Towards an Implementation of Quantum Key Distribution in Optical Fibre Telecommunication Networks

Guido Berlin[a], Gilles Brassard[b], Félix Bussières[a,b], Nicolas Godbout[a], Suzanne Lacroix[a]
Sylvain O'Reilly[a], Daniel Summers-Lépine[a]

[a]Laboratoire des fibres optiques, Dép. de génie physique, École Polytechnique de Montréal,
C. P. 6079, Succ. Centre-ville, Montréal (Québec), H3C 3A7, Canada
[b]Laboratoire d'informatique quantique et théorique, Université de Montréal,
Montréal (Québec), H3C 3J7, Canada

ABSTRACT - Quantum Key Distribution (QKD) is a technique that allows two parties to securely share a random cryptographic key. In this article we propose different schemes to implement QKD in an optical fibre telecommunication network. We show the feasibility of a QKD system for many users with the help of Wavelength Division Multiplexing (WDM) and we discuss strategies to deploy large-scale QKD networks. The question of the required number of trusted signal relays is examined. We also propose ways to build all-fibre sources of entangled photons and stable interferometers. We discuss how the proposed network architectures could greatly benefit from their use.

1. INTRODUCTION

The science of confidentiality in telecommunication, or cryptography, is often of paramount importance, whether it is used for personal, economic or political reasons. The classical approach to cryptography is to allow the two parties, conventionally referred to as Alice and Bob, to use ciphering and deciphering algorithms on the message using a private and random string of bits called the ciphering key. Provided the key is as long as the message, an eavesdropper, usually referred to as Eve, cannot gain any information on the message [1]. This protocol, called the "one-time-pad", thus achieves unconditional security. However, each key bit cannot be used twice, and the difficulty is shifted towards finding a means to privately and continuously share a key at distance. Limiting ourselves to classical physics, no ways to achieve this in a secure fashion are known.

For cryptographic purposes, Quantum Mechanics (QM) succeeds where classical physics does not. In 1984, a breakthrough took place when C.H. Bennett and G. Brassard introduced what is now referred to as the BB84 protocol. According to BB84, Alice sends Bob single photons that are carefully prepared into eigenstates of two non-commuting observables such as the vertical-horizontal and diagonal polarization operators. This can result in the creation of a verifiably secure and random key [2]. Also, by virtue of the Heisenberg uncertainty principle, Eve cannot tamper with the photons without revealing her presence, a feature that is impossible to obtain with classical cryptography. Since then, other protocols were invented and the generic procedure is now called Quantum Key Distribution (QKD). See Ref. 3 for a review.

Over optical fibre links, polarization coding is very unpractical since birefringence randomly fluctuates. Consequently, other ways to encode quantum states were proposed [3]. Without detailing, let's mention that most of these propositions require Alice and Bob to have identical all-fibre Mach-Zehnder interferometers. These are very sensitive to temperature fluctuations and must be actively stabilized. To counter this difficulty, the group of Prof. N. Gisin developed the plug&play scheme that automatically compensates for both birefringence and interferometer fluctuations by a clever use of a Faraday mirror [4]. A different approach uses photonic entanglement, a very unique feature of quantum mechanics, to perform QKD [5,6]. This possibility has also been experimentally demonstrated over optical fibre with the use of actively stabilized all-fibre interferometers [3].

Today, commercial QKD systems are available for dedicated optical fibre links between two parties. However, in order for QKD to become useful on a large scale, optical network architectures on which both classical and quantum communication can efficiently co-exist still need to be built.

2. METHODOLOGY

To go forward from current demonstrations of two-user QKD to a full network architecture, the following issues need to be addressed.

Routing to a particular user: A full QKD network needs a photon routing capabilitiy to enable two arbitrary users to generate a common secret key. As we show in the next section, this can be achieved using Wavelength Division Multiplexing (WDM) in a network architecture where photons at a given wavelength are routed to a particular user. The proposed architecture also allows the use of optical entanglement. This helps in reducing security constraints.

