2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.086

Analysis on the Bit Error Rate Distribution of Eavesdropping Detection and the Minimum Bits for Error Detection in a QKD system

Min He, Yanbo Wang, Yong Zhu, Zhiyong Xu, Zhiyong Zhang

Institute of Communication Engineering, PLA University of Science and Technology, Nanjing, 210007, China

Keywords: QBER, BER fluctuation, reliability, geometric distribution, raw keys, minimum bits for error detection

Abstract. The precise estimation of quantum bit error rate is the base of the eavesdropping detection and data coordination in a quantum key distribution(QKD) protocol. Find that the sample bit-error-rate(BER) obeys the geometric distribution, obtain the relationship between BER, BER fluctuation, reliability and the minimum bits for error detection, get the minimum bits in a QKD When the reliability is given. Results show that with fixed reliability and the total amount of the raw keys reaching the given amount, the minimum bits for error detection is only related to BER and BER fluctuation, and has nothing to do with the total amount of raw keys.

Introduction

In 1949, Shannon first proved that one-time pad is the only unconditional security cryptography. Due to the difficulty in realizing, the one-time pad is only meaningful in theory without practical value. Until 1984, Bennett and Brassard put forward the quantum key distribution protocol(BB84 protocol[1]), which makes it possible to realize the one-time pad coding with quantum states.

BB84 protocol uses two sets of the one pair of the polarization-orthogonal single photon with included angle 45 to encode information and transfer, as shown in fig. 1. For a bit, the sender(Alice) encodes it with code bases selected randomly from R={0°, 90°} and D={ 45°, 135°}, then modulates the polarization of photon and sends it to the receiver(Bob). Bob randomly selects bases from R and D and detects the states. In theory, if and only if the detection base of Alice and Bob is identical, the result of Bob is the same to Alice and the bit is shared by Alice and Bob. After communication, Bob openly sends his detection base sequence and Alice points out the right bases, which is called base comparison. When the base of the partners is the same, the obtained results are the shared bits, which are usually called raw keys.[2][3][4][5]

After base comparison, eavesdropping detection is needed, that is selecting bits randomly from the raw keys and openly testing the consistency. Actually, due to the polarization drift, unsatisfactory to measuring instruments, etc, the shared bits are not all the same even the bases are consistent, which is called channel BER. Therefore the channel BER should be obtained from open experiments in advance for detecting eavesdropping. Alice and Bob randomly select bits from raw keys and calculate BER, which is called sample BER. Without eavesdropping, the sample BER will fluctuate in the limited area near channel BER, or the deviation of sample BER and channel BER will exceed the limited area and the key-consulting is given up. Due to the channel BER, raw keys by base comparison and eavesdropping detection will need data coordination and privacy amplification[6][7][8].

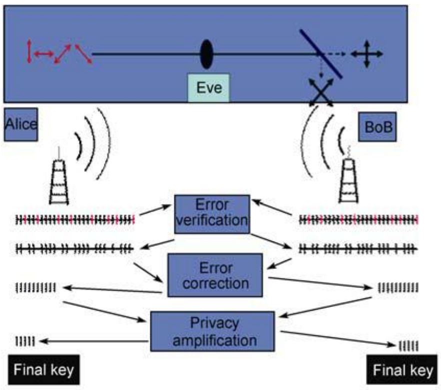


Fig.1: The working principle of BB84 protocol

The practical BER in raw keys is the base of data coordination and privacy amplification. The sample BER is the evaluation of the practical BER. In theory, the sample is more big, the evaluation is more precise. That is, the more the raw key is consumed, the more the evaluation is precise. Actually, the QKD rate is low when too many raw key bits are consumed. The consumption of raw keys and the deviation of sample BER and channel BER restrict the QKD rate. This paper analyzes the relationship between the bits for eavesdropping, the reliability of channel BER, and the fluctuation of sample BER and channel BER, and analyzes the minimum consuming bits of raw keys with fixed reliability of sample BER.

