A Universal Quantum Key Distribution Simulation Method Towards Future Internet

Yan Peng, Bo Liu, Baokang Zhao, Chunqing Wu, Wanrong Yu

College of Computer, National University of Defense Technology, China
pengyan15@nudt.edu.cn, liubo.eecs@gmail.com, {bkzhao, wuchunqing, wlyu}@nudt.edu.cn

Abstract

Quantum Key Distribution (QKD) technology is developing at a rapid pace, it may be the key supporting technology of the space ground integrated internet.

To conduct a long distance QKD experiment is really difficult, it needs not only a lot of manpower, material resources, heavy workload, but also big and continuous financial support. However, there is not any simulation method for the quantum and classical integrated networks.

In this paper, we propose a simulation method for the physical subsystem of quantum communication network. In this method, we establish mathematical models for physical devices and quantum channels, so that we can calculate the loss and efficiency of different modules according to the parameters of the actual equipment, and finally get the simulation data close to the output of the real physical equipment. Therefore, the simulation method is applicable to different quantum communication networks. Unlike previous theoretical based studies, we can get simulated output, and our simulated results can be used as the raw key.

Keywords: QKD, Space-ground integrated internet, Simulation method, Physical components

1 Introduction

Classical cryptography is under tremendous threats with the development of the quantum computer. The security of the widely used encryption algorithm RSA is based on the computing complexity of factoring a large integer [1]. However, Shor [2] has proposed a polynomial algorithm in 1994, allowing fast factorization of integers with a quantum computer. Therefore, if quantum computer is successfully generated, the RSA encryption algorithm can be easily cracked.

One Time Pad (OTP), whose unconditional security has been rigorously proved by Shannon in 1949 [1], is the sole information-theoretically secure encryption algorithm known so far. QKD [1] is a technology which exploits the fundamental laws of quantum mechanics [3], it can generate secret shared key for two separated legal parties called Alice and Bob. Any intruder trying to eavesdrop the key exchange could be detected. Therefore, QKD and OTP together can provide an unconditional secure communication solution, which is called quantum communication.

In recent years, countries around the world are conducting quantum communication networks and quantum communication satellites [4]. Such as China's Micius quantum satellite [5], Tokyo quantum communication network [6], the European SECOQC quantum communication network [7] and the United States DARPA quantum communication network [8]. The communication distance of the QKD system has been enlarged to 404km [9], and the record of final key generation rate has been refreshed to 300kbit/s [10].

QKD is practical in the field of secure mobile communication [11-13]. Liu et al. integrated QKD and VoIP steganography to build a Qphone [14]. Rima et al. proposed an enhanced scheme for deriving a secure encryption key for WLAN using QKD [15]. Morio et al. proposed a simple polarization tracking method enables free-space quantum cryptography between mobile terminals [16]. Michael et al. have evaluated the status of QKD reagrding its practical applicability for securing mobile communication networks [17].

To conduct a long distance QKD experiment is really difficult. However, we could assess the communication distance, the transmission speed, the security and other key performance indicators by modeling and simulation of the quantum communication network.

There are some related researches, Ryan et al. have proposed a framework based on OMNeT++ to model quantum optical components [18], Mailloux et al. have modeled a decoy state enabled QKD system to study the impact of practical limitations [19], Morris et al. use discrete event system to model QKD system components [20]. However, existing studies on modeling QKD systems are based on theoretical analyses.

The heterogeneity of quantum communication networks is a major challenge in building a universal simulation method and tools. Therefore, to propose a universal simulation modeling method and simulation

*Corresponding Author: Baokang Zhao; E-mail: bkzhao@nudt.edu.cn
DOI: 10.3966/160792642018081904024

tool is faced with a great challenge.

In this paper, we propose a simulation method for the physical subsystem of quantum communication network. Our contribution is, we propose a simulation method for the physical subsystem of quantum communication network.

Rest of the paper is structured as follows. In Section 2, we give the brief background information about decoy BB84 protocol. In Section 3, we give the mathematical model of single photon source and single photon detector, and then we survey two different kinds of scenes of QKD link. In Section 4, we propose a universal simulation method and the experimental results are presented in Section 5. Conclusions are drawn in Section 6.

2 Preliminaries

2.1 BB84 Protocol

Bennett and Brassard proposed the first QKD protocol in 1984, known as BB84 [1]. The protocol uses four polarization states: horizontal, vertical, diagonal and anti-diagonal which can constitute two bases, rectilinear or diagonal.

