Weak Coherent and Heralded Single Photon Sources for Quantum Secured Imaging and Sensing

Siddhant Vernekar * and Jolly Xavier *

Posted Date: 14 July 2025

doi: 10.20944/preprints202507.1064.v1

Keywords: quantum secure imaging; quantum secure sensing; quantum key distribution; weak coherent source; heralded single photon source; high dimensional states; photon number splitting attacks

 doi:10.20944/preprints202507.1064.v1

Article

Weak Coherent and Heralded Single Photon Sources for Quantum Secured Imaging and Sensing

Siddhant Vernekar [1,*] and Jolly Xavier [1,2,*]

[1] SeNSE, Indian Institute of Technology Delhi, Haus Khaz, New Delhi, 110016, India

[2] Department of Physics and Astronomy, University of Exeter, Exeter EX4 4QD, UK

* Correspondence: idz228534@iitd.ac.in; jxavier@sense.iitd.ac.in; j.xavier@exeter.ac.uk

Abstract

An ever-increasing demand for higher photon generation rates in quantum light sources often leads to the generation of multiple photon pairs, making quantum secure imaging, sensing, and communication vulnerable to photon number splitting (PNS) attacks. Here, we investigate the use of weak coherent sources (WCS) and heralded single-photon sources (HSPS) in conjunction with quantum key distribution protocols to mitigate these risks. Our initial observation shows that the BB84 protocol using heralded single-photon sources demonstrates an advantage in secured information transfer over the weak coherent sources. We then extend our comparative study between WCS and HSPS to high dimensional protocols and do a rigorous analysis to estimate a benchmark in quantum advantage in such schemes. When combined with high-dimensional states (hybrid encoding), the two-state non-orthogonal encoding protocol offers an increased resistance to PNS attacks. These findings suggest that integrating high-dimensional encoding can significantly strengthen the security and performance of quantum secure imaging, sensing, and communication systems, paving the way for more practical and resilient implementations.

Keywords: quantum secure imaging; quantum secure sensing; quantum key distribution; weak coherent source; heralded single photon source; high dimensional states; photon number splitting attacks

1. Introduction

Quantum imaging and sensing protocols offer enhanced measurement schemes compared to traditional schemes, finding applications in measuring light-sensitive samples under low illumination [1–8]. Quantum communication, particularly through quantum key distribution (QKD), offers a fundamentally secure approach to information transfer against attacks such as intercept resend, photon number splitting(PNS), and unambiguous state discrimination(USD) [9–12]. Quantum secure imaging and sensing are emerging disciplines that enable secure information transfer and measurements [13–21]. However, for practical deployment, it is essential that these protocols remain robust during continuous operation, even in the presence of potential adversarial attacks, and are an active area of research [22–26].

Weak coherent sources (WCS) and spontaneous parametric down-conversion (SPDC) based sources have been widely employed in QKD, quantum imaging, and sensing applications [27–34]. High-dimensional(HD) quantum states have also been explored to improve the quantum communication, imaging, and sensing protocols [35–41]. At high operating speeds, generating all four quantum states (as in BB84 QKD protocol) becomes technically challenging due to the increased voltage demands of modulation devices. In contrast, two-state QKD protocols are more practical under such conditions, requiring less modulation effort. The two-state protocol, however, requires an additional monitoring detector to guard against advanced unambiguous state discrimination (USD) attacks [12].

 doi:10.20944/preprints202507.1064.v1

This work expands the quantum secure information transfer landscape by examining SPDC-based heralded single-photon sources (HSPS) and WCS under decoy and non-decoy QKD protocol configurations. Additionally, we investigate both BB84 and B92 QKD protocols, analyzing their performance in quantum secure information applications. To further enhance the resilience of these systems, we investigate high-dimensional QKD protocols (HD-B92) to improve resistance against PNS and USD attacks. We adapt these countermeasures to our mathematical modelling by drawing on solutions developed in the HD-QKD literature.

2. Mathematical Modelling and Methods

2.1. Photon Number Distribution for Quantum States of a Weak Coherent Source and a Heralded Single Photon Source

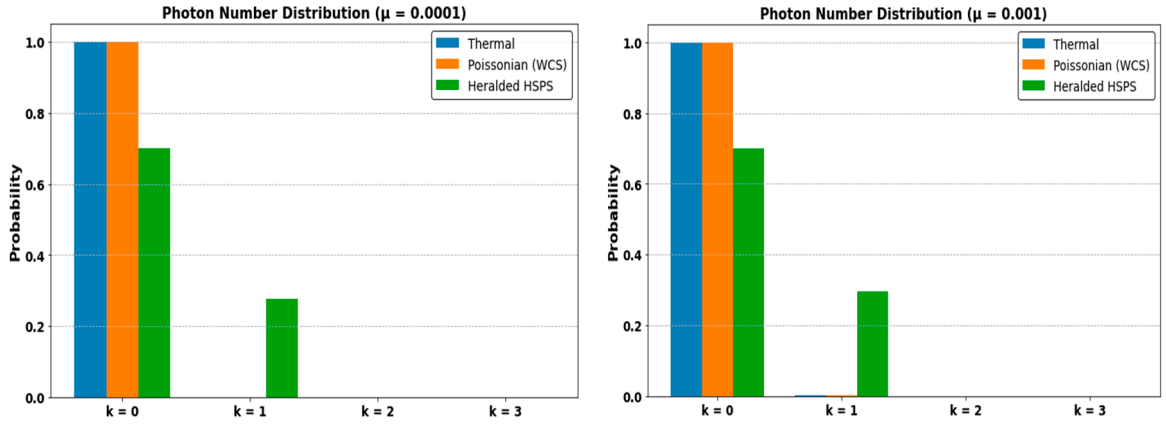
The equation describing the photon number distribution for WCS is given by equation 1, and for SPDC-based HSPS(thermal) is given by equation 2 [42,43].

