Methods and implementation of quantum cryptography

Dheera Venkatraman

MIT Department of Physics

dheera@mit.edu

27 April 2004

Abstract

Quantum mechanical properties of communication lines may be lead to new possibilities in the security of key distribution. By taking advantage of basic quantum mechanical principles, it may be possible to create secure systems that rely upon the physics of the system rather than computational or mathematical methods for security. In this paper, three possible protocols for quantum key distribution are described.

1 Introduction

In the electronic communication networks that facilitate the much of the world's information exchange, privacy and security have always remained important issues to be addressed. Since the very first military applications of electronic communication, encryption algorithms have been developed to keep such information secure between a given sender and receiver. However, many of these algorithms are computationally intense and rely upon the assumption that eavesdroppers do not have sufficiently fast technology or mathematics to break the scheme. The principles of quantum mechanics, however, may offer alternative methods to encryption which may circumvent many of these issues, several of which, along with possible implementations, will be discussed.

1.1 Classical cryptography and the key distribution problem

Using classical communication methods, cryptography has been computationally implemented in a number of ways. One of the simplest such methods involves mathematically transforming a message M, by a given password or key K [1]. In the simplest implementation one could simply add M and K; provided K is at least as large as M, it is easy to see that this system is, in fact, perfectly secure. For example, consider an example of the simple Vernam cipher: Suppose a sender Alice (named by convention) wishes to transmit a message $M = 51242$ to a receiver Bob. They could agree to use a key such as $K = 63143$, for example, and Alice would transmit a *ciphertext* $C(K, M)$:

$$C(K, M) = M + K = 114385 \tag{1}$$

upon which Bob could simply subtract K and obtain the message. Such a system is obviously fully secure if K is at least as long as the message and, is used only once to avoid pattern recognition. While algorithms exist for using a shorter key repeatedly still with a great degree of security, all such *secret-key* schemes, in which a single key is used for encryption and decryption, still fall to one central problem: How do Alice and Bob agree upon K?

This problem, known as the *key distribution problem* [2], arises when Alice and Bob wish to communicate in privacy but cannot meet prior to communication to agree upon a secret key in advance (consider, for example, accessing any secure internet site). In particular, it would be insecure to agree upon a key in plain text over a network in order to actually use such a secret-key algorithm.

Classically, the most common way to resolve this issue is to require different keys for enciphering and deciphering a message. In *public-key encryption* systems such as RSA, it is possible to create a pair of large prime numbers and encipher a message using one prime number in such a way that the other prime number would be needed to decipher the message. Successful eavesdropping would then entail finding the prime numbers given only their product, a problem which is computationally difficult if the prime numbers are sufficiently large. Another protocol known as the Diffie-Hellman key exchange protocol [1] attempts to use similar principles involving prime numbers to produce a single key which could be used for communication. Although widely used today for communication, such methods relying upon the difficulty of factoring large numbers could potentially fail to computational, technological or mathematical advances.

1.2 Quantum cryptosystems

While classical methods have found computational methods to solve the key distribution problem, quantum cryptosystems target the issue in a different manner. By utilizing the *physical* properties of the communication channel it may be possible to securely agree upon a key over a network, after which a computationally simple and secure secret-key scheme can be used, perhaps even over a parallel classical network. The subject of quantum cryptography targets primarily the key distribution problem and not the communication of information itself, since a classical network can already be extremely secure with a secret-key scheme (as shown earlier in the simplest of cases, the Vernam cipher). Phenomena such as the Heisenberg uncertainty principle and basis transformations are be employed to inhibit eavesdropping by unwanted parties. Several quantum mechanical *protocols*, some of which will be discussed in this paper, have been developed to procedurally describe key-distribution schemes.

