Chapter 9
Quantum-Cryptographic Networks from a Prototype to the Citizen

P. Schartner and C. Kollmitzer

9.1 The SECOQC Project

Secure communication is an essential need for companies, public institutions, and in particular the individual citizen. Currently used encryption systems are vulnerable due to the increasing power of computer technology, the emergence of new code-breaking algorithms, and the imperfections of public key infrastructures. Methods considered as acceptably secure today will have a significant risk of becoming weak tomorrow. On the other hand, with quantum cryptography, a technology has been developed within the last decade that is provably secure against arbitrary computing power, and even against quantum computer attacks. When becoming operational, quantum cryptography will raise communication security to an essentially higher level.

The vision of SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography, [15, 1, 12, 2, 3]) was to provide European citizens, companies, and institutions with a tool that allows facing the threats of future interception technologies, thus creating significant advantages for European economy. With SECOQC the basis was laid for a long-range high-security communication network that combines the entirely novel technology of quantum key distribution with components of classical computer science and cryptography.

Within the project the following goals were defined:

1. Realization of a fully functional, real-time, ready-to-market quantum key distribution (QKD) point-to-point communication technology (see Chap. 3).

P. Schartner (✉)
System Security Research Group, Institute of Applied Informatics, Universitaet Klagenfurt, Universitaetsstrasse 65-67, 9020 Klagenfurt, Austria, peter.schartner@uniklu.ac.at
http://www.syssec.at

C. Kollmitzer
Safety & Security Department, Quantum Technologies, AIT Austrian Institute of Technology GmbH, Lakeside B01A 9020 Klagenfurt, Austria, christian.kollmitzer@ait.ac.at; http://www.ait.ac.at

Schartner, P., Kollmitzer, C.: *Quantum-Cryptographic Networks from a Prototype to the Citizen*. Lect. Notes Phys. **797**, 173–184 (2010)
DOI 10.1007/978-3-642-04831-9_9

2. Development of an abstract level architecture, allowing high-security long-range communication by integrating the QKD technology and a set of cryptographic protocols.
3. Design of a real-life, user-oriented network for practical implementation of QKD-based long-range secure communication.

To achieve this goal, all experiences and resources available within the European Research Area were integrated and combined with the expertise of developers and companies within the fields of network integration, cryptography, electronics, security, and software development [16].

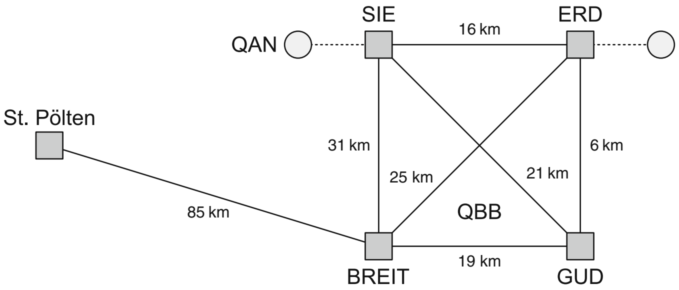


Fig. 9.1 SECOQC Network Vienna

9.1.1 SECOQC Network Vienna 2008

Figure 9.1 shows the concept of the deployed universal building block for QKD networking from [14]. The names refer to the stations of the ring network.

Figure 9.2 shows a map of the fiber ring network in Vienna including the stations SIE (Siemensstraße), ERD (Erdberg), GUD (Gudrunstraße), and BREIT 32 (Breitenfurterstraße) from [14]. Another station, St. Pölten, was located far outside of Vienna.

The SECOQC network was built by using the telecom fiber network from Siemens Austria. As shown in Fig. 9.2 it was built to connect the office buildings of Siemens Austria located in Vienna. The fiber ring connected four nodes (SIE, ERD, GUD, and BREIT) and had a circumference of approximately 85 km. For the SECOQC network, there was also another fiber of about 63 km which connected the city of St. Pölten to the fiber ring. Each connection between two nodes was realized by a QKD device pair which was connected by its own dark fiber. Another fiber loop was used for the classical communication.

