QuintessenceLabs

WHITE PAPER

What is Quantum Key Distribution (QKD)?

Author(s):
Andrew Lance
John Leiseboer
Thomas Symul

Table of Contents

1. Document Scope

This document begins with an overview of classical encryption techniques followed by a detailed discussion of quantum key distribution (QKD).

2. Introduction

Cryptography provides methods to support confidentiality, authentication, and non-repudiation of messages and data. Some cryptographic methods require the use of a key, and therefore cryptography relies on sources of high-quality key material, as well as protocols for securely distributing the key material.

There are three types of security primitives [1]: unkeyed primitives, symmetric-key primitives, and public-key primitives.

a. Unkeyed primitives include arbitrary length hash functions, one-way permutations, and random sequences.
b. Symmetric-key primitives include symmetric-key block ciphers; symmetric-key stream ciphers; arbitrary length hash functions (MACs); signatures; pseudorandom sequences; identification primitives, and one-time pad encryptions.
c. Public-key primitives include public-key ciphers, signatures, and identification primitives.

Symmetric-key ciphers are generally used to keep information confidential, while public-key ciphers are often used for key exchange. Unkeyed primitives do not fulfil security objectives on their own but are often part of a security system or a cryptographic protocol.

Cryptography is widely used to protect information transferred across data and telecommunications networks, and data stored in files and databases. It is also used to ensure the integrity of information, and to identify the parties involved in communications exchanges.

In general, a cryptosystem consists of two or more parties who exchange information using cryptographic methods and protocols, and malicious parties who can eavesdrop or modify the information being exchanged. By convention, two parties exchanging information are referred to as “Alice” and “Bob,” and an eavesdropper referred to as “Eve.”

2.1 Symmetric-Key Ciphers

With symmetric-key ciphers, Alice and Bob share a secret key. When Alice wishes to encrypt a message for Bob, her symmetric-key cipher is fed her plaintext message and the shared secret key as inputs to produce a ciphertext message. Bob uses the same shared secret key to decrypt the ciphertext message and recover Alice’s plaintext message.

Symmetric-key ciphers use algorithms that transform the input data using permutation and transposition primitives. The combinations of permutations and transpositions are designed to make it computationally infeasible to derive the plaintext from the ciphertext without knowledge of the secret key.

All symmetric-key ciphers, except for the one-time pad cipher, use a relatively small, fixed length key. The one-time pad is a special case and will be discussed separately. Examples of symmetric-key ciphers include DES (56-bit key), 3-DES (112 or 168-bit key), and AES (128, 192 or 256-bit key).

An issue that must be addressed in cryptosystems that employ symmetric-key ciphers is secure distribution of the shared secret keys. A simple, non-scalable method for sharing secret keys is for each pair of parties to physically meet in a secure environment and agree on a secret shared key. Alternately, if each party trusts a third party, the third party could be used as a courier to carry the secret keys to the parties. As the number of pairs of parties grows, the number of keys and exchanges grows to an unmanageable size for this method to be feasible for widespread use. To explain this mathematically:

$$k = nCr = \frac{n!}{r!\,(n-r)!}, where\ n\ \geq r\ (r = 2\ for\ pairs\ of\ symmetric\ key\ users)$$

Using the above formula, the following examples illustrate the key exchange issue (n is number of parties, k is number of keys):

a. When n = 100, k = 4,950
b. When n = 1,000, k = 499,500
c. When n = 10,000, k = 49,995,000

2.2 One-Time Pad

The one-time pad (OTP) is a cryptographic algorithm that provides unconditional security. It was proven to be information-theoretically secure by mathematician Claude Shannon in 1949.

The OTP algorithm combines a random key with plaintext information to produce ciphertext. The combination function is simply an "exclusive-or" bitwise operation. The key must be the same length as the plaintext it is protecting. The resulting ciphertext is unconditionally secure, indistinguishable from a true random sequence as long as several conditions are met:

a. The key must never be re-used for encryption. The key should be destroyed after it is used. As long as the key is unique and never reused, there is nothing that can be used to attack the ciphertext; for example, statistical analysis or pattern matching. If the key is reused, the security of the system is reduced, potentially to near zero.
b. The key must be securely shared between the parties exchanging the information.
c. The key must be truly random. A truly random key ensures that statistical methods cannot be used to attack the system. If the key is not truly random, the security of the system is reduced, potentially to near zero.