Interferometer-based implementations: Most of the actual propositions for provably secure pairwise QKD over optical fibre (both with and without entanglement) require stable fibre interferometers. Stability can be achieved either with active compensation, a cumbersome task, or with passive compensation, as in the plug&play scheme [4]. However, this is done at the expense of reducing the security level in a way which remains debated. For a network to be scalable, passively stabilized interferometers that do not threaten the security are required. These interferometers need much improvement in thermal and mechanical stability before they can be deployed in networks.

In the next section, we describe in detail our proposed solutions for the implementation of WDM routing, entangled-photon sources and stable all-fibre interferometers.

3. IMPLEMENTATION

3.1 Multi-user using WDM

Without entanglement, the architecture we propose exhibits a star topology in which a trusted server acts as a key distributor using a WDM component, as illustrated in Fig. 1 [7,8].

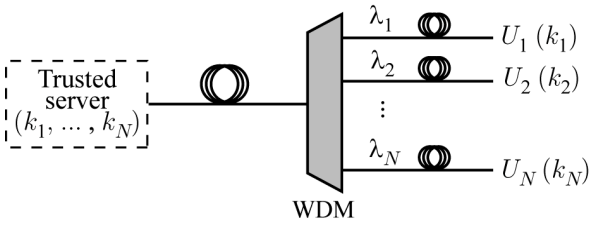

***Figure 1**. Multi-user network using WDM.*

By virtue of WDM, the server can establish simultaneously as many distinct secret keys as needed with any user. For example, the server could generate keys k_i and k_j with users U_i and U_j using wavelengths λ_i and λ_j. When this is done, key k_i can be easily converted into key k_j without revealing any information to the eavesdropper. Thus, users U_i and U_j can exchange information using key k_j.

To demonstrate the feasibility of this proposition, we built a four-user network using the plug&play scheme for pairwise key generation, as illustrated in Fig. 2. We stress that the proposed architecture could be used with any pairwise set-up. The choice of the plug&play scheme was motivated only by the ease with which it can be implemented in the laboratory. The distance between the server and each user was approximately 10 km of single mode fibre.

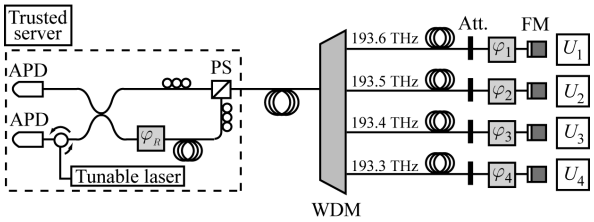

***Figure 2**. Multi-user network using the plug&play scheme* (*see Ref. 4 for details*).

The light source was an Agilent tunable laser operating around 1550 nm. A $LiNbO_3$ electro-optical modulator was used to create 8 ns optical pulses. The detectors were avalanche photodiodes (APDs) operated in the linear mode. The WDM component was a JDSU thin film filter with a 1 dB insertion loss and an isolation of 34 dB between adjacent channels. It showed negligible Polarization Dispersion Loss (PDL). The four channels were in the C-band with a 0.8 nm (100 GHz) spacing. The key parameter to determine the feasibility of the system is the interference visibility [3]. With our system, we measured a visibility of 99.6 ± 0.2 %, or 27 ± 2 dB, for each channel. This implies an optical Quantum Bit Error Rate (QBER) of 0.2 ± 0.1 %, which is well below of the security upper bound for such a system [9]. This demonstrates the feasibility of the proposed architecture over 10 km, and we are confident that the use of WDM will not impose limitations over longer distances.

3.2 Reduction of the number of trusted servers in a network

If the server is operating a wavelength tunable source of entangled photons, it can provide each user in Fig. 1 with a photon of an entangled pair through the WDM device [7]. Users U_i and U_j can then generate a

common key using one of several schemes that take advantage of optical entanglement [3]. A major benefit of this method is that the server cannot cheat or eavesdrop on the key without being caught with overwhelming probability [6]. In other words, the server does not need to be trusted.

