Science in China Series F: Information Sciences

www.scichina.com
info.scichina.com
www.springerlink.com

Realization of error correction and reconciliation of continuous quantum key distribution in detail

QIAN XuDong†, HE GuangQiang & ZENG GuiHua

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200030, China

The efficiency of reconciliation in the continuous key distribution is the main factor which limits the ratio of secret key distribution. However, the efficiency depends on the computational complexity of the algorithm. This paper optimizes the two main aspects of the reconciliation process of the continuous key distribution: the partition of interval and the estimation of bit. We use Gaussian approximation to effectively speed up the convergence of algorithm. We design the estimation function as the estimator of the SEC (sliced error correction) algorithm. Therefore, we lower the computational complexity and simplify the core problem of the reconciliation algorithm. Thus we increase the efficiency of the reconciliation process in the continuous key distribution and then the ratio of the secret key distribution is also increased.

continuous quantum key distribution, reconciliation process, optimal partition of interval, SEC algorithm, estimation function

1 Introduction

Information security plays a more and more important role in this society, and cryptography is an important tool to ensure the security of the information. Now the cryptography system relies on the complexity of the math problem. However, with the improvement of the ability of computer and the study of the quantum computer, the cryptography algorithm such as RSA faces great challenge. Luckily, the quantum cryptography[1−3] based on classical cryptography and quantum physics draws our attention. Its security is ensured by the basic principle of the quantum mechanics. The quantum uncertainty principle and non-cloning of quantum states make the quantum cryptography safe[4−6]. Thus, the quantum cryptography has a compelling prospect and good performance.

Now the study of the quantum cryptography always uses discrete physical variable as the signal carrier such as single photon and week laser pulse. However, discrete quantum key distribution (abbreviated as QKD) needs the production and detection of the single photon, and it is very hard to do the experiment. Moreover, the channel capacity is also very low; it means one pulse can carry very little information. However, if we use continuous quantum signal such as squeezed state or coherent state as the signal carrier, we can use heterodyne balance receiver as the detector, so we can easily control and operate the quantum signal and also it can achieve high channel capacity. Thus,

Received March 12, 2008; accepted October 14, 2008
doi: 10.1007/s11432-009-0147-0
†Corresponding author (email: dictator2002@sjtu.edu.cn)
Supported by the National Natural Science Foundation of China (Grant No. 60773085)

Citation: Qian X D, He G Q, Zeng G H. Realization of error correction and reconciliation of continuous quantum key distribution in detail. Sci China Ser F-Inf Sci, 2009, 52(9): 1598–1604, doi: 10.1007/s11432-009-0147-0

many scholars pay much attention to the continuous QKD[7,8].

The efficiency of reconciliation in the continuous key distribution is the main factor which limits the ratio of secret key distribution. Now the reconciliation algorithm of the continuous QKD[9] consists of three parts: the partition of intervals, the estimation of bit and the error correction. The reconciliation process in this paper is referred to the first two parts. These parts need much computation of the double integrator. Thus, it lowers the efficiency of the reconciliation algorithm. This paper substitutes Gaussian distribution for the none-Gaussian distribution with the same numerical character so it simplifies the computation of the relative entropy. Through the analysis of the bit estimation, this paper proposes a very simple estimation function. Therefore, we can estimate the bit through the comparison of the numbers without the double integrator. These two aspects that we proposed in this paper can improve the efficiency of reconciliation algorithm used in continuous QKD.

The second part of the paper introduces the basic knowledge of the discrete QKD. The third part introduces the relationship and the difference of the discrete QKD and the continuous QKD. The fourth part optimizes the partition of interval. The fifth part optimizes the SEC algorithm, proposes the estimation function and discusses the physical meaning of it. The sixth part gives the summary.

2 Discrete QKD

This paper first introduces the steps we need to implement the discrete QKD, and then we will introduce the difference and relationship between discrete QKD and continuous QKD in order to show how continuous QKD works.