OTP is used in some applications that require the very highest levels of security. In practice, however, key management for OTP is difficult to implement; therefore, OTP is only used for special applications.

2.3 Public-Key Ciphers

Public-key ciphers use algorithms based on difficult mathematical problems, such as factorization (e.g., RSA), discrete logarithms (e.g., DH, DSS) and elliptic curves (ECC).

The security of public-key ciphers relies on the computational complexity of trying to reverse any difficult one-way mathematical functions. An example of a one-way mathematical problem is the relatively easy step of multiplying two large prime numbers. This contrasts with the computationally difficult task of factorizing the product of these two prime numbers.

The absolute security of public-key ciphers is unproven. For example, it has not been proven that there is no algorithm that can efficiently factorize large numbers at a much faster rate than the current best-known factorization algorithms.[1]

Unlike symmetric-key ciphers, public-key ciphers use a pair of different but related keys; one is used for encryption, and the other for decryption. This characteristic is the reason that public-key ciphers are also known as asymmetric-key ciphers.

In public-key cryptosystems, each party generates a pair of keys. The encryption key is made available to all parties participating in the system. This key is called the public key. The decryption key is kept secret by its owner, and is called the private key.

When Alice wishes to send information protected by a public-key cipher to Bob, she uses Bob's public key to encrypt the plaintext message. Bob uses his private key to decrypt the ciphertext received from Alice. The message is secure because only the matching private key — which is kept secret by the intended recipient of the message — can be used to decrypt the message.

[1] In fact, an efficient integer factorisation algorithm has been developed by Shor [2]. It requires a quantum computer of sufficient scale, yet at this time, such a quantum computer is believed to not yet be available.

Public-key ciphers suffer from two limitations:

a. They are relatively slow. Public-key ciphers are typically two to three orders of magnitude slower than equivalent-key length symmetric-key ciphers, and
b. They can only be used to protect relatively tiny amounts of information. If a large message is to be encrypted, it must be broken up into smaller chunks that must be individually encrypted and combined to form the ciphertext message. The recipient must split the ciphertext message into the individual ciphertexts, decrypt each one, and then recombine the individual plaintexts to reproduce the original plaintext message.

Public-key ciphers significantly reduce the complexity of key management. There is no need to secretly share keys. The private key is never shared, while the public key can be openly shared with anyone. However, public-key cryptosystems must ensure the authenticity of public keys; i.e., there must be no doubt that the public key used for encrypting a message to Bob does indeed belong to Bob. If the wrong public key is used to encrypt a message, then the intended recipient would not be able to decrypt the message, and the (unintended) actual owner of the key would be able to decrypt the message intended for Bob.

Most practical deployments of cryptosystems employing public-key ciphers depend on a public key infrastructure (PKI). A PKI requires that all parties using the cryptosystem trust a third party (the certificate authority [CA]) to authenticate the public keys of all parties in the cryptosystem.

2.4 Key Distribution

Current cryptosystems almost universally use both symmetric-key ciphers and public-key ciphers. Public-key ciphers are used to exchange symmetric keys between parties, while symmetric-key ciphers are used to exchange messages between parties, and PKI is used to authenticate the parties.[2]

This hybrid system takes advantage of the high-speed encryption provided by symmetric-key ciphers and the simpler key management offered by public-key ciphers. Public-key ciphers and PKI do not provide a solution for the key management issues of the OTP cipher.

2.5 Conventional Cryptography Issues

Both symmetric-key ciphers and public-key ciphers are vulnerable to brute-force attacks. Increases in computational power are frequent and have required cryptographic algorithms to be removed from use, or required increased key sizes to be used.

With conventional ciphers, there may be efficient means of obtaining the plaintext from the ciphertext. New weaknesses may be found in existing cipher algorithms, and new algorithms may be found to simplify complex mathematical operations.

A breakthrough in technology may render conventional ciphers vulnerable; e.g., a sufficiently powerful quantum computer could use Shor's algorithm to recover the keys of all cryptosystems that use public-key ciphers based on factorisation, discrete logarithms or elliptic curves, and do so much more efficiently than a classical computer using a brute force approach.

Ciphertext captured today can be saved until it is computationally feasible using any or all of the above advances to derive the corresponding plaintext. Current ciphers rely on assumptions of computational infeasibility and algorithm correctness to ensure the ongoing protection of information.