The used QKD devices (for details see Sect. 6.2) had to fulfill the following requirement: a stable secure key rate after authentication of at least 1 kbit/s over 25 km of fibers. The systems of the following organizations have met these criteria and took part in the SECOQC network:

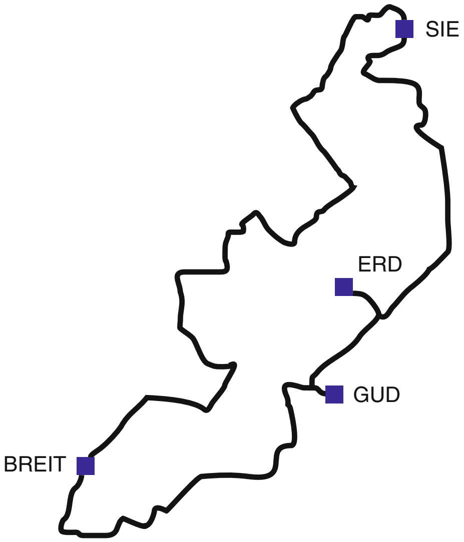


Fig. 9.2 City map of Vienna including the fiber ring network

- IdQuantique (Switzerland) [8],
- GAP Geneva, IdQuantique, ARC (Switzerland, Austria),
- Toshiba (UK),
- University of Vienna, ARC, KTH (Austria, Sweden), and
- CNRS, Thales, ULB (France, Belgium).

9.1.2 Design of a QKD Network

The first practical quantum key distribution took place in 2004 when the headquarters of The Bank Austria Creditanstalt and the Vienna City Hall established a secure communication by using QKD devices. The beeline distance between the communication partners was about 650 m; the installed optical fibers had a length of about 1.45 km [13].

As former QKD schemes, which used to be one-to-one connections, evolve into QKD networks, new network architectures had to be developed. With the SECOQC project, a schema was presented, which consists of two main elements (see Fig. 9.3):

1. A quantum backbone network (QBB), which correlates to a classical backbone network architecture, enhanced for QKD needs like special key stores (see Sect. 8.3.4)
2. A quantum access node (QAN) which allows the user to get the keys, shared with other users within the network.

For more information on global scale QKD-based networks see Chap. 10.

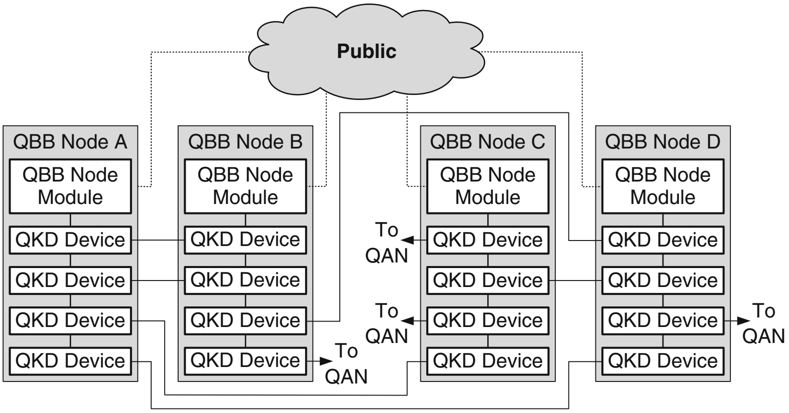


Fig. 9.3 Network architecture used within the SECOQC project

9.2 How to Bring QKD into the "Real" Life

The QBB network at first hand provides one-time pad (OTP) keys for end-to-end security between QBB nodes. In the remainder of this chapter, keys "generated" and used within the QBB network will be called "QKeys." A QKey may be a block of bits, or a stream of bits. In this section, we will discuss some problems which arise, when we want to provide QKeys for everybody. In more detail, we will discuss

- Secure transmission
- Secure storage
- Efficient usage of QKeys

The ideal scenario is that everybody's PC is directly connected to a QAN (Quantum Access Node) by a fiber-optic channel, so that we can protect the last mile by the same mechanisms we employ in the QBB network. We do not think that this scenario will be available in the near future. So, in order to use QKeys everywhere and at any time, we need to design some other techniques. As one possible solution for the problem of secure transport, storage, and usage, we propose small mobile devices like PDAs or SmartPhones with integrated smart cards or special micro SD memory cards (e.g., certgate smart card [5]). These mobile devices may either directly use the QKeys within their applications or they may be used to securely transmit the key to the users' PC.