There are several motivations for exploring such a field. First, quantum mechanical methods may have the potential to greatly reduce computation time by using the theory of quantum mechanical systems, rather than software, to perform computations. Additionally, the security of many quantum mechanical protocols relies on well-known statements and theories of physics, rather than the sheer impossibility of certain calculations with current technology, as used by classical crytosystems of today with prime numbers. The latter may also become instantly vulnerable in the event of breakthroughs in technology or mathematics that enable the solution of such problems. In fact, once developed, quantum mechanical factoring algorithms may even be a promising method to break many of today's prime-number based cryptosystems.

2 The BB84 protocol

Proposed by Bennett and Brassard in 1984 [3], BB84 was the first cryptographic protocol designed to solve the key distribution problem quantum mechanically. It is centered around the measurement of a 2-state system in either of 2 complete bases. One such convenient system is that of light waves, which can be measured in the circular polarization basis $\{|L\rangle, |R\rangle\}$ or the linear polarization basis $\{|x\rangle, |y\rangle\}$ which are each complete such that [4]

$$|x\rangle = \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle) \tag{2}$$

and

$$|y\rangle = \frac{-i}{\sqrt{2}}(|R\rangle - |L\rangle) \tag{3}$$

It is then possible to propose that a 0 be represented by *either* $|R\rangle$ or $|x\rangle$ and that a 1 be represented by *either* $|L\rangle$ or $|y\rangle$. Thus, a given string of binary information represented by 0's and 1's can be represented just as well by a sequence of photons with such states. It is the dual possibilities of representing each 0 or 1 that brings about the security of this key distribution system.

If Alice were to transmit a bit (0 or 1) to Bob using this system, Alice could send it using either the circular or linear basis as previously defined to send the bit. Anyone who reads the communication line could then pick a basis for measurement of each bit and either correctly measure Alice's bit in the basis she used to transmit it, or use the incorrect basis and measure the bit correctly with a probability of 1/2. Thus, the net probability of a correct measurement is

$$\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} \tag{4}$$

which could apply to either Bob, the receiver, or Eve, a hypothetical eavesdropper, neither of whom had knowledge of the bases Alice used to transmit the data. How then, does Alice agree with Bob upon a particular key without telling him the bases, which Eve could listen to and correspondingly measure? The solution is for Alice to discuss which bases she used to transmit the data *after* the measurement itself, upon which Bob and Alice could simply decide to drop the pieces of the key that were incorrectly measured and use the remaining, shorter key.

What if Eve were to eavesdrop upon the line and measure the signal? Eve would also have to pick her own bases for measurements, which would be correct, on average, half of the time. This leads to correct measurement of 3/4 of the signal on her part. While this may seem high at first glance, Eve would need to have *all* of the bits of the key correct in order to decipher any further communication, and for a key several thousand bits long it may be impractical for Eve to guess the correct key by trial and error from her inaccurate version. Furthermore, one final feature unique to quantum cryptography comes to the rescue: it is actually possible for Bob and Alice to determine Eve's presence from their measurements, after which they could redo their entire key distribution.

The basic idea behind this eavesdropping detection is the fact that Eve's incorrect basis choices in any bit collapses the state of the photon into a state of the basis used

by Eve. If this happens to a particular bit which Bob's measurement basis and Alice's transmission basis concur, Bob then makes a 1/2-probability error in measuring the bit. Using a sufficiently long key, Alice and Bob can then select random bits from the key to compare openly to inspect for this error. Following this, if eavesdropping is not detected, the bits used for the check can be discarded, and the remaining bits used as a key.

