10

Quantum Key Management

Peter Schartner[1], Stefan Rass[1] and Martin Schaffer[2]
[1]*Alpen-Adria Universität Klagenfurt*
[2]*NXP Semiconductors Austria GmbH Styria*
Austria

1. Introduction

Quantum key distribution (QKD), invented by Bennett & Brassard (1984) based on previous work of Wiesner (1983), has been recognized as a key-technology of the upcoming decades. With various (experimental) quantum networks existing (cf. the reports of Poppe et al. (2008) and Elliott (2004)), questions regarding the efficient construction and management of such networks arise. While much has been achieved in proving security of QKD under various assumptions (trusted devices as proposed by Salvail et al. (2009) vs. non-trustworthy devices as discussed by Elliott (2008b)), and many cryptographic primitives have been transferred to the quantum setting by Buchmann et al. (2004) and Damgård et al. (2004), some questions are still waiting to be answered. With the invention of public-key cryptography, key management has become an issue of major importance. Authentication is equally crucial for QKD-enhanced links, but authenticating keys here is inherently different to the public key setting. Nevertheless, why should quantum cryptography not benefit from the lessons learnt in classic, particularly public-key, cryptography (one of which is the strict principle not to use one key in two different applications)? Elegant ideas for key management and authentication have arisen in public-key cryptography (such as identity-based cryptography invented by Shamir (1985) or certificateless cryptography discussed in Al-Riyami & Paterson (2003)). Are similarly elegant solutions imaginable for the problem of entity authentication in the quantum setting? More importantly, with the one-time pad (OTP) as the encryption of choice, the key demand equals the data transmission demand in terms of size, so an effective management of keys is crucial for a reasonable quality of service of quantum networks. The whole security can be at stake if (quantum-)key generators cannot cope with the flood of information and run empty, thus logically (in terms of secrecy) cutting the link.

Summarizing some lessons learnt from public-key cryptography, the management of keys includes their creation, activation, assignment, binding (to identities), escrow, recovery, as well as revocation and destruction. Particularly the last point is sometimes neglected, but is of no less importance than any of its predecessors.

What has all this to do with quantum cryptography? At first glance, secret-key cryptography does not suffer from such complicated issues as public-key cryptography does. Once a key has securely been created (or exchanged), why bother with key-management? In fact, public-key cryptography has evolved early enough to have become a fundament to almost all nowadays existing networks. While symmetric encryption is (often, perhaps not always) used for data transfer based on session keys that have been exchanged by virtue of public-key means (hybrid cryptosystem), its (session) keys do require some management too. Indeed,

side-channel attacks and remote timing attacks have demonstrated the need to change symmetric session keys periodically and frequently, in order to avoid the adversary collect sufficiently many transcripts (involving the same key) to potentially breach the system's secrecy. Besides this, data recovery fields that allow for emergency reconstruction in case of lost keys are just one simple example, but many more scenarios exist where authorities may have legitimate interest in "opening" a channel, protected by symmetric cryptography. Guarding against terrorism is only one critical example, which back in the days gave rise to the well-known Escrowed Encryption Standard (1994).

Quantum key management

The core of this chapter is about management of keys created by QKD devices. Several proposals tackling various aspects of this problem are around, such as the quantum network manager proposed by Mink et al. (2008). Commercial solutions, such as the "Scalar Key Manager Appliance" due to Quantum (2009), originally dedicated to the management of keys for tape storages, could be used as a starting point for effective quantum key management. In particular, once the keys are created, the quantum-related part is mostly over, and when it comes to storing the goods in secure places, this expertise becomes valuable.

From the experimental point of view, SwissQuantum (2011) reports on a running quantum network, with a dedicated key management layer. Speaking of the latter, a patent has been submitted by Berzanskis & Gelfond (2009), employing a centralized quantum key certificate authority. Of course, it would be desirable to have a fully decentralized management of such a network, for not only resilience against attacks, but also for relieving trust requirements in each node.

The randomness of QKD keys is vital to the security of subsequent applications based on these keys. Several proposals exist; see the work of Tanaka et al. (2008) as one example. Finally, one should consider the possibility to strengthen existing standards by virtue of QKD. Some steps towards this have been taken, as indicated by Mink et al. (2009).

Chapter organization

Section 2 presents some arguments to substantiate the need for research towards quantum key distribution. Although nowadays cryptography appears to be capable of sufficient protection, it nevertheless pays to look at its (theoretical) limits to motivate why practical quantum key distribution devices are needed at the earliest possible stage. In Section 3, we discuss various ways to attack and defend a quantum network on a higher level than where the QKD protocols run. Since QKD has been extensively studied by researchers with ingenious proofs of security, an attacker will most likely focus his efforts on attacking elsewhere than on the quantum link. Guarding against such incidents, which include denial-of-service attacks or attacks on the perhaps not-so-well protected devices, are subject of this section. Section 4 addresses the benefit that a quantum infrastructure provides from the viewpoint of a decision-maker. After all, the decision maker will be concerned mostly with two questions: how much does it cost and what is the benefit? QKD as such is only capable of point-to-point security, but getting end-to-end security is a completely different problem. The main goal in Section 4 is to analyze the power of quantum networks in terms of end-to-end security. The ability to talk privately is worthless if we cannot assure who we are talking to, hence authentication is crucial to avoid person-in-the-middle attacks. Section 5 briefly discusses continuous authentication in the context of QKD and contains further details about authentication *without* end-to-end shared secrets. Applications of QKD in a wireless area are a live area of research, and Section 6

is a compilation of selected results on wireless QKD performance and some thoughts towards extending the application scenarios to an indoor and ad hoc domain. Final conclusions are drawn in Section 7.

2. Why quantum cryptography matters

Several arguments seemingly limiting the value of quantum key distribution exist. First, it does not come with a natural defense against impersonation attacks, and authentic channels are an inevitable ingredient for secure QKD. As already outlined by Paterson, K.G. and Piper, F. and Schack, R. (2004), this is an occasionally overlooked fact, leading to wrong expectations and perhaps flawed security arguments. Moreover, Shor (1997) has presented algorithms to solve the factorization and discrete logarithm problem, which are a severe threat to many public-key environments once quantum computers come to operation. Fortunately, up to now there is no significant evidence of symmetric algorithms like AES being in danger too. So even if hybrid cryptography fails by Shor's algorithms becoming standard, there are still other public key schemes available residing on problems that are not easily solved on a quantum computer too. Furthermore, post-quantum cryptographic primitives such as signatures (discussed by Buchmann et al. (2004)) or zero-knowledge proofs (discussed by Damgård et al. (2004)) are being developed. It follows that we could just "evade" the technological progress by enlarging the parameter spaces faster than the bit-lengths increase that quantum computers could handle. This is just what is happening nowadays, but transferred to a world full of quantum computers.

Anyone who feels uneasy about computational intractability assumptions (for their validity is hard to assure reliably) will agree that provable security is the more desirable good, compared to keeping the actual scenario alive.

Moreover, much of the field of multi-party computation (cf. the work of Hirt (2001)) relies on secure channels between any two participants. QKD is a natural tool for achieving this. Though this assumption is not obligatory (with corresponding results comprehensively discussed by Goldreich (2008) for instance), perfect end-to-end security between any two players in a multi-party protocol is often implicitly assumed, but rarely explicitly ensured in the literature. As we cannot expect a fully meshed network between players of a multi-party computation, end-to-end security is a vital point of these applications.

