IEEE Access
The journal for rapid open access publishing

Received December 29, 2014, accepted January 22, 2015, date of publication February 5, 2015, date of current version March 3, 2015.

Digital Object Identifier 10.1109/ACCESS.2015.2399101

A Modeling Framework for Studying Quantum Key Distribution System Implementation Nonidealities

LOGAN O. MAILLOUX[1], (Member, IEEE), JEFFREY D. MORRIS[2], (Member, IEEE), MICHAEL R. GRIMAILA[1], (Senior Member, IEEE), DOUGLAS D. HODSON[1], DAVID R. JACQUES[1], JOHN M. COLOMBI[1], (Member, IEEE), COLIN V. MCLAUGHLIN[3], AND JENNIFER A. HOLES[1]

[1]Air Force Institute of Technology, Wright-Patterson AFB, OH 45433-7765, USA
[2]Army Cyber Institute, West Point, NY 10996, USA
[3]Naval Research Laboratory, Washington, DC 20375, USA

Corresponding author: M. R. Grimaila (Michael.Grimaila@afit.edu)

This work was supported by the Laboratory for Telecommunication Sciences under Grant 5743400-304-6448.

ABSTRACT Quantum key distribution (QKD) is an innovative technology that exploits the laws of quantum mechanics to generate and distribute unconditionally secure shared key for use in cryptographic applications. However, QKD is a relatively nascent technology where real-world system implementations differ significantly from their ideal theoretical representations. In this paper, we introduce a modeling framework built upon the OMNeT++ discrete event simulation framework to study the impact of implementation nonidealities on QKD system performance and security. Specifically, we demonstrate the capability to study the device imperfections and practical engineering limitations through the modeling and simulation of a polarization-based, prepare and measure BB84 QKD reference architecture. The reference architecture allows users to model and study complex interactions between physical phenomenon and system-level behaviors representative of real-world design and implementation tradeoffs. Our results demonstrate the flexibility of the framework to simulate and evaluate current, future, and notional QKD protocols and components.

INDEX TERMS Quantum key distribution, modeling & simulation, system performance, system security.

I. INTRODUCTION

Quantum Key Distribution (QKD) is the most mature application of quantum cryptography and heralded as a revolutionary technology offering the means for two parties to generate unconditionally secure shared cryptographic keying material. Employing the laws of quantum mechanics, QKD is unique in that it can detect eavesdropping during the key generation process, where unauthorized observation of quantum communication necessarily introduces discernible errors. QKD security proofs pessimistically assign all errors, regardless of their sources, to a potential eavesdropping adversary [1]. However, QKD is a nascent technology which has not yet gained wide-spread acceptance or use. As an unfamiliar cryptographic technology, there are many questions about the validity of its ''unconditional security'' claim. These concerns are justified because real-world QKD system implementations are constructed using non-ideal components which can adversely impact system security and performance. Thus, there is a clear need to further understand and study QKD system implementations to enable analysis of critical design, performance, and security tradeoff questions [2].

In this paper, we introduce a QKD experimentation modeling framework, which we call ''qkdX,'' designed to enable the rapid modeling, simulation, and evaluation of QKD systems. The framework incorporates hybrid models that perform both Discrete Event Simulation (DES) and Continuous Time (CT) calculations to efficiently and accurately model (to the desired fidelity) a quantum communications system's behavior [3], [4].

IEEE Access
The journal for rapid open access publishing

The framework is organized as a modeling package that defines both abstract and concrete QKD component models using the OMNeT++ DES framework. OMNeT++ is a well-documented, open-source, general purpose simulation framework that provides the capability to easily assemble and execute hierarchal system models collecting simulation data using a friendly graphical user interface [5]. While OMNeT++ natively supports the efficient modeling of communication networks and embedded controller processes, we have extended it by adding CT simulation necessary for modeling quantum optical phenomenon [3]–[7]. The physical component modeling library consists of optical and electro-optical devices designed in a modular and parameterized fashion to support varying levels of abstraction to meet user needs.

In this article, we demonstrate the utility of the simulation framework and component library by modeling a polarization-based, prepare and measure QKD system. The QKD system model is decomposed into individual subsystems and components. The function of each subsystem is described in detail. The primary behaviors of interest for each component can be found in the Appendix. The reference architecture can be used to study the performance and security impacts of implementation non-idealities, examine interactions between physical phenomenon and system-level functions, or explore variations in hardware, software, and protocols.

The remainder of the paper is organized as follows: In Section II, we introduce QKD technology and briefly describe the first QKD protocol, BB84. In Section III, we discuss the modeling capability developed to pursue research objectives. In Section IV we present a detailed discussion of the polarization-based prepare and measure BB84 QKD reference architecture as a means to illustrate the capabilities of the flexible simulation framework. In Section V, we provide conclusions, and discuss ongoing and future research efforts. Finally, we provide an Appendix containing the behavior of modeled optical and electro-optical components.

II. QKD BACKGROUND

The genesis of quantum information theory can be traced back to Wiesner who first developed the idea of quantum conjugate coding in the late 1960s [8]. He described two applications for quantum coding: Quantum Money – a method for the creation of fraud-proof banking notes, and Quantum Multiplexing – a method for transmitting multiple messages in such a way that reading one message destroys information contained within the other message(s).

In 1984, Bennett and Brassard extended this concept when they proposed the first QKD protocol, known as ''BB84'' and subsequently built the first QKD system [9], [10]. The BB84 protocol describes a means for two parties (commonly known as ''Alice'' and ''Bob'') to generate unconditionally secure shared secret key. In the BB84 prepare and measure, polarization-based protocol, Alice prepares quantum bits, known as ''qubits,'' by encoding single photons into one of four polarization states: horizontal, vertical, diagonal, or anti-diagonal. These states are represented as a superposition of the orthogonal horizontal and vertical basis state using Dirac notation as shown in Table 1 (note qubits can also be encoded in right and left circular polarization states):

TABLE 1. BB84 polarization states.

Bit	Basis	Polarization State	Dirac Notation Representation
0	Rectilinear	Horizontal	$\|\leftrightarrow\rangle = 1 \cdot \|\mathrm{H}\rangle + 0 \cdot \|\mathrm{V}\rangle$
1	Rectilinear	Vertical	$\|\updownarrow\rangle = 0 \cdot \|\mathrm{H}\rangle + 1 \cdot \|\mathrm{V}\rangle$
0	Diagonal	Diagonal	$\|\nearrow\rangle = \frac{1}{\sqrt{2}} \cdot \|\mathrm{H}\rangle + \frac{1}{\sqrt{2}} \cdot \|\mathrm{V}\rangle$
1	Diagonal	Anti-Diagonal	$\|\nwarrow\rangle = \frac{1}{\sqrt{2}} \cdot \|\mathrm{H}\rangle - \frac{1}{\sqrt{2}} \cdot \|\mathrm{V}\rangle$

Alice determines the polarization state of each qubit by randomly selecting one of two conjugate bases (e.g., rectilinear for the $\leftrightarrow, \updownarrow$ states or diagonal for the $\nearrow, \nwarrow$ states) and one of two randomly selected classical bit values (e.g., 0 or 1). Once Alice encodes the qubit, she transmits it via the quantum channel to Bob, where he measures the photon using a randomly selected basis (e.g., rectilinear or diagonal).

Assuming ideal transmission, if Bob measures the qubits in the same basis used by Alice, he obtains the encoded bit value with a high degree of accuracy. However, if Bob measures the qubit with the incorrect basis, a random result is obtained and all previously encoded information is lost. This phenomenon is due to the quantum-level interaction necessary for measurement to occur, where the mere act of measuring an encoded quantum state causes it to collapse into a polarization state associated with the measurement basis [11], [12].

This quantum phenomenon ensures an eavesdropper ''Eve'' necessarily introduces detectable errors when attempting to read qubits on the quantum channel, because she does not know the encoding basis used by Alice *a priori*. Thus, by closely monitoring the Quantum Bit Error Rate (QBER) on the quantum channel, Alice and Bob are able to determine if an eavesdropper is listening to the key generation process. By randomly selecting and encoding qubits in two conjugate bases ($\leftrightarrow, \updownarrow$ or $\nearrow, \nwarrow$, the BB84 protocol provides an unconditionally secure means for generating cryptographic key based on the laws of quantum physics [13], [14].

A. IMPLEMENTATION NON-IDEALITIES

However, the BB84 protocol assumes several idealities, which are not valid when building real-world systems, including [1], [15]:

1) On-demand single photon sources in Alice
2) Perfect single photon detection in Bob

3) A lossless quantum channel between Alice and Bob
4) Perfect basis alignment between Alice and Bob

The impact of these implementation non-idealities on QKD performance and security is not entirely understood for system manufactures, users, or certification authorities. For example, reliable on-demand single photon sources are not currently practical, resulting in the use of highly-attenuated laser sources which introduce multiphoton vulnerabilities into the secret key exchange [14]. Commercially available QKD photon detectors have low detection efficiencies and optical fibers have well understood losses, contributing to significant losses which allow for eavesdropping and qubit interference, and severely limit link distances. Basis alignment is limited by the stability of the quantum channel and accuracy of compensation mechanisms, potentially causing increased QBERs allowing adversaries to operate within operational tolerances without detection.

B. QKD MODELING AND SIMULATION EFFORTS

While many researchers perform analytical analysis as part of their overall research activities, almost no discussion has occurred with respect to modeling real-world QKD systems. Previous QKD simulation efforts have primarily focused on modeling abstract protocols [16]–[18], and while a limited number of optical components have been incorporated in [19]–[21], there is no indication of the details necessary to implement a full system-level model (e.g., commercially available hardware or controller software). Furthermore, little consideration of a purposefully designed modular framework for QKD research has been accomplished [22]. Of the various models and tools surveyed, perhaps the most notable is an intuitive, web-based tool for exploring the basics of QKD [23]. At this time, there are no published works or public discussions strongly focused on studying real-world system implementations using a modeling framework.

An efficient means for understanding and studying QKD implementation non-idealities and similar practical engineering limitations is needed. Furthermore, an effective tool for formally characterizing and validating complex QKD behaviors and their impact on system performance and security is warranted before these systems can be widely accepted for use in strict security environments. In the next section, we provide a discussion of the qkdX modeling framework requirements, design, implementation, and its component library.

III. THE QKD MODELING FRAMEWORK

The primary objective of qkdX is to enable efficient modeling and analysis of current and proposed QKD system implementations using varying levels of model abstraction. More specifically, the modeling framework is intended to facilitate additional understanding of QKD performance-security trades with respect to relationships between quantum phenomenon (e.g., pulse propagation, temperature changes, and physical disturbances) and system-level interactions (e.g., hardware designs, software implementations, and protocols).

A. REQUIREMENTS

Five main requirements were identified in the development of the QKD modeling framework: Accuracy, Flexibility, Usability, Extensible, and Total Cost of Ownership [24]. A brief description of each is presented to provide the reader context for the framework.

1) ACCURACY

These requirements included the capability to accurately model (to the degree required to answer the research questions) the quantum properties of light, optical component behaviors, and QKD protocols. In this way, the framework supports tailorable levels of detail to satisfy specific user requirements. For example, in a simulation study we often need to increase the fidelity of components with behaviors of interest (i.e., focused fidelity), while simultaneously reducing the fidelity of non-critical components (i.e., selective abstraction). This is done to avoid unnecessarily complex models and prevent confounded results. This approach also has the potential benefit of reducing runtimes, as only essential behaviors are simulated.

2) FLEXIBILITY

A wide degree of flexibility is required to allow users to more efficiently (i.e., without significant re-programming) model and analyze variations in QKD system hardware configurations, software processes, and communication protocols. Given the diversity of implementation details and possible purposes for a QKD simulation study, the framework concept must support building models and conducting simulations for a variety of research purposes. For example, the framework should support performance analysis, security assessments, return on investment decisions, and design tradeoffs. The framework must also provide enough flexibility to model and evaluate notional and foreseen QKD components and processes. From a software engineering perspective, this implies the development of a common reusable simulation capability (i.e., framework).

3) USABILITY

The framework facilitates user interactions to build and study user-specified QKD models. As designed, the framework supports different types of users (e.g., analysts, developers, and subject matter experts); particularly, the framework is designed to accommodate analysts with a ''user-friendly,'' ''drag-and-drop'' graphical interface for those who are not computer programmers. This approach exposes model functionality without resorting to software level programming concerns. Engineers, developers, or analysts can ''lift the hood'' to investigate and understand the implementation details, if so desired.

4) EXTENSIBLE

These requirements promote a reusable, modifiable and scalable framework design. Furthermore, they support the

maintainability of code through intentional reuse and improvement, along with testing of purposefully modeled behaviors. The simulation capability should support multiple levels of resolution (i.e., abstraction) and provide standardized ''friendly'' interfaces for users. The framework must support integration of customer libraries and parameterization of components. This means extending existing capabilities and modeling new optical components according to their specifications.

