Quantum Private Telecommunications

A project at Instituto de Telecomunicações, Portugal

Yasser Omar
SQIG, Instituto de Telecomunicações
and CEMAPRE, ISEG, Technical University of Lisbon
Lisbon, Portugal
yasser.omar@lx.it.pt

***Abstract*—*QuantPrivTel – Quantum Private Telecommunications* is an ongoing research project that joins the theoretical expertise of the Security and Quantum Information Group (SQIG) at Instituto de Telecomunicações (IT) in Lisbon, Portugal, and the skills in quantum optics experiments of the Optical Communications group (OC-Av) at IT Aveiro, Portugal, to tackle new challenges in the emergent and multidisciplinary area of quantum private telecommunications. After a brief introduction to quantum information and quantum telecommunication, we will present the main results achieved by the project team so far, namely a quantum-enhanced message authentication protocol and a quantum contract signing protocol, as well as the implementation of quantum channels with optical fibers.**

Keywords-quantum telecommunications; quantum cryptography; quantum information; single-photon qubits.

I. INTRODUCTION

Quantum Information Theory is a new area of Information Science that explores the strange properties of Quantum Mechanics to encode, transmit, store and process information. Over the last decade, we understood how to take advantage of these properties for revolutionary applications, such as teleportation of quantum states, communications protected against eavesdropping in a completely secure way or computers astonishingly faster than the current ones (but for the time being limited to a small number of qubits!). This rapid progress in the field happened both at the theoretical and at the experimental level [1,2].

In particular, quantum cryptography, or more precisely, quantum key distribution, evolved in a few years from fundamental physics to a commercial application [3]. With this progress, came the development of photonic quantum telecommunications, both in cable and open-air, albeit currently still limited to a few hundred kilometers given the impossibility to have perfect quantum repeaters. A strong effort is being made to push the record distance and have global quantum telecommunications [4]. Yet, all the effort is focused on quantum key distribution, whereas there are other information security issues where quantum bits can offer enhanced privacy.

QuantPrivTel – Quantum Private Telecommunications is a research project that joins the theoretical expertise of the Security and Quantum Information Group (SQIG) at Instituto de Telecomunicações (IT) in Lisbon, Portugal, and the skills in quantum optics experiments of the Optical Communications group (OC-Av) at IT Aveiro, Portugal, to tackle new challenges in the emergent and multidisciplinary area of quantum private telecommunications. Its main scientific objectives are:

1. To propose new quantum protocols for important problems of privacy in telecommunications that cannot be solved with the now-famous quantum key distribution, namely the authentication of classical messages with enhanced security and fair contract signing;

2. To develop and implement efficient methods to generate and detect single photons in optical fibers, as well as pairs of entangled photons, and to use them to demonstrate in the laboratory our original quantum protocols for message authentication and fair contract signing.

The project started in 2010 and will last until the end of 2012. In this work, we describe the results obtained so far by the QuantPrivTel team and their international collaborators, during the first year of the project, and discuss the outlook of the remaining two years in the context of the state of the art of the field.

II. QUANTUM MESSAGE-AUTHENTICATION

The authentication of public messages is a fundamental problem nowadays for bipartite and network communications. The scenario is the following: Alice sends a (classical) message to Bob through a public channel, together with an authentication tag through a private or public channel. The tag will allow Bob to verify if the message he received via the public channel has been tampered with or if it is indeed the authentic message, originally sent by Alice. A third character, Eve, wants to sabotage this scheme by intercepting Alice's message and sending her own message to Bob, together with a false tag which will convince Bob he is receiving the authentic message. For instance, one could imagine that Alice is sending to Bob her bank account number, to which Bob will transfer some money, and Eve wants to interfere in the communication in such a way that Bob will receive her bank account number believing it is Alice's one, thus giving his money to Eve. The use of authentication tags allows to separate the secrecy

The project *QuantPrivTel – Quantum Private Telecommunications* is supported by Fundação para a Ciência e a Tecnologia, Portugal, through grant PTDC/EEA-TEL/103402/2008.

problem in message transmission from the authentication problem and it is useful even if a secure communication channel is available.

F. M. de Assis[1], P. Mateus and Y. Omar have recently proposed a quantum-enhanced protocol to authenticate classical messages [5], with improved security with respect to the classical scheme introduced by G. Brassard in 1983 [6]. In that protocol, the shared key is the seed of a pseudo-random generator (PRG) and a hash function is used to create the authentication tag of a public message. The authors show that a quantum encoding of secret bits offers more security than the classical XOR function introduced by Brassard. Furthermore, they establish the relationship between the bias of a PRG and the amount of information about the key that the attacker can retrieve from a block of authenticated messages. Finally, they prove that quantum resources can improve both the secrecy of the key generated by the PRG and the secrecy of the tag obtained with a hidden hash function.

III. Quantum Contract Signing

Contract signing between two parties is a procedure that typically involves the parties meeting physically to sign their commitment. To sign a contract at a distance, e.g. online, a trusted third party is required, to ensure there is no fraud in the exchange of signatures. Yet, quantum resources can help us go beyond these limitations.

