Security Analysis and Optimization of BB84 QKD System Post-Processing

Pin Zhang and Xiangjie Mao
Telecommunication Engineering, Hangzhou Dianzi University, Hangzhou, China
Email: zhangpin@hdu.edu.cn; 944474017@qq.com

Abstract. Considering the rapid development of quantum technology, it has become inevitable to use this technology to develop an ultimately secured key exchange system. Quantum key distribution (QKD) technology has become more sophisticated, is expected to provide secure key distribution mechanism for the actual information security systems. The unique advantage of quantum cryptography is precisely its ability to guarantee absolute security. Previous works have demonstrated unconditional security of the ideal BB84 QKD system. However, on a typical QKD system, many practical situations often cannot satisfy the requirements of the ideal condition. This problem causes some security issues for practical QKD system. Therefore, it is necessary to analyze the security of QKD system under practical conditions, and identify the security implications on the practical physical systems and equipment, in order to find a method that guarantees the security of QKD system. The security of QKD system based on BB84 involves many aspects; this paper mainly focuses on how to resolve security issues that may exist, especially in the BB84 protocol post-processing. We introduce ways to tackle these issues and make vital key information leakage very small. Their impact on the security of entire QKD system is analyzed, and the interaction and security optimization between the various parts is researched. Finally, the thesis briefly introduces five sub-modules of post-processing of QKD system: the base comparison, error estimation, information correction, data check and privacy amplification; the existent security factors of each module is given, for error estimation and information correction is provided the secure model with those issues. Thus, the security model of post-processing is further optimized.

Keywords. Quantum key distribution; BB84 protocol; post-processing; privacy amplification.

1. Introduction
Quantum communication realizes the smooth communication between sender and receiver by quantum encryption, and establishes the communication connection between the two parties with the help of quantum mechanics. The communication method can generate a special key in both the sender and receiver, and the key is known only to both parties, thus improving the security of the communication process. The theory of the entire communication system of quantum communication is based on quantum mechanics. Two basic principles constitute the cornerstone of quantum communication. The first is Heisenberg's uncertainty principle, and the second is the unclonable theorem [1]. These principles ensure that both parties can exchange data in a completely secure environment. In addition, in quantum computing, the two parties of communication can easily detect whether there is a third party interferer who has an impact on this communication.

In quantum communication, eavesdroppers who disrupt the communication are detected by both sides of the communication. The reason for the collapse mentioned above USES quantum mechanics measurement. The quantum state measured will lead to the destruction of its current state, and the listener
can use quantum superposition state and quantum entanglement state for detection [2-4]. The classic encryption technology cannot know whether a third party is listening on the channel, and its security is completely based on the reliability of the encryption algorithm. In 1982, Wootters and Zurek proved the principle of non-cloning. It states that under the condition of no information, the user cannot copy the state and quantum bits of the quantum channel, and the illegal eavesdropper can only listen to the data of the quantum channel on the premise of predicting the random basis of the sender, which is also the result of non-cloning principle.

The role of the cloning is to be able to do it as long as there is a channel eavesdroppers tapped, so must be found between two communication parties, greatly improves the confidentiality and integrity of information, but there is a kind of situation is special, is the master in the eavesdropper can advance the sender sends a random base, and measure the qubits and then passed on to the receiver. In order to ensure that the keys of both parties are the same, both parties of communication adopt the error correction method of information negotiation on the keys. It is performed through a common channel, and there is the possibility of being monitored by Eve, so it is important to minimize the sending of information about each key. However, from the perspective of coding theory, information negotiation is essentially the source coding of auxiliary information, so any coding scheme applicable to this problem can be used for information negotiation. In recent years, the latest turbine coding [5], LDPC (low-density check code) [6] and polar coding [7] can effectively improve the cascading effect [8].

This paper analyzes the QKD (Quantum key distribution) post-processing module using these mathematical models. The results of previous studies using LDPC show that the efficiency of QKD systems is reduced. It can be known from the simulation results that future research in this field should focus on the application of improved coding, so that the system can have higher efficiency and better adaptability. The analysis also shows that when some communication between two trusted parties exceeds the security threshold, having a security BER (bit error rate) threshold will cause system redundancy.