5) TOTAL COST OF OWNERSHIP

A robust simulation capability facilitates model changes efficiently without requiring the user to have significant programming expertise (i.e., human capital). Additionally, the framework does not require expensive support infrastructure (i.e., software or hardware) in order to make costs as low as possible.

B. DESIGN

The qkdX is built upon the open source OMNeT++, an extensible and modular simulation library and framework, providing the fundamental infrastructure to develop individual components, build complex systems, and to execute efficient simulations [5]. While OMNeT++ has primarily been used to study conventional communication networks, its generic and flexible architecture lends itself to other areas such as complex communication systems, queuing networks, and hardware architectures. A detailed justification for the choice of OMNeT++ as our underlyng framework is provided in [24].

OMNeT++ defines the concept of a simple module, written in C++, that interacts with other modules through events (i.e., event processing) [5]. Simple modules contain all executable behavior, while compound modules are constructed by interconnecting one or more simple and/or compound modules. The concept of simple and compound modules is similar to the Discrete Event System Specification (DEVS) atomic and coupled models discussed in [7]. This modular approach enables the user to rapidly create, retrieve, and store system representations composed of multiple functional blocks connected in a hierarchical manner. After composable modules have been defined, OMNeT++ provides the infrastructure and support tools to efficiently execute simulation models and analyze results.

Figure 1 depicts the relationship of the QKD modeling framework (i.e., qkdX) to OMNeT++. The tiered design provides a foundation to support code reuse and leverage community-supported open source tools to build ''ad hoc'' simulation products. Top-level executables, shown in orange, are built by analysts or engineers to meet fit-for-purpose research requirements. Each of these products corresponds to valid QKD representations (e.g., polarization or phase-based system architectures); proposed and notional QKD systems can also be modeled in this manner. Additionally, independent test products can be integrated into the framework concept to enable standardized regression testing of QKD systems, subsystems, and various components.

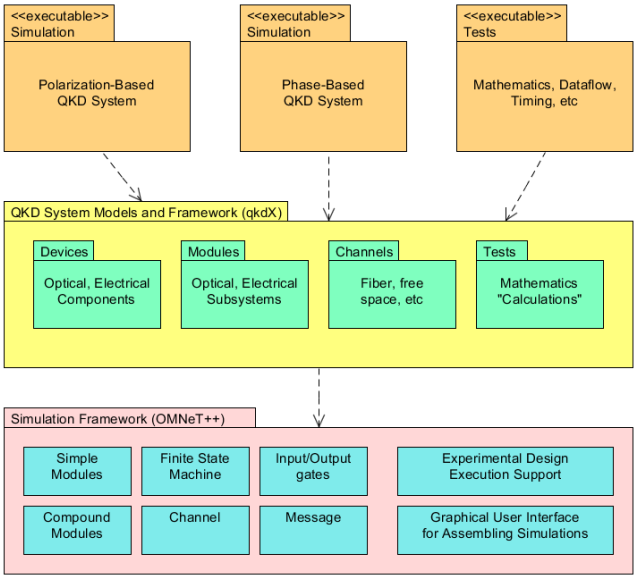


FIGURE 1. qkdX Framework Ecosystem.

The qkdX framework, shown in yellow, is designed to enable the accurate (i.e., valid for a specific purpose) and efficient (i.e., without significant rework) modeling of QKD systems. It defines reusable models (e.g., optical, electro-optical, electrical components), modules (i.e., subsystems or collections of components with supporting control logic), and communication channels (e.g., fiber or free space) common to many QKD architectures. Primarily, the models capture behaviors of interest, while the modules are used to handle timing and state in the DES. The channels account for both modeled physical behaviors and timing. The modeled QKD components and channels are captured in a component library (see Appendix), where they can be reused across differing QKD system representations. For example, a user can build a polarization-based QKD system from the library of components. The qkdX framework supports independent testing of components through comparisons to mathematical ''truth calculations'' and regression testing as individual components are modified.

The qkdX framework employs a hybrid discrete-continuous simulation approach to accurately capture quantum effects, yet provide the desired modularity. Traditionally, DES is used to model processes moving from event to event fast-forwarding over ''dead'' periods of time, while CT simulation is used for detailed temporal analysis. However, the qkdX hybrid approach takes advantage of computational resources to schedule propagation of optical pulses through numerous components using abstract propagation transfer functions, while only performing CT computations when necessary. In the framework, for example, the propagation of a single optical pulse over a length of fiber is a discrete event after which a transfer function is applied representing how the pulse changed during propagation. In contrast,

a continuous time representation of the optical pulse propagation is only used when required for complex interactions such as interference calculations. In this way, qkdX provides an efficient simulation capability for studying system-level effects while accurately (to the degree necessary) modeling CT optical pulses. Tradeoffs associated with modeling a CT optical pulse in a DES framework are more fully discussed in [4].

The framework is built upon the Modeling and Simulation (M&S) environment provided by OMNeT++, shown in red. Specifically, the qkdX leverages the capabilities of OMNeT++ to uniquely support the efficient M&S of QKD optical devices, process-oriented controllers, and quantum-level optical pulses, including [5]:

1) GRAPHICAL USER INTERFACE

OMNeT++ employs an Integrated Development Environment (IDE) which allows QKD systems to be modeled in a drag-and-drop fashion by selecting from inventoried electrical, optical, and electro-optical devices. The IDE also allows developers and users to build QKD systems, modify behaviors, and add new components as desired.

2) DEFINED MESSAGE TYPES

In DES, operations are represented as a chronological sequence of events. Each event occurs at an instant in time and marks a change of state in the simulated system. OMNeT++ controls these events through messages transmitted between components as discrete events. Passing standardized messages between devices supports modularity, promotes ease-of-use, and increases understandability of the framework. The framework employs three message types:

a: OPTICAL MESSAGES

Optical messages are passed between connected optical components. Optical messages contain parameters used to model the optical signal, perform calculations, and process the optical message as it transitions through a modeled system. More details on the optical message pulse model and its constituent elements can be found in [4].

b: ELECTRICAL MESSAGES

Electrical messages represent analog or digital signals passed between connected electrical components. Electrical messages are used only in cases where their explicit representation is required to the simulation study. Otherwise, a behavioral representation is used for simulation efficiency.

c: ENVIRONMENTAL MESSAGES

Environmental messages are simultaneously passed between numerous modeled devices within a localized area. These messages are configured to model environmental temperature changes. Temperature is an important operational consideration as many optical devices and sensors are sensitive to temperature fluctuations.

3) SUPPORTS MULTIPLE PROGRAMMING PARADIGMS

OMNeT++ is structured around the C++ programming language which inherently supports object oriented design principles. This characteristic allows for increasing levels of resolution to be modeled as necessary (e.g., a simple and a complex version of an optical component). OMNeT++, and C++, also supports a multi-paradigm programming design which allows behaviors to be more easily modeled without being tied to specific classes. Thus, interactions (or transformations) between optical pulses and optical components can be more easily modeled at a level of detail suitable for the desired purpose(s). These implementation features allow modelers to implement flexible QKD components, protocols, and architectures.

4) PARAMETERIZATION

OMNeT++ provides dynamic parameterization through Network Description (NED) files which allow models to be reconfigured between simulation runs without recompiling the model code. Each component in the toolbox has a number of configurable parameters that were derived from operational behaviors or characteristics. For example, a polarizing beam-splitter has seven parameters related to its primary behavior, six parameters related to state (normal, degraded, and damaged), and four parameters related to generating reflections on each of its four bidirectional optical ports.

C. COMPONENT LIBRARY

While the framework was designed with considerations to support various QKD architectures, we initially selected to model an optical fiber, polarization-based prepare and measure BB84 QKD system architecture. We selected this architecture because it is a popular implementation choice and demonstrates the functionality of the first QKD protocol. Additionally, it utilizes commercially available technologies such as telecom wavelength lasers, modulation encoders, standardized components, and established infrastructures.

A list of the currently modeled optical, electrical, and electro-optical components common to QKD architectures is provided in Table 2. Descriptions of these components are provided in the Appendix. A list of modeled component, subsystem, and system-level controllers is provided in Table 3. A detailed description and implementation details for each component are provided in Section IV.

TABLE 2. Modeled components.

Attenuator, Fixed Optical	Attenuator, Electrical-Variable Optical	Bandpass Filter	Beamsplitter
Beamsplitter, Polarizing	Circulator	Classical Detector	Dichroic Mirror
Half-wave Plate	In-line Polarizer	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

TABLE 3. Modeled subsystem controllers.

Alice CPU	Alice Public Channel	Alice Quantum Module
Bob CPU	Bob Public Channel	Bob Quantum Module
Classical Pulse Generator	Classical to Quantum Attenuator	Decoy State Generator
Input Stage	Optical Security Layer	Optical Pulse Power Monitor
Polarization Adjustment	Polarization Detection	Polarization Modulator
Timing Analyzer	Timing Pulse Generator	

D. A FLEXIBLE FRAMEWORK

The qkdX design concept enables efficient modeling of QKD systems with the desired flexibility to build models for analysis purposes and accommodate unknown future requirements. It was designed to be extendable to support multiple QKD protocols (e.g., BB84, SARG04, E91, etc. [13]), alternate forms of encoding (i.e., polarization, phase, and entanglement), different quantum communication channels (e.g., buried fiber, aerial fiber, terrestrial free space, satellite free space, and multiplexed transmissions), and various system architectures.

This capability allows users (e.g., engineers or analysts) to more quickly model and study QKD systems than modifying hardware and/or software. The qkdX framework provides the following benefits:

1) Increase understanding of the design and implementation trade space for realized QKD systems.
2) Identify interactions between physical (quantum phenomenon, temperature, and disturbances) and system-level interactions (hardware designs, software implementations, and protocols).
3) Determine the impact of non-idealities and practical engineering limitations in QKD architectures.
4) Model and analyze competing QKD implementations (i.e., variations in hardware, software, or protocols).
5) Propose and assess new QKD implementations and protocols.
6) Study the security implications of protocol modifications and system architectures.
7) Model and explore terrestrial and space-based QKD free-space systems.
8) Maximize research investments and developmental efforts to improve implementations (e.g., should one invest research capital in on-demand single-photon sources or improved single photon detectors?).

IV. THE QKD REFERENCE ARCHITECTURE

In this section, we present the modeling of a polarization-based, prepare and measure BB84 terrestrial fiber QKD system architecture to demonstrate the utility of the qkdX framework. The modeled QKD system architecture also serves as a baseline for understanding and conducting performance-based simulation studies. It was developed from available product specifications, reference literature, and published QKD system designs including [25]–[29] as well as the references presented in the Appendix.

The focus of our modeled reference architecture is a physical representation of the quantum communications path, which is discussed in increasing levels of detail. System and subsystem controllers are modeled using abstract conditional logic written in C++ with "electronic control signals" and "device state" to represent typical system behaviors. The QKD system model is decomposed into a modular hierarchy to promote re-usability through low coupling and high cohesion, as well as understandability and maintainability.

A. ALICE AND BOB DECOMPOSITION

Figure 2 is a high level decomposition of our QKD reference architecture, where Alice and Bob are configured to generate and distribute the shared secret key K. Conventionally, Alice is said to "prepare" photons with candidate secret key bits, while Bob "measures" them (see Table 1). Alice and Bob each include a Central Processing Unit (CPU) to control internal processes, a network interface to facilitate communications over the classical channel (i.e., an authenticated networked communication channel), and a quantum module to facilitate single photon communication over the quantum channel (i.e., an otherwise unused "dark" fiber).

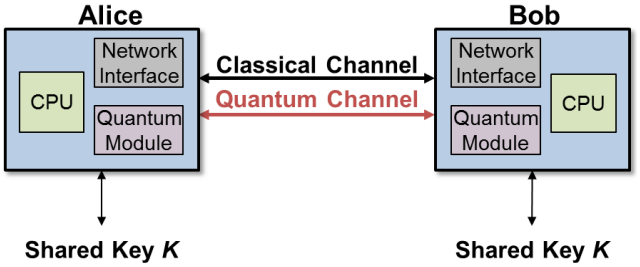


FIGURE 2. QKD System 1st-level Decomposition.

Alice and Bob generate the shared secret key K by following a series of phases according to the BB84 protocol: authentication, quantum exchange, sifting, error estimation, error reconciliation, entropy estimation, privacy amplification, and final key generation [2], [13]. In this model, Alice is responsible for controlling the QKD protocol where Alice and Bob execute the QKD protocol and coordinate their system operations by communicating over the classical channel. These control signals are modeled in an abstract way, facilitating each phase of the QKD protocol.

The quantum channel is modeled with scattering-induced fiber-based loss, typically characterized at 0.20 dB loss per km at a wavelength of 1550 nm [13], and includes details to account for propagation specific phenomenon such as thermal expansion, temperature-dependent changes in index of refraction, and chromatic dispersion. The modeled channel is also capable of simulating the effects of random physical disturbances such as polarization changes due to bends in the fiber, vibration, or other instabilities. These behaviors are intended to represent practical QKD implementations utilizing existing optical infrastructure [2].

