Chapter 1

Security of Quantum Key Distribution Protocols

Mhlambululi Mafu and Makhamisa Senekane

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.74234

Abstract

Quantum key distribution (QKD), another name for quantum cryptography, is the most advanced subfield of quantum information and communication technology (QICT). The first QKD protocol was proposed in 1984, and since then, more protocols have been proposed. It uses quantum mechanics to enable secure exchange of cryptographic keys. In order to have high confidence in the security of the QKD protocols, such protocols must be proven to be secure against any arbitrary attacks. In this chapter, we discuss and demonstrate security proofs for QKD protocols. Security analysis of QKD protocols can be categorised into two techniques, namely infinite-key and finite-key analyses. Finite-key analysis offers more realistic results than the infinite-key one, while infinite-key analysis provides more simplicity. We briefly provide the background of QKD and also define the basic notion of security in QKD protocols. The cryptographic key is shared between Alice and Bob. Since the key is random and unknown to an eavesdropper, Eve, she is unable to learn anything about the message simply by intercepting the ciphertext. This phenomenon is beyond the ability of classical information processing. We then study some tools that are used in the derivation of security proofs for the infinite- and finite-length key limits.

Keywords: quantum cryptography, QKD, protocols, security, finite-security, entanglement, QKD schemes

1. Introduction

Quantum cryptography, specifically QKD, has been built based on physical concepts associated with quantum mechanics. In contrast to conventional cryptography, whose security is based on the complex computational and mathematical algorithms for security, it is founded on the uncertainty relations, Bell's inequalities, entanglement or non-locality [1]. The implementation of QKD consists of detectors, repeaters, quantum memories and decoy states [2–4]. These concepts form the basis of security proofs [5]. In order for Eve to obtain the secret key,

she needs to break the laws of physics, but this is impossible without her presence being detected. Since there is great need for security in a communication system, it is necessary to investigate security proofs for QKD systems.

Regardless of the challenges that come with developing unconditional security proofs, a lot of progress has been realised in the last two decades. An unconditional security proof considers all kinds of attacks that Eve can perform and incorporating this into the security proof is a difficult task. However, a new technique for analysing collective attacks due to an eavesdropper was developed in 1995 by Yao [6]. Later, Bennett et al. realised that if the legitimate parties possess a reliable quantum computer, they can implement an entanglement distillation (ED) protocol to obtain a secure version of an EB key distribution [7]. In 1998, based on this idea, Lo and Chau then developed a formal security proof for the protocol [8]. By using the ideas of Mayers, Lo and Chau then Shor and Preskill developed a simple proof of security for the BB84 protocol in 2000 [9]. This was followed by a proof of Biham who was the second to show an unconditional security proof [10]. In 1991, Biham's proof was then used by Gottesman and Preskill to prove the unconditional security proof of a continuous variable protocol where Alice's signals are sufficiently squeezed [11]. In the same spirit, Inamori et al. showed the unconditional security proof of BB84 protocol where Alice's source emits weak coherent states and Bob's detector remains uncharacterised [12]. However, a complete security proof that is secure against arbitrary attacks by the eavesdropper and full realistic implementation of the QKD protocol remains missing. But this progress depicts that major achievements have been made in this field to prove that protocols used in quantum communication are secure for sending messages. Amongst different approaches to security proofs, a number of publications on composable security [13], de Finetti's theorem [5, 14], post-selection technique [15] and recently the finite-length key analysis [16] are now available.

Regardless of enormous progress that has been made in QKD, there are still some theoretical and experimental problems of communicating in absolute secrecy in the presence of an eavesdropper. In particular, matching the theoretical security proofs to real devices still remains unknown. The security proofs still contain assumptions concerning the behaviour of devices used by the communicating parties [17]. As a result of this mismatch, an eavesdropper can learn part of the key shared by Alice and Bob, thus rendering some schemes insecure over large distances. Moreover, the existing security proofs have been derived in the asymptotic limit which is not very realistic. In fact, the bits which are processed in QKD are necessarily of finite length. Therefore, thanks to Valerio and Renner for introducing the general framework for the security analysis of QKD with finite resources [16]. The security study is mainly based on the framework introduced by Devetak-Winter, Csiszar-Körner and Renner security [5, 18]. For a detailed overview of QKD, we refer the reader to [2, 4].

