Generalization of Quantum Key Distribution Protocol

Muhammad Mubashir Khan and Jie Xu

School of Computing, University of Leeds, Leeds LS2 9JT, UK

Summary
Quantum Key Distribution (QKD) is a secure key sharing technology with unconditional security. Certain well-known protocols for QKD have been presented, which claim their security by means of higher eavesdropping error-rates. A generalized quantum key distribution protocol that can be optimized for arbitrary number of bases and dimensions of photon states is presented in this paper. The protocol can provide higher eavesdropping error-rates than the well-known existing QKD protocols like BB-84 [4] and B-92 [5]. The higher error-rate makes it possible for Alice and Bob to share secure keys on relatively large distances.

Key words:
Quantum Key Distribution, QKD, Quantum Cryptography, Information Security, Security Protocols

1. Introduction

Cryptography is an art that has been the field of interest of human being from ancient times. People used to adopt competitively secure methods, depending upon their capabilities of transferring information. On the eve of and after the 21st century, with the rapid growth in information technology and electronic communications, several modern techniques of securing information transfer were introduced [1]. Few decades after the advent of modern physics *quantum information and computation* flourished as one of the avant-garde technologies which are believed to revolutionize the world of data processing and information security [2]. Based upon the fundamental rules of quantum mechanics, quantum information provides a technique called quantum cryptography or quantum key distribution (QKD) [3] for sharing secret cryptographic keys with unconditional security.

The underlying idea in quantum cryptography is that the secret bits of information or keys are encoded in the quantum particles like photons. When the encoded photons are transmitted from one party to another say, Alice to Bob, an eavesdropper Evan may not copy the message without introducing a significant noticeable error-rate. Although the basic protocol for quantum cryptography, called BB84 [4], was published in 1984 but there have been many variations and novel schemes of quantum cryptography introduced with the notion of improving the error-rate, flexibility and efficiency. Bennett [5] revealed the generalized idea of using any two non-orthogonal quantum states for key distribution thereby providing more flexibility in the choice of bases. Bechmann-Pasquinucci presented the 3-states [6] and six-states [7] protocols for quantum cryptography creating more difficulties for Evan to eavesdrop.

In a recent work [10] it was attempted to improve the error-rate and efficiency in quantum key distribution by using higher dimensional photon states. An alternative quantum key distribution protocol was designed, where Alice and Bob use two mutually unbiased bases e and f with one of them encoding a '0' and the other one encoding a '1'. This means that all the states in the same basis encode same secret bit. The security of the scheme is due to a minimum index transmission error-rate (ITER), introduced by an eavesdropper, which increases significantly for higher dimensional photon states. The beauty of the scheme is that it does not impose any condition on the bases other than that they form a basis. This provides lots of flexibility of selecting the two appropriate bases to maximize the error-rate introduced by an eavesdropper in the case of an intercept–resend attack.

In this paper, we present a generalized key distribution scheme in which Alice and Bob may choose to employ arbitrary number of bases with higher dimensional photon states for acquiring higher error-rates in secret key distribution. Our scheme may be seen as the generalization of [10] in term of number of basis. The encoding in this scheme is such that each basis is assigned a unique alphabet while all the vectors in each basis state encode same alphabet. It is interesting to note that increasing the number of bases in our scheme increases the number of bits transmitted by each alphabet. For example, if the number of basis are four such that ($e \rightarrow 0$, $f \rightarrow 1$, $g \rightarrow 2$, $h \rightarrow 3$) then each alphabet represents two binary digits 00, 01, 10, 11.

The paper is organized into four sections. Section 2 explains the current state of the art. Section 3, presents the proposed generalized scheme in detail, which includes the new encoding and sifting process of our scheme. Section 4 concludes this paper.

2. QKD protocol with two bases

In the key distribution scheme with two bases [10] Alice & Bob prepare and measure the states in any of the two bases *e* and *f* which are pair-wise orthogonal, such that

$$e \equiv \{|e_i\rangle : i = 1,...,N\}$$

and

Manuscript received August 5, 2012
Manuscript revised August 20, 2012

$$f \equiv \{|f_i\rangle : i = 1,...,N\}$$

All the states in each basis encode same bit of information, such that,

$$e \equiv \{|e_i\rangle : i = 1,...,N\} = 0$$

and

$$f \equiv \{|f_i\rangle : i = 1,...,N\} = 1.$$

Table 1. Alice and Bob's interpretation of different basis states. If Bob's measurement index is different from Alice's index then they may assume a value in 0, 1 or ×. An error may occur because of the noise or eavesdropper.