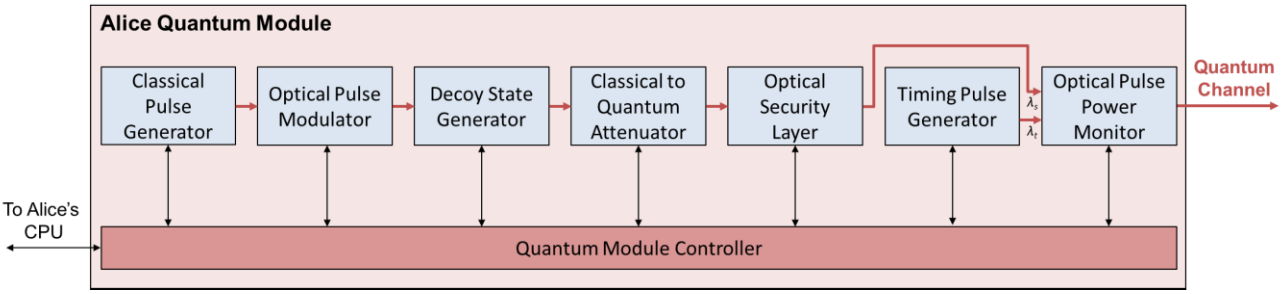


FIGURE 3. Alice Quantum Module Decomposition.

In this model, we are most concerned with the architectural subsystems, components, and behaviors required for quantum communication (i.e., Alice's quantum module, the quantum channel, and Bob's quantum module). The remainder of this section is dedicated to describing these devices and their function(s) in QKD. Details for each modeled component are provided in the Appendix and are not addressed in this section to avoid redundancy.

B. ALICE QUANTUM MODULE DECOMPOSITION

Alice's quantum module is designed to encode qubits through seven configurable subsystems and a controller as illustrated in Figure 3. Ideally, she would generate perfectly encoded qubits using an on-demand single photon source; however, such devices are not currently available. Instead, she uses the Classical Pulse Generator (CPG) to produce ''strong'' optical pulses (i.e., pulses with millions of photons), which are attenuated down to ''weak coherent pulses'' (i.e., pulses with a Mean Photon Number (MPN) of less than 1 photon per pulse). These sub-quantum energy levels (i.e., a MPN ~ 0.1) are necessary to limit the number of multiphoton pulses produced by Alice and attempt to achieve the theoretical security requirements of QKD [14].

The Optical Pulse Modulator (OPM) polarization encodes the classical pulses in one of four polarization states (horizontal, vertical, diagonal, or anti-diagonal) according to the BB84 protocol [9]. The Decoy State Generator (DSG) further encodes these pulses into three states: signal, decoy, and vacuum [30] to mitigate Photon Number Splitting (PNS) attacks on the quantum channel. Explicitly, the signal state is used to generate shared secret key, the decoy state is used to detect eavesdropping through differential analysis between the signal and decoy states, and the vacuum state is used to determine the error rate due to stray ''dark count'' detections [31]. Additional details can be found in [6].

The Classical to Quantum (CTQ) attenuator is configured to reduce the classical strength pulses down to quantum levels. Positioning the DSG before the CTQ allows Alice to more easily measure and verify the decoy states before attenuating the pulses down to quantum levels in the CTQ module. Placing the CTQ attenuator first would require having to measure the relative pulse amplitude levels at the single-photon level, which is much more difficult and expensive.

The Optical Security Layer (OSL) is configured to detect optical probing attacks (i.e., an adversary attempting to shine light into Alice to obtain raw key information) in support of cryptanalysis efforts. The Timing Pulse Generator (TPG) creates timing pulses for quantum communication synchronization and basis measurement reference frame control. These reference pulses are critical to QKD operation, and particularly for polarization-based decoding at Bob. The timing pulse and the signal pulses are multiplexed together in the Optical Pulse Power Monitor (OPPM). The OPPM is configured to monitor the output power of the signal pulses and provide feedback to Alice's quantum module controller.

Each of the subsystems, and their individual optical components, are connected by optical fiber, and specifically Polarization Maintaining (PM) or Single Mode (SM) fiber. In the reference model, PM and SM fibers are represented by a circle labeled with a ''PM'' or ''SM'', respectively. PM fiber is designed to maintain orthogonal polarization states as they propagate through the fiber (though one state will have a slightly slower propagation speed due to necessary retardation to separate the states). SM fiber is designed for long distance propagation with a guiding core and an outer cladding confining light to a single mode, which results in low loss. Its low-loss, and significantly cheaper price than PM fiber, make it suitable for long-haul telecommunication links and general usage within QKD systems. Throughout the reference architecture, PM fiber is primarily used within the CPG to ensure a known polarization state to accurately encode each pulse at the polarization modulator. The majority of optical components use SM fiber. Additionally, the fiber model is also configured to drop pulses which fall below a user defined energy threshold. This option allows users to turn off low-energy pulse reflections that would otherwise propagate endlessly until the simulation trial completes and needlessly consume simulation resources.

1) ALICE CLASSICAL PULSE GENERATOR SUBSYSTEM

Figure 4 provides a decomposition of Alice's Classical Pulse Generator (CPG) subsystem, comprising a controller, laser source, isolator, in-line polarizer, a bandpass filter, a beamsplitter, and a classical detector. The CPG is designed to generate strong coherent pulses and condition them into a

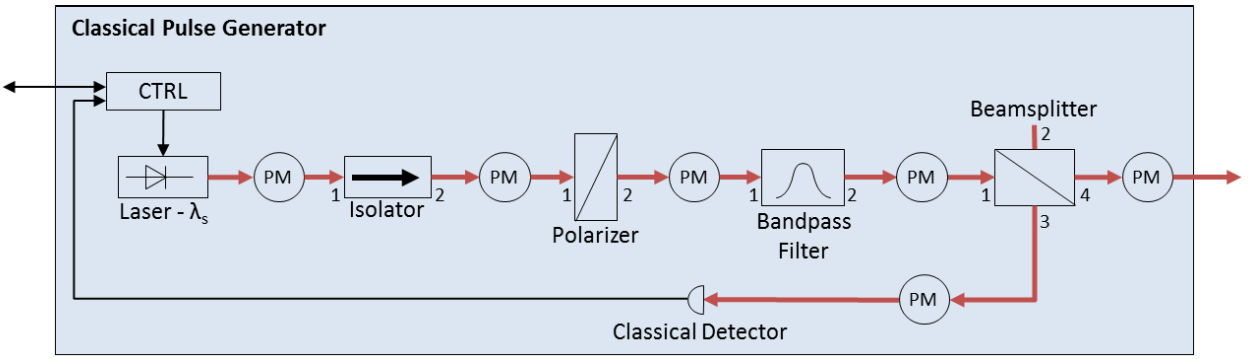


FIGURE 4. Classical Pulse Generator (CPG) Subsystem Decomposition.

known polarization and wavelength. The CPG controller is responsible for triggering the laser to fire with typical pulse rates of 2-5 Mhz. Each laser pulse is generated at the wavelength $\lambda_s = 1550$ nm with a defined shape, amplitude, duration, central frequency, global phase, polarization state (orientation and ellipticity), and pulse energy. Variations in the laser pulse include pulse shape and energy. Additional laser source specifications such as jitter, oscillator relaxation, and frequency chirping can be modeled as needed by the user to meet simulation study requirements. Details regarding the laser pulse can be found in the Appendix and [4].

QKD systems often utilize 1550 nm wavelength light as it provides low-loss propagation within conventional telecom wavelength ranges. Furthermore, commercially available optical components are available at this wavelength. The isolator passes light in one direction, while severely attenuating light attempting to traverse in the opposite direction (e.g., reflections or light from external sources). The placement of the isolator allows a minimum amount of light to enter the laser cavity, preventing perturbations which can result in improper output waveforms. The in-line polarizer and bandpass filter are configured to "clean" the laser output. The polarizer is configured to orient the laser light in a known polarization state and the filter only passes optical light in a narrow band around the desired signal wavelength, λ_s. This ensures that only the appropriate signal polarization and wavelength leaves the subsystem. Since the bandpass filter is a bidirectional device, it also serves to prevent out-of-band sources of light from entering the laser. The conditioned optical pulses enter the beamsplitter, which divides the laser pulse into two paths, transmitting a portion of the light to the next quantum module and a portion to the classical detector. The beamsplitter may be configured as a 75/25 or 90/10 beamsplitter to ensure adequate power for the classical detector. The classical detector model generates an electrical signal proportional to the power contained in the optical pulse, providing feedback to the CPG controller. This feedback is used to measure the power of the laser and provides a means for monitoring the pulse energy leaving the CPG subsystem.

While the CPG is designed with a single classical laser source, the modular nature of the CPG allows alternate laser configurations to be modeled. For example, if so desired a researcher could multiplex multiple laser sources at differing wavelengths to increase secret key rates as demonstrated in [32] or develop a model to study exploratory on-demand photon sources such as quantum dots or color center diamonds [33].

2) ALICE OPTICAL PULSE MODULATOR SUBSYSTEM

The Optical Pulse Modulator (OPM) subsystem is shown in Figure 5, comprising a controller and polarization encoder. According to the BB84 protocol, the controller randomly selects a bit value (0 or 1) and basis (rectilinear or diagonal) to encode each qubit. In the qkdX simulation framework, the random number generators used could be conventional (e.g., the Mersenne Twister [34]) or dedicated quantum random number generators [35]. As illustrated in Table 1, the orientation of each optical pulse is set to one of the polarization states ↔, ↕, ⤡, or ⤢ by the polarization encoder according to the randomly selected bit value and basis.

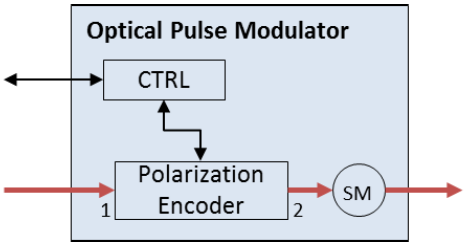


FIGURE 5. Optical Pulse Modulator (OPM) Subsystem Decomposition.

The modeled polarization encoder is based on similar commercial products, generically representing any such device configured to electronically set the polarization of optical pulses from an unknown polarization state. The modular nature of the OPM subsystem allows alternative encoding schemes such as right ↻ and left ↺ circular encoding or phase-based modulation to be more easily incorporated.

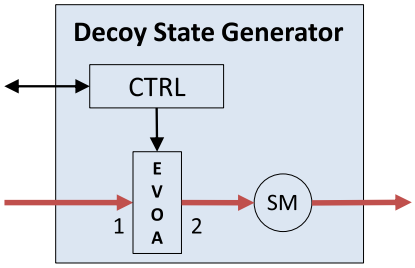


FIGURE 6. Decoy State Generator (DSG) Decomposition.

3) ALICE DECOY STATE GENERATOR SUBSYSTEM

Decoy states are commonly implemented in realized QKD systems, as they increase the secure key generation rate and operational distance with minimal additional requirements. Figure 6 presents the Decoy State Generator (DSG), comprising a controller and an Electronic Variable Optical Attenuator (EVOA) configured to vary the power of the optical pulses to create signal, decoy, and vacuum states. Each state is configured with a different MPN (e.g., 0.65, 0.10, and 0.0^{+}) and randomly transmitted according to an occurrence percentage (e.g., 70%, 20%, and 10%). Note that these occurrence percentages are another variable which can be altered by the user.

The controller uses a random number generator to randomly select the desired pulse type (signal, decoy, or vacuum) according to its occurrence percentage and adjusts the EVOA's attenuation according to the desired MPN. The EVOA has a configurable rate of change, which must accommodate Alice's desired pulse rate (e.g., 2-5 MHz). The modeled EVOA also has a configurable step size which limits the device's accuracy. For example, EVOAs are commonly implemented using an electric motor connected to an opaque slab in the optical path. This type of device is limited by the motor's precision and rate of change, which inherently limits the system's throughput.

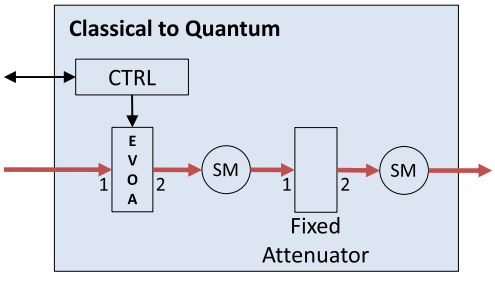


FIGURE 7. Classical to Quantum (CTQ) Subsystem Decomposition.