N. Paunkovic, J. Bouda[2] and P. Mateus have recently presented a fair and optimistic quantum contract signing protocol between two clients that requires no communication with the third trusted party during the exchange phase. They discuss its fairness and show that it is possible to design such a protocol for which the probability of a dishonest client to cheat becomes negligible, and scales as $N^{-1/2}$, where N is the number of messages exchanged between the clients. Their protocol is not based on the exchange of signed messages: its fairness is based on the laws of quantum mechanics. Thus, it is abuse-free, and the clients do not have to generate new keys for each message during the commitment phase. They also discuss the real-life scenario when the measurement errors and quantum bit state corruption due to noisy channels occur and argue that for real, good enough measurement apparatus and transmission channels, the protocol would still be fair. The protocol can be implemented by today's technology, as it requires in essence the same type of apparatus as the one needed for the Bennett-Brassard (BB84) quantum key distribution protocol [3]. Finally, they show that it is possible to generalize this protocol to an arbitrary number of clients.

IV. Single-Photon Experiments

Besides developing new quantum private telecommunication protocols, this project aims also at implementing them in a laboratory. The Optical Communications group (OC-Av) at Instituto de Telecomunicações in Aveiro, Portugal, has started a quantum optics laboratory, with the objective to generate, transmit through optical fibers and detect both single-photon quantum bits and spin-polarized entangled pairs of photons.

During the first year of the project, all these crucial elementary tasks were achieved, with a record distance of more than 20 km for quantum bit transmission and some original methodologic contributions. Namely, N. A. Silva, N. J. Muga and A. N. Pinto proposed a new effective nonlinear parameter measurement using four-wave mixing in optical fibers in a low power regime [8]. The four-wave mixing process in a low power regime is studied both theoretically and experimentally. The coupled-equations for the complex amplitudes are derived and solved. Then, the proposed model is compared with experimental data: the results shows the need of considering both nonlinear and polarization dependent effects in order to obtain an accurate description of the four-wave mixing process in a low power regime. The effective nonlinear parameter is experimentally measured in a dispersion-shifted fiber, and the transition region between an almost co-polarized situation to a decorrelated state of polarization is observed.

The experimental team is now studying the implementation of the original protocols presented here.

V. Outlook

QuantPrivTel is a research project that aims at pushing quantum privacy in telecommunications beyond the famous and now well-established quantum key distributions. The project aims to do so both at the theoretical and experimental levels, by developing new protocols as well as their physical implementation in optical fibers with single photons.

During the first year of the project, two original protocols were developed: quantum-enhanced message authentication and quantum contract signing. These were designed for the case of ideal channels. They are now being revisited in noisy scenarios, in view of their experimental implementation.

At the experimental level, we are now autonomous to generate, transmit through optical fibers and detect single-photon quantum bits, as well as spin-polarized entangled pairs of photons. These are the essential ingredients to tackle the photonic implementation of the two new protocols developed within the framework of the project, which he hope to have running in 2011 (for updated information on the project, please see: www.quantprivtel.org).

Acknowledgment

We acknowledge the support from Fundação para a Ciência e a Tecnologia (Portugal) through the programs POCTI, POCI and PTDC, and the project PTDC/EEA-TEL/103402/2008 QuantPrivTel, which was partially funded by FEDER (EU).

References

[1] M. A. Nielsen, and I. L. Chuang, "Quantum Computation and Quantum Information, Cambridge", UK, Cambridge University Press, 2000.

[2] A. Sernadas, P. Mateus, and Y. Omar, "Quantum Computation and Information", in M. S. Pereira, editor, A Portrait of State-of-Art

[1] Departament of Electrical Engineering, Universidade Federal de Campina Grande, Brazil.

[2] Faculty of Informatics, Masaryk University, Brno, Czech Republic.

Research at the Technical University of Lisbon, 46-65, Springer-Verlag, 2006.

[3] N. Gisin, "Quantum cryptography", Rev. Mod. Phys. 74, 145, 2002.

[4] J. Armengol et al. ,"Quantum communications at ESA: Towards a space experiment on the ISS", Acta Astronautica 63, 165 – 178, 2008.

[5] F. M. Assis, P. Mateus, Y. Omar, "Improving Classical Authentication with Quantum Communication", submitted for publication, 2011.

[6] G. Brassard, "On computationally secure authentication tags requiring short secret shared keys", in Advances in Cryptology, pp. 79–86, Springer-Verlag, 1983.

[7] N. Paunkovic, J. Bouda, and P. Mateus "Fair and optimistic quantum contract signing", submitted for publication, 2010.

[8] N. A. Silva, N. J. Muga, and A. N. Pinto, "Effective Nonlinear Parameter Measurement Using FWM in Optical Fibers in a Low Power Regime", IEEE Journal of Quantum Electronics, Vol. 46, No. 3, pp. 285 - 291, 2010.