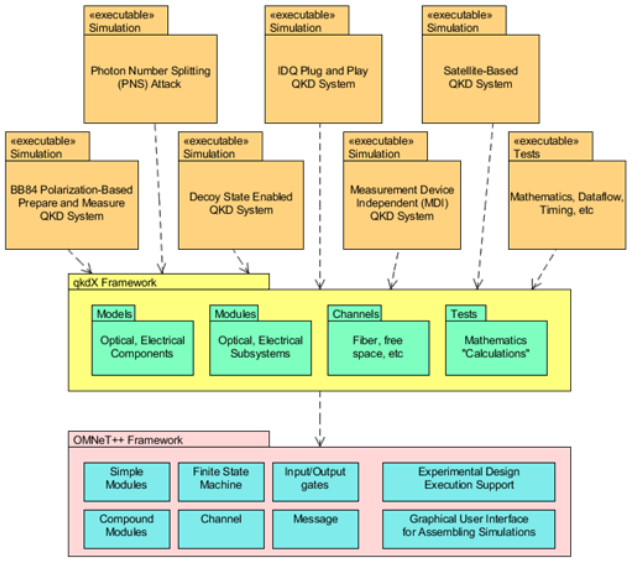


Figure 1. The qkdX Modeling Framework.

The qkdX framework provides a library of components and subsystems to facilitate the rapid construction and simulation of a variety of QKD system architectures. A partial list of the currently modeled optical, electrical, and electro-optical components, common to many QKD architectures, is provided in Table I. Additionally, commonly used subsystems and system-level controllers were developed for use across multiple models. These libraries allow users to more easily

model and analyze QKD systems in order to answer fundamental design and configuration questions. The qkdX also supports varying levels of abstraction to study the behaviors of interest without confounding results.

Table I. Modeled Components.

Fixed Optical Attenuator	Electrical-Variable Optical Attenuator	Bandpass Filter	Beamsplitter, Asymmetric
Beamsplitter, Symmetric	Beamsplitter, Polarizing	Faraday Mirror	Fiber Loop
Circulator	Classical Detector	Dichroic Mirror	Polarizing Beam Splitter
Half-wave Plate	In-line Polarizer	Optical Isolator	Laser
Optical Switch, 1x2	Polarization Controller	Polarization Maintaining (PM) Fiber	Polarization Modulator
Quarter-Wave Plate	Single Photon Detector (SPD)	Single Mode (SM) Fiber	Wave Division Multiplexer

At the core of the qkdX framework is the optical pulse model which defines how optical pulses are represented in the DES environment. Currently, we have Continuous Wave (CW), coherent optical pulses, and Fock state pulse models represented in the framework [7], [8]. The pulse design and associated parameters are shown in Figure 2, where each pulse contains basic information such as amplitude, wavelength, duration, global phase, polarization (i.e., orientation and ellipticity), and pulse shape.

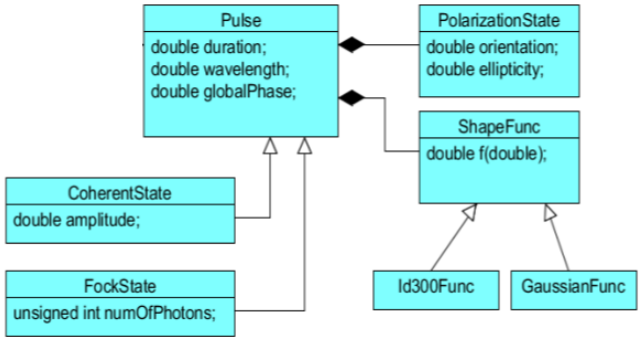


Figure 2. Optical Pulse Model Class Diagram.

III. QKD System Studies

A. Polarization Controller Model

In Figure 3, we present a model used to examine polarization correction in a one-way, prepare and measure QKD system [9]. Accurate polarization alignment is required for quantum communication and particularly polarization-based QKD, commonly used in terrestrial line-of-sight lasers and satellite-based QKD. Our model is loosely based on results from the 2010 Tokyo QKD network demonstration where environmentally induced vibrations over a 45-km aerial optical fiber caused temporary system outages [10].