4) ALICE CLASSICAL TO QUANTUM SUBSYSTEM

Figure 7 depicts the Classical to Quantum (CTQ) subsystem containing a fixed attenuator, an EVOA, and a controller. Since single photon generators are not readily available, practical QKD implementations attenuate classical optical pulses through a fixed attenuator with significant loss (e.g., >40 dB or 99.99% loss) and an EVOA capable of applying additional attenuation (e.g., losses from 0-40 dB) to meet the desired quantum level. Fixed attenuators may be implemented as either doped fibers or misaligned splices designed to partially block optical light. The CTQ EVOA applies attenuation in response to the controller, and specifically feedback from the OPPM module which attempts to precisely calibrate Alice's output MPN.

The CTQ and DSG represent an excellent example of the parameterized capability built into the qkdX framework. While the DSG and CTQ have similar modeled behaviors, they differ significantly in their operational requirements. The DSG EVOA is required to change quickly to generate signal, decoy, and vacuum states, while the CTQ EVOA only adjusts in response to occasional calibration activities. The framework facilitates individual instantiations of the modeled components with unique performance parameters to support specific instances of each component.

5) ALICE OPTICAL SECURITY LAYER SUBSYSTEM

The Optical Security Layer (OSL) is designed to detect optical probing and provide protection against adversaries attempting to discern information about her internal construction (or gain information on encoded qubits). The OSL as shown in Figure 8 comprises an isolator, circulator, and bandpass filter configured to allow light to propagate in the forward direction, while severely attenuating light propagating in the reverse direction. Additionally, the circulator, classical detector, and controller are configured to detect classical light shone into the OSL (i.e., optical probing).

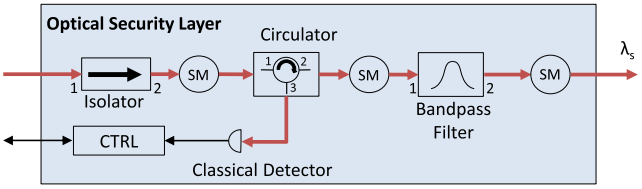


FIGURE 8. Optical Security Layer (OSL) Decomposition.

In the intended forward direction of travel, optical pulses travel through the isolator, enter the circulator which routes light in the clockwise direction from port 1 to 2, and passes through the bandpass filter. In the reverse direction (against the depicted arrows), light entering the OSL from the intended output is filtered by the bandpass filter, blocking light other than the signal wavelength λ_s. Light passing through the filter is routed by the circulator from port 2 to port 3 and towards the classical detector. In this configuration, the detector functions as an 'alert' for Alice. Any light bleeding through the circulator is further attenuated by the isolator. The isolator severely attenuates light travelling in the reverse direction, towards the laser, effectively stopping almost all light in the unintended direction of travel from reaching Alice's sensitive components. For example, light propagating in the forward direction may incur 2.3 dB

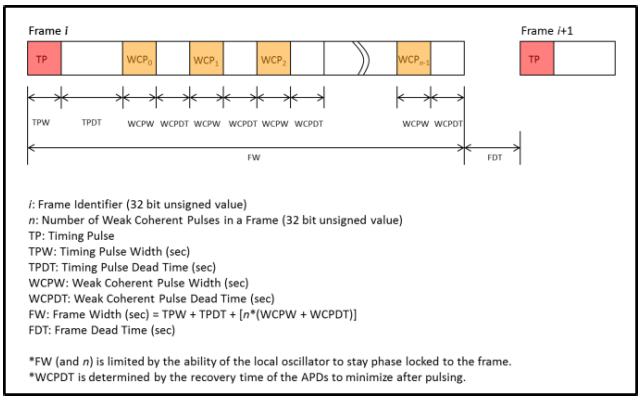


FIGURE 9. Synchronization Data Frame.

loss, while light propagating in the reverse direction incurs 80.0 dB of attenuation.

6) ALICE TIMING PULSE GENERATOR SUBSYSTEM

Optical pulses generated by Alice need to be synchronized with Bob; he needs to know with a high degree of accuracy when to expect optical pulses to arrive and their polarization state. Commonly, this is achieved through frames of pulses beginning with "bright" timing pulses as demonstrated in Figure 9. In our reference model, Alice starts each data frame of qubits with a bright timing pulse (i.e., TP) followed by 1,024 weak signal pulses (i.e., WCPs). The number of frames sent and the WCPs per frame are adjustable for each simulation trial. Bob uses the bright pulse both as a timing and polarization reference to correctly synchronize his detection of single photons. This can be accomplished though fundamental calibration activities such as verifying the expected arrival times and polarization states of the timing pulses and each of the four signal pulses ↔, ↕, ↘, and ↗. Further details are provided with respect to Bob's quantum module decomposition.

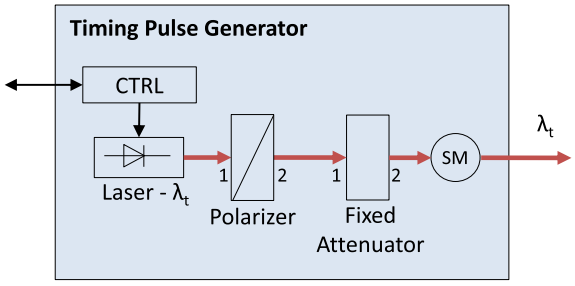


FIGURE 10. Timing Pulse Generator (TPG) Decomposition.

Figure 10 depicts the Timing Pulse Generator (TPG) subsystem with a controller, a laser configured to generate pulses at the timing pulse wavelength $\lambda_t = 1540$ nm, an inline polarizer, and a fixed attenuator. The module is similar to the CPG although this laser produces pulses at the timing wavelength, which are slightly different than signal wavelength. The two wavelengths $\lambda_s = 1550$ nm and $\lambda_t = 1540$ nm have to be close enough to pass through any bandpass filters, but far enough apart so they can be separated in Bob. The polarizer conditions the laser light into a known polarization, while the fixed attenuator is used to slightly reduce the classical power level. Note the timing pulse remains at a classical energy level, unlike the weak signal pulses. This is necessary for synchronization and polarization tracking at Bob.

7) ALICE OPTICAL PULSE POWER MONITOR SUBSYSTEM

The Optical Pulse Power Monitor (OPPM) is configured to verify Alice's output onto the quantum channel according to the desired MPN. Figure 11 depicts the OPPM including a dichroic mirror, an optical switch, a Single Photon Detector (SPD), and a controller. The signal and timing pulses λ_s and λ_t are combined together by the dichroic mirror (i.e., Wavelength-Division Multiplexer (WDM) configured to combine two optical paths) into a single fiber. The optical switch is used to route light between input port 1 and either port 3 to the quantum channel or port 2 to the SPD. The controller will direct the switch depending on the system's status. During normal operation, the switch is configured to send timing and signal pulses over the quantum channel.

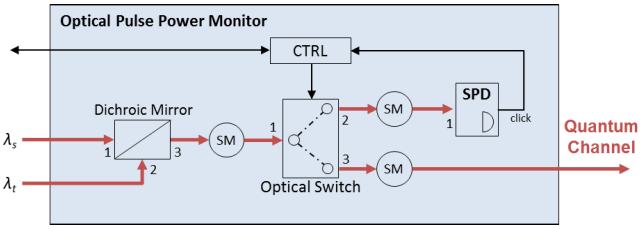


FIGURE 11. Optical Pulse Power Monitor (OPPM) Decomposition.

If the system is in a calibration mode, it may send signal pulses to the SPD to fine tune the desired output MPN. The SPD is an opto-electric device configured to detect the arrival of single photons. When photons are successfully detected, the device sends a "click" to the controller, which is responsible for tracking and estimating the pulse states' MPN (signal, decoy, vacuum). This configuration allows Alice to sample outgoing optical pulses and adjust for time and temperature dependent component variations or verify decoy state protocol MPNs. By sampling the photon numbers, Alice can adjust the CTQ or DSG EVOA to output the desired MPNs.

C. BOB QUANTUM MODULE DECOMPOSITION

Bob's quantum module, shown in Figure 12, is designed to measure polarization-encoded qubits. Bob's Input Stage (IS) is configured to prevent extraneous light from entering his architecture. Thus the IS secures the system against optical probing in a manner similar to Alice's OSL. It also functions to reduce detection errors caused by undesired wavelengths of light. The Polarization Adjustment (PA) subsystem is configured to detect and align incoming pulses to the system's frame of reference based on the known polarization state of

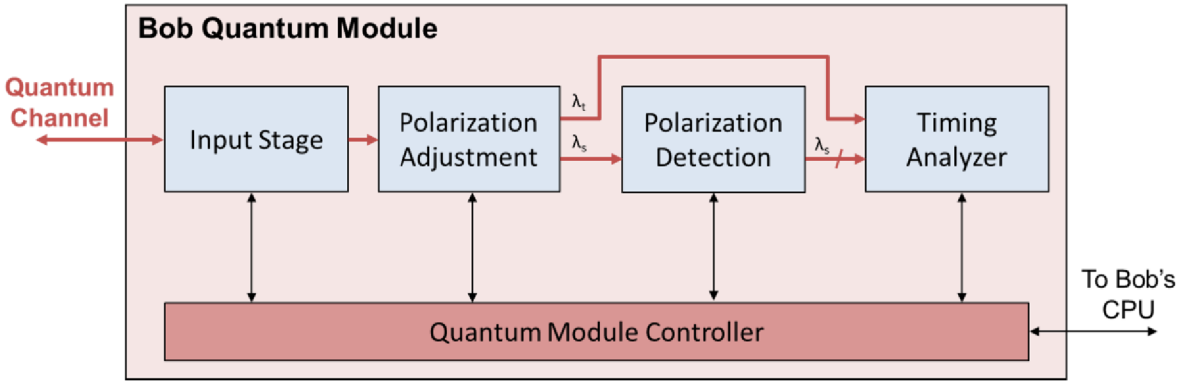


FIGURE 12. Bob quantum module decomposition.

Alice's timing pulses. For each frame of qubits (i.e., a timing pulse followed by signal pulses) received, the PA attempts to correct for "polarization drift" (i.e., random rotation of the photon's polarization state as it propagates through the quantum channel). Accurate and timely performance from the PA is necessary for correct measurement of qubits and for minimizing errors due to polarization misalignment between Alice and Bob.

The Polarization Detection (PD) subsystem is configured to separate the four polarization encoded states: $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\rangle$, and $|\nearrow\rangle$ onto separate paths. The separated polarization states are passed to the Timing Analyzer (TA) where single photons are detected. To reduce erroneous detections and maximize the detection rate, the TA is synchronized using the timing pulse. The majority of the model's complexity resides in the TA as it is configured to probabilistically detect photons and calculate interference between photons where necessary [3].

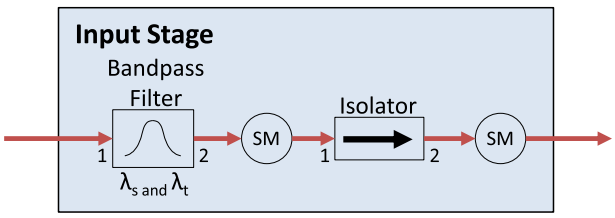


FIGURE 13. Input Stage (IS) Decomposition.

1) BOB INPUT STAGE SUBSYSTEM

The Input Stage (IS) shown in Figure 13 includes a bandpass filter and an isolator. While this device is similar to Alice's OSL, it does not contain the necessary components to detect adversarial light shone into Bob. While a more complex implementation of Bob's IS can be modeled, we chose a simpler version to minimize Bob's internal loss. Bob's bandpass filter is configured to pass wavelengths of light around the timing and signal pulses ($\lambda_t = 1540$ nm and $\lambda_s = 1550$nm). Inbound light proceeding through the filter passes through the isolator in the forward direction, while light (attempting to propagate in the reverse direction (e.g., reflected light used in the analysis optical probing) is highly attenuated.

This configuration provides additional security for Bob by preventing an adversary from using light probes to gain information on his internal structure through component distinctive reflections.

2) BOB POLARIZATION ADJUSTMENT SUBSYSTEM

Figure 14 depicts the Polarization Adjustment (PA) module with a polarization controller, a dichroic mirror, and a subsystem controller. The polarization controller is configured to compensate for polarization drift (i.e., noise due to a dynamic operational environment and non-ideal components) as optical pulses propagate through the quantum channel. Correcting for polarization drift ensures Bob can measure the four signal polarization states $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\rangle, |\nearrow\rangle$ with a high degree of accuracy, thereby reducing errors.

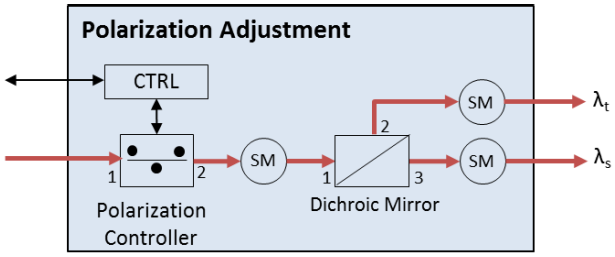


FIGURE 14. Polarization Adjustment (PA) Decomposition.