9.2.1 Secure Transmission to the Mobile Device

The QBB network provides a securely transmitted key-stream between two QANs. In order to use these key-streams within applications, they have to be forwarded to end users, more precisely to the end users' devices. QBB provides unconditional security of the key-streams, so the key-streams have to be protected on the last two links (one at the sender's and one at the receiver's end). Ideally, this protection should provide unconditional security, and if we can't afford unconditional security, we should at least employ a state-of-the-art encryption schemes (e.g., symmetric encryption by means of AES) and some high-entropy key. In this section we will discuss several methods of protecting the last link. Analogous to high-speed Internet we will discuss methods for bridging the last mile (which isn't really a mile here) with existing technologies.

Choosing the appropriate method of data transmission isn't an easy task. Today's mobile devices most commonly provide several communication technologies or input interfaces. Table 9.1 summarizes the advantages and disadvantages of these communication technologies.

The best method for wireless key transmission is obviously freespace QKD. In addition to this method, we will discuss two alternatives. One which uses Near Field Communication (NFC [6]) and another which uses the camera of the mobile device to transmit the session key or the QKey.

Table 9.1 Input interfaces – Pros and Cons

Interface	PROs	CONs
Wireless (QKD)	• unconditional secure	• low bit rate • cumbersomely to use • quite clumsy and expensive
Wireless (RF)	• easy to use • high speed	• sniffing hard to detect • hard to shield
Wireless (IR)	• easy to shield	• difficult alignment • medium bit rate
Wired	• easy to use • high speed	• location of interface not standardized • hidden sniffers hard to detect • vandalism
Audio	• widely supported • easy to use	• hard to shield • low bit rate
Video	• easy usage and alignment • unidirectional communication • easy to shield	• medium bit rate • exotic way of transmission
Text	• widely supported • unidirectional communication	• cumbersomely to use • very low bit rate

9.2.1.1 Quantum Key Distribution – QKD

Ideally, the key material will be transmitted encrypted by use of an unconditionally secure encryption algorithm. Up to now, the one-time pad is the only such algorithm. To employ the one-time pad, we need a key which is as long as the message. Additionally, this key must be random and must not be used twice. So it is obvious, that QKD is the first choice in order to provide unconditional security over all hops, especially the last one. Unfortunately at the time of writing, there are no cheap and small (i.e., size of a standard mobile phone) QKD devices. Additionally, mobile devices should ideally be linked by wireless transmission, in case of QKD this means freespace transmission.

At the time, freespace QKD provides a bit rate of approximately 10–15 kbit/s at a distance of about 80 m [17]. Note that this bit rate can only be achieved under ideal circumstances. A less exact alignment of sender and receiver or atmospheric influences can easily reduce the bit rate.

Using QKD (over fibre optics or freespace) to protect the last mile is desirable, but (at the time) not that practical. So if we do not want to wait, we need other techniques. The second-best choice after OTP encryption with a QKD key is OTP encryption with a high-entropy key exchanged by classical mechanisms. If we need high throughput, we might use a state-of-the-art encryption algorithms and a key of appropriate length. Nevertheless, in all these cases, we need to exchange a session key.

9.2.1.2 Near Field Communication – NFC

In [7], Haselsteiner and Breitfuss proposed an interesting key agreement scheme for Near Field Communication (NFC [6]), which does not involve any security mechanisms at all. The protocol is run between two users *A* and *B*, the adversary will be denoted by *E*. In principle, *A* and *B* repeat the following steps until a sufficient amount of key bits has been generated.

1. Both, *A* and *B*, generate a random bit ($\mathrm{b_A}$ and $\mathrm{b_B}$, respectively) which is sent simultaneously to the other party. In parallel both listen to the communication channel. Since they both send one bit, there are four possible combinations, which are shown in Fig. 9.4. Here, a 1 is represented by sending in the first half of the time slot, whereas a 0 is represented by sending in the second half of the time slot.

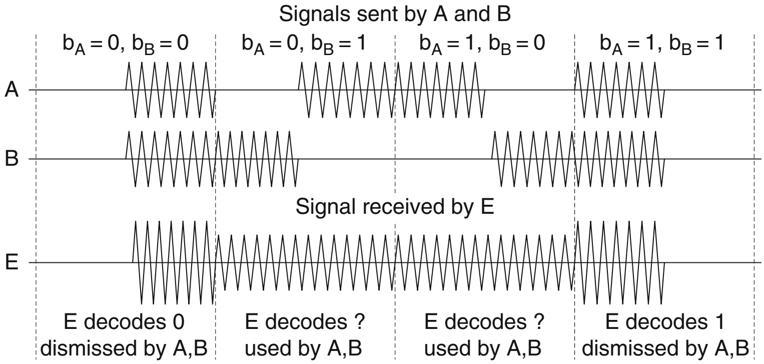


Fig. 9.4 NFC key agreement

2a If $b_A = b_B$, A and B can detect this easily, and so can the attacker E. Hence, A and B have to dismiss their bits and continue with step 1.