The modeled QKD system is configured to transmit frames of qubits, where each timing pulse λ_T begins a frame of 1,000 individually modulated signal pulses λ_S. These frames propagate through 45 km of aerial fiber subject to simulated environmental disturbances such as temperature change, vibration, sway, and inclement weather. When left uncorrected, these disturbances can cause channel misalignment errors proportional to the drift from the reference alignment. The receiver's polarization controller is designed to correct this error but has a limited slew rate.

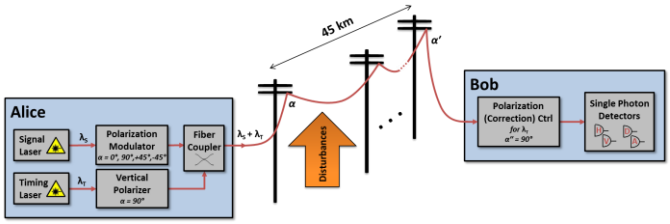


Figure 3. A Model for Studying Polarization Controller Performance [3].

Using this model, we can study the relationship between polarization error compensation and system-level performance allowing system designer to make cost-security-performance trades. Figure 4 shows the system behavior during a 30-second interval which contains a strong wind gust. The graph shows that during the first 10 seconds the polarization controller is able to correct the polarization offset, but is soon unable to compensate which causes the system Quantum Bit Error Rate (QBER) to rapidly increase. The qkdX framework enables the user to rapidly model and simulate a complete QKD system and collect relevant operational performance metrics for scenarios such as this.

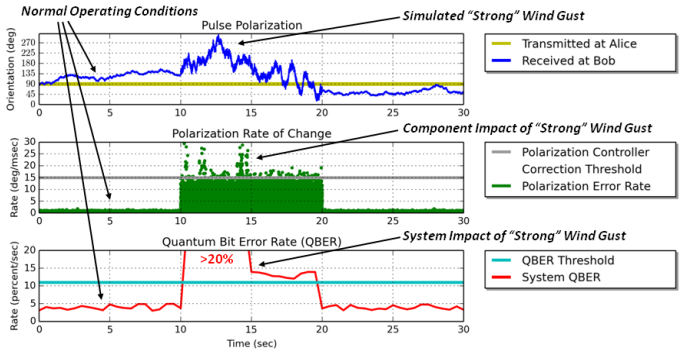


Figure 4. Polarization Controller Performance Analysis [9].

B. Decoy State Protocol Configuration

In Figure 5, we present a decoy state enabled QKD system model used to conduct performance-security studies [11]. Decoy state implementations typically consist of three transmission types: signal, decoy, and vacuum, where each type is configured with a different MPN and occurrence percentage (e.g., the signal state has an MPN of 0.6 and is transmitted 70% of the time, the decoy state has an MPN of 0.2 and is transmitted 20% of the time, and the vacuum state has an MPN near zero and is transmitted 10% of the time). The signal state facilitates higher key rates and greater operational distances due to higher MPNs, while the decoy state is used to increase the likelihood of detecting an eavesdropper on the quantum channel and the vacuum state is used to determine the dark count rate of the receiver's Single Photon Detectors (SPDs). However, the the system's ability to detect eavesdropping using the decoy state is not well understood.

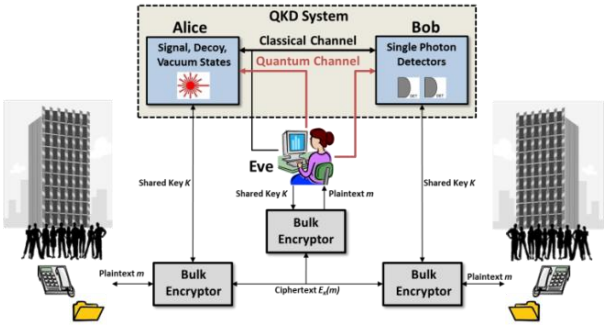
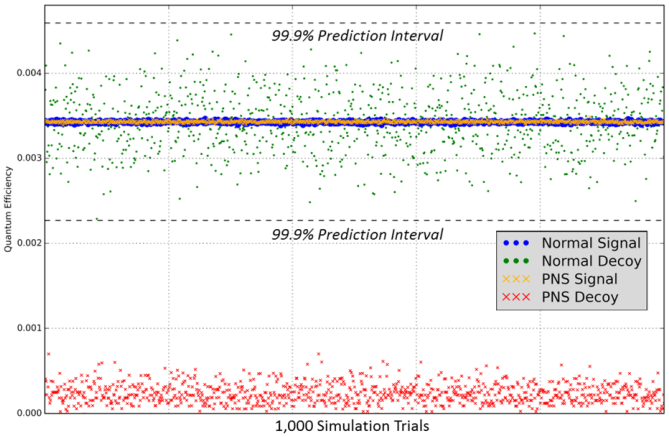


Figure 5. A Model for Studying Decoy State Enabled QKD Systems.