Firstly, Alice randomly chooses individual polarization states among the four states mentioned above and then sends them to Bob through the quantum channel. Secondly, Bob randomly chooses the base to measure the received polarization states. Bob finally gets a bit string with error bits according to Alice, this is called the raw key. Then, Bob tells Alice the base sequence upon every state through the public channel. Alice then sends Bob whether the base is right or not. They discard the bits matching the incompatible bases. At this point, they get the sifted key. In the ideal communication case, there are no remaining error bits in the sifted key. However, error bits may be caused by the disturbance of the quantum channel, the imperfection of the components, and also attacks. Then, they conduct the information reconciliation algorithm to correct the remaining error bits.

The architecture of a typical QKD system is depicted in Figure 1. A QKD systems usually involve two phases: the quantum state transmission-reception phase and the classical post-processing phase [1].

2.2 Photon Number Splitting Attack

The weak coherent light source is used approximately as single photon source in experimental implementations. Therefore, several photons may be emitted in the same pulse. The distribution probability for the number of photons of the source follows a Poisson distribution. The probability of a pulse containing n photons is:

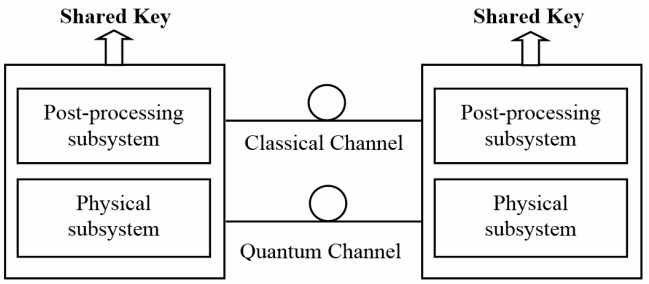

Figure 1. Architecture of the typical QKD system

$$P(n|\mu) = e^{-\mu}\frac{\mu^n}{n!} \quad (1)$$

where μ is the mean photon number in one pulse.

This provides the chance for the attacker to conduct Photon Number Splitting (PNS) attacks [21].

2.3 The Decoy State Protocol

Hwang has proposed the decoy state protocol in 2003 [22].

In the first step, signal and decoy states are randomly selected and sent through quantum channel to Bob. Second, Bob measures the states by randomly selected bases. In the third step, Alice and Bob perform key sifting. Bob announces the bases used to measure each qubit, and Alice returns back the matched bases. For the signal and decoy states mismatching bases are removed from both of their key buffer. In the fourth step, they count decoy state errors by publically announcing and comparing the prepared and measured bit results. In the fifth step, they conduct error reconciliation to correct the remained error bits. In the sixth step, some calculations are made such as the signal gain, the decoy gain, the signal Quantum Bit Error Rate (QBER), the decoy QBER and the dark count yield. In the seventh step, they conduct statistical analysis of the decoy state protocol security condition to ensure there is no unauthorized interference on the quantum channel.

2.4 Key Parameters in QKD System

Supposing the overall transmission and detection efficiency of the QKD system is η, then [23]

$$\eta = \eta_d \cdot \eta_t \cdot \eta_{Bob} \quad (2)$$

where η_d is the efficiency of the single photon detector which defines the detector's probability of detecting a single photon. η_t is the transmission efficiency of the quantum channel, there are two kinds of quantum channel, optical fiber and free space, which will be described in detail later. η_{Bob} is the internal transmission efficiency of Bob's devices, which is given by:

$$\eta_{Bob} = 10^{-\frac{L_{Bob}}{10}} \quad (3)$$

where L_{Bob} (dB) is the internal loss of Bob.

Let's denote μ as the mean photon number. Then the probability the detector click when a signal photon arrived is [24]:

$$p_{signal} = 1 - e^{-\mu\eta} \tag{4}$$

Let p_{dark} denotes the probability the detector click when no photon arrive, then p_{dark} is [25]:

$$p_{dark} = DCR \cdot t_w \tag{5}$$

where DCR is the total dark count rate of Bob's detectors, and t_w is the time window of the measurement of the system.

Therefore, the probability that detector gives a click is [24]:

$$p_{click} \approx p_{signal} + p_{dark} \tag{6}$$

Letting e_s and e_{dark} denote the error rate in the channel and the probability of a photon been erroneously detected respectively, then:

$$e_s = \frac{1-v}{2} \tag{7}$$

where v is the visibility of interference fringes [26], and the quantum bit error rate (QBER) is [27]:

$$QBER = \frac{e_s \cdot p_{signal} + e_{dark} \cdot p_{dark}}{p_{click}} \tag{8}$$

3 Model of Physical Components in QKD System

3.1 Architecture of Physical Subsystem in QKD

The architecture of physical subsystem in QKD is depicted in Figure 2.