Consider now an arbitrarily large network where each point consists of a sub-network as defined in Fig. 1. If, between two users of different sub-networks, there is a communication path that goes through *N* servers (that can now be thought of as relays), we showed that, by using entanglement, only half of them need to be trusted [8]. Therefore, whether employed in a small or large network, entanglement can be used to relax security constraints.

3.3 A tunable source of entangled photons

In order to implement the proposals mentioned above, it is crucial to have an all-fibre tunable source of entangled photons. We are currently working on the design of such a device.

With this device, we seek to achieve what is referred to as energy entanglement by means of four-wave mixing (FWM). Energy entanglement means that the presence of one photon implies the presence of the other. FWM is achieved when there is simultaneous energy conservation and phase matching between two pump photons and two signal photons. In order to obtain FWM, we use "Vectorial Modulation Instability" [10]. This technique takes advantage of birefringence in a fibre in order to modify the phase matching requirement. A first check of entanglement consists of taking the differential signal between two balanced APDs and showing that the noise on the signal is below the individual shot noise.

3.4 Very stable interferometers

As first mentioned in the introduction, long-delay stable all-fibre Mach-Zehnder interferometers are necessary to securely implement scalable QKD networks both with and without entanglement. In the case of all-fibre interferometers, the main contribution to phase drift is due to the thermo-optical effect. This can be passively compensated for by using fibres with different thermal properties for the branches of the interferometer. In our case, one branch is built of SMF-28 and another of specialty fibre. The fibres must be carefully wound on a specially designed mandrel. This mandrel must only minimally support the fibre such that thermal expansion of the mandrel does not itself create phase drift. The shape of this mandrel must be such that the difference in accumulated birefringence phase between the two polarization states is a small multiple of 2π. This condition ensures that the interferometer shows maximal contrast ($\approx$ 20 dB) and negligible PDL.

4. CONCLUSION

Quantum key distribution solves the problem of the generation of secret cryptographic keys of arbitrary length, enabling absolutely secret telecommunications. A quantum key distribution network is envisioned that enables two arbitrary users to generate an encryption key known only to themselves or possibly by as few trusted relays as possible. The technique of wavelength division multiplexing was shown to be applicable to QKD networks with minimal performance degradation and to enable routing of individual photons to the intended user. Entanglement of photons, feasible through four-wave mixing in optical fibre, constitutes a very useful resource for QKD, enabling network architectures where servers on local networks need not be trusted and reducing the number of trusted relays in larger networks. Long-delay interferometers minimize security issues and are necessary for coding when entanglement is used. Suitable thermally and mechanically stable long fibre interferometers are feasible and will be available in the near future. All-optical-fibre implementations of scalable QKD networks are poised to become a reality within the next few years.

CIPI SUPPORT

This work is supported by CIPI, NSERC and the eMPOWR Innovation Platform.

REFERENCES

1. C. E. Shannon, Bell System Technological Journal **28**, 656–715 (1949).
2. C. H. Bennet, G. Brassard, Int. Conf. Computers, Systems & Signal Processing, Bangalore, India, IEEE New York 175 (1984).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. of Mod. Phys. **74**, 145 (2002).
4. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New Journal of Physics **4,** 41.1 (2002).
5. A. Ekert, Phys. Rev. Lett. **67,** 661 (1991).
6. C. H. Bennet, G. Brassard and N. D. Mermin, Phys. Rev. Lett. **68,** 557 (1992).
7. G. Brassard, F. Bussières, N. Godbout, and S. Lacroix, Proc. SPIE **5260**, Application of Photonics Technologies, 149 (2003).
8. G. Brassard, F. Bussières, N. Godbout, and S. Lacroix, QCMC04, accepted for publication, Glasglow (2004).
9. N. Lütkenhaus, Phys. Rev. A **61,** 052304 (2000).
10. E. Brainis, D. Amans, M. Haelterman, P. Emplit, S. Massar, NLGW04, MC17, Toronto (2004).