2. Previous Work

The most widely used and well-known error correction protocol in QKD scenarios is the Cascade algorithm. Brassard and Salvail proposed this algorithm [9]. At present, there are many improved schemes for cascade algorithm [10-11]. However, the basic remote principle and characteristics of the algorithm are still maintained, and the negotiation efficiency is optimized by selecting and increasing the length of the group. By virtue of its simple implementation, high efficiency, strong scalability and robustness, and flexible interaction, cascading algorithm is favored by scholars and experts. Now it is widely used and also becomes the basic standard in this field. Cascade algorithm is often chosen as the benchmark for comparison. Later emerging modern coding techniques such as LDPC have been neglected for a long time, and only in recent years have they been applied to discrete variable QKD systems. And used in Ref. [12]. However, LDPC is mainly not designed for a specific occasion, so the algorithm is not high flexibility, in addition to the advantages of forward error correction, other aspects are still not as good as the cascade algorithm. This coding is also only used in the continuous variable QKD system [13] scenario. In Ref. LDPC was used for the first time to optimize BSC (Binary Symmetric Channel). Although the result is close to the optimal value of the design code, the efficiency curve shows the characteristics of sawtooth wave due to lack of adaptability [14]. Because the bit error rate in transmission can change, algorithm protocols must be able to handle this change. Considering that the unconditional security of the actual QKD system needs to be proven, the screening module in post-processing is described in the paper. Alice uses decoy weak coherent light, which can resist Eve's PNS (photon number splitting) attack. A method of selecting the average of straight and diagonal basis of Alice and Bob is proposed. This method results in a fault tolerance threshold of approximately 11%. Alice and Bob will consider whether to continue the error negotiation or discard the result and start again based on the threshold. Through research, it is proposed to use Shannon coding during error correction. Simulation results show that compared with Cascade algorithm, Shannon coding makes the whole post-processing system more secure.
3. QKD System Post Processing Security Analysis

3.1. Security of Base Comparison Module

Steps during the base module post treatment of BB84 protocol:

(1) For a bit string sequence of length N, Alice prepared a set of randomly selected bases quantum bit string of length N, and then sends it to Bob.

(2) Bob randomly select a group of base pairs quantum bit string of length N for measurement. Excluding empty signal of Raw code, retaining effective signal.

(3) Bob sends his base and location information to Alice through a public channel. Alice compares her base and the location information with Bob’s, the location information obtained under the same group.

(4) Alice again sends the group and location information that are same to Bob, Bob extracts location information bit value under the same base, preliminary we get Alice and Bob shared screening key.

Due to the randomness of bases Alice and Bob selected, according to probability theory shows that if in the absence of the eavesdropper approximately about 50 percent of the base information is the same, then the sifted key length is about half the length of the initial key. Otherwise sifted key length will be less than half of the original, as shown in tables 1 and 2.

Table 1. Basis examples with no eavesdroppers.

| Alice | Bob |
|-------|-----|
| + × + | + × + |
| ↑ ^ ↑ | ^ Z Z |
| 1 1 0 | 0 0 1 |

Table 2. Basis examples with eavesdropper.

| Alice | Eve | Bob | Raw key | Error |
|-------|-----|-----|---------|-------|
| + × + | × × + | + × × | 0 1 | E |
| ↑ ^ ↑ | ^ Z Z | ^ Z Z | ^ 0 0 1 |
| 1 1 0 | 1 1 0 | 1 1 0 | 0 0 1 |
| 0 1 1 | 0 1 1 | 0 1 1 | 0 0 1 |
| 0 1 0 | 1 1 0 | 1 0 1 | E |

The base module safety analysis:

Assuming that Alice has a single photon source in the quantum state transmission process, according to the quantum non-cloning theorem, as long as the eavesdropper intercepts a single photon, the quantum state of the photon must change, and it is easy to find the existence of the listener. The two sides will know about the presence of Eve by error estimate, Alice will resend the message. If Eve measures the single photon Alice sends to Bob, but Eve surely doesn’t know Alice’s base information, she can only randomly select the bases. According to quantum uncertainty principle it shows that, Eve can only get part of the sifted key information. After the error estimate, after information negotiation, the key information Eve obtained will get less. And also by privacy amplification, it shows that the amount of final key information Eve can obtain has been reduced exponentially.
In the actual QKD problem, Alice uses weak coherent light source instead of single photon light source to solve the problem. According to the above description, Eve can use a PNS attack to obtain all the filtering key information on the base module when Alice uses a single photon light source. As Alice uses weakly coherent optical deceptions, Eve cannot distinguish the deceptions from multi-photon pulses by PNS attacks, and the useful information obtained is naturally minimal. Thus, the security of base module information transmission is realized.

3.2. Security of Error Estimation Module

Steps during the error estimation post treatment of BB84 protocol:

1. Alice randomly draws a subset of a certain percentage of from the sifting code (sample size is about 10% of the random subset);
2. Alice transmits the bit value of the subset and location information corresponding to the subset to Bob via a common channel;
3. Bob according to the received position value, takes the same position’s bits information from the sifting keys. Compares if his selected sifting bits information are identical with sifting bits information Alice selected, records the number of mismatches;
4. Bob will transmit the inconsistent values recorded in (3) to Alice via the public channel and them. Alice and Bob calculate the estimated error rate $\varepsilon$ by using the inconsistent values;
5. Alice and Bob according to previously set threshold $\varepsilon_0$ make some decisions. If the error rate $\varepsilon$ is less than a given threshold, the packet is considered safe, otherwise considered that there is a possible eavesdropping, they discard the packet and continue to process the next packet;

Threshold $\varepsilon_0$ refers to the ideal case without eavesdropping, the maximum error rate of information transfer process caused by an eavesdropper eavesdropping on the quantum channel, and will inevitably lead to bit error rate $\varepsilon$ increased on the sifting code of the communicating parties, therefore, by estimating the bit error rate $\varepsilon$ of both communicating parties’ sifting codes, we can determine whether Eve is eavesdropping valid information (as shown in figure 1).

**Figure 1.** The sifting process.
**BER estimate safety analysis module:**

In an ideal case of quantum key distribution, when sifting bit length $N$ is infinitely long, if $n = N - m$ is the remaining length of Alice and Bob key after the error estimate, then let $N \to \infty$ when there is $n/N \to 1(N \to \infty)$, indicating that the information bits of infinite length, the key length and the error estimation loss of qubits are unrelated. We use the randomly selected qubits to estimate the bit error rate $\varepsilon$ of the remaining qubits to ensure there are no errors, BER fluctuation will be close to zero, and then we will get the true value of the BER with the same results.

In the actual quantum key distribution, the qubit length of the key is related to the qubits randomly selected when the bit error rate (BER) estimated length $m$. Since the estimation to BER done in the error estimation module will not be perfect, they tend to produce error $\zeta$, so the actual BER will fluctuate in the interval $(\varepsilon - \zeta, \varepsilon + \zeta)$. Then we obviously according to law of large numbers in probability and statistics estimate the error of the bit error rate $\zeta$. Thus we can be able to sift key of limited length to get the exact value of the BER estimates, to avoid qubits loss during error estimation to make impact on the final key generation [15].

**Theorem:** (law of large numbers) event $\sigma$ ( $\sigma$ classic event or quantum state) of $M$ samples were measured, let the measurement values have $d$ possible results, then there is law of large numbers, the true value of $\sigma$ belongs to the probability of the subset below is greater than $1 - \varepsilon'$.

Using this theorem we can use the probability of to at least get to the interval where the true value is:

$$[\lambda - \zeta(M, \varepsilon), \lambda + \zeta(M, \varepsilon)]$$

(1)

where $\lambda$ is the measured value for $M$ samples of $\sigma$.