Alice sends states	Bob measures states			
	$\|e_j\rangle$		$\|f_j\rangle$	
	Same index	*Different index*	*Same index*	*Different index*
$\|e_i\rangle$	×	*error*	×	0
$\|f_i\rangle$	×	1	×	*error*

Alice randomly chooses and sends any of the *e* or *f* states to Bob. Bob randomly selects one of the measurement bases, *e* or *f*, and measures the incoming photon's state. Alice publicly announces the indices *i* of all the states which she sends to Bob. Bob compares the indices of photons as a result of his measurement outcome with the indices announced by Alice. Bob interprets his measurement outcomes as a function of the index announced by Alice, cf. Table 1. Alice and Bob expect the outcome of their interpretation as '0', '1' or '×' indicating whether a '0', a '1' or no bit is transmitted. If they measure the different indices then they obtain a '0' or a '1', for *e* and *f* respectively, and if they measure the same indices then no bit is assumed to be shared. In an ideal case, it is impossible that they measure the different indices while measuring in the same bases but this may happen because of the system or signal noise or the intervention of an eavesdropper.

3. The transmission error-rates and efficiency

An eavesdropper *Evan* conventionally challenges the secure key distribution between Alice and Bob. In quantum key distribution whenever Evan tries to intercept and measure the encoded photons between Alice and Bob, it introduces an error, which can be measured as the error in the transmission of each state's index. An index transmission error (ITER) occurs when a photon prepared in $|e_i\rangle(|f_i\rangle)$ is measured at Bob's end as $|e_j\rangle(|f_j\rangle)$ with $i \neq j$. Assuming that Alice prepares the *2N* basis states of *e* and *f* with the same frequency and that Bob measures *e* and *f* with the same frequency and $|g_k\rangle$ denotes the Evan's possible measurement outcomes which are forwarded to Bob without alteration, the ITER of the scheme equals

$$P_{ITER} = 1 - \frac{1}{2N}\sum_{i=1}^{N}\sum_{k=1}^{N}\left[|\langle g_k|e_i\rangle|^4 + |\langle g_k|f_i\rangle|^4\right] \quad (1)$$

or in case of two mutually unbiased bases,

$$P_{ITER} = \frac{N-1}{2N} \quad (2)$$

Instead of calculating the transmission error-rate in terms of index, Alice and Bob may estimate the transmission error-rate in terms of bits. A quantum bit error-rate (QBER) is calculated by selecting a certain number of control bits from the obtained key sequence and compare them openly. For the existing scheme QBER is given as

$$P_{QBER} = \frac{2N - \sum_{i=1}^{N}\sum_{k=1}^{N}\left[|\langle e_i|g_k\rangle|^4 + |\langle f_i|g_k\rangle|^4\right]}{4N - \sum_{i=1}^{N}\sum_{k=1}^{N}\left[|\langle e_i|g_k\rangle|^2 + |\langle f_i|g_k\rangle|^2\right]^2} \quad (3)$$

Alice and Bob successfully share a key bit when both use a different basis provided that the index of the state measured by Bob should be different from the index of Alice's state. The success rate of the existing scheme is

$$P_{success} = \frac{N-1}{2N}. \quad (4)$$

It can be easily seen that as we increase the number of dimensions (*N*), the ITER and the success rate approach to *50%*. Suppose, Alice and Bob are agreed to use four dimensional basis states, such that

$$e \equiv \{|e_1\rangle, |e_2\rangle, |e_3\rangle, |e_4\rangle\}$$

and

$$f \equiv \{|f_1\rangle, |f_2\rangle, |f_3\rangle, |f_4\rangle\}$$

are mutually unbiased bases. In this case, the optimal choice of Evan is to measure states which lie on a line between the closest states of the *e* and the *f* bases, such that

$$|g_i\rangle = \frac{\cos\alpha|e_i\rangle + \sin\alpha|f_i\rangle}{(1 + \frac{1}{2}\sin(2\alpha))^{\frac{1}{2}}} \quad (5)$$

It can be calculated that in this case $P_{ITER} \geq 37.5\%$.