2. Quantum features

2.1. Detection of measurements

Based on the measurement postulate of quantum mechanics [19], it is impossible to perform a measurement on an unknown quantum state without introducing a disturbance unless the

state is an eigenstate to the observable being measured [20]. This means that Eve is unable to perform a measurement on an unknown quantum state without introducing a disturbance that can be discovered by Alice and Bob.

2.2. Uncertainty principle

The uncertainty principle states that a measurement of one quantum observable intrinsically creates an uncertainty in other properties of the system. This means that it is impossible to measure the simultaneous values of non-commuting observables on a single copy of a quantum state [21]. This ensures that an eavesdropper cannot perform measurements that leave the quantum state undisturbed [22]. This automatic detection of an eavesdropper is impossible with classical cryptography.

2.3. No-cloning theorem

In quantum mechanics, it is impossible to make a perfect copy of an unknown state with perfect fidelity. This is called the no-cloning theorem [23]. This prevents an eavesdropper from simply intercepting the communication channel and making copies (so as to make measurements on them later) of the transmitted quantum states, while passing on an undisturbed quantum state to Bob [24, 25]. Therefore, the no-cloning theorem forms an important property in the security of QKD protocols [26].

2.4. Non-orthogonality principle

Suppose, we have quantum states $|\psi_i\rangle$ which are not orthogonal, then it can be proved that there exists no quantum measurement that is able to distinguish states [19]. In this case, a non-zero component of the state $|\psi_1\rangle$ parallel to the state $|\psi_2\rangle$ always gives a non-zero probability of the measurement outcome associated with the state $|\psi_2\rangle$ also occurring when the measurement is applied to the state $|\psi_1\rangle$. This is because $|\psi_2\rangle$ can be decomposed into a non-zero component parallel to $|\psi_1\rangle$ and a component orthogonal to $|\psi_1\rangle$. Then, there is no measurement of any kind that can reliably determine which of the two non-orthogonal quantum states were measured [27]. This feature is very useful for cryptographic applications such as QKD [20].

3. QKD schemes

There are two major types of QKD schemes, namely prepare and measure (P&M) and entanglement-based (EB) schemes [2, 4]. A P&M scheme is based on individual qubits, while an EB scheme is based on entangled qubits. Either of these schemes can be used by two parties in order to end up with a shared secret key. However, a P&M scheme can immediately be translated into an EB scheme [4, 28]. However, there exists another family of protocols called continuous-variable protocols and distributed-phase-reference (DPR) protocols [4], which consist of the coherent-one-way protocol [29, 30] and the distributed-phase-reference protocols [31, 32]. In the following sections, we briefly describe the processes for each scheme.

3.1. Prepare and measure (P&M) scheme

In a P&M scheme, Alice encodes some classical information into a set of quantum states and sends them via an insecure quantum channel to Bob. Bob then performs measurements on the quantum states he receives. This results in classical data generated by quantum means being shared between Alice and Bob. Examples of protocols that use this scheme are BB84 [33], B92 [27], six-state [34] and SARG04 [35] protocols.

3.2. Entanglement-based (EB) scheme

In an EB scheme, a source prepares and distributes a maximally entangled quantum state where one system is sent to Alice and another to Bob. Alice and Bob then perform measurements in two mutually unbiased bases on their system, respectively. Upon measurement, they obtain perfectly correlated outcomes which are completely random. Since the source prepares a pure state, it means that this state cannot be correlated with an eavesdropper. This implies secrecy of the key. An example of a protocol which uses this scheme is the E91 protocol [36].

4. QKD procedure

In this section, we describe what happens in a P&M scheme, specifically in the BB84 protocol [33]. In this protocol, Alice and Bob are connected by two communication channels, namely an insecure quantum channel and an authenticated classical channel [2]. The quantum channel is used for the transmission of qubits and is controlled by the eavesdropper. The classical channel is authenticated so that the eavesdropper can only listen to the communication but cannot alter the messages being transmitted. This ensures that Alice and Bob can prove that they are communicating between each other. Otherwise, an eavesdropper could simply block all quantum and classical communication between Alice and Bob and perform QKD with Alice while taking on Bob's role and vice versa. Therefore, Alice and Bob have to identify each message they send as originating from themselves before any post-processing can begin.