Analysis on the Minimum Bits for Detection

Assume that after base comparison in QKD, the number of the shared raw keys of Alice and BOB is *N* pairs with error *T* pairs. Randomly select n pairs from *N* pairs of raw keys. In the *n* pairs, the probability that there are t pairs inconsistency obeys hyper-geometric distribution, that is:

$$P(n,t,N,T)=\frac{C_T^t C_{N-T}^{n-t}}{C_N^n}$$

Which is sample BER.

Sign $p=\frac{T}{N}$, $q=1-p$. p is practical BER(called BER for briefly). Obtain:

$$P(n,t,N,T)=\frac{n!}{t!(n-t)!}\bullet\prod_{i=0}^{n-t-1}\frac{Nq-i}{N-i}\bullet\prod_{j=0}^{t-1}\frac{Np-j}{N-(n-t-j)}\frac{n!}{t!(n-t)!}\bullet\prod_{i=0}^{n-t-1}\frac{q-i/N}{1-i/N}\bullet\prod_{j=0}^{t-1}\frac{p-j/N}{1-(n-t-j)/N} \qquad (1)$$

Obviously, when $N\to\infty$, $P(n,t,N,T)\to B(n,t;p)=C_n^t p^t q^{n-t}$, which obeys binomial distribution.

Assume ε>0, β>0. For n pairs of raw keys, the probability the inconsistency number of pairs is between (*n*(*p*-ε), *n*(*p*+ε)) or the BER of n pairs is between (*p*-ε, *p*+ε) is no less than β, the test is finished with the reliability β and level ε, in which ε is the fluctuation of BER, β is the reliability and 1−β is the rate of missing detection. Then the probability that the number of pairs is between (*n*(*p*-ε), *n*(*p*+ε)) is:

$$P(n,p,\varepsilon,N)=\sum_{t\in(n(p-\varepsilon),n(p+\varepsilon))}P(n,t,N,T)=\sum_{t\in(n(p-\varepsilon),n(p+\varepsilon))}\frac{C_T^t C_{N-T}^{n-t}}{C_N^n} \qquad (2)$$

The minimum n satisfied that $P(n,p,\varepsilon,N)$ no less than β is called the minimum bits for error detection and signed n_0, then:

$$n_0=\min\{n\colon\ P(n,p,\varepsilon,N)\geq\beta\}.$$

Therefore the formula for calculating the minimum bits is:

$$n_0 = \min\left\{ n\mathbf{:} \sum_{t\in\left(n(p-\varepsilon),n(p+\varepsilon)\right)} \frac{n!}{t!\left(n-t\right)!} \bullet \prod_{i=0}^{n-t-1} \frac{Nq-i}{N-i} \bullet \prod_{j=0}^{t-1} \frac{Np-j}{Np-\left(n-t-j\right)/N} \ge \beta \right\} \tag{3}$$

Calculation and Analysis on the Example

Formula (3) cannot be expressed as an apparent function with variables for analyzing the increment relationship between variables, then the relationship between the minimum bits for detection, total number of raw keys N, BER p and fluctuation of BER ε can only be analyzed by numerical calculation. Briefly, the reliability is fixed as β=0.9.

(1)The minimum bits for detection with fluctuation of BER ε=0.01

The relationship between the total number of raw keys N, BER and the minimum bits n_0 with fluctuation of BER ε=0.01 is shown in table 1 and fig. 2.

Table 1: The minimum bits n_0 with fluctuation of BER ε=0.01

Number of raw keys N / BER p	10K	15K	20K	25K	30K	35K	40K	45K	50K
0.01	301	301	301	301	301	301	301	301	301
0.02	467	467	467	467	467	467	467	467	467
0.03	726	726	726	726	726	726	726	726	726
0.04	921	921	961	961	961	961	961	961	961
0.05	1117	1167	1167	1167	1167	1217	1217	1217	1217
0.06	1258	1358	1358	1358	1415	1415	1415	1415	1415
0.07	1463	1513	1563	1613	1613	1613	1613	1663	1663
0.08	1612	1712	1756	1812	1812	1812	1856	1856	1856
0.09	1761	1861	1961	2011	2011	2011	2061	2061	2061
0.10	1910	2055	2110	2155	2210	2210	2255	2255	2255
0.11	2059	2209	2309	2359	2359	2409	2409	2459	2459
0.12	2154	2354	2454	2508	2554	2554	2608	2608	2654