4. The generalized scheme

In order to estimate the full benefit of the existing key distribution scheme it is interesting to increase the number of bases more than two. It seems that if we increase the number of bases then it would create more difficulty for Evan to successfully perform an intercept-resend eavesdropping attack.

5. Basic idea

Suppose, for example, Alice and Bob use three mutually unbiased bases *e, f* and *h*, encoded as (*e*→0, *f*→1, *h*→2) such that

$$e \equiv \{\left|e_i\right\rangle : i = 1,...,N\} = 0,$$

$$f \equiv \{\left|f_i\right\rangle : i = 1,...,N\} = 1,$$

and

$$h \equiv \{\left|h_i\right\rangle : i = 1,...,N\} = 2.$$

However, with the existing key distribution protocol in this case, it would be impossible for Bob to understand which state Alice sends to him. Suppose Alice sends the state $\left|e_i\right\rangle$ and Bob measures in either $\left|f_j\right\rangle$ or $\left|h_j\right\rangle$ with $i \neq j$. Depending upon his measurement basis, Bob can make sure that the incoming photon state is not in one of the *f* or *h* basis but still he cannot confirm exactly in which basis Alice sends the photon.

One possible solution to this problem is to send the same photon state twice. If Alice again sends the same state $\left|e_i\right\rangle$ and Bob measures in a different basis like $\left|f_j\right\rangle$ with $i \neq j$ then Bob can easily confirm which basis state Alice sent to him. Although, repeatedly transmitting the same photon state solves the problem but this technique has some drawbacks. For relatively larger number of bases, say *b*, Alice and Bob have to prepare and measure *(b-1)* photons states to share one secret alphabet. Similarly, Evan will have the chance to perform intercept-resend attack in each round, which decreases the efficiency and security of the key distribution scheme. The better solution to this problem is that Alice and Bob create the pairs of bases, such that each basis has a pair with every other basis. In the case of three basis scheme *e, f* and *h*, three pairs can be constructed, as $S_1 = \{e, f\}$, $S_2 = \{e, h\}$ and $S_3 = \{f, h\}$.

Suppose Alice sends the state $\left|e_i\right\rangle$ and Bob measures in $\left|h_j\right\rangle$ with $i \neq j$, then Bob publicly announces any of the sets, which includes *h*. If, for example, he announces S_3 then Alice can make sure in which basis Bob did the measurement and eventually they share a secret alphabet '0'. On the other hand if, for example, Bob announces S_2 then Alice still cannot make sure in which basis Bob did the measurement. Hence there is a $1/_{b-1}$ chance, after achieving the different index in their measurement, that Alice and Bob cannot deduce the secret key alphabet. However, this reduction in the key rate may be compensated by the significant increase in the error-rate.

Table 2 Alice and Bob's interpretation of different basis states. If Bob's measurement index is different from Alice's index then they may assume a value in 0, 1, 2, ..., *b-1*.

Alice Sends	Bob measures					
	x^0	x^1	x^2	...	...	x^{b-1}
x^0	×	0	0	0	…	0
x^1	1	×	1	1	…	1
x^2	2	2	×	2	…	2
…	…	…	…	×	…	…
…	…	…	…	...	×	…
x^{b-1}	*b*-1	*b*-1	*b*-1	*b*-1	*b*-1	×

6. The generalized protocol

Let us first describe the necessary conditions for our key distribution scheme to complete the protocol.

1. Before starting the protocol Alice and Bob must agree on a set of bases B in two or higher dimensions to prepare and measure the photon states. The set B must contain any two or more bases which are pair-wise orthogonal. Such that $\mathrm{B}=\{x^0, x^1, x^2, ...x^{b-1}\}$, where *b* is the total number of bases in B.
2. Alice and Bob must decide the encoding scheme of the secret keys, which depends upon the number of bases used in the protocol. If *b* is the number of bases then Alice may choose 0, 1, 2…(*b-1)* alphabets to encode the secret key, cf. Table 2.
3. Alice and Bob must prepare the pairs of all the bases used in the protocol, such that, each basis has a pair with every other basis $\{(x^m, x^n) | m \neq n\} \forall x^m, x^n \in \mathrm{B}$ and $m, n = 0,1,2,...,b-1$.
4. To share a secret key Alice and Bob must reveal some information, through classical public channel, to make a strong correlation between the input states and the measurement.
    a. First, Alice must announce the index of each state after sending the photon to Bob.
    b. Secondly, Bob must announce a set S_i in all the cases where Bob's measurement index is different from Alice's index. Bob announces the set by randomly choosing from the sets of bases, which contain his measurement basis.

