Quantum-Enhanced Physical Layer Cryptography: A new paradigm for free-space key distribution

Matthieu LEGRE and Bruno HUTTNER

ID Quantique SA

ABSTRACT

In order to extend the range of QKD and provide a world-wide key distribution network, free-space key distribution, based on satellite-to-ground optical communication, is required. The QuSat project, led by ID Quantique, aims at developing a simple and cost-effective way to implement an industrial solution for global key distribution through satellites. This solution will be based on a new concept for secure free-space quantum communications called quantum-enhanced physical layer cryptography.

EXTENDED ABSTRACT

Current ground-based QKD has a limited point-to-point range, of the order of hundreds of kilometers. This restriction can only be partly lifted through the use of trusted nodes, which can extend the range to thousands of kilometers, but requires an extended and costly infrastructure. The use of satellites implementing QKD can provide a world-wide key distribution network. However, the complexity of QKD protocols leads to a high cost solution. The QuSat project aims at delivering such a network at a lower cost, and therefore provides a practical solution for global key distribution. This project relies on a new quantum communication protocol, based on optical communications, which guarantees the security of the exchange of secret keys in the context of the Wyner wiretap channel scenario [1].

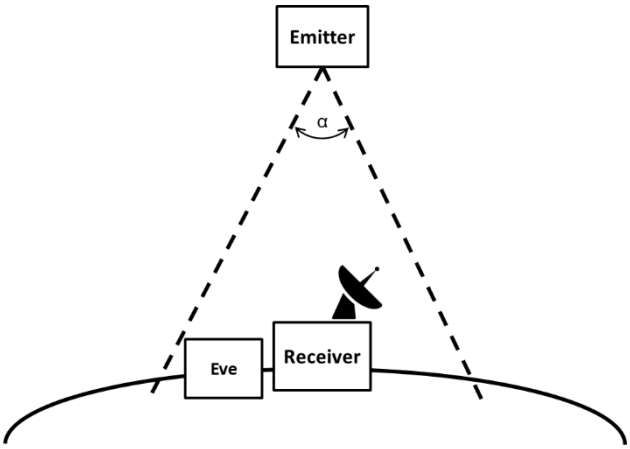

Figure 1: Illustration of a Wyner wiretap channel scenario
The Emitter and Receiver are linked with optical telescopes. Due to diffraction, the beam sent from the Emitter covers an area broader than the receiver (angle α is greatly amplified here for demonstration purposes). Part of the beam can be received by Eve. The legitimate users use a radar to detect any direct interception attempt.

Figure 1 is an illustration of Wyner wiretap channel scenario. In this scenario, the eavesdropper Eve is limited to the ability of extracting a fraction of the optical signal transmitted from the emitter to the receiver. However, Eve cannot intercept/resend any optical signal to the receiver. Wyner wiretap channel is a realistic scenario in the case of free-space communications, for example between a satellite and a ground station. Since the

satellite and the ground station are in a line-of-sight, interception can easily be discovered. For example, radars have been developed and used in order to detect the intrusion of an eavesdropper in an area covering the optical channel between an emitter and a receiver.

Wyner physical layer wiretap channel is part of a research stream which is dedicated to Physical Layer Security. Physical layer security has recently become an emerging technique to complement and significantly improve the communication security of wireless networks. Compared to algorithmic cryptographic approaches, physical layer security is a fundamentally different paradigm where secrecy is achieved by exploiting the physical layer properties of the communication system, such as thermal noise, interference, and the time-varying nature of fading channels. In the physical layer wiretap channel model represented in Figure 1, the goal of the legitimate users, i.e. the emitter and the receiver, is to communicate over a main channel, while ensuring that an eavesdropper Eve is unable to obtain any information about the exchanged information from the outputs of the wiretapped channel, or at least cannot extract signal enabling to get access to the information. The fundamental theoretical framework underlying this case was laid by Csiszár and Körner [2]. The main assumption is that if the channel from the emitter to the eavesdropper is a noisier version of the channel sent from the emitter to the legitimate receiver, a non-zero secrecy rate may be achieved by sacrificing a fraction of the message rate. More recently, the Wyner physical layer wiretap channel was revisited by Maurer and Wolf [3], who showed that, even if the eavesdropping channel is not a degraded version, i.e. if Eve has less noise than the emitter and the receiver, a non-zero secrecy rate could still be achieved, with only assumptions on noise independence between Eve and Receiver. In order to derive secret information, Emitter and Receiver have to know the noise on the eavesdropping channel. However, this technique requires assumptions on Eve's noise level and signal extraction capacity. The noise on Eve's detector has to be lower bounded, and the bound has to be known. This is quite problematic because, one can never be sure of what quality of detectors Eve is provided with. The aim of our quantum communication protocol is introduce a modified Wyner wiretap channel, transmitting quantum objects, and to prove the security of a secret key exchange through a Wyner physical layer wiretap channel under the single assumption that Eve is limited by the laws of Quantum Physics.

