Modeling Continuous Time Optical Pulses in a Quantum Key Distribution Discrete Event Simulation

Logan O. Mailloux¹, Michael R. Grimaila¹, Douglas D. Hodson¹, L. Elaine Dazzio-Cornn¹, and Colin McLaughlin²
¹Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio 45433, United States
²Naval Research Laboratory, Washington, DC 20375, United States
¹{Logan.Mailloux, Michael.Grimaila, Douglas.Hodson, Laura.DazzioCornn}@afit.edu
²Colin.Mclaughlin@nrl.navy.mil

Abstract—Quantum Key Distribution (QKD) is an innovative technology that leverages the fundamental laws of quantum mechanics to securely distribute shared secret cryptographic keys. QKD technology, when paired with the one-time pad encryption algorithm, provides the opportunity for “unconditionally secure” communications between two parties. However, QKD is a nascent technology with non-ideal system implementations where design trade-offs in system architectures are not well understood due to the complexities of physical and system-level interactions. In this paper, we discuss modeling Continuous Time (CT) optical pulses in a hybrid Discrete Event Simulation (DES) framework built to enable performance analysis and characterization of current and future QKD system implementations. Modeling considerations, design decisions, and trade-offs for system-level modeling of QKD systems, and specifically the efficient modeling of CT optical pulses, is described. Finally, the strengths and weaknesses of modeling CT optical pulses in a DES framework are explored.

Keywords—Quantum Key Distribution; Model and Simulation; Discrete Event Simulation; Simulation Framework

I. INTRODUCTION

The beginnings of Quantum Key Distribution (QKD) can be traced back to Stephen Wiesner who developed the idea of securely encoding quantum information in conjugate basis sets during the late 1960s [1]. As a student at Columbia University, he described two applications for quantum coding: (1) a method for the creation of fraud-proof banking notes (i.e., quantum money) and (2) a method for the transmission of multiple messages in such a way that reading one of the messages destroys the others (i.e., quantum multiplexing). In 1984, Charles Bennett and Gilles Brassard operationalized this concept when they proposed the first QKD protocol (i.e., BB84) to securely distribute shared encryption key between two parties in the presence of an eavesdropper [2].

The unique nature of QKD necessitates that any interference on the key distribution channel leaves detectable fingerprints through increased error rates. Thus, QKD provides a secure key distribution technology that when paired with the One-Time Pad (OTP) encryption algorithm offers “unconditionally secure” communications regardless of an eavesdropper’s computational power [3, 4, 5].

A QKD usage scenario is depicted in Fig. 1, illustrating the customarily named sender “Alice” and receiver “Bob” in context with bulk encyptors. Alice and Bob are connected via a quantum channel and a classical channel in order to generate a shared secret key, K, used to encrypt network data. In the scenario, the plaintext message, m, is transformed into the ciphertext, E_k(m), transmitted over the Internet, and decrypted at the distant end where m = D_k(E_k(m)) using the secret key K.

Figure 1. QKD Context Diagram. Note: additional control signals and possible cryptographic parameters are not shown for simplicity.

Over the past decade there has been increasing interest in advancing QKD technology as a practical solution to enable unconditionally secure communications. However, QKD is a nascent technology and non-idealities exist within system implementations [6, 7, 8]. Furthermore, trade-offs in architectural design and implementation choices are not well understood due to the complexities of physical and system-level interactions [9]. To address these needs, the Authors have constructed a hybrid Discrete Event Simulation (DES) framework which enables the efficient modeling and analysis of current and future QKD implementations.

A concise background of QKD technology is provided in Section II to foster an understanding of modeling Continuous Time (CT) optical pulses. Section III introduces the hybrid QKD DES framework used to model, simulate, and analyze QKD systems. Section IV describes modeling considerations and design decisions for CT optical pulses. Section V explores the strengths and weaknesses of modeling CT optical pulses in a DES framework. Finally, conclusions and future work are proposed in Section VI.

II. BACKGROUND

QKD systems have been demonstrated in optical fiber and terrestrial free-space implementations, while initial commercial offerings are available from ID Quantique, MagiQ and others.
error rates.

errors during the key generation process through increased parties in such a way that an eavesdropper generates detectable protocol provides a means for passing secret keys between two an equal likelihood (i.e., 50%). In this manner, the BB84 not match Alice’s basis, a random result will be obtained with encoded bit with a high degree of accuracy. If Bob’s basis does measure the arriving polarized photon. If Bob’s randomly qubit by randomly selecting a basis (rectilinear or diagonal) to measure the basis alignment between Ali ce and Bob is perfect. If these assumptions are not valid when building real-world systems. For example, the BB84 protocol relies on the transmission of single photons, yet reliable on-demand single photon generation is not currently practical. Typically, QKD systems generate coherent optical pulses (with millions of photons) and attenuate optical pulses down to weak coherent pulses with a Mean Photon Number (MPN) of 0.1. A MPN of 0.1 implies a sub-quantum level optical pulse where only 1 in 10 pulses will contain a photon. While this significantly reduces the efficiency of the protocol, it is required to limit and bound the knowledge gained by an eavesdropper for secret key generation [5, 7].

