2-22-2017

Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems

Logan O. Mailloux
Air Force Institute of Technology

Michael R. Grimaila
Air Force Institute of Technology

Douglas D. Hodson
Air Force Institute of Technology

Ryan D. Engle
Air Force Institute of Technology

Colin V. Mclaughlin
Naval Research Laboratory

See next page for additional authors

Recommended Citation

Mailloux, L. O., Grimaila, M. R., Hodson, D. D., Engle, R. D., McLaughlin, C. V, & Baumgartner, G. B. (2017). Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems. Applied Sciences, 7(3), 212. https://doi.org/10.3390/app7020212

applied sciences

MDPI

Article

Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems

Logan O. Mailloux [1,*], Michael R. Grimaila [1], Douglas D. Hodson [1], Ryan Engle [1], Colin McLaughlin [2] and Gerald Baumgartner [3]

[1] Air Force Institute of Technology, Wright-Patterson AFB, OH 45433, USA; michael.grimaila@afit.edu (M.R.G.); douglas.hodson@afit.edu (D.D.H.); ryan.engle@afit.edu (R.E.)
[2] Naval Research Laboratory, Washington, DC 20375, USA; colin.mclaughlin@nrl.navy.mil
[3] Laboratory for Telecommunication Sciences, College Park, MD 20740, USA; gbaumgartner@ltsnet.net
* Correspondence: logan.mailloux@afit.edu; Tel.: +1-937-255-3636

Academic Editors: Zhiwu Li, MengChu Zhou, Naiqi Wu and Yisheng Huang
Received: 26 December 2016; Accepted: 17 February 2017; Published: 22 February 2017

Abstract: Quantum Key Distribution (QKD) systems exploit the laws of quantum mechanics to generate secure keying material for cryptographic purposes. To date, several commercially viable decoy state enabled QKD systems have been successfully demonstrated and show promise for high-security applications such as banking, government, and military environments. In this work, a detailed performance analysis of decoy state enabled QKD systems is conducted through model and simulation of several common decoy state configurations. The results of this study uniquely demonstrate that the decoy state protocol can ensure Photon Number Splitting (PNS) attacks are detected with high confidence, while maximizing the system's quantum throughput at no additional cost. Additionally, implementation security guidance is provided for QKD system developers and users.

Keywords: quantum key distribution; decoy state protocol; photon number splitting attack; implementation security

1. Introduction

Quantum Key Distribution (QKD) is a revolutionary security protocol which generates unlimited amounts of symmetric keying material between two geographically separated parties. Unlike conventional key distribution techniques, the security of QKD rests on the laws of quantum mechanics and not on computational complexity [1]. In theory, these attributes make QKD well suited for high-security applications such as banking, government, and military environments. However, implementation non-idealities and practical engineering limitations in commercially viable QKD systems (i.e., those which balance cost, performance, and security towards affordability) can negatively impact system performance and security [2]. For example, while commercial QKD systems often employ the decoy state protocol to mitigate vulnerabilities in non-ideal photon sources [3,4], its implementation security is poorly understood. Note, the decoy state protocol is well studied with respect to secure key rate generation (see background for details).

This work uniquely studies the decoy state protocol's implementation security in commercially viable QKD systems by modeling, simulating, and analyzing decoy state protocol configurations. The results of this study: (i) demonstrate the effectiveness of the several common decoy state enabled QKD system configurations to detect Photon Number Splitting (PNS) attacks; (ii) optimize the decoy state protocol to maximum quantum throughput; (iii) offer implementation security recommendations for QKD system designers and users; and (iv) present a repeatable methodology for analyzing the

performance and security of QKD systems. This article is an extension of the Author's previous works [5–9].

This article is organized as follows: First, an introduction to QKD is provided with an emphasis on security vulnerabilities, the PNS attack, and the decoy state protocol. Note, Section 2 is intended for those unfamiliar with QKD and the decoy state protocol. If the reader is familiar with these protocols, they should proceed directly to the next Section. In Section 3, the research method is explained, including a comprehensive listing of fielded decoy state enabled QKD systems, the Researcher's experimental design, and the QKD system-level model. Section 4 details the decoy state protocol's ability to detect PNS attacks across 40 common decoy state protocol configurations. Next, an optimization of the protocol is presented and demonstrated through model and simulation. Lastly, several implementation security recommendations are offered. Section 5 presents conclusions and future work. For security specialists desiring to further understand QKD, please see [5,10,11]. For comprehensive physics-based reviews of QKD, please see [1,4].

2. Quantum Key Distribution

The genesis of QKD traces back to the late 1960s, when Wiesner first proposed the idea of encoding information on polarized photons using two conjugate bases [12]. In 1984, Bennett and Brassard extended this idea by introducing the first QKD protocol, known as "BB84", to generate shared secret keying material between two parties [13]. Today, QKD is gaining attention as an important development in the cybersecurity solution space because of its ability to generate unlimited amounts of symmetric keying material for use with the One-Time-Pad (OTP)—the only known encryption algorithm to achieve perfect secrecy [14,15]. In this way, QKD enables unbreakable communications and has inspired research efforts across Asia, Europe, and North America [16]. While there are many competing QKD protocols, BB84 is primarily considered in this work because it remains a popular implementation choice and is relatively easy to understand [1].

2.1. The BB84 QKD Protocol

Figure 1 illustrates a notional QKD system configured to securely generate the secure shared key K, which is used to encrypt/decrypt sensitive data, voice, or video communications. The QKD system consists of a sender "Alice", a receiver "Bob", a quantum channel (i.e., an optical fiber or direct line of sight free space path), and a classical channel (i.e., a conventional networked connection). Alice is shown with a laser source configured to generate and prepare single photons, known as quantum bits or "qubits". The encoded photons are then transmitted over the quantum channel to Bob, whom measures them using specialized single photon detectors. This exchange of encoded single photons is described by the BB84 protocol.

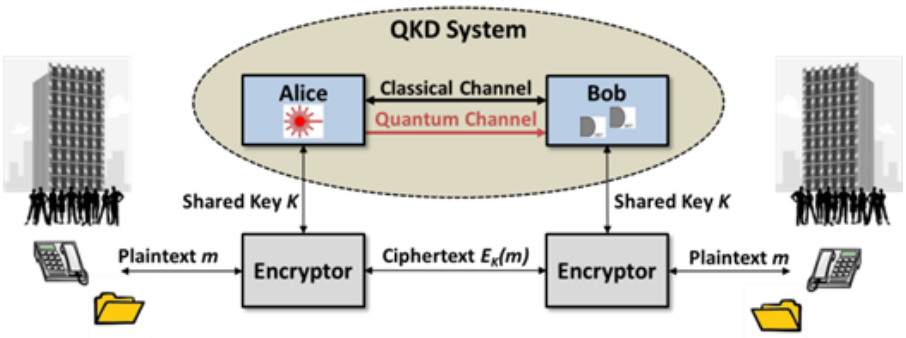

Figure 1. This is a Quantum Key Distribution (QKD) system context diagram. The sender "Alice" and receiver "Bob" generate shared secret key K for use in data encryption/decryption. Reproduced with permission from [9], Copyright IEEE, 2016.

Table 1 describes the BB84 protocol as a prepare and measure protocol where Alice encodes photons in one of four polarization states (e.g., $\leftrightarrow, \updownarrow, \nearrow$ or $\searrow$) according to a randomly selected bit value (0 or 1) and basis ($\oplus$ for the pair $\leftrightarrow$, $\updownarrow$ or $\otimes$ for the pair $\nearrow, \searrow$). Once Alice randomly prepares the photons, they are sent to Bob where he measures each photon using a randomly selected basis ($\oplus$ or $\otimes$). If Alice's encoding and Bob's decoding bases match, the photon's bit value is read correctly with a high probability. Otherwise, a random result occurs (i.e., equal likelihood of a 0 or 1); this is due to the inherent uncertainty in the measurement of an unknown (i.e., a randomly encoded) single photon. Typically, these random results are "sifted" from Bob's recorded detections and do not contribute to the shared key string.

Table 1. Example BB84 Protocol.