According to the law of large Numbers above, the estimated error rate, i.e., the difference between the measured value and the true value, can be obtained based on the selected confidence probability of $1 - \varepsilon'$. The greater the confidence interval $1 - \varepsilon'$, the greater the estimated error rate, the greater the probability of identical measurements, and the greater the true bit error rate; the smaller the confidence interval $1 - \varepsilon'$, the lesser the probability that the measured value and the true value of the bit error rate are same. More importantly, the errors $\zeta(M, \varepsilon)$ between the measurement and true value of bit error rate can be determined according to the above law of large numbers, so that after bit error rate estimation we can make correction to the measured values, thereby enhancing the authenticity and accuracy of the BER measurements. This does not only provide a true and reliable protection for the security of QKD system after treatment, but also plays a vital role for the last three modules: error negotiation, data validation, and important parameter settings in privacy amplification.

### 3.3. Security of Privacy Amplification Module

Steps during privacy amplification in the BB84 protocol:

1. After data validation, Alice and Bob obtain the same key. Alice from array of Universal Hash functions randomly select a Hash function, and send a description of the Hash function to Bob.

2. Bob construct to Hash function according to the received Alice’s message, then sends the “complete” information back to Alice. To ensure synchronization in the next step between the two parties.

3. Alice and Bob conduct Hashing on both sides of the error-free keys, eliminate key information obtained by eavesdropper Eve. Thereby obtaining a final key under a safety factor.

In quantum communication, if an eavesdropper conducts only a small amount of eavesdropping, then it will not cause too much impact on the error rate of the communication parties sifting code. It is easy to submerge in the channel BER fluctuations. Thereby escaping detection in the error estimation stage; in the process, the two sides exchange a lot of comprehensive information on the key string through the classical communication channel, clever eavesdropper can obtain partial key information from comprehensive information. Thus the entire QKD process, an eavesdropper can obtain some information about the key, to ensure the security of QKD system key. We need a process that can removed the information an eavesdropper could get, so that information about the key obtained is sufficiently small, this process need to be implemented by the privacy amplification.
In general, privacy amplification using Universal 2 Hash function, let Alice and Bob have Reconciled Key of n-bit string $x \in \{0,1\}^n$, they estimated that Eve knew of $t$ bits among them and $s$ bits selected as the Security Reference indicator, the length of the key after privacy amplification denoted $r$ bit Hash Function array: $F: \{0,1\}^n \rightarrow \{0,1\}^r$, where $r = n-t-s$. Each publicly selected random $f \in F$, so that $y = f(x)$, the final shared key is $r$ bit string $y \in \{0,1\}^r$. If matrix, $f$ is an $n \times r$ binary matrix.

From the above analysis it is shown that privacy amplification is the most critical stage of QKD post-treatment, it is directly related to the security of the final key. To demonstrate QKD post treatment unconditional security, we need to be introduced Renyi entropy in order to achieve that. Renyi entropy concept in general consists of generalized introduction of probability distribution. Here we use a simple collision probability to introduce Renyi entropy. Let $X$ be a random variable value picked from $\chi$, and its distribution be $P_x$, same probability of occurrence of $X$ in two identical experiments, the collision probability is defined as the sum of squares of all these probabilities, namely:

$$P_c(X) = \sum_{x \in \chi} P_x(x)^2$$  \hfill (2)

Thus Renyi entropy is defined as the $X$ collision probability of the negative logarithm of [10], namely:

$$R(X) = -\log_2 P_c(X)$$  \hfill (3)

In the conditions of the event $y$, we can define the conditional probability distribution $P_{dy}$, collision probability and Renyi entropy as $P_d(X | y)$ and $R(X | y)$ respectively.

The following theorems prove the unconditional security of the key by privacy amplification [10]. According to Bennett C H, Brassard G, Crépeau C [10], Theorem 2 shows:

$$H(Q | G) \geq R(Q | G) \geq r - \frac{2^{r-R(X)}}{\ln 2}$$  \hfill (4)

Promote this theorem to the conditional probability distribution $P_{W|V=v}$, relevant privacy amplification corollary can be obtained.