This system is perhaps best illustrated by an example key distribution between Alice and Bob. Consider an initial binary key K which Alice generates randomly. For example, we can consider the arbitrary string of 0's and 1's:

$$0 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1$$

to be an initial random, raw key. Normally this would be at least several hundred or thousand bits long for practical purposes and security, but for demonstration we only observe a small case. Supposing Alice then picks the following sequence of bases, randomly, to transmit this key:

$$\bigcirc \quad \perp \quad \bigcirc \quad \bigcirc \quad \perp \quad \bigcirc \quad \bigcirc$$

where $\bigcirc$ represents transmission in the circular basis and $\perp$ represents the transmission in the linear basis for polarization. Then, Alice would transmit over the line the following states, as described by the 0 and 1 definitions in the basis chosen for each bit:

$$|R\rangle \quad |y\rangle \quad |L\rangle \quad |R\rangle \quad |x\rangle \quad |R\rangle \quad |L\rangle$$

Then, supposing Bob decides, at random, to measure the signal with the following bases:

$$\bigcirc \quad \bigcirc \quad \perp \quad \bigcirc \quad \perp \quad \perp \quad \bigcirc$$

He would then correctly measure each base that corresponds correctly to Alice's transmission, and a half-half probability distribution of states for the bases he chose incorrectly (noted below as a ?). The resulting bases for which we know Bob's outcome are then

$$|R\rangle \quad ? \quad ? \quad |R\rangle \quad |x\rangle \quad ? \quad |L\rangle$$

Note that Bob actually has a measurement for each ? shown above, but does not yet know which keys are in chosen correctly. This sequence corresponds to a chosen key of

0 ? ? 0 0 ? 1

Bob can then indicate to Alice the entire sequences of bases that he chose. Alice replies to Bob, indicating which bases were chosen incorrectly (at this point, Bob now knows which ones are uncertain and represented above by a '?'). Alice and Bob erase these values from their keys, thus agreeing upon the key 0001, in this case. Upon expanding the key length to a sufficiently long length of perhaps at least a few thousand photons, Alice and Bob could select random bits from the final key to compare. If there are any discrepancies, it could indicate Eve's presence, which would cause an error rate of 1/4. The probability that Eve eavesdrops and goes undetected by this method is thus given by:

$$P_e = (1 - \frac{\lambda}{4})^n \tag{5}$$

where λ is the fraction of bits that Eve eavesdrops on ($\lambda = 1$ for practical eavesdropping), and n is the number of measurements that are discussed and compared. If Eve eavesdrops through the entire communication, comparison of only 100 measurements is sufficient to achieve a rather reasonable $P_e \approx 3 \cdot 10^{-13}$.

2.1 Noise and the BB84 protocol

Particularly in smaller and more sensitive quantum mechanical channels, one must also take into account the fact that noise may have an effect on Bob's measurement of a signal. In cables of practical length, the effect of noise on the signal must be studied. It is sufficient to describe the effects of noise as causing an incorrect measurement by Bob, at a rate per total transmission bits defined as α. If such noise is present, two issues must be resolved. First, the algorithm must be revised such that Alice and Bob still settle upon a secret key in spite of these errors. Second, a method must be determined to distinguish between the effects of noise and the effects of Eve's presence, both of which cause errors in Bob's measurements.

After performing the standard BB84 protocol previously described, Alice and Bob can then transmit, back and forth, intended bases and agreed data to obtain an estimate of the error rate α. Data for this test could be agreed upon in advance either by protocol or over a more reliable or open channel prior to testing. Another possibility, assuming the noise is similar in both directions of communication, is to transmit the data from Alice to Bob and have Bob repeat his measurements back to Alice to determine α [1].

It is reasonable to assume that errors occur as a Poisson process at rate α as the occurence of errors due to noise are statistically independent of one another. It is possible to then select a short enough length l of bits during which it is sufficiently unlikely for 2 errors to occur in the interval. The raw key is then repermuted in a fashion agreed upon over an open channel, then broken into segments of length l. Alice and Bob can then sum the bits in each segment and compare the parity of each segment (1 if the sum of the bits is an odd number, 0 if the sum of the bits is even). It is for this reason that the length l is picked so it is unlikely to have more than one error. If any of the parities compared do not match, further partitioning can be used to determine the erratic bit. This process can be repeated for another agreed permutation of the key for additional checking [1]. After deleting discovered errors each time, and finding a sufficiently long sequence of compared lengths that contains no error, this can be used as an encryption key.

