Spread Photon Transceiver for Quantum Secure Communications

Wesley Webb
Photonics and Quantum Sciences
L3Harris Technologies
Wesley.Webb@L3Harris.com

Michael S. Bullock
Department of Electrical and Computer Engineering
University of Arizona
bullockm@arizona.edu

Samuel H. Knarr
Photonics and Quantum Sciences
L3Harris Technologies
Samuel.Knarr@L3Harris.com

Timothy C. Burt
Photonics and Quantum Sciences
L3Harris Technologies
Timothy.C.Burt@L3Harris.com

Jim A. Drakes
Photonics and Quantum Sciences
L3Harris Technologies
Jim.Drakes@L3Harris.com

Saikat Guha
College of Optics
University of Arizona
saikat@optics.arizona.edu

Boulat A. Bash
Department of Electrical and Computer Engineering
University of Arizona
boulat@arizona.edu

Victor G. Bucklew
Photonics and Quantum Sciences
L3Harris Technologies
Victor.Bucklew@L3Harris.com

***Abstract*—**Quantum communication protocols provide capabilities for private information exchange despite adversarial access to quantum resources. However, existing protocols can be limited by speed, and considerations around their practical implementation. We report on a novel quantum communications protocol, called the spread photon transceiver, which operates on the physical layer of a communications link with a pair of matched receivers, to achieve quantum security. The sensitivity of the matched receiver architecture to experimental error is evaluated. A security analysis of the protocol is conducted, evaluating the private information rate achievable between the intended sender and receiver, assuming a quantum-powerful adversary, with receiver losses reflective of scenarios which may be encountered in a military field environment.

Keywords—Quantum communications, spread photon transceiver, quantum data locking, physical layer security

I. Introduction

Secure communication architectures are vital for modern military operations. With the advent of new types of adversarial threats and increasing mission complexity, more stringent security requirements and higher data rates are increasingly needed.

Quantum mechanics provides novel ways of communicating and securing information based on the laws of physics, rather than computational complexity [1],[2]. However, for most quantum communication protocols, bit rates are often limited to kbit/s or Mbit/s. These rates are throttled by hardware limitations such as fiber loss, and implementation challenges where protocols require large overhead demands to maintain security. Additional barriers often include specialized equipment requirements, which are difficult to integrate into existing communication architectures.

Development of high-speed quantum communication protocols, which can be implemented with available commercial off the shelf (COTS) components, can provide a key capability for the community. Sensitive data encrypted with modern standards [3] (e.g., AES, RSA) is subject to 'download today, decrypt tomorrow' type attacks. In these attacks, data can be stored until quantum computers reach sufficient maturity to break traditional encryption that relies on computational complexity such as RSA.

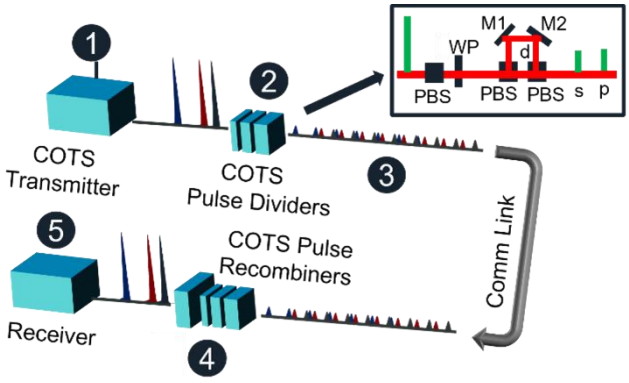

Figure 1: Conceptual diagram of a matched SPT transceiver, for achieving quantum secure communications.

In this paper, we report on practical implementation considerations for the spread photon transceiver (SPT), a novel protocol for quantum-secure communications that can be utilized on top of existing classical encryption methods such as RSA. Our protocol operates on the physical layer, using cascaded unbalanced Mach-Zehnder interferometers (UMZIs) to add a layer of quantum security to a data stream.

Throughout the rest of this article, we describe our protocol and its security in detail. Section II describes a practical method for implementing the SPT protocol with two series of stages, comprising a matched transmitter and receiver pair. Section III details experimental results of a free-space implementation of the technique with bright laser light, and evaluates the impact of waveplate misalignment between the sender and receiver. Section IV analyzes the quantum-secure communication capabilities of the spread photon architecture where a passive eavesdropper Eve has access to unlimited quantum computing, memory, and measurement resources. We calculate secure bit rates for practical link scenarios, including various channel loss regimes for both the intended receiver and adversary. We conclude in Section V by discussing future directions of study needed for practically implementing the SPT protocol for quantum-secure communications.