Alice Prepares			Bob Measures	
Bit	**Basis**	**Prepared State**	**Basis**	**Result**
0	$\oplus$	$\|\leftrightarrow\rangle$	$\oplus$	0
1	$\oplus$	$\|\updownarrow\rangle$	$\oplus$	1
0	$\oplus$	$\|\leftrightarrow\rangle$	$\otimes$	*random*
1	$\oplus$	$\|\updownarrow\rangle$	$\otimes$	*random*
0	$\otimes$	$\|\nearrow\rangle$	$\oplus$	*random*
1	$\otimes$	$\|\searrow\rangle$	$\oplus$	*random*
0	$\otimes$	$\|\nearrow\rangle$	$\otimes$	0
1	$\otimes$	$\|\searrow\rangle$	$\otimes$	1

More specifically, the security of BB84 is based on the uncertainty principle where the measurement result is random when using two conjugate bases (i.e., $\oplus$ or $\otimes$) to prepare single photons [17]. For example, during an intercept-resend attack anyone attempting to listen on the quantum channel must randomly select a measurement basis and will necessarily introduce detectable errors. These unavoidable errors increase the protocol's measured Quantum Bit Error Rate (QBER)—the ratio (or percent) of errors detected with respect to the total number of matched pulse detections—and if the QBER ever exceeds the protocol's security threshold (e.g., QBER > 11% [4]), the secret key distribution process is aborted (or restarted) as it is assumed an eavesdropper is active on the quantum channel. This is because all errors on the quantum channel are attributed to adversarial interference.

2.2. Vulnerabilities in Protocol Implementation

BB84 security proofs assume several idealities, including perfect on-demand single photon sources, lossless quantum transmission, perfect transmitter-receiver basis alignment, and perfect single photon detection [18]. However, these security assumptions are not valid when building real-world systems which deviate from theoretical protocols [2]. For example, reliable on-demand single photon sources are not currently available nor are they expected in the near term [1]. Therefore, most QKD systems attenuate classical laser pulses down from millions of photons to weak coherent pulses with an average photon number less than one. More specifically, the number of photons contained in the pulse is represented using a Poisson distribution with a low (i.e., <1) Mean Photon Number (MPN)

$$P(n|\mu) = \frac{\mu^n e^{-\mu}}{n!}, \tag{1}$$

where μ is the average number of photons in a pulse (i.e., μ is the MPN) and n represents the number of photons in the pulse (i.e., $n = 0, 1, 2, 3, \ldots,$ N). For example, with a typical MPN, $\mu = 0.5$, nearly 60% of the pulses have zero photons, 30% of the pulses have one photon, and 9% of the pulses have two or more photons. This means nearly 23% of the non-empty pulses emitted by Alice are non-ideal multiphoton pulses which leak information about the "unconditionally secure" QKD-generated secret key to eavesdroppers. This introduces a significant security vulnerability into the QKD protocol.

2.3. Photon Number Splitting (PNS) Attacks

The PNS attack is a powerful attack designed to take advantage of the multiphoton vulnerability in order to obtain a full copy of Alice and Bob's shared secret key bits without introducing errors and thus increasing the QBER [19,20]. A brief introduction to the PNS attack is given here, with a detailed, yet easily understandable engineering-oriented explanation available in [9].

Figure 2 provides a simplified depiction of the eavesdropper "Eve" conducting a PNS attack against the QKD system (i.e., Alice and Bob). In accordance with QKD security proofs, Eve is an all-powerful adversary limited only by the laws of quantum mechanics [4]. She is allowed full control of the quantum channel to introduce losses or errors and may eavesdrop on, but not fabricate, messages exchanged on the classical channel. In order to conduct the PNS attack, Eve replaces the quantum channel with a quantum teleportation channel which enables the lossless transmission of photons from Alice to Bob using the properties of entangled quantum systems [21]. An Eve′ entity is also required in close proximity to Bob to regulate the lossless transmission of photons as to not exceed Bob's expected detection rate; thus, avoiding obvious detection.

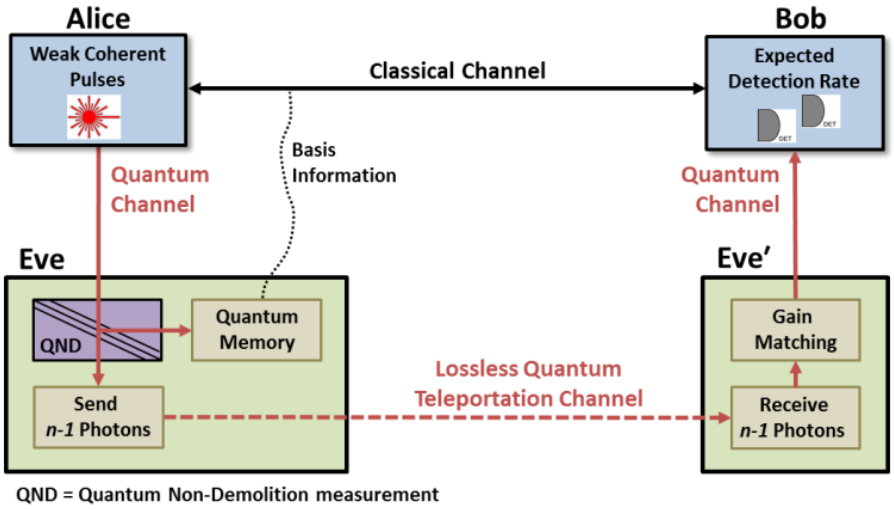

Figure 2. The eavesdropper (Eve and Eve′) is shown conducting a Photon Number Splitting (PNS) attack against the QKD system (Alice and Bob). Adapted with permission from [9], Copyright IEEE, 2016.

For each pulse Alice generates, Eve performs a specialized Quantum Non-Demolition (QND) measurement to determine the number of photons in each pulse $n = 0, 1, 2, 3, \ldots, N$ [22]. If $n \leq 1$, Eve blocks the pulse and sends nothing to Bob. If $n \geq 2$, Eve splits one photon from the pulse and stores it in her quantum memory. She then quantum teleports the remaining $n - 1$ photons to Bob. This attack scheme allows Eve to store an identical encoded copy of each photon sent to Bob without introducing additional errors (which are typically used for detecting eavesdroppers). Once Alice and Bob complete their quantum exchange, they must announce measurement basis information over the classical channel where Eve is able to listen. Eve can then correctly measure each stored photon, and thus, obtain a complete copy of the QKD-generated "secure" key bits.

2.4. The Decoy State Protocol

In 2003, the decoy state protocol was introduced to detect PNS attacks [23]. It was quickly improved upon in a series of works [24–28]; and is now widely employed in commercially viable QKD systems such as Toshiba's record holding system [29] and the world's largest QKD network [30]. In particular, the decoy state protocol is advantageous as it is relatively easy to implement (low cost), increases the system's distributed secret key rate (high performance), and mitigates the PNS

attack (improves implementation security). Note, while the decoy state protocol is designed to detect PNS attacks, other QKD protocols are not vulnerable to the attack (e.g., Continuous Variable or Measurement-Device Independent [1]); however, despite recent advances of alternative protocols, the decoy state protocol continues to be the most cost effective and practical to implement.

As described by Ma et al., the decoy state protocol extends the BB84 protocol by configuring Alice to randomly transmit three types of pulses: (1) Signal; (2) Decoy; and (3) Vacuum, as described in Table 2 [25]. Thus, Alice randomly generates signal, decoy, and vacuum pulses according to their prescribed occurrence percentages and respective MPNs where the state of each pulse must be indistinguishable to Eve (i.e., identical pulse shape, wavelength, duration, etc.) in order to maintain integrity of the security protocol. Eve cannot know a priori the type of pulse received during quantum exchange, the only information available to her is each pulse's specific number of photons $n = 0, 1, 2, 3, \ldots,$ N which she determines using her QND measurement.

Table 2. Example Decoy State Protocol Configuration.

State	Purpose	MPN	Occurrence Percentage
Signal μ	The signal state is used to generate secret key and facilitates improved performance by using a higher MPN (i.e., 0.5 is greater than the value 0.1 typically employed in non-decoy state protocol QKD systems).	0.5	70%
Decoy ν	The decoy state is used to increase the likelihood of detecting unauthorized eavesdropping on the quantum channel through statistical differential analysis with the signal state.	0.1	20%
Vacuum Y_0	The vacuum state is used to determine the noise on the quantum channel known as the "dark count" (i.e., detections when no photons are sent).	0.0	10%

2.5. Unconditionally Secure Key Generation

While the decoy state protocol was introduced to detect PNS attacks, to date it has been primarily used to increase unconditionally secure key rates. More specifically, decoy state research has focused on understanding and bounding Alice's single photon generation rate, Q_1, as it pertains to the secret key generation rate R [25].

$$R \geq q\{Q_1[1 - H_2(e_1)] - Q_\mu f(E_\mu)H_2(E_\mu)\}, \quad (2)$$

where q is the protocol efficiency (e.g., <1), Q_1 is the estimated single photon contribution, e_1 is the estimated error rate of single photon detections, Q_μ is the signal state gain, E_μ is the signal state QBER, $f(E_\mu)$ is the error reconciliation efficiency, and $H_2(\{E_\mu, e_1\})$ is Shannon's binary information function [15]. In a general sense, the positive contribution of Equation (2) accounts for pulses emitted by Alice containing a single photon (i.e., Q_1)—those which can contribute to the QKD-generated "unconditionally secure" key rate R, while the negative contribution accounts for insecure multi-photon pulses and errors which are also consider insecure contributions [25]. More specifically, the parameters of Equation (2) are described in Table 3. For a more detailed, yet readily accessible discussion of these parameters, please see [7]. For more comprehensive treatments, please see the references listed below.

Table 3. Secure Key Rate Parameters [7].

Parameter	Description
q	The protocol efficiency represents the overall efficiency of the QKD protocol (e.g., $q < 1$). For example, in the classical BB84 protocol shown in Table 1, 50% of the detections will be sifted out because of Bob's random choice of basis measurement.
Q_1	The estimated gain of pulses emitted by Alice with one photon (i.e., the single photons prepared by Alice and successfully measured by Bob). This value is typically calculated (or bounded) by several operational parameters such as, ν, Q_μ, and Y_0.
e_1	The estimated error rate associated with pulses emitted by Alice with a single photon. This value is typically calculated (or bounded) by several operational parameters such as, ν, E_μ, Q_μ and Y_0.
Q_μ	The gain of the signal state is calculated from system measurements, where $Q_\mu = \frac{Number\ of\ signal\ state\ detections}{Total\ number\ of\ sent\ signal\ state\ pulses}$
E_μ	The QBER of the signal state is calculated from system measurements, where $E_\mu = \frac{Number\ of\ signal\ state\ bit\ errors}{Total\ number\ of\ matched\ signal\ state\ detections}$
$f(E_\mu)$	The error reconciliation efficiency is dependent upon the signal state QBER E_μ with typical values of ≤ 1.15 for QBERs $\leq 5\%$.
$H_2(\{e_1, E_\mu\})$	Uncertainty in the error rate e_1 or E_μ is calculated using Shannon's binary entropy limit [15].

In their 2005 work, Ma et al. optimized the single photon generate rate Q_1 while simultaneously bounding the error rates e_1 and E_μ to maximize the secure key rate R [25]. More specifically to the decoy state protocol configuration, this optimization results in recommend signal and decoy state MPNs of $\mu \cong 0.5$ and $\nu \cong 0.1$ because of implementation limitations in classical laser sources (as described in Section 2.2) [25]. Following this seminal work, many others have studied this optimization problem to more fully understand and bound the single photon estimate Q_1, the negative impact of associated error rates e_1 and E_μ, and expected fluctuations in commercially available laser sources [31–40]. Additionally, considerations for finite key size statistics (i.e., limitations due to the number of detections) have been carefully investigated by others [28,41–43]. Here, we also note a recent work that benchmarks secret key rates over ideal quantum communication channels to include the decoy state protocol [44]. In addition to these works, several practically-oriented experimental demonstrations have been accomplished as detailed in Table 4 (discussed in Section 3).

2.6. Detecting PNS Attacks

The decoy state protocol is designed to detect PNS attacks by comparing the signal and decoy states during quantum exchange, and specifically, the photon number dependent yields of the signal state Y_n^{signal}, the decoy state Y_n^{decoy}, and the expected yield $Y_n^{expected}$ are compared in the security condition [24].

$$Y_n^{signal} = Y_n^{decoy} = Y_n^{expected}, \tag{3}$$

where Y_n represents the conditional probability that Bob detects a pulse given Alice sent an n-photon pulse. Ideally, Y_n^{signal} and Y_n^{decoy} are measured, while $Y_n^{expected}$ is calculated (or estimated) from a known quantum channel efficiency η.

$$Y_n^{expected} = Y_0 + \eta_n - Y_0\eta_n \approx Y_0 + \eta_n \tag{4}$$

where Y_0 is the measured dark count rate and $\eta_n = 1 - (1 - \eta)^n$ is the photon number specific efficiency based on the number of photons, n, in each pulse and the measured quantum efficiency η. Note, the joint probability $Y_0\eta_n$ is typically disregarded because it is insignificant compared to Y_0 and η_n.

As indicated by Equation (3), under normal operational conditions (i.e., when no PNS attacks are occurring), the signal and decoy state yields should be the same as the expected photon number dependent yield; for example, $Y_1^{signal} = Y_1^{decoy} = Y_1^{expected}$. This security condition should always be true for a decoy state enabled QKD architecture because the signal and decoy state yields are primarily

based on the fixed quantum efficiency η and not the state type. If ever $Y_1^{signal} \neq Y_1^{decoy} \neq Y_1^{expected}$, an eavesdropper is assumed to be actively listening on the key distribution channel and the secret key is considered compromised. While [24] also proposes an error-based condition $e_n^{signal} = e_n^{decoy} = e_n^{expected}$, it is not considered in this work since the PNS attack does not introduce errors [19].

3. Research Methodology

Table 4 provides a comprehensive listing of practically-oriented decoy state enabled systems and experiments. With respect to signal and decoy state MPNs, there is relatively little consistency or adherence to Ma and coworkers' 2005 work where they proved the optimal signal state MPN $\cong 0.5$ and decoy state MPN $\cong 0.1$ [25]. Similarly, there is considerable disparity in the protocol occurrence percentages with signal states ranging from 50% to ~99%, decoy states ranging from <1% to 40%, and vacuum states ranging from 0% to 25%. Note, while these experimental MPN parameters differ from those proposed by Ma et al., such discrepancies do not indicate that the Ma et al. security model is inappropriate. Furthermore, such differences may be due to differences in system architectures such as end-to-end losses (e.g., channel loss, insertion loss, detection efficiencies, etc.), security bounds, and post-processing techniques.

Despite the decoy state protocol's wide-spread employment, its effectiveness in detecting PNS attacks has not been thoroughly addressed in the literature. For example, in his defining work on the decoy state protocol, Lo states "Any attack by Eve that will change the value of any one of the Y_n's and e_n's substantially will, in principle, be caught with high probability by our decoy state method" [24]. Likewise, in the most detailed treatment available on detecting PNS attacks, the author merely states "significant deviation of the measured ratio from this expected value indicates a PNS by Eve" [45]. Thus, we desire to study the decoy state QKD system's ability to detect PNS attacks through model and simulation.

Table 4. Decoy State Enabled QKD System Configurations.

Case	Signal MPN	Decoy MPN	Occurrence Percentage ($\mu/\nu/Y_0$)	Propagation Distance (km)	Key Rate (bps)
1 [46]	0.80	0.12	90/10/0	15	165
2 [47]	0.55	0.152	63.5/20.3/16.2	60	<428 *
3 [5]	0.425	0.204	75/25/0 *	25	5.5 k
4 [48]	0.6	0.2	50/40/10	75	~12
5 [48]	0.6	0.2	50/40/10	102	~8
6 [49]	0.487	0.064	83.1/12.3/4.6	85	~28
7 [49]	0.297	0.099	83.1/12.3/4.6	100	~2
8 [50]	0.27	0.39	87/9/4	144	~13
9 [51]	0.55	0.098	93/6.2/1.6 **	20	10 k
10 [52]	0.48	0.16	93/6.2/1.6 **	25	5.7 k
11 [53]	0.55	0.10	80/16/4	20	1.02 M
12 [54]	0.57	0.13	70/20/10	140	~2
13 [55]	0.65	0.08	75/12.5/12.5	20	1.5 k
14 [55]	0.60	0.20	75/12.5/12.5	20	1.6 k
15 [55]	0.6	0.2	50/25/25	200	11.8
16 [56]	0.6	0.2	50/25/25	200	15
17 [57]	0.5	0.1	98.83/0.78/0.39	50	1.002 M
18 [58]	0.6	0.2	75/12.5/12.5	8–60 ***	1.2–4.5 k ***
19 [30]	0.65	0.1	87.5/6.25/6.25	30–80 ***	0.8–16 k ***
20 [29]	0.4	0.04	98/1.5/0.5	45	300 k

* Value estimated or assumed from reference; ** Values as reported; *** Multiple systems employed.

3.1. Problem Formulation and Research Questions

As the decoy state protocol is often employed in high performance QKD systems, and particularly the most impressive technology demonstrations to date (in terms of delivered key rate [29] and network size [30]), there is a need to understand the protocol's ability to detect PNS attacks more fully. Moreover, it is important for system developers and users to understand how the protocol can be optimized to maximize both quantum throughput for secret key generation and detect PNS attacks with high confidence. Therefore, it is desirable to address the following research questions:

(1) How do the signal and decoy state MPN values affect the system's ability to detect PNS attacks?
(2) How does the difference between the signal and decoy state MPN values affect the system's ability to detect PNS attacks?
(3) How do the signal, decoy, and vacuum state occurrence percentages affect the system's ability to detect PNS attacks?
(4) How does variation in the generation and detection of signal and decoy states affect the system's ability to detect PNS attacks?
(5) How does propagation distance (i.e., loss) affect the system's ability to differentiate between normal behavior and physical disturbances indicative of PNS attacks?

3.2. Experimental Design

From the comprehensive listing of decoy state configurations captured in Table 4, and detailed understanding of the decoy state protocol, five experimental factors are identified as shown in Table 5. First, operational distances of 20 and 50 km are selected to represent common metropolitan network lengths and long-haul backbone links. For those not familiar with quantum communication, losses of ~0.2 dB per km in single mode fiber significantly limit propagation distances where 20 km equates to 4 dB loss (or 40% efficiency) and 50 km equates to 10 dB loss (or 10% efficiency) [1]. Next, signal and decoy MPNs representative of normal and high configurations are chosen for examination, 0.5 and 0.8 respectively. As the main focus of this study, five occurrence percentage configurations are selected for analysis. Lastly, each treatment is examined during normal conditions and when subject to PNS attacks in order to baseline the QKD system's performance and ability to detect PNS attacks. Note, the decoy state protocol does not prevent the attack, it merely detects it.

Table 5. Experimental Design.

Operational Distance	Signal MPN	Decoy MPN	Occurrence Percentage (Signal/Decoy/Vacuum)	PNS Attack
20 km	0.5	0.1	60/30/10	No
50 km	0.8	0.2	70/20/10	Yes
—	—	—	80/10/10	—
—	—	—	90/5/5	—
—	—	—	99/0.5/0.5	—

All other design and configuration settings are held constant (described in Section 3.3).

For this study, a full factorial design was selected, as it is relatively easy to simulate all 80 treatments once the experimental factors are well understood. In order to characterize the modeled system's behavior well across all 80 configurations and make statistically significant conclusions, 1000 simulation runs were executed for each treatment using the DoD's High Performance Computing Modernization Program at Wright-Patterson Air Force Base. In particular, the model was packaged as a single executable application with a series of command line parameters, to account for the design of Table 5, and executed in parallel over 1024 cores for a total of 80,000 simulation runs for a total of nearly 200,000 h of processor time.

Regarding this experimental design, it is important to note that 20 km does not necessarily provide a sufficient loss budget for Eve to conduct PNS attacks without negatively impacting Bob's expected detection rate [59]. This is because Eve introduces loss on the quantum channel as she blocks all the single photon pulses sent by Alice. For example, Eve introduces ~7.4 dB loss against an MPN of 0.5, whereas the 20 km link only provides a ~4 dB loss budget for Eve to take advantage of with her lossless quantum teleportation channel. Despite this constraint, analyzing the decoy state protocol's ability to detect PNS attacks at this distance is desirable because many implementations have operational distances of 15–25 km as noted in Table 4. Moreover, if Eve is able to insert herself on the quantum channel before protocol calibration, her presence would go unnoticed with respect to loss and key rate.

3.3. Research Model

The research model (i.e., Alice, Bob, Eve, communication channels, and their supporting optical components) is described in detail in [6,7,9]; thus, this section merely provides an overview of the model and its most important configuration parameters. The research model was developed in a discrete event simulation framework specifically designed to study the impact of security and performance implementation non-idealities in QKD systems, algorithms, and protocols [6]. For example, performance and security limitations with respect to speed, accuracy, and environmental disturbances are captured in Alice's modeled laser source, decoy state generator, pulse modulator, quantum channel, and Avalanche Photo-Diode (APD) detectors. The decoy state enabled BB84 QKD model was developed in three increments each with increasing capability. The first increment provided a hardware-focused QKD notional architecture built in a modular fashion from a library of optical and electro-optical components with probabilistic weak coherent optical pulses [6]. The second increment added the processes and logic required to execute the decoy state protocol [7,60]. In the third increment, the behaviors of several modeled components were extended to properly handle the propagation of photon number specific representations of optical pulses (i.e., Fock states) and the PNS attack was fully implemented [9]. Throughout model development, considerable effort was spent thoroughly defining, decomposing, modeling, verifying, and validating the decoy state enabled QKD model with each optical component verified against commercial specifications (see Appendix of [6,61]). Additionally, the model was validated against eight fielded QKD systems [7] with additional modeling and simulation details presented in Section 4.

In this study, Alice is configured to generate signal, decoy, and vacuum pulses according to the decoy state protocol and BB84 polarization based prepare and measure modulation scheme as described in Section 2. In particular, Alice is programmed to randomly prepare signal, decoy, and vacuum pulses according to the user's prescribed occurrence percentages at a 5 MHz pulse rate with commercially representative laser fluctuations (see Section 4.2 for details). Alice then transmits the prepared pulses through the appropriate 20 or 50 km quantum channel, which has 4 or 10 dB loss respectively with induced physical disturbances which may cause the pulse's polarization to change over time. In accordance with the polarization based prepare and measure scheme, Bob's model includes beam splitters, polarizing beam splitters, a bandpass filter for a total of 3.5 dB loss. Most importantly, Bob contains models of commercially available APD detectors each configured with 10% detector efficiency, a 5×10^{-6} dark count rate (spontaneous detections when no photons are present), and a 0.01 after pulse rate (erroneous detections following a successful detection).

The research model allows users and developers to more easily (and collectively) study performance and security considerations of the decoy state protocol configurations as presented in Table 4 than when compared to building hardware implementations. Additionally, the model allows security analysts to uniquely study the security profile of decoy state enabled QKD systems in ways that are difficult or impossible with conventional means. For example, the model enables detailed analysis of the PNS attack using a hardware-focused representation—something that cannot yet be fully realized with current technologies [19,20]. In this way, the model allows for detailed traceability of each multiphoton pulse generated by Alice, split by Eve, and detected by Bob. Thus, the security

analyst is able to explicitly know which weak optical pulses are compromised yet contribute to the QKD-generated secret key bits.

4. Analysis of Results

In this section, the decoy state protocol's ability to detect PNS attacks is examined. First, the efficiency based method of detecting PNS attacks is explained, including expected operational variations from non-ideal optical components and processes. Next, simulation results for several common decoy state protocol configurations are described. Based on these results, an optimization of the decoy state protocol is presented and demonstrated. Lastly, implementation security guidance is offered for decoy state enabled QKD systems.

4.1. Detecting PNS Attacks

Despite the creativeness of Eve's PNS attack, her detectability is based on the decoy state protocol's ability to differentiate between subtle changes in the signal and decoy states. In lieu of comparing photon number dependent yields Y_n^{signal}, Y_n^{decoy}, $Y_n^{expected}$ which can be statically bounded or directly measurable using expensive Photon Number Resolving (PNR) detectors [62], this work utilizes the efficiency based security condition which provides a direct measurement in a cost-conscience QKD system implementation [8].

$$\eta^{signal} = \eta^{decoy} \tag{5}$$

where η^{signal} is the signal state efficiency and η^{decoy} is the decoy state efficiency. The efficiency based decoy state security method directly compares the signal and decoy state efficiencies from readily available measurements instead of requiring advanced technologies. The signal (and decoy) state efficiency is defined as

$$\eta^{signal} = \frac{-\ln\left|1 + Y_0 - Q_\mu\right|}{\mu} \tag{6}$$

where Y_0 is the system's measured dark count rate defined as

$$Y_0 = \frac{\text{Number of vacuum state detections}}{\text{Number of vacuum state pulses sent}} \tag{7}$$

and Q_μ is the measured signal state gain defined as

$$Q_\mu = \frac{\text{Number of signal state detections}}{\text{Number of signal state pulses sent}} \tag{8}$$

and μ is the signal state's prescribed MPN (typically 0.5). This method also allows the QKD system to assure the quantum channel is free from unwanted attacks without a priori knowledge such as a well-characterized quantum channel as required in prior art.

4.2. Expected Variation in the Decoy State Protocol

Due to non-ideal devices, physical disturbances, and probabilistic single photon sources, variations are expected in the protocol's operation. These variations directly impact the system's ability to detect PNS attacks and must be accounted for, thus, the security condition becomes

$$\eta^{signal} = \eta^{decoy} \pm \Delta \tag{9}$$

where Δ represents the protocol's expected variation during quantum exchange. Variation in the decoy state efficiency is primarily considered because it exhibits significantly more variation than the signal state due to its reduced occurrence percentage and lower MPN.

While there are many potential sources of variation (e.g., fluctuations in laser sources, polarization dependent losses, variations in decoy state MPNs, temperature changes, physical disturbances,

unstable detector efficiencies, etc.), many of them can be ignored due to the rapid propagation of photons through optical fiber (i.e., 2/3 the speed of light $\approx 2 \times 10^8$ m/s). More explicitly, quantum exchange rounds (i.e., 100,000 signal state detections [63]) are typically very short (e.g., $<20 \times 10^{-3}$ s) and many of these effects are orders of magnitude slower (e.g., temperature change due to direct sunlight). Thus, Alice's pulse-to-pulse variation is of primary interest, and specifically, variation in her laser source (e.g., a commercially available id300 pulsed laser [64]) and decoy state generator (e.g., an electronically controlled Variable Optical Attenuator (VOA) used to control the MPN of each signal, decoy, and vacuum pulse [65]).

