Abstract—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. In this work, we developed a Bell State Analyzer model in order to study Measurement Device Independent (MDI) QKD using the quantum key distribution eXperimentation (qkdX) modeling framework. Modeling and Simulation (M&S) provides an extensible means for studying device non-idealities such as component losses, manufacturing defects, misalignment limitations, physical disturbances, detector inefficiencies, and other sources of noise in MDI QKD. The Bell State Analyzer model is also applicable to the wider field of quantum communication including quantum teleportation, quantum networking, and quantum repeaters.

Index Terms—Bell State Analyzer, Measurement Device Independent, Quantum Key Distribution, Model and Simulation

I. INTRODUCTION

Quantum Key Distribution (QKD) systems generate and distribute shared cryptographic keying material [1]; however, real-world QKD systems are built from non-ideal components and processes which can negatively impact their performance and security [2]. Thus, an efficient means for studying these complex cybersecurity systems is warranted—one which minimizes the extensive resources required to build QKD architectures, conduct tradeoff analysis, and effectively make design decisions. To achieve this objective, our research effort is focused on using Modeling and Simulation (M&S) to further understand the relationships between design parameters, performance, and security. Further, M&S allows various protocol and implementation dependencies to be studied in a cost-effective manner (e.g., time, material, expertise, etc.) [3]. In this work, 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 [4].

II. THE qkdX 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 systems implementations using varying levels of abstraction [4]. Shown in Fig. 1, the qkdX framework (depicted in yellow) is built as a domain specific extension to OMNeT++ (depicted in red) [5]. OMNeT++ is a discrete-event modeling environment, whose architecture lends itself to a wide variety of application domains. In order to model QKD systems (i.e., a combination of protocols, software, and hardware), OMNeT++’s module, message, and channel abstractions are extended to represent optical components, fiber channels, laser pulses, protocols, and processes. Using the 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).

Thus, the qkdX framework defines a variety of processing abstractions and concrete models which result in a library of components and controller models. This capability allows users to more easily model and analyze QKD systems at the appropriate level of fidelity to answer various research questions (e.g., communication protocol efficiency or low-level design considerations).

Fig. 1. The Quantum Key Distribution (QKD) modeling framework (qkdX) allows users to more easily build and analyze QKD systems.

The remainder of this paper describes the MDI QKD requirements, implementation, and testing for a simple (i.e., ideal) BSA model within the qkdX framework.
III. MEASUREMENT DEVICE INDEPENDENT (MDI) QKD

Recent advances in QKD led to the development of Measurement Device Independent (MDI) QKD – a protocol which attempts to mitigate detector implementation non-idealities, which are the target of several recent attacks [6]. MDI QKD utilizes a unique design in which two users, Alice and Bob, use an untrusted third-party, Charlie, to generate secret key. As typically described, Alice and Bob send BB84 encoded photons to Charlie, who performs a Bell State Measurement (BSM) when the photons arrive. Charlie publicly announces his measurement results to Alice and Bob, who combine this information with their private encoded state information to correctly correlate their bits. In this configuration, Charlie is only able to collect information about the joint state of Alice’s and Bob’s photons via the BSM – no actual keying material is revealed. Thus, Charlie is considered an untrusted Charlie entity (often named “Charlie/Eve”), removing the threat of detector side channel attacks [6]. In addition to increasing the overall security, this allows systems to utilize detectors produced by untrusted sources [7]. For a detailed discussion of the MDI QKD protocol and existing experimental implementations, see [8], [9], [10], [11], [12].

A. Bell State Analyzer (BSA)

The most crucial component of a MDI QKD system is Charlie’s BSA. Shown in Fig. 2, a simple BSA model is depicted as a 50:50 beam splitter with two inputs (a and b) and two outputs (c and d). While seemingly simple, understanding its two-photon BSM behavior requires familiarity with what is known as the Hong-Ou-Mandel (HOM) effect [13].