$$P_{k,x}^{weak} = \frac{e^{-x} * x^k}{k!} \quad (1)$$

$$p_{k,x}^{HSPS_{per}} = \frac{x^k}{(1+x)^{k+1}} * \frac{\left(1-(1-\eta_A)^k + d_A\right)}{P_x^{post}}; \quad (2)$$

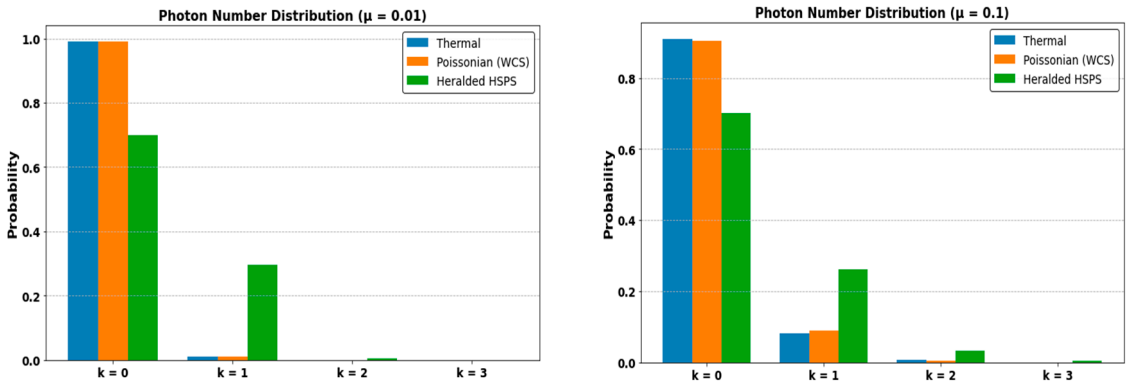
where x is the mean photon number, knumber of photons, η_A represents the efficiency the source end, d_A is the dark count rate for the detectors, P_x^{post} is the post-selected probability given by $P_x^{post} = \frac{x*\eta_A}{1+x*\eta_A} + d_A$; $p_{0,x} = 1 - P_x^{cor} + p_{0,x}^{per} P_x^{cor}$, and $p_{k,x} = p_{k,x}^{per} P_x^{cor}$. $P_x^{cor} = 0.3$;

Figure 1 illustrates the photon number distributions for thermal, WCS (Poissonian), and HSPS(thermal) at various mean photon numbers: 0.0001, 0.001, 0.01, and 0.1. As observed, the vacuum component (zero-photon probability) is significantly suppressed in the heralded single-photon source. However, as the mean photon number increases, multiphoton components begin to appear across all sources, highlighting the growing probability of more than one photon per pulse, which is critical when assessing security and performance in quantum secure communication, imaging, and sensing protocols.



(**a**) (**b**)

 doi:10.20944/preprints202507.1064.v1



(c) (d)

Figure 1. Photon number distributions for thermal (blue), WCS (orange), and HSPS (green) at mean photon numbers (a)0.0001, (b) 0.001, (c) 0.01, and (d) 0.1.

2.2. Security Analysis for Non-Ideal Conditions to Obtain Secure Bit Rate vs Loss in dB

The secure bit rate without decoy state for BB84 and B92 protocol is given by equations 3 and 4, respectively [12,44–46]

$$R_{BB84} = qQ_{\mu}\{(1-\Delta)\{(\log_2 d) - [H_d(e_1)]\}\} - f(E_{\mu}) * H_d(E_{\mu}); \quad (3)$$

Where q is parameter depending on QKD protocol, $q = \frac{1}{2}$ for BB84 and $q = \frac{1}{4}$ for B92; Q_{μ} is the overall gain, d is the dimension, H is the binary Shannon entropy, e_1 is the error rate of single photons given by $e_1 = \frac{E_{\mu}}{\Delta}$; $\Delta = \frac{1-P_0-P_1}{Q_{\mu}}$; here E_{μ} is the overall error rate, Δ is term considering multiphoton probablity against PNS attack. $H_d(p) = -p * log_2[\frac{p}{d-1}] - (1-p) * \log_2(1-p)]$; and $f(E_{\mu}) = 1.22$;

$$R_{B92} = qQ_{\mu}\{(1-\Delta')\{(\log_2 d) - [H_d(e_1)]\}\} - f(E_{\mu}) * H_d(E_{\mu}) - I_{AE}^{USD}\}; \quad (4)$$

Here I_{AE}^{USD} is the information leakage due to USD attack given by $I_{AE}^{USD} = \frac{(1-\eta)(1-cos\alpha)^N}{\eta(1-(1-cos\alpha)^N)}$;

N is the number of multiple qubit encoding which in high dimensional(hybrid encoding) terms is $N = \log_2 d$, $\Delta' = \frac{1-P_0-P_1-P_2}{Q_{\mu}}$ is used by considering the contribution of 2 photon pulses in B92 protocol due to its robutness against PNS attack.