II. SPREAD PHOTON TRANSCEIVER

The SPT protocol operates on the physical layer of a communications link by providing quantum security using a SPT transmitter to divide and spread data in the temporal domain, and an SPT matched receiver to recover the data. The SPT transmitter converts a sequence of bright bits to a temporally longer sequence of lower-photon number overlapping bits, in a loose analogue to a direct-sequence spread spectrum approach [4]. In this section, we describe a physical implementation of the SPT protocol and how it secures information.

We employ free-space optical components, as described below and shown in Figure 1. In step 1 of Figure 1, the data stream is modulated onto the continuous wave laser light. In step 2, the laser beam enters a cascade of n photon spreading stages. The subfigure inset in step 2 shows one of these stages in detail. The laser beam enters the stage and has its polarization arbitrarily rotated by a waveplate. The UMZI following the waveplate uses polarizing beamsplitters (PBSs) to split and recombine the polarization components of the beam with a relative delay determined by the length d. The waveplate (WP) before the UMZI is used to control the splitting ratio and phase between the delayed polarization components. The distance d between the two arms of each UMZI is set so that the time delay between the two polarization components is greater than or equal to the inverse of the bit rate of the data stream. This provides an additional scrambling of the wavefunction, as each bit in the bit stream is spread over multiple time bins and overlapped with neighboring modulated symbols which have been similarly spread into multiple time bins. The power of each input laser pulse is attenuated by temporal spreading while the energy is conserved. The signal propagates through multiple stages where the delay distances in each stage are progressively doubled. This ensures that temporal scrambling affects as many unique modulation time bins as possible.

In step 3, we illustrate the result of the transmitted signal passing through the scrambling stages. The resulting waveform is attenuated to a low-photon-number coherent state and subsequently passed by the transmitter, Alice, through a public link. The link can be free-space or fiber-based, and represents the channel where an adversary, Eve, could gain access to the transmission. We assume that Eve has access to quantum memory, computing, and measurement resources, as well as a copy of the SPT receiver system, but does not know the settings of the waveplates at the beginning of each state. This ensures quantum security for the sender and receiver discussed further in Section IV. In step 4, the receiver, Bob, uses the transmitter's waveplate settings, assumed to have been secretly shared between Alice and Bob before the transmission, to implement a conjugate cascade of equivalent stages, and unscramble the original modulation pulses. In step 5, we measure the optical signal and decode the information stream.

III. PRACTICAL IMPLEMENTATION CONSIDERATIONS

In this section, we report on practical considerations around experimentally implementing the SPT architecture. Specifically, we describe experiments with a four-stage SPT, designed to assess the sensitivity of the SPT architecture to experimental errors in the sender and receiver's implementation of their matched receivers. For the experiment, we assumed that the sender and receiver had identical delays in each stage of their respective transmitter and receiver. This assumption is valid if the matched receiver set is calibrated and optimized publicly and recurringly. We use a 4.25 Gbps on-off keying (OOK) data signal as our input. The relative delays between two arms in each of the four stages were chosen to be 7 cm, 14 cm, 28 cm, and 56 cm, respectively, to ensure that each successive stage spreads the bit into unique time bins, with no overlap between the spread bit copies. We varied the waveplate setting difference between the intended sender and receiver in the experiment, representing an error in implementation. It is assumed that the sender and receiver both have access to the desired settings for each waveplate, possibly through a

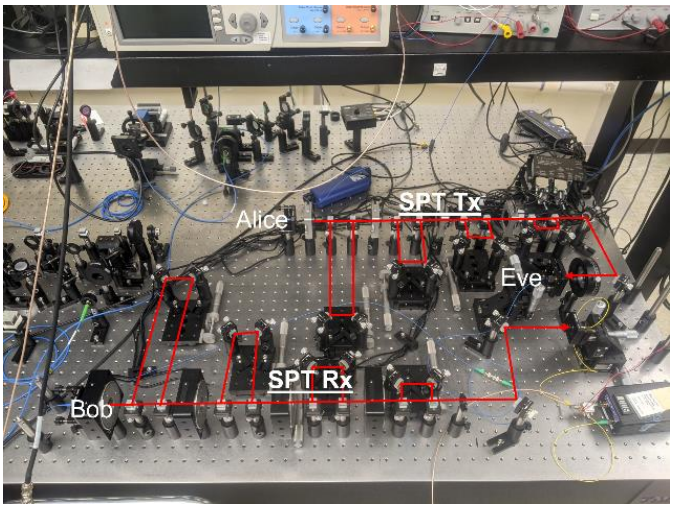

Figure 2: Picture of the experimental layout of the 4-stage free-space-optical breadboard of the matched SPT transceiver.

preshared key, but that setting each waveplate in the transmitter and receiver to matched values, is prone to error.

