Node Modules and Protocols for the Quantum-Back-Bone of a Quantum-Key-Distribution Network

O. Maurhart, T. Lorünser, T. Länger, C. Pacher, M. Peev, A. Poppe

Austrian Research Centers GmbH - ARC, Department Safety and Security, Quantum Technologies, Donau-City-Str. 1, 1220 Vienna, Austria, andreas.poppe@arcs.ac.at

Abstract The very recent demonstration of the SECOQC QKD-network convincingly extended single QKD-links to QKD-networks gaining new functionalities. The needed interfaces, protocols and node modules are explained.

Introduction

Quantum key distribution (QKD) was successfully demonstrated over single QKD-links during the last years. Thereby the key rate expanded from few bits/s to Mbits/s (only quantum part already demonstrated). QKD-networks must replace the single point-to-point QKD-links (Fig. 1) in order to overcome the corresponding quadratic scaling with the number of users. Moreover, well-designed QKD-networks are capable to introduce several more features based on routing of secrets through the Quantum-Back-Bone QBB-network. The EC funded FP6 Integrated Project SECOQC [1] focused on the demonstration of these novel features by fully implementing a QKD-network [2] in a test bed, presented in Vienna, October 2008.

SECOQC QKD-Network

In this prototype a wide range of heterogeneous QKD-systems [3] engineered by SECOQC partners were connected via node modules, which provide standard interfaces and execute the novel network-wide secret distribution protocols. These QKD-links continuously deliver secret keys to key stores allocated in the nodes at the stations BREIT, SIE, ERD and GUD. They are part of the fibre ring network, operated by Siemens Austria. Potential users (U_X in Fig. 1) are connected to the QBB by short distant links of a quantum access network QAN. To connect two users (e.g. Alice and Bob) over the QBB, different paths are possible.

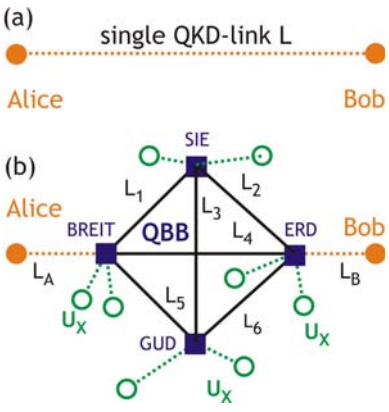

Fig. 1: (a) Point-to point QKD-link L, a typical solution nowadays. (b) Quantum-back-bone (QBB) nodes: squares; QBB-QKD-links: L_1 to L_6; access QKD-links: L_A, L_B and other potential users U_x.

Nodes of the QKD-network

Besides the QKD devices for the QBB and QAN, the nodes host the node modules. Clearly, secure keys are stored there, so all devices need to be placed inside trusted areas. The main objectives of a node module are threefold:

(a) to enable the functionality of all point-to-point QKD links connected to the node, to manage the key generated over these links, and on this basis, to ensure point-to-point information theoretically secure communication connectivity to all nodes in the network associated to the node by direct QKD links,

(b) to determine a path from the node to any arbitrary destination node in the network along a sequence of nodes connected by direct QKD links,

(c) to ensure an end-to-end transport of secret key material along this path using the hop-by-hop transport mechanism.

These three distinct types of functionalities (or services) can be grouped in network layers: Quantum Point-to-Point layer, the Quantum Network Layer and the Quantum Transport Layer.

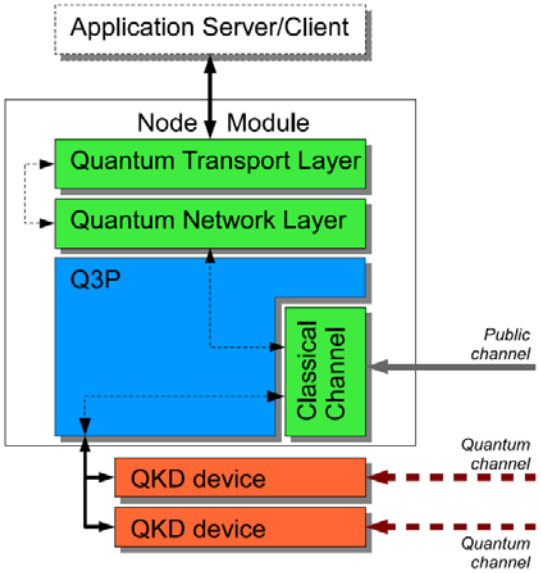

Fig. 2: Block diagram of a node in the QBB. Different QKD devices are operated by the node module by Q3P. The secrets are routed over the QBB by the Network Layer and Transport Layer to the users attached by the QAN or serve an application directly. Each QKD device is connected by the quantum channel to its fixed counterpart operated in another node. The public internet or a dedicated fibre can be used for the public channel.