4.1. Quantum phase

In the quantum phase, Alice and Bob make use of the quantum channel. They employ the quantum mechanical signals (i.e. qubits) and they also perform measurements. Three sub-protocols take place which are as follows:

a. Signal preparation: Alice prepares a random sequence of strings which are drawn from a set of four signal states and encodes each bit value in the state of a quantum system. The basis states are horizontal, vertical, diagonal and anti-diagonal.

b. Transmission: The encoded quantum system is sent to Bob via the quantum channel.

c. Measurement: Bob applies a quantum measurement on the quantum system to decode a bit value. The signals are measured in a random sequence of polarisation bases, either in the horizontal/vertical or diagonal/anti-diagonal bases.

Afterwards, Alice keeps the record of signal choices; Bob keeps the record of his basic choices and the corresponding measurement results.

4.2. Classical phase

In this phase, Alice and Bob use some classical communication protocol in order to distil a secret key from their correlated data. They achieve this by means of a discussion over the authenticated classical channel. The key extraction procedure is described as follows:

a. Parameter estimation: Alice randomly chooses some fraction of her signal slots and announces for these slots to Bob which signal she sent. Bob announces the measurement he performed and the outcome which he obtains. Depending on the amount of errors which they obtain from their comparisons, they may also decide whether to continue or abort the protocol.

b. Sifting: In the sifting protocol, Alice and Bob announce the polarisation bases they used for the preparation of the signals and which bits are discarded. In order to prevent Eve from modifying the transmitted messages, Alice and Bob use the authentication scheme. The remaining data are called sifted data. Alice and Bob proceed to the reconciliation phase or error correction phase.

c. Key map: Alice and Bob discard the basis which they were using so that Eve may not learn any information about the encoding. During key map, Alice and Bob map their event records of the sifted data into a raw key. This step applies to prepare and measure protocol.

d. Error correction: The sifted data may still contain some errors; therefore, Alice and Bob execute a classical error correction protocol in order to reconcile their data. They need to exchange additional information about their respective data over the public channel. In addition, they need to authenticate this phase because Eve is still able to modify the messages in this step. As a result of this protocol, Alice and Bob agree now on a key which is identical with very high probability but Eve might still have some small additional information about the key. After this stage, privacy amplification takes place.

e. Privacy amplification: After Alice and Bob have reconciled their key, they can cut the correlations between their key and Eve by using the so-called privacy amplification. In this stage, Alice and Bob map their string via a special family of functions called universal hash functions to a shorter final key [5].

5. Security in QKD

5.1. Security definition

A good definition of security would allow the key generated by a QKD protocol to deviate by a small parameter ε, from a perfect key [2]. This definition should be able to bound Eve's knowledge about the final key. A perfect key refers to a uniformly distributed bit string whose value is completely independent and remains unknown to an eavesdropper [16]. The main requirement that the definition of security must fulfil is composability [5]. The composable

definition characterises the security of a protocol with respect to the ideal functionality. This means that the security of the key generated could be used in any subsequent cryptographic task such as the one-time pad for message encryption, where an ideal key is expected. However, there always exist some challenges in constructing security proofs without making any assumptions either about the devices or the parties. For example, attacks against practical schemes exist, such as photon-number-splitting attacks (PNS) [37], time-shift attacks [38], large pulse attacks [17, 39], blinding attacks [40] and high-power damage attack [41]. Some of the assumptions made in the definition of QKD security are as follows:

a. there should be no side channels. Side channels are basically discrepancies between the theoretical model and a practical implementation. They always exist if some information about the raw key is encoded in degrees of freedom not considered in the theoretical model. Therefore, this leads to a wrong assessment of the dimension of the Hilbert space which describes the protocol,

b. there should be access to perfect or almost perfect randomness (locally) and

c. quantum theory is correct and complete.

If there is randomness and quantum theory is correct, then this leads to completion of the security proofs. However, in classical cryptography, the security is based on the difficulty or complication of a certain mathematical algorithm to afford security of the protocol. Therefore, the security is mainly based on the failure to solve the algorithm. This can fail in four ways that are as follows:

a. conjecture of hardness/difficulty in this case is wrong,

b. underlying computation model could be wrong or could be unphysical,

c. the algorithm is easy for many instances and.

d. the computation could be small.

5.2. Security requirements

In this section, we follow closely the definitions in [5, 42]. A QKD protocol outputs a key SA on Alice's side and also a key SB on Bob's side. The length of the key is $l > 0$, otherwise no key is extracted. The length of the key depends on the noise level of the communication channel as well as security and on the correctness requirements of the protocol. Depending on the deviation of the output key from the ideal one, the protocol aborts in which case $S_A = S_B = \perp$ [42].