3. Trusted nodes, denial-of-service, maintenance and recovery

Since QKD networks use one-time pad encryption to protect the secrecy of the transmitted messages, the attacker basically has two options:

1. attacking the nodes and extracting the key material, or
2. forcing the QKD nodes into the usage of classical encryption by means of a denial-of-service attack on the (optical) QKD links.

In the remainder of this section, we will describe two methods which will help to mitigate the threats described above. The first method proposed by Schartner & Rass (2009) results in so called strengthened QKD nodes. These nodes are in fact not invulnerable to physical attacks, but these strengthened nodes will stay secure for some period of time even in the case of a physical attack. This time span may be used to securely transmit an alarm message to the network management center. The second approach proposed by Schartner & Rass (2010) resurrects the idea of keeping public parameters secret, like proposed by Kaabneh &

Al-Bdour (2005). Here the idea is to use the remaining key material in the most efficient way and maintain a high level of secrecy during the DOS attack on the QKD link(s).

3.1 Strengthening QKD nodes

As it is with other cryptographic protocols, the security of QKD protocols massively depends on the security of the keys (one-time pads). In contrast to classical cryptographic protocols the space needed to store these keys is quite large (more precisely: as large as the messages). Unfortunately secure storage, can only partially be settled on cryptographic grounds, as leaking key material is in any sense not acceptable. Although the problem of physically stealing a keystore from a QKD-repeating node can be made less emergent using the technique proposed in Schartner & Rass (2009), it cannot be fully overcome. A full solution for that case is presented in Rass (2009), but at the cost of increased communication overhead and a threshold assumption on the number of so compromised nodes. The construction in Rass (2009) is simple, yet too lengthy to be repeated here, but the basic idea of Schartner & Rass (2009) can be sketched as follows: once a node shares (via a QKD channel, denoted as $\leftarrow\!\!-\!\!-\!\!-\!\!\rightarrow$) a key k_A with one neighbor (predecessor A), and another key k_B with another neighbor (successor B), then, instead of storing the pair (k_A, k_B), why not store $k_{AB} := k_A \oplus k_B$, where $\oplus$ denotes the bitwise exclusive-or. Passing a one-time pad encrypted message $c_A := m \oplus k_A$ onwards to the successor is trivial by sending $c_B = c_A \oplus k_{AB} = m \oplus k_B$ straight away. The process is sketched in Figure 1, where Node R forwards an encrypted message from Node A to Node B.

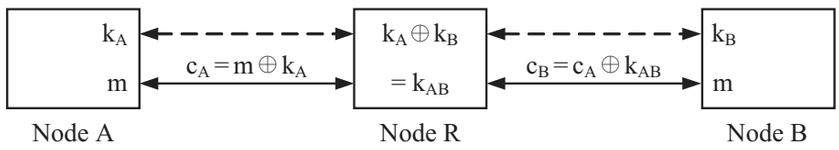


Fig. 1. Protected forwarding of messages

Notice that this re-encryption never reveals the plain text m, and no decryption of c can be performed using only k. This way, the adversary has to wait until all key material is used up, and fresh key material is created, which can then be prevented from being discarded after XORing it pairwise.

This scheme renders information streams between different ports independent from each other, as each pairwise connection enjoys its own key-store. Contrary to the classical design (see Figure 2 (left)), information being passed from port A to port B does not draw from the same key-store as the flow from A to C would do. This naturally facilitates efficient load balancing. Comparing the two designs (the new one shown in Figure 2 (right)) in terms of buffers and keys, reveals that the new design cuts down the number of keys by a factor of two, thus doubling the efficiency. Giving some numbers, a trusted relay with 5 links requires 5 buffers storing 4 keys per buffer (making a total of 20 keys), whereas the design of Schartner & Rass (2009) does this with 10 buffers filled with only 1 key (ending up with only 10 keys). Even this higher number of buffers is no real restriction, as these are located within the same physical memory anyway.

A yet open issue is how the network management traffic can be exploited for mounting attacks or deriving information about the information flow. As key-management is a core task that cannot autonomously be done by a single node, can the "background traffic" be manipulated to mount attacks? This question cannot be answered on general grounds, as it depends on

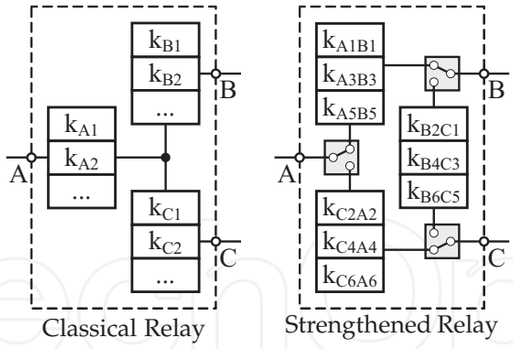


Fig. 2. Two relay methods

the particular implementation of the quantum network (we refer the reader to the report of Los Alamos National Security (2009) for an overview). However, the possibility should be considered when designing such network managers. A problem that has not received much attention yet, as it seems.

A different possibility is offered by secret-sharing. If the secret key is shared among many parties, can this somehow prevent access if only one party is compromised? The question might be trivial and with a negative answer if we really ask for one-time pad keys, but the management of shares in a multi-party computation environment may offer interesting ideas applicable to securing QKD keys as well, if we are willing to use keys shorter than the messages to encrypt. Although this is no secrecy in the sense Shannon envisioned, but still unconditionally provable and could be good enough for practical use. Apart from this, it seems that the keystore has to be secured by non-cryptographic means in order to protect keys from unauthorized access.

3.2 Counteracting DoS-attacks

In case of a denial of service attack on the QKD links, the first option ist to suspend the transmission of messages when the nodes run short of key material. Unfortunately, there may be scenarios where no communication is no option. So we can continue to use the remaining key material in the most secure way: as one-time pads. Unfortunately, in this case each encrypted and transmitted bit "costs" one bit of key material. If we have to transit more message bits, than key bits remaining, we could switch to some emergency communication mode, which uses the key material already stored in the connected nodes in the most efficient way and continues to send (encrypted) messages on an alternate path. Figure 3 shows such a QKD network, which securely connects a sending node A and a receiving node B. There are several paths between A and B, like $A \leftrightarrow B$, $A \leftrightarrow 1 \leftrightarrow B$, $A \leftrightarrow 1 \leftrightarrow 2 \leftrightarrow B$ or $A \leftrightarrow 4 \leftrightarrow 2 \leftrightarrow B$, but obviously all these paths start at A and end in B. So a good place to mount a DoS attack is somewhere nearby the sending node A or receiving node B. Even worse, if the links directly connected to A or B are bundled, because now the attacker can affect all of them with a single strike. As shown in Figure 3, the attacker has brought down all links directly connected to B. Hence, secure key exchange over the QKD network and subsequently secure communication between A and B becomes impossible.