$$Q_x^{WCS} = Y_o + 1 - e^{-\mu*\eta}; E_x = \frac{(e_0-e_d)d_B}{Q_x^{WCS}} + e_d;$$

$$Q_x^{HSPS} = \frac{1}{P_x^{post}}\left[\frac{x\eta(1+d_A)}{1+x\eta} + \frac{x\eta_A(1+d_B)}{1+x\eta_A} + \frac{1}{1+x(\eta+\eta_A-\eta\eta_A)} - (1-d_Ad_B)\right] \; ; \; E_x =$$

$$\frac{(e_0-e_d)d_B}{Q_x^{HSPS}} + e_d.$$

The secure bit rate with decoy state for BB84 and B92 protocol is given by equation 5 [10,38,43]

$$R = q\{Q_0 * (\log_2 d) + Q_1 * [\log_2 d - H_d(e_1)] - Q_{\mu} * f(E_{\mu}) * H_d(E_{\mu})\}; \quad (5)$$

where $Q_0 = Y_0 * p_0(\mu)$; $e_0 = \frac{d-1}{d}$; $Y_0 = 1-(1-d_B)^d$; $Q_1 = Y_1 * p_1(\mu)$;

$$Y_1 = \frac{p_2(\mu)*Q_v - p_2(v)*Q_{\mu} - Y_0[p_0(v)*p_2(\mu) - p_0(\mu)*p_2(v)]}{(p_1(v)*p_2(\mu) - p_1(\mu)*p_2(v)\}}; \; e_1 = \{Q_{\mu} * E_{\mu} - e_0 * Y_0 * p_0(\mu)\}/\{Y_1 * p_1(\mu)\}.$$

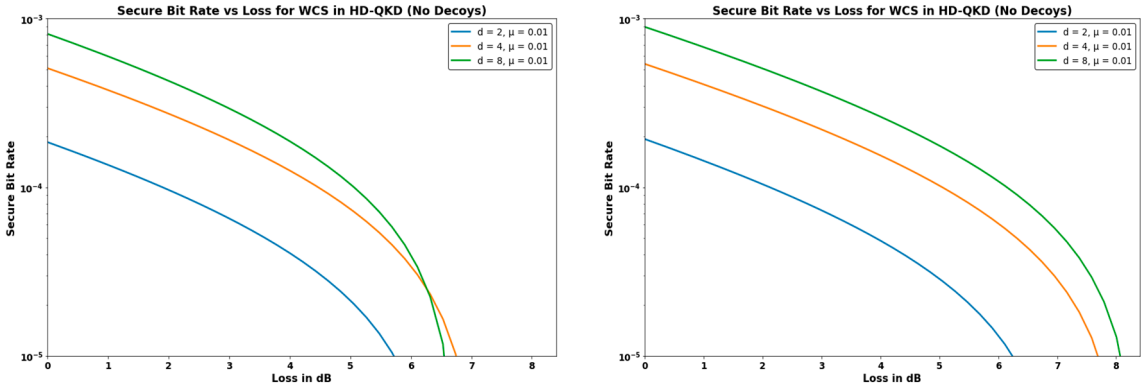
The shared parameter values used in simulations are as follows: channel attenuation(α) = 0.21 (dB/km), detection efficiencyat receiver (η_b) = 0.045, heralding arm efficiency(η_A) = 0.8, dark count probablity in heralding detector (d_A) =10^{-5}, misalignment error (e_d)= 0.033.

3. Results and Discussion

Figure 2 presents the secure bit rate as a function of channel loss (in dB) for the BB84 QKD protocol using a WCS without decoy state analysis. Two scenarios are shown, corresponding to

 doi:10.20944/preprints202507.1064.v1

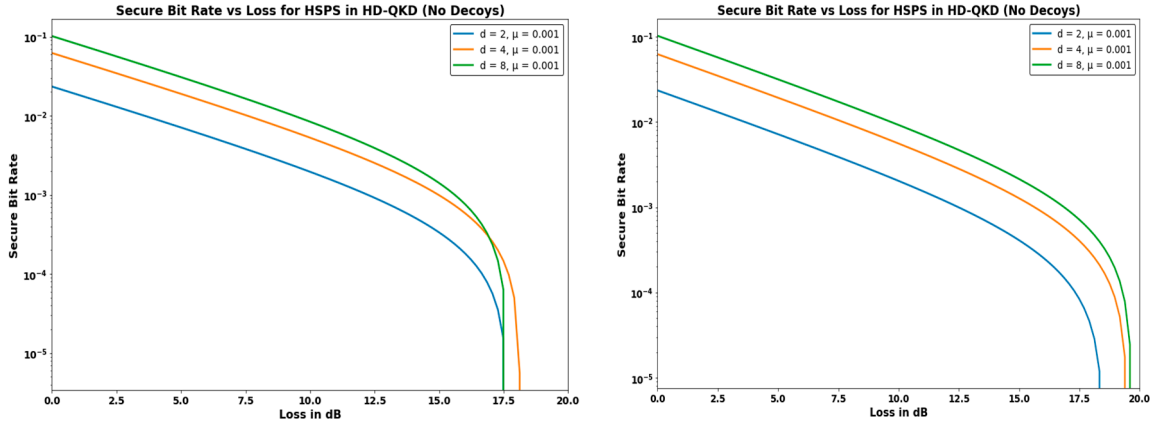
different dark count probabilities of Bob's detector: (a) $d_b = 10^{-6}$ and (b) $d_b = 10^{-7}$. A lower dark count probability enhances the signal-to-noise ratio, thereby improving the maximum quantum secure information transfer distance. This performance improvement demonstrates the importance of low-noise detectors in practical quantum communication. When such low-noise conditions are combined with high-dimensional encoding schemes, secure distance and bit rate gains can be expected.



(**a**) (**b**)

Figure 2. Secure bit rate versus channel loss (dB) for the BB84 protocol using a WCS without decoy state analysis. Two detector dark count probabilities are considered: (**a**) WCS $d_b = 10^{-6}$; (**b**) WCS $d_b = 10^{-7}$.

Figure 3 shows the secure bit rate versus channel loss (in dB) for the BB84 protocol using a HSPS without decoy state analysis. The results are plotted for two different dark count probabilities of Bob's detector: (a) $d_b = 10^{-5}$and (b) $d_b = 10^{-6}$. It can be observed that the HSPS remains effective even in the presence of relatively high detector noise ($d_b = 10^{-5}$), achieving a reasonable secure distance. This robustness to noise highlights one of the key advantages of HSPS in practical quantum secure information transfer scenarios, particularly when high-performance detectors are not available. It is observed that the BB84 protocol using HSPS demonstrates an advantage in secure distance of around 10 dB over WCS without decoy states.