An effective way to study such assumptions and implementation limitations is needed to adequately understand QKD system performance.

III. A HYBRID QKD SIMULATION FRAMEWORK

In order to study QKD implementations, the Authors desired to build a modular framework for the efficient modeling and simulation of QKD systems. More specifically, the Authors sought to build a flexible framework through modularization and parameterization where each device (or component) stands alone and can be individually conceptualized, implemented, and verified with the desire to enable performance analysis and system characterization of current and future QKD architectures. Designing and building the desired framework required understanding various modeling considerations and making numerous design decisions.

A. Model & Simulation Frameworks

In general, Model & Simulation (M&S) is used to analyze complex behaviors, processes, or interactions. A number of industries use M&S to study behaviors which are cost prohibitive to examine or unfeasible to reproduce otherwise (e.g., comparison of proposed systems, deep-space missions, the effects of natural disasters on a metropolitan area, etc.). The two main types of simulation paradigms are discrete (i.e., DES) — where state variables change only at specific points in time and continuous (i.e., CT) — where state variables change
Discrete simulation paradigms are commonly used to model manufacturing and production capabilities, logistics systems, and service queues; these process-oriented systems readily lend themselves to DES. Alternatively, continuous simulation paradigms are generally used to more precisely model detailed behaviors such as power consumption or signal strength.

Choosing an appropriate simulation framework is a critical design decision, one that enables and limits the entirety of the M&S solution. Competing simulation paradigms should be thoroughly examined by both the sponsor and developer to determine how to meet the intended purpose(s).

B. The QKD hybrid DES Framework

In some cases, the previously specified M&S paradigms can be combined to form a hybrid M&S solution. The Author’s QKD simulation framework (qkdX) is a hybrid M&S solution, where DES is used to schedule and execute the majority of transactions and continuous behaviors are modeled where appropriate (i.e., when studying CT optical pulses). In this way, the qkdX simultaneously supports parameterized physical devices, process-oriented controllers, and quantum phenomenon of weak coherent optical pulses. The framework can be used to study or compare competing architectures, assessments of new QKD protocols, or the study of environmental effects.

The QKD framework is built upon the open source modeling platform OMNet++ [17], where a unique device library is employed. This feature allows QKD systems to be modeled in a drag and drop fashion selecting from inventoried electrical, optical, and electro-optical devices. Further, the framework enables increasing levels of detail (i.e., fidelity) to be modeled through an object-oriented design. For example, interactions (or transformations) between optical pulses and optical devices can be modeled to a level of detail suitable for performance analysis with or without environmental effects.

This approach accommodates unknown future requirements across a broad spectrum of QKD system implementation possibilities, quantum communication protocols, and plausible electrical, optical, and electro-optical devices in both fiber and free-space applications. Furthermore, the object-oriented qkdX allows modelers to more quickly adapt new devices, protocols, and architectures for experimentation.

C. Ensuring Valid Model Representations

Flexibility to model QKD systems accurately (i.e., valid for a specific purpose) and efficiently (i.e., without significant rework) is an expressed objective of the QKD framework. Formally, the aggregation of various modeling components into valid system representations is described as model composability; it is a concept that enables modelers to assemble trustworthy system configurations from a variety of modeled elements to satisfy user requirements in a timely manner [18]. Composability requires that individual model elements be developed such that implementation details (e.g., parameter passing mechanisms, external data access, timing assumptions, etc.) are appropriately accounted for in all potential system configurations. To achieve model composability, detailed system elements should be verified through analytical means based on design specifications and legitimate behaviors.

Model composability is also achieved through conceptual model definition, to ensure simulated models will never enter an unexpected state regardless of what combination of elements are assembled [19]. Conceptual model definition and composability are of particular interest to our project as unique QKD systems are modeled to analyze performance of architectural implementations while optical pulses are passed from one device to another in a structured, assured manner.