In order to keep secure communication alive, A and B use an alternate communication path somewhere outside the QKD network. The only question remaining is how to secure this link, if there is no way to generate new key material. The straight forward solution is to use the

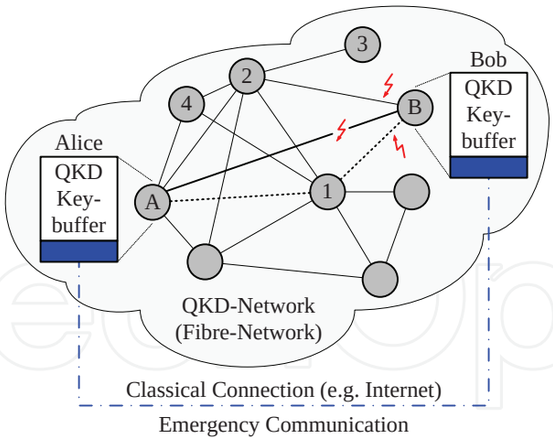


Fig. 3. Usage of the proposed scheme

remaining key material as keys for classical symmetric encryption (e.g. AES). Note that this is exactly the way, some commercial products like Cerberis (ID Quantique ID Quantique (2011)) use to exchange keys for classical symmetric encryption by means of OTP-protected links.

When using such a hybrid scheme of QKD and symmetric encryption, we should keep in mind that the strongest assumption on the attacker is, that he knows the protocol, the cipher, the block length and the key length. Hence, if the attacker gets hold of transmitted ciphertexts, he can (at least) start a brute force attack to find the key. If the attacker can insert some plaintext into the encryption system, he can start a known plaintext attack as well. After retrieving the key, all messages encrypted with this key can be decrypted. Hence, the key has to be changed quite often if we want to keep the damage low in case of a successful attack on the key.

If we want the attacker to face a harder problem, the idea is to hide essential parameters from the attacker (but assume that the employed protocols and algorithms are still known). In case of symmetric encryption (like AES) there is nothing to hide except the key length (128, 192, or 256 bit). All other parameters (like block length) are fixed. In order to overcome this drawback, the scheme proposed by Schartner & Rass (2010) uses a hybrid encryption system which consists of three layers (also see Figure 4):

1. QKD is used to establich OTP in connected nodes. These OTPs are used to encrypt parameters of a public key encryption scheme (message c_1).
2. The public key encryption scheme is used to transmit the keys for the classical symmetric encryption (message c_2).
3. Finally the (fast) symmetric encryption scheme secures the transmitted messages m_1 to m_n (ciphertexts c_{31} to c_{3n}).

The best attacking method on RSA, known by now, is factorizing the modulus and deriving the private key from the public key. If the attacker never sees the modulus (as it is encrypted by use of an OTP), he has no chance to factorize it. And if the attacker retrieves the primes of the modulus by other means, he is still missing the public key (which is also transmitted encrypted by use of an OTP). For assessing how hard these problems really are, and an alternative that replaces RSA and AES by ECC, we refer the reader to Schartner & Rass (2010).

It is clear, that the key for the symmetric encryption has to be changed quite frequently (as mentioned above). But now, this does not cost valuable QKD key material.

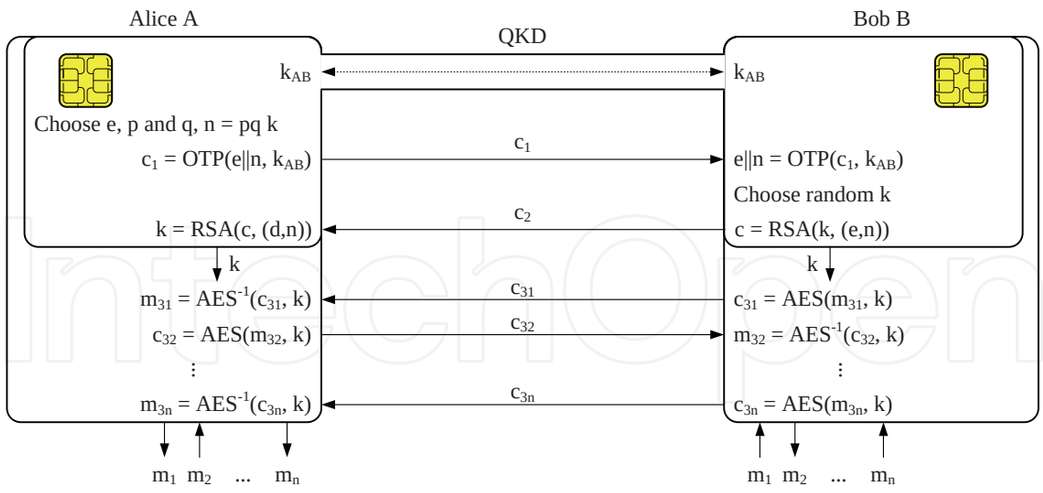


Fig. 4. A three step hybrid system: QKD+RSA+AES

Note that this special mode of operation of the QKD nodes may be used during the maintenance of QKD links as well.

4. Risk management in a quantum network

It is well-known that quantum key distribution is limited in terms of distance and that it can create cryptographically strong keys between directly connected peers. Also, most plain QKD protocols are intended for two-party key-exchange. The problem of *quantum conference keying* has been studied and some interesting solutions were proposed by Jin et al. (2006) and Hwang et al. (2007). However, we will confine ourselves to the simpler two-party point-to-point key-exchange here. The problem of achieving end-to-end security from this kind of point-to-point security is nontrivial, and several solution proposals to overcome the distance limitation exist. Among the most important are the following:

- Quantum repeater
- Trusted relay
- Multipath transmission

The well-known no-cloning theorem due to Wootters & Zurek (1982) rules out the possibility of copying photons in a similar manner as electrical signals can be reproduced for amplification. Hence, a quantum repeater appears impossible at first glance. Fortunately, however, entanglement of photons can be exploited to achieve almost the same effect as a (classical electrical) repeater would have. This concept is known as *quantum repeater*. The theory behind this is much beyond the scope of this chapter and the interested reader is referred to the work of Dür et al. (1999) and Yuan et al. (2008) for a theoretical as well as practical introduction. Here, we will confine ourselves to conveying the underlying ideas. Unfortunately, however, quantum repeaters have not yet reached a level of maturity beyond experimental implementations in the laboratory.

Roughly speaking, the idea behind a quantum repeater is to create a chain of entangled photons. That is, one starts with a single pair of entangled photons ϕ_1, ϕ_2, and creates another pair of photons ϕ_3, ϕ_4 such that ϕ_2 is in addition entangled to ϕ_3. Hence, the states

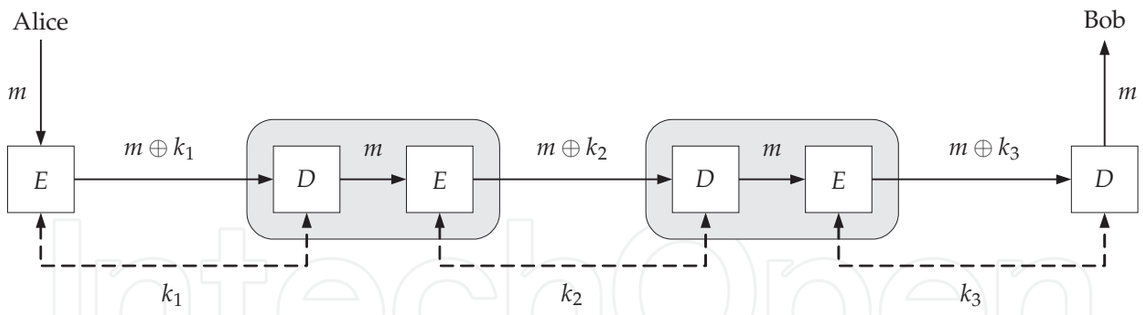


Fig. 5. One-time pad based single path transmission with two intermediate nodes

of ϕ_1 and ϕ_4 are entangled, meaning that information can be transported from ϕ_1 to ϕ_4. This idea can be repeated (endlessly) to bridge arbitrary distances. It goes without saying that practical implementations are far more complex than this simple sketch. For instance, entanglement purification (a highly nontrivial process on its own) are crucial ingredients to avoid the entanglement becoming "messed up" with noise. Nevertheless, various approaches and implementations exist in the lab, and future networks might employ such technology soon.