Clearly the length l must not be chosen too short. If it were as short as 1, the parities would simply be the key data itself, defeating the system. Since the length must also not be too large to avoid double errors in a segment, this puts an upper bound to the error rate α. If the error rate is too large, the protocol fails and further work on the physical system would be needed. Finally, Alice and Bob can agree on randomly-selected subsets of the key as the final key. If randomly-selected bits are checked only now for errors and subsequently discarded, with an error rate significantly larger than α, Alice and Bob can agree that Eve may have been watching and repeat the process or inspect the communication channel.

3 The B92 protocol

The B92 protocol [5] attempts to simplify the BB84 protocol by using only 2 states, although *non-orthogonal*, on Alice's side to represent a 0 or 1. Using the same photon polarization description as presented earlier, it is possible to pick such non-orthogonal states, based on the fact that a polarization state rotated by θ from the x-axis can be represented as [4]

$$|\theta\rangle = \cos(\theta)\,|x\rangle + \sin(\theta)\,|y\rangle \tag{6}$$

Using a value of $\theta < \pi/4$, the $|\theta\rangle$ state can be defined to represent a 1 while the $|x\rangle$ represents a 0.

Alice then transmits each 0 or 1 as a $|x\rangle$ or a $|\theta\rangle$, respectively. Bob can pick either

of 2 bases for measurement: the $\{|x\rangle, |y\rangle\}$ basis or the $\{|\theta\rangle, |\theta'\rangle\}$ basis, where $\theta' = \theta + \pi/2$, making the $|\theta\rangle$ and $|\theta'\rangle$ states orthogonal. Note that under these circumstances, if Alice transmits a $|x\rangle$ there is no chance that Bob will measure $|y\rangle$ due to orthogonally. Bob's possibilities are only to either measure it in the correct basis as $|x\rangle$, or in the incorrect basis to obtain $|\theta\rangle$ or $|\theta'\rangle$. Thus, if Bob does in fact measure $|y\rangle$ he can conclude that Alice must have transmitted a 1, since Alice used only $|x\rangle$ (0) and $|\theta\rangle$ (1) for transmission. By similar logic, if Bob receives a $|\theta'\rangle$ he can conclude that Alice transmitted a 0. If Bob measures $|\theta\rangle$ or $|x\rangle$, however, the test is inconclusive since he may have picked the wrong basis and collapsed it into that particular state. This situation is known as an *erasure*, and occurs with a probability of 1/2. The positions of such erasures can be announced and dropped from the key, allowing the remaining portion to become the agreed key.

One advantage of the B92 system is clear: Alice need not transmit which bases she used for measurement; Bob can simply respond with the positions of the bases to keep, making the protocol simpler and faster to execute. However, it should be noted that detectors must be made extremely precise in order to not trigger a non-erasure due to a misaligned polarization measurement. For example, suppose Alice transmits a $|\theta\rangle$ (representing 1). If Bob decides to do the measurement of the photon in the $\{|\theta\rangle, |\theta'\rangle\}$ basis but due to experimental error in his angular alignment by ϵ measures it in the $\{|\theta + \epsilon\rangle, |\theta' + \epsilon\rangle\}$ basis, he may have a small probability of measuring a $|\theta' + \epsilon\rangle\}$ in which case he would decide that Alice transmitted a 0. The probability of this occurrence is given by

$$|\langle\theta|\theta' + \epsilon\rangle|^2 = \sin^2\epsilon \approx \epsilon^2 \tag{7}$$

which approximates the frequency of such errors in his measurement (where ϵ is measured in radians). Thus, roughly speaking, in order to reduce errors to a rate lower than ϵ^2 it is necessary to have an angular precision of ϵ or better. However, by using a parity check scheme it may be possible to identify rare errors and request for a retransmission. The larger the error rate, however, the harder it is to differentiate between such errors and the presence of Eve by parity checking.

