Network Architectures for QKD

Benjamin A. Small and Keren Bergman
Department of Electrical Engineering, Columbia University, New York 10027
bas@ee.columbia.edu; 212.854.2768

We present two schemes for QKD network architectures based on two ubiquitous topologies: the tree and the ring. Quantum key addressing schemes and their implications are also discussed.

Introduction

The distribution of cryptography keys by exploiting the fundamental laws of quantum mechanics offers an unprecedented degree of network security [1]–[3]. Recent demonstrations have illustrated the feasibility of quantum key distribution (QKD) over conventional optical telecommunications hardware [4]–[6], and even through sufficiently transparent photonic switching devices [7].

The next step in the evolution of QKD systems is likely to involve networks that offer more than simple point-to-point communications pathways. The distribution of quantum keys to multiple cryptographic clients ("Bobs") could potentially save hardware costs over simple one-to-one distribution models. We investigate possible schemes and architectures for multiple-client QKD networks.

Conventional network topologies, viewed in the context of QKD, offer unique advantages and disadvantages. Conventional network analyses focus on performance metrics like latency, throughput, and acceptance rate, which are not of major importance to QKD systems. Instead, a QKD network should be characterized by its secret key rate (or sifted key rate), and sensitivity to eavesdropping or security.

We consider architectures derived from two basic network topologies: the tree or multiple-stage butterfly, and the ring or one-dimensional torus.

Distribution Tree

A tree topology is perhaps the most intuitively obvious choice of network structure for QKD from a single host (Alice) to multiple clients (Bobs). In this architecture, the keys are accompanied by a header or label, transmitted on a different wavelength or wavelength band in parallel with the single-photon dataline. At each branch in the network, the routing nodes set up a $1\times b$ (generally 1×2) transparent optical switch based upon the wavelength-parallel header or label. The quantum encoded information is then allowed to pass to the correct branch, continuing down the tree until the correct client destination is reached (Fig. 1). The unencrypted public communication channel can be transmitted on the same hardware at yet another wavelength or wavelength band.

Assuming the attenuation of the network to be dominated by the switching elements, the total line loss for the QKD scales with

$$l \sim \log_b N/b = \tfrac{1}{2}\log_2 N\,,$$

and all clients experience exactly this attenuation for a balanced network. This loss is important because the sifted key rate for the dataline is given by approximately

$$R = d + (1-d)(1-l)\eta\mu\,,$$

where d is the probability of dark current on the receiver, η is its quantum efficiency, and μ is the mean photon rate [8].

However, in order for Eve to successfully eavesdrop on any particular client within the network, she need only exploit any portion of the network which is upstream of that client. Because classical addresses accompany the quantum key bits, she can easily determine which bits are destined for which client.

Alice can send decoy bits or words to minimize Eve's knowledge of the quantum key. These bits can be in the form of unused quantum words, as in [8],[9]. For the tree architecture, implementing network-layer decoys may be difficult.

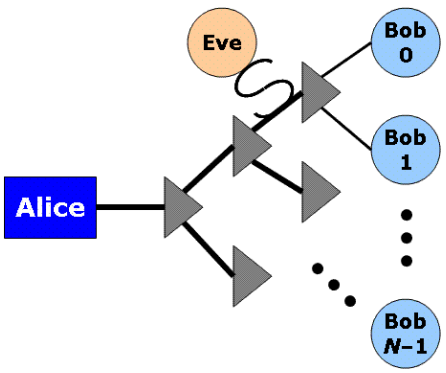

Fig. 1. Schematic of distribution tree architecture with one QKD host (Alice) and N clients (Bobs), in addition to an eavesdropper (Eve). Triangles represent transparent optical switching elements.

Distribution Ring

The ring topology, commonly implemented as a token ring in computer networks, is another basic topology that may be used for QKD. While this architecture could allow multiple cryptographic hosts (Alices) to communicate with multiple clients (Bobs), we focus on a single-host scheme as a means of reducing cost by minimizing the number of expensive single-photon sources and other transmission hardware.

Here, bidirectional optical hardware is used in the network. This allows for the quantum key information to be sent through the network in one direction, and the address information to be sent through the network in the counter-propagating direction. Different wavelength or wavelength bands are used in this architecture as well, again allowing for the unencrypted public communication channel on additional wavelengths or wavelength bands.

In order to address a particular client in this architecture, the host transmits a semaphore or marker so that it reaches the desired client at the same time as the quantum key word or bits, traveling in the opposite direction (Fig. 2). Because the total circumference of the network is unknown to the eavesdropper (Eve), she has no way of knowing which bits are intended for which hosts. It is therefore extremely difficult for her to determine which eavesdropped bits belong to which keys. If Eve attempts to determine the network circumference by launching a pulse onto the line, Alice will also see that pulse and will immediately know that the network is compromised. Furthermore, Alice can generate network-layer decoys by sending quantum key information without an appropriate semaphore.

Although this architecture provides network-layer security, its dataline performance is worse than the distribution tree. Here, the line loss can vary on the interval $2 \le l \le N+1$, with a mean of $\langle l \rangle \sim \frac{1}{2}(N+3)$. In order to eliminate the variance of loss from host to host, additional attenuation can be added to the earlier hosts.

Conclusions

We have presented two schemes for QKD network architectures based on two commonly found topologies. The benefits and shortcomings of each to QKD rate and security were enunciated.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Intl. Conf. Comput., Syst., Signal Process.*, Bangalore, India, 175–179, 1984.

[2] C. H. Bennett, *et al.*, "Experimental quantum cryptography," *J. Cryptol.* **5** (1), 3–28, 1992.

[3] N. Gisin, *et al.*, "Quantum cryptography," *Rev. Mod. Phys.* **74** (1), 145–195, 2002.

[4] K. J. Gordon, *et al.*, " A short wavelength gigahertz clocked fiber-optic quantum key distribution system," *IEEE J. Quant. Electron.* **40** (7), 900–908, 2004.

[5] N. I. Nweke, *et al.*, "Experimental characterization of wavelength separation for 'QKD+WDM' co-existence," in *Proc. CLEO* **2**, Baltimore, CWO6, 2005.

[6] R. J. Runser, *et al.*, "Demonstration of 1.3 μm quantum key distribution (QKD) compatibility with 1.5 μm metropolitan wavelength division multiplexed (WDM) systems," in *Proc. OFC* **3**, Anaheim, OWI2, 2005.

[7] P. Toliver, *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photon. Technol. Lett.* **15** (11), 1669–1671, 2003.

[8] D. Stucki, *et. al.*, "Fast and simple quantum key distribution," *Appl. Phys. Lett.* **87**, 194108, 2005.

[9] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Appl. Phys. Lett.* **91**, 057901, 2003.

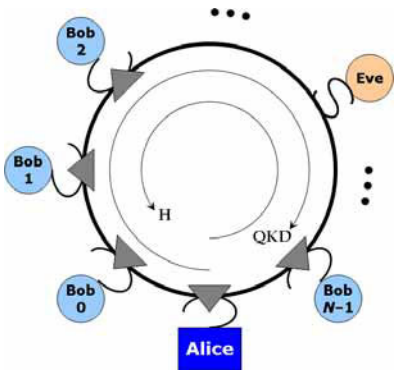

Fig. 2. Schematic of distribution ring architecture with one QKD host (Alice) and *N* clients (Bobs), in addition to an eavesdropper (Eve). Triangles represent transparent optical switching elements. The QKD information and the header semaphore (H) propagate in opposite directions.