In Figure 6, we study the security posture of decoy state enabled QKD systems by monitoring and conducting statistical comparisons between the signal and decoy states to determine if an eavesdropper is interfering on the quantum channel, thereby preventing Eve from gaining information on Alice and Bob's shared secret key [12], [13]. Using the presented model, we also conducted experiments exploring signal and decoy state occurrence percentages and MPNs in order to optimize the decoy state protocol's performance and secure configuration for metropolitan operating regimes [14]. This type of analysis provides benefit to system designers and security specialists in determining appropriate performance parameters to meet user requirements and certification.



IV. Conclusions and Future Work

In this abstract, we described the qkdX modeling framework developed to support performance and security analysis of practically oriented QKD systems. We presented a summary of two case studies conducted using the qkdX framework that demonstrate its utility.

V. Acknowledgements

This work was supported by the Laboratory for Telecommunication Sciences [grant number 5743400-304-6448] and in part by a grant of computer time from the DoD High Performance Computing Modernization Program at the Air Force Research Laboratory, Wright-Patterson AFB, OH.

VI. Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[2] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *arXiv:0906.4547v2,* 2009.

[3] L. O. Mailloux, J. D. Morris, M. R. Grimaila, D. D. Hodson, D. Jacques, J. M. Colombi, C. V. McLaughlin and J. A. Holes, "A modeling framework for studying quantum key distribution system implementation non-idealities," *IEEE Access,* 2015.

[4] OMNeT++ Community, "OMNeT++," OMNeT++ Community, [Online]. Available: http://omnetpp.org. [Accessed 11 02 2015].

[5] J. D. Morris, D. D. Hodson, M. R. Grimaila, D. R. Jacques and G. Baumgartner, "Towards the modeling and simulation of quantum key distribution systems," *International Journal of Emerging Technology and Advanced Engineering,* vol. 4, no. 2, pp. 829-838, 2014.

[6] N. T. Sorensen and M. R. Grimaila, "Discrete Event Simulation of the Quantum Channel within a Quantum Key Distribution System," *Journal of Defense Modeling and Simulation,* Accepted Publication.

[7] B. Saleh and M. Teich, Fundamentals of Photonics, Wiley-Interscience, 2007.

[8] K. Friedrichs, Mathematical aspects of the Quantum Theory of Fields, Interscience Publishers, 1953.

[9] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Security and Privacy,* vol. 15, no. 1, pp. 30-40, 2015.

[10] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang and M. Sasaki, "Performance of Long-Distance Quantum Key Distribution Over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan Area," *Lightwave Technology, Journal of,* vol. 32, no. 1, pp. 141-151, 2014.

[11] L. O. Mailloux, R. D. Engle, M. R. Grimaila, D. D. Hodson, J. M. Colombi, and C. V. McLaughlin, "Modeling Decoy State Enabled Quantum Key Distribution Systems," *Journal of Defense Model and Simulation,* Accepted 2015.

[12] L. O. Mailloux, M. R. Grimaila, J. M. Colombi, D. D. Hodson, C. V. McLaughlin, R. D. Engle and G. Baumgartner, "Quantum key distribution: examination of decoy state enabled networks," *IEEE Communications Magazine,* Accepted 2015.

[13] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam and e. al., "High speed prototype quantum key distribution system and long term field trial," *Optics Express,* vol. 23, no. 6, pp. 7583-7592, 2015.

[14] L. O. Mailloux, M. R. Grimaila, J. M. Colombi, D. D. Hodson, C. V. McLaughlin and G. B. Baumgartner, "Performance-security characterization of decoy state enabled quantum key distribution systems," *IEEE Transactions on Dependable and Secure Computing,* Submitted 2015.