![Fig. 2. A 50:50 beam splitter with two input ports a and b, and two output ports, c and d.](image)

When two identical photons perfectly overlap in the inputs of the beam splitter, both will always exit the same output port due to quantum interference. Mathematically, we can describe this behavior using creation operators and a unitary, symmetric beam splitter transformation [14]

$$B = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$$  \hspace{1cm} (1)

where the $i = \sqrt{-1}$ entries represent a phase shift of $\pi/2$ if the photon is transmitted. Next, let the operators $a^\dagger$, $b^\dagger$, $c^\dagger$, and $d^\dagger$ represent the creation of single photons in their respective ports (as labeled in Fig. 2). When two photons are incident in the two input ports (a and b), the beam splitter input state can be written as

$$|in\rangle = a^\dagger b^\dagger |0,0\rangle = |1,1\rangle_{ab}$$  \hspace{1cm} (2)

where $|0,0\rangle$ is the two-photon vacuum state. Applying the beam splitter transformation to this input state gives

$$|out\rangle = (\frac{c^\dagger + id^\dagger}{\sqrt{2}})(\frac{ic^\dagger + d^\dagger}{\sqrt{2}})|0,0\rangle_{cd}$$

$$= \frac{1}{2} (c^\dagger + id^\dagger)(ic^\dagger + d^\dagger)|0,0\rangle_{cd}$$

$$= \frac{1}{2} (c^\dagger c^\dagger + d^\dagger d^\dagger)|0,0\rangle_{cd}$$

$$= \frac{1}{\sqrt{2}} (|2,0\rangle_{cd} + |0,2\rangle_{cd})$$  \hspace{1cm} (3)

This indicates that the two photons will both appear in output port c or d, but never in separate output ports. Thus, in an ideal configuration, if we placed Single Photon Detectors (SPD) at each output port and repeatedly inserted pairs of indistinguishable photons into ports a and b, simultaneous clicks (i.e., known as coincidences) should never occur.

However, in non-ideal configurations, the number of coincidences detected is a function of the distinguishability between the input two photons (commonly referred to as their indistinguishability) [13]. The photons’ distinguishability is primarily affected by its relative frequency, polarization, and temporal properties [12]. For example, adjusting the temporal offset between otherwise identical photons incident on the beam splitter produces the well-known “HOM dip” as shown in Fig. 3 [13].

![Fig. 3. Varying the difference between the two photons’ path length to the beam splitter, produces a temporal offset, which results in the classic HOM dip plot [13].](image)

B. The Bell State Measurement (BSM)

BSAs leverage both the HOM effect and the entanglement characteristics of 50:50 beam splitters to measure incoming photons in the Bell basis, an operation known as a Bell State Measurement (BSM) [6]. The Bell basis consists of four maximally entangled states. For rectilinear polarization, these states can be written [15]

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle|H\rangle \pm |V\rangle|V\rangle)$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle \pm |V\rangle|H\rangle)$$  \hspace{1cm} (4)
A simple BSA device is presented in Fig. 4. If the photons are distinguishable, HOM interference is not seen, and the two photons entering the beam splitter will independently choose a random port from which to exit. This process erases the “which way” information in the photons, causing them to enter an entangled state. For orthogonally polarized photons, this state is one of the maximally entangled Bell states \(|\psi^\pm\rangle\). Bosonic symmetry requires that two photons randomly exiting the same port be entangled into \(|\psi^+\rangle\), while photons randomly exiting different ports will be entangled into \(|\psi^-\rangle\) [14]. Therefore, if photons are incident on the beam splitter, and the detectors record a coincidence (i.e., simultaneous clicks), we can determine that the two photons were in the \(|\psi^-\rangle\) state. For example, consider the state \(|\psi^-\rangle\). If exiting from the same output port, the photons will be separated at the PBS and cause a coincidence between detectors in the same arm of the BSA, resulting in a successful \(|\psi^+\rangle\) BSM. If exiting from different ports, the PBSs will separate the photons, resulting in a coincidence of detectors assigned to orthogonal polarizations in opposite arms of the BSA. This gives a successful \(|\psi^-\rangle\) BSM.

