The SECOQC quantum key distribution network in Vienna

2009 New J. Phys. 11 075001

(http://iopscience.iop.org/1367-2630/11/7/075001)

New Journal of Physics
The open-access journal for physics

The SECOQC quantum key distribution network in Vienna

M Peev[1,20], C Pacher[1], R Alléaume[2], C Barreiro[3], J Bouda[4], W Boxleitner[1], T Debuisschert[5], E Diamanti[2,6], M Dianati[7], J F Dynes[8], S Fasel[3], S Fossier[5,6], M Fürst[9], J-D Gautier[3], O Gay[10], N Gisin[3], P Grangier[6], A Happe[1], Y Hasani[1], M Hentschel[11], H Hübel[12], G Humer[1], T Länger[1], M Legré[10], R Lieger[1], J Lodewyck[5,6,13], T Lorünser[1], N Lütkenhaus[14,15], A Marhold[16], T Matyus[1], O Maurhart[1], L Monat[10], S Nauerth[9], J-B Page[10], A Poppe[1], E Querasser[1], G Ribordy[10], S Robyr[10], L Salvail[17], A W Sharpe[8], A J Shields[8], D Stucki[3], M Suda[1], C Tamas[1], T Themel[1], R T Thew[3], Y Thoma[3], A Treiber[12], P Trinkler[10], R Tualle-Brouri[6], F Vannel[3], N Walenta[3], H Weier[9], H Weinfurter[9,18], I Wimberger[19], Z L Yuan[8], H Zbinden[3] and A Zeilinger[11,12]

[1] AIT Austrian Institute of Technology GmbH (formerly Austrian Research Centers GmbH—ARC), Donau-City-Straße 1, 1220 Vienna, Austria
[2] Telecom ParisTech and LTCI—CNRS, 37/39 rue Dareau, 75014 Paris, France
[3] Group of Applied Physics, University of Geneva, 1211, Geneva 4, Switzerland
[4] Faculty of Informatics, Masaryk University, Botanická 68a, 602 00, Brno, Czech Republic
[5] Thales Research and Technology France, RD 128, 91767 Palaiseau Cedex, France
[6] Laboratoire Charles Fabry de l'Institut d'Optique – CNRS – University Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France
[7] University of Surrey, Guildford, Surrey GU2 7XH, UK
[8] Toshiba Research Europe Ltd, 208 Cambridge Science Park, Cambridge CB4 0GZ, UK
[9] Department für Physik, Ludwig-Maximilians-Universität, 80799 München, Germany
[10] id Quantique SA, Chemin de la Marberie 3, 1227 Carouge/Geneva, Switzerland
[11] Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria
[12] Quantum Optics, Quantum Nanophysics and Quantum Information, Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria

1367-2630/09/075001+37$30.00

[13] Observatoire de Paris—SYRTE, 61 Avenue de l'Observatoire 75014 Paris, France
[14] Institute of Theoretical Physics, University Erlangen-Nuremberg, Staudtstrasse 7/B3, 91058 Erlangen, Germany
[15] Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[16] Bearingpoint INFONOVA GmbH, Seering 6, 8141 Unterpremstätten/Graz, Austria
[17] Département d'informatique et de recherche opérationnelle, Université de Montréal, Pavillon André-Aisenstadt, Montréal H3C 3J7, Canada
[18] Max-Planck-Institut für Quantenoptik, 85748 Garching, Germany
[19] Siemens AG Österreich, Siemensstraße 92, 1211 Wien, Austria
E-mail: Momtchil.Peev@ait.ac.at

New Journal of Physics **11** (2009) 075001 (37pp)
Received 25 March 2009
Published 2 July 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/7/075001

Abstract. In this paper, we present the quantum key distribution (QKD) network designed and implemented by the European project *SE*cure *CO*mmunication based on *Q*uantum *C*ryptography (SECOQC) (2004–2008), unifying the efforts of 41 research and industrial organizations. The paper summarizes the SECOQC approach to QKD networks with a focus on the trusted repeater paradigm. It discusses the architecture and functionality of the SECOQC trusted repeater prototype, which has been put into operation in Vienna in 2008 and publicly demonstrated in the framework of a SECOQC QKD conference held from October 8 to 10, 2008. The demonstration involved one-time pad encrypted telephone communication, a secure (AES encryption protected) videoconference with all deployed nodes and a number of rerouting experiments, highlighting basic mechanisms of the SECOQC network functionality.

The paper gives an overview of the eight point-to-point network links in the prototype and their underlying technology: three plug and play systems by id Quantique, a one way weak pulse system from Toshiba Research in the UK, a coherent one-way system by GAP Optique with the participation of id Quantique and the AIT Austrian Institute of Technology (formerly ARC[21]), an entangled photons system by the University of Vienna and the AIT, a continuous-variables system by Centre National de la Recherche Scientifique (CNRS) and THALES Research and Technology with the participation of Université Libre de Bruxelles, and a free space link by the Ludwig Maximillians University in Munich connecting two nodes situated in adjacent buildings (line of sight 80 m). The average link length is between 20 and 30 km, the longest link being 83 km.

[20] Author to whom any correspondence should be addressed.
[21] Austrian Research Centers GmbH—ARC is now operating under the new name AIT Austrian Institute of Technology GmbH following a restructuring initiative.

The paper presents the architecture and functionality of the principal *networking agent*—the SECOQC *node module*, which enables the authentic classical communication required for key distillation, manages the generated key material, determines a communication path between any destinations in the network, and realizes end-to-end secure transport of key material between these destinations.

The paper also illustrates the operation of the network in a number of typical exploitation regimes and gives an initial estimate of the network transmission capacity, defined as the maximum amount of key that can be exchanged, or alternatively the amount of information that can be transmitted with information theoretic security, between two arbitrary nodes.

Contents

1. Introduction

The project 'Development of a Global Network for SEcure COmmunication based on Quantum Cryptography' (SECOQC) was a major research effort of 41 research and industrial organizations from the European Union, Switzerland and Russia, which was initiated in 2003 and carried out between April 2004 and October 2008. It was realized as an Integrated R&D project within the 6th Framework programme of the European Commission. The main

objective was to decisively bring forward and pave the way for practical application of the quantum key distribution (QKD) technology, most often referred to as 'quantum cryptography'. QKD has gradually matured from an initial theoretic construct [1], through first experimental realizations [2] to a broad range of distinct QKD technologies [3, 4] and initial commercial products (e.g. http://www.idquantique.com). In spite of this spectacular progress QKD has been considered (especially at the start of the project) as a discipline still mainly remaining in the academic and long-term research domain. While this opinion was and to some extent still is intimately related to psychologic restraints and acceptance barriers with experts in main-stream security research, QKD is in any case limited by a number of constraints:

- limited distance over which key distribution is possible,
- limited (low) rate of key distribution—exponentially decreasing as a function of distance, and
- inherent point-to-point character of communication, which could be a significant obstacle in the majority of relevant application scenarios.

The first two constraints are being gradually lifted but they are still dominating as of today. One of the declared objectives of SECOQC has therefore been to contribute to fostering the performance of QKD systems and simultaneously to improving their technological maturity. A non-exhaustive list of publications of SECOQC results to this end includes the following references [5]–[18].

The third constraint has been principally addressed already in the early days of quantum cryptography. The natural idea to extend point-to-point connections to networks has been studied in the QKD case theoretically [19] and experimentally [20, 21]. In parallel to the conception of SECOQC a first proof-of-principle QKD network demonstrator, the 'DARPA Quantum Network', was deployed between Harvard University, Boston University and BBN in 2004 [22, 23].

The SECOQC approach has been to systematically treat the issue of QKD networks, including their security, their design and architecture, the relevant network communication protocols and finally the implementation, demonstration and test operation of a QKD network prototype. In particular, a trusted repeater QKD network type has been chosen[22].

A number of important results in the discussed fields are published elsewhere [24]–[26]. This publication concentrates on the SECOQC prototype, which has been put into operation in Vienna in 2008, its architecture and functionality. The paper is organized as follows. In section 2, we briefly overview different approaches to QKD networks. We then discuss the principle architecture of the SECOQC network and its basic building blocks, QKD link devices and node modules. We also elaborate the overall SECOQC network prototype topology. Section 3 is devoted to an overview of the QKD link devices integrated in the Vienna SECOQC prototype. Section 4 deals with conceptual design and functionality of the node modules, whereas section 5 highlights the operation and transmission capacity of the overall SECOQC prototype. An outlook to future research objectives in the field of QKD networks is given in the conclusions.

[22] This term is specified in more detail in section 2.

2. The SECOQC prototype—an overview

2.1. Quantum networks

As pointed out above, QKD links (pairs of QKD devices associated by a quantum and a classical communication channel which perform QKD protocol and realize QKD key[23] agreement between the parties controlling the devices) can only operate over point-to-point connections between two users, and cannot be deployed over any arbitrary network topology. To overcome those limitations, it is important to realize networking of QKD links or QKD networks between multiple users.

In general, there are different ways to define QKD networks and types thereof. Below we give a short summary (see [25] for a more detailed discussion).

The SECOQC approach was to define a QKD network as an infrastructure, based on point-to-point QKD capabilities, that aims at information theoretically secure (ITS) *key agreement* and NOT at secure communication[24]. This definition naturally extends the properties of point-to-point QKD and allows us to split the key distribution problem from the related but independent problem of secure communication and thus to concentrate on the essentials of key agreement between parties that do not share a direct, fixed quantum channel. It is important to underline that a QKD network not only allows for a multiuser communication but (depending on realization) also enables ITS key distribution over long distances, increases the key agreement capacity and ensures robustness against denial of service attacks and technical service break-downs.

There are two principal types of QKD network paradigms [19, 25]:

1. quantum channel switching paradigm—creating an end-to-end quantum channel (or more generally distributing quantum resources) between Alice and Bob, or
2. trusted repeater paradigm—transport of keys over many intermediate locations (nodes), which are trustworthy.

End-to-end quantum-channel-based networks could be created by using quantum repeaters [27, 28] that are not yet technically realized. Current technology allows, however, *optical switching* (whereby switching is meant in general terms as some appropriate active or passive classical optical function) that can be applied to the quantum signals in order to create physically, so to say on demand, a direct quantum channel. The interest in such optical QKD networks is that they allow going beyond the two-user QKD, whereby no intermediate sites need to be trusted. This model can, however, not be used to extend the distance over which keys can be distributed. Indeed, the extra amount of optical losses introduced in the switching devices will in reality decrease the transmission capacity of quantum channels and thus the maximal key distribution distance. In addition, in a fully switched optical network any two parties have to share an initial secret to be able to start the QKD key agreement process. So, overall, these types of networks are not scalable and thus suitable for long distance key distribution, although they can be applied to certain metropolitan scale or local area scenarios.

Trusted repeater QKD networks have been discussed in various contexts since the advent of quantum cryptography. Essentially these networks are composed of QKD links, each link

[23] In this section, we use the term *QKD key* to denote key material generated over a single QKD point-to-point link.

[24] Note that key material distributed along the network does not necessarily have a QKD origin, e.g. it can also stem from a true random number generator, and shall be denoted simply as *key* or *key material*.

connecting two separate locations or nodes. A QKD trusted repeater network is then a connected graph, the vertices of which are nodes, and the edges are QKD links. The QKD devices—the end points of the links pointing to a node—are an integral part of this node.

Using the links connected to a node it is possible to retransmit (repeat or relay) key material along the network. The particular mechanism (sometimes called hop-by-hop) works as follows (see e.g. [29] or [23]). The nodes are equipped with classical memories accumulating the QKD key material generated over the connected QKD links. Key distribution is performed over a QKD path, i.e. a chain of QKD links and corresponding nodes, establishing a connection between a sender node and a recipient node. Keys (generated e.g. by a quantum random number generator) are forwarded using unconditionally secure transport along the path: in each node the outgoing key is encrypted by one-time pad (OTP) using QKD key material, stored in the memory of the node, which was previously generated over the outgoing QKD link from the chain. The one-time pad encrypted key is classically dispatched, together with an ITS authentication tag, to the next node on the path, i.e. to the one connected to the other end of the very same link. After being received the authentication tag is verified, the transported key is then decrypted using the identical QKD key material, as the one used for encryption[25]. The process is repeated until the transported key reaches its destination.

End-to-end information-theoretic security is obtained between the sender and recipient nodes, *provided* that all the intermediate nodes can be trusted, as these possess the full communicated information. The trusted nodes play thus the role of (classical) trusted repeaters. Generally speaking trusted repeater QKD networks allow covering arbitrary distances, connecting arbitrary number of participants, and, in contrast to the case of switched QKD networks, utilizing QKD links of different types, provided by different vendors.

As mentioned above, the SECOQC QKD network prototype relied solely on the trusted repeater paradigm. The rationale behind this decision was twofold. On the one hand, it allowed us to concentrate on the novel QKD network-specific issues such as security, design and network communication protocols, mentioned in the introduction, which arise only in the trusted repeater case. (Indeed at any time a switched QKD network is equivalent to a collection of QKD links, whereby mixed—involving both trusted repeating and switching—networks can be seen as trusted repeater networks with dynamic topology.) On the other hand, as pointed out above, this model gave the opportunity of assembling a network out of the devices produced by a number of research groups and featuring a broad variety of QKD technologies. In turn this required both achieving a high degree of stability and engineering maturity in all these technologies and even more importantly contributed to introducing initial interoperability and standardization solutions and simultaneously initiated a world-wide QKD standardization discussion, which is critical for a subsequent practical application of quantum cryptography.

The specific QKD trusted repeater network type, realized by SECOQC, featured the additional constraint that initial secrets (needed for authentication) are only shared between neighboring nodes (i.e. ones directly connected by a QKD link) and not between any arbitrary pair. This constraint ensures that the number of initial secrets to be shared scales (asymptotically in the case of wide area networks) with the number of network nodes and not with their square. This in turn largely simplifies the initialization of a QKD network and the adoption of additional nodes during operation.

[25] This material is stored in the memory of the node and, naturally, originates from the incoming QKD link.

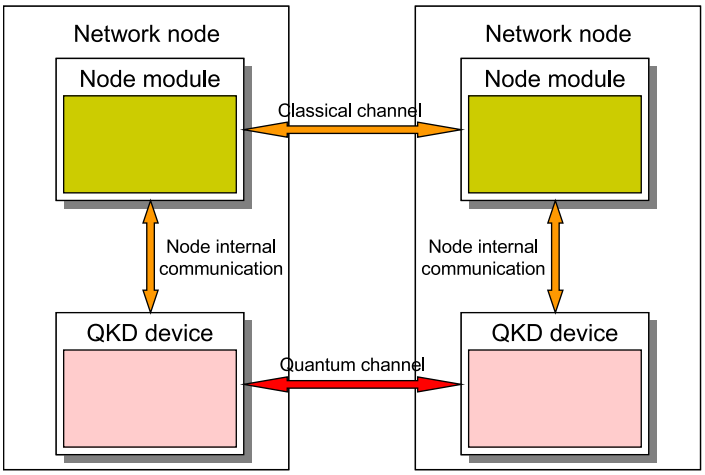

Figure 1. Two QKD network nodes with a node module and QKD device in each node. The QKD devices communicate directly only over the quantum channel. Classical communication between the QKD devices is managed by the node modules.