Let $P_w$ is an arbitrary probability distribution, $v$ is Eve observed $V$ values. If Eve on $W$ of Renyi entropy $R(W | V=v)$ the entropy is at least $c$, Alice and Bob choose $K=G(w)$ as a key. Where $G$ is the universal class Hash function in a randomly selected amount $G:W \rightarrow \{0,1\}^t$. Then

$$H(K | G, V = v) \geq r - \log_2 (1 + 2^{-r}) \geq r - \frac{2^{r-c}}{\ln 2}$$  \hfill (5)

According to this deduction drawn when $r < c$, Eve about entropy of $K$ approaches its maximum value, and $K$ distribution about Eve tends to be uniform. In particular, she obtained $K$ information about $H(K)$ - $H(K | G, V = v)$ can be made arbitrarily small. More specifically, the amount of information she obtained in accordance with the key index $r-c$ decrease exponentially. Thus may know the key is unconditionally secure.

4. Simulation of QKD System Analysis

Through research, some methods can be proposed to deal with Eve, an eavesdropper, in the actual QKD system. Protocols such as B92 [16] and EPR [17] do not provide authentication functions between the communicating parties. Using MATLAB for simulation experiments, Shannon coding was introduced during the simulation to reduce the actual number of bits leaked during error correction. At the same time, a LFSR (linear feedback shift register) was used during the error correction certification.

In the simulation phase of this work, 500 qubits are selected in table 3 as the initial value for key transmission. At this point, eavesdropping is disabled to simulate the absence of eavesdropping in the system. The simulation results are shown in the first column of table 4. When repeated simulations are performed, the initial values in table 3 remain unchanged, and the simulation conditions are changed. At
this time, eavesdropping is enabled, and the statistics in the second column of table 4 are obtained. The results show that the length of the final key has become shorter, the leakage of information has increased, and the length of the key before error correction has become longer.

Table 3. Initial values with eavesdropping off.

| Property             | Value |
|----------------------|-------|
| Qubit Count          | 500   |
| Basis choice bias    | 0.5   |
| Eve basis choice bias| 0.5   |
| Eavesdropping        | 0     |
| Eavesdropping rate   | 0.1   |
| Error estimation sampling rate | 0.2 |
| Biased error estimation | 1 |
| Error tolerance      | 0.11  |

Table 4. Statistics and overview without eavesdropping.

| Property                                      | Value   |
|-----------------------------------------------|---------|
| Initial number of qubits                      | 500     |
| Final key length                             | 68      |
| Estimated error                              | 0.0     |
| Eavesdropping                                | 0       |
| Eavesdropping rate                           | 0.1     |
| Alice/Bob basis selection bias               | 0.5     |
| Eve basis selection bias                     | 0.5     |
| Raw key mismatch after error correction      | 0       |
| Information leakage (Total number of disclosed bits) | 109 |
| Overall key cost for authentication          | 256     |
| Key length before error correction           | 197     |
| Bit error probability                        | 0.0508  |
| Bits leaked during error correction          | 77      |
| Shannon bound for leakage                    | 58      |
| Security parameter                           | 20      |

As the error sampling rate increases, information leakage becomes very small. This also reduces the loss of Shannon coding. These advantages have a huge impact on the length of the final key. Therefore, it is more secure for the system to determine an error sampling rate threshold that allows useful key information to be transmitted along the channel.

4.1. The Process of BB84 Quantum Transmission Is as Follows:

Alice prepares to send a sequence of 500 qubits to Bob through the quantum channel, and she randomly selects a basis for each qubit, linear polarization (horizontal /0 degrees and vertical /90 degrees) or diagonal polarization (+45 degrees and -45 degrees deviation). She then plotted the horizontal and vertical qubit states |0⟩ and |1⟩, and |+⟩ and |−⟩ states with +45 degree and -45 degree displacements. Further details:

Alice sends Bob 500 qubits with a base selection bias of 0.5.
Eve is not eavesdropping on the quantum channel.
4.2. Sifting
Bob announced the qubits he successfully measured on the public classic channel. Alice and Bob then exchange the case of their chosen basis through the channel. They verify these three information exchange processes. Whenever the base selection situation is the same, they add the corresponding bits to their personal key, and the average probability of this situation is 50%. In the absence of channel noise, the two keys should be the same unless there is an eavesdropper.