2b If A and B sent different bits, they can detect this easily, too. But now, the attacker only knows that A and B sent different bits. He does not know if $b_A = 0$ and $b_B = 1$ or $b_A = 1$ and $b_B = 0$. So A and B can use either the bit sent by A or the bit sent by B to generate a session key. They only need a strategy, whose bit will be used. After adding the selected bit to the session key, A and B continue with step 1.

Note that this describes only the operating principle. In order to provide a high level of security, the sending units of A and B have to be "absolutely" synchronous. Additionally, the amplitudes of the signals generated by A and B have to be indistinguishable.

Since the NFC key agreement uses radio transmission, we have to provide some electromagnetically shielded environment. This raises the question "Why not transmit the key in clear?" or, for the sake of security, encrypted by use of a rather short key and high-speed symmetric encryption scheme?

9.2.1.3 Optical Transmission

When we think of wireless transmission of the key-stream, we should not restrict ourselves to radio frequency (i.e., WLAN, Bluetooth, of NFC). Since almost all current phones and most PDAs are equipped with a camera, we might use optical transmission of the QKeys instead of radio transmission. Again, this is not the ideal (i.e., high-speed, unconditional-secure) mechanism. But it is cheap, easy to implement, and easy to use! Additionally, optical transmission is much easier to shield than radio frequency transmission (light doesn't propagate around corners that easily).

So how to apply optical transmission between the key terminal and the mobile device? One method to encode the data is so-called QR codes (quick response codes) [9, 10, 11]

Figure 9.5 shows some QR codes which have been generated by use of the free tool of KAYWA AG, Switzerland (http://qrcode.kaywa.com). The left one encodes

Fig. 9.5 QR codes

the URL "www.secoqc.net," the middle one encodes the text "SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography," and the right one encodes the first 236 characters of the first paragraph of the Wikipedia page on QR codes ("http://en.wikipedia.org/wiki/QR_Code"). These sample QR codes correspond to about 77, 528, and 1.298 bits, respectively (∼5.5 bits per alphanumerical character).

According to Denso Wave Incorporated, QR codes – which use Reed-Solomon for error detection and error correction – come with the following maximum data capacity:

- 1.817 Kanji/Kana characters, or
- 4.296 alphanumeric characters, or
- 7.089 numeric only characters, or
- 2.953 bytes (8 bits each, so 23.624 bits in total).

Most PDA and Smartphone cameras come with a minimal focus distance of about 30–50 cm. This means that the LCD screen displaying the QR codes has to be in similar distance to the camera (see the left side of Fig. 9.6 for a sketch of such a system). In order to reduce the size of the key terminal, we could use the camera to detect the presence or absence of light only (binary coding). In this case, the minimal focusing distance doesn't matter and we can shrink the size of the key terminal to a minimum.

In order to overcome the reduced bandwidth of binary transmission, we could split the camera image into several subsections (each detecting the presence/absence of light) or we could use several colors like indicated in the right half of Fig. 9.6. In both cases the bandwidth will be increased by 2^n, where n is the number of sections or colors, respectively. Additionally, the images are now much simpler than QR codes and hence can be decoded much faster.

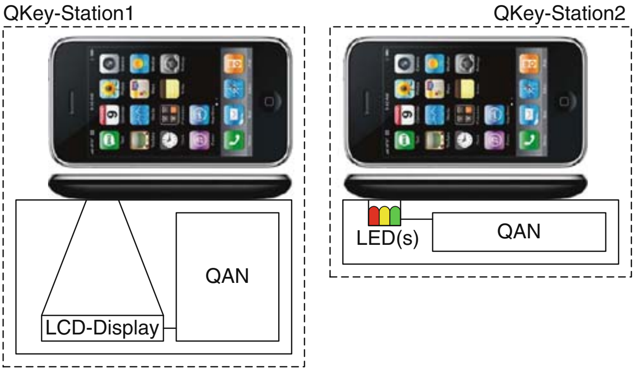


Fig. 9.6 iPhone 3G at a key terminal

9.2.2 Secure Storage

In our scenario, there is no online connection between the QAN and the mobile device. So it is obvious that we have to securely store an appropriate amount of key material within the mobile device over a longer period of time. So let us briefly analyze some types of mobile devices with respect to secure storage:

- *Laptops and Netbooks:* Indisputably, these devices provide a huge storage capacity, but they are quite clumsy and very hard to secure.
- *PDAs and SmartPhones:* These devices are rather handy and come with sufficient memory, but are still quite hard to secure.
- *Smart Cards:* Smart Cards come with two flavors: smart cards (also known as ICCs – integrated circuit cards) and special secure memory cards.

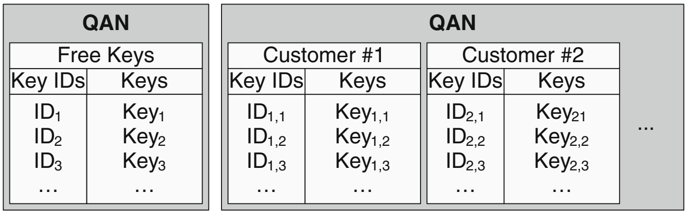
  - *Smart Cards or ICCs:* By now, there are four standardized formats: ID-0 (credit card size), ID-00, ID-000 (plugin or SIM size), and Mini-UICC (about half plugin-size). These cards can provide up to 1 GB of non-volatile memory and most commonly come with a cryptographic co-processor (e.g., 2048 RSA in 10 ms, AES in 10 μs). Besides these positive features, smart cards come with a major disadvantage: that we need some type of special terminal in order to connect them to a PC, Laptop, PDA, or SmartPhone.
  - *Secure memory cards:* Within memory cards, a special type of SD memory crads (short SDCards [4]) is quite promising: the certgate SDCard [5]. This SDCard (1 GB) is provided with a smart card microprocessor. Since this processor can be used over the standard SDCard interface, no special reader is needed.

Up to now, Personal Digital Assistants (PDAs) or SmartPhones which are equipped with a smart card or some other security token (e.g., a certgate SDCard) will fulfill our security requirements. It is obvious that this type of equipment is not ideal (e.g., it is not unconditional secure), but it is available, quite cheap, widely adopted and accepted by the customers.

9.2.3 Efficient Key Usage

In the SECOQC design, a standard QBB node has three types of key buffers (called KeyStores):

- *In-KeyStore:* Keys within this KeyStore are reserved for incoming messages of the QBB network.
- *Out-KeyStore:* Keys within this KeyStore are reserved for outgoing messages of the QBB network.
- *Application KeyStore:* Keys within this KeyStore are handed over to external applications.



QAN

Free Keys	
Key IDs	Keys
ID_1	Key_1
ID_2	Key_2
ID_3	Key_3
…	…

(a) Free Keys

QAN

Customer #1		Customer #2		
Key IDs	Keys	Key IDs	Keys	
$\text{ID}_{1,1}$	$\text{Key}_{1,1}$	$\text{ID}_{2,1}$	Key_{21}	...
$\text{ID}_{1,2}$	$\text{Key}_{1,2}$	$\text{ID}_{2,2}$	$\text{Key}_{2,2}$	
$\text{ID}_{1,3}$	$\text{Key}_{1,3}$	$\text{ID}_{2,3}$	$\text{Key}_{2,3}$	
…	…	…	…	

(b) Customer/Application specific Keys

Fig. 9.7 Quantum access node keystore

In order to guarantee a minimum number of QKeys for special applications, we would like to propose an additional component which divides the keys of the Application KeyStore into two classes: so-called free keys and designated keys (see Fig. 9.7. The IN- and OUT-buffer of the QBB node will remain reserved for internal use (i.e., key forwarding).

- *Free Keys:* Free keys may be used for any purpose (i.e., encryption or authentication of any data type) and any receiver. After retrieval of the communication key at the sender's end, the system does not know the receivers address. So there are at least two possible strategies:

  1. The sender already knows the receiver (respectively, his address). Now, the receiver can be informed by the system and the receiver can immediately retrieve the communication key.
  2. The sender does not want to send data right now, he simply wants to get some keys for his local key storage. Now there can't be done anything in advance at the receiver's end. The receiver has to wait for the encrypted/authenticated message in order to identify the used key. Now he can retrieve the key and decrypt/check the message.