The polarization controller first determines the arriving timing pulse's polarization state using a polarimeter (i.e., a device designed to detect the polarization of classical light). Next it determines the difference between the timing pulse's measured polarization state and the known reference polarization (typically chosen by system designers and set by Alice). Finally, the device applies polarization compensation to the quantum channel to correctly adjust the polarization state of the signal pulses.

Polarization controllers often employ electro-mechanical squeezing techniques or variable fiber wave plates to manipulate the state of polarization, each of which have

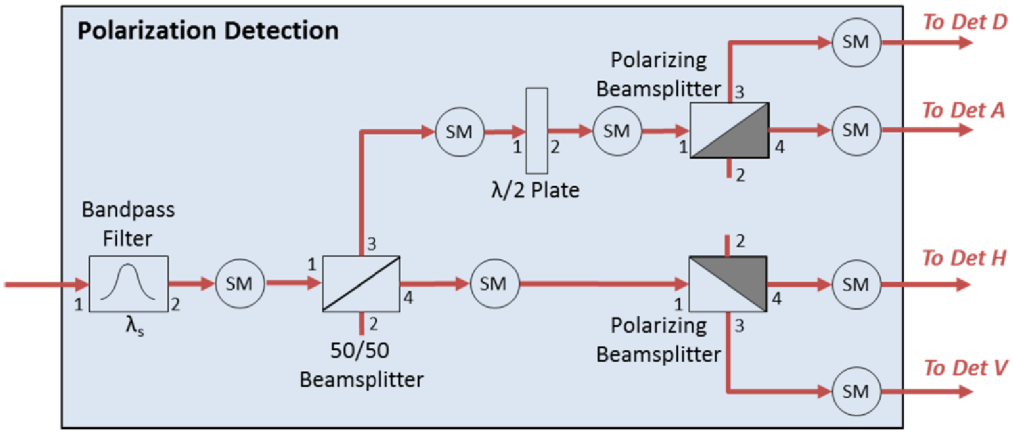


FIGURE 15. Polarization Detection Decomposition.

limited response times (see Appendix for further details and references). If the rate of change in polarization between successive frames is too great, the controller cannot fully correct for polarization drift; when left uncorrected, this drift can result in detection errors as demonstrated in [2].

The polarization-corrected signal and timing pulses are passed to the dichroic mirror which splits them onto two optical outputs (i.e., a WDM configured to transmit light of one wavelength, λ_s, and reflect light of another wavelength, λ_t). The choice of the dichroic mirror depends on the timing and signal wavelengths, which need to be close enough to one another in wavelength to pass through Bob's input bandpass filter but still far enough apart to be separated by the WDM's optics.

The signal pulses λ_s are passed to the PD module and further delimited into their respective polarization states $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\rangle, |\nearrow\rangle$ for detection, while the timing pulse λ_t is passed directly to the TA to precisely control single photon detection, thereby reducing background noise. Once the polarization state has been corrected, the optical paths must be stabilized. Meaning Bob must control vibration, physical disturbances, and temperature fluctuation to reduce polarization changes in the pulses. Assuming changes due occur over time, they can be measured and accounted for through timing and polarization calibration activities.

3) BOB POLARIZATION DETECTION SUBSYSTEM

Figure 15 details the Polarization Detector (PD) architecture. The module comprises a bandpass filter, a 50/50 beamsplitter (BS), a half wave plate (HWP or $\lambda/2$), and two polarizing beamsplitters (PBSs). This bandpass filter is configured with a very narrow wavelength window to limit the light entering and passing through the subsystem. The BS, HWP, and PBSs are configured in a "passive basis selection," where Bob randomly chooses the measurement basis without the need for additional control logic or random number selection. Specifically, the measurement basis selection (i.e., rectilinear or diagonal) inherently occurs at the 50/50 BS, while the polarization states (Horizontal/Vertical or Diagonal/Antidiagonal) are further delineated at their respective PBS.

When the 50/50 BS transmits $|\leftrightarrow\rangle, |\updownarrow\rangle$ pulses out port 4 (i.e., to the rectilinear basis detectors), the PBS further directs the quantum pulses according to their polarization state and sends them to their appropriate H or V detector. When the 50/50 BS reflects $|\nwarrow\rangle, |\nearrow\rangle$ pulses out port 3 (i.e., to the diagonal basis detectors), they pass through the HWP which is configured to rotate photons by 45 degrees to adjust for diagonally encoded qubits. The PBS further directs the photons to their appropriate D or A detectors.

The modeled passive basis selection ensures pulses prepared and measured in the same basis are correctly detected with a high degree of accuracy, while non-matching bases (due to the 50/50 beamsplitter's random choice) result in erroneous detections which are later sifted out from the final secret key. For example, pulses prepared in the rectilinear basis are randomly measured in both the matching rectilinear basis resulting in a correctly detected qubit and the unmatched diagonal basis which is removed from the final key.

4) BOB TIMING ANALYZER SUBSYSTEM

Figure 16 illustrates the Timing Analyzer (TA) containing a classical detector which receives the timing pulse λ_t, four Single Photon Detectors (SPDs), each configured to detect qubits encoded in one of four polarizations states (Antidiagonal, Diagonal, Horizontal and Vertical), and a controller. SPDs are perhaps the most critical components of realized QKD systems, as they are the principle limiter of secret key generation rates. Commercially available SPDs are complex opto-electrical devices generally consisting of an Avalanche PhotoDiode (APD) and complementary control logic.

APDs are classical optical detectors reverse-biased with higher than normal voltage, causing them to become sensitive to single photons. They have low production and operation costs because of their ability to operate in close proximity to room temperature with inexpensive thermal-electric coolers. Despite their practicality, these detectors severely

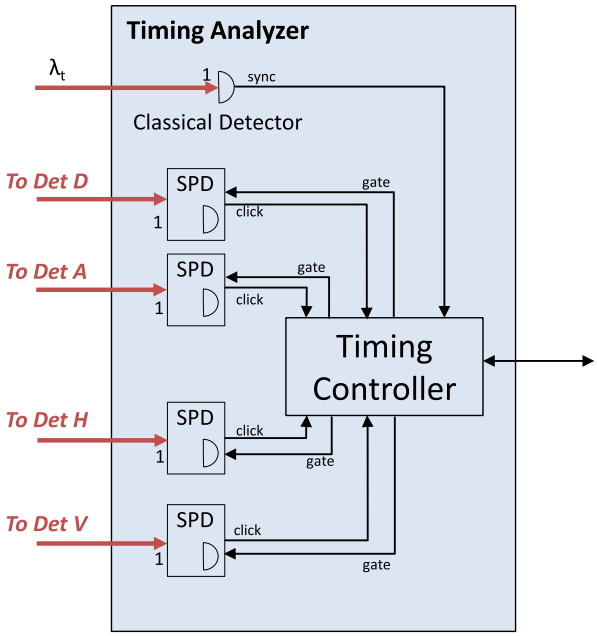


FIGURE 16. Timing Analyzer Decomposition.

constrain system performance due to poor detection efficiencies (e.g., 10%) and relatively long recovery "dead" times (e.g., 10^{-6} sec) necessary to prevent erroneous "after pulse" detections [36]. Their performance is further limited by spontaneous "dark counts" and variation "jitter" in the detector's response time. Although these limitations can be partially mitigated by advanced control circuitry, they are inherent to the devices material makeup and operational environment.

In our model, the timing signal λ_t is used to "gate" the SPDs to reduce the likelihood of erroneous dark counts. The detectors are "gated" when qubits are expected to arrive, transitioning from a classical linear detection mode to a heightened Geiger mode sensitive to single photon energy levels (i.e., 10^{19} Joules per photon at 1550 nm). For example, the simulation can be configured with a 1 ns gating window with a 400 ps signal pulse expected to arrive 100 ps after the window opens. The modeled SPDs are also actively quenched, which attempts to limit the device's avalanching time and after pulsing effect to improve quantum throughput and reduce errors.

When a sub-quantum-level signal pulse λ_s arrives at the appropriately designated SPD (i.e., a $|\leftrightarrow\rangle, |\updownarrow\rangle, |\nwarrow\rangle, |\nearrow\rangle$ signal pulse with an MPN $\ll 1.0$), the number of photons in the pulse is probabilistically determined according to the Poisson distribution. If one or more photons are in the pulse, the arrival time of each photon is probabilistically determined according to the pulse's shape. The time of arrival within the gated detection window is important to calculate the energy incident upon the detector and interference calculations between multiple arriving photons. Next, the detector's efficiency (e.g., 10%) is taken into consideration where each photon in the pulse is treated independently. If the pulse is going to be detected, it scheduled to send a "click" to the timing controller.

During each gating period, device specific dark counts and after pulsing are also probabilistically considered. The modeled SPDs take into consideration recovery times for detection events, where they are prevented from entering the Geiger mode until the dead time is over. Each SPD is a unique instance and can be configured to study the impact of detector performance imbalances (e.g., one detector with 10% efficiency and another with 12% efficiency).

In the reference model, we have chosen to implement APDs because of their long history in QKD experimentation and widespread use in commercially available QKD systems; however, we have also experimented with emerging detector technologies such as Superconducting Nanowire SPD (SNSPD) and Transition Edge Sensor arrays (TES) [2]. Conducting performance analysis of emerging SPD technologies is yet another example of how the qkdX can be used to model and evaluate developmental (or even proposed) QKD technologies to more authoritatively determine if the costs are worth the performance gain.

TABLE 4. Reference model simulation configuration and results.

Configuration	Signal MPN	Decoy MPN	Vacuum MPN	Signal %	Decoy %	Vacuum %
Reported System	0.65	0.08	~0	75.0	12.5	12.5
Modeled System	0.65	0.08	~0	75.0	12.5	12.5
Performance	**Signal Gain**	**Decoy Gain**	**Signal QBER**	**Decoy QBER**	**Dark Count**	**R_{secure}**
Reported Results	6.36E-3	8.61E-4	1.44E-2	7.84E-2	1.0E-4	4.10E-4
Simulation Results	*6.28E-3*	*9.61E-4*	*1.21E-2*	*6.57E-2*	*9.9E-5*	*6.68E-4*

D. SIMULATION RESULTS

The modeled reference architecture has been verified, validated, and used to support practically-oriented research efforts [2], [6]. Configuring the reference model similar to Chen *et al.*'s experimental QKD system presented in [37], we were able to reasonably match their reported performance as demonstrated in Table 4 (see [6] for details) . The system's quantum channel was 20 km with a measured loss of 5.6 dB, and an additional 3.5 dB loss due to Bob's internal architecture. Our simulation results are from a fixed treatment with ~100M sent pulses with confidence bounds of 10 standard deviations.

Simulation runs can be run in serial or parallel, where trials are generally executed until a user-specified number of pulses is detected (e.g., 30,000, 50,000, or 100,000). Typically, these numbers are chosen to support the desired key buffer block size (e.g., 10,000 bits) for error reconciliation, where the number of detections is reduced by 50% due to sifting and 25% for error estimation. The simulation framework is designed to support multiple error reconciliation approaches to include: Winnow, Cascade, Low-Density Parity-Check (LDPC), and an abstract "perfect" correction to increase the speed of simulations.

IEEE Access
The journal for rapid open access publishing

The final length of the QKD-generated secret key is further reduced by privacy amplification depending on the estimated amount of information "leaked" during error reconciliation. See [2] for details on these QKD protocol phases.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we introduced a QKD modeling framework (i.e., the modeling package qkdX) designed to support the development and performance analysis of practically-oriented QKD system representations. We demonstrated the qkdX's utility by modeling and simulating a polarization-based, prepare-and-measure BB84 QKD reference architecture. Detailed decompositions of the modeled architecture and its subsystems are provided with discussions highlighting design features. Furthermore, a listing of the qkdX's modeled optical component library is provided in an Appendix. This paper communicates three distinct aspects:

A. INTRODUCES THE QKD SIMULATION FRAMEWORK BUILT TO EFFICIENTLY STUDY IMPLEMENTATION NON-IDEALITIES

The framework provides a means for efficiently building and analyzing QKD technologies. Specifically, we have enumerated the framework's benefits realized to-date in Table 5.

TABLE 5. Benefits of the qkdx modeling framework.

Perspective	Benefits
Manager	- allows "product" lines to be easily developed - facilitates code reuse through reusable components and subsystems - saves money in development and sustainment
Software Engineer	- allows for easily extendable functional capability - reduces code updates/maintenance overhead - facilitates continuous quality improvement - bugs only need to be corrected once
Analyst	- can select existing models in accordance with experimental goals - can build new models to meet research objectives - allows "simpler" simulations to run - reduces extraneous inputs - reduces complexity of results - limits confounding behaviors

B. PROVIDES A TOOL FOR UNDERSTANDING QKD ARCHITECTURES, DESIGN DECISIONS, AND TRADEOFFS

The described modeled reference architecture can be used to evaluate current or proposed QKD implementations including variations in hardware, software, or protocols. It can also be used to study complex relationships between physical phenomenon and system-level performance to more fully understand the design and implementation trade space. In addition, the model can be used to increase the understanding of the capabilities and limitations of various applications (e.g. space-based QKD).