Trusted relay is the simple concept of having each intermediate node along a lengthy chain re-encrypt its incoming payload before forwarding it to the next hop. This comes at the price of each intermediate node getting to see the message. Figure 5 illustrates the problem. Still, this transmission paradigm finds itself implemented in various quantum demonstration networks, such as the SECOQC network (cf. Peev et al. (2009)) or the DARPA network (cf. Elliott (2007)). From a risk manager's perspective, such trust assumptions are rather undesirable, since it is difficult to quantify the risk and hence to meaningfully relate it to business assets (confidential information) that are communicated over the quantum network. *Multipath transmission* is a straightforward remedy to relieve the stringent assumptions that trusted relay requires, and to avoid complex technologies like the quantum repeater. Hence, we describe this third paradigm in more detail now. As usual in quantum cryptography, we consider a computationally unbounded adversary. The only constraint that we require is his incapability of compromising more than a fixed portion of the network. That is, we cannot allow the adversary to conquer arbitrary large parts in the network, for otherwise we would have a classical person-in-the-middle situation. In the absence of end-to-end shared secrets, confidential communication is impossible in this situation (for obvious reasons).

Consider the well-known polynomial (k, n)-secret-sharing due to Shamir (1979) as a motivating example, and let the adversary's threshold be t, i.e. no more than t nodes in the network can be compromised. Furthermore, assume that the network topology (graph) G connecting Alice and Bob admits r node-disjoint paths between them. Obviously, if $r > t$, then we transmit a secret message in a perfectly secure manner as follows:

1. Choose a set of at least k out of $r > t$ node-disjoint paths for transmission (a simple choice is $k = n$ so that the adversary is forced to intercept all n paths, which is impossible if $t < n$. However, more careful choices of $k \leq n$ can yield to protocols with less overhead but no loss of security).
2. Decompose the secret message into k shares traveling over the k paths from Alice to Bob.

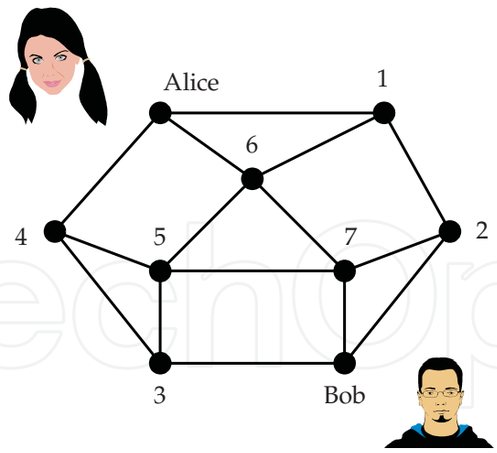


Fig. 6. Example network topology

3. Let the receiver reconstruct the secret from the received shares, possibly invoking an error correction algorithm (perhaps the one devised by Berlekamp & Welch (1986)) to recover from corrupted shares.

This is the rough skeleton that many protocols for multipath transmission embody. Moreover, it constitutes a necessity for perfectly secure communication, as has rigorously been proven by Wang & Desmedt (2008), Fitzi et al. (2007) and Ashwin Kumar et al. (2002). The remaining problem with these results still is their limited applicability in real-life networks, as many known criteria for perfectly secure communication impose strong requirements on the graph's (vertex) connectivity. We shall not go into details about this, and confine ourselves to the following simple observation:

Provided that $r > t$, it is easy to see that even if $k \leq t$, we still have some chance to have chosen paths that the adversary has not yet intercepted. In other words, as long as he cannot have all paths under his control, we have some chance of at least partially circumventing the adversary. Now, the problem has changed into finding a clever way of choosing these paths. It is trivial to enumerate all possible choices, along with all possibly compromised sets of nodes. Having these lists, we can set up a matrix whose entries contain either zero if the transmission failed, or 1 if the transmission was successful. At this point, we can invoke *game-theory* to provide us with the best way of choosing among our options (paths). A full discussion of this idea is given by Rass & Schartner (2010b), and we will use a simple example to illustrate the idea here.

Suppose Alice and Bob being interconnected through the simple network depicted in Figure 6. Implementing the above skeleton, they use multipath transmission based on a $(2,2)$-sum-sharing of the form $m = s_1 \oplus s_2$, where m is the secret message and $\oplus$ is the bitwise exclusive-or. This scheme directly resembles a one-time pad encryption and is therefore information-theoretically secure, as Shannon (1949) has proved. For illustration, let the adversary have the assumed threshold $t = 2$. Call PS_1 the list of all selections of two disjoint paths, and write PS_2 to denote the list of all nodes that are possibly compromised (two-element subsets of $V = \{1, 2, \ldots, 7\}$). Let S_1 and S_2 be the set of *probability distributions* over PS_1, PS_2, respectively. For each scenario $(s_1, s_2) \in PS_1 \times PS_2$, we decide about success for Alice and Bob (outcome 1) or failure (outcome 0). Collect all these in a matrix $A \in \{0,1\}^{n \times m}$. Let $\theta_1 \in S_1$ be the probability distribution from which Alice and Bob draw their paths

PS_1 (Alice and Bob)	PS_2 (adversary)
s_1^{AB}: $\{A—4—3—B, A—1—2—B\}$	s_1^{adv}: $\{1,4\}$
s_2^{AB}: $\{A—4—5—7—B, A—1—2—B\}$	s_2^{adv}: $\{1,6\}$
s_3^{AB}: $\{A—6—5—3—B, A—1—2—B\}$	s_3^{adv}: $\{4,6\}$
s_4^{AB}: $\{A—6—7—B, A—1—2—B\}$	s_4^{adv}: $\{1,7\}$
s_5^{AB}: $\{A—6—7—B, A—4—3—B\}$	s_5^{adv}: $\{1,3\}$
	s_6^{adv}: $\{1,5\}$

(a) Strategies

A	s_1^{adv}	s_2^{adv}	s_3^{adv}	s_4^{adv}	s_5^{adv}	s_6^{adv}
s_1^{AB}	0	1	1	1	0	1
s_2^{AB}	0	1	1	0	1	0
s_3^{AB}	1	0	1	1	0	0
s_4^{AB}	1	0	1	0	1	1
s_5^{AB}	1	1	0	1	1	1

(b) Utility matrix

Fig. 7. Security Game

(randomized routing), and let θ_2 describe the probabilities for certain subsets of nodes to be compromised. Then, the bilinear form ${\theta_1}^T A\theta_2$ is the long-run average success-rate, or in other words the probability for Alice and Bob being successful. Presuming the adversary having precisely opposite intentions than Alice and Bob have, we can set up a zero-sum competition giving the best strategy of path selection and the strongest strategy for attacking. Formally, this is the *Nash-equilibrium* of the game induced by A. Its average outcome is the value $v(A)$ of the game, and defined as

$$v(A) = \max_{\theta_1 \in S_1} \min_{\theta_2 \in S_2} {\theta_1}^T A\theta_2$$

because Alice and Bob try to maximize their success-rate, while the adversary tries to minimize it (thus maximizing his chances of eavesdropping).