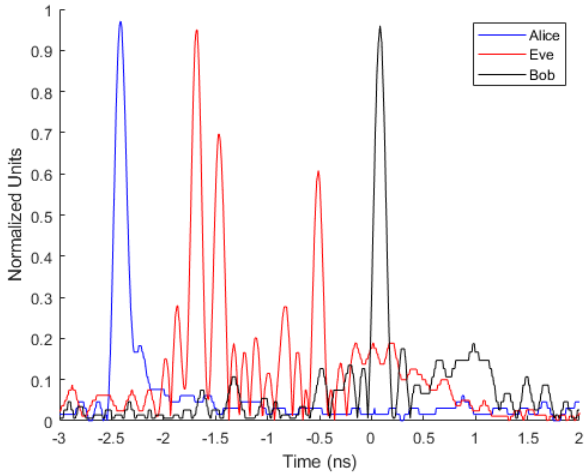

Figure 3: The impulse response of a 235 ps temporal pulse (corresponding to the time bin width of a 4.25 Gbps data rate), passed through the SPT transceiver is experimentally measured at Alice, Eve, and Bob. The impulse is well recovered and temporally localized, at Alice, and Bob, but is temporally spread, and not localized, at Eve.

Figure 2 shows a picture of the experimental layout. We use an arbitrary waveform generator (AWG) to modulate the OOK data stream onto a 1550 nm laser. This input is then launched into the free-space-optical series of cascaded stages. After coupling into fiber, the scrambled waveform can be measured at the midpoint of the link, emulating Eve. Finally, the waveform is collected and passed through a matched receiver, shown in Figure 2, with equivalent stage lengths but with errors in implementation in the waveplate settings between the sender and receiver. An example of an impulse response of a 235 ps wide pulse (corresponding to the time bin width of a 4.25 Gbps data rate), measured experimentally at the sender, midpoint of the link, and receiver, is shown in Figure 3. Here, the sender and receiver have perfectly matched their waveplate settings. As expected, their measured waveforms are localized in time and matched. However, the waveform measured mid-link, before passing through a matched receiver, does not match the waveform of the sender, and does not reflect the data impulse initially input into the SPT module.

Figure 4 shows the measured response at different link locations for a short bit stream. Using simple thresholding on normalized units (NU), with value above .5 NU decoded as 1, and below .5 NU as 0, Bob recovers Alice's waveform, while Eve observes a waveform which is substantially different from the sender and receiver. Additional stages serve to broaden the temporal spreading and scrambling of Eve's waveform.

Based on confirmation that the SPT module was behaving as expected, we then conducted experiments with the waveplate settings of the sender and receiver offset from each other. Figure 5 shows preliminary results of these experiments. Each point on the $x-axis$ represents an average over multiple measurements of different half-waveplate permutations of matched stages of the SPT transceiver in Figure 2. Misalignments in the waveplate setting in each matched stage between Alice and Bob are added together to arrive at the $x-axis$ value for total misalignment in degrees, as a figure of merit for the SPT transceiver's sensitivity to misalignment. Measurements of different permutations of waveplate settings for each total misalignment value are not consistent in number, or representative of the full set, so error bars are not displayed

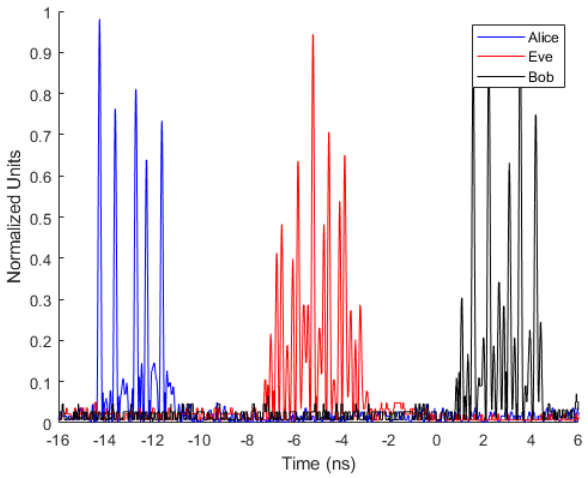

Figure 4: An OOK bit series of '101001101' is experimentally measured at Alice, Eve, and Bob. The waveform is accurately measured by Alice and Bob, who have a set of matched SPT transceivers, but is not recovered by Eve, who does not have a matched SPT transceiver.

in this preliminary data.