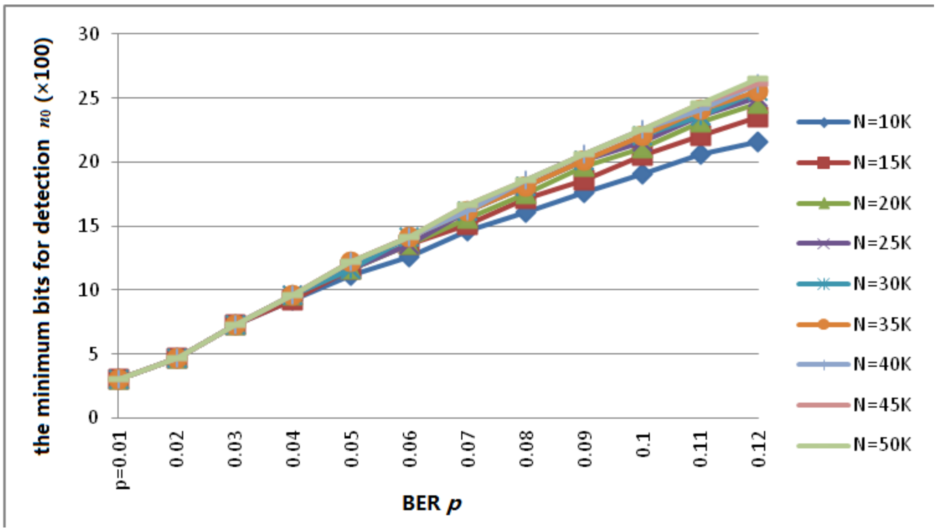


Fig.2: The relationship between BER and the minimum bits n_0 with fluctuation of BER ε=0.01

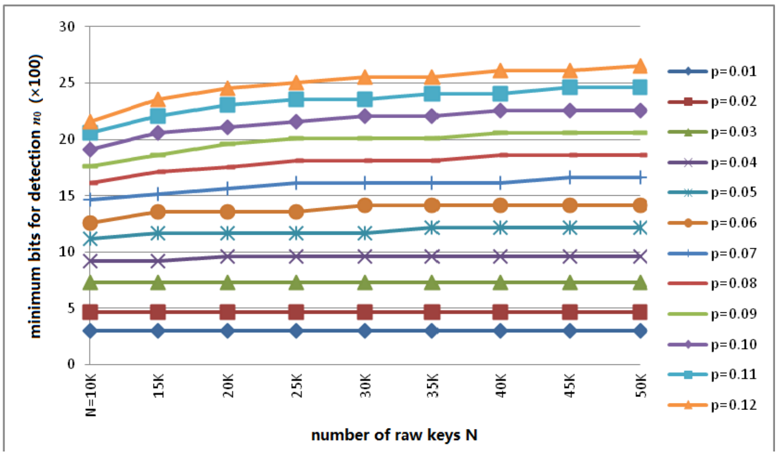


Fig.3: The relationship between N and n_0 with ε=0.01

From fig. 2 can we see, for fixed N, the minimum bits for detection has mainly linear relationship with BER.

Table 1 provides the relationship between BER and n_0 and also the relationship between N and n_0, as shown in fig. 3.

Fig. 3 shows that for a given BER, the number of raw keys N has little effect on the minimum bits for detection. In other words, for a fixed BER, number of bits for eavesdropping detection is a constant value for the total number of raw keys N. The number of bits for detection is the same, no matter how many the generating number of raw keys in QKD is, which can save a large number of bits for detection.

It is obtained from the analysis above that BER is the main factor affecting the minimum bits for detection.

