Entanglement and Wavelength Division Multiplexing for Quantum Cryptography Networks

Gilles Brassard[*], Félix Bussières[*†], Nicolas Godbout[†] and Suzanne Lacroix[†]

[*]*Laboratoire d'informatique théorique et quantique, Université de Montréal*
C.P. 6128, Succ. Centre-ville, Montréal (Québec), H3C 3J7 Canada
[†]*COPL, Laboratoire des fibres optiques, École Polytechnique de Montréal*
C.P. 6079, Succ. Centre-ville, Montréal (Québec), H3C 3A7 Canada

Abstract. We describe how optical wavelength division multiplexing (WDM) can be used to build a fibre-based network allowing many users to communicate in a secure fashion using quantum key distribution (QKD). In the simplest implementation, a certain number of trusted relays are necessary when the network gets large. However, we also show that, by using entangled QKD, trusted relays are not necessary for metro-distance networks, and their required number is cut in half for global networks. We also report on a successful demonstration of the proposed architecture over a fibre link of 10 km with the plug&play configuration, which uses weak pulses of light and a Faraday mirror to compensate for the errors introduced by the fibre. The average interference visibility per user is $99.6 \pm 0.2\%$ (27 ± 2 dB). This guarantees the feasibility of the proposed WDM architecture.

INTRODUCTION

Twenty years ago, quantum cryptography (QC) was theoretical speculation at best [1], while today it is commercially available [2, 3]. In a world in which the global economy is relying more and more on the secrecy in information exchange, there is an inevitable growing need for provably secure communications [4]. The mature technology of optical fibre communication is suitable for QC. Indeed, because of the commercial availability of the required optical components, combined with their low loss figures at wavelengths around 1550 nm, the degrees of freedom of light (such as polarization, phase and frequency) have been experimentally used over fibre links by several groups [5].

Despite the tremendous progress in two-user implementations, the development of efficient optical networks that can allow classical and quantum communication for secure data transmission is still in its early stages. We propose a new architecture for implementing a fibre-based network of quantum key distribution using optical wavelength division multiplexing (WDM). The paper is divided into the following sections. First, we show how WDM enables the creation of a local optical network in which any pair of users can communicate in a secure fashion through a trusted relay using non-entangled QKD. To demonstrate the feasibility of the proposed architecture, we report on a four-user network proof-of-principle experiment. Then, we discuss the possibility of using wavelength-tunable entanglement to build a local network that cannot be subverted by an untrustworthy relay. Finally, in a global network made up of several local networks, we show how the use of entangled QKD can reduce by half the number of relays that need be trusted.

MULTI-USER DESIGN USING WDM

Without entanglement, the architecture we propose exhibits a star topology in which a trusted relay acts as a key distributor using a WDM component [6], as illustrated in Fig. 1. We shall say that the network is *local* when there is only one relay for all the users. By virtue of WDM QKD, the relay can establish as many distinct secret keys as it wants with any user. The key generation proceeds as follows between any pair of users.

1. The trusted relay generates keys k_i and k_j with users U_i and U_j using QKD at wavelengths λ_i and λ_j.
2. The trusted relay computes $k = k_i \oplus k_j$, the bitwise exclusive-or of k_i and k_j, and sends it to U_i.

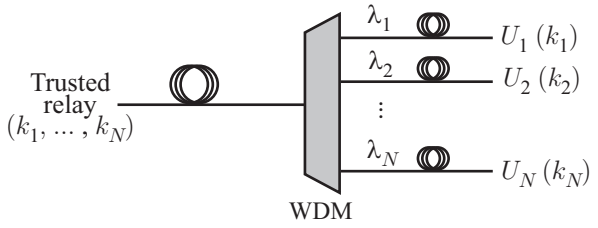

FIGURE 1. Local star network using WDM.

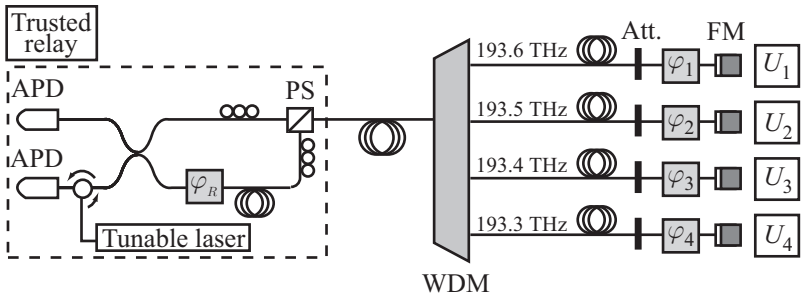

FIGURE 2. Local star network with WDM using the plug&play configuration.