As the total magnitude of error in the waveplate settings between the sender and receiver is increased, the error in reconstructing the original bit stream with the matched receiver dramatically increases. This experiment gives insight into the matched receiver's sensitivity to error. Although these experiments employ bright laser light, and direct detection, we expect that the results will translate to the low-photon-number coherent state realm. Based on the preliminary experimental results, when the sender and receiver have waveplate setting errors adding up to ≥10 degrees, Bob's bit error ratio (BER) increases to a level unusable for many communications applications. Additional experiments with greater resolution of the waveplate misalignment between Alice and Bob are needed to determine the exact limits of tolerable misalignment based on BER calculations of demodulated bit streams. That said, to ensure that the sender and receiver can practically implement the SPT protocol, a careful pre-calibration of their waveplate settings would be required. Tolerances of one degree or less in alignment are possible with closed loop electronically controlled waveplates and proper calibration technique.

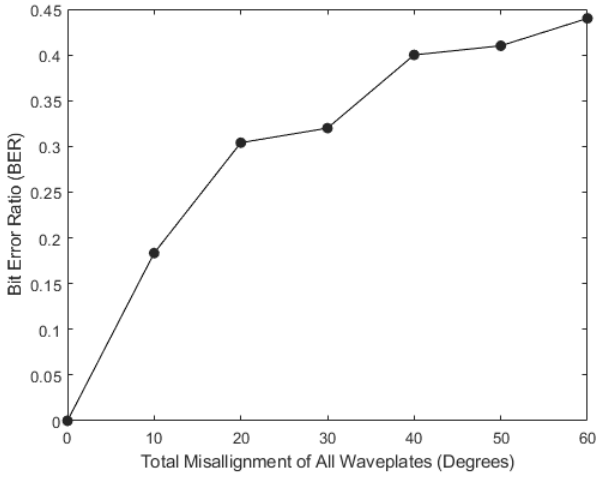

Figure 5: Experimental bit error ratio (BER) versus total misalignment of waveplates in degrees from all stages. As can be seen, as the sender and receiver's waveplate settings are progressively misaligned from each other, their BER increases.

IV. SECURITY ANALYSIS

In this section, we numerically analyze the quantum security of the SPT protocol with practical link scenarios against a quantum powerful adversary. Here, we assume a passive eavesdropper Eve has access to unlimited quantum computing, memory, and measurement resources.

For our analysis, we use the wiretap lossy bosonic channel model with quantum powerful Eve. We seek to characterize the advantage in information throughput that Bob has over Eve when he knows the key and collaborates with Alice on the transmission scheme. Therefore, to quantify this advantage and characterize secure transmission rate, we use the private information defined as [Defn. 13.6.1, 5]

$$P(\mathcal{N}) \coloneqq \max_{\phi_{XA}} [\chi(\{p_X(x), \hat{\sigma}_B^x\}) - \chi(\{p_X(x), \hat{\rho}_E^x\})], \quad (1)$$

where $\mathcal{N}$ is the quantum channel used, X is the random variable with distribution $p_X(x)$ corresponding to the classical information to transmit, $\hat{\sigma}_B^x$ and $\hat{\rho}_E^x$ denote the conditional quantum states at Bob and Eve, respectively, and the maximization is taken over all possible input classical-quantum states $\hat{\phi}_{XA}$. Furthermore, $\chi(\cdot)$ denotes the Holevo information [Sec. 11.6.1, 5] of a classical-quantum ensemble. We are interested in the quantum channel $\mathcal{N}_{T,\boldsymbol{\eta}}$ induced by our transmission scheme T and the transmittances $\boldsymbol{\eta} = (\eta_B, \eta_E)$ to Bob and Eve in the physical link. Here, Bob's key-aided measurement gives rise to a classical random variable Y. Thus, (1) reduces to

$$P\left(\mathcal{N}_{T,\boldsymbol{\eta}}\right) = \max_{p_X(x),N} [I(X;Y) - \chi(\{p_X(x), \hat{\rho}_E^x(N, \eta_E)\})], \quad (2)$$

where N is the mean photon number of the input state prescribed by T, and $I(X;Y)$ is the classical mutual information of random variables X and Y. Since we have constrained input state $\hat{\rho}_{XA}$, maximization only takes place over Alice's tunable parameters: the input power N and input distribution $p_X(x)$. We note that the above analysis makes no constraints on Eve's detection strategy.