2.2. Quantum network in Vienna—basic prototype architecture and topology

The basic functionality of a trusted repeater network, as evident from the above discussion, is provided by the nodes of the network. Therefore a central part of the architecture of such networks is that of a network node. It essentially has to contain entities that manage the QKD keys generated over QKD links and ensure crypto services (encryption and authentication) for keys' transport. Simultaneously, each QKD device has to be equipped with a mechanism for device-to-device classical communication, internal key management (of initial and subsequent authentication keys) and crypto services (authentication) in order to have the capacity of distilling a key.

To overcome this redundancy SECOQC has put forward the following approach. QKD devices are stripped off stand-alone key distillation functionality. They have access to the quantum channel alone and perform only a node internal classical communication with a dedicated device, called the node module. The node module manages the QKD key material of all the QKD devices within the node and takes over the authenticated classical communication with the partner QKD devices. In this sense, the only objective of the QKD device is to communicate over the quantum channel, distill and push a QKD key to the node, using the communication facilities of the latter. The node in turn has to manage the point-to-point connections (including classical communication to the neighbors, key management, crypto-services), to be in the position to find paths to required destinations and to realize secure transport protocols as outlined above. A sketch of such an architecture (two nodes each with a QKD device) is schematically represented in figure 1.

The advantage of this approach is its modularity, essentially provided by the node modules, which mask the network to the QKD devices. These operate on a standard point-to-point basis without 'noticing' the network. Simultaneously the nodes encapsulate the underlying QKD technology to the network. From the perspective of the latter it is immaterial what particular QKD technology is used in a link as long as the respective QKD devices communicate with

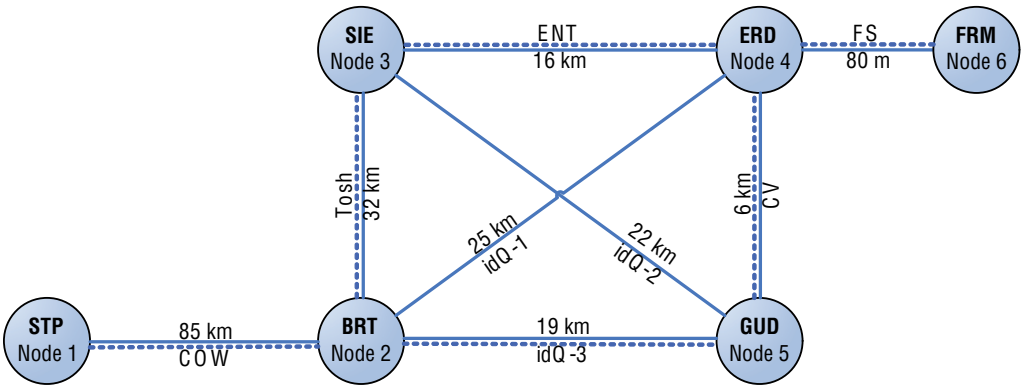

Figure 2. Network topology of the SECOQC QKD network prototype. Solid lines represent quantum communication channels, dotted lines denote classical communication channels.

Figure 3. Satellite map with the locations of the nodes of the prototype.

the corresponding node modules and push up QKD key. In this sense, the essential QKD interface allowing interoperability of heterogeneous QKD devices is the interface between the node module and a QKD device. This interface was designed in the framework of the overall development of the node module which is discussed in more detail in section 4. Here it is important to note that the interface is set up as a SECOQC internal standard and all SECOQC QKD links comply with it. Altogether the SECOQC QKD-network architectural design guarantees seamless scalability, i.e. the ability to arbitrarily extend the network and integrate additional QKD devices in the already deployed nodes.

The SECOQC prototype in particular features six nodes connected by eight QKD links. The network was deployed in the internal glass fiber communication ring of Siemens (a SECOQC project partner) in Vienna, Austria. Overview diagrams of this QKD network are given in figures 2 and 3.

The nodes SIE, BRT, GUD, ERD and FRM were located in the premises of different Siemens dependencies in Vienna (Siemensstraße, Breitenfurterstraße, Gudrunstraße, Erdberger Lände and Siemens Forum, respectively), while the node STP was hosted by a repeater station, near St Pölten, Lower Austria, on a communication line from Vienna to Munich, Germany. The quantum links between the nodes are discussed in more detail in section 3.

Note that a classical communication channel between two nodes does not necessarily follow the corresponding quantum channel. For example any two of the nodes SIE, ERD, GUD and BRT are connected by a direct quantum channel, while direct classical channels connect only sequential locations of the ring SIE–ERD–GUD–BRT–SIE. Classical connectivity between ERD and BRT is routed over SIE or GUD, whereas SIE and GUD are connected over ERD or BRT.

A map showing the particular geographic locations of the SECOQC network nodes is presented in figure 3. The nodes ERD and FRM are located in different buildings in the area of ERD for which reason FRM is not depicted separately. On the map the diagonals between SIE and GUD on the one hand, and between ERD and BRT on the other, are seemingly missing. In fact these *direct* quantum connections pass over ERD and GUD, respectively, as can readily be deduced from figure 2 by comparing the length of the corresponding connections.

The network deployment took place in summer, 2008. After a preliminary test period the network functionality was publicly demonstrated in the framework of a SECOQC QKD conference held from October 8 to 10, 2008. The demonstration took place at Siemens Forum, Vienna, which is situated in the building hosting the node FRM. The demonstration involved one-time pad encrypted telephone communication between FRM and BRT, a secure video-conference with all deployed nodes and demonstration of a number of rerouting experiments, highlighting basic mechanisms of the SECOQC network functionality. These mechanisms will be discussed in section 5 below. Here we would underline that, as pointed out above, a QKD network has the objective of generating identical keys between any two nodes of the network. The classical pay-load secure communication utilizing this key material could potentially use any communication channel between the corresponding nodes. In the SECOQC prototype, we used the physical classical communication channels, shown in figure 2 to pass on the pay-load communication. The corresponding application hardware is represented, together with QKD devices and communication channels on a detailed prototype wiring diagram given in figure 4.

The nodes were situated in 19-inch racks. The photographs of the racks of nodes SIE, ERD, GUD, BRT and STP are shown in figure 5. BRT and STP are both photographed in the premisses of BRT (during deployment) as taking photos in the repeater station near St Pölten was forbidden for security reasons.

3. QKD systems in the SECOQC prototype

One of the main objectives of SECOQC was to bring about a significant advance of the enabling QKD technology. As pointed out in the introduction, the realization of this objective culminated in a major dedicated effort of developing highly mature QKD link devices for the SECOQC network prototype. It was decided to include a wide range of different QKD implementations, while imposing a set of stringent requirements.

For the stage of prototype deployment, all devices had to comply with the following criteria:

- Interoperability:
  - Each QKD-device communicates classically with its peer over a standardized interface, provided by the node module.
  - The QKD-devices push the generated key to the node.
  - The QKD-devices share management information with and accept commands from the node.

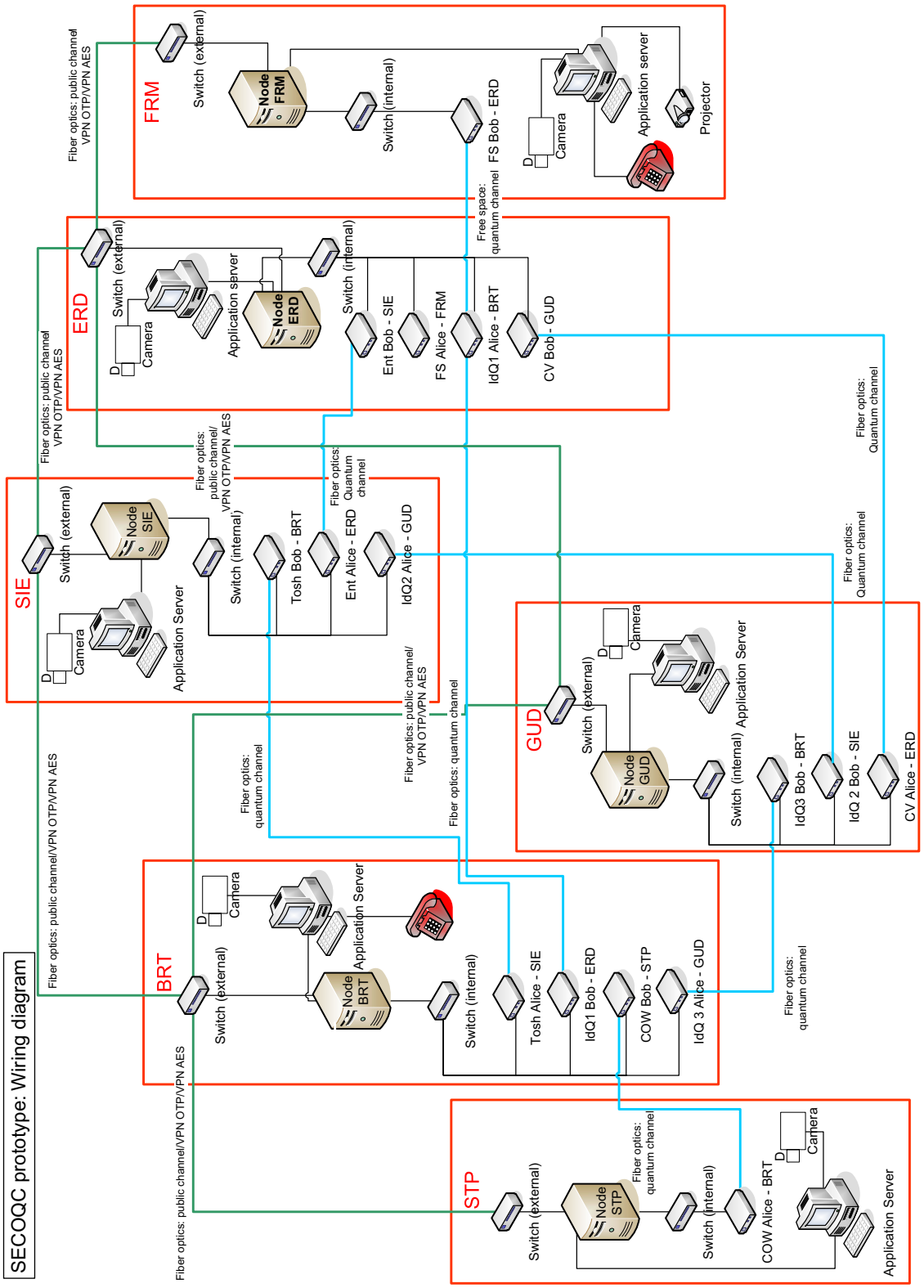

Figure 4. Wiring diagram of the SECOQC protoype. Blue lines represent quantum channels, green lines—classical communication channels, black lines—internal wiring within a node and in the corresponding secure location.

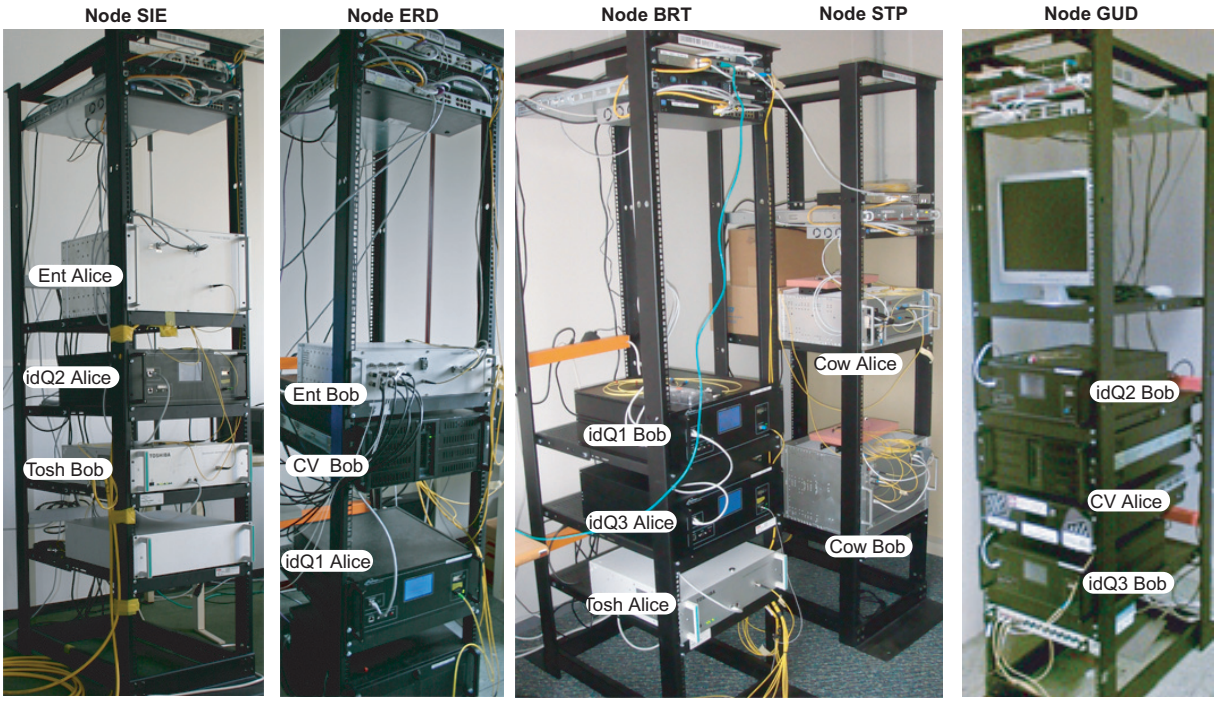

Figure 5. Photographs of the SECOQC network node racks.

- Performance:
  - The QKD links operate at distance exceeding 25 km over standard telecom fiber (equivalent to 6 dB loss with fiber attenuation of approximately 0.25 dB km^{-1}).
  - The key generation rate at 25 km exceeds 1 kbit s^{-1}.

All QKD-devices were fully automated, designed for reliable autonomous operation after deployment and packaged in standard 19-inch racks.

The Vienna prototype integrated eight QKD links, belonging to six different system types: weak laser pulse autocompensated system—the Swiss company id Quantique delivered three 'plug & play' device pairs (idQ1, idQ2 and idQ3), which are modified and upgraded versions of the commercially available 'Cerberis' system. One-way weak coherent pulse system with decoy states—the group of A Shields (Toshiba UK) brought a phase-encoding QKD system (Tosh) with two interferometers, stabilized by pulses that are time multiplexed with the quantum signals. Coherent-one-way—the team of N Gisin at GAP (University of Geneva) provided one QKD system (COW) belonging to the novel class of devices realizing distributed phase reference protocols. Entangled photons—the group of A Zeilinger (University of Vienna) and the AIT Austrian Institute of Technology (formerly ARC[21]) provided a polarization entanglement QKD-system (Ent) featuring long-term automatic operation based on concurrent active stabilization of optical elements. Continuous variables (CV): the consortium CNRS-Thales-ULB led by P Grangier developed a CV QKD system, with Gaussian modulation, reverse reconciliation and homodyne detection of the coherent light pulses.