2.1 Initialization phase

This paper uses the satellite model[10] to show the initialization phase of the QKD. Suppose a satellite source sends the information to Alice, Bob and Eve through three binary symmetrical channels. The error rates of the three channels are ε_a, ε_b and ε_e respectively. Thus, Alice, Bob and Eve obtain a relevant discrete sequence X, Y, Z, respectively. Under the certain condition, Alice and Bob can obtain secret key from X and Y through reconciliation and privacy amplification. The study of Maurer[10] shows that if and only if $\varepsilon_e > 0$ can Alice and Bob obtain a secret key from X and Y. Moreover, he also gives us the minimum and maximum rate of the secret key.

2.2 Communication phase

Communication phase consists of three parts: data distillation, information reconciliation and privacy amplification.

2.2.1 Data distillation. Alice and Bob process data distillation through authenticated channel (Eve can eavesdrop on the content they exchange but he cannot modify or delete the information). After data distillation, we obtain three discrete sequences X', Y', Z'. They meet the requirement $I(X';Y') > I(X';Z')$, $I(X';Y') > I(Y';Z')$. Now we have some mature data distillation algorithm[11] such as repeat code protocol and binary check protocol.

2.2.2 Information reconciliation. After data distillation, we can obtain two discrete sequences X' and Y' with low error rate. The process of information reconciliation is as follows: Through authenticated channel, Alice and Bob exchange some information. They can find errors, and correct or discard them by using this information. After the process, Alice and Bob can obtain X'' and Y'' with $\Pr(X'' = Y'') \approx 1$, we use S to represent this bit sequence.

2.2.3 Privacy amplification. After information reconciliation, we obtain S, but S is not secure. Since Eve can eavesdrop the information exchanged through the authenticated channel, he can obtain a sequence S'. S' consists of some part of the S, and the objective of the privacy amplification is to discard the information Eve knows and obtain a secret key.

3 The relationship and difference between discrete QKD and continuous QKD

The main difference between discrete QKD and continuous QKD is in the initialization phase, data

distillation phase and information reconciliation phase. The initialization phase in the continuous QKD is as follows: Alice receives an x, and x is a realization of the continuous random variable X. Bob receives an x', and x' is also a realization of the continuous random variable X'. X and X' likes the X and Y discussed in section 2.1. The only difference is that X and Y are bit sequences whereas X and X' are continuous random variable. During the data distillation phase in continuous QKD, some information is exchanged through the authenticated channel. Some x and x' are discarded, while others are reserved. The reserved x and x' form the random variable X'' and X'''. Eve eavesdrops on the information exchanged through the authenticated channel and obtains a random variable Y'. The objective of the data distillation in the continuous QKD is to make $I(X'';X''') > I(X'',Y')$ and $I(X'';X''') > I(X''',Y')$. We use X and X' to substitute for X'' and X''' respectively for easy use.

The information reconciliation phase (reconciliation process and error correction process) is the most important step in continuous QKD. The reconciliation process includes two steps:

1) The partition of the interval. The x received by Alice and x' received by Bob meet some probability distribution. In order to distill some information from them, we should discretize x. It is the process of partition of the interval. Then, Alice encode the interval, and tell Bob the rule of the encoding.

2) Bit estimation. According to the reconciliation information and x' received from Alice, Bob can distill some information. This process is called bit estimation.

After these two steps, Alice and Bob share two long bit sequences. The errors in the two sequences can be corrected through the algorithm used in the discrete QKD. This means after bit estimation, the error correction phase and privacy amplification process are the same as the ones in discrete QKD.

In the next two sections we will discuss the optimization of the partition of the interval and the design of the bit estimation function.

4 The partition of the interval

First, we will introduce the principle of the reconciliation algorithm[9]. Suppose Alice sends L copies of x to Bob, so the average information carried by x is $H(K(X)) - I(K(X);E) - (|C|/L)$. Obviously, the algorithm's objective is to minimize the $I(K(X);E) + (|C|/L)$ so that the single symbol carries more information. $I(K(X);E)$ represents the information Eve eavesdropped. Since this paper will not discuss the privacy amplification, we do not pay attention to $I(K(X);E)$. The minimum of $|C|$ is $LH(K(X)|X')$[7], so the maximum of $H(K(X)) - (|C|/L)$ is $I(K(X);X')$.