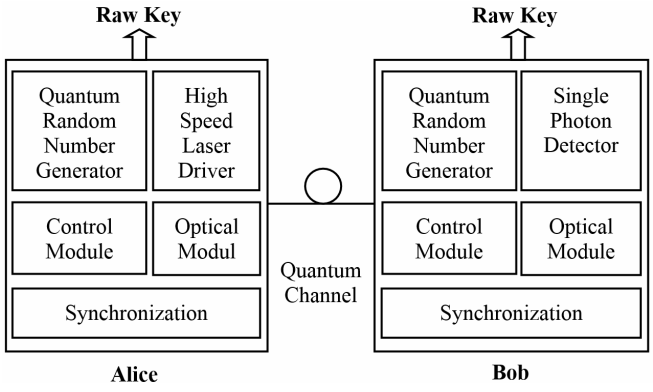

Figure 2. Architecture of physical subsystem in QKD

The quantum random number generator module is used to generate true random numbers, the synchronization module is used to realize the time synchronization between Alice and Bob, the control module is used to control the single photon source and the single photon detector and the optical module is used to modulate and transmit the quantum photons.

As a sender, Alice has laser module. As a receiver, Bob has single photon detectors. Alice and Bob are connected via quantum channel.

Mathematical model of single photon source. Laser is the most common used single photon source at the moment. The weak coherent light source has been choosed in most QKD systems to be the single photon source. The output is approximately to be coherent state $|\alpha\rangle$,

$$|\alpha\rangle = \left|\sqrt{\mu}e^{i\theta}\right\rangle = e^{-|\alpha|^2/2}\sum_0^\infty \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{9}$$

where $\mu = |\alpha|^2$ is the mean photon number. Suppose that the photon emitted from Alice has been randomized in terms of phase, so the quantum state will be transformed into the mixture of the classical photon number:

$$\rho = \int_0^{2\pi} \frac{d\theta}{2\pi}|\alpha\rangle\langle\alpha| = \sum_n P(n|\mu)|n\rangle\langle\mu| \tag{10}$$

where

$$P(n|\mu) = e^{-\mu}\frac{\mu^n}{n!} \tag{11}$$

Mathematical model of single photon detector. Avalanche Photon Diode (APD) is wildly used in experimental demonstrations. There are three main characteristics: η_d, p_{dark} and t_{dead}. η_d is the detector efficiency which defines the detector's probability of detecting a weak coherent pulse. p_{dark} is dark-count rate, which gives the detection events due to background including dark counts and stray light from timing pulses. t_{dead} is the interval time for the detector to restart after a detection event.

3.2 Mathematical Model of Quantum Channels

There are mainly two kinds of channel, optical fiber and free space.

Model of point-to-point fiber link. The structure of point-to-point fiber QKD link is depicted in Figure 3, which contains laser source, splitter, phase modulator (PM), phase randomizer (PR), attenuator, optical fiber, photon beam splitter (PBS) and single photon detector.

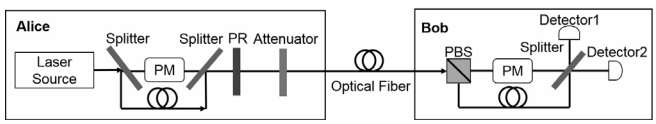

Figure 3. The structure of point-to-point fiber QKD link

Optical fiber loss is mainly described by two parameters: the loss coefficient α and the optical fiber transmission distance l:

$$L = \alpha l \tag{12}$$

The transmission efficiency of the optical fiber is:

$$\eta_t = 10^{-\frac{L}{10}} \tag{13}$$

In the standard single-mode fiber, the lowest loss factor of the wavelength is 1550 nm, which is the most commonly used fiber network communication wavelength, whose loss cofficient is 0.2dB/km. This part of work has been presented in [28].

In the Tokyo QKD Network [6], the key management agent can relay a secure key shared with one node to a second node by OTP-encrypting the key, using another key shared with the second node. Therefore, a secure key can be shared between nodes that are not directly connected to each other by a quantum channel.

In this model, the length of the secure key shared between two indirectly connected nodes is the minimum length among all the secure key generated by each QKD link:

$$len\left(k_{relayed}\right) = \min\left\{len\left(k_1\right), len\left(k_2\right), \cdots, len\left(k_n\right)\right\}.$$

Therefore, the fiber loss coefficient between two indirectly connected nodes is the maximum of that among all the QKD link.

$$\eta_t = 10^{-\frac{\alpha_{\max} l}{10}} \tag{14}$$

where $\alpha_{\max}$ means the maximum fiber loss coefficient among all the QKD link.