C. Possible Bell State Measurement (BSM) Outcomes

To understand the results of the BSM further, we must examine the possible measurement outcomes of each valid photon input combination summarized in Fig. 6. A valid input occurs when the senders “Alice” and “Bob” encode their photons in the same BB84 basis (e.g., both rectilinear or both diagonal). If Alice and Bob send photons with identical encoding in the rectilinear basis (Case 1), the photons will exit the same port of the beam splitter due to the HOM effect. The PBS will then direct both photons to the same detector because of their matching polarization, resulting in no coincidence detection and a failed BSM.

If Alice and Bob send photons in orthogonal rectilinear polarizations (Case 2), the photons will randomly either exit the same output port in the \(|\psi^+\rangle\) state or different output ports in the \(|\psi^-\rangle\) state. If exiting from the same output port, the photons will be separated at the PBS and cause a coincidence between detectors in the same arm of the BSA, resulting in a successful \(|\psi^+\rangle\) BSM. If exiting from different ports, the PBSs will separate the photons, resulting in a coincidence of detectors assigned to orthogonal polarizations in opposite arms of the BSA. This gives a successful \(|\psi^-\rangle\) BSM.

If Alice and Bob send photons with identical encodings in the diagonal basis (Case 3), the photons will exit the same port of the first beam splitter due to the HOM effect. However, because the photons are diagonally encoded, there is a 50% chance that the photons will randomly collapse to opposite rectilinear polarizations. Thus, there is a 50% chance that a \(|\psi^+\rangle\) state will be registered and 50% chance of a failure.

If Alice and Bob send photons in orthogonal diagonal polarizations (Case 4), the photons will randomly exit either the same output port in the \(|\psi^+\rangle\) state or different output ports in the \(|\psi^-\rangle\) state, just like the analogous states in the rectilinear basis. However, these states behave differently at the PBS due to their entanglement. The following section explains the behavior of two photon polarization states (including entangled states) when measured in an arbitrary basis.

D. Measuring Two-Photon Polarization States

Polarization state functions can be rotated to determine the measurement outcome probabilities in different bases. For example, consider the state

\[
|\psi\rangle = \alpha|0\rangle + \beta|1\rangle
\]

in basis \(X\), where we desire to determine the value of this state in basis \(Y\), \(|\psi\rangle_Y\). First, we formally define \(X\) and \(Y\) as

\[
X = \{|0\rangle_X, |1\rangle_X\}
\]

\[
Y = \{|0\rangle_Y, |1\rangle_Y\}
\]

TABLE I

<table>
<thead>
<tr>
<th>Bell State Measurement Results [6]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bell state</td>
</tr>
<tr>
<td>--------------------------------</td>
</tr>
<tr>
<td>(</td>
</tr>
<tr>
<td>(</td>
</tr>
</tbody>
</table>

Fig. 4. A 25% efficient BSA device. A simultaneous click on detectors D1 and D2 indicates a successful projection onto the \(|\psi^-\rangle\) state.

Fig. 5. A 50% efficient polarization-based BSA device. A click on detectors D1H & D2V or D1V & D2H indicates a successful projection onto the \(|\psi^+\rangle\) state. A click on detectors D1H & D1V or D2H & D2V indicates a successful projection onto the \(|\psi^-\rangle\) state.

Fig. 5. A 50% efficient polarization-based BSA device. A click on detectors D1H & D2V or D1V & D2H indicates a successful projection onto the \(|\psi^+\rangle\) state. A click on detectors D1H & D1V or D2H & D2V indicates a successful projection onto the \(|\psi^-\rangle\) state.
Given that the transformation from X to Y can be written as a rotation of angle $\theta$, where $\theta$ is the angle from X to Y, we have

$$
\begin{bmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{bmatrix} \alpha_X^Y = \gamma
$$

where

$$\gamma = \begin{bmatrix} |0\rangle_Y & |1\rangle_Y \end{bmatrix}
$$

from [16] where

$$|\gamma\rangle_Y = \gamma|0\rangle_Y + \delta|1\rangle_Y
$$

Applying the matrix formula above, we find that $|\gamma\rangle_X$ can be written in the Y basis as

$$|\gamma\rangle_Y = (\alpha \cos \theta + \beta \sin \theta)|0\rangle_Y + (\beta \cos \theta - \alpha \sin \theta)|1\rangle_Y
$$

Consider, for example, the rectilinear basis $\oplus$ and the diagonal basis $\otimes$, defined as

$$\oplus = \{|H\rangle, |V\rangle\}
$$

$$\otimes = \{|D\rangle, |A\rangle\}
$$

where $|D\rangle = |45^\circ\rangle$ and $|A\rangle = |135^\circ\rangle$. If we desire to measure a diagonal state in the rectilinear basis (i.e., map $\otimes \rightarrow \oplus$), then $\theta = -\pi/4$. Thus, $|D\rangle$ can be written in the $\oplus$ basis as

$$|D\rangle = \cos\left(-\frac{\pi}{4}\right)|H\rangle - \sin\left(-\frac{\pi}{4}\right)|V\rangle
$$

$$= \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)
$$

This procedure for rotating single photon polarization states between bases is straightforward and extends to two photon states as well. Consider the non-entangled, two photon state $|D\rangle|A\rangle$ where converting to the $\oplus$ basis gives

$$|D\rangle|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle) \frac{1}{\sqrt{2}}(-|H\rangle + |V\rangle)
$$

$$= \frac{1}{2}(-|H\rangle|H\rangle + |H\rangle|V\rangle - |V\rangle|H\rangle + |V\rangle|V\rangle)
$$

Thus, the state $|D\rangle|A\rangle$ has an equal probability of being measured as any of the possible two photon states in the $\oplus$ basis. In general, it is useful to define a transformation matrix to convert the joint state of two photons in the $X$ basis to a joint state of two photons in the $Y$ basis. If we define the $V$ and $W$ bases as

$$V = \{0\rangle_x |0\rangle_x, |0\rangle_x |1\rangle_x, |1\rangle_x |0\rangle_x, |1\rangle_x |1\rangle_x\}
$$

$$W = \{0\rangle_y |0\rangle_y, |0\rangle_y |1\rangle_y, |1\rangle_y |0\rangle_y, |1\rangle_y |1\rangle_y\}
$$

we may generate the matrix of transformation:

$$
[T]_{V,W} =
\begin{bmatrix}
\cos^2 \theta & \sin \theta \cos \theta & \sin \theta \cos \theta & \sin^2 \theta \\
-\sin \theta \cos \theta & \cos^2 \theta & \sin^2 \theta & -\sin \theta \cos \theta \\
-\sin \theta \cos \theta & -\sin^2 \theta & \cos^2 \theta & \sin \theta \cos \theta \\
\sin^2 \theta & -\sin \theta \cos \theta & -\sin \theta \cos \theta & \cos^2 \theta
\end{bmatrix}
$$

From this transformation, we are particularly interested in the behavior of maximally entangled Bell states. The Bell states in the $V$ basis are

$$|\phi^\pm\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_x |0\rangle_x \pm |1\rangle_x |1\rangle_x),
$$

$$|\psi^\pm\rangle_V = \frac{1}{\sqrt{2}}(|0\rangle_x |1\rangle_x \pm |1\rangle_x |0\rangle_x)
$$

Written in vector form, the states $|\phi^+\rangle_V$, $|\phi^-\rangle_V$, $|\psi^+\rangle_V$, and $|\psi^-\rangle_V$ are
Int'l Conf. Scientific Computing | CSC'17 | 131

\[
\begin{bmatrix}
\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\
\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\
0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\
0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & -1 \\
0 & 1 & 0 & -1 \\
\end{bmatrix}
\]

(16)

Projecting into the \( W \) basis (left multiplying by \([T]_{W,v}\)) gives

\[
\begin{bmatrix}
0 \\
0 \\
1 \\
1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
\cos^2 \theta - \sin^2 \theta \\
\cos^2 \theta - \sin^2 \theta \\
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\end{bmatrix}
\]

(17)

\[
\begin{bmatrix}
1 & 0 & 1 & 0 \\
0 & 1 & 0 & -1 \\
1 & 0 & 1 & 0 \\
0 & 1 & 0 & -1 \\
\end{bmatrix}
\]

(18)

Since these are wave functions, the probability of each outcome is found by component-wise squaring the above vectors. For example, the expected results of measuring a diagonally encoded Bell state in the rectilinear basis can be found by setting \( \theta = -\pi/4 \) and simplifying the above expressions:

\[
\begin{bmatrix}
0 \\
0 \\
1 \\
1 \\
\end{bmatrix}
\]

\[
\begin{bmatrix}
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\cos^2 \theta \cos \theta - \sin^2 \theta \\
\end{bmatrix}
\]

IV. THE BELL STATE ANALYZER MODEL

Fig. 7 presents an initial, ideal BSA model created using the \( qkdX \) modeling framework. Key additions to achieve the desired BSM capability include: (i) a BsaBeamSplitter module that implements the desired HOM behavior; (ii) a BellState class that enables polarization entanglement of two independently generated photons; (iii) a FockStatePbs module that implements the desired BellState functionality; and (iv) a CoincidenceDetector that monitors for clicks from the SPDs.

Collectively, these software extensions provide the necessary functionality for the BSA. First, the laserController directs the lasers “Alice” and “Bob” to generate single photon pulse messages. These single photon pulse messages are processed by the BsaBeamSplitter’s interference model which calculates and outputs pulse messages based on temporal, spectral, and special overlap. In the FockStatePbs, the pulses are routed according to their encoded polarization to the appropriate SPDs. Finally, the coincidenceDetector monitors for distinguishable results at the four SPDs corresponding to Table I.

A. BsaBeamSplitter Module

The primary component of the BSA model is the BsaBeamSplitter, which extends the basic OMNeT++ cSimpleModule class and performs interference calculations through a dedicated model class, BsaBeamSplitterModel. More specifically, when single photon (Fock state) pulses arrive at the input ports, the BsaBeamSplitter temporarily stores them in a queue of incoming pulses. The model then determines how similar the photons are and whether they should exit the same port in accordance with the HOM effect. We assign a polarization similarity score ranging from zero to one, described as

\[
S_p = \cos^2(\theta_2 - \theta_1)
\]

(19)

where \( \theta_1 \) and \( \theta_2 \) are the polarization orientations of the two interfering photons. This score determines the probability that the two photons will exit the same port, given by

\[
P_{\text{same}} = \frac{1}{2} + \frac{1}{2} S_p
\]

(20)

When the two photons are identical, \( S_p = 1 \) and \( P_{\text{same}} = 1 \), thus, the photons will always exit through the same output port. When the photons are fully distinguishable \( S_p = 0 \), \( P_{\text{same}} = 0.5 \), indicating that the two photons have equal probability of exiting the beam splitter together or separately (i.e., acting independently of one another the model randomly determines whether the photons will exit together). A second random choice assigns each individual photon to a specific output port based on this result. According to the HOM effect, if the input polarizations are not the same, the photons must also be entangled, as described in Section IV-C. Lastly, the BsaBeamSplitter randomly assigns an OMNeT++ scheduling priority to each outgoing PulseMsg based on each pulse’s exit port information.
The BsaBeamSplitterModel is also capable of processing weak coherent state pulses which may result in multiple photons per pulse. This is accomplished by converting coherent state pulses into Fock state pulses via its Mean Photon Number according to the Poissonian distribution where each photon is treated independently.

### B. BellState Entanglement

If the photons are entangled, future measurements of the photons’ polarization at the PBSs must be correlated. The BSA model accomplishes this correlation by using a BellState object which is shared between the outgoing pulse polarizations. The BellState holds information about the joint state of the photons, including: (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 each pair of entangled created, the BsaBeamSplitter instantiates a new BellState object, sets the relevant parameters, and passes references to the object to each of the outgoing pulses which have access to the shared object for correlation between future measurements (i.e., entanglement).

To illustrate this behavior, consider the case in which Alice and Bob send the states $|D\rangle$ and $|A\rangle$, respectively. The similarity calculations result in $P_{\text{same}} = 0.5$, and assuming the pulses randomly exit different output ports, the two photons must be entangled into a $|\psi^-\rangle$ state. In this case, the BsaBeamSplitterModel creates a BellState object, sets the state to $|\psi^-\rangle$ and the basis to $\theta = \pi/4$ (i.e., the diagonal basis), and passes the BellState reference to the polarization property of each outgoing entangled pulse.