In the information reconciliation process of continuous QKD, we should find a good way to partition the interval so the $I(K(X);X')$ can approach the maximum $I(X;X')$. From ref. [12] we know the sufficient and necessary condition is as follows:

$$\alpha(x_A) = \arg\min_{k=1}^{N} D(p(X_B|X_A = x)||p(X_B|K = k)), \tag{1}$$

$$D(q(x)\|t(x)) = \int_{-\infty}^{+\infty} p(x)\log\frac{q(x)}{t(x)}dx$$

is the relative entropy of $q(x)$ and $t(x)$, and it describes the similarity of them.

We cannot retrieve the optimal interval partition through one computation, so we should use iterative operation. The theory is discussed in ref. [12] and we give the summary here:

Theoretical iterative algorithm:

S1: Random choose N intervals $Q_k(1 \leqslant k \leqslant N)$.

S2: Compute the average conditional probability density of each interval

$$\forall k = 1, 2, ..., N : f_k = E[p(x'|X)|X \in Q_k].$$

S3: $\forall k = 1, ..., N : Q_k \leftarrow \{x|\forall j \neq k\ D(p(x'|X = x)||f_j) > D(p(x'|X = x)||f_k)$.

S4: Continue the steps above until the convergence.

From the above steps, we know we should always use double integrator, and we also need iteration. Thus, if we use it directly, the efficiency is low. This restricts the efficiency of the information phase of the secret key agreement protocol. In this section we propose a simplified solution for the partition of the interval.

First we will introduce the properties of the relative entropy. In order to simplify the computation of the relative entropy, we constructed a Gaussian distribution with the same numerical character to replace the none-Gaussian distribution. We used the properties of the relative entropy of the Gaussian distribution and compute the separation of the adjoining interval. Thus, the partition of the interval is simplified. We use $\Gamma \sim N(\mu, \Sigma^2)$ to represent a random variable Γ—its variance and mathematical expectation are Σ^2 and μ, respectively, and it also follows a Gaussian distribution.

1) The properties of the relative entropy. Suppose $A \sim N(\mu_1, \sigma_1^2), B \sim N(\mu_2, \sigma_2^2)$, so the relative entropy of the density functions of random variable A and B is

$$D(A(x)||B(x)) = \ln \frac{\sigma_2}{\sigma_1} - \frac{1}{2} + \frac{\sigma_1^2 + (\mu_1 - \mu_2)^2}{2\sigma_2^2} nats. \tag{2}$$

2) The real probability distribution. Since the coherent state is the Gaussian state, it likes the AGWN, so

$$C(x') = p(x'\,|X = x\,) = \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}. \tag{3}$$

The average conditional probability density function in the interval $Q_k = \{x|a \leqslant x \leqslant b\}$ is

$$\begin{aligned} D(x') = p(x'|K = k) &= \int_a^b p(X = x) p(x'\,|X = x\,) dx \\ &= \int_a^b p(X = x) \frac{1}{\sqrt{2\pi}\sigma} \mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}} dx. \end{aligned} \tag{4}$$

3) The equivalent Gaussian distribution. If we put eqs. (3) and (4) into eq. (1), we can compute the relative entropy of $C(x')$ with respect to $D(x')$. After many iterations, we can obtain the exact partition of the interval. However, the computation of the relative entropy of a Gaussian function with respect to a none-Gaussian function is very complex. Thus, the efficiency of the information reconciliation is low. According to the properties of the relative entropy, the computation of the relative entropy of a Gaussian function with respect to another Gaussian function is very easy. Since $C(x')$ is a Gaussian distribution, if we can construct a Gaussian distribution $F(x')$ which has the same numerical characters with $D(x')$, we can easily compute the partition of the interval. Although it is not very precise, we can compute the exact one based on this computation. Using these two steps to compute the partition of the interval is much easier to implement and also faster than the original method.