[2] Strictly, this is only true for systems employing mutual authentication. It is more likely in real-world systems that only one of the parties will be authenticated using the PKI; e.g., a banking website will have a certificate issued by a CA, but the bank client will usually authenticate after an encrypted session has been established using a username and password, or a one-time password scheme such as RSA SecurID®.

Cryptosystems employ PKI to simplify key management. However, PKI relies on a number of assumptions and has a number of vulnerabilities of its own, especially when cryptosystems operate over public infrastructure or infrastructure controlled by untrustworthy parties outside the cryptosystem.

In short, symmetric-key (excepting OTP) and public-key cipher primitives are not information-theoretically secure. Both require assumptions to be made about an adversary's capabilities and the ongoing strength and correctness of the algorithm. Information protected by these ciphers is vulnerable to attack from the time it is encrypted until any time in the future. The future confidentiality of information secured with these ciphers cannot be guaranteed.

PKI has significantly decreased the cost and complexity of cryptosystems. It can be argued that it has been the most important technology leading to the global success of electronic commerce. However, PKI is a single point of failure — when it fails, the ramifications (financial or political) will be enormous. PKI relies on the ongoing security of public-key ciphers, trust in third parties, and trust in third-party infrastructure and systems.

The one-time algorithm offers unconditional security. Conventional cryptographic primitives are unable to provide a practical method of key management for cryptosystems to employ the OTP algorithm. Therefore, the only proven absolutely-secure cipher is not commonly used in conventional cryptosystems.

3. Quantum Key Distribution

3.1 Conventional Cryptosystems

A point of weakness in conventional symmetric key cryptographic systems is the safe and secure distribution of key material between parties. This key distribution problem has several solutions involving public key algorithms (RSA, DH, ECC, DSS, etc.) or symmetric key protocols (e.g., Kerberos). Issues with conventional systems are:

a. Trust of third parties (e.g., CA in PKI, TGS in Kerberos);
b. Assumptions about an attacker's limited capability;
c. Reliance on difficulty to efficiently reverse conventional ciphers;
d. Belief that significant technology breakthroughs (e.g., quantum computer) will be a long time coming, and
e. All information (past, present and future) protected by conventional cryptography is, and always will be, vulnerable to attack with the passage of time. Captured ciphertext can be stored now and attacked in the future when methods and/or technology advance sufficiently.

3.2 QKD Advantages

The principal advantage quantum key distribution offers over conventional cryptographic techniques is ennabling the continuous generation of information-theoretically secure key material "on the fly" between two parties, where the security of the generated key is guaranteed by the laws of quantum physics.

This generation of information-theoretically secure key material enables Alice and Bob to communicate with unconditional security using the OTP encryption algorithm. No technology or algorithm advances can weaken the OTP cipher.

QKD addresses the aforementioned weaknesses of conventional cryptographic systems by way of the following:

a. Trust of third parties. Alice and Bob initially require some shared key material but can then generate new secret key material independently without requiring a trusted third party.
b. Assumptions about an attacker's limited capability. It is assumed that an eavesdropper is limited only by the laws of quantum physics.
c. Reliance on difficulty to efficiently reverse conventional ciphers. QKD is used to generate key material for OTP encryption; an absolutely secure encryption algorithm.

d. Belief that significant technology breakthroughs (e.g., quantum computers) will be a long time coming. OTP encryption is proven to be secure even against quantum computers.

e. All information (past, present and future) protected by conventional cryptography is, and always will be, vulnerable to attack with the passage of time. The absolute security of OTP encryption is timeless; it is always secure.

3.3 Types of QKD Systems

In general, there are two different (but complementary) approaches to QKD to generate secret key material. Analogous to the particle-wave duality of light, these two approaches either put the emphasis on the corpuscular, or wave aspect of the quantum carrier of information in order to provide the security.

3.3.1 Discrete Variable QKD

Historically, the original QKD protocol was proposed by Bennett and Brassard in 1984 and is commonly known as the BB84 protocol [3], named after its two discoverers. The BB84 protocol is originally based on the transmission and measurement of random polarizations of single photon states. There have been many subsequent theoretical QKD protocols using single photon states: In 1991, Ekert proposed a QKD protocol using maximally entangled Bell states [4]; in 1992, Bennett simplified the original BB84 protocol by proposing a two-state QKD protocol known as the B92 protocol that used only two non-orthogonal states [5]. In 1998, a six-state QKD protocol was also proposed [6], where the quantum state basis set is symmetrically distributed about the Poincaré sphere.