In general, QKD network actually is the accumulation of several point to point QKD link.

Model of the free space link. There are two kinds of space links: vertical link and horizontal link. Several factors could influence the transmission quality of free space channel: diameter of the lens, temperature, background light, atmospheric turbulence and bad weathers.

The transmission efficiency of the free space is given by [26]:

$$\eta_t = \left(\frac{d_r}{d_t + D \cdot l}\right)^2 10^{-\frac{\alpha l}{10}} \tag{15}$$

where d_t is the diameter of the active area of the transmitter, d_r is the diameter of the receiving surface of the receiver, l is the channel length, D is the opening angle of the beam field of view, α is the atmospheric attenuation. The first term of the equation in the right is the estimation of the geometric losses, and the second is the losses caused by scattering.

4 A Universal Simulation Method towards QKD System

We propose a **S**imulation **S**ystem of **P**hysical **C**omponents (SSPC) of QKD, which quantitatively analyzes the imperfections caused by the non-ideal physical components in different types of links.

The structure of the simulation system is depicted in Figure 4. It consists of two parts, Alice and Bob. The Data Generation Modules at both sides are responsible for the generation of random numbers and code words. The Data Transmission Modules at both sides are responsible for sending and receiving data encapsulated by the network protocol stack.

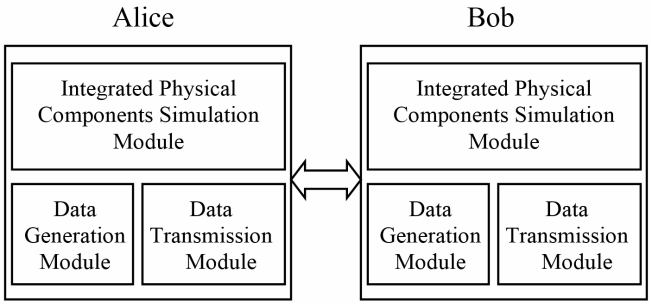

Figure 4. Structure of SSPC

At Alice's side, the integrated physical components simulation module consists of single photon source simulation sub-module and quantum states production sub-module, which is designed to simulate the preparation of single photon stream.

At Bob's side, we simulated the single photon detector and quantum channel in the integrated physical components simulation module.

4.1 Procedures of the Simulation System

The flowchart of Alice's side is shown in Figure 5. The Alice's side mainly includes four phases:

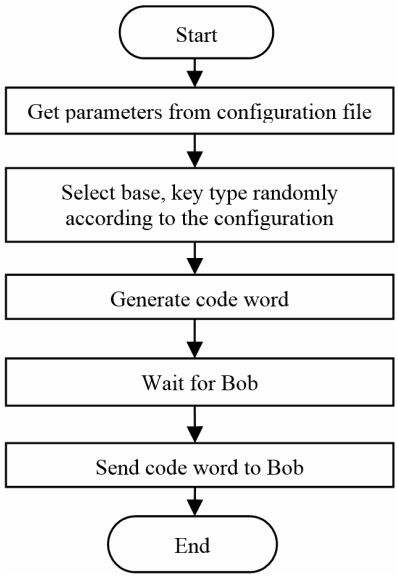

Figure 5. The flowchart of Alice's side in SSPC

Configuration phase. Before the simulation start, Alice's side set the parameters by loading the configuration file.

Photon generation simulation phase. First, Alice calculates the probability distribution of the signal photons and decoy photons according to the parameters of the physical components. Next, Alice randomly selects the base and the key of each photon according to the probability distribution.

Code word generation phase. Alice generates the code word for each photon according the format specified. The format will be described later.

Data transmission phase. Alice waits for Bob's connection. After the connection is established, Alice sends all the code words to Bob.

The flowchart of Bob's side is shown in Figure 6. The Bob's side mainly includes seven phases:

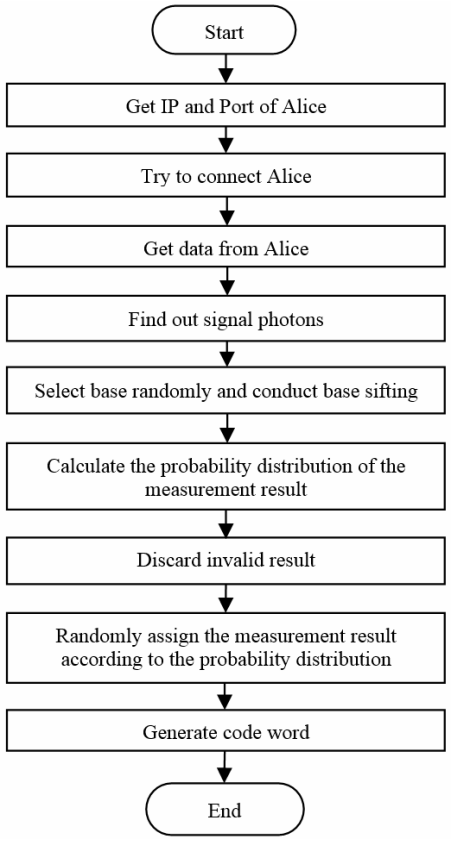

Figure 6. The flowchart of Bob's side in SSPC

Connection phase. Bob tries to establish a network link with Alice.

Data reception phase. Bob receives the code words from Alice and records them into the storage.

Pre-sifting phase. Bob divides the signal photons from the vacuum photons and the decoy photons.

Base sifting phase. Bob randomly chooses each base used to measure each photon and discards the code word whose base is different to Alice.

Parameter estimation phase. Bob calculates the QBER and the probability distribution of the measurement result using the parameters received from Alice.

Post-sifting phase. Bob discards the code word whose measurement result is invalid according to the probability distribution.

Photon detection simulation phase. For each photon, Bob checks the base of the code word from Alice, the probability of right measurement is $p_{click}(1\text{-}QBER)$, in this case, Bob's detection result is the same as the key of Alice in the code word; The probability of false measurement is $p_{click} \cdot QBER$, in this case, Bob's detection result is different from that of Alice.

The procedure of photon detection simulation is given in Algorithm 1.

Algorithm 1. Photon Detection Simulation Algorithm

Input: the code word number N, the Quantum bit error rate of the sifted key QBER, the random number x, Alice key KAlice ;

Output: Bob's Detection result KBob

```
for i = 0; i < N; i++ do
    if x in [0, 1-QBER]
        KBob[i] = KAlice[i]
    else
        KBob[i] = 01 XOR KAlice[i]
    end if
end for
```

The space complexity of Photon Detection Simulation Algorithm is $o(n)$ and the time complexity is $o(n)$.

Code word generation phase. Bob generates the code word for each photon according the format specified. The format will be described later.

4.2 The Representation of the Photon

We use the code word to express the information carried by the photon.

As shown in Figure 7 and Figure 8, in the code word of Alice, the eighth bit means the base used to generated the photons, which has two types, 0 or 1; The seventh bit means the key carried by the photon, which has two values, 0 or 1; The sixth bit and the fifth bit means the type of state of the photon, which has three value, 00, 01 and 10, standing for vacuum state, signal state and decoy state respectively; The fourth bit to the first bit are paddings.

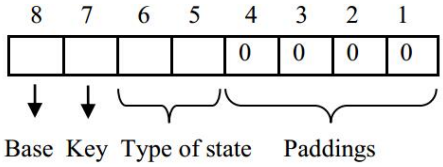

Figure 7. Code word of Alice

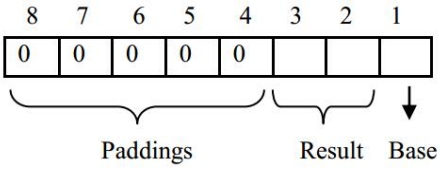

Figure 8. Code word of Bob

In the code word of Bob, the eighth bit to the fourth bit are paddings; The third bit and the second bit means the measurement results, which has three values, 11, 00, 01, standing for invalid, key zero and key one; The first bit stands for the base used to measure the photon, which has two types, 0 or 1.

5 Simulation and Results

We use the parameter in Shibata14 [25], Shuang12 [24], Takesue07 [29] and Wang13 [30] to test our simulation system.

5.1 Simulation Platform Setup

The parameters of our simulation platform are presented in Table 1. The throughput of our simulation system is 96786.4pulses/s.

Table 1. Parameters of the simulation platform

Parameter	Value
Operation System	Windows 7
CPU version	Intel Core i7-4710MQ
CPU frequency	2.5GHz
Core numbers	4
Memory size	8G

5.2 Simulation Results

The key parameters of Shibata14 [25] is shown in Table 2. They used a differential phase shift QKD scheme with a 1GHz system clock rate using a weak coherent light.