Figure 3 illustrates Alice's modeled variation when calibrated to produce weak coherent optical pulses with an MPN of 0.55. Because of the large number of pulses, the 99.9% Prediction Interval (PI) characterizes her expected MPN variation well. This means Alice will generate pulses with an MPN between 0.49 and 0.61 nearly 100% of the time. Thus, variations in generating signal, decoy, and vacuum pulses should be expected and addressed when considering the effectiveness of the decoy state protocol in detecting PNS attacks.

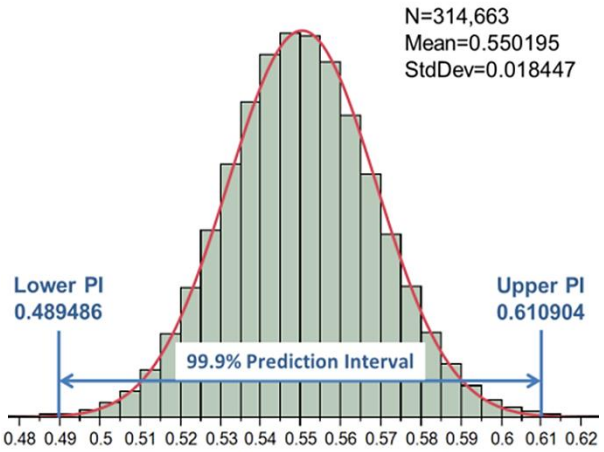

Figure 3. Variation in weak coherent pulse Mean Photon Number (MPN) emitted from Alice's modeled laser due to expected fluctuations and performance limitations in the modeled decoy state generator (i.e., the variable optical attenuator). The upper and lower Prediction Intervals (PI) are shown to bound the expected performance.

4.3. Studying Detection Results

Figure 4 illustrates the normal operating conditions for 20 configurations over an operational distance of 50 km (the 20 km results are not shown because they are very similar). The results are grouped with respect to signal and decoy MPNs with each treatment labeled across the bottom of the graph by signal-decoy-vacuum occurrence percentages (e.g., 60–30–10 means 60% signal states, 30% decoy states, and 10% vacuum states). The overlapping box plots imply $\eta^{signal} = \eta^{decoy}$; thus, the system is operating in a secure state. Of note, variation in the signal state remains relatively fixed, while variation in the decoy state increases as the occurrence percentage lessens from 30% to 0.5%. Likewise, the lower MPN (i.e., 0.1 compared to 0.2) results in slightly more variation in each configuration. This occurs because less decoy states are sent by Alice, and therefore, detected by Bob, causing more variation. In all 40 configurations studied without PNS attacks at both 20 and 50 km, the signal and decoy state efficiencies are overlapping with no statistically significant differentiation.

Figure 5 illustrates results over the 50 km operational distance from 20 configurations when subject to PNS attacks (the 20 km results are not shown because they are very similar). For each configuration studied, there is a clear separation between the decoy state efficiencies and the signal state efficiencies. This is because Eve inadvertently blocks most of the decoy state pulses since the majority of them contain only a single photon due to its lower MPN. Conversely, relatively few signal state pulses are

blocked since the higher MPN generates more multi-photon pulses. Thus, Eve significantly reduces the decoy state efficiency. This behavior is precisely why the decoy state protocol requires two different MPNs in otherwise indistinguishable states (i.e., Eve is unaware of the pulse type she is acting upon, since any of the pulses (signal, decoy, or vacuum) *could* consist of 0, 1, or $\geq$2 photons). Additionally, as can be seen in the downward trending efficiencies, these responses are tempered by the protocol's occurrence percentages and Eve's gain matching.

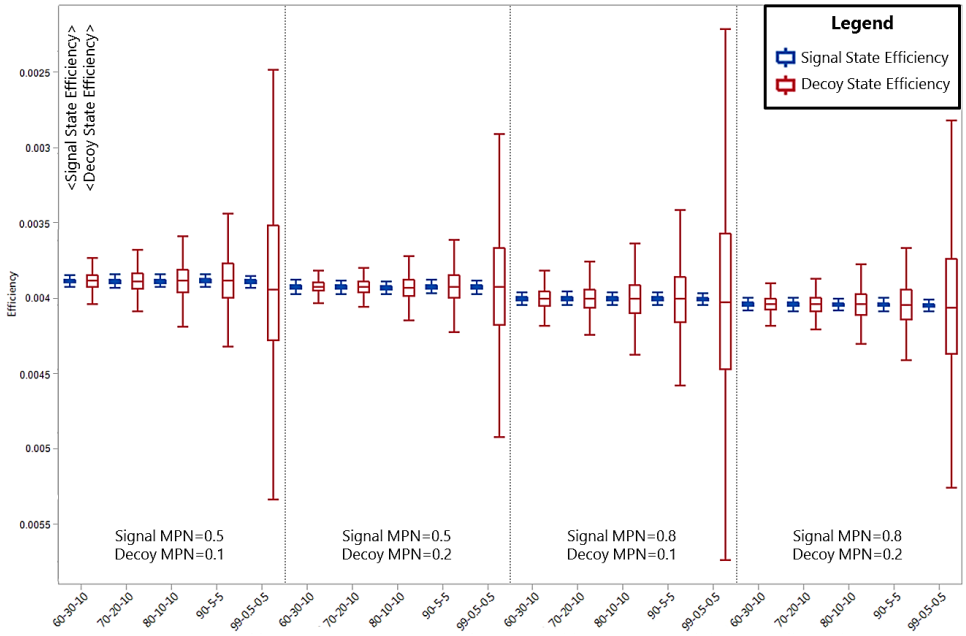

Figure 4. Simulation results are shown for the for the 50 km decoy state protocol configurations examined when operating under normal conditions. In each configuration studied, the signal and decoy state efficiencies are the same $\eta^{signal} = \eta^{decoy} \pm \Delta$ (within expected variation tolerances).

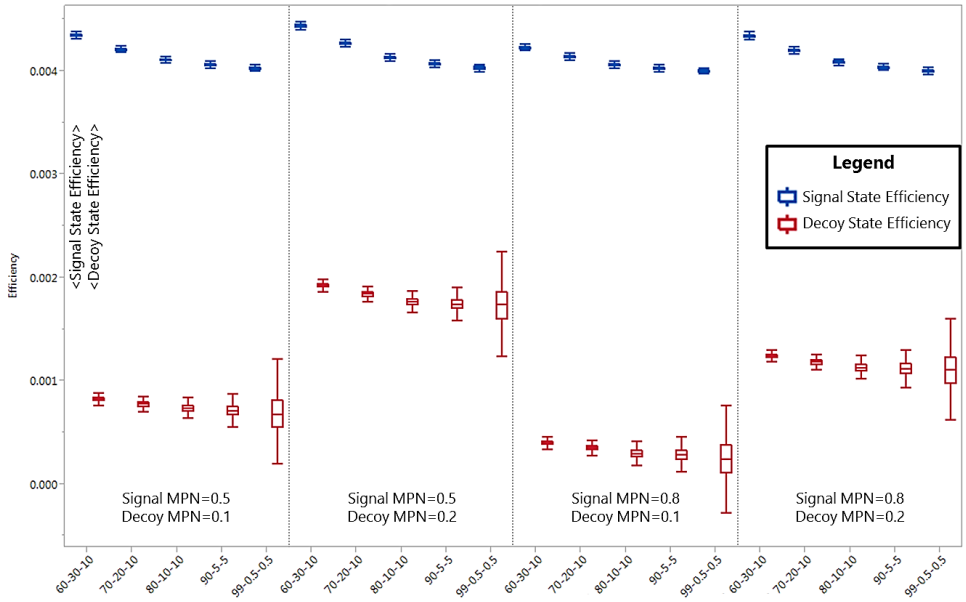

Figure 5. Simulation results are shown for the 50 km decoy state protocol configurations examined when subject to PNS attacks. In each configuration studied, the signal and decoy state efficiencies are statistically different $\eta^{signal} \neq \eta^{decoy} \pm \Delta$ (outside expected variation tolerances).

In the 40 configurations considered at both 20 and 50 km distances, the PNS attack was successfully detected in all 40,000 trials (i.e., 1000 trials in each of the 40 PNS attack configurations simulated). For example, in the worst case scenario, when the signal and decoy state MPNs are closest (0.5 and 0.2) with the least amount of decoy states (99% signal, 0.5% decoy, and 0.5% vacuum) and the most loss (10 dB loss over the 50 km channel), there is very strong statistical evidence that the PNS attack will be detected because $\eta^{signal} \neq \eta^{decoy} \pm \Delta$. More specifically, based on 1000 simulations in the worst case configuration, the decoy state enabled QKD system has less than one in a thousand chance of not detecting the attack with a low probability of $p < 0.001$. These results demonstrate the decoy state protocol's ability to detect PNS attacks across a wide set of commonly implemented configurations to include when the decoy state intensity is very weak and the occurrence percentage is very small. Moreover, these results illustrate that the protocol can be further optimized with respect to the signal and decoy state occurrence percentages to maximize quantum throughout on the signal state as identified by the large "white space" between the signal and decoy states efficiencies in Figure 5 for even the most stringent configurations (when the occurrence percentages are: 99% signal, 0.5% decoy, and 0.5% vacuum).

4.4. Optimization for Performance and Security

While the decoy state protocol has been optimized with respect to MPNs contributing to secret key distribution [25], the signal and decoy state occurrence percentages have not been optimized for maximizing quantum throughout while simultaneously detecting PNS attacks with high confidence. Hence, we provide an optimization which assures high security confidence and allows the protocol's performance to be maximized based on a detailed study of signal and decoy state MPNs and occurrence percentages, as well as, design decisions and architectural considerations.

From this study, we learn that the protocol's ability to detect PNS attacks is primarily controlled by losses due to each state's occurrence percentage, MPN, and the end-to-end quantum communication path. More specifically, to detect PNS attacks in real-time with high confidence only a few decoy state detections are necessary during each round of quantum exchange (i.e., a predetermined number of detections). For example, the decoy state protocol can be configured to perform the PNS attack check after each round of 100,000 detections. Furthermore, we learn that an arbitrarily high level of confidence (e.g., >99.9%) is possible because statistical confidence is increased through multiple rounds of quantum exchange and not the number of decoy state detections per round. Note this optimization is meant to maximize quantum throughput and requires that other secret key rate estimations such as Q_1 and e_1 for Equation (2) be derived from dedicated, periodic calibration runs.

In order to optimize the decoy state protocol, the developer should choose the highest signal state occurrence percentage possible, while meeting the minimum number of decoy state detections to reliably detect PNS attacks (i.e., choose the minimal decoy occurrence percentage possible). Assuming the suggested MPNs of Ma et al. are used ($\mu = 0.5,\ \nu = 0.1$) [25], the optimized decoy state protocol configuration can be described in a system of equations. First, the signal state occurrence percentage S_μ should be as a close to unity as possible

$$S_\mu \rightarrow 1 \tag{10}$$

where S_μ is limited by the decoy and vacuum state occurrence percentages S_ν, S_{Y_0}, respectively

$$S_\mu = 1 - S_\nu - S_{Y_0}. \tag{11}$$

Accordingly, it is advantageous to minimize both S_ν and S_{Y_0}; however, the decoy state occurrence percentage S_ν must be high enough to effectively differentiate between noise on the quantum channel and a PNS attack where the decoy state gain Q_ν must exceed the system's measured dark count rate Y_0.

$$Q_\nu > Y_0. \tag{12}$$

This condition implies at least one decoy state detection N_ν per round of quantum exchange which is not due to a dark count (i.e., a signal to noise ratio >1).

Thus, the optimized decoy state configuration can be further clarified

$$S_\nu \ll 1 \tag{13}$$

$$N_\nu \geq 1. \tag{14}$$

For a given architecture, the optimized decoy state protocol can be determined from the minimum number of decoy state detections N_ν, the desired number of signal state detections N_μ, the signal and decoy state gains Q_μ, Q_ν, and their occurrence percentages S_μ, S_ν where

$$N_\nu = S_\nu Q_\nu N_{total\ pulses\ sent} \tag{15}$$

$$N_{total\ pulses\ sent} = \frac{N_\mu}{S_\mu Q_\mu} \tag{16}$$

$$S_\nu = \frac{N_\nu S_\mu Q_\mu}{Q_\nu N_\mu}. \tag{17}$$

While the necessary parameters for optimization are readily available, in order maximize performance the system's architecture must be well-characterized in the desired operational environment. This is because the decoy state protocol is being configured to operate at its minimum threshold and is extremely sensitive to implementation non-idealities and performance variations to include Alice's ability to generate weak coherent pulses, losses in the quantum channel, physical disturbances, detector efficiency, and particularly the system's operational dark count rate.

4.5. Example Optimization

In this section, an optimization of a fielded decoy state enabled QKD system is demonstrated. As one of the most well documented decoy state protocol implementations and a major milestone in the world's largest QKD network, Chen and coworkers' work lends itself well to detailed analysis [55]. The protocol's configuration is provided in Table 6.

Table 6. Example Decoy State Protocol Configuration.

Protocol Configuration	Operational Results
$S_\mu = 0.75$	$\eta = 0.00985$
$S_\nu = 0.125$	$Q_\mu = 6.36 \times 10^{-3}$
$S_{Y_0} = 0.125$	$Q_\nu = 8.61 \times 10^{-4}$
$\mu = 0.65$	$Y_0 = 1.0 \times 10^{-4}$
$\nu = 0.08$	—

Assuming $N_\mu = 100,000$ detections per quantum exchange and an arbitrarily small vacuum state occurrence percentage $S_{Y_0} = 0.005$, the decoy state protocol occurrence percentages can be optimized to $S_\mu = 0.99435$, $S_\nu = 0.00065$ using the approach described in Equations (9)–(16). This optimized configuration is particularly advantageous as it results in a >30% increase in key rate (i.e., a signal state occurrence percentage 99.435% instead of 75%) and the ability to detect PNS attack with 99.9% confidence at no additional cost. This optimization accounts for expected real-world variations in the source but does not account for significant disturbances in the quantum channel which would quickly eliminate the ability to reliably perform QKD regardless of the decoy state configuration.

Figure 6 presents detailed results of the optimized protocol while operating under normal conditions and when subject to PNS attacks. Shown on the left, during normal operations the signal and decoy state efficiencies (blue and red) overlap as expected. Shown in the middle, PNS attacks cause

the signal and decoy state efficiencies (green and purple) to become non-overlapping. In particular, since the protocol is configured to operate with a minimum number of decoy state detections, the PNS attack reduces the decoy state from a small number of detections to zero during nearly every round of quantum exchange. This results in a reported decoy state mean efficiency of 0.000 with relatively little variation (see Figure 7 for further details). Consequently, the optimized decoy state protocol configuration serves to emphasize the negative impact of the PNS attack by forcing the decoy state's efficiency below the measured dark count rate (shown in brown with a detailed inlay) because so few decoy state detections are expected per round of quantum exchange.

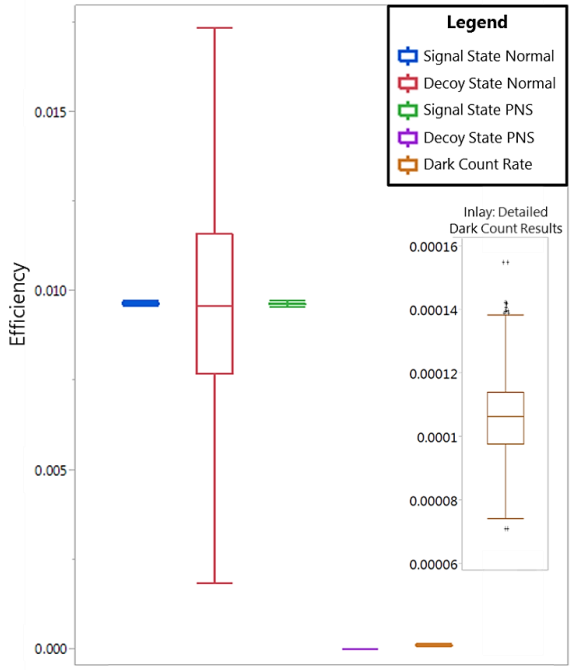

Figure 6. Simulation results show the optimized decoy state protocol for detecting PNS attacks based on the fielded QKD system [55]. The inlay details the expected dark count rate complete with outliers to illustrate the modeled noise over the QKD communication channel.

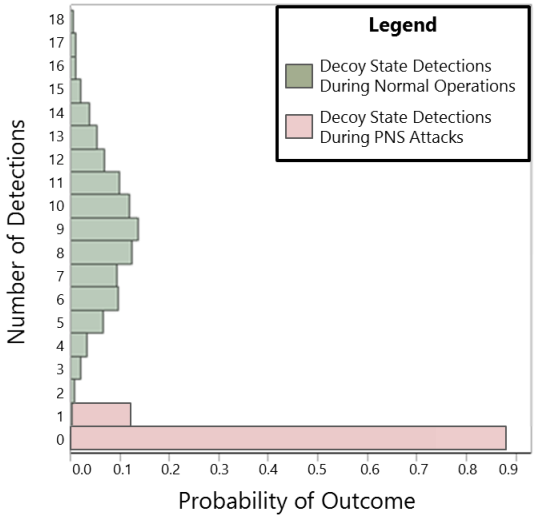

Figure 7. Simulation results detailing the number of decoy state detections per round of quantum exchange for the optimized decoy state protocol based on the fielded QKD system parameters shown in Table 6.