(**a**) (**b**)

Figure 3. Secure bit rate as a function of channel loss (dB) for the BB84 protocol using a HSPS without decoy state analysis. Two dark count probabilities are considered: (**a**) HSPS $d_b = 10^{-5}$; (**b**) HSPS $d_b = 10^{-6}$.

Figure 4 presents the secure bit rate versus channel loss for the B92 protocol using a WCS. Subplot (a) shows the case where two-photon contributions are excluded, while (b)–(d) incorporate the two-photon components. WCS-based B92 protocol benefits from its intrinsic resistance to PNS attacks, allowing the secure bits to be extracted even in the presence of multiphoton pulses using high

 doi:10.20944/preprints202507.1064.v1

dimensional (hybrid encoding). This demonstrates that B92, when used with a WCS, can maintain security without decoy state analysis and avoid the protocol to stop under PNS attack.

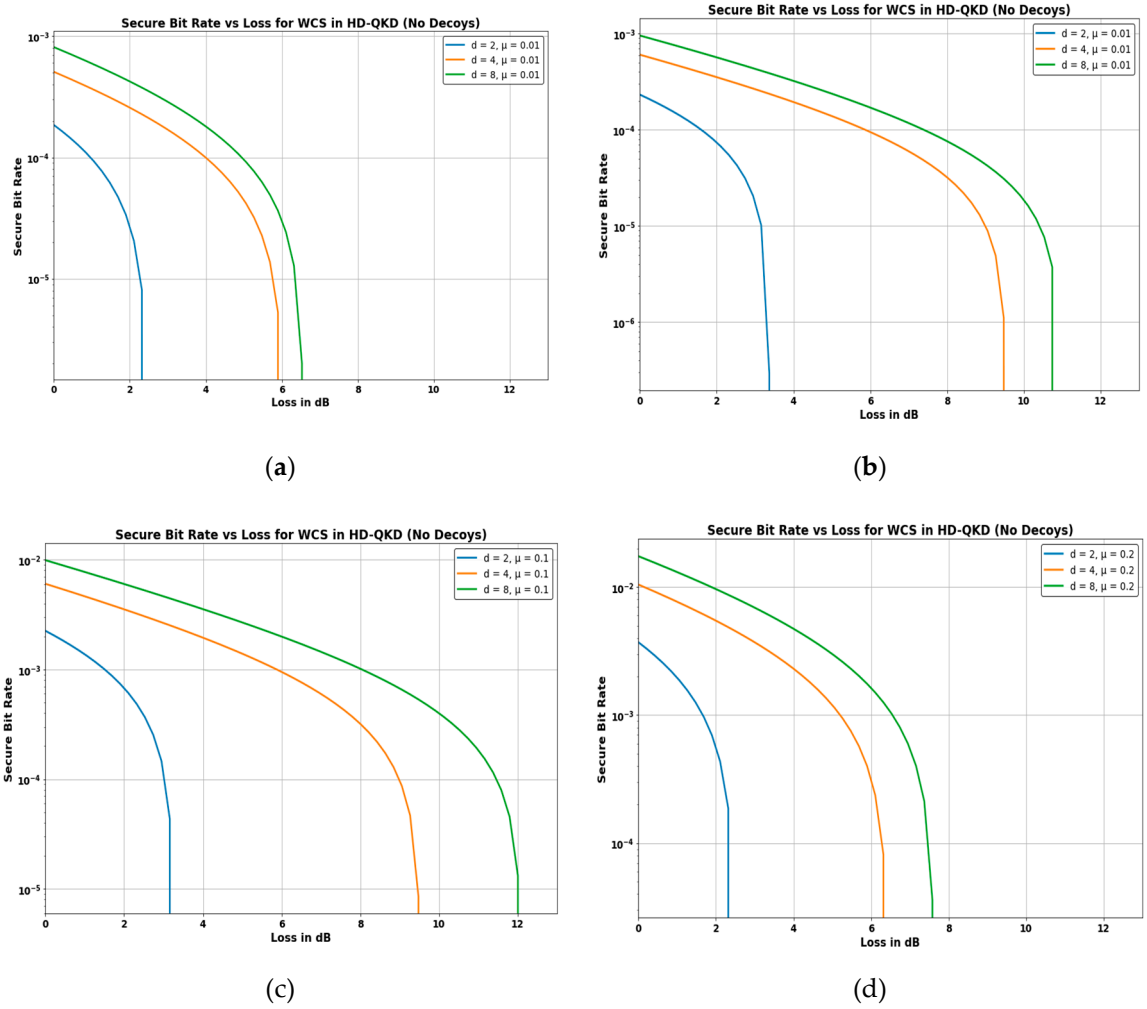


Figure 4.: Secure bit rate versus channel loss (dB) for the B92 protocol using a WCS without decoy state analysis. (**a**) WCS $\Delta = \frac{1-P_0-P_1}{Q_\mu}$; $\mu = 0.01$; (**b**) WCS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.01$. (**c**) WCS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.1$. (**d**) WCS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.2$.

Figure 5 presents the secure bit rate versus channel loss for the B92 protocol without decoy state analysis for HSPS. Plot (a) shows the case where two-photon contributions are excluded from the key rate calculation, while plots (b)–(d) incorporate two-photon contributions. In the HD B92 with WCS, d=8 over d=2 has an advantage of around 9dB, while the HSPS-based HD B92 protocol achieves around 15 dB advantage for the same high dimensional (hybrid encoding) upgrade. Moreover, in secure information transfer distance, HSPS outperforms WCS by around 6-7 dB in the HDB92 configuration in terms of quantum secure information transfer distance.