Observe that ${\theta_1}^T A\theta_2$ is just the expected value of the random variable selecting an entry from the matrix A, if the rows and columns are chosen according to the distributions θ_1 and θ_2. Because A is set up over the set $\{0,1\}$, this is essentially the expectation of an indicator variable, and therefore nothing else than a probability. By construction, we therefore have

$$\mathsf{P}(\text{successful transmission}) = v(A), \tag{1}$$

assuming a zero-sum competition. In case that the adversary does not play a zero-sum regime, the equality changes into a lower-bound to the probability (this can be proven by twice-exploitation of the saddle-point property of the Nash-equilibrium; cf. Rass & Schartner (2010b)).

Carrying out the above sketched method for all path selections and possibly compromised nodes, we end up with a 34×21-matrix. In doing so, we notice that some rows are element-wise greater or equal than others, so we can delete the respective "smaller" rows, because these are obviously suboptimal strategies (as the alternative will give better revenue in every case). Such a uniformly better strategy is said to *dominate* the other one. Analogously, from the adversary's point of view, we can delete all columns for which another column gives less utility in every row, because the latter strategy is obviously a better way of attacking. Repeating this reduction, we end up with a 5×6-matrix and corresponding strategies as shown in Figure 7. The core concept introduced by Rass & Schartner (2010b) is the *vulnerability*, defined as the difference between the maximum possible outcome and the average outcome. Formally, the vulnerability $\rho(A) := 1 - v(A)$ for a (zeros-sum) game-matrix $A \in \{0,1\}^{n \times m}$. Based on this quantity, the following result has been obtained. Notice that Theorem 4.1 *does not* assume a zero-sum competition, i.e. the adversary is not bound to behave according to a Nash-equilibrium.

Theorem 4.1 (Rass & Schartner (2010b)). *Let Alice and Bob set up their matrix (game) with binary entries $a_{ij} \in \{0,1\}$, where $a_{ij} = 1$ if and only if a message can securely be delivered by choosing the i-th (set of) paths, and the adversary uses his j-th strategy of attacking. Then $\rho(A) \in [0,1]$, and*

1. *if $\rho(A) < 1$, then a protocol exists upon which Alice and Bob can secretly communicate with an eavesdropping probability of at most ε for any $\varepsilon > 0$ (arbitrarily small).*
2. *if $\rho(A) = 1$, then the probability of the message becoming extracted by the adversary is 1.*

Summarizing this result, we can say that perfectly secure transmission is possible if and only if $v(A) > 0$ for a game-matrix A modeling the underlying multipath transmission scenario. Notice that this generalizes previous results due to Ashwin Kumar et al. (2002) and Wang & Desmedt (2008) along these lines.

Generalized risk management

If we work through the above arguments carefully, we observe that neither the theory nor its results hinge on the binary scale for setting up the game-matrices. It turns out that we can fill in any meaningful number in the slots of the game-matrix. Hence, we can use discrete scales modeling nominal valuation of messages, say a classification in terms of "public" (i.e. no particular protection required), "confidential" (protection is required) or "top secret" (eavesdropping would have devastating consequences). Also, one can use a continuous scale $[a,b]$ with $a,b > 0$ to directly associate the monetary loss suffered from a message that falls into the adversary's hands. In other words, we can equally well set up the game with a utility functional that gives the monetary value of a secretly delivered message, or 0 otherwise (in case of eavesdropping). The *vulnerability* in this case is the monetary loss suffered when communicating valuable data over the network. Rephrasing this differently, the vulnerability directly equals the decision-theoretic risk.

A valuable application of such quantitative risk assessment is the design of quantum networks. As the technology has reached a state of maturity that permits thinking about globally spanning networks, a considerable number of research articles (Alleaume et al. (2009); Dianati et al. (2008); Elliott et al. (2005); Fernandez et al. (2007); Kumavor et al. (2006); Le et al. (2008); Rass & Schartner (2009); Tang et al. (2006) and many more), as well as several patents (by Elliott (2008a) and Elliott (2008b) among others) have arisen. An economic implementation of such networks can be tackled from various directions. One approach is presented by Alleaume et al. (2009), where the network topology is optimized to provide best performance, assuming that security is retained by secure point-to-point connections. In particular, this article employs the trusted node relay and optimizes the costs for building a secure network on this paradigm. In contrast to this, the approach presented by Rass & Schartner (2009) aims at squeezing out a maximal level of secrecy, assuming that point-to-point connections are perfectly secure. This approach is more focused on maximizing security with given environmental constraints. We believe that a successful roll-out of such networks amounts to a highly constrained optimization problem that has to account for both, topological aspects (to be tackled with stochastic geometry, such as done by Alleaume et al. (2009)), as well as taking security not for granted by QKD itself, such as posed by Rass & Schartner (2009).

5. Authentication with and without pre-shared keys

It is easy to see that a quantum channel is only as secure as it is authentic. For otherwise, an adversary may easily become the person-in-the-middle acting as a proxy and reading

all the traffic through his node in plain text. Quantum cryptography is therefore often misunderstood as a method of creating a key "from nothing", while it is actually a method of "expanding" an already existing shared key. This pre-shared secret is required for authentication purposes, and the most common way of authenticating the channel is authenticating each message flowing over it. This approach is known as *continuous authentication*. Key-management for this form of authentication is involved, as the amount of produced key-material has to exceed the respective expenditure for authentication. Hence, the actual amount of key-material that is consumed for creating authentication tags crucially depends on the specific QKD protocol in charge. Gilbert & Hamrick (2000) provide a full-detailed discussion of the key-consumption for the BB84 and related protocols. The calculations are a matter of simple yet messy algebra. We leave this to the interested reader consulting the work of Gilbert & Hamrick (2000) for details. In the following, we shall sketch an alternative way of authentication that is compatible with the game-theoretic risk-management approach sketched in Section 4.

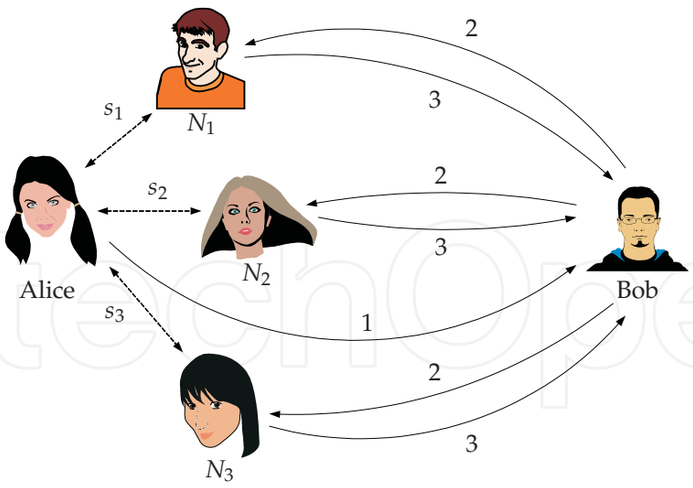
The idea of PGP's web-of-trust can be rephrased into setting up a threshold authentication scheme based on shared secrets between adjacent nodes and not requiring any end-to-end shared secrets (cf. Rass & Schartner (2010a)). If Alice wishes to authenticate a message for Bob, without having a secret in common with him, she may use her current or past direct neighbors to prove her reputation. Notice that this scheme is easily transferred to a *wireless* setting too: suppose that Alice's neighborhood looks as sketched in Figure 8. Because she does not have any secret with Bob in common, her only way of proving her reputation to Bob is by having her neighbors confirm her identity to Bob. Let a general message authentication code be given by a mapping $MAC : \{0,1\}^* \times \{0,1\}^{l_1} \to \{0,1\}^{l_2}$ that takes a message m of arbitrary length and a key of length l_1, returning a MAC of length l_2. We denote the MAC for m with key s by $MAC(m,s)$. Furthermore, let $H : \{0,1\}^* \to \{0,1\}^{l_3}$ be any collision-resistant cryptographic hash function (e.g. SHA-256).

