Indian Institute of Technology, Kharagpur

Term Paper for Quantum Mechanics

Submitted by –
Kuhu Sharan (22PH10022), Neha Anand Narayankar (22PH10033),
Thejaswini Devakumar (22PH10050)

Decoy State Protocol in Quantum Key Distribution (QKD) systems

Abstract

This paper investigates the effectiveness of Decoy State Quantum Key Distribution (QKD) in mitigating Photon Number Splitting (PNS) attacks. We begin by reviewing the requirements of QKD in changing times and the advantages of Decoy State QKD in thwarting PNS attacks compared to traditional protocols like the BB84 protocol.

Building upon this foundation, the paper delves into establishing a threshold for PNS attack detection with high confidence in high-loss satellite QKD systems. Moving forward, we aim to optimize the selection of decoy MPNs and determine the minimum number of decoy pulses needed to guarantee the absence of PNS attacks for given system parameters.

Table of Contents

1 Introduction

The urgent need for secure communication in our hyper-connected world, which is fuelled by constant technological leaps, is undeniable. Traditional encryption methods are facing challenges due to the rise of quantum computing technology and ever-more-devious hacking tactics. Quantum Key Distribution (QKD), an innovative field combining quantum physics and information theory, emerges as a transformative solution for secure communication.

QKD utilizes the unique principles of quantum mechanics, to establish a secret cryptographic key between parties separated by distance. This key's strength lies in its foundation – the fundamental laws of physics itself..

Over the years, QKD has matured significantly, with protocols like BB84, BBM92, B92, and six-state protocols establishing its theoretical impregnability against any future advancements in computing or technology. Researchers are constantly innovating and pushing the boundaries of secure communication with new ideas like entanglement-based and device-independent QKD.

As the world embraces the potential of quantum technologies, QKD stands tall as a leader in the secure communication revolution. Its unique ability to expose eavesdroppers and remain immune to future quantum-based attacks positions it as the cornerstone of cryptography in the years to come. In this work, we have studied in detail about Decoy State QKD systems, how they are effective in detecting PNS attacks.

2 Literature Review

2.1 Quantum Key Distribution

Unlike traditional cryptographic techniques that rely on complex mathematical algorithms, Quantum Key Distribution exploits the principles of quantum mechanics, specifically superposition and entanglement, to ensure unparalleled security. QKD is an advanced cryptographic method designed to address the inherent challenge of establishing secure encryption keys over vulnerable communication channels.

We consider two parties, commonly known as Alice (the sender) and Bob (the receiver) who want to communicate securely. QKD encodes data using quantum states, typically involving single photons or entangled particle pairs. The quantum states are then transmitted through a specialized quantum channel. The unique principles of quantum mechanics guarantee that any attempt to intercept or measure the transmitted quantum states would inevitably alter their properties, a change immediately detectable by Alice and Bob, thus thwarting any eavesdropping attempts.

The security of these QKD systems is further reinforced by the no-cloning theorem, a fundamental aspect of quantum mechanics. This theorem states that creating identical copies of an unknown quantum state is impossible. Consequently, an eavesdropper (Eve) cannot intercept the quantum states, clone them, and later measure them without detection. Thus, QKD ensures unconditional security, even against adversaries equipped with powerful quantum computers.

Notably, the BB84 protocol, introduced by Bennett and Brassard in 1984, represents one of the pioneering QKD protocols, employing single photons with specific polarizations to represent the encryption key bits. Additionally, the E91 protocol, proposed by Ekert in 1991, utilizes entangled particle pairs to distribute the encryption key securely.

While incredibly secure, QKD faces challenges. Building reliable channels for these quantum states, creating consistent single-photon sources, and scaling the system for long distances are ongoing hurdles. Despite these, researchers are continuing to make strides towards practical QKD applications.

As QKD research continues to evolve, it promises a brighter future for secure communication in the digital age by serving as an invincible safeguard against potential threats posed by quantum computing, guaranteeing the confidentiality and integrity of sensitive information.

