Modeling and Studying Measurement Device Independent Quantum Key Distribution Systems

M. B. Russell, L. O. Mailloux, M. R. Grimaila, and D. D. Hodson
Air Force Institute of Technology, Wright-Patterson AFB, OH USA 45433

I. Studying QKD Implementation Non-Idealities

Quantum Key Distribution (QKD) systems generate and distribute shared secure cryptographic keying material; however, real-world QKD systems are built from non-ideal components and processes which can negatively impact their performance and security [1]. Thus, an efficient means for studying these complex systems is warranted – one which minimizes the extensive resources required to build QKD architectures, conduct tradeoff analysis, and effectively make design decisions (e.g., time, material, expertise, etc.). To achieve this objective, our research effort is focused on using Modeling and Simulation (M&S) to understand the relationships between design parameters, performance, and security. Further, M&S allows functional dependencies to be studied in a cost effective manner [2]. Specifically, we developed a Bell State Analyzer (BSA) model in order to study Measurement Device Independent (MDI) QKD using the quantum key distribution eXperimentation (*qkdX*) modeling framework [3].

II. The QKD Modeling Framework

The primary objective of the *qkdX* framework is to enable the rapid and efficient modeling, simulation, and analysis of current and proposed QKD system implementations using varying levels of abstraction [3]. The *qkdX* framework is built upon OMNeT++, a discrete-event modeling environment, whose architecture lends itself to a wide variety of application domains [4]. In order to model QKD systems, OMNeT++'s module, message, and channel abstractions are extended to represent optical components, fiber channels, laser pulses, protocols, and processes. Our research defined these abstractions and created a variety of concrete models, resulting in a library of component and controller models. These models have been used to build a variety of QKD simulations.

The framework also defines higher-level aggregate models to represent subsystems and system-level controllers. This capability allows users to more easily model and analyze QKD systems in order to answer design and configuration questions at varying levels of fidelity and study behaviors of interest.

In Fig. 1, the *qkdX* framework (shown in yellow) is built as domain specific extensions to the abstract OMNeT++ discrete event simulation modules (shown in red). Using *qkdX* modules (e.g., lasers, fiber channels, beam splitters, etc.), researchers can build custom, standalone executables (i.e. simulations) to represent different QKD system architectures and attacks (shown in orange).

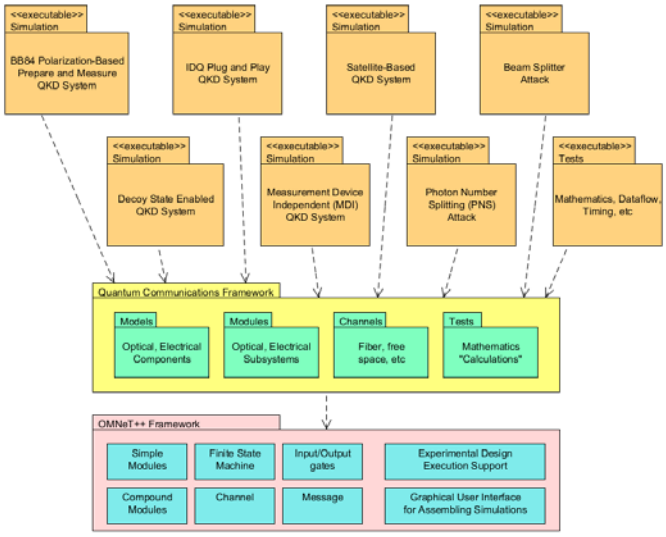

Fig. 1. The QKD modeling framework allows users to more easily build and analyze QKD systems of interest (i.e., protocols, software, and hardware).

III. Modeling MDI-QKD

Leveraging this capability, we have begun to investigate MDI-QKD – a recent quantum communication protocol purported to be immune from detector and side-channel attacks [5]. MDI-QKD is appealing because it is designed to execute on untrusted receiver hardware; thus avoiding the most popularly targeted vulnerability in QKD systems – non-ideal Single Photon Detectors (SPDs). For a more detailed discussion of the MDI protocol, see [5], [6], and [7].

A. The MDI-QKD Bell State Analyzer

Our focus on MDI centers on modeling and simulation of the Bell State Analyzer (BSA). As our simulation model shows in Fig. 2, MDI-QKD takes advantage of the quantum entanglement inherent in a BSA to generate keying material between "Alice" and "Bob" using untrusted hardware typically described as "Charlie/Eve" [5]. For example, as Table I indicates, successful Bell State Measurements (BSM) occurs when detections are registered at two complementary Single Photon Detectors (SPDs) at orthogonal outputs of the polarizing beam splitters. Combining the detection outcomes with Alice/Bob's respective secret knowledge of the photons' originally encoded state, Alice and Bob are able to generate shared secret key material without disclosing any additional information to Eve. Thus, Eve knows when Charlie's detectors "clicked" but has no information regarding the secret key bits.