To let Alice's neighbors confirm her identity without telling them the message m that is intended for Bob, Alice authenticates the hash-value $H(m)$ instead of m, so that Bob can present $H(m)$ to the neighbors to let them check the MACs that he received from Alice. The verification is done over disjoint paths, and he accepts if and only if all verifications come back positive.

Security

We assume the hash-function H collision-resistant, as well as the MAC to be secure in the sense of permitting a negligible chance of forgery, if we choose a universal hash-family for both purposes. Appropriate constructions are given by Krawczyk (1994), Shoup (1996) and Bierbrauer (1998) for instance. We therefore focus on the threshold property, taking the threshold t of the adversary into account. Let Alice have attached k MACs for her message. It is easy to see that if $t \geq k$, then the adversary can conquer and control all of Alice's neighbors thus successfully fooling Bob into thinking a forged message is authentic. On the other hand, if $t < k$, then at least one verification will reveal the impersonation, and Bob will reject the message as not coming from Alice.

Similarly as for a multipath transmission scenario, we require node-disjoint paths here too. Alas, graphs with sufficiently strong connectivity are rarely found in real-life infrastructures. At this point, we can re-use the ideas described in Section 4: just as for multipath transmission, it is equally trivial to set up a similar matrix over $\{0,1\}$, storing a "1" for a successful



Initialization:
Alice shares secrets $s_1, \ldots, s_k$ with her neighboring nodes $N_1, \ldots, N_k$.
Protocol:

1.	Alice $\rightarrow$ Bob	$(m, MAC(H(m),s_1), MAC(H(m),s_2) \ldots, MAC(H(m),s_k))$
2.	Bob $\rightarrow N_1$	$(H(m), MAC(H(m),s_1))$
	Bob $\rightarrow N_2$	$(H(m), MAC(H(m),s_2))$
	$\vdots$	
	Bob $\rightarrow N_k$	$(H(m), MAC(H(m),s_k))$
3.	$N_1, \ldots, N_k \rightarrow$ Bob	each neighbor responds with either "OK" or failure ("NOK")

Bob accepts if all verifications come back OK

Fig. 8. Threshold authentication protocol and example

authentication and "0" for a successful impersonation attack. An analogue result as Theorem 4.1 can be stated for this kind of authentication too:

Theorem 5.1 (Rass & Schartner (2010a))**.** *Let A denote the matrix, modeling the authentication game as described above, and let Alice share secrets of length l with $n > 1$ neighbors of hers, but no secret with Bob is shared. If $\rho(A) < 1$, then Alice can transmit a message to Bob in an authentic manner, where the probability of forgery is less than 2^{-l}. If $\rho(A) = 1$, then the adversary can forge messages with probability 1.*

We draw almost an analogous conclusion as before: perfectly secure authentication is possible, if and only if $v(A) > 0$ for the game-matrix A modeling the authentication in the way as described above.

6. Outlook: Towards mobile and Ad-hoc QKD networks

The question, regarding the possibility of mobile or ad-hoc quantum networking, is perhaps the most promising one, which if it can be answered positively, would drastically increase the call for QKD in daily work environments. Sheikh et al. (2006) discuss various QKD-algorithms in terms of their applicability in a wireless setting. In particular, they consider attenuation and losses in the atmosphere, and report on various environmental influences that free-space QKD may suffer from. Interestingly, the first demonstration of QKD has been using a wireless channel with about 30 cm distance between the sender and the receiver. Using strongly

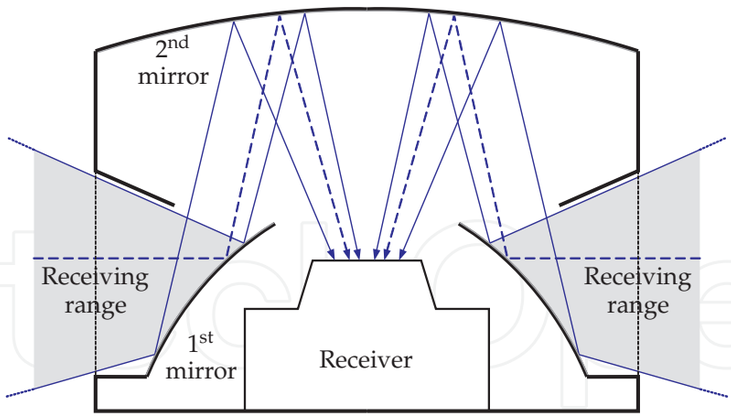


Fig. 9. Table-mounted omnidirectional Receiver

attenuated laser pulses, distances of 500 m have been bridged, as reported by Weier et al. (2006). Hughes et al. (2002) described experiments over a distance of 10 km at daylight and at night, and Kurtsiefer et al. (2002) demonstrated the possibility of globally spanning networks. Studies regarding QKD between a terrestrial station and an orbit satellite have been conducted by Rarity et al. (2002) and Pfennigbauer & Leeb (2003). Experimental implementations covering a distance of about 144 km have been reported by Schmitt-Manderbach et al. (2007).

Free-Space QKD in the standard form requires a straight line of sight connection. It is thus fair to assume that the connection may be temporarily unavailable and in possible misalignment for short periods of time, particularly in a mobile ad-hoc environment. We could therefore focus on wireless networks with (almost) static participants. Such peers naturally arise in any environment where environmental conditions disallow using cables of any kind. Newly created networks within buildings, within or between cities or spanning mountainous terrain are only some examples, not to mention communication among geostationary satellites. Transferring the techniques to a mobile environment, however, is indeed possible, as the key-establishment can run entirely decoupled from the encryption process. A simple approach is loading a mobile device with key material for subsequent encryption, and then cut the quantum channel. Kollmitzer & Pivk (2010) further elaborate on this. A much simpler application of QKD in an in-door environment, the receiver that might be placed in the middle of a conference table (Figure 9) could be built similar to an omnidirectional (surveillance) camera. This could make QKD feasible even in a wireless setting within buildings.