C. SERVES AS A REFERENCE ARCHITECTURE FOR CONDUCTING SECURITY AND PERFORMANCE ANALYSIS OF QKD SYSTEMS

Current and future work includes modeling additional components, controllers, and protocols necessary to research other QKD implementations. These include phase-based protocols, quantum entanglement systems, and emerging QKD technologies and applications. More specifically, we are currently working on simulation studies to support various QKD research questions:

1) Define the security-performance trade space for decoy state enabled QKD systems
2) Determine the practical limitations of Measurement-Device-Independent (MDI) protocols
3) Understand the capabilities and limitations of space-based QKD applications.
4) Explore the performance-security tradeoffs of emerging SPD technologies in realized QKD systems.

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.

OPTICAL COMPONENT APPENDIX

Component Name	Component Description
Generic Optical Component	All optical components share certain behaviors, which are modeled in a generic optical component. Specifically, all components generate reflections at their inputs where the amplitude and global phase of the reflected pulse is calculated in Eqs. (1) and (2). $$\text{Amplitude}_{\text{Reflected}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-\text{ReturnLoss}}{10}}} \quad (1)$$ $$\text{GlobalPhase}_{\text{Reflected}} = \text{GlobalPhase}_{\text{Input}} + \pi \quad (2)$$
Attenuator, Fixed Optical (FOA)	The Fixed Optical Attenuator (FOA) is a passive two port, bidirectional optical component used to reduce the strength of optical pulses. The amplitude of the output pulses is calculated in Eq. (3). Note that the fixed attenuation, insertion loss, and return loss can be varied in the range of 0.0 and 80.0 dB. The modeled behaviors are based on [38]–[41]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-(\text{InsertionLoss}+\text{FixedAttenuation})}{10}}} \quad (3)$$

Attenuator, Electrical Variable Optical (EVOA)

The Electrical Variable Optical Attenuator (EVOA) is an active two port, bidirectional optical component used to reduce the strength of optical pulses. The variable attenuation is controlled through a modeled electrical signal and can be varied in the range of 0.0 to 60.0 dB. The EVOA also has a configurable slew rate to account for the rate of change in attenuation the device can achieve. The amplitude of the output pulse is calculated in Eq. (4). The modeled behaviors are based on [40], [42]–[44].

$$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-(\text{InsertionLoss}+\text{VariableAttenutation})}{10}}} \tag{4}$$

Bandpass Filter

The bandpass filter is a passive two port, bidirectional optical component used to transmit only the desired wavelength of light, while other wavelengths of light (i.e., noise) are blocked. The modeled filer has four filtering ranges, including: 1. within the Central Wavelength (CWL), 2. within the upper/lower middleband Central Frequency (CF), 3. within the upper/lower outer CF, and 4. outside the device's range. If the optical pulse's CWL is the same as the bandpass filter the pulse is transmitted according to Eq. (5). If the pulse's CWL is outside the bandpass filter's CWL and within the limits of middleband CF, the pulse is transmitted according to Eq. (6). If the pulse's CWL is outside the limits of the middleband CF and within the bandpass filter CF, the pulse is transmitted according to Eq. (7). If the pulse's CWL is outside the limits of the bandpass filter, the pulse is transmitted according to Eq. (8). The bandpass filter is designed to support optical communication at 1550 nm and can be varied in the range 1.45E-6 to 1.60E-6 m. The modeled behaviors are based on [45]–[49].

$$\text{Amplitude}_{\text{output}} = \text{Amplitude}_{\text{input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \tag{5}$$

$$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} * \sqrt{10^{-\left(\frac{\text{bandpass}_{\text{CWL}}-\text{Amplitude}_{\text{inputCWL}}}{\frac{\text{MidBandWidth}}{2}}\right)*\frac{\text{MidBandLoss}}{10}}} \tag{6}$$

$$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} * \sqrt{10^{\frac{-\text{MidBandLoss}}{10}}} * \sqrt{10^{-\left(\frac{\text{MidBandLow}_{\text{CF}}-\text{Amplitude}_{\text{input}}}{\text{MidBandLow}-\text{OutBandLow}}\right)*\frac{(\text{OutBandLoss}-\text{MidBandLoss})}{10}}} \tag{7}$$

$$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} * \sqrt{10^{\frac{-\text{OutBandLoss}}{10}}} \tag{8}$$

Beamsplitter

The beamsplitter is a passive four port, bidirectional optical component used to divide optical pulses into two pulses: a reflected and a transmitted pulse according to a defined High Output Percentage (HOP) and Low Output Percentage (LOP). For example, a 99:1 beamsplitter would output a reflected pulse with 99% of the input pulse's energy and the transmitted pulse would have 1%. The amplitude of the reflected pulse is calculated in Eqs. (9), (10), and (11), where α is the orientation of the input pulse and γ is the component offset angle. The transmitted pulse's amplitude is calculated similarly; however, the LOP is utilized instead. The beamsplitter exhibits insertion loss, device specific excess loss, and polarization dependent loss for both outputs (i.e., the reflected and transmitted ports), which can be varied in the range 0.0 to 80.0 db. The pulse's output orientation is calculated in Eq. (12). Note the global phase of the reflected pulse is adjusted using Eq. (13). The modeled behaviors are based on [50]–[53].

$$\text{Amplitude}_{\text{Output}} = \sqrt{\left(\text{Amplitude}_{\text{X}_{\text{Output}}}\right)^2 + \left(\text{Amplitude}_{\text{Y}_{\text{Output}}}\right)^2} \tag{9}$$

$$\text{Amplitude}_{\text{X}_{\text{Output}}} = \text{Amplitude}_{\text{Input}} * \cos(\alpha+\gamma) * \sqrt{\frac{\text{HOP}}{100}} * \sqrt{10^{\frac{-\text{ExcessLoss}}{10}}} * \sqrt{10^{\frac{-\text{PolarDependentLoss}_{\text{X}}}{10}}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \tag{10}$$

$$\text{Amplitude}_{\text{Y}_{\text{Output}}} = \text{Amplitude}_{\text{Input}} * \sin(\alpha+\gamma) * \sqrt{\frac{\text{HOP}}{100}} * \sqrt{10^{\frac{-\text{ExcessLoss}}{10}}} * \sqrt{10^{\frac{-\text{PolarDependentLoss}_{\text{Y}}}{10}}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \tag{11}$$

$$\text{Orientation}_{\text{Output}} = \text{atan2}(\text{Amplitude}_{\text{Y}}, \text{Amplitude}_{\text{X}}) \tag{12}$$

$$\text{GlobalPhase}_{\text{Reflected}} = \text{GlobalPhase}_{\text{Input}} + \gamma + \frac{\pi}{2} \tag{13}$$

IEEE Access
The journal for rapid open access publishing

Beamsplitter, Polarizing (PBS)

The Polarizing Beamsplitter (PBS) is a passive four port, bidirectional optical component used to split optical pulses into two pulses: a reflected and a transmitted pulse according to orthogonal polarizations (e.g., the reflected pulse will be vertically polarized, while the transmitted pulse is horizontally polarized). The amplitude of the transmitted pulse is calculated in Eqs. (14), (15), and (16) where the reflected pulse's amplitude has an extinction ratio of 0.0, α is the orientation of the input pulse, and γ is the component offset angle. The reflected pulse's amplitude is calculated similarly, where the transmitted pulse's amplitude has an extinction ratio of 0.0 and cosine is utilized instead of sin. The PBS exhibits insertion loss, device specific excess loss, and polarization dependent loss for both outputs (i.e., the reflected and transmitted ports), which can be varied in the range 0.0 to 80.0 db. The pulse's output orientation is calculated in Eq. (17). Note the global phase of the reflected pulse is adjusted using Eq. (18). The modeled behaviors are based on [46], [51], [54]–[56].

$$\text{Amplitude}_{\text{Ouput}} = \sqrt{\left(\text{Amplitude}_{\text{X}_{\text{Output}}}\right)^2 + \left(\text{Amplitude}_{\text{Y}_{\text{Output}}}\right)^2} \tag{14}$$

$$\text{Amplitude}_{\text{X}_{\text{Output}}} = \text{Amplitude}_{\text{Input}} * \sin(\alpha + \gamma) * \sqrt{10^{\frac{-\text{ExcessLoss}}{10}}}$$
$$* \sqrt{10^{\frac{-\text{PolarDependentLosses}_{\text{X}}}{10}}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \tag{15}$$

$$\text{Amplitude}_{\text{Y}_{\text{Output}}} = \text{ExtinctionRatio} \tag{16}$$

$$\text{Orientation}_{\text{Output}} = \text{atan2}(\text{Amplitude}_{\text{Y}}, \text{Amplitude}_{\text{X}}) \tag{17}$$

$$\text{GlobalPhase}_{\text{Reflected}} = \text{GlobalPhase}_{\text{Input}} + \gamma + \frac{\pi}{2} \tag{18}$$

Circulator

The circulator is a passive three port, directional optical component used to route optical pulses from one port an adjacent port. Optical pulses propagating in the forward direction are merely reduced by the insertion loss as calculated in Eq. (19). Pulses attempting to propagate in the reverse direction are severely attenuated using an isolation loss as calculated in Eq. (20). The modeled behaviors are based on [60]–[62].

$$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \tag{19}$$

$$\text{Amplitude}_{\text{Isolated}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-(\text{InsertionLoss}+\text{IsolationLoss})}{10}}} \tag{20}$$

Detector, Classical

The classical detector is an active one port, directional optical-electrical component used to detect classical optical pulses (i.e., pulses with millions of photons) passing into the optical receiver. The classical detector is abstractly modeled and configured to generate electrical signals according to the peak power of the input pulse as calculated in Eq. (21). The modeled behavior is based on [57].

$$\text{Electrical}_{\text{Output}} = \text{ConversionFactor} * \text{PeakPower}_{\text{Input}} \tag{21}$$

Detector, Single Photon (SPD)

The Single Photon Detector (SPD) is an active one port, directional optical-electrical component used to detect weak optical pulses (i.e., pulses with a small number of photons). The SPD is modeled as an Avalanche Photodiode (APD) with supplementary controller logic to account for detector efficiency, dark counts, and after pulsing, as well as, gating and active quenching to reduce noise. The SPD is configured to detect weak optical pulses during gated periods according to the detector efficiency, where errors due to the dark count probability and after pulsing are considered. Once a pulse is detected, an electrical signal (i.e., a click) is generated and transmitted through an electrical output port. While the SPD's behavior is complex, it is generically presented in Eq. (22). For a detailed description of SPD behaviors and technologies, please see [58], [59].

$$\text{Electrical}_{\text{Output}} = \text{Gating} * \text{Efficiency}_{\text{Detector}} * \text{Probabilty}_{\text{DarkCount}} * \text{Probability}_{\text{Afterpulse}} \tag{22}$$

Half-Wave Plate and Quarter-Wave Plate

The half-wave plate and quarter-wave plate are passive two port, bidirectional optical components used to create a phase shift to rotate linearly polarized light. The orientation, ellipticity, and global phase of the output pulse are calculated in Eqs. (23) to (28), where α is the orientation, φ is the ellipticity, and γ is the device offset angle. The desired half-wave or quarter-wave rotation is obtained by appropriately adjusting the offset angle γ. The modeled behaviors are based on [63]–[67].