Screening authentication LFSR common hash:

If Alice and Bob communicate, we first need to authenticate the exchange information sent, and LFSR the common hash scheme to operate the data information by sharing the key held in advance. Further details:

- When Bob tells Alice he successfully measured the qubit information, an authentication label needs to be added to the original data as a voucher. Certification fee for key materials: 64.
- Bob told Alice, he chose the basis for measuring qubits and attached an authentication tag to the data message as a voucher. Certification fee for key materials: 64.
- Alice told Bob she chose the basis for preparing qubits and she attached an authentication label to her message. Certification fee for key materials: 64. During the filtering phase, the above three messages that establish interactive connections require authentication.

4.3. Reconciliation

4.3.1. Bias Error Estimate. Here, Alice and Bob uses the biased error estimation scheme to measure the deviation value, random linear and diagonal based two test subset to do all the measurement, but it can only be used in a particular situation, is targeted at a specific situation, also in listening to the attack, he also has the advantages of strong preset fault tolerance threshold error message or consultation to determine the realization of the error correction, how it works: Alice and Bob to filtered key arrangement in the first place, and then by comparing the error a subset of the planar filter button is used to estimate error. Eliminates errors in bitstrings.

An error rate of 0.0 was estimated using a sampling ratio of 0.2.

4.3.2. Error Correction, Cascade. Alice and Bob perform an interactive error correction scheme called Cascade on the public channel in order to locate and correct the erroneous bits in their sifted bit strings. Figure 2 clearly compares the sifting results in different circumstances. Further details:

- Cascade was run 4 rounds in order to correct the errors.
- 10 erroneous bits were detected and corrected.
- 77 bits were leaked in order to correct the errors.

With an error probability of 0.0508, the Shannon bound for the number of leaked bits is: 58.0, compared to the actual number of leaked bits: 77.

4.4. Error Correction Confirmation and Authentication
Alice and Bob confirm and authenticate the error correction phase by computing the hash of their error corrected keys using their mutually pre-shared secret key and by comparing their respective digests. As shown in figure 3, information leakage becomes significantly small when error sampling rate is increased. Further details:

- 64 bits of key material (pre-shared secret key) were used to authenticate.
- The LFSR universal hashing scheme was used for authentication.

4.5. Privacy Amplification
When Alice and Bob transmit data, they use the privacy enhancement protocol, which realizes the global hash function based on the Toeplitz matrix to achieve the purpose of protecting privacy. Meanwhile, the key information obtained by Eve will be minimized, and a security parameter can be defined to ensure
that the information obtained by Eve can be reduced to a certain length freely. This also reduce Shannon bound losses, as shown in figure 4. Specific process:

109 bits were leaked up to this point.
The key length before running privacy amplification: 197 bits.
The final key length is: 68 bits.
The chosen security parameter is: 20.

Figure 2. Sifting plot.

Figure 3. Biased error estimation plot.
The simulation stage of this work, table 3 shows the initial values where 500 qubits are used for the key transmission. Eavesdropping is disabled to show a situation where there is no eavesdropping on the system, and the results are shown in table 4. When the simulation is repeated with the initial values in table 3 remain unchanged, we obtain the statistics presented in table 5. The final key length becomes shorter, information leakage has increased, and key length before error correction has become longer, all as a result of eavesdropping due to Eve’s presence in the system.