7. Conclusion

Quantum key distribution has reached a level of maturity that renders a vast range of applications in sight. However, while the basic technology has been studied extensively, most solutions remain focused on perfect point-to-point security. Careful management of keys created by QKD is vital to any application, building upon a quantum network infrastructure, because end-to-end security, authenticity and availability cannot be assured by QKD alone. Here, we surveyed a selection of ideas related to the management of quantum networks, covering various topics such as failure and recovery management, general end-to-end security and risk-management, as well as authentication and possible applications in the wireless setting. Quantum key distribution is for sure a promising direction of research, in fact a key technology of upcoming decades. Nevertheless, it is only another brick in the wall which cannot by itself do all the protection. It is the combination of mechanisms (and QKD is only

one of them), that makes the defense against an adversary strong. Key-management is another often neglected but nevertheless important building block for a successful defense. In the public-key domain, its importance has been widely recognized. In the quantum domain, the issue remains equally important, but seemingly has not yet received the full amount of attention that it deserves.

8. References

Al-Riyami, S. S. & Paterson, K. G. (2003). Certificateless public key cryptography, *ASIACRYPT*, pp. 452–473.

Alleaume, R., Roueff, F., Diamanti, E. & Lütkenhaus, N. (2009). Topological optimization of quantum key distribution networks, *New Journal of Physics* 11: 075002.

Ashwin Kumar, M., Goundan, P. R., Srinathan, K. & Pandu Rangan, C. (2002). On perfectly secure communication over arbitrary networks, *PODC '02: Proceedings of the twenty-first annual symposium on Principles of distributed computing*, ACM, New York, NY, USA, pp. 193–202.

Bennett, C. & Brassard, G. (1984). Public key distribution and coin tossing, *IEEE International Conference on Computers, Systems, and Signal Processing*, IEEE Press, Los Alamitos, pp. 175–179.

Berlekamp, E. & Welch, L. (1986). Error correction of algebraic block codes, US Patent Nr. 4,633,470.

Berzanskis, A. & Gelfond, R. (2009). Key management and user authentication for quantum cryptography networks. IPC8 Class: AH04L906FI, USPC Class: 380277.

Bierbrauer, J. (1998). Authentication via algebraic-geometric codes, *Rend. Circ. Mat. Palermo (2) Suppl.* 51: 139–152.

Buchmann, J., Coronado, C., Döring, M., Engelbert, D., Ludwig, C., Overbeck, R., Schmidt, A., Vollmer, U. & Weinmann, R.-P. (2004). Post-quantum signatures, Cryptology ePrint Archive, Report 2004/297.

Damgård, I. B., Fehr, S. & Salvail, L. (2004). Zero-knowledge proofs and string commitments withstanding quantum attacks, *in* M. Franklin (ed.), *Advances in Cryptology (CRYPTO)*, LNCS 3152, pp. 254–272.

Dianati, M., Alleaume, R., Gagnaire, M. & Shen, X. (2008). Architecture and protocols of the future european quantum key distribution network, *Security And Communication Networks* 1: 57–74.

Dür, W., Briegel, H.-J., Cirac, J. I. & Zoller, P. (1999). Quantum repeaters based on entanglement purification, *Phys. Rev. A* 59(1): 169–181.

Elliott, B. B. (2008a). Key distribution center for quantum cryptographic key distribution networks.
URL: *http://www.freepatentsonline.com/7457416.html*

Elliott, B. B. (2008b). Quantum cryptographic key distribution networks with untrusted switches.

Elliott, C. (2004). The DARPA Quantum Network, *ArXiv Quantum Physics e-prints* .
URL: *http://adsabs.harvard.edu/abs/2004quant.ph.12029E*

Elliott, C. (2007). The DARPA quantum network. arXiv:quant-ph/0412029v1.

Elliott, C., Colvin, A., Pearson, D., Pikalo, O., Schlafer, J. & Yeh, H. (2005). Current status of the DARPA quantum network, arXiv:quant-ph/0503058v2.

Escrowed Encryption Standard (1994). Federal Information Processing Standards (Publication 185).

Fernandez, V., Collins, R. J., Gordon, K. J., Townsend, P. D. & Buller, G. S. (2007). Passive optical network approach to gigahertz-clocked multiuser quantum key distribution, *IEEE Journal Of Quantum Electronics* 43(2): 130–138.

Fitzi, M., Franklin, M. K., Garay, J. & Vardhan, S. H. (2007). Towards optimal and efficient perfectly secure message transmission, *in* S. Vadhan (ed.), *4th Theory of Cryptography Conference (TCC)*, Lecture Notes in Computer Science LNCS 4392, Springer, pp. 311–322.

Gilbert, G. & Hamrick, M. (2000). Practical quantum cryptography: A comprehensive analysis (part one).
URL: *http://www.citebase.org/abstract?id=oai:arXiv.org:quant-ph/0009027*

Goldreich, O. (2008). *Computational Complexity*, Cambridge University Press.

Hirt, M. (2001). *Multi-Party Computation: Efficient Protocols, General Adversaries, and Voting*, PhD thesis, ETH Zürich.

Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G. (2002). Practical free-space quantum key distribution over 10 km in daylight and at night, *New Journal of Physics* 4: 43.1–43.14.

Hwang, T., Lee, K.-C. & Li, C.-M. (2007). Provably secure three-party authenticated quantum key distribution protocols, *IEEE Transactions On Dependable And Secure Computing* 4(1): 71–80.

ID Quantique (2011). Website of "CERBERIS – A fast and secure solution: high speed encryption combined with quantum key distribution". http://www.idquantique.com/network-encryption/cerberis-layer2 -encryption-and-qkd.html (last access: September 27th, 2011).

Jin, X.-R., Ji, X., Zhang, Y.-Q., Zhang, S., Hong, S.-K., Yeon, K.-H. & Um, C.-I. (2006). Three-party quantum secure direct communication based on GHZ states, *Physics Letters A* 354(1-2): 67–70.

Kaabneh, K. & Al-Bdour, H. (2005). Key Exchange Protocol in Elliptic Curve Cryptography with No Public Point, *American Journal of Applied Sciences* 2(8): 1232–1235.

Kollmitzer, C. & Pivk, M. (eds) (2010). *Applied Quantum Cryptography*, Lecture Notes in Physics 797, Springer.

Krawczyk, H. (1994). LFSR-based hashing and authentication, *CRYPTO '94: Proceedings of the 14th Annual International Cryptology Conference on Advances in Cryptology*, Springer, London, UK, pp. 129–139.

Kumavor, P. D., Beal, A. C., Donkor, E. & Wang, B. C. (2006). Experimental multiuser quantum key distribution network using a wavelength-addressed bus architecture, *Journal Of Lightwave Technology* 24(8): 3103–3106.

Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R. & Rarity, J. G. (2002). A step towards global key distribution, *Nature* 419(2): 450.

Le, Q.-C., Bellot, P. & Demaille, A. (2008). *Information Security Practice and Experience*, Springer, chapter Towards the World-Wide Quantum Network, pp. 218–232.

Los Alamos National Security (2009). Quantum cryptography roadmap, *Technical report*, Los Alamos National Security. http://qist.lanl.gov/qcrypt_map.shtml (last accessed: September 27th, 2011).

Mink, A., Frankel, S. & Perlner, R. (2009). Quantum key distribution (qkd) and commodity security protocols: Introduction and integration, *International Journal of Network Security & Its Applications (IJNSA)* 1(2): 101–112.

Mink, A., Ma, L., Nakassis, T., Xu, H., Slattery, O., Hershman, B. & Tang, X. (2008). A quantum network manager that supports a one-time pad stream, *Proceedings of the second*

International Conference on Quantum, Nano and Micro Technologies, IEEE Computer Society Press, pp. 16–21.