It is both difficult and resource intensive to produce a true on-demand single-photon source. Typically, single-photon sources are approximated using an attenuated laser, or single-photon pairs produced via a parametric down conversion process. However, in practice, the photon number distributions for both single photons produced by attenuated lasers, and pairs of single photons produced by parametric down conversion, both obey Poissonian statistics, which leads to a security risk that is due to the non-zero probability of generating two photons or two pairs of photons per pulse respectively. In this case, it was shown that the security of QKD protocols could be compromised over long transmission distances in the case where Eve used sophisticated photon-number splitting attacks [7]. It was recently shown, however, that the security of QKD protocols using weak coherent pulses could be improved by using decoy state protocols [8].

In practice, the secret key rates of single-photon QKD protocols are inherently limited by the detection of single photons [9]. Typically, single photons or weak coherent pulses are detected using photon detectors such as avalanche photodiodes. At present, four main factors limit the rate of these single photon detectors: a) finite quantum detection efficiency; b) electronic noise (or dark noise); c) timing resolution (jitter), and d) the detector recovery time (known as detector dead time). Although there has been steady technological advancement, the secret key rate of single photon QKD protocols to date, is generally low.

3.3.2 Continuous Variable QKD

In the last few years, there has been considerable interest in the relatively new QKD protocols based on Continuous Variables (CV), which are limited by neither single-photon generation nor single-photon detection techniques. This new generation of QKD protocols are based on the transmission of coherent states, such as those readily produced by a laser, which are detected using shot-noise limited homodyne detectors [10].

These CV-QKD protocols offer the advantage of high total detection efficiencies by using homodyne detectors with high quantum efficiency photodiodes. Furthermore, CV-QKD systems are compatible with current telecommunication technologies, such as modern telecommunication encoding, transmission and detection techniques. These advantages can potentially enable CV-QKD protocols to achieve higher secret key rates compared to their single photon counterparts.

In addition, CV-QKD protocols are relatively simple to implement and require significantly less quantum resources compared with other QKD protocols. Coherent states can be readily produced by well stabilized off-the-shelf lasers and commercial coherent optical communication modulators and detectors.

In discrete variable QKD protocols, it is required for Bob to randomly switch measurement basis. However, counter intuitively, with CV-QKD protocols it is not only possible to simultaneously encode information onto both the amplitude and phase quadratures of a coherent laser beam, but also to measure simultaneously both the amplitude and phase quadratures of the light. This so-called "no-switching" protocol [11] not only vastly simplifies the implementation of CV-QKD protocols but also enables higher secret key transmission rates.

Furthermore, it has been shown that the security of CV-QKD protocols could be ensured for high-channel transmission losses (i.e., long transmission distances) by employing either reverse reconciliation [12] or post-selection [13] techniques. This development has extended the potential range of CV-QKD systems up to intra-city distances.

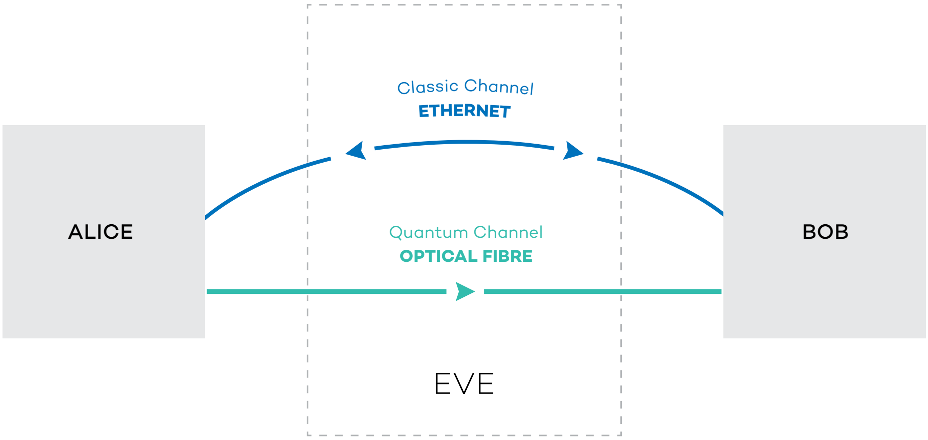
Importantly, CV-QKD protocols were recently proven to be unconditionally secure [14], that is, it has been mathematically shown that these QKD protocols are absolutely secure against any eavesdropping attacks. This unconditional security proof adds substantial credence and credibility to CV-QKD protocols.

