Architecture, security and topology of a global Quantum Key Distribution network

Romain Alléaume[1], François Roueff[1], Oliver Maurhart[2], Norbert Lütkenhaus[3]
[1] *Ecole Nationale Supérieure des Télécommunications, Paris.*
[2] *Austrian Research Center Seibeldorf, Vienna.*
[3] *Institute for Quantum Computing, Waterloo.*

The performances of Quantum Key Distribution (QKD) systems have notably progressed since the early experimental demonstrations and several recent works [1, 2, 3, 4] indicate that the pace of this progression is very likely to be maintained -if not increased- in the future years. In parallel to this fast progression of QKD techniques, commercial products are also being developed [5], making QKD deployment for securization of some specific "real" data networks more and more likely to occur. It is the goal to the European project Secoqc [6] to deploy a secure long-distance network based on quantum cryptography. It implies the conception of a specific architecture able to connect multiple users that may possibly be very far away from each other while QKD links are currently"point-to-point only" and intrinsically limited in distance.

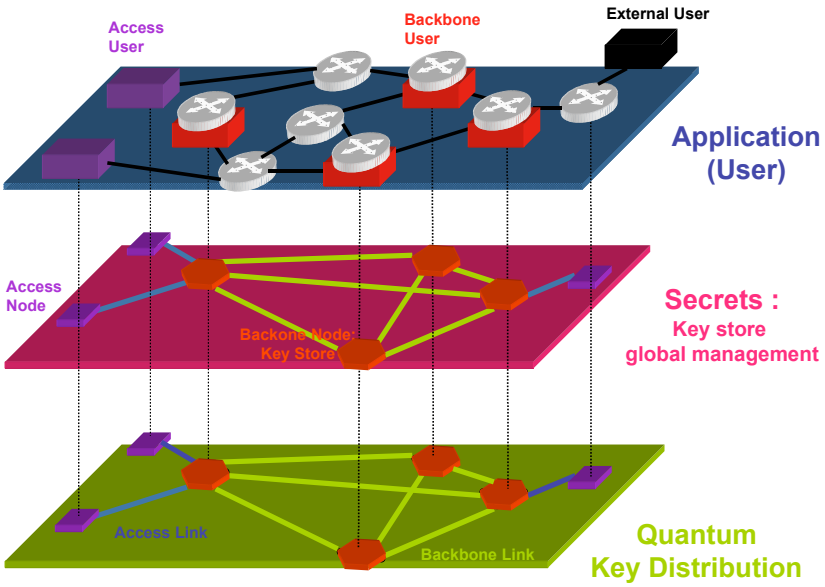

Figure 1: Logical Architecture for the QKD network.

As depicted on figure 1, we have chosen an approach allowing key management on a network-wide level. To gain this ability, we have proposed an original network architec-

ture articulated around a dedicated network, the "network of secrets" ensuring global management of secret keys. This architecture allows to decouple secret key management from quantum key distribution and from the use of the symmetric keys in secure applications.

On a cryptographic level, our network of secrets can ensure long-distance symmetric key distribution with information-theoretic security and we will explain how one can derive rigorous bounds on the security of global key distribution in this framework.

On a more practical basis, in collaboration with the other teams involved in the Secoqc, dedicated protocols and standardized interfaces are being developed and we will give an overview of the work achieved and of the progress towards a network prototype demonstration.

Finally we will present our work on the topological design of QKD networks, showing how the geography together with the structural properties of the graph associated to the network impact its performances.

References

[1] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue, Y. Yamamoto,"Differential phase shift quantum key distribution experiment over 105 km fibre", quant-ph/0507110.

[2] C. Gobby, ZL Yuan, and AJ Shields,"Quantum key distribution over 122km standard telecom fiber", Appl. Phys. Lett. 84, 3762-3764(2004).

[3] H.-K. Lo, X. Ma and K. Chen, "Decoy State Quantum Key Distributio", Phys. Rev. Lett. 94, 230504 (2005).

[4] N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, V. Scarani,"Towards practical and fast Quantum Cryptograph", quant-ph/0411022.

[5] www.magiqtech.com, www.idquantique.com

[6] www.secoqc.net