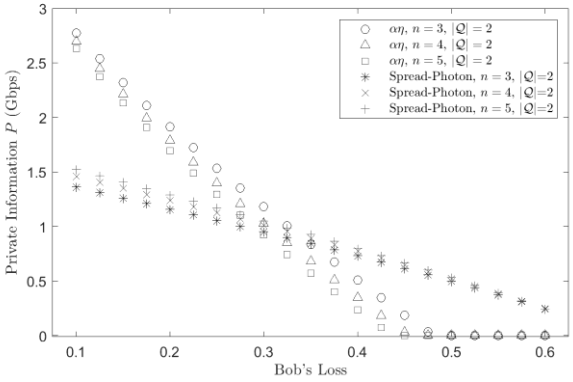

Figure 6: Numerically simulated private information rate between Alice and Bob, with varying levels of loss in Bob's receiver, and a quantum-powerful Eve who retains 60% of the transmitted photons not obtained by Bob. As Bob's loss increases, the private information rate decreases, based on the type of protocol utilized, and how it is implemented. The spread photon protocol offers an advantage for Gbps speed, quantum secure communications, for scenarios where Bob may incur large losses, such as in a non-ideal military field-use scenario.

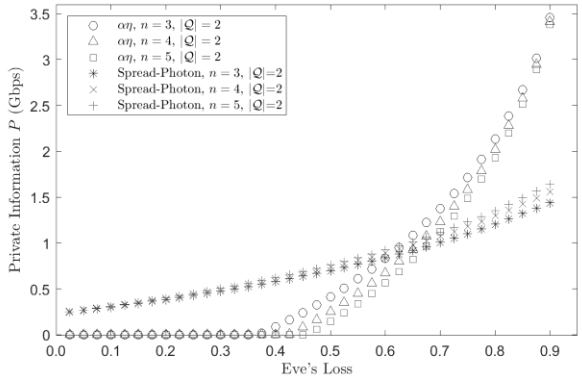

Figure 7: Numerically simulated private information rate between Alice and Bob, with varying levels of loss relative to Bob in a quantum powerful Eve's receiver. Here, we assume Bob loses half his photons to the environment. As Eve's loss increases, the private information rate increases, based on the type of protocol utilized, and how it is implemented.

Figure 6 shows the private information (2) of the spread photon architecture with two stages for differing loss parameters and codeword lengths n at Bob. Here, we assume that Eve obtains 60% of the photons not received by Bob. In the cases of free-space optical and fiber links, practical limitations all but ensure that an eavesdropper can only collect a fraction of the light lost

to the environment. Figure 7 shows the private information for differing loss parameters at Eve, where Bob loses half the photons to the environment. In both figures, we show comparisons to $\alpha\eta$ protocol [6], a laser-light protocol that addresses the same secure communication scenario. For the $\alpha\eta$ protocol, we assume BPSK modulation and homodyne detection. For the spread photon architecture, we allow Alice to modulate phase-randomized on-off keyed symbols on only one of the polarization modes so the other mode may be used for error correction, while in the $\alpha\eta$ protocol, we allow both polarization modes to be used for transmission. In both cases, we modulate symbols at 4.25 GHz and keep the key consumption rate at 1 bit per codeword by constraining $|\mathcal{Q}| = 2$, where $\mathcal{Q}$ is the waveplate angle set (resp. phase transformation set) for the spread-photon (resp. $\alpha\eta$) protocol. ,. In practice, one may instead use classical key expansion to artificially increase this consumption rate and bolster private information through increased number of stages, though the results on misalignment in Section III suggest an upper limit to the number of stages that can be practically implemented. We omit key expansion for reasons of mathematical tractability and delegate analysis on practical limits of the number of stages to future work.