$$\text{Orientation}_{\text{Output}} = \arccos \text{P}(\gamma, \alpha, \varphi) \tag{23}$$

$$\text{Ellipticity}_{\text{Output}} = \text{Gamma}(\gamma, \alpha, \varphi) - \text{Delta}(\gamma, \alpha, \varphi) \tag{24}$$

$$\text{GlobalPhase}_{\text{Output}} = \text{GlobalPhase}_{\text{Input}} + \text{Delta}(\gamma, \alpha, \varphi) \tag{25}$$

$$\text{P}(\gamma, \alpha, \varphi) = \frac{1}{2}\sqrt{2 + 2\cos(2\alpha) * \cos(4\gamma) + 2\cos(\varphi) * \sin(2\alpha) * \sin(4\gamma)} \tag{26}$$

	$$\text{Gamma} = \text{atan2}\left(\frac{-2\cos\left(\frac{\varphi}{2}\right)*\sin\left(\frac{\varphi}{2}\right)*\sin(\alpha)*\cos(2\gamma)}{\sin(2\gamma-\alpha)+2\left(\sin\left(\frac{\varphi}{2}\right)\right)^2*\sin(\alpha)*\cos(2\gamma)}\right) \quad (27)$$ $$\text{Delta} = \text{atan2}\left(\frac{2\cos\left(\frac{\varphi}{2}\right)*\sin\left(\frac{\varphi}{2}\right)*\sin(\alpha)*\sin(2\gamma)}{\cos(2\gamma-\alpha)-2\left(\sin\left(\frac{\varphi}{2}\right)\right)^2*\sin(\alpha)*\sin(2\gamma)}\right) \quad (28)$$
In-line Polarizer	The in-line polarizer is a passive two port, bidirectional optical component used to polarize optical pulses into a known orientation. Pulses with the same polarization as the in-line polarizer are transmitted, while pulses orthogonal to the in-line polarizer are blocked. The amplitude and orientation of the output pulses are calculated in Eqs. (29) and (30), where α is the orientation, φ is the ellipticity, and γ is the device offset angle. Note that the output ellipticity is set to 0.0 as well. The modeled behaviors are based on [68]–[70]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} *\sqrt{(\cos(\alpha)*\cos(\gamma))^2+(\sin(\alpha)*\sin(\gamma))^2+2*\cos(\alpha)*\cos(\gamma)*\sin(\alpha)*\sin(\gamma)*\cos(\varphi)} \quad (29)$$ $$\text{Orientation}_{\text{Output}} = \gamma \quad (30)$$
Isolator	The isolator is a two port, directional optical component used to transmit optical pulses in the forward direction and severely attenuate or isolate optical pulses passing in the reverse direction. The amplitude and orientation of the output pulses are calculated in Eq. (31) and (32), respectively. The amplitude of the isolated pulses is calculated in Eq. (33). The modeled behaviors are based on [71], [72]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \quad (31)$$ $$\text{Orientation}_{\text{Output}} = \text{Orientation}_{\text{Input}} + \frac{\pi}{2} \quad (32)$$ $$\text{Amplitude}_{\text{Isolated}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-(\text{InsertionLoss}+\text{IsolationLoss})}{10}}} \quad (33)$$
Laser	The laser is an active one port, directional optical-electrical component configured to generate coherent optical pulses. The laser is configured to generate classical pulses representative of commercially available laser sources according to an electrical signal (i.e., a trigger). The laser pulses can be characterized as timing, signal, decoy, or vacuum pulses. The modeled behaviors are based on [73]–[76].
Optical Switch 1×2	The optical switch 1×2 is an active three port, unidirectional optical-electrical component used to route optical pulses from the input port to one or two output ports according to an electrical signal (i.e., a switch state). When a pulse is transmitted to the desired output port, an isolated pulse is also generated on the non-desired port. The amplitude of the desired output pulse is calculated in Eq. (34), while the amplitude of the isolated pulse is calculated in Eq. (35). The modeled behaviors are based on [77]–[81]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \quad (34)$$ $$\text{Amplitude}_{\text{Isolated}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-(\text{InsertionLoss}+\text{IsolationLoss})}{10}}} \quad (35)$$
Polarization Controller	The polarization controller is an active two port, directional optical-electrical component used to correct for polarization errors in orientation and ellipticity. Typically, these devices are implemented to correct for polarization drift occurring over the quantum channel, where the receiver adjusts the pulse's polarization according to a known reference state. The amplitude of the output pulses is calculated in Eq. (36). The polarization controller also has a configurable slew rate to account for the rate of correction the device can achieve. The modeled behaviors are based on [82]–[87]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \quad (36)$$
Polarization Maintaining Fiber Channel	The polarization maintaining (PM) fiber is a passive two port, bidirectional optical component used to propagate optical pulses while maintaining the pulse's polarization state. Largely dependent upon the distance traveled, the amplitude of the output pulse is calculated using Eqs. (37) and (38). The optical fiber can also induce ''random walk'' effects, which cause the pulse's polarization to drift from the encoded state. These effects are caused by environmental and physical disturbances and simulated with the Brownian motion approximation in Eq. (39), where P is polarization, t is time, Δt is displacement, q is a random number, and τ is a scalable time constant used to control the random walk. If the enabled, the orientation and ellipticity are randomly rotated according to Eqs. (38) and (39). The modeled behaviors are based on [88]–[91]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}}*\sqrt{10^{\frac{-(\text{InsertionLoss}+\text{FiberLoss})}{10}}} \quad (37)$$ $$\text{FiberLoss} = \text{Loss/km}*\text{Length} \quad (38)$$

IEEE Access
The journal for rapid open access publishing

	$$P(t) = P(t - \Delta t) + q * \sqrt{\Delta t}/\tau \quad (39)$$ $$\text{InducedOrientationRotation} = q * \sqrt{\frac{\text{Time}_{\text{Current}} - \text{Time}_{\text{Initial}}}{\text{OrientaitonTimeConstant}}} \quad (40)$$ $$\text{InducedEllipticityRotation} = q * \sqrt{\frac{\text{Time}_{\text{Current}} - \text{Time}_{\text{Initial}}}{\text{EllipticityTimeConstant}}} \quad (41)$$
Polarization Modulator	The polarization modulator is an active two port, bidirectional optical-electrical component used to modify the polarization of optical pulses. In this manner qubits are encoded by modifying the orientation to the desired angle as described in Eq. (42). For example, a horizontally encoded pulse can represent a "0" and a vertically encoded pulse can represent a "1" in the polarization based BB84 protocol. The amplitude of the output pulse is calculated in Eq. (43). The modeled behaviors are based on [82]–[87]. $$\text{Polarization}_{\text{Output}} = \text{Polarization}_{\text{Encoded}} \quad (42)$$ $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \quad (43)$$
Wave Division Multiplexer and Dichroic Mirror	The wave division multiplexer is a passive, three port bidirectional optical component used to combine or split multiple wavelengths of light. When configured as a splitter, the multiplexer has one input port and two or more output ports, where co-propagating wavelengths are separated onto individual outputs. When configured as a combiner, the multiplexer has two or more input ports and one output port, where multiple wavelengths of light are joined on a single fiber. Whether functioning as a combiner or splitter, the device operates according to each port's passing wavelength. If the pulse's wavelength is within the passing bandwidth, its amplitude is calculated from Eq. (44); otherwise the isolated pulse's amplitude is calculated using Eq. (45). The WDM's behavior is similar to that of a dichroic mirror. The modeled behaviors are based on [92]–[95]. $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-\text{InsertionLoss}}{10}}} \quad (44)$$ $$\text{Amplitude}_{\text{Output}} = \text{Amplitude}_{\text{Input}} * \sqrt{10^{\frac{-(\text{InsertionLoss}+\text{IsolationLoss})}{10}}} \quad (45)$$

REFERENCES

[1] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Phys. Rev. A*, vol. 72, no. 1, p. 012332, 2005.

[2] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, G. Baumgartner, and C. McLaughlin, "Performance evaluations of quantum key distribution system architectures," *IEEE Security Privacy*, vol. 13, no. 1, pp. 30–40, 2015.

[3] N. T. Sorensen and M. R. Grimaila, "Discrete event simulation of the quantum channel within a quantum key distribution system," *J. Defense Model. Simul., Appl., Methodol., Technol.*, 2015.

[4] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, L. E. Dazzio-Cornn, and C. McLaughlin, "Modeling continuous time optical pulses in a quantum key distribution discrete event simulation," in *Proc. Int. Conf. Security Manage. (SAM)*, Jul. 2014, pp. 229–235.

[5] (Mar. 3, 2014). *OMNeT++*. [Online]. Available: http://www.omnetpp.org/, accessed Nov. 8, 2013.

[6] L. O. Mailloux, R. D. Engle, M. R. Grimaila, D. D. Hodson, and C. McLaughlin, "Modeling decoy state quantum key distribution systems," *J. Defense Model Simul.*, submitted for publication.

[7] J. D. Morris, M. R. Grimaila, D. D. Hodson, C. V. McLaughlin, and D. R. Jacques, "Using the discrete event system specification to model quantum key distribution system components," *J. Defense Model. Simul., Appl., Methodol., Technol.*, 2014.

[8] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, 1983.

[9] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Aug. 1984, pp. 475–480.

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, 1992.

[11] S. Loepp and W. K. Wootters, *Protecting Information*. New York, NY, USA: Cambridge Univ. Press, 2006.

[12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2010.

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Modern Phys.*, vol. 74, no. 1, pp. 145–195, 2002.

[14] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, pp. 1301–1350, 2009.

[15] V. Scarani and C. Kurtsiefer. (2009). "The black paper of quantum cryptography: Real implementation problems." [Online]. Available: http://arxiv.org/abs/0906.4547

[16] S. Zhao and H. De Raedt, "Event-by-event simulation of quantum cryptography protocols," *J. Comput. Theoretical Nanosci.*, vol. 5, no. 4, pp. 490–504, 2008.

[17] M. Niemiec, Ł. Romański, and M. Święty, "Quantum cryptography protocol simulator," in *Multimedia Communications, Services and Security*. Berlin, Germany: Springer-Verlag, 2011, pp. 286–292.

[18] G. Mogos, "Quantum key distribution—QKD simulation," in *Proc. 18th Conf. Quantum Inf. Process.*, Sydney, NSW, Australia, Jan. 2015.

[19] A. Buhari, Z. A. Zukarnain, S. K. Subramaniam, H. Zainuddin, and S. Saharudin, "An efficient modeling and simulation of quantum key distribution protocols using OptiSystem," in *Proc. IEEE Symp. Ind. Electron. Appl. (ISIEA)*, Bandung, Indonesia, Sep. 2012, pp. 84–89.

[20] A. Buhari, Z. A. Zukarnai, S. K. Subramaniam, H. Zainuddin, and S. Saharudin, "BB84 and noise immune quantum key distribution protocols simulation: An approach using photonic simulator," in *Proc. Int. Conf. Comput. Intell. Syst., Int. Conf. Elect., Electron. (ICCIS)*, Bangkok, Thailand, 2012, pp. 30–36.

[21] M. Halip, N. Hafizah, M. Mokhtar, and A. Buhari, "Simulation of Bennet and Brassard 84 protocol with Eve's attacks," in *Proc. IEEE 5th Int. Conf. Photon. (ICP)*, Kuala Lumpur, Malaysia, Sep. 2014, pp. 29–31.

[22] X. Zhang, Q. Wen, and F. Zhu, "Object-oriented quantum cryptography simulation model," in *Proc. 3rd Int. Conf. Natural Comput. (ICNC)*, Haikou, China, Aug. 2007, pp. 599–602.

[23] A. Atashpenda. (2014). *Simulation and Analysis of QKD (BB84)*. [Online]. Available: http://www.qkdsimulator.com/, accessed Feb. 23, 2015.