**Table 5.** Statistics and overview with eavesdropping.

| Property                                      | Value  |
|-----------------------------------------------|--------|
| Initial number of qubits                      | 500    |
| Final key length                              | 46     |
| Estimated error                               | 0.0833 |
| Eavesdropping                                 | 1      |
| Eavesdropping rate                            | 0.1    |
| Alice/Bob basis selection bias                | 0.5    |
| Eve basis selection bias                      | 0.5    |
| Raw key mismatch after error correction       | 0      |
| Information leakage                           | 135    |
| (Total number of disclosed bits)              |        |
| Overall key cost for authentication           | 256    |
| Key length before error correction            | 201    |
| Bit error probability                         | 0.0796 |
| Bits leaked during error correction           | 103    |
| Shannon bound for leakage                     | 81     |
| Security parameter                            | 20     |

**5. Conclusion**

In the above analysis. First, this paper experiments with Alice by weak coherent light in the process of the state of decoy and Eve can’t distinguish the bait from the multiphoton pulse state, so its get very little information, ensure the information security of the base module; Second, this article confirmed the estimation error rate to help the eavesdropper if eavesdropping on the quantum channel information.
effectively, bias laws help to judge the difference between measured value and the bit error rate, and make a correct and improve the authenticity and validity of measurement values; Third, the global hash function can play a key role in the privacy module. Renyi entropy is introduced to prove that the post-processing of QKD system can achieve unconditional security.

When the error sampling rate is increased, information leakage becomes significantly small. This also reduce Shannon bound losses. But these advantages have significant impact on the final key length. Therefore, it’s considered safer for the system to have a lower error sampling rate.

References
[1] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned Nature 299 802-803.
[2] Gerhardt I, Liu Q, Antía Lamas-Linares, Skaar J, Kurtsiefer C and Makarov V 2011 Full-field implementation of a perfect eavesdropper on a quantum cryptography system Nature Communications 2 14.
[3] Brassard G and Salvail L 1994 Secret-Key reconciliation by public discussion Lecture Notes in Computer Science 765 410-423.
[4] Sugimoto T and Yamazaki K 2000 A study on secret key reconciliation protocol “Cascade” IEICE Trans. Fundam. Electron. Commun. Comput. Sci. E83-A (10) 1987-1991.
[5] Liu S, Van Tilborg H C A and Van Dijk M 2003 A practical protocol for advantage distillation and information reconciliation Designs Codes Cryptogr. 30 (1) 39-62.
[6] Buttler W T, Lomareaux S K, Torgerson J R, Nickel G H and Peterson C G 2003 Fast, efficient error reconciliation for quantum cryptography Phys. Rev. A 67 (5) 052303.
[7] Nguyen K-C, Van Assche G and Cerf N J 2004 Side-information coding with turbo codes and its application to quantum key distribution arXiv: cs/0406001.
[8] Elkouss D and Martínez-Mateo J and Martí V 2011 Quantum Information & Computation 11 226.
[9] Jouguet P and Kunz-Jacques S 2013 Quantum Information and Computation 14 (3&4).
[10] Bennett C H, Brassard G, Crepeau C and Maurer U M Generalized privacy amplification IEEE Transactions on Information Theory 41 (6) 1915-1923.
[11] Lo H-K, Curty M and Tamaki K 2014 Secure quantum key distribution Nature Photonics 8 (8) 595-604.
[12] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouil R and Grangier P 2009 Field test of a continuous-variable quantum key distribution prototype New. J. Phys. 11 (4) 045023.
[13] Elliott C, Colvin A, Pearson D, Pickalo O, Schlafer J and Yeh H 2005 Current status of the DARPA quantum network quant-ph/0503058.
[14] D Elkouss, A Leverrier, R. Alleaume and J J Boutros 2009 Efficient reconciliation protocol for discrete-variable quantum key distribution IEEE Int. Symposium on Inf. Theory pp 1879-1883.
[15] Elkouss D, Martinez J, Lanco D and Martin V 2010 Rate compatible protocol for information reconciliation: An application to QKD IEEE Inf. Theory Workshop (ITW) pp 145-149.
[16] Zou M and Zhang G 2004 Information investigation for B92 protocol in quantum cryptography Photonics Asia 2004 pp 181-191.
[17] Khan M I and Sher M 2003 Protocols for secure quantum transmission: A review of recent developments Pakistan Journal of Information and Technology 2 265-276.