The BellState object’s most important feature is the “measure” method which facilitates measuring the Bell state in a given basis. If the entangled Bell state has not yet been determined, this method calculates the rotation from its current basis to the measurement basis and uses Eq. (17) to project the Bell state into the new basis. The probabilities of each resulting photon state are used to select into which state the measurement basis the entangled, two photon system will collapse. Specifically, the value of the first collapsed photon in the quantum system is returned as the measurement result. If the entanglement has already collapsed when the measurement occurs, the BellState simply returns the collapsed value of the second photon. As a final step, the entanglement link is destroyed as the two photons have decohered after the measurement (i.e., they are no longer entangled).

#### C. FockStatePbs Module

In order to utilize the BellState object to enforce measurement correlation, we created the polarizing beam splitter FockStatePbs. When this module receives a pulse message, it queries the incoming pulse’s polarization object for the appropriate measurement result in the rectilinear basis. If the polarization object is entangled, the polarization calls the “measure” method of its BellState object to determine the result. The FockStatePbs module then transmits or reflects the pulse accordingly. Since the PBS is symmetric, a $\pi/2$ phase shift is applied to any transmitted pulses.

### D. The CoincidenceDetector and State Determination

The CoincidenceDetector is an OMNeT++ cListener extension which monitors for click signals broadcasted by the four SPDs. Each time an SPD clicks, internal flags are set which are used to determine the appropriate BSM result according to Table I. Aggregated BSM results (i.e., counts of $|\psi^+\rangle$, $|\psi^-\rangle$, and failed results) are stored in an output file.

### V. Modeling the HOM Dip

Extension of the similarity calculation allows us to model the effects of temporal delay on HOM interference. First, we define temporal similarity in addition to polarization similarity ranging from zero to one [13]:

$$ S_t = e^{-\Delta \omega^2 (r_2 - r_1)^2} \quad (21) $$

where $\Delta \omega$ is the bandwidth of the pulse Gaussian frequency distribution function with units of rad·s$^{-1}$, and $r_1$ and $r_2$ are the arrival times of the two pulses, respectively. A composite similarity is calculated from $S_p$ and $S_t$ by

$$ S = S_p S_t \quad (22) $$

and the probability of exiting the same beam splitter output port becomes

$$ P_{\text{same}} = \frac{1}{2} + \frac{1}{2} S \quad (23) $$

This model of temporal delay, particularly (21), was constructed under several assumptions: (i) only single photon Fock states are simulated and does not apply to weak coherent pulses; (ii) both pulses have the same central wavelength and Gaussian frequency distribution (i.e., equal bandwidths); and (iii) the beam splitter has equal transmittance and reflectance (i.e., an ideal 50:50 beam splitter). For more detail regarding assumptions made, we ask that the reader consult the description of the experimental setup given in [13].

### VI. Simulation Results

#### A. Polarization-Encoded Bell State Measurements

To assess our model, each valid combination of input photon polarizations from Alice and Bob (i.e., $|H\rangle|H\rangle$, $|V\rangle|V\rangle$, $|H\rangle|V\rangle$, $|V\rangle|H\rangle$, $|D\rangle|D\rangle$, $|A\rangle|A\rangle$, $|D\rangle|A\rangle$, and $|A\rangle|D\rangle$) was tested by firing 100,000 laser pulses through the model and monitoring for BSM detection counts. The results of these trials are compared to the expected theoretical distributions of Bell state measurements for single photon Fock states in Table II. The theoretical values presented in Table II are the probabilities that a successful Bell state projection will result in either a $|\psi^+\rangle$ or $|\psi^-\rangle$ measurement [10]. For example, when two single photons are encoded in the rectilinear basis as $|H\rangle|V\rangle$, Table II shows that $|\psi^+\rangle$ and $|\psi^-\rangle$ should be detected with equal probability, as indicated by Case 2 of Fig. 6. The simulation results presented in Table II are the likelihoods of each measurement result occurring given a successful BSM, calculated from the Bell state detection counts recorded during the simulation.


V. 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