The described framework expressly enables the modeling of valid QKD system representations for performance analysis and characterization. Specifically, the qkdX allows for quantum phenomenon and system-level interactions between hardware, software, and protocols to be modeled and studied at user specified levels of detail.

IV. MODELING CONSIDERATIONS AND DESIGN DECISIONS FOR CONTINUOUS TIME OPTICAL PULSES

Given infinite time and resources a modeler could conceivably describe every behavior of interest. However this is obviously never the case nor would such a complex effort provide the clarity desired to understand the QKD design and implementation trade space. In a resource constrained environment, model developers are forced to make design decisions and trade-offs. This forces sponsors and developers to more fully understand the system of interest, essential system behaviors, and intended purpose(s). These considerations should provide additional clarity and understanding in the study of difficult problems and complex phenomenon, resulting in more explicitly designed simulation capabilities and value-added simulation results.

Modeling CT optical pulses is one of the most critical design decisions within the QKD framework. QKD systems will generate hundreds of millions of optical pulses during secure key distribution, each of which will propagate through multiple optical devices potentially requiring complex mathematical transformations. As a consequence, an efficient mathematical representation must be chosen to model weak coherent optical pulses at the appropriate level of abstraction necessary to account for the desired resolution and accuracy.

While each pulse is most accurately represented as a CT optical pulse, it is computationally infeasible to model a
complete QKD system using CT simulation. Our approach is to model optical pulses as abstract, parameterized objects (i.e., pulses within temporal packets), where the optical pulse can be manipulated through individual parameters when performing simple transforms and fully reconstructed when performing complex transforms.

A. Modeling Light as Weak Coherent Optical Pulses

Light is electromagnetic radiation that can be viewed in two complementary ways: as an electromagnetic wave or as a stream of particles called photons [20]. We adopt the wave nature of light when calculating propagation through the QKD framework. This convention (wave nature) allows for standard calculations of optical effects such as propagation, dispersion, attenuation, or interference. Eq. (1) allows time-dependent propagation of the optical pulse’s electric field to be handled through individual components (e.g., fiber, wave plates, beam splitters, etc.) in the OMNeT++ environment. Defining the z-direction to be along the axis of travel through the optical fiber, the electric field vector of an optical wave then lies in the x-y plane, where:

\[ \vec{E}(t) = \begin{bmatrix} E_x(t) \\ E_y(t) \end{bmatrix} = E_0 e^{i\omega t} e^{i\phi} \begin{bmatrix} \cos \alpha \\ (\sin \alpha) e^{i\phi} \end{bmatrix} \]  

(1)

In this continuous-wave representation, the orientation of the electric field is given by \( \alpha \). The relative phase, or ellipticity, between the x and y components of the electric field is given by \( \phi \). The amplitude, relative phase, and angular frequency of the field are given by \( E_0 \), \( \theta \), and \( \omega_0 \), respectively. The angular frequency, \( \omega_0 \), is determined from the optical frequency \( f \) by the relation \( \omega_0 = 2\pi f \). The 2 x 1 column vector on the right side of Eq. (1) is the Jones vector representation of the electric field [21]. Upon passing through a linear optical device, the polarization state of the emerging light can be determined by multiplication of the Jones vector with an appropriate Jones matrix. Note: Jones calculation applies only to light which is fully polarized, as is generally the case for polarization based QKD systems. Randomly polarized, partially-polarized, and incoherent light cannot be represented in this manner.

Modeling pulsed optical sources requires the inclusion of a time-dependent power envelope, \( G(t) \), where the power envelope is proportional to the square of the electric field envelope. Thus, the model for the electric field of a pulsed optical source will take the form,

\[ \vec{E}(t) = \begin{bmatrix} \overline{E}_x(t) \\ \overline{E}_y(t) \end{bmatrix} = \sqrt{G(t)} E_0 e^{i\omega_0 t} e^{i\phi} \begin{bmatrix} \cos \alpha \\ (\sin \alpha) e^{i\phi} \end{bmatrix} \]  

(2)

This representation allows classical operations (or transformations) to be efficiently conducted on the optical pulse model. For example, integrating Eq. (2) over the duration of the pulse will yield the total energy contained in the pulse. The photon count of the pulse can then be determined by dividing the total pulse energy by the energy per photon at the given frequency, \( \omega_0 \).

Within the QKD framework we have chosen to use Poisson Distribution statistics to model the presence of photons in a weak coherent optical pulse. The distribution in Eq. (3) gives the probability of the presence of “k” photons in a single pulse given a MPN of \( \lambda \).

\[ P(k) = \frac{\lambda^k e^{-\lambda}}{k!} \]  

(3)

A stream of weak coherent optical pulses with, for example, a MPN=0.1 (\( \lambda=0.1 \)) will yield no photons per pulse with a probability of 90.48%, one photon per pulse with a probability of 9.05%, and two or more photons with an approximate probability of 0.47%.