978-3-8007-3173-2

QKD-Network Protocols

The following three protocols present a standard-like interface, which can easily be embedded in current telecom network infrastructures. Applications running on upper layers need not to be modified in order to use the unconditionally secure key material:

The lower layer realizes a novel *Quantum Point-to-Point Protocol Q3P*, which provides standard classical communication interfaces to the QKD devices. Key Stores inside the Q3P protocol-engines take care of the generated secrets, which are used for One-Time-Pad encrypted communication and information-theoretically secure message authentication between adjacent nodes. This design strictly separates key production from key usage. As Q3P manages the communication to the peer nodes, the QKD devices are exempted from any classical networking configuration maintenance and focus on performing the key distillation process alone.

Q3P is capable of enclosing any higher-layer protocol. For example running IPv4 or IPv6 over Q3P for routing purposes appears straight-forward, but turns out to be suboptimal. To take care of economic and careful utilization of the underlying key material the *Quantum Network Layer QKD-NL* was designed. Based on OSPF the routing information exchanged by QKD-NL as link state packets holds additional properties addressing the average secure key generation rate on each link as well as the current amount of key material, available in the respective key store. Routing information is exchanged non-encrypted, but authenticated over the Q3P links. As this introduces a constant key consumption on the lines even if no traffic occurs, one has to take care in fine tuning the link state announcement frequency.

The *Quantum Transport Layer QKD-TL* protocol is responsible for an end-to-end transport between non adjacent peers in the SECOQC QKD-network. Derived from TCP/IP, this protocol introduces new techniques to prevent network congestion. As in a packet switched network, a congested node tends to discard packets, QKD-TL tries to prevent this condition by reacting pro-actively on the basis of a newly introduced signalling mechanism, triggered by key store shortages within the intermediate nodes.

Results

Figure 3 demonstrates routing in the QBB of the QKD network. The key store contents of the individual links and the transport rate of secure key through the QBB are plotted as a function of time. A user connected to the QBB node ERD is demanding a shared secret key with another user connected to the QBB node BRT in bursts with an average rate of approx. 1 KiB/s=8192 bit/s, far more than a secure key rate of typical single QKD-links nowadays. First the direct link L4 (Fig. 1) is used. After one hour approx 3.5MiB of secret key have been consumed and L4 reaches its minimum keystore threshold and stops delivering keys for the moment (The minimum key threshold ensures that enough key remains in the keystore to authenticate the classical channel during further key generation). The route L2-L1=ERD-SIE-BRT takes over. Approx. 1.5 hours later this route reaches its minimum key threshold too, and ERD-GUD-BRT takes over for the next half an hour until all keystores are emptied.

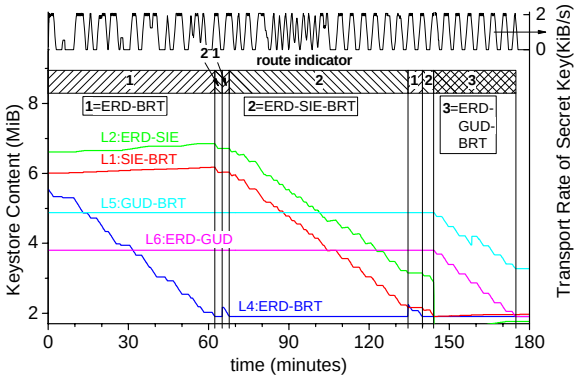

Fig. 3: Measured results: An application demands bursts of secure keys much higher as the QKD-link generation rates. The transport rate of secure key between the QBB-nodes ERD and BRT reduces the keystores of the direct link (route indicator = 1), secondly the keystores of the links combined at node SIE (2) and at the end also over node GUT (3).

Conclusions

We successfully demonstrated the functionalities of a QKD-network on the deployed test-bed, where highly mature QKD-links worked together with the novel protocols Q3P, QKD-NL and QKD-TL. This important step towards future markets for QKD was achieved by a collaboration of 41 partners within SECOQC.

References

1 http://www.secoqc.net/
2 A. Poppe et al., IJQI **6** 209 (2008).
3 M. Peev et al., submitted to NJP, special edition.