(2)The minimum bits for detection with fluctuation of BER ε=0.02

Table 2 and fig. 4 show the relationship between the total number of raw keys N, BER and the minimum bits n_0 with fluctuation of BER ε=0.01

Table 2: The minimum bits for detection n_0 with ε=0.02

Number of raw keys *N* BER *p*	10*K*	15*K*	20*K*	25*K*	30*K*	35*K*	40*K*	45*K*	50*K*
0.01	1	1	1	1	1	1	1	1	1
0.02	151	151	151	151	151	151	151	151	151
0.03	161	161	161	161	161	161	161	161	161
0.04	234	234	234	234	234	234	234	234	234
0.05	286	286	286	286	315	315	315	315	315
0.06	363	363	363	363	363	363	363	363	363
0.07	378	412	412	412	412	412	412	412	412
0.08	461	461	461	461	461	461	481	481	481
0.09	510	510	510	528	528	528	528	528	528
0.10	559	559	559	584	584	584	584	584	584
0.11	577	608	608	631	631	631	631	631	631
0.12	629	658	658	679	679	679	679	679	679

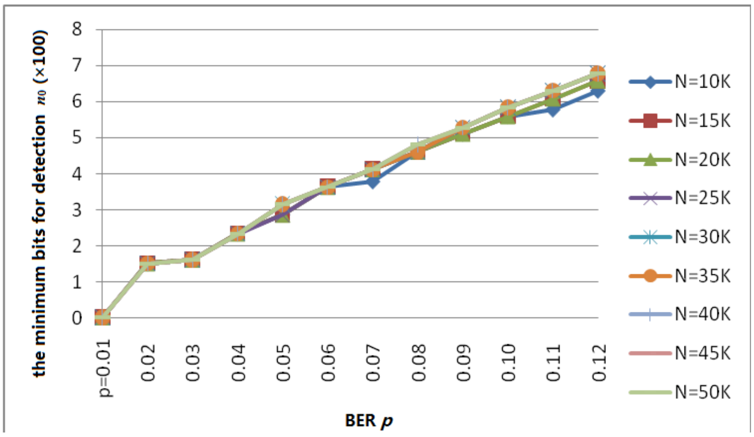


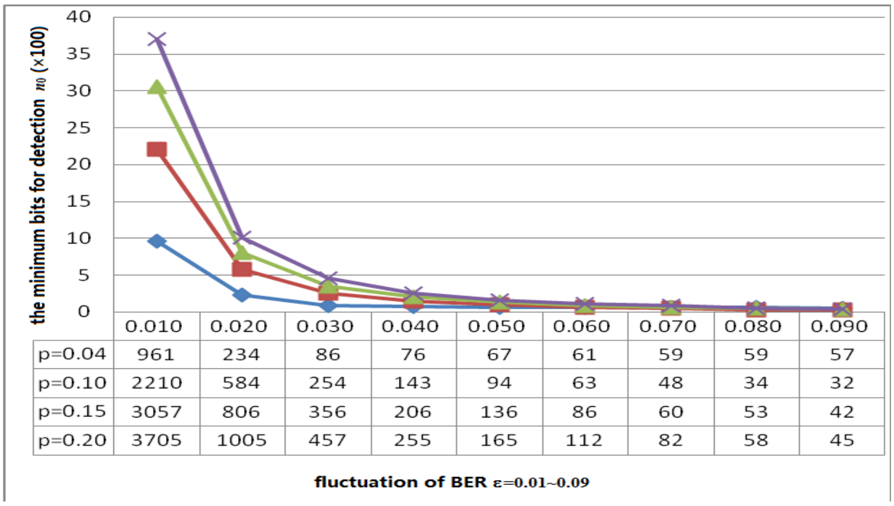
Fig.4: The relationship between BER and n_0 with ε=0.02

(3)The relationship between the fluctuation of BER and the minimum bits for detection

Table 3: The linear fitting relationship and variance of the minimum bits for detection and BER