Figure 7 displays the number of decoy state detections per round of quantum exchange during normal operations (shown in green) and when subject to PNS attacks (shown in red). During normal operations, the optimized configuration results, shown in green, demonstrate at least one decoy state detection per 100,000 detections and a mean of nine detections. Conversely, as shown in red, very few decoy state detections are expected during PNS attacks. Detections occur in only 134 out of the 1000 rounds of quantum exchange, which constitute statistical outliers. In terms of efficiency, the mean decoy state efficiency is 0.0096 during normal operations (shown in red in Figure 6) and drops to 0.0013 (shown in purple in Figure 6) during PNS attacks. As a result, the PNS attack is readily detectable with a high statistical confidence of (i.e., >99.9% or $p < 0.001$) when considering 1000 rounds of quantum exchange with a total of 100,000 detections per round.

While the decoy state occurrence percentage S_ν can be further reduced, statistical significance begins to diminish because the number of decoy state detections per round of quantum exchange approaches zero during normal operations. Moreover, as the occurrence percentage is further reduced the protocol's integrity is jeopardized as the decoy state gain must be larger than the system's dark count rate (i.e., $Q_\nu > Y_0$).

4.6. Implementation Recommendations

In addition to the protocol optimization described above, this research effort brought to our attention several design and implementation recommendations for commercially viable QKD systems. While these recommendations are not entirely new or novel, they are important to highlight for QKD performance, implementation security, and potentially formal certification efforts.

(1) Upon system startup, the decoy state protocol should be configured to quickly perform initial security checks to ensure the quantum channel is free from PNS attacks. For example, 1000 rounds of quantum exchange can be executed in a relatively short amount of time during initial calibration activities.
(2) Configure the decoy state protocol to continuously monitor for PNS attacks in real-time and over several rounds of quantum exchange to increase confidence in the system's security.
(3) The noise level (i.e., the dark count rate) should be measured during dedicated calibration activities with very large numbers of vacuum signals (e.g., $\geq 10^9$) intermixed with signal and decoy states to well-characterize the operational environment and system architecture.
(4) During operation, the dark count rate should be compared to the calibration results in order to detect changes in the operational environment such as temperature changes or additional physical disturbances.
(5) Minimize the vacuum state occurrence percentage but do not eliminate it. The state can be used as an indicator to monitor for attacks such as the blinding attack [66].

Additionally, while Ma and coworkers' work optimized the signal state MPN at ~0.5, users may want to consider higher signal state MPNs such as those successfully demonstrated in the world's largest QKD network (i.e., $\mu = 0.65$) [30]. Moreover, past work on the subject recommends MPNs on the order of 1.0–1.2 based on pragmatic technical assumptions [67].

5. Conclusions

In this study, the ability of the decoy state enabled QKD systems to detect PNS attacks is analyzed and demonstrated. In contrast to most decoy state protocol research which focus on decoy state security bounds and estimates, this work focuses on the protocol's occurrence percentages to both maximize signal state quantum throughput and assure PNS attacks are detectable with high confidence. Additionally, practical implementation performance and security guidance is provided for system developers and users. Lastly, this work demonstrates a repeatable methodology for studying QKD system implementation security to support formal certification efforts [68].

Future suggested work includes optimization of the decoy state protocol in a fielded QKD system along with a detailed study of how the recommended occurrence percentages should be balanced with other constraints such as the need for bounded error rates. Additionally, in terms of validating the proposed decoy state configuration's ability to detect PNS attacks, a decoy state enabled QKD system should be tested against PNS-like attacks (see [20] for an example), since it is currently impossible to build a fully functional PNS attack. Lastly, the author recommends continued emphasis on studying QKD implementation security issues towards formal certification of decoy state enabled systems as they remain the most commercially viable option in the near future (especially when considering practical issues such as distance limitations and delivered key rates).

Author Contributions: In this work Logan O. Mailloux is the principle investigator with Michael R. Grimaila providing research advisement and expertise in quantum key distribution, Douglas D. Hodson providing modeling and software expertise, Ryan Engle providing assistance in model development and execution, Colin McLaughlin providing expertise in quantum optics, and Gerald Baumgartner providing expertise in quantum communications.

Conflicts of Interest: The authors declare no conflict of interest. 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. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
2. Scarani, V.; Kurtsiefer, C. The black paper of quantum cryptography: Real implementation problems. *arXiv* **2009**, arXiv:0906.4547v2.
3. Oesterling, L.; Hayford, D.; Friend, G. Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012.
4. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
5. Mailloux, L.O.; Grimaila, M.R.; Hodson, D.D.; Baumgartner, G.; McLaughlin, C. Performance evaluations of quantum key distribution system architectures. *IEEE Secur. Priv.* **2015**, *13*, 30–40. [CrossRef]
6. Mailloux, L.O.; Morris, J.D.; Grimaila, M.R.; Hodson, D.D.; Jacques, D.R.; Colombi, J.M.; McLaughlin, C.; Engle, R.; Holes, J. A modeling framework for studying quantum key distribution system implementation non-idealities. *IEEE Access* **2015**, *3*, 110–130. [CrossRef]
7. Mailloux, L.O.; Engle, R.D.; Grimaila, M.R.; Hodson, D.D.; McLaughlin, C. Modeling decoy state quantum key distribution systems. *J. Def. Model. Simul. Appl. Methodol. Technol.* **2015**, *12*, 489–506. [CrossRef]
8. Mailloux, L.O.; Grimaila, M.R.; Colombi, J.M.; Hodson, D.D.; Engle, R.D.; McLaughlin, C.V.; Baumgartner, G. Quantum key distribution: Examination of the decoy state protocol. *IEEE Commun. Mag.* **2015**, *53*, 24–31. [CrossRef]
9. Mailloux, L.; Hodson, D.; Grimaila, M.; Engle, R.; McLaughlin, C.; Baumgartner, G. Using modeling and simulation to study photon number splitting attacks. *IEEE Access* **2016**, *4*, 2188–2197. [CrossRef]
10. Elliott, C. Quantum cryptography. *IEEE Secur. Priv.* **2004**, *2*, 57–61. [CrossRef]
11. Qi, B.; Qian, L.; Lo, H.-K. A brief introduction of quantum cryptography for engineers. *arXiv* **2010**, arXiv:1002.1237.
12. Wiesner, S. Conjugate coding. *ACM Sigact New* **1983**, *15*, 78–88. [CrossRef]
13. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984.
14. Vernam, G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Trans. Am. Inst. Electr. Eng.* **1926**, *45*, 295–301. [CrossRef]
15. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
16. Quantum Cryptography Conference. QCrypt 2015. Available online: 2015.qcrypt.net (accessed on 24 September 2015).