TABLE I
BELL STATE DETECTIONS [5]

State	Detector Click
$\|\psi^+\rangle$	spd_H1 and spd_V1 or spd_H2 and spd_V2
$\|\psi^-\rangle$	spd_H1 and spd_V2 or spd_H2 and spd_V1

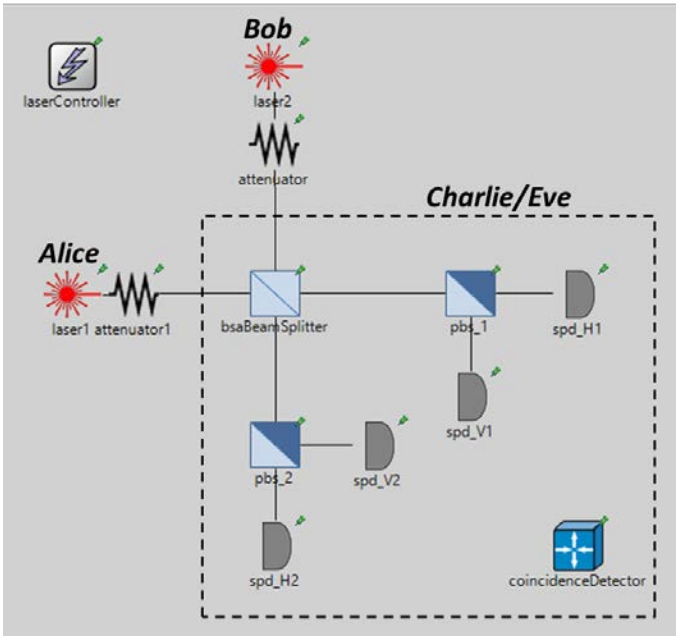

Fig. 2. A Bell State Analyzer (BSA) model for studying Measurement Device Independent QKD systems.

B. Modeling the Bell State Analyzer (BSA)

The primary component of the BSA is the 50:50 beam splitter "bsaBeamSplitter" near the center of Fig. 2. As modelled, the bsaBeamSplitter performs interference calculations on photons which arrive simultaneously at each input port. When such an event occurs, the beam splitter compares how similar the photons are, and decides which port(s) they should exit according to the Hong-Ou-Mandel (HOM) effect [8]. For example, if the two incident photons are identical with the same polarization encoding they should always exit the same port without modification.

If the photons have oppositely encoded polarizations, they will randomly exit from the same or different port(s). Additionally, the BSA beam splitter places the photons in a maximally entangled state since it erases any previous "which way" information. Moreover, as the entangled photons propagate towards the Polarizing Beam Splitters (PBS), their measurement outcomes must be correlated. To accomplish this behavior, entangled photons are given a reference to a shared "BellState" object that stores: (i) which of the four Bell states the pair is in; (ii) whether the pair has been measured; and (iii) the measurement basis and outcome state when measured. For example, when the first entangled photon reaches a PBS, the PBS measures the photon in the rectilinear basis, and if entangled, the photon queries its shared BellState object for the appropriate result. If the BellState object has not yet collapsed, it calculates the probabilities of each possible two-photon state (i.e., $|HH\rangle$, $|HV\rangle$, $|VH\rangle$, or $|VV\rangle$) and randomly collapses into one of them, returning the value of the first photon in the quantum system as the measurement result. When the second photon reaches the PBS, the same process occurs; however, this time the BellState has already collapsed and the value of the second photon in the collapsed state is returned as the measurement result. As a final step, the entanglement link is destroyed as the two photons have decohered (i.e., they are no longer entangled).

IV. MDI-QKD SIMULATION RESULTS

To evaluate the model described in Section III, each valid combination of input photon polarizations (i.e., HH, VV, HV, VH, DD, AA, DA, AD) was tested by firing 100,000 laser pulses through the model and monitoring the successful BSM detections counts. The results of these trials indicated that our model was able to replicate the expected theoretical distributions of Bell state detections for single photon Fock states (see Table II) and for weak coherent pulses with a Mean Photon Number (MPN) of 0.5 (see Table III).

The theoretical values presented in Table II and III are the probabilities that a successful Bell state projection will result in either a $|\psi^+\rangle$ or $|\psi^-\rangle$ measurement. For example, when two single photons are encoded in the rectilinear basis as HV, Table II shows that $|\psi^+\rangle$ and $|\psi^-\rangle$ should be detected with equal probability. In contrast, if two weak coherent pulses are encoded as DD in the diagonal basis, Table III indicates that a successful BSM result has a 75% chance of registering $|\psi^+\rangle$ and a 25% chance of registering $|\psi^-\rangle$. The simulation results presented in Table II and III are the likelihoods of each measurement result occurring given a successful BSM, calculated from the Bell state detection counts recorded during the simulation. Fig. 3 presents these detection counts for the weak coherent pulse trials.