Table 2. Parameters in Shibata14 [25]

Parameter	Value		
l	local	306km	336km
η_d	6.7%	6.7%	4.4%
L (dB)	52.7	66.0	72.0
L_{Bob} (dB)	2.0	2.0	2.0
μ_{signal}	0.2	0.2	0.2
DCR (Hz)	0.04	0.04	0.01
t_w (ps)	100	100	100
e_s	1.0%	1.0%	1.0%
e_{dark}	0.5	0.5	0.5

The values of simulated (Sim) QBER and the experimental (Exp) QBER in Shibata14 are listed in Table 3. When long distance optical fiber is used, there are some kinds of disturbances which cannot be quantified, which lead to the deviation of the QBER.

Table 3. Experimental and simulated results of shibata14 [25]

Type	QBER		
	Local	306km	336km
Exp	1.02%	2.25%~3.27%	1.75%~3.65%
Sim	1.01%	1.18%	1.28%

The key parameters of Shuang12 [24] is shown in Table 4. They used differential phase shift QKD protocol and implemented with a 2GHz system clock rate.

Table 4. Parameters in Shuang12 [24]

Parameter	Value	
l	205km	260km
η_d	2.5%	2.5%
L (dB)	41.6	52.9
L_{Bob} (dB)	1.5	1.5
μ_{signal}	0.2	0.2
DCR (Hz)	1.0	1.0
t_w (ps)	200	200
e_s	1.8%	1.8%
e_{dark}	0.5	0.5

Figure 9 presents the comparison between the experimental results and the simulated results in Shuang12 [24], we can see that the simulated results is very close to the experimental results.

The key parameters of Takesue07 [29] is shown in Table 5. They used the differential phase shift QKD protocol, and implemented with a 10GHz clock frequency.

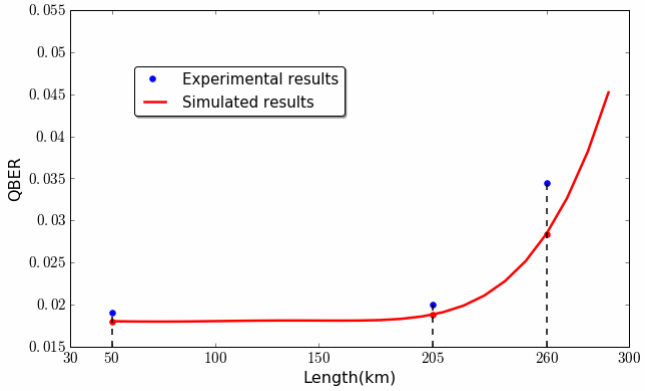

Figure 9. Comparison between the experimental results and the simulated results in Shuang12

Table 5. Parameters in Takesue07 [29]

Parameter	Value	
l	105km	200km
η_d	1.4%	1.4%
L (dB)	21.7	42.1
L_{Bob} (dB)	2.5	2.5
μ_{signal}	0.2	0.2
DCR (Hz)	50	50
t_w (ps)	50	50
e_s	2.3%	2.3%
e_{dark}	0.5	0.5

The values of simulated (Sim) QBER and the experimental (Exp) QBER in Takesue07 [29] are listed in Table 6.

Table 6. Experimental and simulated results of Takesue07 [29]

Type	QBER	
	105km	200km
Exp	2.41%	4.74%
Sim	2.32%	4.64%

In the experiment, there are some additional disturbance that we cannot calculate in the simulation, such as the disturbance caused by the bad weather and the shake of the fiber, therefore, the loss of the channel in the experiment will be higher than the simulated results, so the experimental QBER is a little bit higher than the simulated QBER.

The key parameters of the free space link QKD experiment setup in Wang13 [30] is shown in Table 7. We set v as 0.985.

Our simulated QBER is 3.93%, which is very close to the experimental results 4.04%. Our simulated result is a little smaller than the experimental result because the paper do not provide the specific value of the loss for us, then we take the smallest value of the loss, therefore, our simulated result is smaller than the experimental result.

Table 7. Parameters in Wang13 [30]

Parameter	Value
l	96km
η_d	1.8%
L (dB)	10.0
L_{Bob} (dB)	-
Diameter of transmitter	200mm
Diameter of receiver	600mm
Divergence angle	80urad
μ_{signal}	0.6
p_{dark}	4.3e-7
e_{dark}	0.5

6 Conclusion

In this paper, we present a universal QKD simulation method towards future internet, which could simulate the procedure of the production, transformation and detection of photons and provide a method to model different kinds of QKD systems. Parameters of the physical components are configurable in our system, therefore, solutions can be deployed in different QKD physical systems. Our contribution is, we propose a simulation method for the physical subsystem of quantum communication network.

Acknowledgements

This work was supported by NSFC No. 61202488, and Guangxi Cooperative Innovation Center of cloud computing and Big Data (No YD16505).