2.2 BB84 Protocol

This protocol was proposed by Bennett and Brassard in 1984 (hence called BB84 protocol). Here, Alice and Bob (the two parties who want to communicate securely) define two basis: rectilinear and diagonal. In the rectilinear basis, photons with horizontal polarization (0°) represent bit 0, while vertical polarization (90°) represents bit 1. Similarly, in the diagonal alphabet, photons with polarization angles -45° and 45° represent bits 0 and 1, respectively.

The key distribution process starts with Alice sending Bob a string of bits encoded using photon polarization (qubits) through a quantum channel which is governed by laws of quantum mechanics to transit single photons, each in one of four polarizations: horizontal (0°), vertical (90°), diagonal(45°), antidiagonal (135°).

Bob randomly chooses one of two bases: rectangular (+) or diagonal (×) to measure the arrived signals and keeps the result privately. Observing a photon with diagonal polarization (45°) using the rectilinear basis results in the photon "choosing" horizontal or vertical polarization with a probability of 1/2. Thus, only photons with polarization 0° and 90° can be perfectly measured using a detector aligned in the vertical/horizontal directions (rectilinear basis), while information about diagonally polarized photons (-45° and 45°) is lost. Similarly, using the

diagonal basis, only photons with polarization -45° and 45° can be measured perfectly, losing information about horizontally and vertically polarized photons (0° and 90°). If the basis choice does not match a random result occurs (equal likelihood of 0 or 1); this is due to the inherent uncertainty in the measurement of a randomly encoded single photon.

Bob randomly chooses to measure on the rectilinear or diagonal basis and informs Alice of his choice over a public channel without revealing the measurement result. The new key is formed by retaining the bits where Bob's basis choice aligns with Alice's encoding. Thus, this algorithm ensures that the distributed key comprises approximately half of the bits sent by Alice, while discarding the other half.

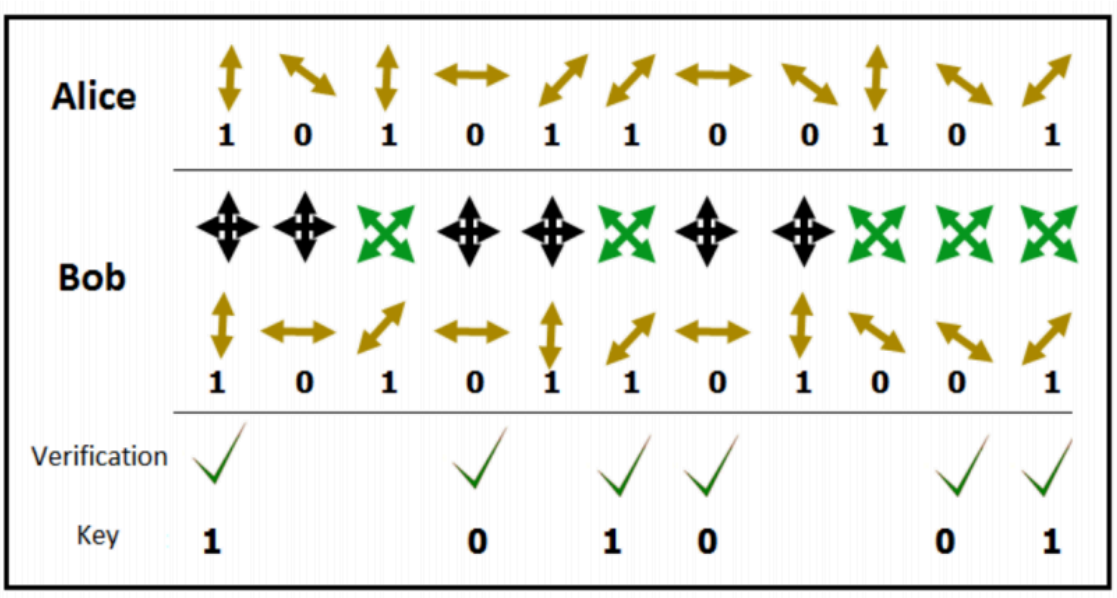


Fig.1 An example of BB84 Protocol

Now, we consider a situation where the eavesdropper Eve is attempting to eavesdrop on the communication between Alice and Bob through the quantum channel, as shown in **fig n**. To obtain information, Eve measures the polarisation of photons using a rectilinear or diagonal basis randomly, similar to Bob. However, if Eve selects the wrong basis, the polarisation changes. If the bit initially has vertical polarisation (coded as 1), but after Eve's eavesdropping using the diagonal basis, the photon's polarisation becomes 45°. After Bob's measurement, the photon exhibits horizontal polarisation, leading to a decoded value of 0. Despite Alice sending a vertically polarised photon and Bob using the correct rectilinear basis, they obtain different bits. Comparing the parts of the key exchanged publicly allows Alice and Bob to detect eavesdropping.

Therefore, passive eavesdropping is not possible, as Eve's attempts to eavesdrop change the quantum states of the photons, and she cannot clone an unknown state of the photon. Consequently, the BB84 protocol ensures a high level of security.

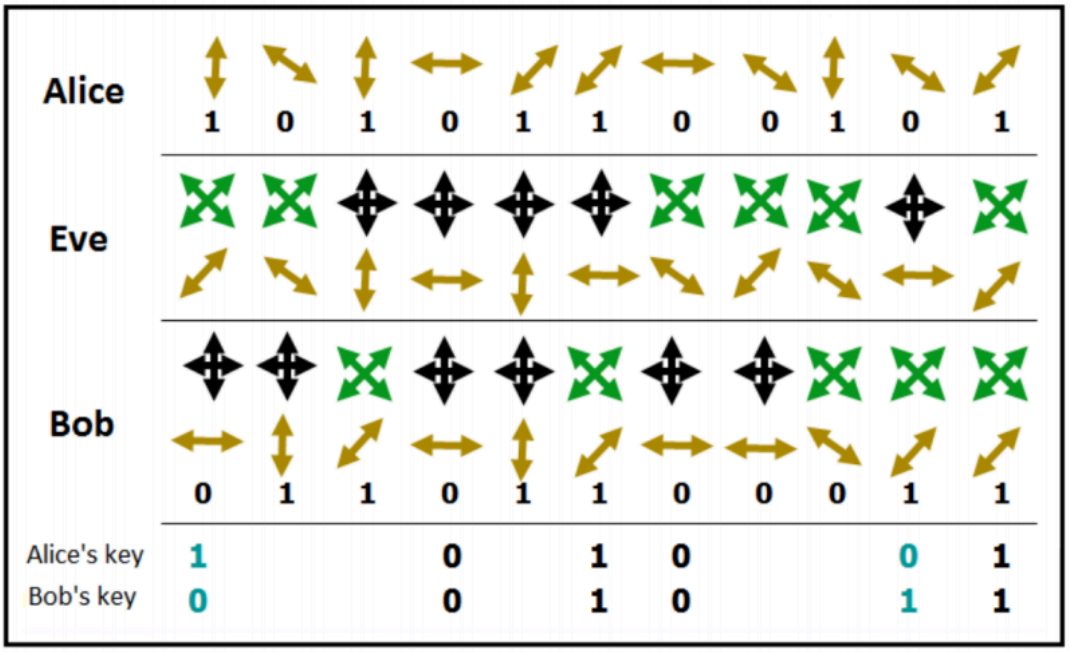


Fig. 2 Eavesdropping in BB84 Protocol

3 Photon Number Splitting Attack

BB84 security proofs assume several idealities, including perfect on-demand single photon sources. Currently, reliable on-demand single photon sources are not available nor are they expected in the near term. Therefore, most QKD systems attenuate classical laser pulses down from millions of photons to weak coherent pulses (WCP) 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 Mean Photon Number (MPN).

$$P(\mu) = \frac{\mu^n e^{-\mu}}{n!} \tag{2.3.1}$$

Where μ represents the average number of photons in a pulse (MPN) and n represents the number of photons contained in the pulse.

Thus, there is a nonzero probability to get a state with more than one photon. Then Eve may suppress the quantum state and keep one photon of the state that has more than one photon (commonly called multi photon, correspondingly, single photon denotes the state with only one photon). Moreover, Eve may block the single photon state, split the multi photon state and improve the transmission efficiency with her superior technologies to compensate for the loss of blocking single photon.