First, we will calculate the mathematical expectation and variance of the random variable D with $D(x')$ as its probability density function.

$$\begin{aligned} \mathrm{E}[D] &= \int_{-\infty}^{+\infty} x' D(x') dx' = \int_a^b p(X_A = x) x dx, \\ \mathrm{Var}[D] &= \int_{-\infty}^{+\infty} (x' - E[D])^2 D(x') dx' \\ &= (\sigma^2 + E[D]^2) \int_a^b p(X = x) dx - 2E[D] \\ &\quad \cdot \int_a^b x p(X = x) dx \\ &\quad + \int_a^b x^2 p(X = x) dx. \end{aligned} \tag{5}$$

Thus, we can construct an equivalent Gaussian variable $F \sim N(\mathrm{E}[D], \mathrm{Var}[D])$, so the partition of the interval can be simplified as

$$D(C(x')||D(x')) \approx D(C(x')||F(x')). \tag{6}$$

4) The boundary condition. Suppose$b$ is the boundary of adjoining intervals $[a,\ b]$ and $[b,\ c]$. After the iteration algorithm

$$\begin{aligned} &D(C(x')||F(x'), x \in K = [a, b]) \\ &= D(C(x')||F(x'), x \in K + 1 = [b, c]). \end{aligned} \tag{7}$$

Use the properties of the relative entropy of the Gaussian distribution and put eqs. (2) and (5) into eq. (7); we can obtain

$$\begin{aligned} &\frac{1}{2} \ln \frac{\{\sigma^2 + (\int_a^b x p(X = x) dx)^2\} \int_a^b p(X = x) dx + 2(\int_a^b x p(X = x) dx)^2 + \int_a^b x^2 p(X = x) dx}{\sigma^2} \\ &+ \frac{\sigma^2 + (b - \int_a^b x p(X = x) dx)^2}{2\{[\sigma^2 + (\int_a^b x p(X = x) dx)^2] \int_a^b p(X = x) dx + 2(\int_a^b x p(X = x) dx)^2 + \int_a^b x^2 p(X = x) dx\}} \\ &= \frac{1}{2} \ln \frac{\{\sigma^2 + (\int_b^c x p(X = x) dx)^2\} \int_b^c p(X = x) dx + 2(\int_b^c x p(X = x) dx)^2 + \int_b^c x^2 p(X = x) dx}{\sigma^2} \end{aligned}$$

$$+\frac{\sigma^2+(b-\int_b^c xp(X=x)dx)^2}{2\{[\sigma^2+(\int_b^c xp(X=x)dx)^2]\int_b^c p(X=x)dx+2(\int_b^c xp(X=x)dx)^2+\int_b^c x^2p(X=x)dx\}}. \quad (8)$$

Although eq. (8) seems complex, you can know from it that b is only relevant to a, c, $p(X=x)$ and the variance of the AWGN σ^2. This means the partition of the interval is only relevant to the probability distribution of the source and the channel. Thus, we can use eq. (8) to program the code and let computer compute the partition of the interval.

5) Simplified partition of the interval. If we partition the $(-\infty,+\infty)$ into $N=2^m$ parts. If x follows a Gaussian distribution, $P(-3\Sigma \leqslant x \leqslant +3\Sigma)=99.7\%$, so we choose $Q_1=\{x|-\infty<x<-3\Sigma\}$, $Q_N=\{x|3\Sigma<x<+\infty\}$ and the iteration algorithm can be as follows:

S1: Suppose $j=1$, $a_1=-3\Sigma$, $a_{N-1}=3\Sigma$ and from a_2 to a_{N-2} evenly partition the interval.

S2: If $j<N-1$, we put a_j and a_{j+2} into eq. (8) and calculate the boundary a_{j+1}.

S3: $j=j+1$.

S4: After one circulation, we set $j=1$ and return to S2.

The core of the algorithm is that we use eq. (8) to substitute for eq. (1), so the algorithm we proposed is faster and easier to program.

5 The design and optimization of the estimation function

After the partition of the interval, we could use bit estimation function to achieve the discrete bit sequence, the detail of the bit estimation function is as follows:

1. Suppose the interval $[a,b]$ is divided into 2^m subintervals. We encode the intervals $\underbrace{00\ldots0}_{m}$ to $\underbrace{11\ldots1}_{m}$ from left to right. Alice sends a $x\in[a,b]$ to Bob, x can be decoded into bit sequence $(S_m(x),S_{m-1}(x),\cdots S_1(x))$.