References

[1] B. Liu, B.-K. Zhao, W.-R. Yu, C.-Q. Wu, FiT-PA: Fixed Scale FFT Based Privacy Amplification Algorithm for Quantum Key Distribution, *Journal of Internet Technology*, Vol. 17, No. 2, pp. 309-320, March, 2016.

[2] P.-W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, *The 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, 1994, pp. 124-134.

[3] X.-P. Lou, J. Dai, Z.-G. Chen, M.-H. Lee, An Efficient Quantum Anonymous Communication with Hybrid Entanglement Swapping, *International Journal of Internet Protocol Technology*, Vol. 8, No. 2/3, pp. 87-95, December, 2014.

[4] Y. Peng, C.-Q. Wu, B.-K. Zhao, W.-R. Yu, B. Liu, S.-S. Qiao, QKDFlow: QKD Based Secure Communication Towards the OpenFlow Interface in SDN, *The 4th Annual International Conference on Geo-Informatics in Resource Management and Sustainable Ecosystem*, Hong Kong, China, 2016, pp. 410-415.

[5] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, J.-W. Pan, Satellite-based Entanglement Distribution over 1200 Kilometers, *Science*, Vol. 356, No. 6343, pp. 1140-1144, June, 2017.

[6] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J.-F. Dynes, A.-R. Dixon, A.-W. Sharpe, Z.-L. Yuan, A.-J. Shields, S. Uchikoga, M.

Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, A. Zeilinger, Field Test of Quantum Key Distribution in the Tokyo QKD Network, *Optics Express*, Vol. 19, No. 11, pp. 10387-10409, May, 2011.

[7] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J.-F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A.-W. Sharpe, A.-J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R.-T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R.-T. Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z.-L. Yuan, H. Zbinden, A. Zeilinger, The SECOQC Quantum Key Distribution Network in Vienna, *New Journal of Physics*, Vol. 11, No. 7, pp. 075001, July, 2009.

[8] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, H. Yeh, *Current Status of the DARPA Quantum Network*, arXiv preprint quant-ph/0503058, March, 2005.

[9] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y.-Q. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M.-J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, J.-W. Pan, Measurement-device-independent Quantum Key Distribution over a 404 km Optical Fiber, *Physical Review Letters*, Vol. 117, No. 19, pp. 190501, November, 2016.

[10] A.-R. Dixon, J.-F. Dynes, M. Lucamarini, B. Fröhlich, A.-W. Sharpe, A. Plews, S. Tam, Z.-L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, A.-J. Shields, High Speed Prototype Quantum Key Distribution System and Long Term Field Trial, *Optics Express*, Vol. 23, No. 6, pp. 7583-7592, March, 2015.

[11] C.-L. Li, L.-Y. Li, Efficient Mobile Cloud Service Allocation for Mobile Commerce, *International Journal of Ad Hoc and Ubiquitous Computing*, Vol. 26, No. 2, pp. 71-81, August, 2017.

[12] I. Moscholios, V. Vassilakis, P. Sarigiannidis, N. Sagias, M. Logothetis, An Analytical Framework in LEO Mobile Satellite Systems Servicing Batched Poisson Traffic, *IET Communications*, Vol. 12, No. 1, pp.18-25, May, 2018.

[13] C.-Y. Chen, G.-J. Zeng, F.-J. Lin, Y.-H. Chou, H.-C. Chao, Quantum Cryptography and Its Applications over the Internet, *IEEE Network Magazine*, Vol. 29, No. 5, pp. 64-69, October, 2015.

[14] B. Liu, B.-K. Zhao, Z.-L. Wei, C.-Q. Wu, J.-S. Su, W.-R. Yu, F. Wang, S.-H. Sun, Qphone: A Quantum Security VoIP Phone, *ACM SIGCOMM 2013 Conference*, Hong Kong, China, 2013, pp. 477-478.

[15] R. Djellab, M. Benmohammed, Securing Encryption Key Distribution in WLAN via QKD, *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, Sanya, China, 2012, pp. 160-165.

[16] M. Toyoshima, C. Schaefer, Y. Shoji, Y. Takayama, H. Kunimori, M. Takeoka, M. Fujiwara, M. Sasaki, *Mobile Quantum Cryptography Enhances Secure Communications*, Spienewsroom, 2008.

[17] M. Marhoefer, I. Wimberger, A. Poppe, Applicability of Quantum Cryptography for Securing Mobile Communication Networks, in: A. U. Schmidt, M. Kreutzer, R. Accorsi (Eds.), *Long-Term and Dynamical Aspects of Information Security: Emerging Trends in Information and Communication Security*, Nova Science Publishers, 2007, pp. 97-111.