3. User U_i computes the bitwise exclusive-or of k and k_i, resulting in key k_j.
4. Users U_i and U_j communicate using secure key k_j.

This architecture displays several advantages. First, WDM allows for simultaneous use of two-way classical and quantum communication between relay and users. Therefore, the error correction and privacy amplification procedures can take place over the network itself. Also, any QKD implementation can be used for pairwise key generation. Finally, the network can bear as many users as the maximum achievable number of wavelength channels in the fibre (approximately 240 channels/fibre in the C-band with a channel spacing of 50 GHz). The drawback is that the network relay has to be trusted. However, as it is shown later, this limitation can be eliminated by using entangled QKD.

FOUR-USER NETWORK EXPERIMENT

To test the proposed architecture, we built a network of four users with the plug&play configuration [7] for pairwise key generation, as shown in Fig. 2. The link between the relay and each user was 10 km of single mode fibre. The WDM component was a JDSU thin film filter showing a 1 dB insertion loss. Its four channels were in the C-band and spaced by 100 GHz (0.8 nm). The light source was an Agilent tunable telecom laser (linewidth of 100 kHz) modulated in intensity with a fast $LiNbO_3$ electro-optical modulator.

With unattenuated short light pulses, we measured an average interference visibility of $99.6 \pm 0.2\%$ (27 ± 2 dB) for all the channels, yielding an optical Quantum Bit Error Rate (QBER) of $0.2 \pm 0.1\%$. This error rate is well below the security upper bound for individual attacks [8], not taking into account the detector noise and the channel finite transmission. This demonstrates the feasibility of the proposed architecture over 10 km.

The WDM component had an isolation of 34 dB between adjacent channels and showed negligible polarization dependent loss. Therefore, only its insertion loss can affect the performance of the quantum communication when no other channels are in use. We are confident that the use of WDM components should not affect the visibility of the plug&play configuration (or other pairwise QKD configurations that don't use entanglement) over distances much longer than 10 km. However, if many channels were being used simultaneously for classical and/or quantum communication, nonlinear effects such as cross-phase modulation could spoil the crucial phase information carried by single-photon pulses. This possible limitation is under investigation by our group. Note that with the plug&play configuration, it is possible to modify slightly the relay's set-up to keep the key generation rate independent of the number of users in the network, as shown in [6].

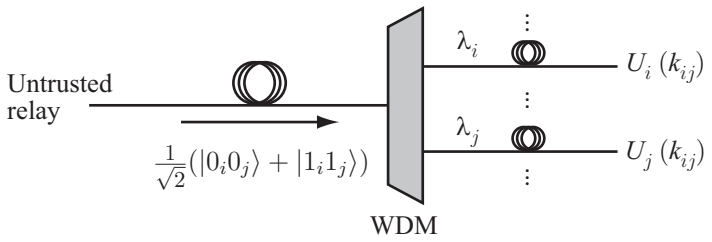

FIGURE 3. Local network using entangled QKD.

NETWORK USING ENTANGLEMENT

Using entangled QKD [9, 10], the relay need not be trusted anymore. For this, we use a wavelength-tunable source of optical entanglement that uses any degree of freedom. The key generation proceeds as follows (please refer to Fig. 3):

1. The relay generates pairs of entangled photons at wavelengths λ_i and λ_j.
2. The entangled photons are sent to users U_i and U_j, through to the WDM component.
3. Users U_i and U_j use standard quantum cryptographic methods to distil a common key k_{ij} from their shared entanglement.

Even if the relay has full control over the quantum states it sends to U_i and U_j (possibly entangling them with some local quantum probe under its control), it cannot fool them into thinking that they have succeeded in establishing a cryptographic key when, in fact, the secrecy of their key is compromised by the relay [10]. Therefore, the relay cannot cheat or eavesdrop on the key without being caught with overwhelming probability.

On the experimental side, such a tunable source of entanglement would have to satisfy strict conditions. Among them is the need for a wide range of tunability around 1550 nm. Also, the linewidth of the two entangled photons should be smaller than the spacing between the WDM channels. The availability of such a source seems reasonable in the near future.

Since entangled QKD is more sensitive to losses, this reduces the maximum spanning distance of the network. However, a recent proof-of-principle experiment showed that QKD with time-bin entanglement could be realized over 50 km of fibre [11], which would be enough for an untrusted network to be deployed over a metropolitan area.

SECURITY CONSTRAINTS IN A GLOBAL NETWORK

Consider now a global network in which each vertex is a local star network as defined above. We suppose that only the relay in each local network has direct physical access to the global network. For the sake of generality, we shall keep the structure of this global network unspecified: for example, it could be a ring network or another network with star topology.