Suppose, Alice prepares her state in x^m and Bob measures in x^n with $m \neq n$ and Bob's measurement index is different from Alice's index. A shared key

alphabet can only be interpreted, according to **Table 2**, if the set announced by Bob is (x^m , x^n).

5. Alice should have equally many states to encode every alphabet to retain the symmetry.

In general, if *N* is the number of dimensions in each basis state, x^n denotes the *n*th basis and *b* denotes the total number of bases then the complete protocol works as follows:

1. Alice generates a random key sequence of classical bits and randomly assigns each bit value a random index $i = 1, 2, \ldots, N$.
2. Alice then uses her key sequence and sends single photons prepared accordingly in any of the bases states in $x^0, x^1, x^2, \ldots x^{b-1}$ to Bob.
3. Bob measures the state of every incoming photon, thereby randomly switching the measurement bases among $x^0, x^1, x^2, \ldots x^{b-1}$.
4. Alice publicly announces the random sequence of indices *i* used to establish the secret key.
5. Bob tells Alice which photon measurements have been successful and announces an appropriate pair set for each of them.
6. Alice tells Bob which pair sets successfully provide a secret key alphabet.
7. Alice and Bob interpret the corresponding photons states according to **Table 2**.
8. Finally, Alice and Bob determine whether an eavesdropper introduced an error into their communication. Whenever this error-rate is sufficiently small, Alice and Bob can assume that no eavesdropping has occurred otherwise they the protocol.

In this protocol it can be noted that Alice and Bob have a large variety of alphabets in terms of number of bases used in the scheme. In the following research it will be explored that how this increase in the number of bases influences the error-rate and efficiency of the scheme.

7. Conclusion

Its is shown in this paper that increasing the number of dimensions or the number of bases of the photon states may result in a significant increase in the error-rates introduced by an eavesdropper as a result of an intercept-resend attack. However, depending upon the number of bases the protocol may need to be modified in order to complete the process of sifting successfully. This has been shown in an example where Alice and Bob use three bases. The scheme may be further optimized to achieve better error-rates in terms of quantum bits and efficiency.

Acknowledgment

The authors appreciate help and support of DSS Group University of Leeds, UK, and funding from NED University of Engineering & Technology, Karachi for this research.

References

[1] Singh, S.: The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography. Anchor Books, New York (1999)

[2] Bennett, C., DiVincenzo, D.: Quantum information and computation. NATURE **404** (2000) 247-255

[3] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Reviews of Modern Physics **74** (2002) 145-195

[4] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (1984) 175

[5] Bennett, C.H.: Quantum Cryptography Using Any 2 Nonorthogonal States. Physical Review Letters **68** (1992) 3121-3124

[6] Bechmann-Pasquinucci, H., Peres, A.: Quantum cryptography with 3-state systems. PHYSICAL REVIEW LETTERS **85** (2000) 3313-3316

[7] Bechmann-Pasquinucci, H., Gisin, N.: Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. PHYSICAL REVIEW A **59** (1999) 4238-4248

[8] Beige, A., Englert, B.G., Kurtsiefer, C., Weinfurter, H.: Secure communication with a publicly known key (vol 101, pg 357, 2002). Acta Physica Polonica A **101** (2002) 901-901

[9] Beige, A., Englert, B., Kurtsiefer, C., Weinfurter, H.: Secure communication with single-photon two-qubit states. JOURNAL OF PHYSICS A-MATHEMATICAL AND GENERAL **35** (2002) L407-L413

[10] Khan, M.M., Murphy, M., Beige, A.: High error-rate quantum key distribution for long-distance communication. New Journal of Physics **11** (2009) 063043