Figure 6 compares the performance of (a) WCS and (b) HSPS under decoy state analysis using the BB84 protocol. Including decoy states significantly enhances the secure distance and enables detection of PNS attacks. While HSPS achieves a longer secure transmission distance, WCS benefits from a much higher photon emission rate. As a result, although HSPS provides superior distance performance, the overall bit rate is often higher for WCS when the overall figure of merit is considered concerning the photon counts obtained from the source, making it a practical choice in many real-world systems. Finally, implementing decoy states provides a further gain of 15–20 dB compared to schemes without decoy states.

 doi:10.20944/preprints202507.1064.v1

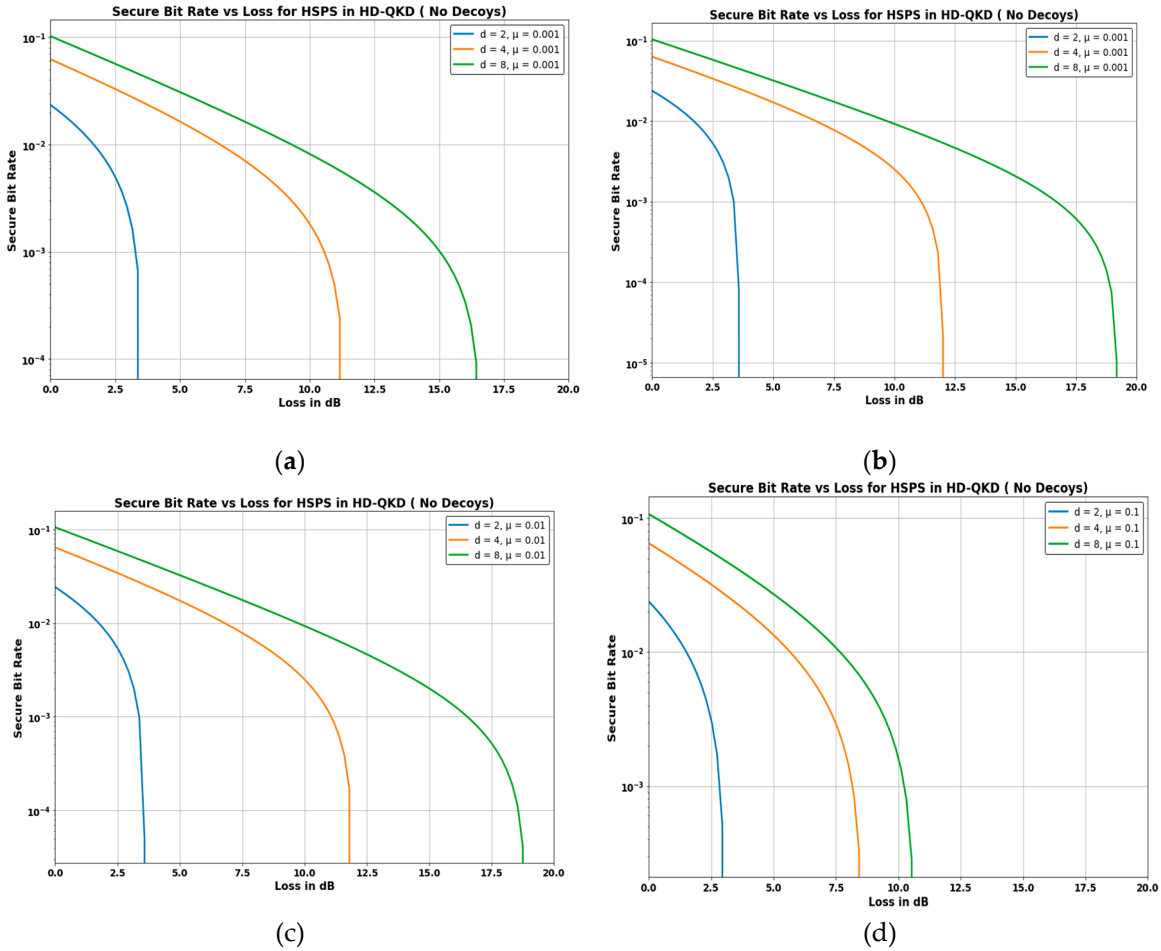


Figure 5.: Secure bit rate versus channel loss (dB) for the B92 protocol without decoy state analysis. (**a**) HSPS $\Delta = \frac{1-P_0-P_1}{Q_\mu}$; $\mu = 0.001$; (**b**) HSPS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.001$. (**c**) HSPS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.01$. (**d**) HSPS $\Delta = \frac{1-P_0-P_1-P_2}{Q_\mu}$; $\mu = 0.1$.

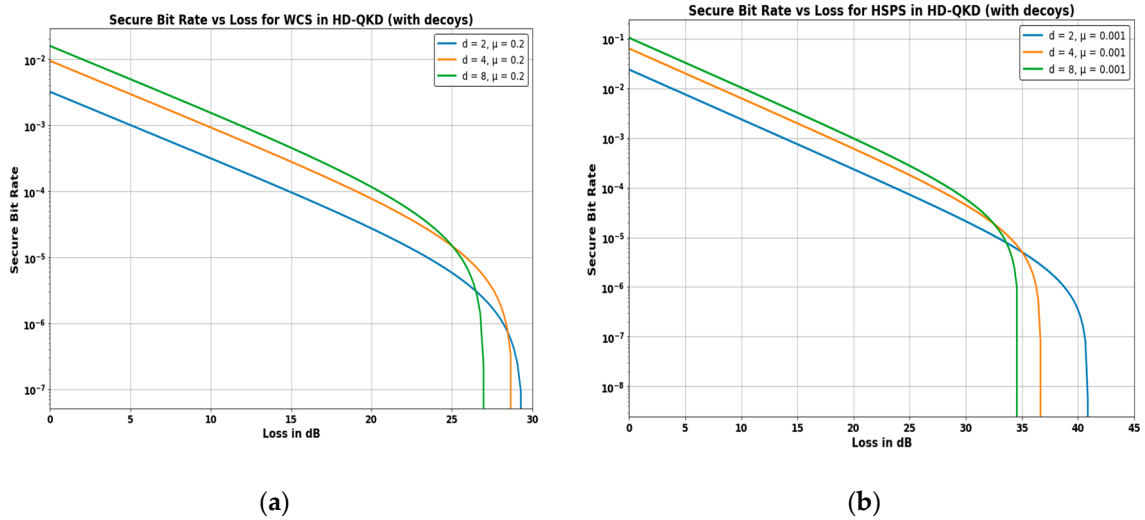


Figure 6. Secure bit rate versus channel loss (dB) with decoy state analysis for the BB84 protocol using (**a**) WCS $d_b = 10^{-6}$ *and* $v = 0.1$.; (**b**) HSPS $d_b = 10^{-6}$ *and* $v = 0.0001$.

HD quantum states enhance both security and bits per pulse in quantum communication. In quantum imaging and sensing, samples may exhibit sensitivity to high-dimensional photon degrees of freedom, or multiple degrees of freedom, such as polarization and orbital angular momentum, can

 doi:10.20944/preprints202507.1064.v1

be exploited for probing. WCS can generate higher photon rates, which are advantageous for key generation rates in communication. Considering the WCS advantage of higher photon counts of about three orders based on current technology, it gives a higher secure bit rate of 1-2 orders when considering the overall figure of merit for secure bits with repetition rate of the source. In contrast, HSPS, which have reduced vacuum contributions, are more suitable to securely probing samples over longer distances at low photon illumination.

4. Conclusion

Our analysis focuses on the photon number statistics of WCS and HSPS, examining their roles in quantum secure imaging, sensing, and communication. Nonorthogonal two state protocols offer resilience to PNS attack to a certain threshold of multi-photon components without halting the quantum secure information transfer in non-ideal source conditions. HSPS is particularly beneficial in high-loss settings due to its reduced vacuum component, allowing for extended secure distances. However, their practical advantage relies on highly efficient and low-loss components in encoding, detection, and coupling. In contrast, WCSs produce higher photon rates, making them advantageous for high-throughput applications, including precision quantum sensing. Despite a higher vacuum component, their compatibility with GHz clock rates and decoy-state methods makes them suitable for secure communication, imaging and sensing scenarios. Combining HD state encoding introduces a trade-off: while it improves security and bits per pulse in ideal conditions, performance declines with increasing channel loss. Also, the modulation speed of devices to encode high dimensional quantum states need to improve to outperform low dimensional high-speed counterparts. Still, such configurations support a broader range of secure imaging and sensing applications. Resistance to both quantum and classical jamming attacks is possible, where the framework can adapt by subtracting mutual information of an adversary from the secure bit rate equation, to estimate secure distances accordingly. Moreover, these findings have direct implications for the design of quantum networks, where flexible combinations of source types dimensionality and protocol choices can be optimized based on channel conditions and application goals—whether it be quantum secure imaging, sensing, or communication. Thus, the proposed analysis supports resilient architectures for quantum networks operating in real-world noisy and lossy conditions.

Author Contributions: Both authors contributed equally to this work

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

Acknowledgments: SV gratefully acknowledges PhD research financial support from MHRD, Government of India.

Conflicts of Interest: The authors declare no conflicts of interest

Abbreviations

The following abbreviations are used in this manuscript:

PNS	Photon number splitting attacks
QKD	Quantum key distribution
HSPS	Heralded single photon sources
WCS	Weak coherent sources
HD	High dimensional states
SPDC	Spontaneous parametric down conversion
USD	Unambiguous state discrimination attacks