Finally a 'last mile' (80 m), access free space link has been developed by a Ludwig-Maximilians-University (Munich, Germany) team led by H Weinfurter, which offers a high rate (>10 kbit s^{-1}), stable connectivity to the QKD network in a 24/7 operation regime.

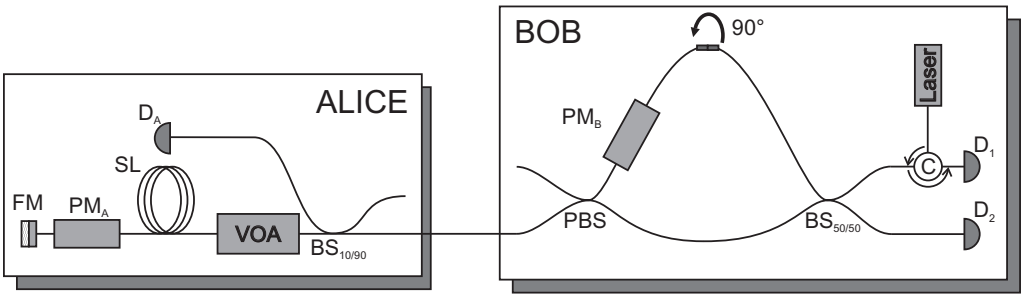

Figure 6. Sketch of plug and play system; C: circulator, $BS_{50/50}$: 50/50 beam splitter, PM_B: Bob's phase modulator, PBS: polarizing beam splitter, $BS_{10/90}$: 10/90 beam splitter, VOA: variable optical attenuator, SL: storage-line, PM_A: Alice's phase modulator, FM: Faraday-mirror, D: detector; see text for details.

These devices are briefly presented below with a focus on the underlying physical principles and the essential performance figures, to give a comprehensive although concise overview of the QKD technology employed in the SECOQC prototype. The reader is referred to the detailed descriptions of the separate systems in dedicated publications (see references in the separate subsections), whereby a number of these publications can be found in this focus issue of *New Journal of Physics*.

The security of the prototype QKD devices has been carefully analyzed by a dedicated quantum information theory group in SECOQC led by N Lütkenhaus. This analysis catalyzed a comprehensive review of security of practical QKD systems [4] for which reason the security of the systems, described below, is not discussed. Note that after the preparation of this review important results on the security of the CV systems have been published. The unconditional security of this protocol against coherent attacks, which are the most general attacks allowed by quantum mechanics, has recently been demonstrated [30].

3.1. Plug and play

A scheme of the plug and play auto-compensating system [31, 32] designed by id Quantique SA (idQ) is shown in figure 6. It employs a strong laser pulse ($\lambda = 1550$ nm) emitted by Bob's laser diode at a frequency of 5 MHz. The pulse is separated at a first 50/50 BS. The two pulses travel down to the two input ports of a PBS, after having traveled, respectively, through a short and a long arm of an unbalanced interferometer. The linear polarization is turned by 90° in the long arm, so that the two pulses exit the PBS through the same port. The separated pulses travel down to Alice, are reflected on a FM, attenuated by the VOA and come back orthogonally polarized. In turn, both pulses now take the other path at Bob's interferometer and arrive simultaneously at the first BS where they interfere. They are detected by InGaAs APD's. Since the two pulses follow the same path in the interferometer (short–long or long–short), the system is auto-compensated. The BB84 [1] and the SARG [33] protocols are implemented using phase coding. Alice applies one of the four phase shifts on the second pulse of each pair and Bob's phase modulator completes the protocol. PM_A is synchronized thanks to the detection of the strong optical pulses coming from Bob with the classical detector D_A. In order to avoid noise enhancement by elastic Rayleigh scattering, the laser pulses are emitted in trains (1250 pulses per train) and are stored in a long delay line at Alice's side before being sent back to

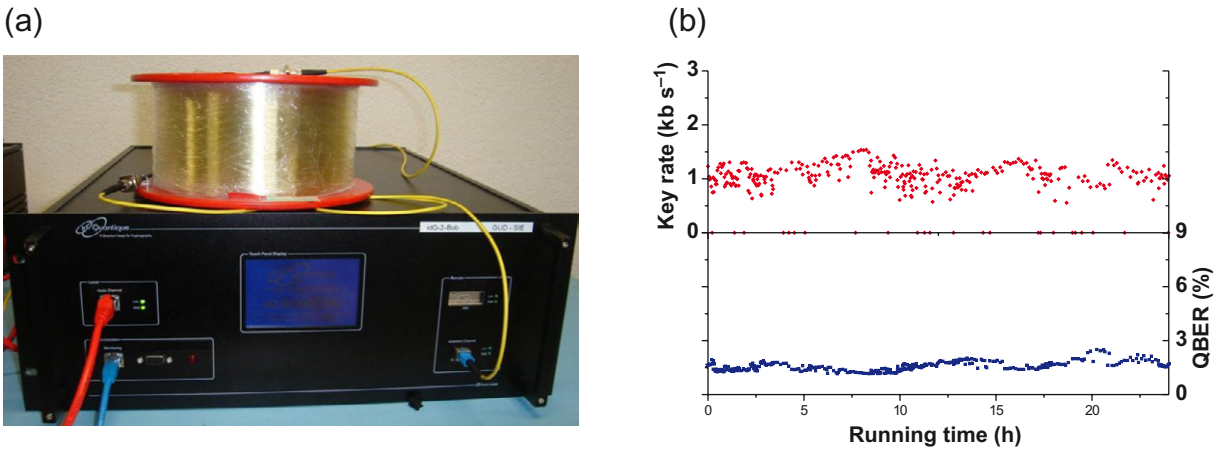

Figure 7. (a) Picture of one id Quantique device. Alice and Bob device look exactly the same. (b) Secret key rate of system id Quantique1 over one day.

Bob. The plug and play auto-compensating design offers the advantage of being highly stable and passively aligned.

On the way back from Alice to Bob, the plug and play system is a usual QKD system using phase encoding between coherent pulses. The strong pulses sent from Bob to Alice do not yet carry an information payload: the quantum information travels only one way, namely from Alice to Bob.

id Quantique developed a QKD-device pair for the SECOQC project based on its commercial quantum key server platform 'Cerberis' (see figure 7(a)). In the quantum cryptography hardware layer, only the length of SL has been changed for the SECOQC project. The SL length has been increased to 25 km (instead of 12 km) to fulfill SECOQC criteria in terms of secret key rate performance (1 kbit s^{-1} over a distance of 25 km (6 dB of loss)). In the software layer, the main modification is the key management. In the standard version of id Quantique QKS system, the key management is performed by an embedded PC and the secret keys are stored in a key buffer. The dispatching of the secret keys to the applications (encryptors normally) is managed by the embedded PC. In the case of the SECOQC project, the key management is performed by the network node module. So, the embedded PC performs the key distillation and sends the secret keys to the node which manages them. Furthermore, the classical communication between Alice and Bob is performed through their respective nodes.

The QBER and secret key rate, over one day, of one of the three id Quantique systems involved in the SECOQC project are shown in figure 7(b). This system was located between BREIT and ERD, and the link loss was 5.75 dB. In order to perform secure key exchanges, id Quantique conforms to instructions of [34] and [35] for BB84 and SARG, respectively. The SARG protocol has been used for the link BREIT–ERD, hence according to [35] the mean number of photons per pulse was equal to 1.03. The mean secret key rate provided by this device is almost equal to the value prescribed by the SECOQC criteria (1 kbit s^{-1}). Moreover, id Quantique strongly focuses on the stability with time of its systems. The one-day data set is a part of a 20 days working period during which similar results have been obtained: this shows the high reliability of id Quantique systems. These have been tested over longer periods as for example for the first real-world application of quantum cryptography. The aim of this

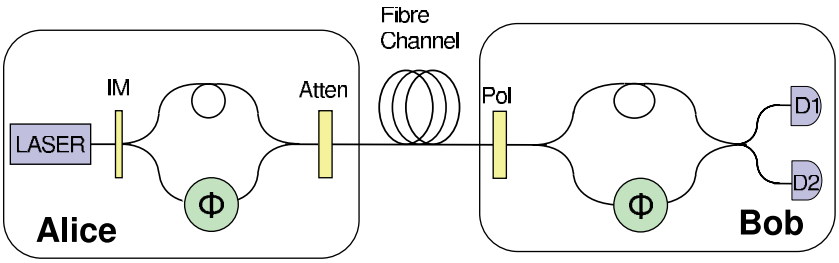

Figure 8. Sketch of the optical layout of the TREL one-way weak coherent pulse QKD system (phase coding). The system represents a BB84 phase encoding protocol incorporating weak + vacuum decoy states. Atten.: attenuator, IM: intensity modulator, Pol: polarization controller, Φ: phase modulators, D1 and D2: avalanche photodiodes.

application was to use quantum cryptography for ensuring the integrity of the dedicated line used for counting the ballots of the Swiss national elections on October 21, 2007. On this occasion, an id Quantique system has been tested during a period exceeding one month before the elections to be sure that the system was reliable enough to be used during critical events. Since this first successful demonstration, an id Quantique QKD system has been used for each election in the Geneva canton.

3.2. One-way weak coherent pulse QKD, phase coding

The one-way weak pulse system (phase coding) designed by Toshiba (Tosh) Research Europe Ltd (TREL) is a fiber optic, decoy state system with phase encoding. It employs a decoy protocol using weak and 'vacuum' pulses. This decoy protocol has been proven to be secure against all types of eavesdropping attacks. A single laser diode, operating with an intensity modulator, is used to produce signal and decoy pulses, so as to prevent attacks on any side channels that allow an eavesdropper to distinguish decoy pulses from signal ones.

The principle design of this one-way fiber optic QKD system is presented in figure 8. It uses two asymmetric Mach–Zehnder interferometers for encoding and decoding. Alice and Bob are linked by a quantum channel (optical fiber). The signal (an optical pulse with wavelength $\lambda = 1.55\,\mu$m) is transmitted along the quantum channel at a repetition rate of about 7 MHz. The clock pulses ($\lambda = 1.3\,\mu$m), which do not temporally overlap with the signal pulses, have a duration of 5 ns each and serve for synchronization purposes. An intensity modulator is used in order to produce signal and decoy pulses of different intensities at random times whereas vacuum decoy pulses are produced by omitting trigger pulses to the signal laser. The signal and decoy pulses are strongly attenuated to the single photon level, while a strong clock pulse is then multiplexed with them to provide synchronization. Bob's detectors are two single photon sensitive InGaAs avalanche photodiodes (APDs). The properties of the detectors are carefully adjusted in order to avoid so-called fake-state attacks [36]–[38] and time-shift attacks [39, 40]. An active stabilization technique is used for continuous operation.

A weak coherent pulse (WCP) decoy state + vacuum state BB84 protocol is implemented [41]. The mean number of photons per pulse for signal μ and decoy states ν are chosen depending on the fiber distance used. For the SECOQC fiber link of 33 km, the values $\mu = 0.48$ and $\nu = 0.16$ were selected, as obtained from numerical optimization of the secure bit rate.

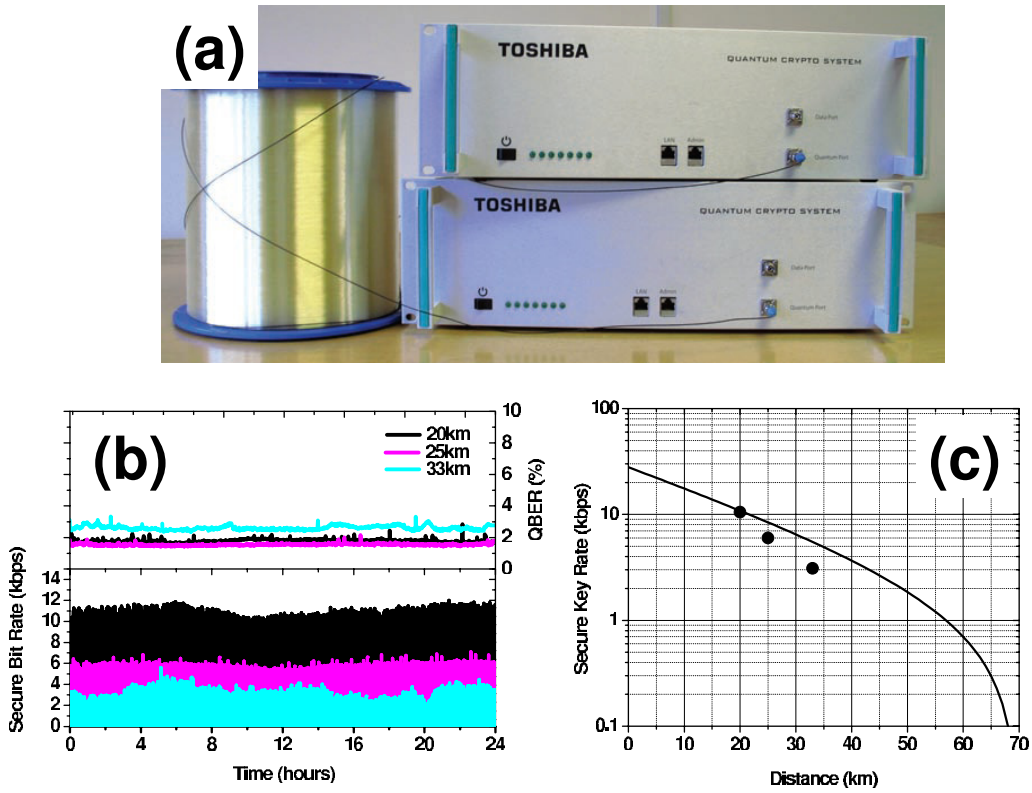

Figure 9. (a) The TREL quantum key distribution system. (b) Lower panel: secure bit rates for 24 h continuous operation for various fiber lengths: 20, 25 and 33 km. Upper panel: corresponding QBER for the various fiber lengths. (c) Secure bit rate as a function of fiber distance. Circles: experimental data derived from (b). Solid line: theoretical calculation optimized for a fiber length of 20 km.

The corresponding optimal probabilities of the various pulses are: signal $N_\mu = 0.92$, decoy $N_\nu = 0.06$ and vacuum $N_0 = 0.02$.

To take into account the uncertainty in the distribution of decoy pulses we set the key distribution session sizes so Bob's detectors received 2×10^6 detection events, which equates to 1×10^6 sifted bits. This permitted very conservative bounds to be placed on the statistical distribution of decoy states mean values. We used ten standard deviations away from the mean decoy photon numbers which for normally distributed data yields a probability of less than 1.5×10^{-23} that the decoy intensity is over or under estimated.

Error correction and privacy amplification was carried out in real time on the devices. All messages exchanged between the two devices including sifting, error correction or privacy amplification were authenticated using a delayed authentication scheme. Delayed authentication was performed at the end of each key generation turn after which the key was pushed to the respective node.