4 Entanglement and the EPR protocol

It is possible to create key distribution algorithms using entangled states, as first described by Ekert [6]. By using Einstein-Podolsky-Rosen (EPR) pairs it is possible to create spatially separated particles that are *entangled*, or whose states are constructed in such a way that the measurement of one determines with certainty the outcome of the measurement of the other. This situation is easily created in theory by placing the two partices in either identical or orthonormal states to each other, and superposing this state with another similar state in a manner that there is a 1-1 correlation between the states of the first particle and the states of the second. For example, in a general two-state system with states $|A\rangle$ and $|B\rangle$, the following are entangled states between two distinguishable such systems:

$$|\chi_0\rangle = \frac{1}{\sqrt{2}}(|A\rangle\,|B\rangle + |B\rangle\,|A\rangle) \tag{8}$$

$$|\chi_1\rangle = \frac{1}{\sqrt{2}}(|A\rangle\,|A\rangle + |B\rangle\,|B\rangle) \tag{9}$$

Note that in these cases, if one particle was found to be in a particular state, knowledge of the entanglement would lead one to immediately know what the measurement of the other particle would yield. For example, in the state described by equation 9 measurement of one particle to be $|A\rangle$ would indicate a collapse into the state $|A\rangle\,|A\rangle$ and thus the other particle could be expected to be measured as $|A\rangle$ as well. The EPR protocol requires that three such states be used. This is easily created in the context of photons by using orthogonal polarizations. However, as photons are bosons, opposite polarizations must be used in each part of the entangled state and the superposition must be antisymmetrized. One possible way to do this is by using the following three entangled polarization states [1]:

$$|\Psi_A\rangle = \frac{1}{\sqrt{2}}(|0\rangle\left|\frac{\pi}{2}\right\rangle - \left|\frac{\pi}{2}\right\rangle|0\rangle) \tag{10}$$

$$|\Psi_B\rangle = \frac{1}{\sqrt{2}}(\left|\frac{\pi}{6}\right\rangle\left|\frac{2\pi}{3}\right\rangle - \left|\frac{2\pi}{3}\right\rangle\left|\frac{\pi}{6}\right\rangle) \tag{11}$$

$$|\Psi_C\rangle = \frac{1}{\sqrt{2}}(\left|\frac{\pi}{3}\right\rangle\left|\frac{5\pi}{6}\right\rangle - \left|\frac{5\pi}{6}\right\rangle\left|\frac{\pi}{3}\right\rangle) \tag{12}$$

In the state described by equation 10, a measurement in the $\{0,\pi/2\}$ basis of either

photon would determine the state of the other. If one photon were to be measured to be in the state $|\pi/2\rangle$, one could be certain that the other was collapsed into the state $|0\rangle$, and vice versa. Similarly, measurements can be made in any of 3 bases corresponding to each of these entangled states. Measurement in a basis matching the respective entangled state will result in a theoretically perfect correlation between the measurements made by Alice and Bob.

Thus, the two particles from a randomly selected entangled state (either $|\Psi_A\rangle$, $|\Psi_B\rangle$ or $|\Psi_C\rangle$ can be sent to Alice and Bob for each desired raw bit. Bob and Alice can then each use one of three measurement operators corresponding to these entangled states to measure each bit. Similar to the BB84 protocol in procedure at this point, Bob then indicates which measurement operators he used. Alice replies, revealing which measurements were taken in the same basis as hers. At this point, for each bit that was measured correctly, Bob will have measured exactly the complement of Alice's key due to the entanglement and can subsequently invert these bits, after which Alice and Bob will have completed generating an agreed key [7].

Although the basic algorithm for key distribution under the EPR protocol is similar to BB84, the advantage to using entangled states is that the presence of eavesdropping can be detected *without* selecting samples of the key to compare and discard. Instead, as shown in [1] the already rejected bits due to incorrect measurements by Bob can be studied. In order to describe the mechanics of the detection procedure, it is necessary to understand Bell's theorem, which relates to the fundamentals of entanglement itself.