We remark that, under the assumptions given for Figure 6 ,the spread-photon architecture outperforms $\alpha\eta$ when Alice and Bob use a channel with loss above approximately 0.3 or 1.55 dB. Conversely, under the assumptions for Figure 7, the spread-photon architecture outperforms $\alpha\eta$ when Eve's loss relative to Bob is less than approximately 0.6 or 3.98 dB.

V. Conclusion

In this paper, we have focused on practically implementing the SPT architecture for quantum secure communications. Specifically, we discussed the role of mismatch between sender and receiver's waveplate settings on the overall BER with bright laser light and an OOK data series. A security analysis of the SPT architecture, considering practical link losses for the intended receiver and the adversary, as well as losses at the receiver and adversary's respective receivers, was also conducted. It was shown that the SPT architecture can provide quantum secure communications in scenarios where high rates of private information are needed, and the intended recipient may have a lossy matched receiver, as possible in some degraded military communication applications. Additionally, the SPT architecture was shown to provide quantum level security in scenarios where an adversary may have a low loss receiver, which would be consistent with expectations of an intelligent, well-designed adversarial attack.

Future work on the SPT protocol includes security analysis for large-stage-number SPT architectures. The security analysis becomes computationally burdensome as the number of stages and photon number increases, but we expect the security of the protocol to increase with the number of stages. This analysis, along with experiments implementing the SPT matched receivers on smaller platforms, at high data rates, such as photonic integrated circuits, would provide additional insight into optimizing the SPT matched receivers. A trade-off between stage number, security, size, weight, and power (SWaP), and complexity of physical implementation could then be evaluated. Techniques such as chirped pulse sum frequency generation with diffraction gratings could be implemented on an array of single photon detectors, to effectively increase the data rate and fully realize the high-speed potential of the SPT protocol.

Finally, employing the SPT quantum-secure communication protocol with attenuated low-photon-number laser light to obtain experimental metrics for quantum security performance will be the ultimate test of the practical usefulness of the proposed secure communication protocol.

In addition to quantum-secure private communication, the spread-photon architecture may be useful for covert or low probability of detection/intercept (LPD/LPI) communication [7]-[9] due to its ability to spread the power of a given information carrying signal over a wide range of time. This may effectively hide the signal from adversaries who are only sensitive to high peak power in the channel that they observe. For a similar reason, it may be useful for active covert or LPD/LPI sensing [10]-[12], where smaller intensity radiation over a larger time window may appear innocent to an adversary while a large peak intensity pulse will not.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys., vol. 81, pp. 1301–1350, Sep. 2009.

[2] S. Pirandola et al., "Advances in quantum cryptography", Adv. Opt. Photon., vol. 12, no. 4, pp. 1012–1236, Dec. 2020.

[3] J. Talbot and D. Welsh, Complexity and Cryptography: An Introduction. Cambridge, UK: Cambridge University Press, 2006.

[4] Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, Barry K. Levitt, "Spread-Spectrum Communications Handbook," McGraw-Hill, 1994

[5] M. Wilde, Quantum Information Theory, 2nd ed. Cambridge University Press, 2016, arXiv:1106.1445v7.

[6] H. P. Yuen, "KCQ: A New Approach to Quantum Cryptography I. General Principles and Key Generation," 2004. arXiv:quant-ph/0311061.

[7] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," Nat. Commun., vol. 6, Oct. 2015.

[8] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," IEEE J. Select. Areas Commun., vol. 38, no. 3, pp. 471–482, Mar. 2020.

[9] C. N. Gagatsos, M. S. Bullock and B. A. Bash, "Covert Capacity of Bosonic Channels," in IEEE Journal on Selected Areas in Information Theory, vol. 1, no. 2, pp. 555-567, Aug. 2020.

[10] B. A. Bash, C. N. Gagatsos, A. Datta, and S. Guha, "Fundamental limits of quantum-secure covert optical sensing", in 2017 IEEE International Symposium on Information Theory (ISIT), 2017, pp. 3210–3214.

[11] C. N. Gagatsos, B. A. Bash, A. Datta, Z. Zhang, and S. Guha, "Covert sensing using floodlight illumination", Phys. Rev. A, vol. 99, p. 062321, Jun. 2019.

[12] S. Hao et al., "Demonstration of Entanglement-Enhanced Covert Sensing", *Phys. Rev. Lett.*, vol. 129, p. 010501, Jun. 2022.