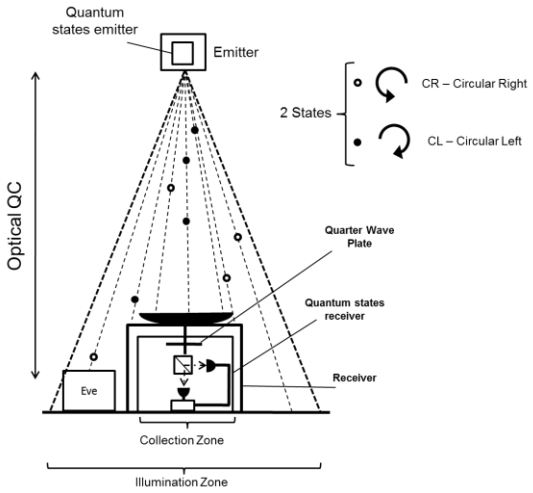

Figure 2: Illustration of one implementation of quantum-enhanced physical layer cryptography The Emitter sends single photons, with polarisation encoding. Any photon received by Eve is not received by the Receiver and will not be used in the final key.

Our quantum-enhanced physical cryptography protocol is based on the fact that a single photon is either collected by the receiver or by Eve, but cannot be measured by both under the assumption of Wyner wiretap channel. Figure 2 shows one possible

implementation of our protocol. The emitter, in the satellite, randomly chooses to emit one of two orthogonal polarization states. These polarization states are carried by single photons. The receiver is in the illumination zone on the ground and can collect a portion of those single photons, and measure their polarization state with a polarization beamsplitter. If the emitter and the receiver agree on a bit value associated to each polarization states, they can exchange sequences of bits. If Eve is within the illumination zone, she can collect some of the single photons. However, one photon collected and measured by Eve cannot be collected by the receiver. The corresponding exchange will therefore be discarded. This guarantees the security of the bit sequences exchanged between the emitter and the receiver under the assumption of Wyner wiretap channel. Note that quantum-enhanced physical layer cryptography is limited to secret random key exchange, because most of the single photons will not be detected by the receiver. This is a main difference and limitation compared to conventional physical layer cryptography which guarantees the security of the data transfer under strong assumptions on the noise of Eve's detection system.

As single-photon states are not easy to generate, we now turn to a second, more practical example. The same quantum communication protocol can be implemented with weak coherent pulses, which contain less than one photon on average. In this case, the security of the key exchange relies on the independence of the detection probabilities at the receiver and at Eve. Based on this independence, the maximum amount of information obtained by an eavesdropper is linked to the mean number of photon, which may be received by Eve. Therefore, the receiver and the emitter can bound the information, which may have leaked to Eve, and extract a secret key following a distillation process similar to the processes used in physical layer security and QKD protocols.

CONCLUSIONS

In order to facilitate and reduce the cost of implementations of secure key exchanges between a satellite and a ground station base, we propose a new quantum communication protocol, called quantum-enhanced physical layer cryptography. This protocol guarantees the security of the key exchange under the assumptions of the Wyner wiretap channel, namely that the eavesdropper cannot intercept the beam between the emitter and the receiver, and of having the eavesdropper limited by the laws of Quantum Physics.

REFERENCES:

[1]: A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J. 54(8), 1355–1387 (1975).

[2]: I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory 24(3), 339–348 (1978).

[3]: U. Maurer and S. Wolf "Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free". In: Preneel B. (eds) Advances in Cryptology — EUROCRYPT 2000. EUROCRYPT 2000. Lecture Notes in Computer Science, vol 1807. Springer, Berlin, Heidelberg; https://link.springer.com/chapter/10.1007%2F3-540-45539-6_24