4.1 Bell's Theorem and eavesdropping detection

In 1935, Einstein, Podolsky and Rosen [8] came upon what is commonly referred to as the EPR paradox. Their associated thought experiment involved separating two entangled particles to an appreciable distance (for theory's sake, we can even consider light-years) and measuring them at close to the same, agreed time at both ends. According to classical theories, the information from the first measurement should not reach the second particle faster than light; however, quantum mechanics dictates that both cannot be measured independently and thus the first measurement must affect the second instantaneously. These conflicting ideas led Einstein, Podolsky and Rosen to propose that quantum mechanics was incomplete and that there could exist additional variables that dictated the outcomes of both particles before they were even separated.

Bell investigated this case and in 1964 [9] formulated a way to test such hidden variable theories, describing his arguments in terms of Stern-Gerlach measurements of spin. The basic setup involves repeated measurements of the spin two spatially-separated entangled states at the same time. The spin measurements at each end are each performed in any of three directions $\vec{a}$, $\vec{b}$ or $\vec{c}$ (which need not be orthogonal to each other). Suppose the first particle is measured at the same time as the second particle despite the spatial separation. If the EPR hidden variable hypothesis was correct, the results of the first measurement should be predetermined and independent of the choice of measurement operator used at the second particle [10]. Bell's work showed that given these conditions, it must be true that [9]

$$1 + P(\vec{b}, \vec{c}) \geq |P(\vec{a}, \vec{b}) - P(\vec{a}, \vec{c})| \tag{13}$$

for any hidden variable theory, where $P(\vec{a}, \vec{b})$ represents the mean value of the product of measurements of the first particle in the $\vec{a}$ direction and the second vector in the $\vec{b}$ direction. Bell's notation of P as a product is not to be confused with a probability, as $-1 \leq P(\vec{a}, \vec{b}) \leq 1$ where ± 1 are the eigenvalues of measurement in any direction. Later experiments showed that this inequality did not hold, confirming that hidden variables were not present in the Stern-Gerlach case.

We can apply Bell's results to the case of the EPR key-distribution protocol [1]. Define $p(i, j)$ to be the probability that the eigenvalue of any given rejected bit matches the respective eigenvalue of Alice's intended bit when Alice uses basis i and Bob uses basis j, out of the 3 possible bases, $A = \{0, \pi/2\}$, $B = \{\pi/6, 2\pi/3\}$ and $C = \{\pi/3, 5\pi/6\}$. Then, it is straightforward to compute the mean value of the product of the eigenvalues Alice and Bob measure to be

$$P(i, j) = 1 - 2p(i, j) \tag{14}$$

Under normal circumstances, Alice and Bob would find, as did other experimentalists in the past with Stern-Gerlach experiments, that Bell's inequality applied to this case

$$1 + P(B, C) \geq |P(A, B) - P(A, C)| \tag{15}$$

does not hold for their rejected bits.

If Eve were to be present, however, certain measurements would already be collapsed before they reached Alice and Bob. This has the same effect as a hidden variable

predetermining their measurements [1] and will cause Bell's inequality to hold true in such a case. Through statistical analysis, Alice and Bob could determine if Bell's inequality held true for any communication and detect Eve's presence in this manner. Note that since these measurements are already rejected from the key, it is safe for Alice and Bob to discuss these over an open channel, unlike the system used in BB84 where parts of the determined key needed to be compared and dropped.

5 Vulnerabilities and implementation

None of the discussed protocols are able to guard against opaque eavesdropping. In this case, Eve completely intercepts the line, acting as Bob to Alice and Alice to Bob. In this case, Eve can pass messages back and forth, correctly using the protocol in both directions. Although this is a vulnerability in most cryptosystems, it is an extremely difficult attack to perform with physical disruption of the line service. Theoretical development of further, more advanced key-distribution protocols is currently underway. Many other vulnerabilities have been proposed in various protocols including BB84 and B92 when under experimental imperfections. For example, the release of multiple photons per bit by Alice could be nearly fatal to the security of BB84 and B92 due to the Photon Number Splitting attack [11]. Much further research aims to strengthen protocols to withstand such imperfections. A well-developed quantum key distribution algorithm should meet at a balance between low sensitivity to experimental difficulties and good security.

As proposed in theory and used as an example system in this paper, quantum cryptography can be implemented using photons over fiber optic cables. At wavelengths of roughly 800 nm there exist good silicon photon counters [13] which can be used for this purpose. Special cables are needed to achieve long distances at this wavelength as existing telecommunication cables are designed for wavelengths of around 1300-1500 nm [13].

IBM first demonstrated an implementation of quantum cryptography over a 30 cm line in 1989 [12]. Since then, improvements have led to experimental BB84 implementations of upto lengths of 30 km [14] of optical cables. Projects are underway to extend this to beyond 100 km. Implementations of the EPR protocol including one by Enzer et. al. [7] have been performed, demonstrating eavesdropping detection on rejected bits. Although physical distance still remains the primary limitation of quantum key distribution in being used for long-distance communications, solutions

may include placing repeaters to reencode data at each of several segments to a given destination.

6 Conclusion

In today's world of computing and electronic information, privacy is often a critical issue. For years, classical prime-number based algorithms have dominated this field and relied upon computational difficulty as a security solution to the key distribution problem. Such a solution could be defeated by future developments in technology or mathematics. However, quantum-based cryptosystems that rely on physical properties of the communication channel may provide a more assuring solution to key distribution security. By eliminating the need for private and public keys, as well as large computations, quantum cryptosystems, possibly based on the same foundations as the early BB84, B92 and EPR protocols may prove to be faster, simpler and more secure than the classical systems of today.

Acknowledgements

This article was written as a term paper for 8.06, Quantum Physics III, Spring 2004 at MIT. Thanks to Professor Krishna Rajagopal for support, to Andrew Childs for much help during the editing process and to Huanqian Loh for review, discussion and support with this paper.

References

[1] S. J. Lomonaco, Jr., *A quick glance at quantum cryptography*, University of Maryland.

[2] P. W. Shor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE, Los Alamitos, CA, 1994) p. 124.

[3] B. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10-12 December 1984, p. 175-179.

[4] R. P. Feynmann, *Lectures on Physics* **3**, 11-9 (Addison-Wesley, 1965).

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

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

[7] D. G. Enzer, P. G. Hadley, R. J. Hughes, C. G. Peterson, and P. G. Kwiat, *Entangled-photon six-state quantum cryptography*, New Journal of Physics **4**, 45.1 (2002).

[8] A. Einstein, B. Podolsky and N. Rosen, *Can quantum-mechanical description description of physical reality be considered complete?*, Phys. Rev. **47**, 777 (1935).

[9] J. S. Bell, *On the Einstein-Podolsky-Rosen paradox*, Physics **1**, 195 (1964).

[10] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley, 1994).

[11] V. Scarani, A. Acin, G. Ribordy and N. Gisin, *Quantum cryptography protocols robust against photon number splitting attacks for wear laser implementations*, Phys. Rev. Lett. **92** 5 (2004).

[12] J. A. Smolin, *The early days of experimental quantum cryptography*, IBM J. Res. & Dev. **48** 1 (2004).

[13] Ch. Kolmitzer, Ch. Monyk, M. Peev, M. Suda, *An advance towards practical quantum cryptography*, ARC Selbersdorf Research Ltd., Selbersdorf, Austria.

[14] C. Elliott, D. Pearson, G. Troxel, *Quantum cryptography in practice*, BBN Technologies.