TABLE II
SINGLE PHOTON FOCK STATE PULSE RESULTS

Encoded Pair	BSM Result			
	Theoretical [9]		Simulation Results	
$\oplus$ Basis	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
HH	0	0	0.000	0.000
VV	0	0	0.000	0.000
HV	0.5	0.5	0.500	0.500
VH	0.5	0.5	0.500	0.500
$\otimes$ Basis	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
DD	1	0	1.000	0.000
AA	1	0	1.000	0.000
DA	0	1	0.000	1.000
AD	0	1	0.000	1.000

TABLE III
WEAK COHERENT PULSE RESULTS

Encoded Pair	BSM Result			
	Theoretical [9]		Simulation Results	
⊕ Basis	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
HH	0	0	0.000	0.000
VV	0	0	0.000	0.000
HV	0.5	0.5	0.502	0.498
VH	0.5	0.5	0.502	0.498
⊗ Basis	$\|\psi^+\rangle$	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\psi^-\rangle$
DD	0.75	0.25	0.743	0.257
AA	0.75	0.25	0.740	0.260
DA	0.25	0.75	0.255	0.745
AD	0.25	0.75	0.259	0.741

V. FUTURE WORK

This model is an initial, ideal model of a BSA for studying polarization-based MDI-QKD. By creating the components and developing the BSA model, we have provided an extensible foundation for modeling and studying device non-idealities such as component losses, manufacturing defects, misalignment limitations, physical disturbances, detector inefficiencies, and other sources of noise.

Overall, the goal of this research is to provide an understanding of how practical implementation non-idealities impact the MDI protocol's security and performance to include:

1. What behaviors should be implemented in a MDI system model to identify, formalize, and analyze the protocol's security and performance?
2. How do device imperfections and practical engineering limitations in timing synchronization, polarization encoding, and variations in pulse duration, wavelength, shape, and MPN impact the protocol's ability to operate on untrusted hardware?
3. How can the differences between the theoretical MDI protocol and realized systems be characterized towards system certification?

VI. CONCLUSION

In this abstract, we introduced a BSA model which accurately represents the HOM effect and provides a means to entangle pulses incident on a 50:50 beam splitter. This model provides a basis for further studying the performance and security of MDI-QKD systems.

VII. DISCLAIMER

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

REFERENCES

[1] V. Scarani and C. Kurtsiefer, "The black paper of quantum cryptography: real implementation problems," *Theoretical Computer Science*, vol. 560, pp. 27-32, 2014.

[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 and Privacy*, vol. 13, no. 1, pp. 30-40, 2015.

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

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

[5] H.-K. Lo, M. Curty and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, 130503, 2012.

[6] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian and H. K. Lo, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 112, no. 19, 190503, 2014.

[7] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, no. 6, pp. 397-402, 2015.

[8] C. K. Hong, Z. Y. Ou and L. Mandel, "Measurement of subpicosecond time intervals between two photons by interference," *Phys. Rev. Lett.*, vol. 59, no. 18, pp. 2044-2046, 1987.

[9] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporao and J. P. von der Weid, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," *Phys. Rev. A*, vol. 88, no. 5, 2013.

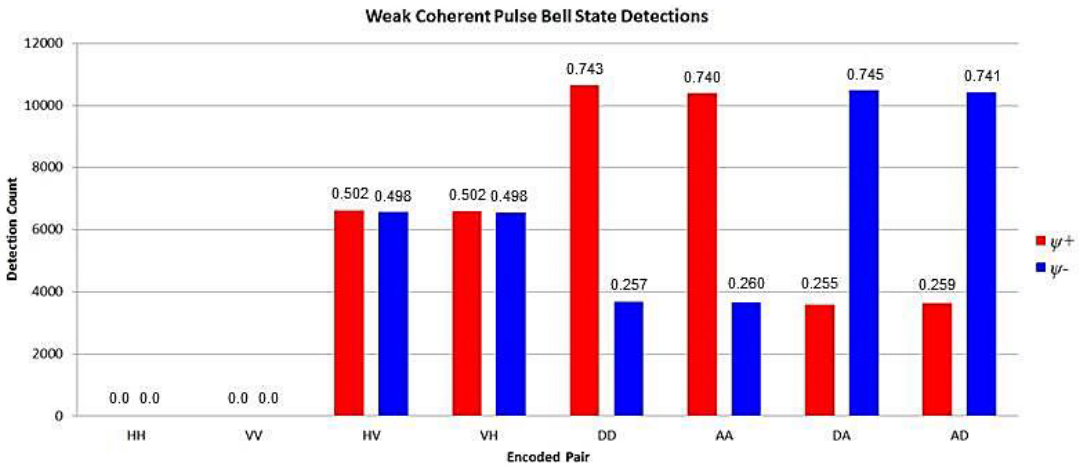

Fig. 3. Graph of weak coherent pulse bell state detection counts for pulses with a MPN of 0.5. The calculated likelihood of the given detection result appears above each column.