17. Gottesman, D.; Lo, H.-K.; Lutkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. In Proceedings of the International Symposium on Information Theory (ISIT 2004), Chicago, IL, USA, 27 June–2 July 2004.
18. Renner, R.; Gisin, N.; Kraus, B. An information-theoretic security proof for QKD protocols. *Phys. Rev. A* **2005**, *72*, 012332. [CrossRef]
19. Brassard, G.; Lutkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef] [PubMed]
20. Lütkenhaus, N. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **2000**, *61*, 052304. [CrossRef]
21. Loepp, S.; Wootters, W.K. *Protecting Information*; Cambridge University Press: New York, NY, USA, 2006.
22. Nogues, G.; Rauschenbeutel, A.; Osnaghi, S.; Brune, M.; Raimond, J.M.; Haroche, S. Seeing a single photon without destroying it. *Nature* **1999**, *400*, 239–242.
23. Hwang, W.-Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
24. Lo, H.-K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef] [PubMed]
25. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. *Phys. Rev.* **2005**, *72*, 012326. [CrossRef]
26. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef] [PubMed]
27. Wang, X.-B. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A* **2005**, *72*, 012322. [CrossRef]
28. Harrington, J.W.; Ettinger, J.M.; Hughes, R.J.; Nordholt, J.E. Enhancing practical security of quantum key distribution with a few decoy states. *arXiv* **2005**, arXiv:quant-ph/0503002.
29. Dixon, A.R.; Dynes, J.F.; Lucamarini, M.; Fröhlich, B.; Sharpe, A.W.; Plews, A.; Tam, S.; Yuan, Z.L.; Tanizawa, Y.; Sato, H.; et al. High speed prototype quantum key distribution system and long term field trial. *Opt. Express* **2015**, *23*, 7583–7592. [CrossRef] [PubMed]
30. Wang, S.; Chen, W.; Yin, Z.Q.; Li, H.W.; He, D.Y.; Li, Y.H.; Zhou, Z.; Song, X.T.; Li, F.Y.; Wang, D.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739–21756. [CrossRef] [PubMed]
31. Wang, X.-B. Secure and efficient decoy-state quantum key distribution with inexact pulse intensities. *arXiv* **2006**, arXiv:quant-ph/0609081.
32. Mauerer, W.; Silberhorn, C. Quantum key distribution with passive decoy state selection. *Phys. Rev. A* **2007**, *75*, 050305. [CrossRef]
33. Hayashi, M. General theory for decoy-state quantum key distribution with an arbitrary number of intensities. *New J. Phys.* **2007**, *9*, 284. [CrossRef]
34. Wang, X.-B.; Peng, C.-Z.; Pan, J.-W. Simple protocol for secure decoy-state quantum key distribution with a loosely controlled source. *Appl. Phys. Lett.* **2007**, *90*, 031110. [CrossRef]
35. Tsurumaru, T.; Soujaeff, A.; Takeuchi, S. Exact minimum and maximum of yield with a finite number of decoy light intensities. *Phys. Rev. A* **2008**, *77*, 022319. [CrossRef]
36. Wang, X.-B.; Yang, L.; Peng, C.-Z.; Pan, J.-W. Decoy-state quantum key distribution with both source errors and statistical fluctuations. *New J. Phys.* **2009**, *11*, 075006. [CrossRef]
37. Hu, J.Z.; Wang, X.B. Reexamination of the decoy-state quantum key distribution with an unstable source. *Phys. Rev. A* **2010**, *82*, 012331. [CrossRef]
38. Hu, J.Z.; Wang, X.B. Secure quantum key distribution in an easy way. *arXiv* **2010**, arXiv:1004.3730.
39. Li, Y.; Bao, W.; Li, H.; Zhou, C.; Wang, Y. Passive decoy-state quantum key distribution for the weak coherent photon source with intensity fluctuations. *arXiv* **2013**, arXiv:1312.7383[quant-ph].
40. Sun, Q.C.; Wang, W.L.; Liu, Y.; Zhou, F.; Pelc, J.S.; Fejer, M.M.; Peng, C.Z.; Chen, X.; Ma, X.; Zhang, Q.; et al. Experimental passive decoy-state quantum key distribution. *Laser Phys. Lett.* **2014**, *11*, 085202. [CrossRef]
41. Hasegawa, J.; Hayashi, M.; Hiroshima, T.; Tanaka, A.; Tomita, A. Experimental decoy state quantum key distribution with unconditional security incorporating finite statistics. *arXiv* **2007**, arXiv:0705.3081.

42. Lucamarini, M.; Patel, K.A.; Dynes, J.F.; Fröhlich, B.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **2013**, *21*, 24550–24565. [CrossRef] [PubMed]
43. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]
44. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *arXiv* **2015**, arXiv:1510.08863.
45. Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. Unconditionally secure one-way quantum key distribution using decoy pulses. *Appl. Phys. Lett.* **2007**, *90*, 011118. [CrossRef]
46. Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K.; Qian, L. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.* **2006**, *96*, 070502. [CrossRef] [PubMed]
47. Zhao, Y.; Qi, B.; Ma, X.; Lo, H.-K.; Qian, L. Simulation and implementation of decoy state quantum key distribution over 60 km telecom fiber. In Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, WA, USA, 9–14 July 2006.
48. Peng, C.-Z.; Zhang, J.; Yang, D.; Gao, W.-B.; Ma, H.-X.; Yin, H.; Zeng, H.; Yang, T.; Wang, X.-B.; Pan, J.-W. Experimental long-distance decoy-state quantum key distribution based on polarization encoding. *Phys. Rev. Lett.* **2007**, *98*, 010505. [CrossRef] [PubMed]
49. Rosenberg, D.; Harrington, J.W.; Rice, R.; Hiskett, A.; Peterson, C.G.; Hughes, R.J.; Lita, A.E.; Nam, S.W.; Nordholt, J.E. Long-distance decoy-state quantum key distribution in optical fiber. *Phys. Rev. Lett.* **2007**, *98*, 010503. [CrossRef] [PubMed]
50. Schmitt-Manderbach, T.; Weier, H.; Fürst, M.; Ursin, R.; Tiefenbacher, F.; Scheidl, T.; Perdigues, J.; Sodnik, Z.; Kurtsiefer, C.; Rarity, J.G.; et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.* **2007**, *98*, 010504. [CrossRef] [PubMed]
51. Dynes, J.F.; Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. Practical quantum key distribution over 60 hours at an optical fiber distance of 20km using weak and vacuum decoy pulses for enhanced security. *Opt. Express* **2007**, *15*, 8465–8471. [CrossRef] [PubMed]
52. Dynes, J.F.; Yuan, Z.L.; Sharpe, A.W.; Shields, A.J. Decoy pulse quantum key distribution for practical purposes. *IET Optoelectron.* **2008**, *2*, 195–200. [CrossRef]
53. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shield, A.J. Gigahertz decoy quantum key distribution with 1 Mbit/s secure key rate. *Opt. Express* **2008**, *16*, 18790–18979. [CrossRef] [PubMed]
54. Rosenberg, D.; Peterson, C.G.; Harrington, J.W.; Rice, P.R.; Dallmann, N.; Tyagi, K.T.; McCabe, K.P.; Nam, S.; Baek, B.; Hadfield, R.H.; et al. Practical long-distance quantum key distribution system using decoy levels. *New J. Phys.* **2009**, *11*, 045009. [CrossRef]
55. Chen, T.-Y.; Liang, H.; Liu, Y.; Cai, W.-Q.; Ju, L.; Liu, W.-Y.; Wang, J.; Yin, H.; Chen, K.; Chen, Z.B.; et al. Field test of a practical secure communication network with decoy-state quantum cryptography. *Opt. Express* **2009**, *17*, 6540–6549. [CrossRef] [PubMed]
56. Liu, Y.; Chen, T.Y.; Wang, J.; Cai, W.Q.; Wan, X.; Chen, L.K.; Wang, J.H.; Liu, S.B.; Liang, H.; Yang, L.; et al. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express* **2010**, *18*, 8587–8594. [CrossRef] [PubMed]
57. Dixon, A.R.; Yuan, Z.L.; Dynes, J.F.; Sharpe, A.W.; Shields, A.J. Continuous operation of high bit rate quantum key distribution. *Appl. Phys. Lett.* **2010**, *96*, 161102. [CrossRef]
58. Chen, T.; Wang, J.; Liang, H.; Liu, W.; Liu, Y.; Jiang, X.; Wang, Y.; Wan, X.; Cai, W.; Ju, L.; et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **2010**, *18*, 27217–27225. [CrossRef] [PubMed]
59. Lütkenhaus, N.; Jahma, M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J. Phys.* **2002**, *4*, 44. [CrossRef]
60. Engle, R.; Grimaila, M.; Mailloux, L.; Hodson, D.; McLaughlin, C.; Baumgartner, G. Implementing the decoy state protocol in a practically-oriented quantum key distribution system-level model. *J. Def. Model. Simul. Appl. Methodol. Technol.* **2017**, in press.
61. Holes, J.; Mailloux, L.; Grimaila, M.; Hodson, D. An Efficient Testing Process for a Quantum Key Distribution System Modeling Framework. In Proceedings of the International Conference on Scientific Computing (CSC15), Las Vegas, NV, USA, 27–30 July 2015.

62. Hadfield, R.H. Single-photon detectors for optical quantum information applications. *Nat. Photonics* **2009**, *3*, 696–705. [CrossRef]
63. Mink, A.; Nakassis, A. LDPC for QKD reconciliation. *Comput. Sci. Technol. Int. J.* **2012**, *2*, 6–14.
64. ID Quantique. id300 Series Sub-Nanosecond Pulsed Laser Source Datasheet. 2012. Available online: http://www.idquantique.com/images/stories/PDF/id300-laser-source/id300-specs.pdf (accessed on 5 March 2014).
65. OPLINK. Electronically Variable Optical Attenuators. 2014. Available online: http://www.oplink.com/pdf/EVOA-S0012.pdf (accessed on 2 March 2015).
66. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
67. Pearson, D.; Elliott, C. On the optimal mean photon number for quantum cryptography. *arXiv* **2004**, arXiv:quant-ph/0403065.
68. ETSI. Quantum Key Distribution. 8 June 2015. Available Online: www.etsi.org/technologies-Clusters/technologies/quantum-Key-distribution (accessed on 13 June 2016).