- *Designated Keys:* If a sender retrieves a key reserved for a special receiver (or purpose), the designated receiver can automatically be informed as soon as the key has been retrieved by the sender. Hence, the receiver is able to fetch his key at the moment, the sender requests it from the KeyStore.

9.3 Resumee

So far, the field of QKD has been analyzed from several different points of view. Especially, networks have been in the center of research interest. With the SECOQC demonstration in October 2008 it has been shown that networks based on QKD are realizable, which changed the focus on the security research. On one hand there will be growing interest on QKD-based applications and, on the other hand, we expect an increasing research activity on the enhancement of already existing communication infrastructures regarding a secured key exchange. In our opinion, transmission, storage, and usage of keys generated by QKD becomes the new emphasis of research work.

In order to achieve an appropriate market throughput, QKD systems will have to offer solutions for different security levels. Thereby, different areas must be covered, e.g., QR codes offer the possibility of a fast, widely spread, and easy to use method for applications of a lower security level.

From our point of view, QKD is a massive future topic. The research focus will spread in the next years and not only the physical fundamentals will be examined but also the aspects of applications will be more and more of interest. We think in particular that scenarios with simple, easy to access interfaces, designed for a large number of users such as telephone boxes or ATM-like systems, will be of strong interest.

References

1. Alléaume, R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Leverrier, A., Lütkenhaus, N., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., Zeilinger, A.: SECOQC white paper on quantum key distribution and cryptography (2007). http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/07%01168 173
2. Alléaume (Editing author), R., Bouda, J., Branciard, C., Debuisschert, T., Dianati, M., Gisin, N., Godfrey, M., Grangier, P., Länger, T., Leverrier, A., Lütkenhaus, N., Painchault, P., Peev, M., Poppe, A., Pornin, T., Rarity, J., Renner, R., Ribordy, G., Riguidel, M., Salvail, L., Shields, A., Weinfurter, H., Zeilinger, A.: Quantum key distribution and cryptography. SECOQC White Paper (2007) 173
3. Assche, G., Cardinal, J., Cerf, N.: IEEE Trans. Inf. Theory **50**, 394 (2004) 173
4. Association, S.: (2009). http://www.sdcard.org 181
5. Certgate: Certgate Secure Digital Card (2009). www.certgate.de 176, 181
6. Forum, N.: (2009). http://www.nfc-forum.org/home 177, 178
7. Haselsteiner, E., Breitfuss, K.: Security in near field communication (NFC). Handout of Workshop on RFID Security RFIDSec06 (2006). http://events.iaik.tugraz.at/RFIDSec06/Program/papers/002%20-%20Security%20in%20NFC.pdf 178
8. IdQuantique: (2009). http://www.idquantique.com 175
9. Inc., D.W.: QR-Code Standardization (2009). http://www.denso-wave.com/qrcode/qrstandard-e.html
10. ISO: (2006). ISO/IEC 18004:2006 – Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification
11. ISO: (2009). ISO/IEC 18004:2006/Cor 1:2009
12. Monyk (Coordinator), C.: Development of a global network for secure communication based on quantum cryptography. EC/IST Integrated Project SECOQC **Contract No. 506813** (2004-2008) 173
13. Poppe, A., Fedrizzi, A., Ursin, R., Böhm, H.R., Lorünser, T., Maurhart, O., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T., Zeilinger, A.: Practical quantum key distribution with polarization entangled photons. Opt. Express 3865 **12** (2008) 175
14. Poppe, A., Peev, M., Maurhart, O.: Outline Of The SECOQC quantum-key-distribution network in Vienna. Int. J. Quantum Inf. **6**(2) (2008) 174
15. SECOQC – Development of a Global Network for Secure Communication based on Quantum Cryptography: (2009). http://www.secoqc.net 173

16. Sheet, I.P.F.: (2009). http://cordis.europa.eu/fetch?CALLER=PROJ_IST&ACTION=D&RCN=71407 174
17. Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., Ömer, B., Fürst, M., Meyenburg, M., Rarity, J., Sodnik, Z., Barbieri, C., Weinfurter, H., Zeilinger, A.: Free-Space distribution of entanglement and single photons over 144 km (2006) 178