Secure QKD has been demonstrated over a number of fiber distances with this system, as shown in figure 9(b). For a fiber distance of 20 km (4 dB loss), we obtained a secure bit rate of around 11 kbit s^{-1} over 24 h of continuous, autonomous operation [5]. The secure bit rate reduces to an average of 5.7 kbit s^{-1} over a fiber length of 25 km (5 dB loss) over 24 h [6]. This

secure bit rate is almost six times higher than the SECOQC network specification of 1 kbit s^{-1} average secure bit rate over 25 km of fiber.

The QKD link was implemented on the 33 km link in SECOQC network running between Breitenfurterstrasse and Siemenstrasse. During the field trial, we recorded a secure bit rate of 3.1 kbit s^{-1} averaged over a 24 h period. The quantum bit error rate (QBER) was stable and averaged 2.6% over the test. It should be noted that the secure bit rates recorded with the system are over two orders of magnitude higher than those achieved using the BB84 protocol without decoy pulses [42].

A total of 1410 keys were distributed over the 24 h which on average is almost 60 keys an hour. The high secure key refresh rate observed here is important for the security of cryptographic applications [29]. The key refresh rate is also within the SECOQC target of requiring a key latency time of under 60 s (for a 25 km fiber link).

Figure 9(c) plots the dependence of the secure bit rate on the fiber distance, along with a calculation based on the parameters of the 20 km experiment. The bit rate recorded during the field trial over the 33 km link lies considerably below the calculated line. This is because the total loss of this link, measured to be 7.5 dB, is considerably higher than that of standard single-mode fiber. Indeed an equivalent loss is obtained for 40 km of standard single-mode fiber, in good agreement with the calculation. It is noteworthy that the field operation does not reduce the bit rate compared with laboratory conditions, even when comparing values averaged over 24 h of operation. At fiber distances shorter than 20 km, the secure key rate increases to 18 kbit s^{-1} for 10 km and attains 27 kbit s^{-1} for the very short fiber distance of 1 km. Even higher secure bit rates could be obtained at these shorter distances by adjusting the decoy parameters and efficiencies/dark count rates of the detectors.

3.3. Coherent one-way (COW) system, time coding

The COW QKD (time coding) system, designed by GAP (Group of Applied Physics) University of Geneva, with contributions from id Quantique SA and AIT Austrian Institute of Technology (formerly ARC[21]), realizes a novel distributed phase reference COW protocol. Alice, using a CW laser (1550 nm) and an intensity modulator, prepares pulses of weak coherent states or completely blocks the beam (empty or 'vacuum' pulses). A time-of-arrival measurement and an interferometer at Bob's side provide both optimal unambiguous determination of bit values and check the coherence for signal and decoy sequences. The visibility of the various pulse sequences behind the interferometer provides information about an attack by an eavesdropper.

The COW QKD system was developed by GAP [7]–[10]. A schematic of the configuration is drawn in figure 10. The COW-protocol is distantly related to the well-known BB84 protocol [1, 3]. In the latter, two mutually orthogonal bases, e.g. X and the Y in phase-coding schemes, are utilized. However, a third (Z) basis $\{|1\rangle|0\rangle, |0\rangle|1\rangle\}$ can also be used in principle, where applying this basis means simply measuring the time-of-arrival of photons, and is thus insensitive to optical errors [43]. In this way, the COW-protocol can be seen as a BB84 modification, whereby the Y basis is replaced by the Z basis and the X basis is used only occasionally to check coherence [44].

In practice, the logical bits 0 and 1 are encoded in two-pulse sequences, which can be written in each case as a product of a coherent states $|\sqrt{\mu}\rangle$ and $|\sqrt{0}\rangle$. The k-th logical bit is given by

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}|\sqrt{0}\rangle_{2k}, \qquad |1_k\rangle = |\sqrt{0}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}. \tag{1}$$

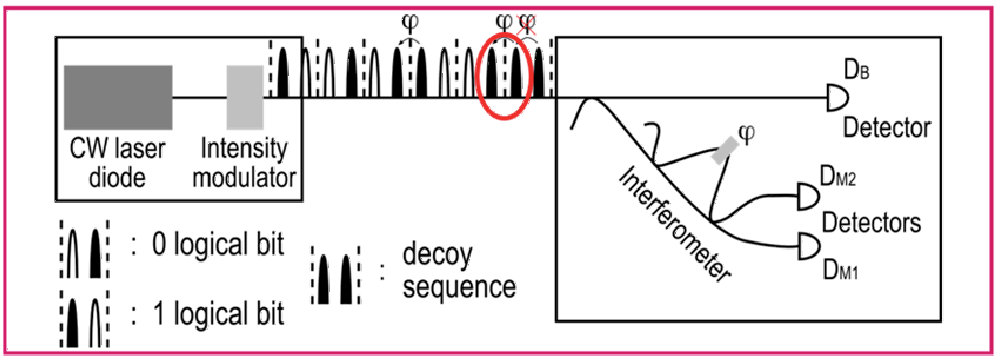

Figure 10. Schematic of the COW QKD system; the left (right) box belongs to Alice (Bob). See text for details.

Note that in equation (1) the states $|0_k\rangle$ and $|1_k\rangle$ are not orthogonal. A time-of-arrival measurement, whenever conclusive, provides the optimal unambiguous determination of the bit value [8]. Moreover, for security reasons, a fraction $f \ll 1$ of *decoy sequences* are produced, which can be written as a tensor product $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$. Now, due to the large coherence length of the CW laser, there is a well-defined phase between any two non-empty pulses across the *bit separation* (a $(1-0)-$ bit sequence) and within *decoy sequences*. Since equally spaced pulses are produced, the coherence can be checked with a single interferometer. Eve cannot count the number of photons in any finite number of pulses without introducing errors: photon number splitting (PNS) attacks can be detected [8, 45]. This is in contrast to the BB84 protocol where PNS attacks must be countered, e.g. by a decoy-state technique, which is based on varying μ [41, 46, 47].

The pulses propagate to Bob through a quantum channel characterized by a transmission t, and are split at a $[t_B : (1-t_B)]$-beamsplitter with a transmission coefficient $t_B < 1$ (in our case, $t_B = 0.9$). Hence, 10% of the pulses are reflected into Bob's interferometer (*monitoring line*) to check the quantum coherence. The transmitted pulses are used to establish the raw key by measuring the times-of-arrival. The counting rate at detector D_B is $R = 1 - e^{-\mu t t_B \eta} \approx \mu t t_B \eta$, where η is the quantum efficiency of the photon detector (10%) and $\mu \approx 0.5$. The detectors are InGaAs SPADs used in free running mode [11].

Security is ensured by considering only detections on Bob's monitoring detectors D_{M1} and D_{M2} originating from two successive interfering non-empty pulses. The wavelength of Alice's laser is adjusted in a way that only detector D_{M1} should click in these cases. Clicks on detector D_{M2} reveal the action of an eavesdropper. (In practice, clicks are also due to detector noise and imperfect interference.) From the probability of a click on D_{M2}, we can estimate Eve's information. Note, imperfect interference does not introduce errors on the key, but is taken into account for privacy amplification.

In conclusion, the COW QKD system is compatible with standard telecom components, insensitive to polarization fluctuations in the fiber and robust against PNS attacks.

3.4. Entanglement-based (Ent) QKD

The Ent QKD system was developed by an Austrian–Swedish consortium (University of Vienna, AIT Austrian Institute of Technology (formerly ARC[21]) and Royal Institute of Technology of Kista) [13]. The system, as shown in figure 12, is based on the unique quantum mechanical

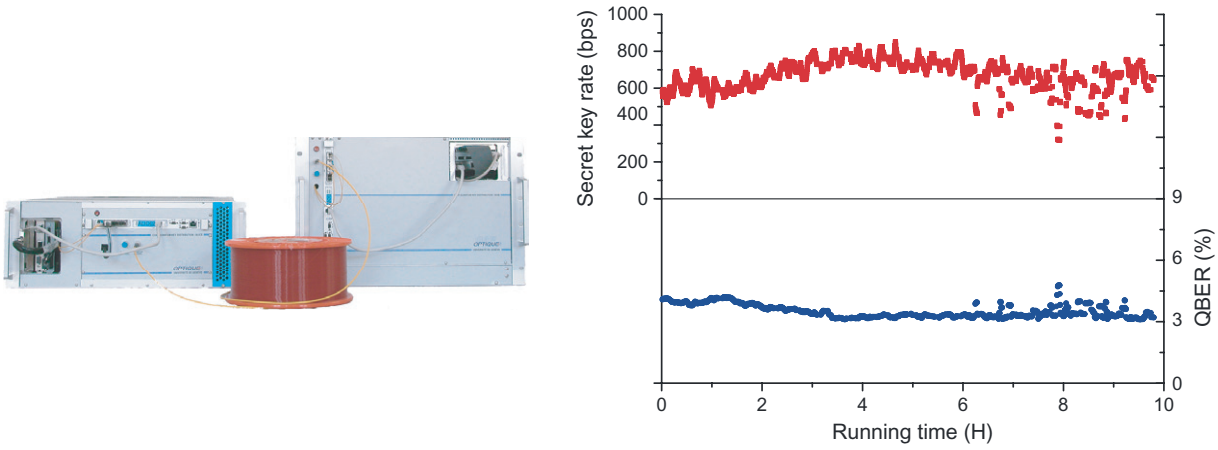

Figure 11. Left: the Alice and Bob units of the COW system in the prototype. Right: real-time secret bit and error rates measured for 10 h in the SECQOC network over the 82 km BRT to STP link.

property of entanglement for generating a secure key from the correlated measurements at Alice and Bob [48, 49]. The asymmetric source at Alice [12] produces two photons of different wavelengths (810 and 1550 nm) by spontaneous parametric down-conversion in a ppKTP crystal set. The 810 nm photon is measured by Alice in a passive polarization analyzer (one 50/50 beamsplitter and two polarizing beamsplitters) and detected by four Si-APDs (avalanche photo diodes). The 1550 nm photon of the pair travels down the quantum channel with low transmission losses and is registered by Bob using a similar passive polarization analyzer but with four InGaAs-APDs for detection. Implementing the BBM92 protocol [49] for entangled states, the polarization measurement results at Alice and Bob are processed by the onboard electronics and forwarded to external computers, where the QKD protocol stack is executed to generate the secure key [4].

In order to guarantee the long-term stability of the key exchange as required in the SECOQC network, several active and automated stabilization modules had to be included:

- *Source stabilization*: the photon flux emitted from the crystal must be efficiently coupled into the single mode fibers leading to the detectors at Alice and Bob. Piezo-actuated fiber couplers readjust automatically to achieve maximum photon detection rates.
- *State alignment*: to minimize the error, the bases at Alice's and Bob's units have to be aligned with respect to each other. Polarization drifts in the units are actively compensated by electronic polarization controllers.
- *Polarization control*: to have a reliable distribution of polarization encoded qubits the quantum channel (optical fiber) must be stabilized. Employing a time-multiplexed polarization control the system can correct polarization drifts occurring along the fiber due to environmental influences.
- *Delay synchronization*: the trigger signals used to gate Bob's InGaAs-APDs must be synchronized to open the gate when a single photon is expected. Automated electronic delay lines can be readjusted to compensate for drifts in the timing.

These modules also allow for a fully automated start up, which takes about 10–20 min after the system is newly installed. The units at Alice and Bob are packed into 19-inch cases for integration into standard telecommunication racks (figure 13(a)).

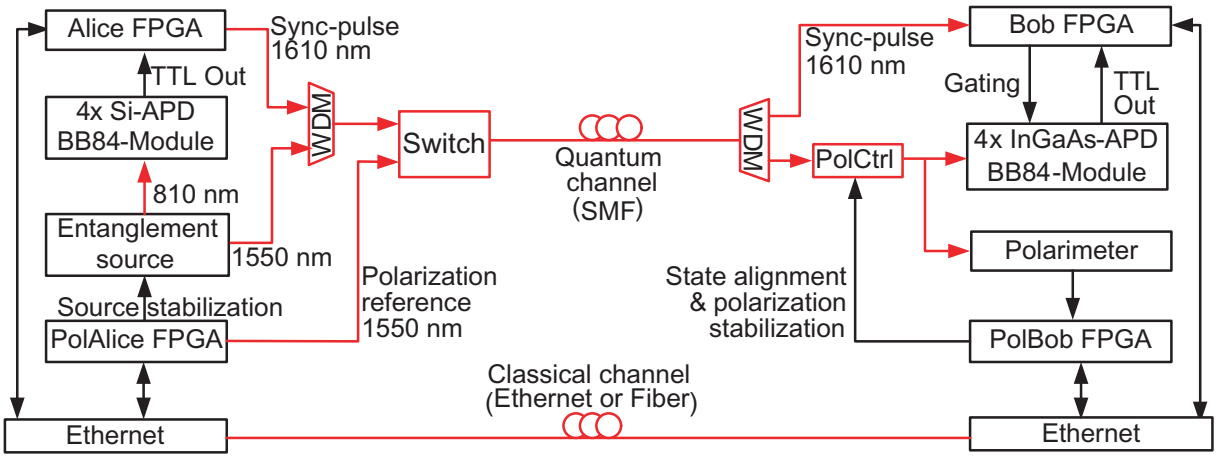

Figure 12. Schematic of the Ent QKD system with optical connections in red and electronic connections in black. The source, located at Alice, produces polarization-entangled photon pairs ($|\phi\rangle = \frac{1}{\sqrt{2}}(|H_{810}H_{1550}\rangle + e^{i\phi}|V_{810}V_{1550}\rangle)$) at highly non degenerate wavelengths (810 nm and 1550 nm). The 810 nm photons are analyzed locally at Alice in four polarization states (0°, 90°, +45° and −45°) and detected using four Si-APDs (avalanche photo diode). The 1550 nm photon is transmitted to Bob using standard single-mode telecom fibers. At Bob, the photons are analyzed in the same four polarizations and detected using four InGaAs-APDs. All detection events are processed on FPGA electronics boards and logged onto computers. A classical communication channel is used to establish the secret key between Alice and Bob. Trigger pulses (1610 nm) are generated at Alice and multiplexed on the quantum channel to gate the InGaAs-APDs at Bob. Additional FPGA electronics control the source stabilization module at Alice and, together with a polarimeter, the polarization stabilization module at Bob.

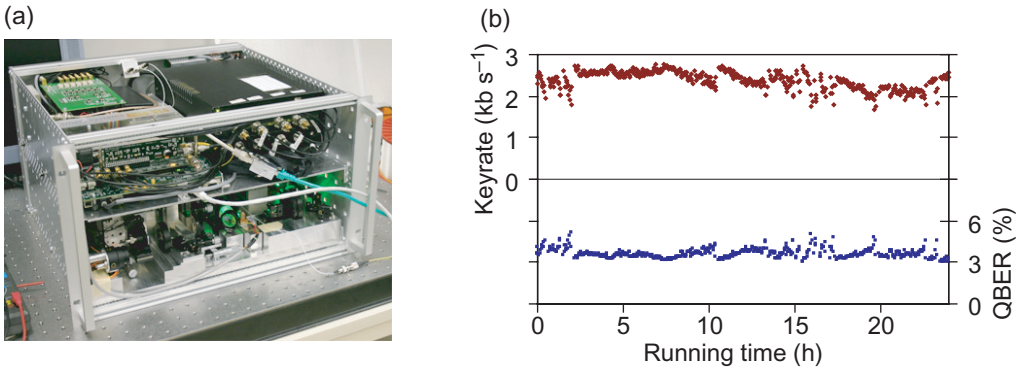

Figure 13. (a) The Alice unit of the Ent QKD system in its compact casing. (b) A typical 24 h plot of the secure keyrate and QBER measured over a 16 km fiber in the SECOQC network.

During the SECOQC network demonstration the source at Alice was operated with 6 mW pump power, yielding a local detection rate of 750 kHz at the Si-APDs. Using a 16 km long fiber between the nodes ERD and SIE, the detected coincidence rate at Bob was 8 kHz. The measured QBER for the link was 3.5% throughout the whole demonstration, as seen in figure 13(b). In this figure, the resulting secure key rate of 2.5 kbit s^{-1} is also plotted over 24 h. The system operated far longer than this period and provided a reliable key rate (> 2 kbit s^{-1}) during the whole SECOQC demonstration [13]. In terms of entanglement distribution, the system achieved an average polarization visibility of 93%. Throughout the complete prototype operation the visibility was higher than 90% for 99.9% of the active time.

The QKD device, as presented for the SECOQC network demonstration, is the first Ent system that can offer long-term operation without user intervention. It displays the maturity reached by two-photon entanglement distribution systems, with stability obtained by automatic correction of the effects of environmental changes affecting the deployed fiber link and the device. The high purity of the shared entangled state allows the device to efficiently extract a secure key from the measured correlations.

3.5. CV QKD with coherent states

The CV system developed in a collaboration between Laboratoire Charles Fabry de l'Institut d'Optique, THALES Research and Technology France and Université Libre de Bruxelles implements a coherent-state reverse-reconciliated QKD protocol [16, 50]. In this protocol, the key information is encoded on both quadratures of a coherent state of the electromagnetic field, which Bob measures with a homodyne detection that uses standard PIN photodiodes. The system is stable and automatic, and has demonstrated continuous operation during 57 h, yielding an average secret key distribution rate of 8 kbits s^{-1} over a 6.2 km standard optical fiber (this fiber has an attenuation of approx. 2.8 dB; the length of an equivalent fiber with a loss of 0.2 dB km^{-1} would be 14 km), including all quantum and classical communication.

3.5.1. Implementation of the CV QKD protocol. As presented in detail in [16, 51], Alice uses a pulsed 1550 nm telecom laser diode to generate coherent light pulses with a duration of 100 ns and a repetition rate of 500 kHz (see figure 14). The pulses are separated into a weak signal and a strong local oscillator (LO) using a 99/1 asymmetric coupler. The signal is then randomly modulated, using amplitude and phase modulators, following a centered Gaussian distribution in both quadratures $\hat{x} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a})$ and $\hat{p} = \frac{\mathrm{i}}{\sqrt{2}}(\hat{a}^\dagger - \hat{a})$, so that the variance of the Gaussian distribution reaches a target value of $V_A N_0$. In these expressions, $\hat{a}$ and $\hat{a}^\dagger$ are, respectively, the bosonic annihilation and creation operators of the electromagnetic field, and N_0 is the shot-noise variance that appears in the Heisenberg relation $\Delta x \Delta p \geqslant N_0$.

Time and polarization multiplexing are used so that the signal and LO are transmitted to Bob in the same optical fiber without any cross-talk. First, the signal is delayed by 400 ns using a 2×40 m delay line, in which the pulse is reflected by a Faraday mirror, as shown in figure 14. This system imposes a $\pi/2$ polarization rotation to the pulse when it is reflected, and thus compensates all the polarization drifts undergone by the signal. The LO is then coupled with the signal in the transmission fiber, using a polarization beamsplitter (PBS). Thanks to this double multiplexing, the two pulses can be separated at Bob's site very efficiently and with minimal losses, by using a simple PBS and delaying the LO after the separation.

Finally, in Bob's system, the signal and LO interfere in a pulsed, shot-noise limited homodyne detector. This detection system outputs an electric signal, whose intensity is

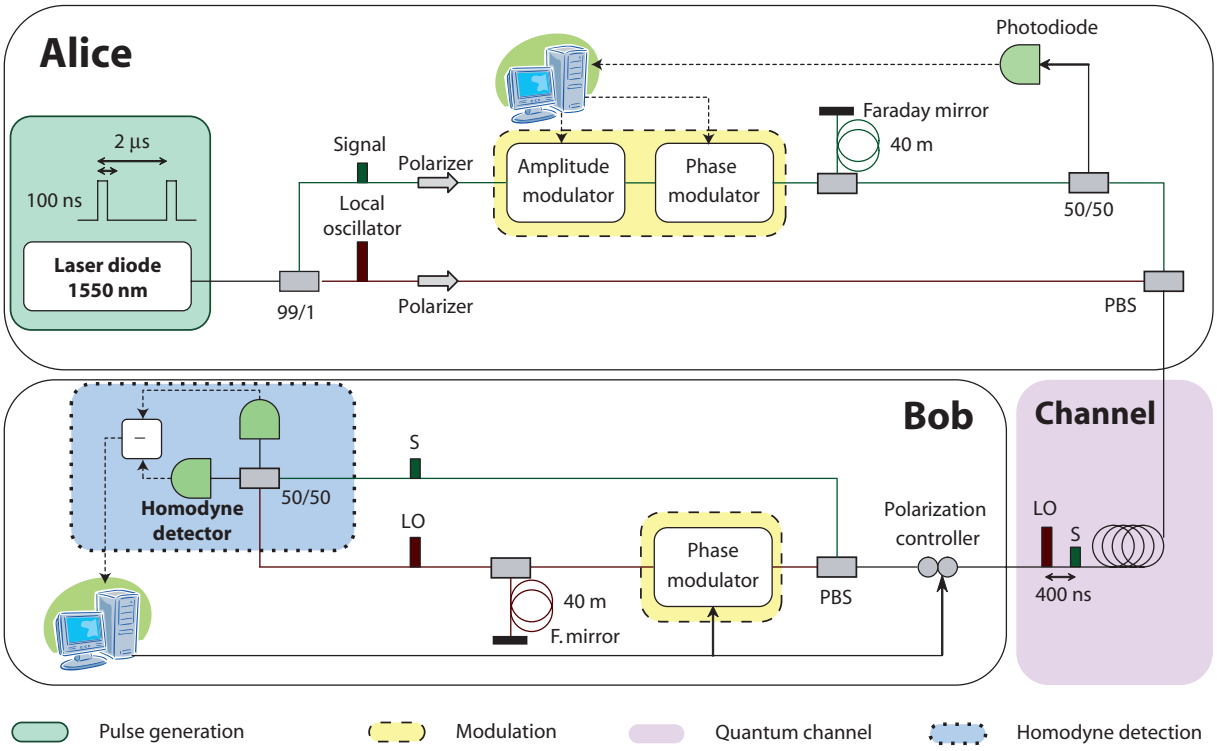

Figure 14. Optical layout of the CV QKD prototype.

proportional to the quadrature $\hat{x}_\phi$ of the signal, where ϕ is the phase difference between the signal and the LO. Following the implemented protocol, Bob measures randomly either $\hat{x}_0$ or $\hat{x}_{\pi/2}$ to select one of the two quadratures. For this purpose, he imposes randomly a $\pi/2$ phase shift to the local oscillator using a phase modulator placed in the LO path.

3.5.2. Classical processing of the information. After the quantum transmission, Alice and Bob share continuous correlated data, affected by a noise $N \geqslant N_0$, where N_0 is the shot-noise variance. The parameters of the transmission are then evaluated by comparing a random sample of the distribution. In particular, the shot-noise level, the noise due to the losses and the excess noise have to be determined precisely, since they intervene in the calculation of the secret information available in the shared data. In order to extract a secret key, Alice and Bob need to apply sophisticated error–correction algorithms on their data, based on low-density parity-check codes, followed by the application of a privacy amplification scheme to the quantized data. The efficiency of these classical algorithms is critical for CV protocols, since it is the main cause of limitation in terms of distance and rate.

3.5.3. System performances and results. The system is first calibrated in the laboratory yielding a transmission efficiency $\eta = 0.6$ and an electronic noise $v_{\mathrm{el}}N_0 = 0.01N_0$ for Bob's apparatus. In laboratory conditions, the measured excess noise is typically $0 \leqslant \varepsilon N_0 < 0.01N_0$. After the calibration procedure, the setups of Alice and Bob are placed at each side of a preinstalled optical fiber featuring a transmission efficiency $T = 0.51$. The measured excess noise is typically of $0.04N_0$, mainly due to vibrations in the system. With those parameters,

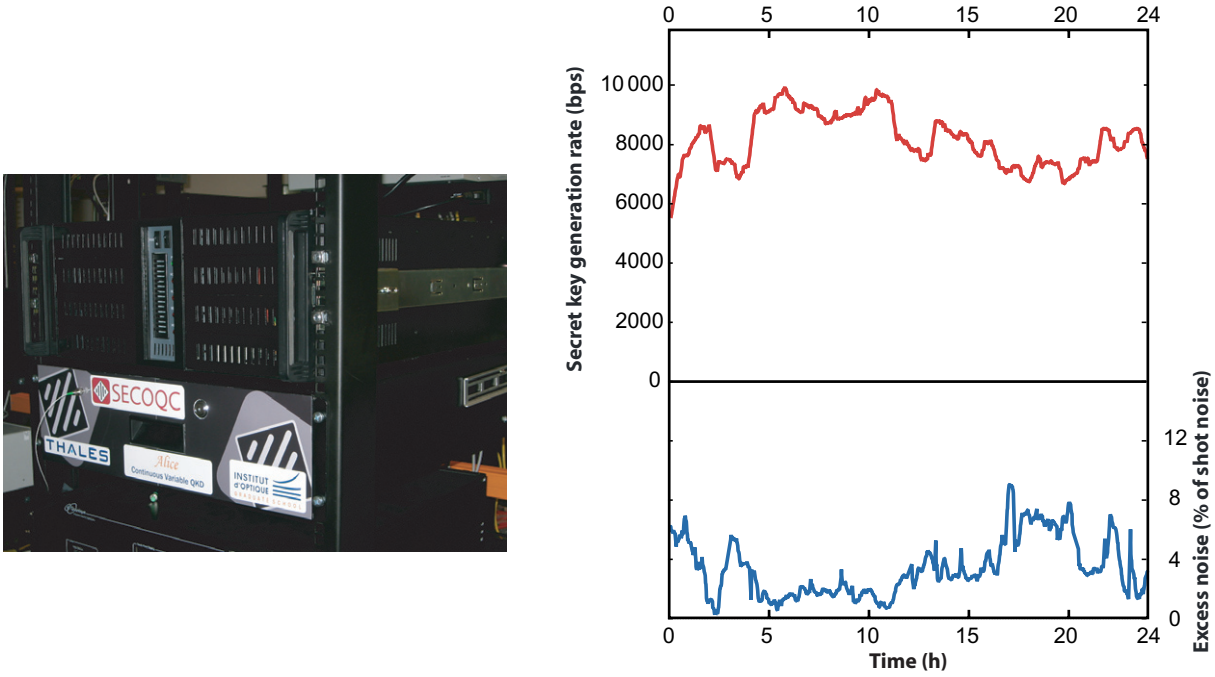

Figure 15. Left: prototype of the CV QKD system (Alice's part) installed in the GUD node rack. Right: secret key generation rate, and measured excess noise, over 24 h of the SECOQC conference.

the reconciliation efficiency is optimized at $\beta = 0.9$. In the current implementation, blocks of 2 million pulses are used for each key generation. The amplitude and phase (coded on 16 bits) of 1 million of them are sent for the channel evaluation, and the remaining 1 million are the material used for the key generation. With the parameters given above, the final key size is typically of the order of 150 000 bits, for a total processing time of 20 s. Therefore, we have measured an average secret key rate of 8 kbits s^{-1} (figure 15) during 57 h of uninterrupted operation with peak values up to 10 kbits s^{-1}. In practice, as shown by the SECOQC field demonstration, CV protocols allow for very high key generation rates at operational distances (10–20 km), which makes them very efficient for implementations in metropolitan-sized networks.

3.6. Free-space (FS) QKD

The FS QKD system, developed at the University of Munich employs the BB84 protocol with decoy states [41, 46, 52] using polarization encoded attenuated laser pulses with a wavelength of 850 nm. The system can be operated during night and day, using excessive filtering in order to suppress background light. The transmitter (Alice) uses laser diodes for the generation of random sequences of WCPs of different polarization and mean photon number. In the installation at the Siemens premises in Vienna, the photons pass a FS quantum channel with a distance of 80 m (figure 16).

In the transmitter unit (figure 17), the pulses of eight laser diodes are combined, using a custom design of conical and pyramidal mirrors, into a spatial filter, which is realized by a single-mode fiber. The diodes are driven according to the random choices of basis, bit and decoy values to produce WCPs of polarized light (polarization: H, V, +45°, −45°) with mean

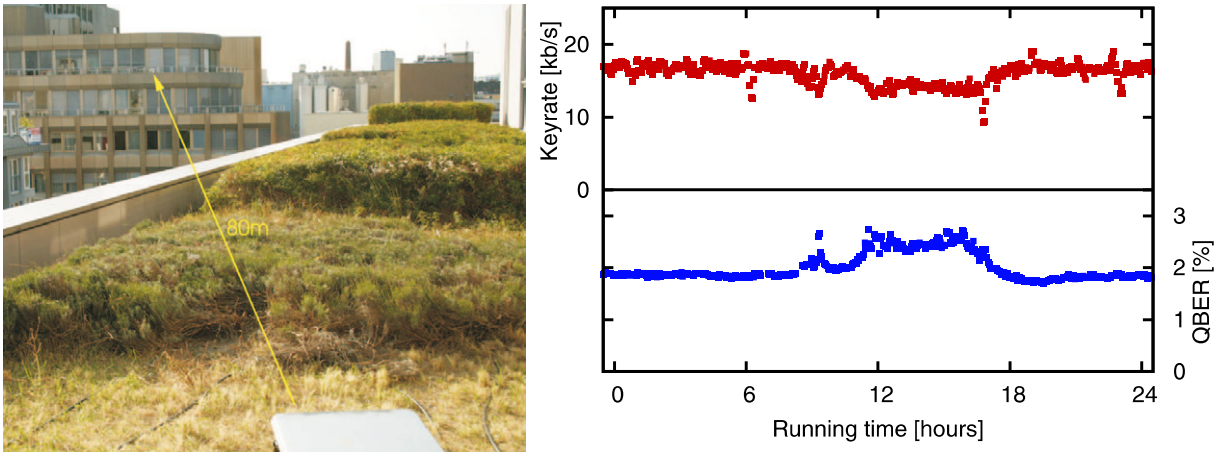

Figure 16. Left: view from the FS transmitter to the receiver installed on the building across the street. Secret key was established between these to sites via the freespace QKD system over a distance of 80 m. Right: a typical 24 h plot of secret bit rate and QBER as measured in the SECOQC prototype

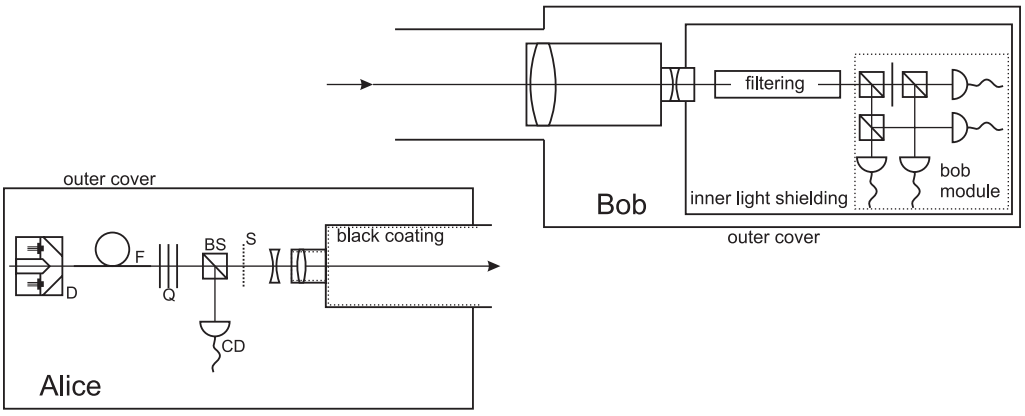

Figure 17. Simplified diagram of the free-space Alice and Bob setup: D: cube, housing the laserdiodes, F: fiber modefilter, Q: quarter- and half-wave plates for polarization compensation of the fiber, BS: beamsplitter, CD: detector for calibration of mean photon numbers, S: shutter to prevent daylight coming in when calibrating the mean photon numbers. The polarization analyzing unit (Bob module) as described in [17]. The front lens of the Alice telescope is protected from sunlight by a 25 cm long black coated tube. Therefore the receiver collects less stray light.

photon number of $\mu = 0.3$ or 0.35, respectively. The advantage of this method is that no active manipulation is needed for the polarization nor for the different values of μ. The cube, housing the laser diodes, can be seen on the left side of figure 17. A single-photon detector is mounted in the reflective output of a beamsplitter and enables the calibration of the specific μ for each of the eight diodes. The attenuated pulses are fed into the telescope, which together with Bob's telescope establishes the quantum channel. The acceptance angle of the receiver's telescope is

limited by spatial filtering to less than 200 μrad. Therefore, the area the receiver can detect photons from, is smaller than the exit lens of the sender's telescope (25 mm) and well shielded from daylight by black coated tubes. Both telescopes are constantly realigned to each other automatically. Otherwise the channel transmittivity would decrease on short timescales to only a small fraction. The remaining coupling, however, is nearly always enough to restart the system without manual interaction—even after a shutdown for several days.

The receiver unit (Bob's setup, right side of figure 17) houses a light-tight box, which is directly attached to the telescope, and which includes the optics for the spatial filtering. Thereafter, in the actual Bob module, a non polarizing BS, a set of two PBSs and a HWP are used to perform the polarization analysis of the incoming photons. Detection behind the 50/50 BS selects the basis (H/V or $\pm 45^{\circ}$) randomly. The photons are detected by four silicon APDs and registered by a timestamp unit that records the time-of-arrival of each detection event (timing resolution better than 0.5 ns) and feeds this data into a computer for further processing.

The necessary synchronization is done on the weak pulse signal itself. Techniques such as fast Fourier transform are used to recover both the 10 MHz beat and the absolute start time using the signals from pseudo random sequences in additional frame headers. Once the synchronization task is finished, Alice and Bob can start the key sifting process used for error analysis and correction, followed by the privacy amplification step. The CASCADE algorithm is used subsequently [53].

During the testing period, a sifted key of about 50 kbit s^{-1} (QBER = 2.3%) and a secure key of up to 17 kbit s^{-1} could be achieved. Unfortunately there have been unexpected fluctuations in the decoy parameter Δ, which are not yet fully understood, but which most likely occurred due to temperature changes during the operation. In these cases, the decoy parameter Δ thus had to be fixed to a reasonable value without the option to recognize PNS attacks.

During the test period between September 25 and October 27, the link operated well in quite different weather conditions. Only fog, very heavy rain (or, possibly, snowfall) limits the transmission severely as do strong turbulences above sun-heated roofs close to the optical path.

4. The SECOQC node module

In this section, we describe the architecture of the SECOQC network node module and its basic functional elements. The principal design of the node module was carried out by the AIT Austrian Institute of Technology (formerly ARC[21]) in close collaboration with groups from University of Aarhus, Telecom ParisTech, University of Erlangen-Nuremberg, Bearing Point Infonova and Siemens Austria. The technical design and implementation of the module software was realized by a dedicated team from the AIT.

In what follows, we first of all give an account of the basic building blocks of the node module. As already discussed in section 2, in the SECOQC approach, the main objectives of a node module are threefold:

1. 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 ITS communication connectivity to all nodes in the network associated with the node by direct QKD links;

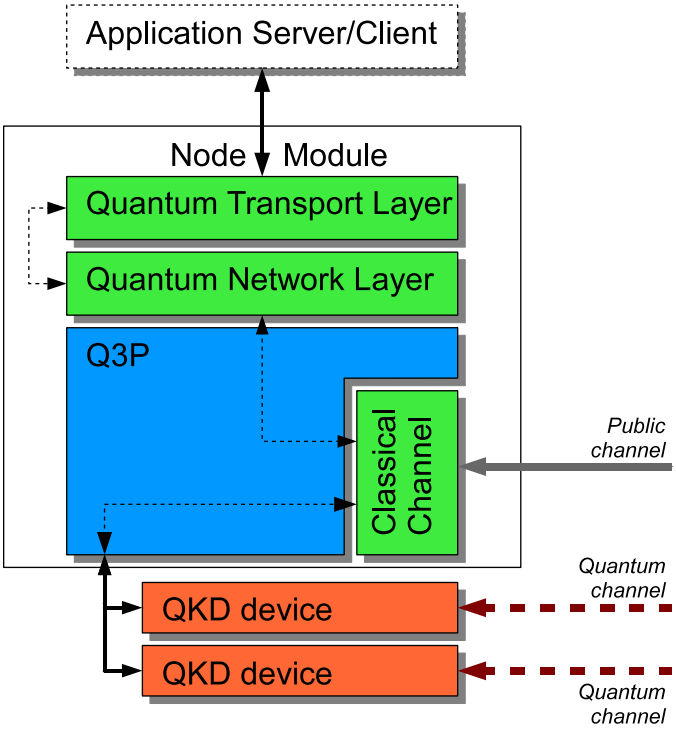

Figure 18. Design of the node module.

2. 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; and
3. to ensure an end-to-end transport of secret key material along this path using the hop-by-hop transport mechanism outlined in section 2.

These three distinct types of functionalities (or services) can be grouped in network layers: a quantum point-to-point (Q3P) layer, a quantum network layer and a quantum transport layer [24]. A schematic representation of the node module design is given in figure 18.

4.1. Quantum point-to-point protocol—Q3P

The interface between the QKD device(s) and the node module on one side as well as between a pair of node modules is realized by the *quantum point-to-point protocol—Q3P*. The node module sets up a Q3P connection to each node associated with it by a QKD link and thus initiates Q3P links. A Q3P link realizes a context-dependent ITS communication channel. That is, depending on a header attached to the transmitted messages, it switches between different modes: (i) one-time pad encrypted and ITS authenticated communication, (ii) non-encrypted but ITS authenticated communication or (iii) non-encrypted and non-authenticated communication. To carry out this functionality each Q3P link maintains two functional entities: a *key store* (managing the key material), and a *crypto engine* (performing the crypto operations using key material from the key store), which are discussed below.

The Q3P protocol also maintains a communication line with the underlying QKD device corresponding to each Q3P link in the node. It takes care of transmitting transparently the QKD protocol messages between the peer QKD devices over the Q3P link, applying the security level,

which is explicitly set in the QKD protocol communication calls. Additionally, Q3P accepts the key material that is pushed up by the QKD device and also passes over to it general node management commands.

This design strictly separates key production from key usage. As Q3P manages the communication to the peer nodes and establishes the device-to-device classical communication channel, the QKD devices are exempted from any classical networking configuration maintenance and focus on performing the key distillation process alone.

4.1.1. The key store. The central element of this approach is the key store. The key store itself is organized in several levels:

- *Pickup store*: More then one pair of QKD devices can be attached to a single Q3P link. Every QKD device is now associated with a pickup store to which it pushes the generated keys. There are no restrictions neither in size nor in time on the devices. However, finite size considerations related to privacy amplification [4] indicate that reasonably large chunks of key materials are to be expected.
  Note that the presence of key material in the pickup store has not yet been confirmed by the peer Q3P instance. Every chunk of key material has an unique identifier issued by the underlying QKD device. Using this identifier the peer key stores can perform a negotiation. A Q3P subprotocol is run, which ensures synchronous key presence on both sides. Once this protocol terminates successfully, the key material is moved to the common store.
- *Common store*: There is only one single common store for the Q3P link, where all keys created by all QKD devices on the very same Q3P link are collected. Here, key boundaries as present in the pickup stores are disbanded and all chunks form a homogeneous mass of key bits. The common store is persistent and will be available after system reboot.
- *In/out buffers*: As the communication over a Q3P link is bidirectional, pieces of key material have to be withdrawn from the common store to be dedicated for inbound or outbound communication. To prevent race conditions each key store participating on a Q3P link has one of two preselected roles—that of a *master* or of a *slave*. The master key store decides which concrete key material is to be withdrawn from the common store. The in/out buffers are crosswise interconnected. Once key material has been successfully used it is shredded and no longer available.

The key store architecture is schematically presented in figure 19.

Accompanying this design is a *crypto engine*. This instance serves as a container of algorithms for encryption and authentication techniques. After a successful application of a function of the crypto engine the corresponding key material is destroyed as outlined above. There is no other entity outside of Q3P having access to any key material from the key store. That is: Q3P solely uses QKD generated keys for providing an ITS communication primitive between two nodes. No secret ever leaves the node module but any message can be transmitted over the Q3P link, with the desired degree of security.

4.2. QKD-network layer protocol—QKD-NL (routing)

Q3P is capable of enclosing any higher layer protocol. For example running IPv4 or IPv6 over Q3P for routing purposes appears straight-forward. However, using traditional IPv4 or IPv6 [54, 55] over Q3P is suboptimal. To this end the SECOQC project defined the QKD-network

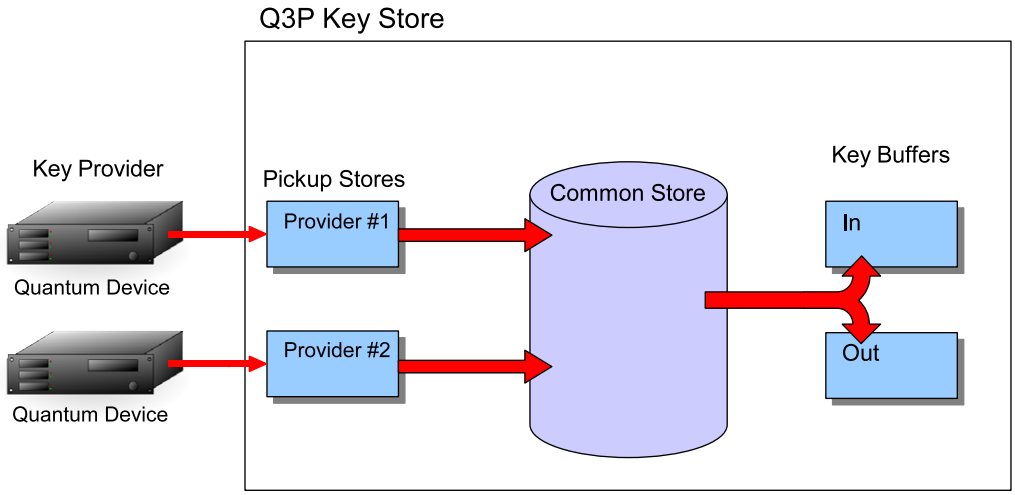

Figure 19. Architecture of the key store. Two QKD devices serving the same Q3P link are connected.

layer protocol, or QKD-NL [24], which is especially designed to take care of economic and careful utilization of the underlying key material.

Based on OSPF [56] 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.

4.3. QKD-transport layer protocol—QKD-TL

Finalizing the SECOQC protocol stack is the QKD transport layer protocol, or QKD-TL, which is responsible for transport over Q3P [24]. QKD-TL realizes an end-to-end transport between non-adjacent peers in the SECOQC QKD network. This is done by using the hop-by-hop encryption/decryption mechanism described in section 2: in each node an incoming message is decrypted and authenticated, and then encrypted and supplied with an authentication tag for dispatch to the next node along the hop-by-hop path. This is achieved by pulling an incoming message from a Q3P-link, examining its destination network address and pushing the message on the proper Q3P-link along the route.

Derived from TCP/IP [57], 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 signaling mechanism, triggered by key store shortages within the intermediate nodes.

QKD-TL also specifies an end-to-end key exchange subprotocol, which enables entities (applications users, etc) securely connected to some ingress (entering) QKD node[26] to share

[26] Here we implicitly assume that each QKD network node is situated within a secure local area network in which different application and client servers operate. Naturally, these servers could be just computers situated in the secure premises of the QKD node, as was the case with the SECOQC prototype.

an arbitrary number of secret bits with entities securely connected to any other egress node. QKD-TL has been designed with a client–server model in mind. Application servers register themselves to a QKD node to which they are securely connected. Respectively, clients desiring to share keys with this application server request QKD-TL connections to it over a QKD node they are securely connected to. As soon as a QKD-TL connection is established, one QKD node picks up a string of random numbers and transmits these across the QKD network to the peer QKD node. On receipt these values are handed out to the participating client and server, which in turn treat these values as random keys.

Each pay-load communication inside the QKD network is routed on the basis of the information provided by QKD-NL. Every QKD-TL packet is enclosed by Q3P and dispatched using the ITS hop-by-hop mechanism discussed above, generating a constant stream of secret bits between a client and a server for any application purpose.

It should be stressed that the secure communication between the client and server by means of the key distributed over the QKD network can use any communication channel of (generally any type of) a secure communication infrastructure. The only objective of the QKD network is key distribution between the secure locations of the network.

This approach effectively defines three separate network planes, a quantum plane (quantum channels and QKD devices which push key to the node-modules), secret's plane (node-modules and classical communication channels between them with three logical layers Q3P, network layer, transport layer, which utilize the QKD generated key to distribute information-theoretically secure key between any two nodes on the network), and data plane (in which the distributed key is utilized by a secure communication infrastructure to ensure end-to-end network secure communication).

5. The quantum network in Vienna—prototype operation and transmission capacity

5.1. Prototype operation in typical regimes

The primary objective of a QKD network is key distribution. Therefore its performance potential is given by the state of the network's key stores, their dynamics and interdependencies. As discussed above, each node carries as many key stores as is the number of Q3P links connected to it, whereby the two nodes on both sides of the same Q3P link carry one key store copy out of an identical pair. The state of a key store is given by the amount of key material it contains, as function of time, which in turn depends on two independent factors: the key generation rate of the underlying QKD devices and the key consumption rate by the pay-load applications. While key generation is link-specific and does not depend on the activities of the remaining links, key consumption is highly agile and is determined by the needs of the pay-load applications. Which key stores are affected is dependent on routing, the latter in turn being a function of the network topology and the state of the separate link key stores along the possible routes. Obviously, the overall system of key stores is a highly dynamic and distributed one. It is therefore difficult to determine a clear cut characteristic network behavior as is always the case with systems driven by multiagent interoperation.

For this reason here we make an attempt to demonstrate different essentials in the SECOQC prototype network operation, by starting from simple scenarios, trying to pin-point typical performance of key store pairs and then proceed to discuss collective dynamics of nodes in a nontrivial communication pattern.

It should be underlined that these examples serve actually as an illustration of the types of studies of QKD network performance that appear reasonable to be carried out. Certainly future research in this direction would have to borrow from approaches and methods from classical communication networks that have a long tradition in this domain.

We base our analysis on recorded data of approximately one month of the SECOQC prototype operation, taken in the period between the end of September and end of October 2008.

Before we proceed we note that the term 'key material amount in a key store' requires specification, due to the multilevel anatomy of the key store discussed above. In order to gain a more integral perspective we ignore the dynamic interplay between the pick-up store, the common store and the in/out buffers and consider only the total key in the key store, which is the sum of the key material that is saved as a function of time in each of these entities. Note that in the following, we use the binary prefixes Ki for 2^{10}, and Mi for 2^{20} (as defined in IEC 60027-2), i.e. 1 KiB (kibibyte) is equal to 1024 bytes, 1 MiB (mebibyte) is equal to 1048 576 bytes.

5.1.1. Simple key store behavior. Obviously the simplest key store dynamics is the one that corresponds to a link that is generating key but no key consumption takes place. Naively this key amount in the key store would linearly increase, provided the underlying key generation rate would be constant. In fact, the real key generation process is discrete as the QKD key distillation protocol processes blocks of raw key material, to produce secure key, which are then pushed to the key stores. Simultaneously, even pure generation is accompanied by key consumption, due to the authentication of the QKD protocol communication, carried out by Q3P. This process is illustrated in the left part of figure 20, which shows a phase when two nodes (BRT and SIE) are accumulating shared key. In the time interval shown key material is not consumed by any application. Thus the key store content is (nearly) monotonically increasing. The inset that shows a close-up of the time interval between two consecutive key pushes reveals that actually small portions (each of size 96 bytes) of the previously generated key are used for authenticating the classical channel. The communication being authenticated is related to the QKD protocol, i.e. sifting, error correction, key confirmation and privacy amplification. It should be mentioned that communication authentication is not instantaneous as the Q3P approach is based on delayed authentication, taking place before a distilled key is declared 'secure' by the QKD link.

Another simple key store dynamics occurs when the QKD link does not generate a key but a pay-load application consumes a key. It should be stressed that application development was not a task of the SECOQC project. In order to be able to observe and demonstrate some nontrivial network operation, however, we needed to have applications running on top of the QKD network. For this purpose, we have adopted a number of standard communication utilities such as IP telephony and IP-based video-conferencing, whereby their end-to-end security is guaranteed by a virtual private network (VPN) tunnel, acting in two different realizations. The basic construct is a *one-time pad* tunnel with ITS authentication between two application/client servers running on PCs, directly connected to corresponding node modules. We either send pay-load data directly over the OTP tunnel, in which case an ITS transmission security is guaranteed, or use a standard IPsec tunnel based on AES encryption and authentication, with frequent key exchange. In the latter case, the standard Diffie–Hellman key exchange is tunneled through the OTP tunnel. The latter procedure is equivalent to the conceptually more straight forward but technically less trivial replacement of the Diffie–Hellmann key exchange with a key, directly provided by the QKD-TL layer of the quantum network. The following figures illustrate the two different modes of key consumption in the absence of key generation.

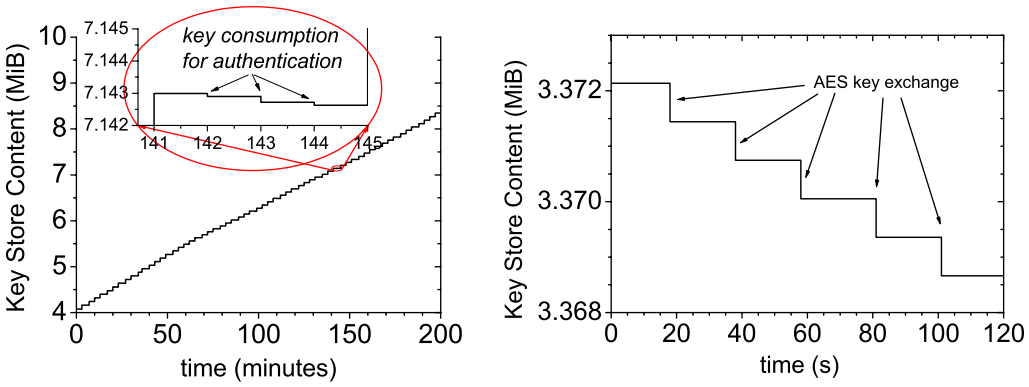

Figure 20. Left: key *generation* between the nodes BRT and SIE as a function of time (here, this link is *not* using keys for encryption of messages). The small steps up correspond to individual key pushes. The inset shows a close-up of the time interval between two consecutive key pushes. During this time the link consumes previously produced key for the authentication of the classical channel. Right: key *consumption* between ERD and GUD as a function of time. A virtual transmission channel, which is AES encrypted, is created. This encrypted channel can be used for example to transmit a video stream. For clarity the link has been put into non-key-generating mode so that it is *not* creating keys during this phase. The steps down demonstrate that the AES key is changed every 20 s.

The right part of figure 20 shows the link between ERD and GUD when it is only consuming previously generated key for the encryption of a VPN with AES. The steps down (each of size 728 bytes) correspond to individual changes of the AES-key every 20 s[27]. In this case the consumed key rate is approximately 36 bytes s^{-1} and does not depend on the actual size of the plaintext message that is to be encrypted.

Figure 21 depicts the consumption of key material from the key store by an application that uses the OTP tunnel. Clearly, for the information-theoretical secure encryption with a one-time pad, the amount of consumed key is of the same size as the plain text message to be encrypted. For the time shown the QKD device is not generating keys. In the left part of figure 21, the key store content decreases as several key blocks are withdrawn from the key store for OTP encryption. The right part of the figure demonstrates the effect of reporting the key usage rate as a moving average over 1 min (the standard reporting mechanism implemented in the prototype). Only during the decrease of the key store content key is actually consumed. However, due to the moving average key usage is not reported until 1 min later.

5.1.2. Traffic rerouting under heavy communication load. Here, we discuss the complex behavior of the QKD network during a network rerouting test (cf figure 2 for the network topology). The goal has been to study the network reaction to heavy communication load when individual links experience key material shortages. The network dynamics in this case is illustrated in figure 22.

[27] The IPsec tunnel needs two portions of 256 bits on both sides in each exchange round. The remaining bits are OTP tunnel authentication overhead.

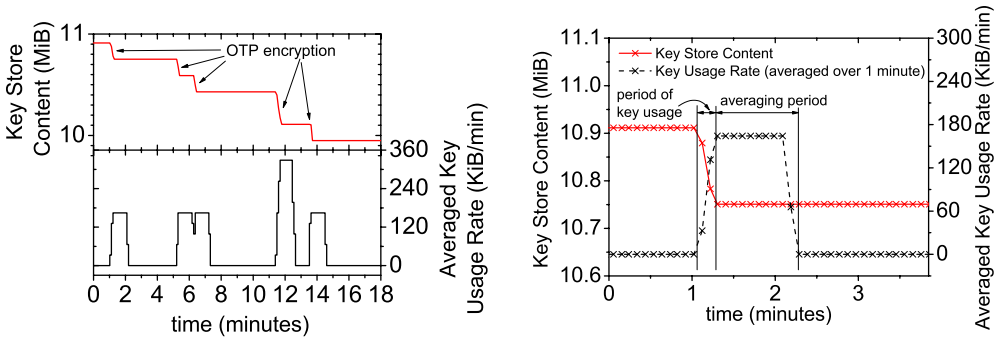

Figure 21. The key store content and the averaged key usage rate versus time of the link between ERD and BRT that provides several keys to an application that encrypts messages via *one-time pad*. The link between is *not* creating keys during this phase. Left: medium time range. Right: close-up demonstrating that the moving average of the key usage rate actually shows the key usage delayed.

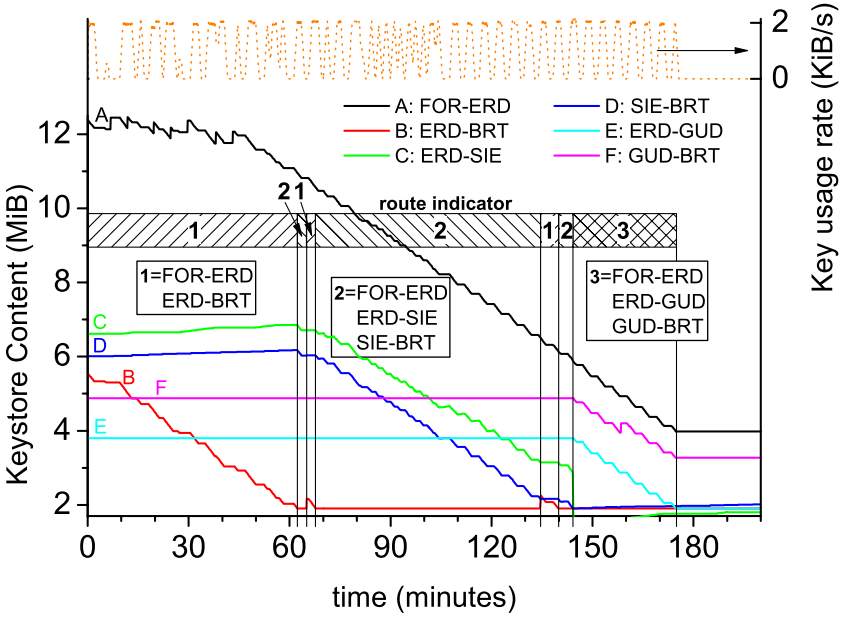

Figure 22. An experiment demonstrating routing in the QKD network. The key store contents of the individual links and the key usage rate are plotted as a function of time. A shared secret key is consumed between node FOR and node BRT. After turning some QKD devices off, an application that consumes a relatively high (approximately $1\,\mathrm{KiB\,s^{-1}} = 8192\,\mathrm{bit\,s^{-1}}$) amount of key over a longer period is started. The link between FOR and ERD is used all the time. Between ERD and BRT first the direct link is used. It reaches its minimum key threshold after approximately one hour and the route FOR–ERD–SIE–BRT takes over. Approximately one and a half hours later, this route reaches its minimum key threshold, and FOR–ERD–GUD–BRT takes over for the next half an hour. More details are explained in the text.

The experiment is set up to generate a shared secret between the nodes FOR and BRT. *A priori* five possible routes between nodes FOR and BRT can be followed (see section 5.2 below) but three of these are effectively operative in the experiment: **1** FOR–ERD–BRT, **2** FOR–ERD–SIE–BRT and **3** FOR–ERD–GUD–BRT. The link FOR–ERD starts with a key store content of approximately 12 MiB and provides key material throughout the experiment. During the first 45 min the generation rate equals the consumption rate so that the key store content of this link remains approximately constant. Then key generation is turned off and the key store content shrinks monotonically. Initially route **1** with the direct link between ERD and BRT is used. This link starts with a key store content of approximately 5.5 MiB of which approximately 3.5 MiB are consumed over the next hour until the link reaches the minimum key store content threshold of 2 MiB. As a consequence the link ERD–BRT stops delivering key for the moment. (The minimum threshold is set to ensure that (in any practical case) enough key remains in the store to authenticate the future communication on the classical channel during further key generation.)

When ERD–BRT ceases to transport key, route **2** FOR–ERD–SIE–BRT steps in (for approximately 2 min route **1** recovers, when fresh key is added to the key store of ERD–BRT). The links ERD–SIE and SIE–BRT are generating key throughout the experiment (ERD–SIE and SIE–BRT start with key store contents of approximately 6.6 and 6 MiB, respectively). The key generation rate of ERD–SIE is slightly above the rate of SIE–BRT. Nevertheless, the application consumes more than is being generated and the key store content shrinks. 134 min after the start of the experiment route **1** recovers again for a short time when fresh key is added to the ERD–BRT key store. At minute 144 the SIE–BRT link reaches its minimum threshold and stops delivering key. Due to a bug in the routing algorithm the link ERD–SIE then starts to consume key at a very high rate (vertical line) and stops operating until the threshold is reached again due to key generation. The link SIE–BRT continues to generate key.

The third route **3** FOR–ERD–GUD–BRT now takes over. The links ERD–GUD and GUD–BRT start with approximately 3.8 and 4.9 MiB key store content and are not generating key during the experiment (except that GUD–BRT pushes one key at minute 159). After about another half an hour (in minute 175) the ERD–GUD link reaches the minimum threshold and stops delivering keys. From this moment on there is no possible route between FOR and BRT.

The experiment clearly demonstrates the functionality of the network in highly unfavorable regimes—low key generation, some links deliberately do not operate or are even stopped during the test. It is obvious that the prototype exhibits a high degree of robustness—i.e. it has the ability to deliver key (ensure end-to-end secure pay load communication) even in the case of a multiple link failure and/or impossibility of separate links to cope individually with the load. Additionally, and independently of the practically relevant implications, the graphs of the key store content allow us to study the complex pattern of simultaneous key generation and key consumption, at different relative rates for the different involved links. These patterns can readily be interpreted in terms of the simple key store 'evolution mechanisms' discussed above.

5.2. Maximal secret transmission capacity of the SECOQC network

The simple routing mechanism, presented in the previous section, raises a more important question: what is the maximal transmission capacity between two nodes and how to find optimal (routing) strategies that allow achieving this maximum?

We want to determine the maximum shared key length (or equivalently, the maximum shared key generation rate) between any two nodes, if the complete network is only dedicated

Table 1. Non-cyclic paths between node s and t in our network graph.

Path index	Nodes	Generated key
1	$s \sim t$	$p_1(s,t) = c(s,t)$
2	$s \sim u \sim t$	$p_2(s,t) = \min[c(s,u), c(u,t)]$
3	$s \sim v \sim t$	$p_3(s,t) = \min[c(s,v), c(v,t)]$
4	$s \sim u \sim v \sim t$	$p_4(s,t) = \max[0, \min[c(s,u) - c(u,t), c(u,v), c(v,t) - c(s,v)]]$
5	$s \sim v \sim u \sim t$	$p_5(s,t) = \max[0, \min[c(s,v) - c(v,t), c(u,v), c(u,t) - c(s,u)]]$

to that task. Using OTP, this maximum shared key length is equal to the maximum length of a message that can be exchanged with information-theoretic security (in either of the two directions) between those two nodes. In this sense, we can view this quantity as a maximal secret transmission capacity.

In general, to answer this question, one can employ methods from graph theory. There this problem is known as the *maximum flow problem*, some times also called maximum s–t flow problem (where s and t denote source and sink, respectively). Most of the literature available is dedicated to this problem for directed graphs [58]–[61] but there has been some progress for undirected graphs [62] as well. For general graphs this problem is complex. However, the SECOQC network topology allows the solution to be presented in a simple form, which can be intuitively understood.

Here, we consider only the fully connected part of the SECOQC network graph consisting of the four nodes BRT (n_2), SIE (n_3), ERD (n_4), and GUD (n_5) and the connecting links. The two nodes that should generate the shared key of maximum possible length are called s and t ($s \neq t$; $s, t \in \{n_2, n_3, n_4, n_5\}$). The remaining two nodes are called u and v. Each link $\{n_i, n_j\}$ corresponds to the key generated over this link, the length of which is $c(n_i, n_j)$.

In this graph, the maximum length of the shared key between s and t, $f(s,t)$ can be easily calculated by considering all five non-cyclic paths between s and t. The generated key through path i is denoted p_i.

Basically, we obtain the maximal secret transmission capacity by following the classical Ford–Fulkerson algorithm [59]. Path 1 is the direct edge (link) $s \sim t$, which of course can be fully exploited. Paths 2 and 3 include only one intermediate node, u and v, respectively. Paths 1–3 are completely independent, that is they include no common links. Obviously, these three paths can be maximally utilized. If $c(s,u) > c(u,t)$ and $c(v,t) > c(s,v)$ then path 4 can be exploited in addition to paths 1–3. If $c(s,v) > c(v,t)$ and $c(u,t) > c(s,u)$ then path 5 can be exploited in addition to paths 1–3. At any given time generation of key via path 4 and path 5 is mutually exclusive.

Finally[28], $f(s,t) = \sum_{i=1}^{5} p_i(s,t)$.

Figure 23 shows the maximum length of the shared key between nodes BRT (n_2) and GUD (n_5), and SIE (n_3) and ERD (n_4), respectively, and the contributions of the separate paths as indicated in table 1 above. Obviously, the point-to-point secret transmission capacity is substantially improved compared with that of the direct point-to-point link through exploiting the capacities of the other connecting paths. The redundancy of the network ensures an almost linear growth of the available key in spite of temporary shutdowns of individual links.

[28] By construction of paths 4 and 5, it can be seen that an augmenting path does not exist in the residual network, which shows that the maximal secret transmission capacity has been reached [59].

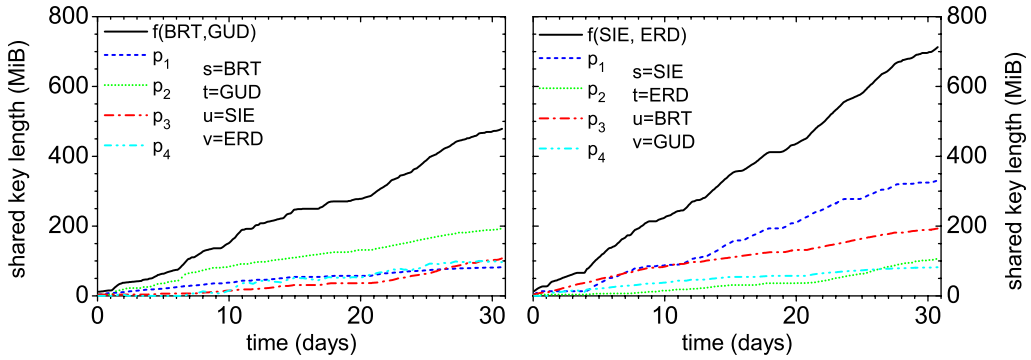

Figure 23. Left: maximum length of the shared key between nodes BRT (n_2) and GUD (n_5) (solid) and corresponding shared key generation along individual paths (dashed/dotted), all as functions of time. Right: same for nodes SIE (n_3) and ERD (n_4). For the meaning of s, t, u, v and therefore p_1, p_2, p_3, p_4 see text and table 1.

Incidentally, in both examples the link capacities led to the exclusion of path 5 throughout the experiment. Additionally, path 4 is not continuously contributing to the maximum transmission capacity. In the left part of figure 23, there are two periods of inactivity of path 4, whereas in the right part there is only one such period lasting approximately one day from the start of the experiment.

The above analysis does not aim to be comprehensive in any form, but just to give additional insights into the added value provided by the network in comparison to stand-alone QKD links.

6. Conclusions

In this publication, we have comprehensively described the SECOQC prototype QKD network.

We have given a detailed analysis of the trusted repeater paradigm and have discussed the SECOQC approach to architectures for QKD networks of this type. We have put forward, for the first time, a systematic design that allows unrestricted scalability and interoperability of arbitrary QKD technologies.

The general architecture principles are embodied in the first highly integrated QKD network prototype, including five types of innovative QKD systems constituting eight different links. We have given an overview of each of these systems, referring the reader to dedicated publications on the separate technologies. Overall, in addition to improved performance and high degree of technologic stability and robustness, all QKD devices in the prototype seamlessly interact with the higher network layers by utilizing the SECOQC internal standard—the Q3P communication interface.

The latter is an essential building block of the SECOQC network layer protocols: Q3P, QKD-NL and QKD-TL, which define the intrinsic innovative core of the active SECOQC ‘network agent’, i.e. the trusted repeater network node module. It is this module that makes it possible to interconnect a broad variety of QKD link devices and (in principle) allows the network to grow perpetually by adding new links, whenever required. The paper gives a comprehensive outline of the node module architecture and discusses the mechanisms of end-to-end secret pay-load communication on top of these network layers.

This paper also gives an account of the prototype functionality and is a first attempt to identify simple key store patterns, which underline the potentially complex dynamics of a QKD trusted repeater network. We also define the concept of secrecy transmission capacity and give a closed form representation of this quantity, together with an optimal routing strategy, albeit only for the simple topology of the SECOQC prototype.

In this place, it is essential to stress that there are issues on QKD networks that remain open and require further research beyond SECOQC.

First and foremost is and remains the further development of the underlying QKD technology. This statement is immediately confirmed by a simple illustration. Inspecting figure 23, one discovers that the order of magnitude of secret transmission capacity of the prototype is in the range of 1 GiB per month. This figure is still very low indeed but yet only three to four orders of magnitude away from an adequate transmission capacity. This is not beyond reach! Indeed, recent developments, e.g. the advent of high-speed single photon detectors [63], allow us to expect to increase the performance of QKD devices by several orders of magnitude in the near future that would in turn allow broadband ITS communication based on QKD networks.

The layers and the corresponding protocols of the trusted repeater network also deserve an additional reiteration. It would be important not only to perform simple routing, as discussed in this paper, but also to be able to preselect routes depending on user provided parameters or in relation to quality of service issues. This would also allow us to go beyond the current paradigm, to trespass the rigid trusted repeater approach and (following [25]) enable secure communication in partially trusted networks.

Finally, it must be also stressed that the SECOQC approach allows complete interoperability in the trusted repeater regime but is not directly transferable to switched or mixed networks. Therefore a further major QKD network development task is the design of adequate QKD network architecture(s) for the mixed regime, which is simultaneously the most general one. This would widen the scope of application scenarios, introducing new ITS network models, such as trusted repeater backbones combined with local area switched networks.

Acknowledgments

This work was supported by the EC/IST Integrated Project SECOQC (contract no. 506813).

Additional financial support by Swiss NCCR-Quantum Photonics (to GAP, University of Geneva); the French National Research Agency Project SEQURE (grant no. ANR-07-SESU-011-01) (to Laboratoire Charles Fabry de l'Institut d'Optique—CNRS, to Thales Research and Technology France and to Telecom ParisTech); QCCC, QPENS and the German Bundesministerium der Verteidigung (to Ludwig-Maximilians-Universität, to Max-Planck-Institut für Quantenoptik and to University Erlangen-Nuremberg) is acknowledged.

ED acknowledges support from the European Union through a Marie-Curie fellowship and a Marie-Curie reintegration grant.

References

[1] Bennett C and Brassard G 1984 *Conf. on Computers, Systems and Signal Processing (Bangalore, India)* (New York: IEEE) p 175

[2] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[4] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dusek M, Lütkenhaus N and Peev M 2008 *Rev. Mod. Phys.* at press (arXiv:0802.4155)
[5] Dynes J, Yuan Z, Sharpe A and Shields A 2007 *Opt. Express* **15** 8465
[6] Dynes J, Yuan Z, Sharpe A and Shields A 2008 *IET Optoelectron.* **2** 195
[7] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[8] Gisin N, Ribordy G, Zbinden H, Stucki D, Brunner N and Scarani V 2004 arXiv:quant-ph/0411022
[9] Stucki D, Barreiro C, Fasel S, Gautier J D, Gay O, Gisin N, Thew R, Thoma Y, Trinkler P, Vannel F and Zbinden H 2008 arXiv:0809.5264
[10] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 arXiv:0903.3907
[11] Thew R, Stucki D, Gautier J D, Zbinden H and Rochas A 2007 *Appl. Phys. Lett.* **91** 201114
[12] Hübel H, Vanner M, Lederer T, Blauensteiner B, Lorünser T, Poppe A and Zeilinger A 2007 *Opt. Express* **15** 7853
[13] Treiber A, Poppe A, Hentschel M, Ferrini D, Lorünser T, Querasser E, Matyus T, Hübel H and Zeilinger A 2009 arXiv:0901.2725
[14] Lodewyck J, Debuisschert T, Tualle-Brouri R and Grangier P 2005 *Phys. Rev.* A **72** 050303
[15] Lodewyck J, Debuisschert T, Garcia-Patron R, Tualle-Brouri R, Cerf N J and Grangier P 2007 *Phys. Rev. Lett.* **98** 030503
[16] Fossier S, Diamanti E, Debuisschert T, Villing A, Tualle-Brouri R and Grangier P 2009 *New J. Phys.* **11** 045023
[17] Weier H, Schmitt-Manderbach T, Regner N, Kurtsiefer C and Weinfurter H 2006 *Fortschr. Phys.* **54** 840
[18] Duligall J, Godfrey M, Harrison K, Munro W and Rarity J 2006 *New J. Phys.* **8** 249
[19] Biham E, Huttner B and Mor T 1996 *Phys. Rev.* A **54** 2651–8
[20] Townsend P D 1997 *Nature* **385** 47–9
[21] Townsend P D 1998 *Opt. Fiber Technol.* **4** 345–70
[22] Elliott C 2002 *New J. Phys.* **4** 46
[23] Elliott C, Colvin A, Pearson D, Pikalo O, Schlafer J and Yeh H 2005 *Quantum Information and Computation III* (*Proc. SPIE* vol 5815) ed E J Donkor, A R Pirich and H E Brandt (Bellingham, WA: SPIE) pp 138–49 (arXiv:quant-ph/0503058)
[24] Dianati M, Alléaume R, Gagnaire M and Shen X 2008 *Secur. Commun. Netw.* **1** 57–74
[25] Salvail L, Peev M, Diamanti E, Alléaume R, Lütkenhaus N and Länger T 2009 *J. Comput. Sec.* at press (arXiv:0904.4072)
[26] Alléaume R, Roueff F, Diamanti E and Lütkenhaus N 2009 arXiv:0903.0839
[27] Briegel H J, Dür W, Cirac J and Zoller P 1998 *Phys. Rev. Lett.* **81** 5932–5
[28] Dür W, Briegel H J, Cirac J and Zoller P 1999 *Phys. Rev.* A **59** 169–81
[29] Alléaume R *et al* 2007 arXiv:quant-ph/0701168
[30] Renner R and Cirac J 2008 arXiv:0809.2234
[31] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41
[32] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793
[33] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[34] Niederberger A, Scarani V and Gisin N 2005 *Phys. Rev.* A **71** 042316
[35] Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev.* A **72** 032301
[36] Makarov V and Hjelme D 2005 *J. Mod. Opt.* **52** 691
[37] Makarov V, Anisimov A and Skaar J 2005 *Phys. Rev.* A **74** 022313
[38] Makarov V and Skaar J 2008 *Quantum Inf. Comput.* **8** 622 http://rinton.net/xxqic8/qic-8-67/0622-0635.pdf
[39] Qi B, Fung C H, Lo H K and Ma X 2007 *Quantum Inf. Comput.* **7** 73 http://rinton.net/xqic7/qic-7-12/073-082.pdf
[40] Zhao Y, Fung C H, Qi B, Chen C and Lo H K 2007 arXiv:0704.3253
[41] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[42] Gobby C, Yuan Z and Shields A 2004 *Electron. Lett.* **40** 1603
[43] Debuisschert T and Boucher W 2004 *Phys. Rev.* A **70** 1042306
[44] Lo H K, Chau H and Ardehali M 2005 *J. Cryptol.* **18** 133
[45] Branciard C, Gisin N and Scarani V 2008 *New J. Phys.* **10** 013031
[46] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[47] Lo H K, Ma X and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[48] Ekert A 1991 *Phys. Rev. Lett.* **67** 661
[49] Bennett C, Brassard G and Mermin N 1992 *Phys. Rev. Lett.* **68** 557
[50] Assche G, Cardinal J and Cerf N 2004 *IEEE Trans. Inf. Theory* **50** 394
[51] Lodewyck J *et al* 2007 *Phys. Rev.* A **76** 042305
[52] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325 http://www.rinton.net/xqic4/qic-4-5/325-360.pdf
[53] Brassard G and Salvail L 1993 *Advances in Cryptology: Eurocrypt '93 (Lect. Notes Comput. Sci.* vol 765*)* pp 410–23 doi: 10.1007/3-540-48285-7_ 35
[54] del Rey M 1981 RFC 791: Internet protocol http://www.ietf.org/rfc/rfc791.txt
[55] Deering S and Hinden R 1998 RFC 2460: Internet Protocol, Version 6 (IPv6) specification http://www.ietf.org/rfc/rfc2460.txt
[56] Moy J 1998 RFC 1131: OSPF specification http://www.ietf.org/rfc/rfc2328.txt
[57] del Rey M 1981 RFC 793: Transmission control protocol http://www.ietf.org/rfc/rfc793.txt
[58] Elias P, Feinstein A and Shannon C E 1956 *IRE Trans. Inf. Theory* **2** 117–9
[59] Ford L R and Fulkerson D R 1956 *Can. J. Math.* **8** 399–404
[60] Chekuri C S, Goldberg A V, Karger D R, Levine M S and Stein C 1997 *SODA '97: Proc. Eighth Annual ACM-SIAM Symp. on Discrete Algorithms* (Philadelphia, PA: Society for Industrial and Applied Mathematics) pp 324–33 (ISBN 0-89871-390-0)
[61] Goldberg A V and Rao S 1998 *J. Assoc. Comput. Mach.* **45** 783–97
[62] Tsay A A, Lovejoy W S and Karger D R 1999 *Math. Oper. Res.* **24** 383–413
[63] Yuan Z, Kardynal B E, Sharpe A W and Shields A 2007 *Appl. Phys. Lett.* **91** 041114