This limitation of the source is taken up by Photon Number splitting (PNS). PNS is a powerful attack and focuses on a realistic photon source. In accordance with QKD security proofs, Eve is an all-powerful adversary limited only by the laws of

quantum mechanics. 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.

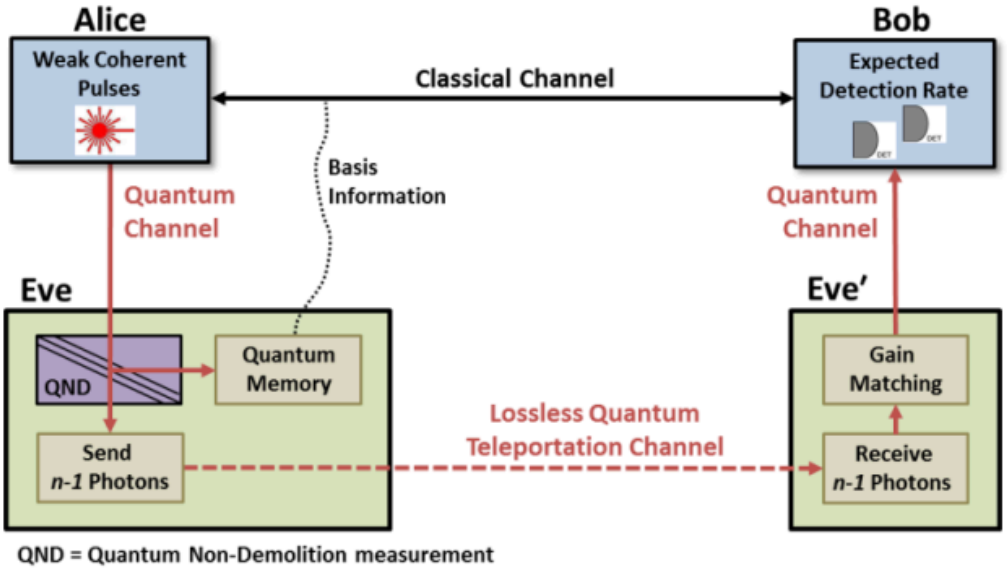
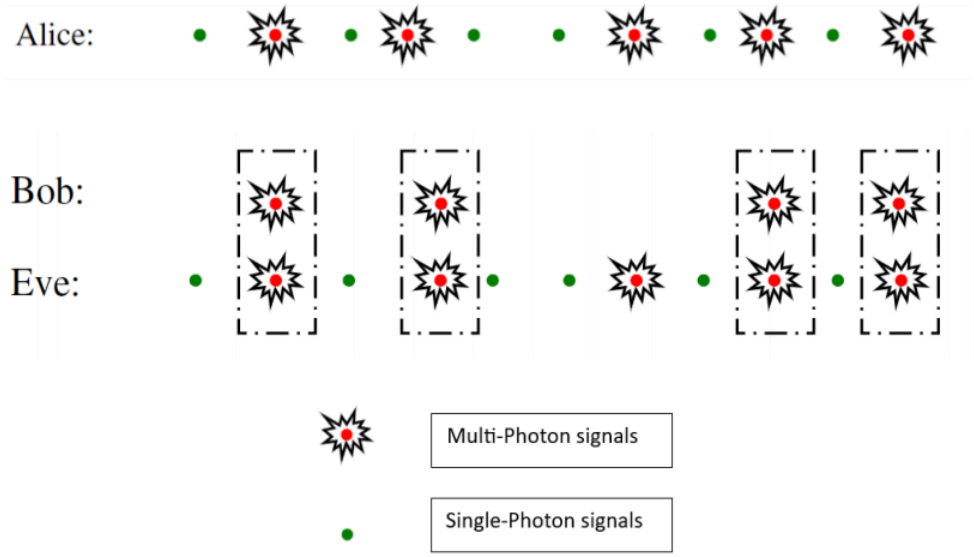


Fig. 3 Eavesdropper is shown conducting a PNS attack against the QKD System.

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. An Eve' entity is also present in close proximity to Bob to regulate the lossless transmission of photons so as to not exceed Bob's expected detection rate; thus, avoiding obvious detection.