3.4 Making QKD Practical

A QKD system comprises a sender unit (Alice) and a receiver unit (Bob) housed in secure locations. A passive optical link ("dark fibre") connects the two units and provides the physical layer for the quantum channel. The quantum channel must be continuously characterized to determine the maximum information a potential eavesdropper (Eve) could have obtained if she was able to effectively harness channel transmission losses and additional excess noise from the transmission process.

An authenticated conventional communication link (e.g., an IP/Ethernet network) between Alice and Bob is used for peripheral communication between the two parties. This classical channel is used by Alice and Bob to communicate information that allows them to distil absolutely secure key material from their raw key material.

This pair of links (the quantum channel and the classical channel) forms the basis of the "QKD layer" of all QKD systems.

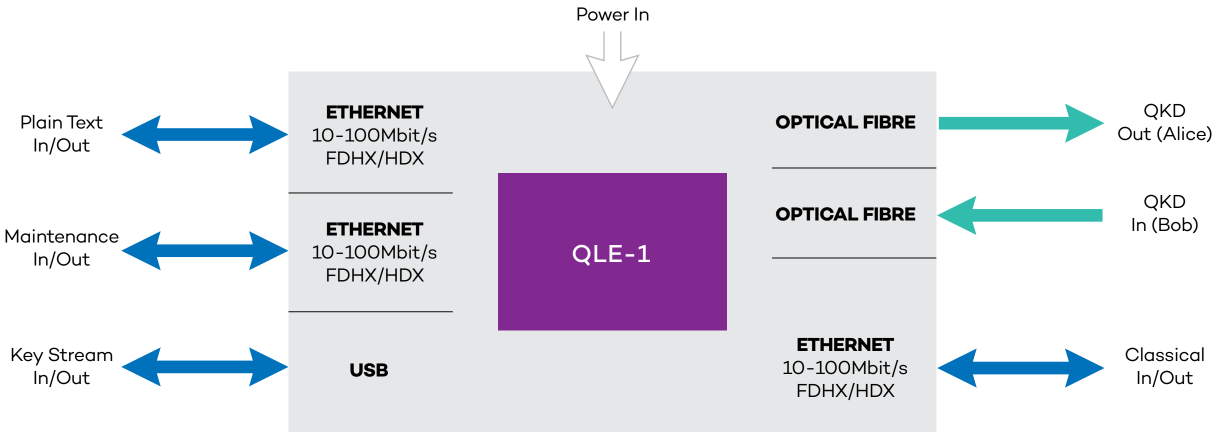


Alice and Bob Units with "QKD Layer" Links in the QKD System

A practical QKD system used to perform link encryption must also contain several additional interfaces and functions:

a. An interface and method to seed the system with initial key material for authentication at start-up;
b. High-speed true random number generator;
c. Interfaces to connect into end-user information systems, and methods to protect and forward user information;
d. Peer-to-peer network interfaces to carry protected end-user traffic between QKD nodes (this can be the same physical network as the classical channel);
e. A peer-to-peer key management protocol to ensure the secure and efficient use of key material generated from the QKD layer;
f. Management interfaces that provide a means to control and monitor the QKD system using conventional network management tools and protocols (e.g., SNMP).

The block diagram below shows the interfaces provided by the first generation QuintessenceLabs Quantum Link Encryptor (QLE-1).



First Generation QLE-1 Link Encryptor Interfaces

3.4.1 Optical Components

Typically, an Alice unit has a fibre-coupled laser that is split into two arms using a coupler: a local oscillator reference arm (LO) and a signal arm (Signal). Two independent sequences of random numbers are generated using a pair of quantum random number generators (QRNG), the outputs of which are encoded onto the amplitude and phase of the laser in the signal arm using an amplitude modulator (AM) and phase modulator (PM) laser in the signal arm. The signal and local oscillator lasers are recombined (polarization multiplexed) using a polarized beam splitter (PBS). The two lasers are then transmitted to Bob along the optical fibre that connects the Alice and Bob units.