B. QKD Laser Sources

An example of a commercial sub-nanosecond laser source is the ID Quantique (IDQ) id300 [22]. The id300 laser is capable of generating short pulses at a wavelength of 1310 nm or 1550 nm. The laser source, based on Fabry-Perot (FP) or on distributed-feedback (DFB) laser diodes, is externally triggered to produce sub-nanosecond laser pulses with a pulse rate ranging from 0 to 500 MHz. Fig. 3 shows the time profile of the optical pulse for the id300 laser source when triggered by a 1 MHz clock source [22]. Note that the peak of the pulse is specified as 0 dBm (i.e., 1 mW) and the nominal pulse duration is specified as 0.3 ns or 300 ps Full Width at Half Maximum (FWHM).

![Figure 3. id300 Laser Pulse Specification [22].](image)

Fig. 4 shows Lydersen et al.’s measured time profile of the IDQ id300 laser source when using a 12.5 GHz sampling oscilloscope and a 45 GHz optical probe [23]. While the peak of the measured waveform is close to that specified in the id300 data sheet, the pulse shape is quite different from that depicted in Fig. 3.

C. Efficient Modeling of Continuous Time Optical Pulses

While the time profile of each pulse could be represented by a set of (time, value) pairs collected in these laboratory measurements, the Authors choose to represent the coherent optical pulse as a CT optical pulse. We believe this representation is more conducive for modeling photon detection and performing interference calculations necessary to understand the impact of quantum interactions on system performance.
As a consequence, we approximated the measured pulse’s time profile using a sum of Gaussian functions [24]. From Lydersen et al.’s experimental measurements, a three Gaussian curve approximation was made as shown in Fig. 5 and detailed in Table 2. Comparing the measured and approximated optical power waveforms, the adjusted R square fit value $R^2$ is 0.9962, which constitutes a reasonably good fit [25].

Approximating the measured shape with Gaussian waveforms allows the QKD framework to take advantage of optimized Gaussian integration techniques and reduces the computational burden placed on the simulation platform.

Table 2. Parameters to Approximate Continuous Time Optical Pulse

<table>
<thead>
<tr>
<th>Gaussian Curve</th>
<th>Gaussian Amplitude</th>
<th>$\mu$ [ps]</th>
<th>$\sigma$ [ps]</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>45.5</td>
<td>95.48</td>
<td>19.82</td>
</tr>
<tr>
<td>2</td>
<td>38.1</td>
<td>181.12</td>
<td>58.14</td>
</tr>
<tr>
<td>3</td>
<td>4.76</td>
<td>352.32</td>
<td>49.02</td>
</tr>
</tbody>
</table>

D. Object-Oriented Modeling of Optical Pulses

The qkdX employs an object-oriented design to efficiently model weak coherent optical pulses. Several related classes define the CT optical pulse as shown in Fig. 6. The abstract Pulse class serves as the principle interface for a wide variety of pulse definitions. This design allows end users, analysts, or modelers to define pulse representations at an adequate level of detail (i.e., fidelity) suitable to the desired experimental purpose(s).

Each pulse has a specified duration that serves as a windowing function to identify the interval of time which the pulse covers. The duration is represented in the simulator using a double precision variable with a value greater than or equal to zero. The duration is a required parameter to facilitate the efficient processing of optical pulses at the detectors. As described in Eq. (2), each pulse has an electric field amplitude $E_0$ named amplitude, an angular frequency $\omega_0$ named centralFrequency, a global phase $\theta$ named globalPhase, an angle of the vector with respect to the x axis $\alpha$ named Orientation, and a relative phase $\phi$ named ellipticity. Additionally, the pulse class contains functional calls associated with calculating the pulse energy getPulseEnergy(), peak power getPeakPower(), and MPN getMPN().

The typical use of the Pulse class will be to represent weak coherent pulses, however it is also desirable to provide a means to represent long duration, Continuous Wave (CW) light. For this reason, we employ inheritance to capture the unique characteristics of each type of coherent pulse represented as CWPulse or ShapedPulse. In the case of weak coherent optical pulses, we define the pulse shape using a composite pattern. This enables optical pulse shapes to be modeled using multiple Gaussians curves to approximate the optical pulse shape as shown in Fig. 5. Each of the Gaussian curves has an associated amplitude, mean, and standardDeviation. If pulseType=CW, none of the Gaussian shape parameters described are used.