1. Correctness: A QKD protocol is called "correct", if, for any strategy by the eavesdropper $S_A = S_B$. This occurs whenever Alice and Bob output the classical keys S_A and S_B, respectively, such that $Pr[S_A \neq S_B] \leq \varepsilon_{cor}$. The term ε_{cor} is the maximum probability that the protocol deviates from the behaviour of the correct protocol. In order for correctness to be achieved, the QKD devices must perform what they are supposed to do according to a specified model. The devices generate the correct correlations which they are supposed to output, otherwise the protocol aborts. In other terms, the devices should not send any

other information to the outside world, in which it is not supposed to do (i.e. devices work according to their specification),

2. Secrecy: A random variable S drawn from the set S is said to be ε-secure with respect to an eavesdropper holding a quantum system E, if.

$$\min_{\in \sigma E} \frac{1}{2} \mathrm{tr}|\rho_{SE} - \rho_U \otimes \sigma_E| \leq \varepsilon, \tag{1}$$

where $\rho_{SE} = \sum_{s \in S} P_s(s)|s\rangle\langle s| \otimes \rho_E$ |S = s is the actual state that contains some correlations between the final key and Eve and ε gives the maximum failure probability of the key extraction process. The state $\rho_U = \sum_{s \in S} |s\rangle\langle s|/|S|$ is the completely mixed state on S and |S| is the size of S. Since the trace distance, that is, $\frac{1}{2}\mathrm{tr}|\rho_0 - \rho_1|$ refers to the maximum probability of distinguishing between the two quantum states (ρ_0,ρ_1), this composable security definition naturally gives rise to the operational meaning that the protocol is ε-secure, that is, S is identical to an ideal key U except with probability ε [5]. Again, according to Helstrom's Theorem, the probability of distinguishing between the two quantum states ρ_0 and ρ_1 is bounded by $\frac{1}{2} + \frac{1}{4}\,\mathrm{tr}|\rho_0 - \rho_1|$ [43].

3. Robustness: A QKD protocol is said to be "not robust" if the protocol aborts even though the eavesdropper is inactive. While correctness and secrecy are difficult to prove, robustness can simply be proven by running the protocol.

5.3. Infinite-length key security in QKD

Over the last decade, a lot of work in QKD has been devoted to the derivation of unconditional security proofs [8, 16, 44–47]. One of the main problems is that Eve has the power to perform any type of eavesdropping strategy. In particular, she can evade detection by attributing noise caused by her eavesdropping attack to normal noise in the channel. Therefore, it remains difficult to accurately bound the amount of information that Eve may obtain from the communication channel. The most important resource which should be determined when constructing security proofs for QKD protocols is the secret key rate. Therefore, all QKD protocols must be able to provide a clear expression for the secret key rate. In the asymptotic limit, the secret key rate is expressed as

$$r = \lim_{n \to \infty} \frac{l}{n}, \tag{2}$$

where l is the length of the final secret key and n is a list of symbols called r raw keys [2]. This rate was established by Devetak and Winter [18]. The secret key rate against collective attacks was derived by Kraus, Gisin and Renner [48] and is expressed as

$$r = I(X : Y) - \chi(X : E) \tag{3}$$

where I(X: Y) = H(X) − (X|Y) quantifies the amount of bits need to be satisfied for error correction. The term χ(X: E) = H(X) + S(E) − S(X, E) refers to the Holevo quantity, where H is

the Shannon entropy and S is the von Neumann entropy [49, 50]. The Holevo quantity refers to the amount of privacy amplification required in order to eliminate Eve's information.

The upper bound on the secret key rate r, can be expressed as.

$$r \leq I(A : B \downarrow E), \tag{4}$$

where I(A: B ↓ E) is the intrinsic conditional mutual information (intrinsic information for short) between two information sources held by Alice and Bob after Eve has performed an optimal individual attack [51]. The intrinsic information between two information sources A and B given E^- is defined as, $I(A : B \downarrow E) = \inf_{E^-} I(A : B|E^-)$, where the infimum is taken over all discrete random variables E such that $AB \rightarrow E \rightarrow E^-$ is a Markov chain [52]. It has been shown that I(A: B ↓ E) is an upper bound on the rate S = S(A;B||E) at which such a key can be extracted [51].

5.4. Finite-length key security

Many efforts have been made to improve the bounds on the secret key rates for a finite amount of resources [5, 16, 53–58]. Since the tools for analysing the security under non-asymptotic regime have become available, there is need to provide new security definitions. In this section, we follow closely the techniques demonstrated in [16] to discuss some of the parameters used in the security of QKD for finite-length key limit. The main goal of finite-length key security is to obtain a secret key rate r, based on a certain number of signals, a security parameter ε, and certain losses from the error correction without making any assumptions about the post processing (sifting, error correction and privacy amplification). For example, one can recognise that the limit in this expression of Eq. (2) is unrealistic because in all implementations of QKD protocols finite resources are used. This is because in this scenario, N is assumed to be large, that is, it approaches infinity, while in practice Alice and Bob exchange a limited number of symbols or signals. In the non-asymptotic limit, the secret key rate can be expressed as.

$$r = n/N[S_\xi(X|E) - \triangle - leak_{EC}/n]. \tag{5}$$

This shows that only a fraction of n out of N signals exchanged contributes to the key. This is because of the fact that m = N − n is used for parameter estimation thus leading the presence of a pre-factor of n/N. The expression S_ξ (X |E) takes into account the finite precision of the parameter estimation. Eve's information is calculated by using measured parameters, for example, error rates. In the finite-key scenario, these parameters are estimated on samples of finite length. The parameter △ is related to the security of privacy amplification. Its value is given by.

$$\triangle \equiv (2\log d + 3)\sqrt{[\log 2(2/\varepsilon)/n] + 2/n\log_2 1/\varepsilon_{PA}}, \tag{6}$$

where d is the dimension of the Hilbert space, ε^- is a smoothing parameter and ε_{PA} is the failure probability of the privacy amplification procedure. Eve's uncertainty is quantified by a generalised conditional entropy called the smooth min-entropy and is denoted as $H_{min}{}^{\varepsilon^-}(X^{(n)}|E^{(N)})$ [5]. The smoothing parameters, ε^- and ε_{PA}, are parameters which should be optimised

numerically. The square-root term corresponds to the speed of convergence of the smooth-min entropy, which is used to measure the key length of an identical and independently distributed (i.i.d) state toward the von Neumann entropy. In the asymptotic limit, the smooth-min entropy of an i.i.d state is equal to the von Neumann entropy. The second term ε_{PA} is directly linked to the failure probability of the privacy amplification procedure. Finally, $leak_{EC}/n$ corresponds to the amount of information which needs to be exchanged by Alice and Bob during the reconciliation phase. This quantity may not reach the Shannon limit, so $leak_{EC} \geq nH(X|Y)$. Typically,

$$leak_{EC} \approx f_{EC} H(X|Y) + 1/n \log_2(2/\varepsilon_{EC}), \tag{7}$$

where $f_{EC} > 1$ depends on the code and ε_{EC} refers to the failure probability of the error correction procedure.

Unlike in the asymptotic scenario, one needs to fix an overall security parameter ε for the QKD protocol. The parameter ε corresponds to the maximum probability failure that is tolerated on the key extraction protocol. This can be expressed as $\varepsilon = \varepsilon_{PE} + \varepsilon_{EC} + \bar{\varepsilon} + \varepsilon_{PA}$, where ε_{PE} is the error in the parameter estimation step and the other terms are as previously defined. All the parameters, ε_{PE}, ε_{EC}, $\bar{\varepsilon}$, ε_{PA}, can be independently fixed at arbitrarily low values.

As a result, the overall security parameter ε can be chosen arbitrarily small, to a value corresponding to Alice and Bob's wishes, but this comes at a cost of decreasing the final secret key rate. If m signals have been used to estimate the parameter λ, then the deviation of measurement outcomes λ_m obtained from measuring the m samples from the ideal estimate λ_∞ can be quantified by using the law of large numbers resulting [5, 59].

$$|\lambda_m - \lambda_\infty| \leq \xi(m, d) = \sqrt{[\ln(1/\varepsilon_{PE}) + d\ln(m+1)/2\, m]} \tag{8}$$

The objective of the privacy amplification step is to minimise the quantity of correct information which the eavesdropper may have obtained about Alice and Bob's reference raw key. After privacy amplification, the length of the raw key that remains will be.

$$l \leq H_{min}^{\varepsilon}(X|E) - 2\log_2(1/\varepsilon_{PA}), \tag{9}$$

where $H_{min}(X|E)$ expresses Eve's uncertainty and ε_{PA} is the error in the privacy amplification step.

6. Conclusion

In the general philosophy of proving the security of QKD protocols, standard methods are known to exist. However, these seem to fail for other classes of protocols, for example, the distributed phase reference protocols. In this chapter, we discussed that QKD is a technique, which uses the power of quantum mechanics to establish a string of random bits called a key. We also showed how the secret key is generated and shared between Alice and Bob. Since the key is random and unknown to an eavesdropper, Eve, she is unable to learn anything about

the message simply by intercepting the ciphertext. This phenomenon is beyond the ability of classical information processing.

In this chapter, we provided a background study of QKD and also defined the basic notion of security in QKD protocols. In particular, the tools for analysing the security proofs for both infinite- and finite-key QKD protocols were discussed and demonstrated. Further, we discussed that the finite-key analysis offers more realistic results than the infinite-key one, while the infinite-key analysis provides more simplicity.

Author details

Mhlambululi Mafu[1]* and Makhamisa Senekane[2]

*Address all correspondence to: mhlambululi.mafu@gmail.com

1 Department of Physics and Astronomy, Botswana International University of Science and Technology, Palapye, Botswana

2 Department of Physics and Electronics, National University of Lesotho, Roma, Lesotho

References

[1] Nielsen M, Chuang I. Quantum Computation and Quantum Information. Cambridge: Cambridge University Press; 2002

[2] Gisin N, Ribordy G, Tittel W, Zbinden H. Reviews of Modern Physics. 2002;**74**:145-195

[3] Lo HK, Ma X, Chen K. Physical Review Letters. 2005;**94**:230504

[4] Scarani V, Bechmann-Pasquinucci H, Cerf N, Dušek M, Lütkenhaus N, Peev M. Reviews of Modern Physics. 2009;**81**:1301-1350. ISSN 1539-0756

[5] Renner R. International Journal of Quantum Information. 2008;**6**:1-127

[6] Yao ACC. Proceedings of the Twenty-Seventh Annual ACM Symposium on Theory of Computing; 1995. pp. 67-75

[7] Bennett CH, Brassard G, Popescu S, Schumacher B, Smolin JA, Wootters WK. Physical Review Letters. 1996;**76**:722

[8] Lo HK, Chau HF. Science. 1999;**283**:2050-2056

[9] Shor PW, Preskill J. Physical Review Letters. 2000;**85**:441-444

[10] Biham E, Boyer M, Boykin PO, Mor T, Roychowdhury V. Journal of Cryptology. 2006;**19**: 381-439

[11] Gottesman D, Preskill J. Quantum Information with Continuous Variables. Amsterdam: Springer; 2003. pp. 317-356

[12] Inamori H, Lütkenhaus N, Mayers D. The European Physical Journal D-Atomic, Molecular, Optical and Plasma Physics. 2007;**41**:599-627

[13] Ben-Or M, Horodecki M, Leung D, Mayers D, Oppenheim J. In: Kilian J, editor. Theory of Cryptography: Second Theory of Cryptography Conference TCC 2005; vol. 3378 of Lecture Notes in Computer Science. Springer Verlag; 2005. pp. 386-406

[14] Renner R, Cirac J. Physical Review Letters. 2009;**102**:110504

[15] Christandl M, König R, Renner R. Physical Review Letters. 2009;**102**:20504

[16] Scarani V, Renner R. Physical Review Letters. 2008;**100**:200501

[17] Makarov V, teknisk-naturvitenskapelige universitet Institutt for elektronikk og telekommunikasjon N. Quantum Cryptography and Quantum Cryptanalysis. Department of Electronics and Telecommunications, Faculty of Information Technology, Mathematics and Electrical Engineering, Norwegian University of Science and Technology; 2007. ISBN 824711478X

[18] Devetak I, Winter A. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science. 2005;**461**:207-235

[19] Nielsen M, Chuang I, Grover L. American Journal of Physics. 2002;**70**:558

[20] Audretsch J. Entangled Systems: New Directions in Quantum Physics. New York: Wiley-VCH; 2007

[21] Deutsch D. Physical Review Letters. 1983;**50**(9):631-633. DOI: 10.1103/PhysRevLett.50.631