If users U_a and U_b belong to different local networks and there is a communication path between them that goes through N relays, how many of these relays must be trusted? Using entangled QKD, we show here that it is sufficient to trust a well-chosen set of $\lfloor N/2 \rfloor$ relays. To illustrate this, let us label the relays R_1 to R_N, where R_1 is the relay of U_a and R_N the relay of U_b, as shown in Fig. 4. Whenever N is odd, the key generation proceeds as follows.

1. The odd-labelled relays generate entangled photon pairs and send each halves to their nearest neighbours. For example, relay R_3 sends one photon to R_2 and its sibling to R_4. They repeat this process until the even-labelled relays, as well as U_a and U_b, possess sufficiently long keys, $k_1, k_3, \ldots, k_N$, where the index refers to the relay that sent the photons. After this step, users U_a and U_b respectively possess keys k_1 and k_N, and relay R_ℓ, where ℓ is even, possesses keys $k_{\ell-1}$ and $k_{\ell+1}$. By virtue of entanglement, the odd-labelled relays cannot gain information about any of the keys without being caught.
2. User U_a sends the cipher $C_1(m) = m \oplus k_1$ to R_2, which, in turns, applies the one-time pad $k_1 \oplus k_3$ to $C_1(m)$ and gets cipher $C_3(m) = m \oplus k_3$.
3. Relay R_2 repeats step 2 with R_4, and so on until U_b receives the cipher $C_N(m) = m \oplus k_N$, from which he recovers the message m.

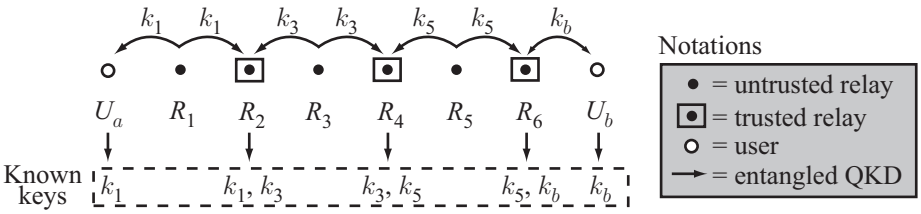

FIGURE 4. Trusted-relay distribution in a global network: case of an even number of relays.

Therefore, assuming the even-labelled relays are trustworthy, the message cannot be deciphered by the odd-labelled untrusted relays. This corresponds to $\lfloor N/2 \rfloor$ trusted relays out of N. For the case when N is even, we get the same result by allowing the relay R_N, which is trusted, to share another key k_b with user U_b by using any bipartite QKD protocol. After the steps mentioned above, R_N sends cipher $C_b(m) = m \oplus k_b$ to U_b, who can safely recover message m.

CONCLUSION

In this article, we showed how WDM can enable the creation of a multi-user local network using non-entangled and entangled QKD. While the local network relay has to be trusted in the first case, this condition can be lifted in the second case, yielding a local network whose security can be trusted even if the relay is adversarial. We experimentally demonstrated the feasibility of the first case with the plug&play configuration. Finally, we showed how the use of entangled QKD helps in reducing by half the number of relays required to be trusted between two users in a global network.

At this point, the challenge lies in the experimental realization of the proposed ideas, especially in the building of a wavelength tunable source of entanglement. Such a source, combined with WDM, could be used to implement other quantum communication tasks, especially if tunable higher-order entanglement could be generated.

ACKNOWLEDGMENTS

This work was supported by Canada's NSERC, the NSERC-EMPOWR Innovation Platform and the Canadian Institute for Photonic Innovations (CIPI).

REFERENCES

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *International IEEE Conference on Computers, Systems & Signal Processing*, Bangalore, India, 175–179 (1984).
2. IdQuantique, `http://www.idquantique.com`.
3. MagiQ Technologies, `http://www.magiqtech.com`.
4. R. Hughes (editor), "Quantum cryptography roadmap", `http://qist.lanl.gov/qcrypt_map.shtml`.
5. N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography", *Review of Modern Physics* **74**, 145–195 (2002).
6. G. Brassard, F. Bussières, N. Godbout and S. Lacroix, "Multiuser quantum key distribution using wavelength division multiplexing", *Proceedings of SPIE 5260: Applications of Photonic Technology 6*, 149–153 (2003).
7. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system", *New Journal of Physics* **4**, 41.1–41.8 (2002).
8. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", *Physical Review A* **61**, 052304.1–052304.10 (2000).
9. A. Ekert, "Quantum cryptography based on Bell's theorem", *Physical Review Letters* **67**, 661–663 (1991).
10. C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical Review Letters* **68**, 557–559 (1992).
11. I. Marcikic. H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré and N. Gisin, "Distribution of time-bin qubits over 50 km of optical fiber", `http://arxiv.org/abs/quant-ph/0404124` (2004).