The pulse class design simplifies and centralizes the modeling effects due to transmission through optical fiber and transformations associated with optical devices as represented within a modeled QKD architecture. For example, consider a pulse passing through a simple optical attenuator as shown in Fig. 7. Only the e-field magnitude $E_0$ of the optical pulse is reduced by the attenuator, while the pulse shape remains unchanged. Therefore, the object’s amplitude attribute is efficiently updated without using unnecessary computational resources to perform integration.
Centralizing these calculations within the pulse class allows for simplified modeling of optical components throughout the entire QKD framework. Additionally, because all calculations are centralized, efficient integration algorithms can be more easily localized and applied.

V. STRENGTHS AND WEAKNESSES OF MODELING CONTINUOUS TIME OPTICAL PULSES IN A QKD DES

In this section we explore the strengths and weaknesses of modeling CT, weak coherent optical pulses in a QKD DES framework. In DES future events are scheduled and stored, where the next scheduled event is ‘jumped to’ saving computational resources between scheduled events. An equivalent continuous model would require constant processing regardless of when the next transaction occurs, causing undue processing burden and potentially generating significant amounts of superfluous data. For systems that have considerable dead time between transactions, the DES modeling construct is generally advantageous. However, this efficiency begins to fall away with large numbers of scheduled events and increasingly smaller dead times, which is the case for QKD systems. For example, during operation potentially millions of events are scheduled with delays on the order of nano (10^{-9}) and pico (10^{-12}) seconds placing a significant burden on scheduling resources.

A. STRENGTHS OF DES FOR MODELING QKD SYSTEMS

While attempting to discretely model continuous quantum phenomenon may seem counter-intuitive, an investigation of quantum simulation literature demonstrates that continuous simulations of QKD systems are generally more complex than necessary and even impractical to model and/or simulate for system-level behaviors [26]. For example, the wave-particle duality of light in a continuous simulation would require a complete characterization of the optical path as each pulse is created, adding significant computational overhead and negating the desired temporal interactions of a system-level simulation [26].

In the QKD DES framework, these complexity shortcomings are efficiently overcome by probabilistically modeling the frequency of a photon striking the detector after propagating through the system as described in Eq. (3). Despite the heavy scheduling burden, the DES paradigm allows for system-level interactions and CT optical pulses to be modeled and simulated more efficiently than continuous simulations.

Additionally, scheduled events in DES highlight critical dependencies in the subject system. Identifying these system-level interactions and temporal relationships can lead to additional clarity when studying complex systems. This feature of DES is particularly useful when attempting to gain further understanding of QKD systems or conducting performance analysis and characterization of competing architectures.

B. WEAKNESSES OF DES FOR MODELING QKD SYSTEMS

Lower fidelity in DES is a limiting issue that needs to be fully understood because it can lead to inaccurate results and incorrect system behaviors. Consider for example, the optical pulse shown in Fig. 4, it has a duration of approximately 400 ps, while the optical attenuator shown in Fig. 7 has a scheduled delay of 5 ps (a significantly smaller time elapse). In the QKD DES framework, the pulse is received, processed, and scheduled for the next event according to the attenuator’s 5 ps delay. There is little consideration for the 400 ps pulse propagation time through the attenuator, which can result in erroneous representations of CT coherent optical pulses within the qkdX.

Figs. 8(a-c) demonstrate the problematic nature of low fidelity DES in the case where conflicting events occur within the optical pulse’s 400 ps duration. Each of these scenarios can result in invalid outputs because of scheduling constraints inherent in DES. In Fig. 8(a) a conflicting environmental message indicates an “overheat” of the attenuator such that the device’s performance and output pulse should be severely degraded. In Fig. 8(b) a continuous light source is shone into the attenuator input which should overpower the weak optical pulse output. In Fig. 8(c) multiple overlapping pulses should cause interference on the output pulse.
VI. CONCLUSIONS

This research is part of an ongoing effort to model, simulate, and analyze QKD system architectures. This paper discusses considerations, design decisions, and trade-offs for modeling CT optical pulses in a hybrid QKD DES framework. A discussion of modeling physical and system-level interactions is facilitated through a QKD simulation framework, and specifically in the modeling of CT weak coherent optical pulses. Strengths and weaknesses of modeling CT optical pulses in a DES framework are explored. Future work includes modeling alternative QKD encoding schemes (i.e., phase-based and entanglement) and free-space implementations.

DISCLAIMER

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

REFERENCES