The Bob unit has a polarization controller (PC) and a polarized beam splitter (PBS) that are both used to split the signal (Signal) and reference local oscillator (LO) lasers. The power of the reference local oscillator is coherently amplified, or generated, to allow for dual-homodyne detection of the signal. The two homodyne detectors are used to measure the amplitude and phase quadratures of the signal laser, where the phases of the local oscillator lasers are independently controlled using two independent phase modulators (PM).

3.4.2 QKD Protocol

In more detail, the QKD protocol operates as follows:

a. In Alice's unit, two independent sequences of random numbers are continuously generated and stored.
b. The random number sequences are encoded as modulation signals onto the amplitude and phase quadratures of the signal laser.
c. The modulated laser is transmitted to Bob's unit through the optical fibre that connects both units.
d. In Bob's unit, the amplitude and phase quadratures of the received laser are simultaneously measured using two optical homodyne detectors.

At the end of this process, Alice and Bob both possess a correlated sequence of random numbers. However, their number sequences are not identical due to a) inherent quantum noise on the laser beam; b) attenuation and losses of the laser beam during transmission through the optical fibre, and c) excess channel noise.

3.4.3 Eavesdropping

After the transmission and detection of the modulated coherent states, it is necessary to bound the maximum amount of information Eve could have obtained during the transmission process. It is assumed that Eve's capabilities are limited only by the laws of physics and quantum mechanics. For example, Eve is assumed to be able to perfectly recuperate, store, measure and process using quantum computer hardware any laser light that is lost during transmission through the optical fibre linking Alice and Bob. Hence, from any transmission losses, Eve obtains some information about the sequence of random numbers shared by Alice and Bob. In fact, in the case of high transmission losses through the optical fibre, Eve might initially appear to have more information about what either Alice transmitted and/or Bob measured, compared to the mutual information shared between Alice and Bob. This apparent information advantage is overcome in the following steps.

3.4.4 Post-selection

Alice and Bob can reverse any potential information advantage that Eve might initially possess by performing a post-selection algorithm. In this process, Alice and Bob discard data for which they determine Eve has more information, while keeping data for which Alice and Bob determine that they have more information than Eve. Through this post-selection process, Alice and Bob keep a subset of data for which they have more mutual information than an eavesdropper, thus reversing any initial information advantage Eve might have had from eavesdropping. The cost of this post-selection process is a reduction in the amount of secret key material.

3.4.5 Error Correction

In the second post-processing step, Alice and Bob use an information reconciliation algorithm to correct any errors in their respective random number sequences. These information reconciliation algorithms are optimised to efficiently correct errors while at the same time reveal as little additional information as possible to an eavesdropper.

3.4.6 Privacy Amplification

In the final post-processing step, Alice and Bob use privacy amplification algorithms to reduce an eavesdropper's information to approximately zero, at the cost of reducing the size of the final sequence of random binary numbers. Typically, privacy amplification algorithms used are based on universal hashing functions.

At the end of this process, Alice and Bob share a random number sequence that can serve as secret encryption and decryption keys for absolute secure communication using the OTP cipher for encryption.

4. Additional Information

For more information on this topic please contact QuintessenceLabs by emailing **info@quintessencelabs.com** or visit **quintessencelabs.com**.

4.1 References

[1] A. Menezes, P. van Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, (1996).

[2] Peter W. Shor, Algorithms for Quantum Computation, Discrete Logarithms and Factoring, Proceedings, 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, November 20-22, 1994, IEEE Computer Society Press, pp. 124.

[3] C. H. Bennett and G. Brassard, Proceedings IEEE International Conference on Computers, Systems and Signal Proceedings (Bangalore), page 175, (1984).

[4] A. K. Ekert, Phys. Rev. Lett. 67 661, (1991).

[5] C. H. Bennett, Phys. Rev. Lett. 68 3121, (1992).

[6] D. Bruß. Phys. Rev. Lett. 81 3018, (1998). H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A 59 4238, (1999).

[7] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. 85 1330, (2000).

[8] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94 230504, (2005).

[9] N.Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. 74 145, (2002).

[10] S. L. Braunstein and P. Loock. Rev. Mod. Phys. 77 513 (2005).

[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul. T. C. Ralph and P. K. Lam, Phys. Rev. Lett. 93 170504, (2004).

[12] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature 421 238, (2003).

[13] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. 89 167901, (2002).

[14] R. Renner and J. I. Cirac, Phys. Rev. Lett. 102 110504 (2009), A. Leverrier and P. Grangier, 102 180504 (2009).