2. Bob estimates to which interval the x belongs according to the x' he receives and the information reconciliation exchanged through the authenticated channel. The information exchanged is the lower j bits of the sequence $(S_m(x),S_{m-1}(x),\cdots S_1(x))$. Bob uses the following process to guess the higher $m-j$ bits. S1: $i=j$; S2: $b=S_{i,i-1,\cdots,1}(x)$; S3: $S'_{i+1}(x)=S(x',b)$; S4: $S_{i+1}(x)=S'_{i+1}(x)$; S5: $i=i+1$; S6: If $i\leqslant m-1$ return to S2, otherwise, go to S7; S7: Bob gets the higher $m-j$ bits $(S'_m(x),S'_{m-1}(x),\cdots S'_{j+1}(x))$.

3. After Alice and Bob process n realizations of the continuous variable, they obtain $(m-j)n$ bits. These bits form the discrete random variable X and X'. Then we can implement error correction and privacy amplification.

Van Assche[9] only gave us the process, but he did not deeply analyze the estimator of the ith bit. Therefore this section designs the bit estimation function and discusses the physical meaning of it.

5.1 The bit estimator of SEC algorithm

The ith bit's estimator in SEC algorithm is as follows:

$$S'_i(x',b)=\arg\max_s \Pr[S_i(X)=s|S_{i-1,\ldots,2,1}(X)=b, X'=x'] \quad s\in\{0,1\}. \quad (9)$$

Eq. (9) means that if you put $s=0$ and $s=1$ into eq. (9), you will obtain two probabilities. We are interested in the larger one. If you put $s=0$ into eq. (9) and obtain the larger one, we can think the ith bit is bit 0; otherwise we can think the ith bit is bit 1. Since

$$\Pr[S_i(X)=s|S_{i-1,\ldots,2,1}(X)=b,X'=x'] = \frac{\Pr[S_i(X)=s,S_{i-1,\ldots,2,1}(X)=b,X'=x']}{\Pr[S_{i-1,\ldots,2,1}(X)=b,X'=x']}, \quad (10)$$

thus, Bob can guess the ith bit through the lower $i-1$ bits $S_{i-1,\ldots,2,1}(X)=b$. Then, Bob can guess all the bits.

Analysis: Suppose we have m bits in all. Thus, Alice partitioned the interval into 2^m parts. If we know the lower $i-1$ bits, there are 2^{m-i+1} subintervals meeting the requirement. We use $\Pr[S_{i-1,\ldots,2,1}(X)=b,X'=x']$ to represent the sum of the probabilities from these subintervals to the $X'=x'$.

1. If $s=0$, we can obtain 2^{m-i} subintervals from all the 2^{m-i+1} subintervals. We put $s=0$ into eq. (10) and obtain the probability $p(0)$. If we put $s=1$ into eq. (10), we can obtain $p(1)$. If

$p(0) > p(1)$, we think the ith bit is bit 0; otherwise, we think the ith bit is bit 1.

2. All the computation can be modeled as the calculation of the probability from one interval to a point. The denominator in eq. (10) is the sum of these probabilities. We can easily know that this probability is 0. Thus, eq. (10) is the Law of L′Hospital, and we should simplify the formula and obtain an estimation function. If the estimation function can be used instead of the Law of L′Hospital, the efficiency is increased.

3. The difficulty of eq. (10) is finding an estimation function to replace for the complex computation of planar Gaussian distribution.

5.2 The design of the estimation function

If we use margin probability density function $p(x)$ and $p(x')$ to compute the joint probability density function $p(x, x')$ and then use $p(x, x')$ to compute the probability of the model we discussed earlier, the condition is complex. Therefore, this paper proposes two easier ways to compute the probability from the interval to the point.