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

Fig.4



Multi-photon events and Photon Number Splitting attacks

4 Mitigation of attack - Decoy State Protocol

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 [4]

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, . . . , N which she determines using her QND measurement.

State	Purpose
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).
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.
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).

Table 1. Example Decoy State Protocol Configuration

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

$$Y_n^{signal} = Y_n^{decoy} = Y_n^{expected}$$

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.

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

Other researchers utilize a efficiency based security condition [5] which provides a direct measurement in a cost-conscience QKD system implementation $\eta^{signal} = \eta^{decoy}$

Where,

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

and,

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

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

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

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

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) 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) [5] mentions Alice's pulse-to-pulse variation is of primary interest, and specifically, the variation in her laser source.

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 pulses are blocked since the higher MPN generates more multi-photon pulses. Thus, Eve significantly reduces the decoy state efficiency. This behaviour 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 ≥2 photons).

5 Application of Decoy State QKD - BB84 Protocol

As mentioned earlier Alice and Bob are the two parties who wish to communicate securely while an eavesdropper Eve attempts to listen to the channel and gain some information about the secret key

5.1. Quantum Exchange

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 has 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, who measures them using specialized single photon detectors.

At the end of this process, Alice and Bob both possess a correlated but not identical sequence of random numbers. This is called the "raw key"

5.2. Key Sift

After the raw key exchange, the Key Sifting step becomes instrumental in refining the shared key between Alice and Bob. In this phase, both parties publicly compare the measurement bases they used during the quantum state transmission. They discard all the bits from their lists for which the bases are incompatible. The remaining bits constitute the "sifted key".

Despite the sifting process, the sifted key may not be identical between Alice and Bob due to various imperfections in the quantum communication channel or the presence of an eavesdropper, Eve. Any errors resulting from channel malfunction or eavesdropping are attributed to Eve.

In practice, achieving a completely error-free QKD system is challenging, and the possibility of Eve's interference necessitates additional security measures. To address this, further steps, such as error correction and privacy amplification, are often employed to identify and correct errors in the sifted key and enhance its security. These additional processes are vital in mitigating potential eavesdropping attempts and ensuring the final shared key is both reliable and secure for confidential communication between Alice and Bob.

5.3 Error Estimation

Bit error estimation is a crucial aspect of Quantum Key Distribution (QKD) systems as it helps identify and quantify errors in the transmitted quantum states. These errors can result from various causes, such as disturbances in the quantum channel, optical misalignment, or noise in detectors.

In QKD, the error rate is referred to as the Quantum Bit Error Rate (QBER), which measures the ratio of the number of wrong bits to the total number of bits exchanged.

The expected value of error rate is an essential parameter in QKD systems and is typically measured without eavesdropping. Practical measurements of the QBER allow us to estimate its expected range.

While a stricter threshold on calculated QBER given by expected value, increases the likelihood of rejecting eavesdropped communication, fluctuations in the optical channel may lead to accepting a higher level of QBER in practice. Therefore, some eavesdropped bits may be accepted if Eve uncovers only a small part of the distributed key.

Another critical parameter in bit error estimation is the number of compared bits. To estimate the number of errors in the exchanged key, a portion of the bits needs to be uncovered and compared. A larger number of compared bits during QBER estimation enhances the probability of rejecting eavesdropped communication. However, all uncovered bits must be rejected, leading to a reduction in the length of the secret key.

5.4 Error Reconciliation

Error reconciliation is a crucial process in Quantum Key Distribution (QKD), a state-of-the-art cryptographic technique that ensures secure key exchange over insecure channels. During QKD, errors may occur in the transmitted quantum states due to technical imperfections or external disturbances. Error reconciliation aims to correct these errors in the exchanged key without revealing excessive information to potential eavesdroppers.

Error reconciliation is vital because errors can occur due to various reasons, and a reliable method is needed to rectify these errors efficiently and securely. The success of error reconciliation plays a significant role in establishing a trustworthy encryption key for secure communication between Alice and Bob in a quantum communication network

5.5 Privacy Amplification

Privacy amplification is the art of distilling a highly secret key from a partially secure string. Privacy amplification in Quantum Key Distribution (QKD) ensures a secure secret key by distilling a shorter, random key from the initial key, mitigating information leakage to potential eavesdroppers. It involves bitwise operations with a pre-shared random seed, making the final key robust against attacks and ensuring reliable quantum communication.