Number of raw keys N	The linear fitting relationship of the minimum bits for detection n_0 and BER p	The linear fitting variance σ
N=10K	n_0=8.08+5401.40p	26.44
N=15K	n_0=1.55+5622.38p	22.75
N=20K	n_0=1.55+5622.38 p	22.75
N=25K	n_0=–7.18+5868.18 p	20.75
N=30K	n_0=–2.79+5837.76p	22.19
N=35K	n_0=–2.7912+5837.76p	22.19
N=40K	n_0=–2.48+5858.74 p	22.62
N=45K	n_0=–2.48+5858.74 p	22.62
N=50K	n_0=–2.48+5858.74 p	22.62

For N=30000, calculate n_0 when p=0.04, 0.10, 0.15, 0.20. p=0.04 is the BER of a QKD system with good performance, p=0.10 is the BER of a QKD system with bad performance, and p=0.15~0.20 is the BER with eavesdropping. Fig. 5 shows the relationship between the fluctuation of BER ε and the minimum bits for detection n_0.



	0.010	0.020	0.030	0.040	0.050	0.060	0.070	0.080	0.090
p=0.04	961	234	86	76	67	61	59	59	57
p=0.10	2210	584	254	143	94	63	48	34	32
p=0.15	3057	806	356	206	136	86	60	53	42
p=0.20	3705	1005	457	255	165	112	82	58	45

Fig.5: The relationship between the fluctuation of BER and the minimum bits for detection

In fig. 5, when the fluctuation of BER increases, the needed minimum bits for detection will decrease sharply. Too much fluctuation of BER is inadvisable and the evaluation needs to be relatively precise because the QBER is mainly used for data coordination. ε=0.02 is suitable in practical application.

It follows that for a system with BER 0.04 and rate of generating raw keys 30*K*, when the tolerance deviation of error code is 0.01 and the reliability of eavesdropping detection is 90%, the needed minimum bits for detection is 961 bits. When the he tolerance deviation is 0.01, the needed bits is 234 bits.

Summary

According to conclusions above, for the fixed rate of missing detection, when the total number of raw keys reaches a given amount, the minimum bits is only related to BER and fluctuation of BER, while the effect of the number of raw keys is little. In other words, in theory, the minimum bits for detection is the same no matter how many the generating number of raw keys in QKD is.

The minimum bits for detection is not only a consuming threshold of raw keys for detecting eavesdropping, but also a consuming threshold for detecting BER. Focusing on the security of BB84 protocol, Mayers etc[9][10] proved Alice and Bob can obtain ideal security keys through error correction in open channels only when BER p <11%. Table 1 shows that for 2459 sample inspection bits, if the sample BER is 11% ±0.01, the channel BER is 11% with the reliability of 90%.

References

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India, 1984, 175(0).

[2] HE Min, YAO Ze-qing, LIU Rong, GONG Jing. Study on Quantum key D istribution System and Simulated Quantum key Distribution Protocol Based on Fiber [J]. Quantum Optics Journal 2009(01)

[3] HE Min,CHEN Yi-wang,YAO Ze-qing,LIU Rong,GONG Jing. Simulation of Phase-shift Quantum Key Distribution Protocol [J]. Journal of Communications technology 2009(10)

[4] He Min.Wang YanBo.Wang Rong,Zhu Yong,Guan Yu,Wang Xiao.Quasi one-time padding secure communications based on QKD[A] NCOQE 2011 [C]

[5] HuJiaZhong,WangXiangBin. Quantum key distribution with the decoy-state method [J]. Chinese Science: Physics Mechanics Astronomy. 2011(04)

[6] Hwang W Y. Quantum key distribution with high loss: Toward global secure communication. Phys Rev Lett, 2003, 91: 057901

[7] Hu J Z, Wang X B. Quantum key distribution with the decoy-state method (in Chinese). Sci Sin Phys Mech Astron, 2011, 41: 459–465

[8] Chen Yan,Yang Hongyu, Deng Ke. Effects of Photon-Number-Splitting Attacks on the Security of Satellite-to-Ground Quantum Key Distribution Systems(in Chinese).ACTA OPTICA SINICA, 2009,11(in Chinese)

[9] Mayers D. Unconditional security in quantum cryptography. J Assoc Comput Mach, 2001, 48: 351–406

[10] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett, 2000, 85: 441–444