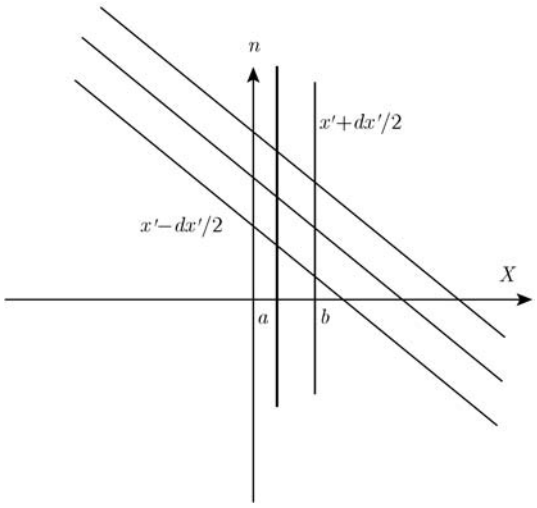

Figure 1 The analysis of the problem.

Method 1. Since $p(x, x')$ is very complex, we use another easily computed joint probability density function $p(x, n)$. Suppose the random variable $X \sim N(0, \Sigma^2)$, the interval we are interested in is $[a, b]$. The white noise $N \sim N(0, \sigma^2)$. Since X and N are individual, $X' = X+N \sim N(0, \Sigma^2+\sigma^2)$. Suppose the interval of the X' is $[x' - \frac{dx'}{2}, x' + \frac{dx'}{2}]$, then the interval of the $N = X' - X$ is $[x' - \frac{dx'}{2} - x, x' + \frac{dx'}{2} - x]$. Then we can draw a figure to illustrate it (Figure 1).

Then we can compute the joint probability density function of X and N

$$p(x, n) = p(x)p(n) = \frac{1}{\sqrt{2\pi}\Sigma} \exp(-\frac{x^2}{2\Sigma^2}) \times \frac{1}{\sqrt{2\pi}\sigma} \exp(-\frac{x^2}{2\sigma^2}). \quad (11)$$

Thus, the joint probability density function of X and X' is

$$P(X, X') = \int_a^b \int_{x'-dx'/2}^{x'+dx'/2} p(x, x')dxdx' = \int_a^b \int_{x'-x-(dx'/2)}^{x'-x+(dx'/2)} p(x, n)dndx. \quad (12)$$

We put eq. (11) into eq. (12), and then we obtain

$$P(X, X') = \int_a^b p(x) \int_{x'-x-(dx'/2)}^{x'-x+(dx'/2)} p(n)dndx. \quad (13)$$

Suppose $\Phi(x) = \int_{-\infty}^{x} \frac{1}{2\pi} e^{-\frac{z^2}{2}} dz$, then

$$\begin{aligned} M(x) &= \int_{x'-x-(dx'/2)}^{x'-x+(dx'/2)} p(n)dn \\ &= \Phi\left(\frac{x' - x + (dx'/2)}{\sigma}\right) - \Phi\left(\frac{x' - x - (dx'/2)}{\sigma}\right) \\ &\xrightarrow{dx' \to 0} \frac{1}{\sigma} \Phi'\left(\frac{x' - x}{\sigma}\right) dx' \\ &= \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x'-x)^2}{2\sigma^2}} dx'. \end{aligned} \quad (14)$$

We put eq. (14) into eq. (13), and then we can obtain the joint probability density function.

$$\begin{aligned} &P\left(a \leqslant X \leqslant b, x' - \frac{dx'}{2} \leqslant X' \leqslant x' + \frac{dx'}{2}\right) \\ &= \int_a^b p(x)M(x)dx \\ &= \int_a^b \frac{1}{\sqrt{2\pi}\Sigma} e^{-\frac{x^2}{2\Sigma^2}} \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x'-x)^2}{2\sigma^2}} dxdx' \\ &= \left(\frac{1}{2\pi\sigma\Sigma} \int_a^b e^{-\frac{x^2}{2\Sigma^2}} e^{-\frac{(x'-x)^2}{2\sigma^2}} dx\right) dx'. \end{aligned} \quad (15)$$

So the probability from the interval $[a, b]$ to the point x' is

$$P(a \leqslant X \leqslant b, x') = \frac{P(a \leqslant X \leqslant b, x')}{dx'}$$

$$= \frac{1}{2\pi\sigma\Sigma}\int_a^b \mathrm{e}^{-\frac{x^2}{2\Sigma^2}}\mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}dx. \quad (16a)$$

Method 2. Since the source is a Gaussian distribution and the channel is AWGN. Thus,

$$p(x) = \frac{1}{\sqrt{2\pi}\Sigma}\exp\left(-\frac{x^2}{2\Sigma^2}\right),$$
$$p(x'|x) = \frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(x'-x)}{2\sigma^2}\right).$$

Moreover, the joint probability density function is

$$p(x,x') = p(x'|x)p(x) = \frac{1}{2\pi\Sigma\sigma}\exp\left(-\frac{x^2}{2\Sigma^2}-\frac{(x'-x)}{2\sigma^2}\right). \quad (17)$$

Therefore, the probability from one interval to a point is

$$P(a\leqslant x\leqslant b, x') = \int_a^b p(x,x')dx = \frac{1}{2\pi\Sigma\sigma}\int_a^b \exp\left(-\frac{x^2}{2\Sigma^2}-\frac{(x'-x)}{2\sigma^2}\right)dx. \quad (16b)$$

From eqs. (16a) and (16b) we know, the different methods result in the same estimation function. This function is a simple definite integral. Thus, it can be used as the estimation function. It is easier to implement the program using this estimation function than the double integral.

5.3 Physical meaning

Since the channel is the AWGN, when $X = x$, the conditional probability density function of random variable X' is

$$p(x'|X=x) = \frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}. \quad (18)$$

Since $X \sim N(0, \Sigma^2)$, the average conditional probability is

$$\int_a^b p(X=x)p(x'|X=x)dx = \int_a^b p(X=x)\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}dx = \int_a^b \frac{1}{\sqrt{2\pi}\Sigma}\mathrm{e}^{-\frac{x^2}{2\Sigma^2}}\frac{1}{\sqrt{2\pi}\sigma}\mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}dx = \frac{1}{2\pi\sigma\Sigma}\int_a^b \mathrm{e}^{-\frac{x^2}{2\Sigma^2}}\mathrm{e}^{-\frac{(x'-x)^2}{2\sigma^2}}dx. \quad (19)$$

Obviously, eq. (19) is the same as eq. (16). Thus, the physical meaning of the estimation function is the average probability density from the interval $[a, b]$ to the point x'.

6 Summary

This paper optimizes the two parts of the information reconciliation: the partition of the intervals and the estimation function. We use the Gaussian distribution to replace for the none-Gaussian distribution and design the effective estimation function for the estimator for the SEC algorithm. The two parts efficiently lower the complexity of the algorithm, increase the efficiency and simplify the core problem of the continuous QKD. It has the instructive meaning for the reconciliation algorithm of the continuous QKD.

1 Zeng G H. Quantum Cryptography (in Chinese). Beijing: Science Press, 2006
2 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
3 Bennett C H, Brassard G. Publish—key distribution and coin tossing. In: Proceedings of the IEEE International Conference, on Computers, Systems and Signal Processing. Bangalore, India, 1984. 175–179
4 Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444
5 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
6 Mayers D. Unconditional security in quantum cryptography. J ACM, 2001, 48: 351–406
7 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88: 057902
8 Grosshans F, Assche G V, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states. Nature, 2003, 421: 238–241
9 Assche G V, Cardinal J, Cerf N J. Reconciliation of a quantum-distributed Gaussian key. IEEE Trans Inf Theory, 2004(2): 394–400
10 Maurer U M. Secret key agreement by public discussion from common information. IEEE Trans Inf Theory, 1993, 39(3): 733–742
11 Wolf S. Unconditional Security in Cryptography. Berlin: Springer-Verlag, 1999. 217–250
12 Cardinal J, Assche G V. Construction of a shared secret key using continuous variables. In: Proc 2003 IEEE Information Theory Workshop (ITW2003), Paris, France, Mar./Apr. 2003
13 Slepian D, Wolf J K. Noiseless coding of correlated information sources. IEEE Trans Inf Theory, 1973, 19(7): 471–480