 doi:10.20944/preprints202507.1064.v1

References

1. Defienne, H.; Bowen, W.P.; Chekhova, M.; Lemos, G.B.; Oron, D.; Ramelow, S.; Treps, N.; Faccio, D. Advances in Quantum Imaging. *Nat. Photonics* **2024**, *18*, 1024–1036, doi:10.1038/s41566-024-01516-w.
2. Vernekar, S.; Xavier, J. Quantum Correlation Enhanced Optical Imaging. *Quantum Beam Sci.* **2024**, *8*, 19, doi:10.3390/qubs8030019.
3. Moodley, C.; Forbes, A. Advances in Quantum Imaging with Machine Intelligence. *Laser Photonics Rev.* **2024**, *2300939*, doi:10.1002/lpor.202300939.
4. Jones, C.; Xavier, J.; Vartabi Kashanian, S.; Nguyen, M.; Aharonovich, I.; Vollmer, F. Time-Dependent Mandel Q Parameter Analysis for a Hexagonal Boron Nitride Single Photon Source. *Opt. Express* **2023**, *31*, 10794, doi:10.1364/oe.485216.
5. Xavier, J.; Yu, D.; Vollmer, F.; Jones, C.; Zossimova, E. Quantum Nanophotonic and Nanoplasmonic Sensing: Towards Quantum Optical Bioscience Laboratories on Chip. *Nanophotonics* 2021, *10*, 1387–1435.
6. Meda, A.; Losero, E.; Samantaray, N.; Scafirimuto, F.; Pradyumna, S.; Avella, A.; Ruo-Berchera, I.; Genovese, M. Photon-Number Correlation for Quantum Enhanced Imaging and Sensing. *J. Opt. (United Kingdom)* **2017**, *19*, doi:10.1088/2040-8986/aa7b27.
7. Berchera, I.R.; Degiovanni, I.P. Quantum Imaging with Sub-Poissonian Light: Challenges and Perspectives in Optical Metrology. *Metrologia* 2019, *56*.
8. Genovese, M. Real Applications of Quantum Imaging. *J. Opt.* **2016**, *18*, doi:10.1088/2040-8978/18/7/073002.
9. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in Quantum Cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012, doi:10.1364/aop.361502.
10. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 15–18, doi:10.1103/PhysRevLett.94.230504.
11. Dušek, M.; Jahma, M.; Lütkenhaus, N. Unambiguous State Discrimination in Quantum Cryptography with Weak Coherent States. *Phys. Rev. A - At. Mol. Opt. Phys.* **2000**, *62*, 9, doi:10.1103/PhysRevA.62.022306.
12. Ko, H.; Choi, B.S.; Choe, J.S.; Youn, C.J. Advanced Unambiguous State Discrimination Attack and Countermeasure Strategy in a Practical B92 QKD System. *Quantum Inf. Process.* **2018**, *17*, 1–14, doi:10.1007/s11128-017-1784-7.
13. Malik, M.; Magaña-Loaiza, O.S.; Boyd, R.W. Quantum-Secured Imaging. *Appl. Phys. Lett.* **2012**, *101*, 1–10, doi:10.1063/1.4770298.
14. Zhao, Y.B.; Zhang, W.L.; Wang, D.; Song, X.T.; Zhou, L.J.; Ding, C.B. Proof-of-Principle Experimental Demonstration of Quantum Secure Imaging Based on Quantum Key Distribution. *Chinese Phys. B* **2019**, *28*, doi:10.1088/1674-1056/ab3e66.
15. Vernekar, S.; Xavier, J. Secure Quantum Imaging with Decoy State Heralded Single Photons. *arXiv Prepr. arXiv2402.11675.* **2024**, 1–4.
16. Yin, P.; Takeuchi, Y.; Zhang, W.H.; Yin, Z.Q.; Matsuzaki, Y.; Peng, X.X.; Xu, X.Y.; Xu, J.S.; Tang, J.S.; Zhou, Z.Q.; et al. Experimental Demonstration of Secure Quantum Remote Sensing. *Phys. Rev. Appl.* **2020**, *14*, 1, doi:10.1103/PhysRevApplied.14.014065.
17. Heo, J.; Kim, J.; Jeong, T.; Ihn, Y.S.; Kim, D.Y.; Kim, Z.; Jo, Y. Quantum-Secured Single-Pixel Imaging with Enhanced Security. *Optica* **2023**, *10*, 1461, doi:10.1364/optica.494050.
18. Moore, S.W.; Dunningham, J.A. Secure Quantum Remote Sensing without Entanglement. *AVS Quantum Sci.* **2023**, *5*, doi:10.1116/5.0137260.
19. Rahim, M.T.; Khan, A.; Khalid, U.; Rehman, J. ur; Jung, H.; Shin, H. Quantum Secure Metrology for Network Sensing-Based Applications. *Sci. Rep.* **2023**, *13*, 1–7, doi:10.1038/s41598-023-38802-6.
20. He, W.; Huang, C.; Guan, R.; Chen, Y.; Zhang, Z.; Wei, K. Experimental Secure Entanglement-Free Quantum Remote Sensing over 50 Km of Optical Fiber. *Phys. Rev. A* **2025**, *111*, 1–7, doi:10.1103/PhysRevA.111.062607.
21. Moore, S.W.; Dunningham, J.A. Secure Quantum-Enhanced Measurements on a Network of Sensors. *Phys. Rev. A* **2025**, *111*, 1–12, doi:10.1103/PhysRevA.111.012616.
22. Bash, B.A.; Gheorghe, A.H.; Patel, M.; Habif, J.L.; Goeckel, D.; Towsley, D.; Guha, S. Quantum-Secure Covert Communication on Bosonic Channels. *Nat. Commun.* **2015**, *6*, doi:10.1038/ncomms9626.