[18] R.-D. L. Engle, D.-D. Hodson, M.-R. Grimaila, L.-O. Mailloux, C.-V. McLaughlin, G. Baumgartner, *Modeling Quantum Optical Components, Pulses and Fiber Channels Using OMNeT++*, arXiv preprint arXiv:1509.03091, September, 2015.

[19] L.-O. Mailloux, M.-R. Grimaila, D.-D. Hodson, R.-D. Engle, C.-V. McLaughlin, G.-B. Baumgartner, A Model and Simulation Framework for Studying Implementation Non-Idealities in Quantum Key Distribution Systems, *IEEE Access*, Vol. 3, pp. 110-130, September, 2015.

[20] J.-D. Morris, *Conceptual Modeling of a Quantum Key Distribution Simulation Framework using the Discrete Event System Specification*, Ph.D. Thesis, Air Force Institute of Technology, Wright-Patterson, OH, 2014.

[21] B. Huttner, N. Imoto, N. Gisin, T. Mor, *Quantum Cryptography with Coherent States, Physical Review A*, Vol. 51, No. 3, pp. 1863-1870, March, 1995.

[22] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, *Physical Review Letters*, Vol. 91, No. 5, pp. 057901, August, 2003.

[23] M. Lopes, N. Sarwade, Simulation and Modeling Approach for Performance Analysis of Practical Quantum Key Distribution, *2015 Annual IEEE India Conference (INDICON)*, New Delhi, IN, 2015, pp. 1-5.

[24] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, Z.-F. Han, *2 GHz Clock Quantum Key Distribution over 260 km of Standard Telecom Fiber, Optics Letters*, Vol. 37, No. 6, pp. 1008-1010, March, 2012.

[25] H. Shibata, T. Honjo, K. Shimizu, Quantum Key Distribution over a 72 dB Channel Loss using Ultralow Dark Count Superconducting Single-photon Detectors, *Optics Letters*, Vol. 39, No. 17, pp. 5078-5081, September, 2014.

[26] V. Scarani, H. Bechmann-Pasquinucci, N.-J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, *The Security of Practical Quantum Key Distribution, Reviews of Modern Physics*, Vol. 81, No. 3, pp. 1301-1350, September, 2009.

[27] N. Lütkenhaus, *Security against Individual Attacks for Realistic Quantum Key Distribution, Physical Review A*, Vol. 61, No. 5, pp. 052304, April, 2000.

[28] X.-L. Mao, Y. Li, Y. Peng, B.-K. Zhao, Physical Components Modeling in Quantum Key Distribution Towards Security Analysis, in: I. You, F.-Y. Leu, H.-C. Chen, I. Kotenko (Eds.), *Mobile Internet Security*, Springer Nature, Switzerland, 2016, pp. 154-163.

[29] H. Takesue, S.-W. Nam, Q. Zhang, R.-H. Hadfield, T. Honjo,

K. Tamaki, Y. Yamamoto, *Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-photon Detectors, Nature Photonics*, Vol. 1, No. 6, pp. 343-348, June, 2007.

[30] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, J.-W. Pan, *Direct and Full-scale Experimental Verifications towards Ground-satellite Quantum Key Distribution, Nature Photonics*, Vol. 7, No. 5, pp. 387-393, April, 2013.

Biographies

Yan Peng, received his B.S. degree at School of Computer Science and Technology in Harbin Institute of Technology. Currently he is taking a master's course at College of Computer, National University of Defense Technology. His research interests include quantum key distribution (QKD) and Network and Information Security.

Bo Liu, received the B.S. degree in network engineering from National University of Defense Technology, China, in 2012. He is currently a Ph.D. candidate in the School of Computer at the National University of Defense Technology. His research interests include computer network and communication, quantum communication and network security. He is a student member of the IEEE.

Baokang Zhao, received his B.S., master and Ph.D. degree from National University of Defense Technology, all in Computer Science. Currently he is an associate professor in College of Computer, National University of Defense Technology. His current research interests include computer networks, artificial intelligence, distributed computing and information security.

Chunqing Wu, received her B.S. and Ph.D. degrees from National University of Defense Technology, both in Computer Science and Technology. Currently, she is a full professor in the School of Computer Science, National University of Defense Technology. Her current research interests include computer network and high performance router.

Wanrong Yu, received the B.S. degree, the master degree and the Ph.D. degree in computer science in 1999, 2002, and 2006 respectively, all from National University of Defense Technology. Currently, he is an associate professor in the School of Computer Science, National University of Defense Technology. His current research interests include computer network and quantum communication.