[24] 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," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 4, no. 2, pp. 829–838, 2014.
[25] R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, "Quantum cryptography over underground optical fibers," in *Advances in Cryptology*. Berlin, Germany: Springer-Verlag, 1996.
[26] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, "'Plug and play' systems for quantum cryptography," *Appl. Phys. Lett.*, vol. 70, no. 7, pp. 793–795, 1997.
[27] D. Stucki *et al.*, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, p. 123001, 2011.
[28] C. Elliott, "The DARPA quantum network," in *Quantum Communications and Cryptography*, A. V. Sergienko, Ed. Boca Raton, FL, USA: CRC Press, 2006, pp. 83–102.
[29] M. Peev *et al.*, "The SECOQC quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, p. 075001, 2009.
[30] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, p. 057901, 2003.
[31] H. -K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 3, p. 230504, 2005.
[32] W. Chen *et al.*, "Field experiment on a 'star type' metropolitan quantum key distribution network," *IEEE Photon. Technol. Lett.*, vol. 21, no. 9, pp. 575–577, May 1, 2009.
[33] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, 2011.
[34] M. Matsumoto and T. Nishimura, "Mersenne twister: A 623-dimensionally equidistributed uniform pseudo-random number generator," *ACM Trans. Model. Comput. Simul.*, vol. 8, no. 1, pp. 3–30, 1998.
[35] ID Quantique SA. *QUANTIS (USB, PCI Express, PCI)*. [Online]. Available: http://www.idquantique.com/random-number-generators/products/quantis-usb.html, accessed Nov. 17, 2014.
[36] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photon.*, vol. 3, no. 12, pp. 696–705, 2009.
[37] T. -Y. Chen *et al.*, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Opt. Exp.*, vol. 17, no. 8, pp. 6540–6549, 2009.
[38] Thor Labs. *Fixed Fiber Optic Attenuators, Single Mode*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=1385, accessed Jun. 13, 2014.
[39] Newport. *Fixed Fiber Optic Attenuator*. [Online]. Available: http://www.newport.com/Fixed-Fiber-Optic-Attenuator/835678/1033/info.aspx#tab_orderinfo, accessed Jun. 13, 2014.
[40] OZ Optics. *Fixed Attenuators and Attenuating Fiber Patchcord*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0030.pdf, accessed Jun. 13, 2014.
[41] Pacific Interconnections. *Fiber Build Out Attenuators*. [Online]. Available: http://www.pacificinterco.com/attenuators/fiber-optic-attenuator.htm, accessed Jun. 13, 2014.
[42] OPLINK. (2014). *Electronically Variable Optical Attenuators*. [Online]. Available: http://www.oplink.com/pdf/EVOA-S0012.pdf
[43] Lightwaves 2020. (2014). *Liquid Crystal Based Variable Optical Attenuation for Open-Loop Architecture*. [Online]. Available: http://www.amstechnologies.com/fileadmin/amsmedia/downloads/1073_VOA-LowTDL.pdf
[44] OZ Optics. (2014). *Electronically Controlled Variable Fiber Optic Attenuator*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0010.pdf
[45] Newport. (2014). *Tunable Bandpass Fiber Optic Filter*. [Online]. Available: http://www.newport.com/Tunable-Bandpass-Fiber-Optic-Filter/835502/1033/info.aspx#tab_orderinfo
[46] Thor Labs. (2014). *NIR Bandpass & Laser Line Filters 700–1650 nm Center Wavelength*. [Online]. Available: http://www.thorlabs.com/NewGroupPage9.cfm?ObjectGroup_ID=1000
[47] AFW Technologies. (2014). *Fiber Optic Band Pass Filter*. [Online]. Available: http://www.afwtechnologies.com.au/band_pass_filter.html
[48] Gould Fiber Optics. (2014). *High Isolation Fiber Optic Wavelength Division Multiplexers*. [Online]. Available: http://www.gouldfo.com/highisolationwdm.aspx#specs
[49] D. A. Satorius, "Tension-tuned acousto-optic bandpass filter," U.S. Patent 6 647 159, Nov. 11, 2003.
[50] Edmund Optics. (2014). *What are Beamsplitters?* [Online]. Available: http://www.edmundoptics.com/technical-resources-center/optics/what-are-beamsplitters/
[51] OZ Optics. (2014). *Beam Splitters/Combiners*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0095.pdf
[52] Edmund Optics. (2014). *Cube Beamsplitters*. [Online]. Available: http://www.edmundoptics.com/optics/beamsplitters/cube-beamsplitters/
[53] Thor Labs. (2014). *Optical Beamsplitters*. [Online]. Available: http://www.thorlabs.com/navigation.cfm?guide_id=18
[54] Thor Labs. (2014). *Fiber-Based Polarization Beam Combiners/Splitters, 1 SM and 2 PM Ports*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=6673
[55] Thor Labs. (2014). *Variable Polarization Beamsplitter Kit*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=316
[56] DPM Photonics. (2014). *Specifications*. [Online]. Available: http://www.dpmphotonics.com/product_detail.php?id=170
[57] Thor Labs. (2014). *Calibrated Photodiodes*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=2822
[58] R. H. Hadfield, "Single-photon detectors for optical quantum information applications," *Nature Photon.*, vol. 3, no. 12, pp. 696–705, 2009.
[59] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Rev. Sci. Instrum.*, vol. 82, no. 7, p. 071101, 2011.
[60] Gould Fiber Optics. (2014). *Fiber Optic Circulators*. [Online]. Available: http://www.gouldfo.com/circulator.aspx
[61] Thor Labs. (2014). *Single Mode Fiber Optic Circulators*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=373
[62] Thor Labs. (2014). *InGaAs Avalanche Photodetectors*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=4047
[63] Newport. (2014). *Zero-Order Precision Wave Plates*. [Online]. Available: http://www.nxtbook.com/nxtbooks/newportcorp/resource2011/#/800
[64] Wolfram. (2014). *Polarization of Light through a Wave Plate*. [Online]. Available: http://demonstrations.wolfram.com/PolarizationOfLightThroughAWavePlate/
[65] OZ Optics. (2014). *Polarization Rotators/Controllers/Analyzer*. [Online]. Available: http://www.icwic.com/icwic/data/pdf/cd/cd069/Polarizers%20FO/a/111999.pdf
[66] OZ Optics. (2014). *Polarization Rotators/Controllers/Analyzers*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0072.pdf
[67] Newport. (2014). *Polarization*. [Online]. Available: http://www.newport.com/Polarization/144921/1033/content.aspx
[68] Thor Labs. (2014). *In-Line Fiber Optic Polarizers*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=5922
[69] Newport. (2014). *Fiber Optic In-Line Polarizers*. [Online]. Available: https://www.newport.com/Fiber-Optic-In-Line-Polarizers/849607/1033/info.aspx#tab_Specifications
[70] OZ Optics. (2014). *Polarizers—Fiber Optic*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0018.pdf
[71] Thor Labs. (2014). *IR Fiber Optic Isolators With SM Fiber (1290–2010 nm)*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=6178
[72] K. W. Chang and W. V. Sorin, "High-performance single-mode fiber polarization-independent isolators," *Opt. Lett.*, vol. 15, no. 8, pp. 449–451, 1990.
[73] Thor Labs. (2014). *Coherent Sources*. [Online]. Available: http://www.thorlabs.com/navigation.cfm?guide_id=31
[74] ID Quantique. (2012). *ID300 Series Sub-Nanosecond Pulsed Laser Source Datasheet*. [Online]. Available: http://www.idquantique.com/images/stories/PDF/id300-laser-source/id300-specs.pdf, accessed Mar. 5, 2014.
[75] L. Lydersen *et al.*, "Superlinear threshold detectors in quantum cryptography," *Phys. Rev. A*, vol. 84, p. 032320, Aug. 2011.
[76] L. O. Mailloux, M. R. Grimaila, D. D. Hodson, L. E. Dazzio-Cornn, and C. McLaughlin, "Modeling continuous time optical pulses in a quantum key distribution discrete event simulation," in *Proc. Int. Conf. Secur. Manage. (SAM)*, 2014, pp. 1–7.
[77] oeMarket. (2014). *1x1/1x2 Fiber Optical Switch*. [Online]. Available: http://www.oemarket.com/catalog/product_info.php/1x11x2-fiber-optical-switch-p-81?osCsid=4618a22aaa4eae756f73ad2fd2a293b1
[78] DiCon Fiberoptics, Inc. (2014). *Optical Switches*. [Online]. Available: http://www.diconfiberoptics.com/products/prd_switches.php

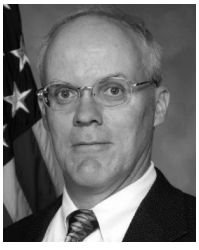
[79] DiCon Fiberoptics, Inc. (2014). *MEMS 1xN Singlemode Optical Switches*. [Online]. Available: http://www.diconfiberoptics.com/products/?prod=0044&menu=swt&sub=0
[80] Thor Labs. (2014). *OSW12-1310-SM—Vis/NIR MEMS 1x2 Switch, 1310 nm, SMF*. [Online]. Available: http://www.thorlabs.com/thorProduct.cfm?partNumber=OSW12-1310-SM
[81] Luminos. (2014). *Single 1x2 Fiber Optic Switch*. [Online]. Available: http://luminos.com/products/switches/s12/?gclid=CIWE-4f29LMCFYZM4Aod4F4AWQ
[82] Thor Labs. (2014). *Deterministic Polarization Controller—DPC5500*. [Online]. Available: http://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=930
[83] Phoenix Photonics. (2014). *Fiber Polarization Controller*. [Online]. Available: http://www.phoenixphotonics.com/documents/polarizationcontroller_01202.pdf
[84] Phoenix Photonics. (2014). *Electronic In-Line Fiber Polarization Controller—EPC With Optional Microprocessor Based PC Interface*. [Online]. Available: http://www.phoenixphotonics.com/website/products/Electronically_Controlled_Polarization_Controller.htm
[85] OZ Optics. (2014). *Electrically Driven Polarization Controller-Scrambler*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0011.pdf
[86] Fiber Logix. (2014). *Electronically Addressed Polarization Controller*. [Online]. Available: http://www.fiberlogix.com/Passive/Electronically%20addresses%20Polarization%20controller.html
[87] General Photonics. (2014). *Dynamic Polarization Controller/Scrambler*. [Online]. Available: http://www.ainnotech.com/pdf/GP-Modules-Polarization%20Management-Dynamic%20Polarization%20Scrambler%20Controller.pdf
[88] Corning. (2014). *PANDA PM Specialty Optical Fibers*. [Online]. Available: http://www.corning.com/WorkArea/showcontent.aspx?id=18341
[89] O. Sezerman and G. Best, "Accurate alignment preserves polarization," *Laser Focus World*, vol. 33, no. 12, pp. S27–S30, 1997. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/ART0001.pdf
[90] Encyclopedia. (2014). *Polarization-Maintaining Fibers*. [Online]. Available: http://www.rp-photonics.com/polarization_maintaining_fibers.html
[91] Thor Labs. (2014). *Polarization-Maintaining FC/PC Fiber Optic Patch Cables*. [Online]. Available: http://www.thorlabs.com/search/thorsearch.cfm?search=polarization+maintaining+fiber+optics
[92] Pacific Interconnections Group. (2014). *Fiber Optic WDM*. [Online]. Available: http://www.pacificinterco.com/Splitters_N_Couplers/1310-1550-WDM.htm
[93] OZ Optics. (2014). *Wavelength Division Multiplexers*. [Online]. Available: http://www.ozoptics.com/ALLNEW_PDF/DTS0089.pdf
[94] Gould Fiber Optics. (2014). *Fiber Optic Wavelength Division Multiplexers (WDMs)*. [Online]. Available: http://www.gouldfo.com/wdm.aspx
[95] Thor Labs. (2014). *Dichroic Mirrors/Beamsplitters*. [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=3313

LOGAN O. MAILLOUX (M'12) received the B.S. degree in 2002, and the M.S. degree in 2008. He is a Certified Information Systems Security Professional. He is a Commissioned Officer with the United States Air Force Institute of Technology, Wright-Patterson AFB, OH, USA, and is currently pursuing the Ph.D. degree with the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA. His research interests include system security engineering, complex information communication and technology implementations, and quantum key distribution systems. He is a member of the Tau Beta Pi, the Eta Kappa Nu, the International Council on Systems Engineering, and the Association for Computing Machinery.

JEFFREY D. MORRIS (M'11) received the B.S. degree in 2001, the M.M.I.S. degree in 2006, the M.S.S.I. degree in 2007, and the Ph.D. degree in 2014. He is currently a Master Sergeant with the United States Army, and serves as a Researcher and an Instructor with the Army Cyber Institute, United States Military Academy, West Point, NY, USA. His research interests include systems engineering, discrete event modeling and simulation, and quantum key distribution systems. He is a member of the Tau Beta Pi, the Sigma Iota Epsilon, the International Council on Systems Engineering, and the International System Security Association.

MICHAEL R. GRIMAILA (SM'05) is a Certified Information Security Manager and a Certified Information Systems Security Professional. He received the B.S. degree in 1993, the M.S. degree in 1995, and the Ph.D. degree in 1999. He is a Professor and the Head of the Department of Systems Engineering, and a member of the Center for Cyberspace Research with the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA. He is a member of the Tau Beta Pi, the Eta Kappa Nu, the International Council on Systems Engineering, and the Association for Computing Machinery, and a fellow of the International System Security Association. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management and security, and systems engineering.

DOUGLAS D. HODSON received the B.S. degree in 1985, the M.S. degree in 1987, and the Ph.D. degree in 2009. He is currently an Assistant Professor of Computer Engineering with the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA. His research interests include computer engineering, software engineering, real-time distributed simulation, and quantum communications. He is also a Dayton Area Graduate Studies Institute Scholar and a member of Tau Beta Pi.



DAVID R. JACQUES received the B.S. degree in 1983, the M.S. degree in 1989, and the Ph.D. degree in 1995. He is currently an Associate Professor of Systems Engineering with the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA. His research interests are in the areas of concept definition and evaluation, architecture modeling, and optimal system design. He had prior military assignments in intelligence analysis, research and development, and test and evaluation.

JOHN M. COLOMBI (M'05) received the B.S. degree in 1986, the M.S. degree in 1992, and the Ph.D. degree in 1996. He is currently an Associate Professor of Systems Engineering with the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, OH, USA. Before joining AFIT, he had 21 years of military experience, where he led systems engineering for the E-3 aircraft, managed C2ISR portfolio integration, developed and tested biometrics and information security, and performed research on secure tactical networking with the Air Force Research Laboratory. His research interests include systems and enterprise architecture, complex adaptive systems, acquisition process modeling, and human systems integration. He is a member of the International Council on Systems Engineering.

COLIN V. MCLAUGHLIN received the B.A. degree in 2003, and the Ph.D. degree in 2010. He is currently a Research Physicist with the Naval Research Laboratory, Washington, D.C., USA. He specializes in photonic communication devices and systems.

JENNIFER A. HOLES received the B.S. degree in 2013. She is currently a Research Assistant with ORISE, Air Force Institute of Technology, Wright-Patterson AFB, OH, USA, and a Graduate Student with Wright State University, Dayton, OH, USA. Her research interests are in the areas of applied mathematics, quantum cryptography, quantum key distribution, and coding computer simulations.