 doi:10.20944/preprints202507.1064.v1

23. Walter, D.; Pitsch, C.; Paunescu, G.; Lutzmann, P. Quantum Ghost Imaging for Remote Sensing. **2019**, *2023*, 32, doi:10.1117/12.2529268.
24. Gregory, T.; Moreau, P.A.; Mekhail, S.; Wolley, O.; Padgett, M.J. Noise Rejection through an Improved Quantum Illumination Protocol. *Sci. Rep.* **2021**, *11*, doi:10.1038/s41598-021-01122-8.
25. Johnson, S.; Rarity, J.; Padgett, M. Transmission of Quantum-Secured Images. *Sci. Rep.* **2024**, *14*, 1–7, doi:10.1038/s41598-024-62415-2.
26. Sternberg, J.; Voisin, J.; Roux, C.; Chassagneux, Y.; Amanti, M. Secure Communication Based on Sensing of Undetected Photons. *EPJ Web Conf.* **2024**, *309*, doi:10.1051/epjconf/202430908009.
27. Liao, S.K.; Cai, W.Q.; Liu, W.Y.; Zhang, L.; Li, Y.; Ren, J.G.; Yin, J.; Shen, Q.; Cao, Y.; Li, Z.P.; et al. Satellite-to-Ground Quantum Key Distribution. *Nature* **2017**, *549*, 43–47, doi:10.1038/nature23655.
28. Li, Y.; Cai, W.Q.; Ren, J.G.; Wang, C.Z.; Yang, M.; Zhang, L.; Wu, H.Y.; Chang, L.; Wu, J.C.; Jin, B.; et al. Microsatellite-Based Real-Time Quantum Key Distribution. *Nature* **2025**, *640*, 47–54, doi:10.1038/s41586-025-08739-z.
29. Yang, J.Z.; Li, M.F.; Chen, X.X.; Yu, W.K.; Zhang, A.N. Single-Photon Quantum Imaging via Single-Photon Illumination. *Appl. Phys. Lett.* **2020**, *117*, doi:10.1063/5.0021214.
30. Kim, J.; Jeong, T.; Lee, S.Y.; Kim, D.Y.; Kim, D.; Lee, S.; Ihn, Y.S.; Kim, Z.; Jo, Y. Heralded Single-Pixel Imaging with High Loss-Resistance and Noise-Robustness. *Appl. Phys. Lett.* **2021**, *119*, doi:10.1063/5.0078973.
31. Johnson, S.; McMillan, A.; Torre, C.; Frick, S.; Rarity, J.; Padgett, M. Single-Pixel Imaging with Heralded Single Photons. *Opt. Contin.* **2022**, *1*, 826, doi:10.1364/optcon.458248.
32. Shafi, K.M.; Padhye, A.; Chandrashekar, C.M. Quantum Illumination Using Polarization-Path Entangled Single Photons for Low Reflectivity Object Detection in a Noisy Background. *Opt. Express* **2023**, *31*, 32093, doi:10.1364/oe.496776.
33. Ying, J.W.; Zhao, P.; Zhong, W.; Du, M.M.; Li, X.Y.; Shen, S.T.; Zhang, A.L.; Zhou, L.; Sheng, Y.B. Passive Decoy-State Quantum Secure Direct Communication with a Heralded Single-Photon Source. *Phys. Rev. Appl.* **2024**, *22*, 1, doi:10.1103/PhysRevApplied.22.024040.
34. Mahdavifar, M.; Hashemi Rafsanjani, S.M. Violating Bell Inequality Using Weak Coherent States. *Opt. Lett.* **2021**, *46*, 5998, doi:10.1364/ol.441499.
35. Sit, A.; Bouchard, F.; Fickler, R.; Gagnon-Bischoff, J.; Larocque, H.; Heshami, K.; Elser, D.; Peuntinger, C.; Günthner, K.; Heim, B.; et al. High-Dimensional Intracity Quantum Cryptography with Structured Photons. *Optica* **2017**, *4*, 1006, doi:10.1364/optica.4.001006.
36. Iqbal, H.; Krawec, W.O. Analysis of a High-Dimensional Extended B92 Protocol. *Quantum Inf. Process.* **2021**, *20*, 1–22, doi:10.1007/s11128-021-03276-w.
37. Dutta, A.; Muskan; Banerjee, S.; Pathak, A. Analysis for Satellite-Based High-Dimensional Extended B92 and High-Dimensional BB84 Quantum Key Distribution. *Adv. Quantum Technol.* **2024**, *2400149*, 1–21, doi:10.1002/qute.202400149.
38. Cañas, G.; Vera, N.; Cariñe, J.; González, P.; Cardenas, J.; Connolly, P.W.R.; Przysiezna, A.; Gómez, E.S.; Figueroa, M.; Vallone, G.; et al. High-Dimensional Decoy-State Quantum Key Distribution over Multicore Telecommunication Fibers. *Phys. Rev. A* **2017**, *96*, 1–8, doi:10.1103/PhysRevA.96.022317.
39. Otte, E.; Nape, I.; Rosales-Guzmán, C.; Denz, C.; Forbes, A.; Ndagano, B. High-Dimensional Cryptography with Spatial Modes of Light: Tutorial. *J. Opt. Soc. Am. B* **2020**, *37*, A309, doi:10.1364/josab.399290.
40. Nape, I.; Sephton, B.; Ornelas, P.; Moodley, C.; Forbes, A. Quantum Structured Light in High Dimensions. *APL Photonics* **2023**, *8*, doi:10.1063/5.0138224.
41. Nothlawala, F.; Moodley, C.; Gounden, N.; Nape, I.; Forbes, A. Quantum Ghost Imaging by Sparse Spatial Mode Reconstruction. *Adv. Quantum Technol.* **2025**, *8*, 1–10, doi:10.1002/qute.202400577.
42. Wang, S.; Zhang, S.L.; Li, H.W.; Yin, Z.Q.; Zhao, Y.B.; Chen, W.; Han, Z.F.; Guo, G.C. Decoy-State Theory for the Heralded Single-Photon Source with Intensity Fluctuations. *Phys. Rev. A - At. Mol. Opt. Phys.* **2009**, *79*, 1–5, doi:10.1103/PhysRevA.79.062309.
43. Wang, Q.; Chen, W.; Xavier, G.; Swillo, M.; Zhang, T.; Sauge, S.; Tengner, M.; Han, Z.F.; Guo, G.C.; Karlsson, A. Experimental Decoy-State Quantum Key Distribution with a Sub-Poissionian Heralded Single-Photon Source. *Phys. Rev. Lett.* **2008**, *100*, 1–4, doi:10.1103/PhysRevLett.100.090501.

 doi:10.20944/preprints202507.1064.v1

44. Schiavon, M.; Vallone, G.; Ticozzi, F.; Villoresi, P. Heralded Single-Photon Sources for Quantum-Key-Distribution Applications. *Phys. Rev. A* **2016**, *93*, 1–10, doi:10.1103/PhysRevA.93.012331.
45. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.* **2004**, *92*, 4, doi:10.1103/PhysRevLett.92.057901.
46. Acín, A.; Gisin, N.; Scarani, V. Coherent-Pulse Implementations of Quantum Cryptography Protocols Resistant to Photon-Number-Splitting Attacks. *Phys. Rev. A - At. Mol. Opt. Phys.* **2004**, *69*, 16, doi:10.1103/PhysRevA.69.012309.