[22] Fuchs CA, Peres A. Physical Review A. 1996;**53**:2038-2045

[23] Wooters W, Zurek W. A single quantum cannot be cloned. Nature. 1982;**299**:802

[24] Bruss D, Leuchs G. Lectures on Quantum Information. New York: Wiley; 2007

[25] Peres A, Wootters W. Physical Review Letters. 1991;**66**:1119-1122

[26] Dieks D. Physics Letters A. 1982;**92**:271-272

[27] Bennett CH. Physical Review Letters. 1992;**68**(21):3121-3124. DOI: 10.1103/PhysRevLett.68.3121

[28] Meyer T. Finite key analysis in quantum cryptography [PhD Thesis]. Heinrich Heine University, Dsseldorf; 2007. http://d-nb.info/987330772. URL: http://docserv.uni-duesseldorf.de/servlets/DerivateServlet/Derivate-6444/thesis_noextras.pdf

[29] Stucki D, Fasel S, Gisin N, Thoma Y, Zbinden H. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 6583; 2007. p. 18

[30] Mafu M, Marais A, Petruccione F. Applied Mathematics & Information Sciences. 2014;**8**: 2769

[31] Inoue K, Waks E, Yamamoto Y. Physical Review Letters. 2002;**89**:037902

[32] Marais A, Konrad T, Petruccione F. Journal of Physics A: Mathematical and Theoretical. 2010;**43**:305302

[33] Bennett C, Brassard G. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175; Bangalore, India. 1984

[34] Bruß D. Physical Review Letters. 1998;**81**:3018-3021

[35] Scarani V, Acín A, Ribordy G, Gisin N. Physical Review Letters. 2004;**92**:057901

[36] Ekert A. Physical Review Letters. 1991;**67**:661-663

[37] Lütkenhaus N. Physical Reviews A. 2000;**61**(5):052304

[38] Qi B, Fung C, Lo H, Ma X. Quantum Information and Computation. 2007;**7**:073-082

[39] Vakhitov A, Makarov V, Hjelme D. Journal of Modern Optics. 2001;**48**:2023-2038

[40] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Nature Photonics. 2010;**4**:801-801

[41] Bugge AN, Sauge S, Ghazali AMM, Skaar J, Lyderseb L, Makarov V. Physical Review Letters. 2014;**112**:070503

[42] Tomamichel M, Lim CCW, Gisin N, Renner R. Nature Communications. 2012;**3**:634

[43] Helstrom CW. Journal of Statistical Physics. 1969;**1**:231-252

[44] Wolf S. Lectures on Data Security. Amsterdam: Springer; 1999. pp. 217-250

[45] Mayers D. Journal of the ACM (JACM). 2001;**48**:351-406

[46] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S, Sanpera A. Physical Review Letters. 1996;**77**:2818

[47] Tamaki K, Lo H. International Symposium on Information Theory, IEEE 2005. ISIT 2005. Proceedings. 2005. pp. 1603-1606. ISBN 0780391519

[48] Kraus B, Gisin N, Renner R. Physical Review Letters. 2005;**95**:80501

[49] Holevo A. Proceedings of the Second Japan-USSR Symposium on Probability Theory. Springer; 1973. pp. 104-119

[50] Holevo A. Probabilistic and Statistical Aspects of Quantum Theory. Amsterdam: Springer; 1982

[51] Christandl M, Renner R, Wolf S. IEEE International Symposium on Information Theory. 2003. pp. 258-258

[52] Maurer U, Wolf S. IEEE Transactions on Information Theory. 1999;**45**:499-514

[53] Hayashi M. Physical Review A. 2007;**76**:012329

[54] Cai R, Scarani V. New Journal of Physics. 2009;**11**:045024

[55] Sheridan L, Le TP, Scarani V. New Journal of Physics. 2010;**12**:123019

[56] Abruzzo S, Kampermann H, Mertz M, Bruß D. Physical Review A. 2011;**84**:032321

[57] Mafu M, Garapo K, Petruccione F. Finite-size key in the Bennett 1992 quantum key distribution for Renyi entropies. Physical Review A. 2013;**88**(6):1-4

[58] Mafu M, Garapo K, Petruccione F. Physical Review A. 2014;**90**:032308

[59] Cover TM, Thomas JA. Elements of Information Theory. New York: John Wiley; 1991

IntechOpen