Paterson, K.G. and Piper, F. and Schack, R. (2004). Why Quantum Cryptography?, http://eprint.iacr.org/2004/156.pdf.

Peev, M., Pacher, C., Alleaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J. F., Fasel, S., Fossier, S., Furst, M., Gautier, J. D., Gay, O., Gisin, N., Grangier, P., Happe, A., Hasani, Y., Hentschel, M., Hubel, H., Humer, G., Länger, T., Legre, M., Lieger, R., Lodewyck, J., Lorünser, T., Lütkenhaus, N., Marhold, A., Matyus, T., Maurhart, O., Monat, L., Nauerth, S., Page, J. B., Poppe, A., Querasser, E., Ribordy, G., Robyr, S., Salvail, L., Sharpe, A. W., Shields, A. J., Stucki, D., Suda, M., Tamas, C., Themel, T., Thew, R. T., Thoma, Y., Treiber, A., Trinkler, P., Tualle-Brouri, R., Vannel, F., Walenta, N., Weier, H., Weinfurter, H., Wimberger, I., Yuan, Z. L., Zbinden, H. & Zeilinger, A. (2009). The SECOQC quantum key distribution network in vienna, *New Journal of Physics* 11(7): 075001. URL: *http://dx.doi.org/10.1088/1367-2630/11/7/075001*

Pfennigbauer, M. & Leeb, W. R. (2003). Free-space optical quantum key distribution using intersatellite links, *Proceedings of the CNES Intersatellite Link Workshop*.

Poppe, A., Peev, M. & Maurhart, O. (2008). Outline of the SECOQC Quantum-Key-Distribution network in vienna, *International Journal of Quantum Information* 6(2): 209–218.

Quantum (2009). Scalar key manager. http://quantum.com/products/tapelibraries/scalarkeymanager/index.aspx, (last access: September 27th, 2011).

Rarity, J., Tapster, P., Gorman, P. & Knight, P. (2002). Ground to satellite secure key exchange using quantum cryptography, *New Journal of Physics* 4: 82.1–82.21.

Rass, S. (2009). *On Information-Theoretic Security: Contemporary Problems and Solutions*, PhD thesis, Klagenfurt University, Institute of Applied Informatics.

Rass, S. & Schartner, P. (2009). Security in quantum networks as an optimization problem, *Proceedings of the International Conference on Availability, Reliability and Security*, pp. 493–498.

Rass, S. & Schartner, P. (2010a). Multipath authentication without shared secrets and with applications in quantum networks, *Proceedings of the International Conference on Security and Management (SAM)*, Vol. 1, CSREA Press, pp. 111–115.

Rass, S. & Schartner, P. (2010b). A unified framework for the analysis of availability, reliability and security, with applications to quantum networks, *IEEE Transactions on Systems, Man, and Cybernetics – Part C: Applications and Reviews* 40(5): 107–119.

Salvail, L., Peev, M., Diamanti, E., Alleaume, R., Lütkenhaus, N. & Länger, T. (2009). Security of trusted repeater quantum key distribution networks, `arXiv:0904.4072v1 [quant-ph]`.

Schartner, P. & Rass, S. (2009). How to overcome the trusted node model in quantum cryptography, *Proceedings of the 12th IEEE International Conference on Computational Science and Engineering*, Los Alamitos, California, pp. 259–262.

Schartner, P. & Rass, S. (2010). Quantum key distribution and denial-of-service: Using strengthened classical cryptography as a fallback option, *Proceedings of ICS 2010 Workshop of Information Security*, IEEE, pp. 131–136.

Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J. G., Zeilinger, A. & Weinfurter, H. (2007). Experimental demonstration of free-space decoy-state quantum key distribution

over 144 km, *Physical Review Letters* 98(1): 010504.
URL: *http://link.aps.org/abstract/PRL/v98/e010504*

Shamir, A. (1979). How to share a secret, *Commun. ACM* 22(11): 612–613.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes, *Proceedings of CRYPTO 84 on Advances in cryptology*, Springer-Verlag New York, Inc., New York, NY, USA, pp. 47–53.

Shannon, C. (1949). Communication theory of secrecy systems, *Bell System Technical Journal* 28: 656–715.

Sheikh, K. H., Hyder, S. S. & Khan, M. M. (2006). An overview of quantum cryptography for wireless networking infrastructure, *CTS '06: Proceedings of the International Symposium on Collaborative Technologies and Systems*, IEEE Computer Society, Washington, DC, USA, pp. 379–385.

Shor, P. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Journal on Computing* 26: 1484–1509.

Shoup, V. (1996). On fast and provably secure message authentication based on universal hashing, *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, Springer-Verlag, London, UK, pp. 313–328.

SwissQuantum (2011). Key management layer. http://www.swissquantum.com/?-Key-Management-Layer (last access: September 27th, 2011).

Tanaka, A. andMaeda, W., Takahashi, S., Tajima, A. & Tomita, A. (2008). Randomize technique for quantum key and key management system for use in qkd networks, *SECOQC Demonstration Conference*.

Tang, X., Ma, L., Mink, A., Nakassis, A., Xu, H., Hershman, B., Bienfang, J., Su, D., Boisvert, R. F., Clark, C. & Williams, C. (2006). Demonstration of an active quantum key distribution network, *Technical report*, National Institute of Standards and Technology.

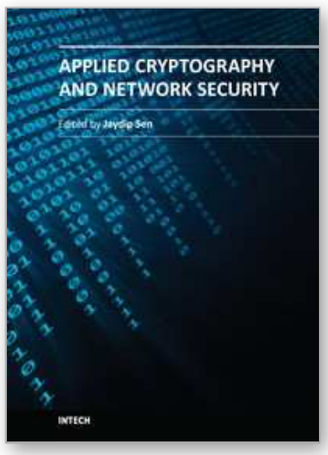
Wang, Y. & Desmedt, Y. (2008). Perfectly secure message transmission revisited, *IEEE Transactions on Information Theory* 54(6): 2582–2595.

Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C. & Weinfurter, H. (2006). Free space quantum key distribution: Towards a real life application, *Fortschritte der Physik* 54(8-10): 840–845.

Wiesner, S. (1983). Conjugate coding, *Sigact News* 15(1): 78–88. original manuscript written circa 1970.

Wootters, W. K. & Zurek, W. H. (1982). A single quantum cannot be cloned, *Nature* 299(802): 802–803.

Yuan, Z.-S., Chen, Y.-A., Zhao, B., Chen, S., Schmiedmayer, J. & Pan, J.-W. (2008). Experimental demonstration of a BDCZ quantum repeater node, *Nature* 454: 1098–1101.



Applied Cryptography and Network Security

Edited by Dr. Jaydip Sen

ISBN 978-953-51-0218-2

Hard cover, 376 pages

Publisher InTech

Published online 14, March, 2012

Published in print edition March, 2012

Cryptography will continue to play important roles in developing of new security solutions which will be in great demand with the advent of high-speed next-generation communication systems and networks. This book discusses some of the critical security challenges faced by today's computing world and provides insights to possible mechanisms to defend against these attacks. The book contains sixteen chapters which deal with security and privacy issues in computing and communication networks, quantum cryptography and the evolutionary concepts of cryptography and their applications like chaos-based cryptography and DNA cryptography. It will be useful for researchers, engineers, graduate and doctoral students working in cryptography and security related areas. It will also be useful for faculty members of graduate schools and universities.

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen