EPJ Web of Conferences **309**, 08009 (2024) https://doi.org/10.1051/epjconf/202430908009
EOSAM 2024

Secure communication based on sensing of undetected photons

Jean Sternberg[1,*], *Julien* Voisin[1], *Charline* Roux[1], *Yannick* Chassagneux[2], and *Maria* Amanti[1,**]

[1]Laboratoire Matériaux et Phénomènes Quantiques (MPQ), Université Paris Cité, CNRS-UMR 7162, Paris 75013, France
[2]Laboratoire de Physique de l'ENS, Université PSL, CNRS, Sorbonne Université, Université Paris Cité, Paris, France

Abstract. In this paper, we introduce a secure optical communication protocol that harnesses quantum correlation within entangled photon pairs. A message written by acting on one of the photons can be read by measuring exclusively the other photon of the pair. In this scheme, a bright, meaningless optical beam hides the message, rendering it inaccessible to potential eavesdroppers. Unlike traditional methods, our approach only affects unauthorized users, fundamentally limiting their access to the communication channel. We demonstrate the effectiveness of our protocol by achieving secure communication through both amplitude and phase modulation, relying on single-photon measurements, as opposed to most approaches which rely on coincidence measurements. We successfully demonstrate the resilience of the data transfer to noise up to 10^5 times greater than the signal, and we employ this technique for the secure transfer of an image.

1 Introduction

In today's data-driven era, efficient data transmission is crucial, and photons are emerging as efficient carriers due to their speed and low susceptibility to interlink interference. Quantum physics provides robust frameworks for secure communication, employing principles such as the quantum no-cloning theorem to safeguard data integrity. Despite the advancements in Quantum Key Distribution (QKD) [1], current security protocols are constrained by reliance on mathematical models of quantum devices. In this paper, we present an innovative approach to secure optical communication, harnessing quantum correlation within entangled photon pairs [2]. Our method involves embedding a message within a bright, meaningless optical beam, rendering interception and decryption by unauthorized parties exceedingly challenging.

Traditional interception methods encounter statistical limitations. By concealing the message within the shot noise of a powerful laser beam, accessibility to unauthorized parties is severely impeded. However, ensuring accessibility to the intended recipient poses a challenge.

Here, we exploit quantum correlation within entangled photon pairs to address this challenge. While one photon serves for transmission, the other remains at the receiver's location, immune to external attacks. The transmission photon carries the concealed message, obscured by the intense beam, while the receiver photon facilitates message retrieval through quantum correlations.

This concealment technique, leveraging quantum correlation, has proven effective in mitigating background noise in coincidence measurements within quantum illumination schemes. Unlike approaches reliant on coincidence measurements, where noise directly impacts data detection (see [3]), our protocol ensures noise only affects the undetected photon, thereby preserving message integrity. Furthermore, our method obviates the need for post-treatment such as reconciliation or error correction required by QKD protocols.

In summary, our proposed method presents a novel approach to secure optical communication, leveraging quantum correlation within entangled photon pairs to ensure data confidentiality and integrity.

2 Experimental setup

To implement our secure communication scheme we implement a quantum interferometer setup commonly used for sensing of undetected photons [4, 5]. A 532 nm continuous wave laser acts as a pump for a second order non linear process in a PPLN crystal with a periodicity suitable for the spontaneous generation of idler/signal pairs at 1550nm/810nm. A first dichroic mirror separates the pump from the photon pairs and a second one splits the signal and the idler along two different paths. An object, that we model by a beam-splitter of reflectivity α and dephasing $\Delta\phi$, can be inserted into the signal path. Planar mirrors, positioned on precision translation stages, direct the three optical modes back to the crystal in the same spatial mode as the outgoing ones. After the second pass in the crystal, dichroic mirrors again separate the three modes, and the idler and signal modes are detected by fiber-coupled superconducting single-photon detectors. Perfect mode overlap during both passes in the crystal creates indistinguishability, leading to quantum interference. Hence the detection rate at the idler detector:

$$R_A = 2\eta_{det} N_{Quantum}[1 + \sqrt{1-\alpha^2} cos(\phi - \phi_i - \phi_s)], \quad (1)$$

*e-mail: jean.sternberg@u-paris.fr
**e-mail: maria.amanti@paris7.jussieu.fr

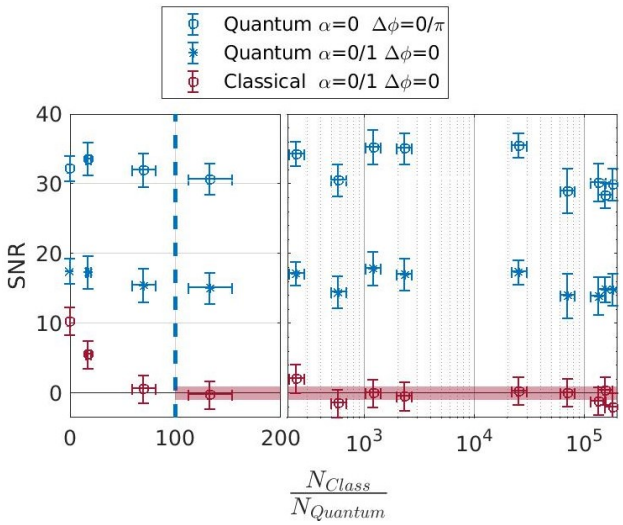

Figure 1. Signal-to-noise ratio of the communication protocol. Experimental data correspond to measurements on the same photon used to write the message, the signal, (Classical-Eve) and on the other photon of the pair, the idler (Quantum-Alice). Data are reported as function of $\frac{N_{Class}}{N_{Quantum}}$. Data correspond to amplitude based communication ($\alpha = 0/1$) and phase based ($\Delta\phi = 0/\pi$).

where α^2 is the probability of deviation of the signal mode at the beam-splitter, η_{det} is the detection efficiency, $N_{Quantum}$ is the number of pairs generated per second, per pass in the crystal, ϕ, ϕ_i and ϕ_s are the propagation phases along the pump, idler and signal path respectively.

In our secure communication scheme Alice, the message receiver, possesses the pump laser, the crystal, the pump and idler paths as well as the detectors. Bob, the message sender, is at the extremity of the signal path. Bob can manipulate the signal via the reflectivity of the object α, altering the visibility of the interference, and via the phase ϕ_i by translating the planar mirror or by acting on $\Delta\phi$. Additionally, Bob overlaps the returning signal beam with a continuous wave laser emitting at 810 nm, effectively concealing the message within the shot noise of the laser during its propagation back to Alice's location.

3 Results

3.1 Signal-to-noise ratio

In Figure 1, we present the experimental dependence of the signal-to-noise ratio (SNR) of the communication protocol as a function of $\frac{N_{Class}}{N_{Quantum}}$, where $N_{Quantum}$ is the number of pairs generated per second, and N_{Class} is the number of photons per second of the jamming source in the same mode as the quantum photons. Experimental points labeled as classical correspond to counts measured on the signal detector (Eve), and points labeled as quantum correspond to measurements on the idler detector (Alice). The threshold on the value of N_{Class} needed for secure communication is represented by the dashed line, and the shaded area corresponds to $-1 \leq SNR \leq 1$.

We demonstrate high SNR and the viability of this communication scheme. We observe that the signal photons, i.e., the ones that can be intercepted by an eavesdropper (Eve), carry no information for $\frac{N_{Class}}{N_{Quantum}} \gtrsim 100$, and that the idler photons are not affected by the jamming laser, as the SNR remains constant with respect to $\frac{N_{Class}}{N_{Quantum}}$ for measured values exceeding 10^5. This confirms that our protocol ensures data confidentiality and integrity.

3.2 Secure image transfer

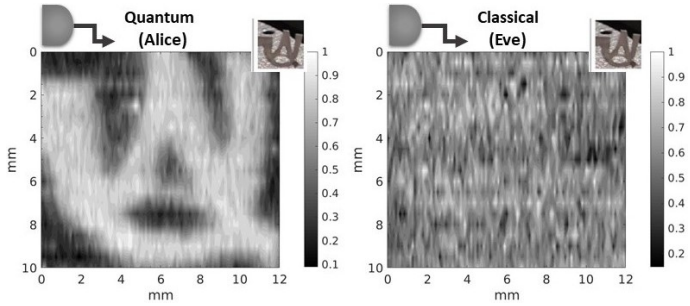

Figure 2. Experimental demonstration of the transmission of the image of the logo of the University Paris Cité. Data are compared for detection at Alice's (left panel) and Eve's place (left panel) in the presence of the jamming laser ($\frac{N_{Class}}{N_{Quantum}} \sim 10^5$).

We demonstrate amplitude-based secure communication of an image. The results are presented in Figure 2. The object of interest is an opaque foil shaped to resemble the logo of Université Paris Cité (See the inset). The transfer of the image is performed by placing Bob's translation stage in a position of maximally destructive interference and horizontally scanning the logo through the signal beam every 0.5 mm on the vertical axis.

This shape can be clearly recognized by Alice, while Eve is completely blinded by the jamming laser. To estimate the security of the image transfer, we calculated the correlations between measurements at the eavesdropper's location and Alice's. We found a value of 0.038, comparable to that which would be obtained for a random distribution of intensity between 0 and 1.

In summary, we have demonstrated successful communication based on undetected photon sensing with amplitude and phase encoding, achieving high SNR and securely transferring a full image. The jamming source serves as a securing tool, which can be exploited to provide a reference for interferometric measurements between the two parties. Moreover, the presented scheme can be easily adapted to fiber-based communication systems.

References

[1] Y.A. Chen et al., Nature **589**, 214 (2021)
[2] J. Sternberg, J. Voisin, C. Roux, Y. Chassagneux, M.I. Amanti, arXiv.2403.15557 (2024)
[3] Johnson et al., Optics Express **31**, 5290 (2023)
[4] X.Y. Zou, L.J. Wang, L. Mandel, PRL **67**, 318 (1991)
[5] M. Gilaberte Basset et al., Laser & Photonics Reviews **15**, 2000327 (2021)