5.6 Detecting PNS attack using Decoy State QKD

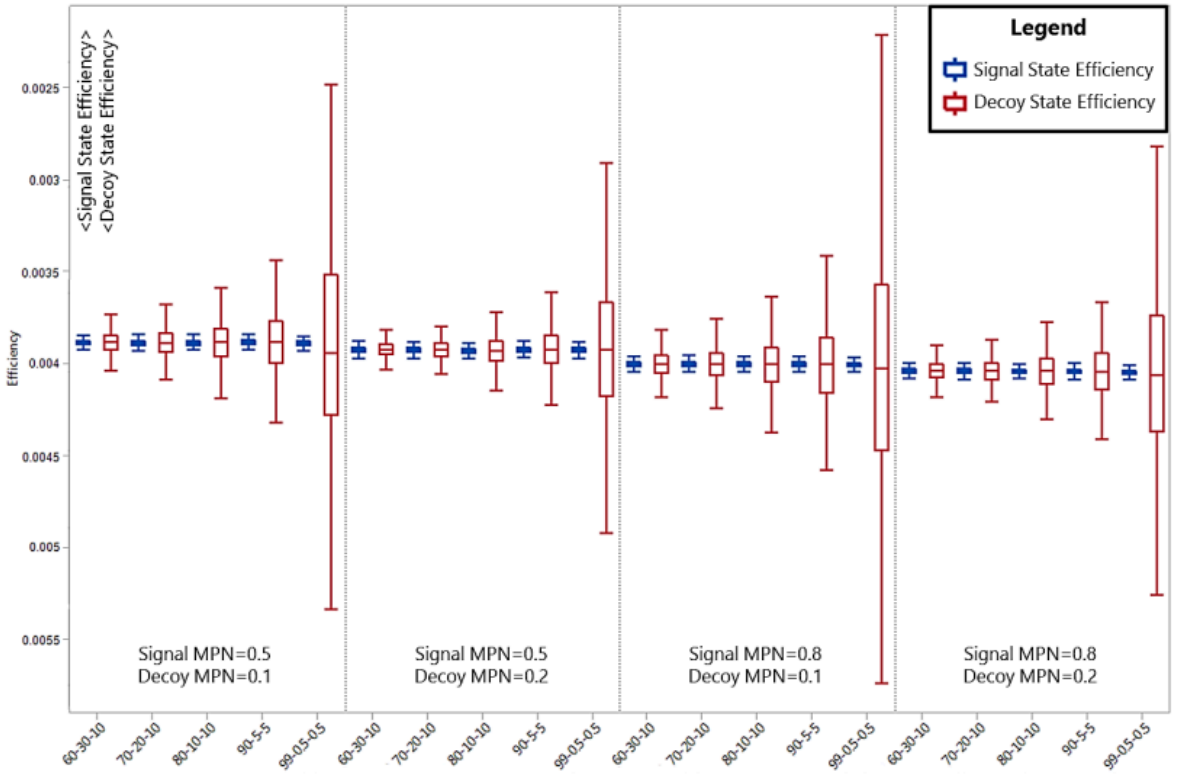


Fig. 5 Simulation Results from [5] examined when operating in normal conditions. In each configuration studied, the signal state efficiency and decoy state efficiencies are the same (within expected variation tolerances). The security condition equation is satisfied.

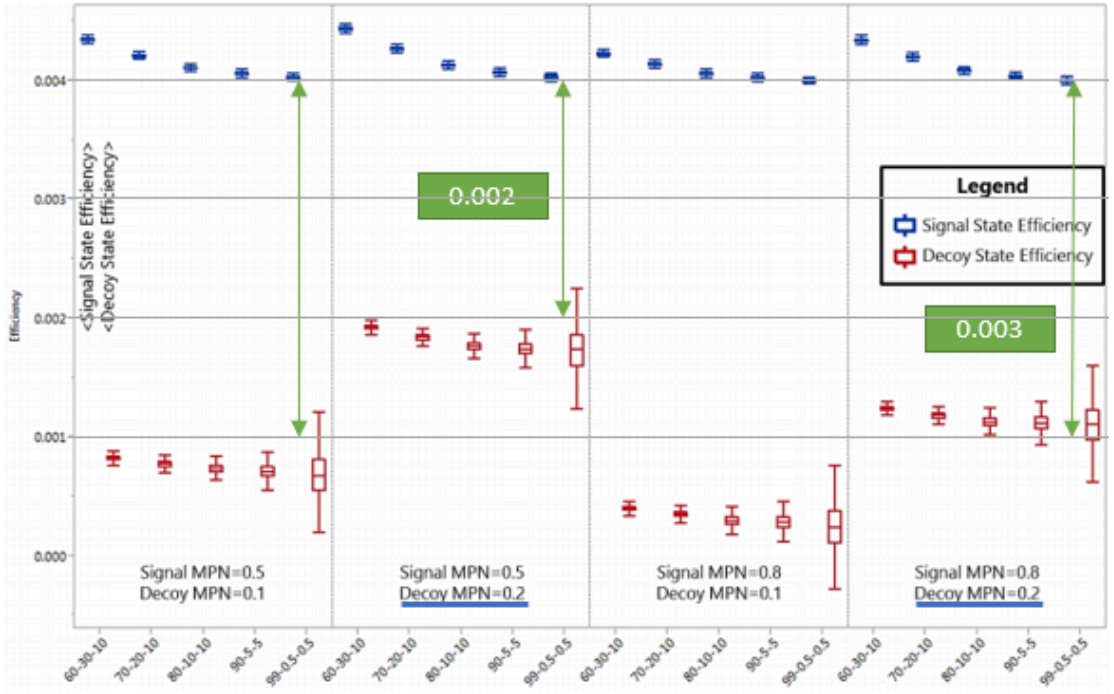


Fig. 6 Simulation Results examined when subject to PNS attacks [5].

In each configuration studied, the signal state efficiency and decoy state efficiencies are statistically different (outside expected variation tolerances). The security condition equation is not satisfied. Observe the difference in Decoy state efficiency with reference to the signal state efficiency for the same decoy MPN and different signal MPN.

6 Conclusion

In conclusion, this report briefly explained simple QKD protocols, and investigated the potential of Decoy State Quantum Key Distribution (QKD) to safeguard communication against Photon Number Splitting attacks, particularly in high-loss environments like satellite-to-ground channels. We began by highlighting the growing need for secure communication solutions and the inherent vulnerabilities of traditional protocols like BB84 to PNS attacks. Decoy State QKD, on the other hand, offers a significant advantage by introducing decoy states alongside signal pulses, enabling robust detection of PNS attempts.

7 References

[1] Bennett CH and Brassard G. Quantum cryptography: public key distribution and coin tossing. In:Proceedings of IEEE international conference on computers, systems and signal processing, Bangalore, India, December 10–12, 1984.

[2]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.

[3] Loepp, S.; Wootters, W.K. Protecting Information; Cambridge University Press: New York, NY, USA, 2006

[4] Ma, X.; Qi, B.; Zhao, Y.; Lo, H.-K. Practical decoy state for quantum key distribution. Phys. Rev. 2005,72, 012326.

[5] Modeling, Simulation, and Performance Analysis of Decoy State Enabled Quantum Key Distribution Systems Logan O. Mailloux, Michael R. Grimaila, Douglas D. Hodson, Ryan Engle, Colin McLaughlin, and Gerald Baumgartner

[6] Implementing the decoy state protocol in a practically oriented Quantum Key Distribution system-level model- Ryan D Engle, Logan O Mailloux, Michael R Grimaila, Douglas D Hodson, Colin V McLaughlin, and Gerald Baumgartner

[7] Efficient decoy-state quantum key distribution with quantified security" by Huang et al. (2013) -M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty and A. J. Shields

[8] Pulse number splitting attacks in decoy-state quantum key distribution" by Lucamarini et al. (2010) - Xiao-Ming Chen, Lei Chen, Ya-Long Yan, Yan-Lin Tang