# Physical Components Modeling in Quantum Key Distribution Towards Security Analysis

Xilong Mao, Yan Li, Yan Peng, and Baokang Zhao *,
College of Computer, National University of Defense Technology
mxilong@263.net,9375422@qq.com, {pengyan15,bkzhao}@nudt.edu.cn

**Abstract**

Quantum Key Distribution (QKD), based on fundamental principles of quantum mechanics, plays an irreplaceable role in national defense, financial and government affairs. Security analysis of QKD system is of great importance. However, existing studies on modeling QKD system are theory analysis based. In this paper, we propose a **S**imulation **S**ystem of **P**hysical **C**omponents (SSPC) in QKD system which modeling the three key modules: single photon source, quantum channel and single photon detector. Its parameters of the physical components are configurable. Therefore, solution can be deployed in different QKD physical systems.

**Keywords**: QKD, security analysis, physical components, modeling

## 1 Introduction

Quantum key distribution (QKD)[1], based on fundamental principles of quantum mechanics, is unconditionally secure. It plays an irreplaceable role in national defense, financial and government affairs. Field-test demonstrations of QKD networks have been conducted[2, 3, 4, 5, 6].

Security analysis based modeling of QKD system is of great importance in Quantum Communication. As shown in Figure 1, the structure of a typical QKD system consists of two sub-system, physical sub-system and post-processing sub-system[7]. However, real-world system implementations differ significantly from the ideal theoretical representations. Especially the single photon source and the detector have imperfections. Therefore, a majority of existing studies on security analysis are not very practical[8, 9]. Therefore, quantitatively analysis upon the real QKD system is very critical, especially to generate the data from the physical components.

Existing studies on modeling QKD systems are theory analysis based. Ryan et al. have proposed a framework based on OMNeT++ to model quantum optical components[10], Mailloux et al. have modeled a decoy state enabled QKD system to study the impact of practical limitations[11, 12, 13, 14]. Morris et al. use discrete event system to model QKD system components[15, 16].

However, most of existing models could not generate the data from the physical components. In this paper, we have developed a **S**imulation **S**ystem of **P**hysical **C**omponents (SSPC) in QKD. Our research is focused on getting the simulated data generated by the physical components, and the data is the raw key. Therefore, we can use SSPC to get the raw key, and then conduct further research.

## 2 Architecture of SSPC

The physical components of a typical QKD system are shown in Figure 1 which contains laser source, splitter, phase modulator (PM), phase randomizer (PR), attenuator, optical fiber, photon beam splitter

*Corresponding author: Prof. Baokang Zhao, College of Computer, National University of Defense Technology, Changsha, 410073, China, bkzhao@nudt.edu.cn

(PBS) and single photon detector. SSPC generalize the model into three parts: single photon source, quantum channel and single photon detector. In SSPC, we can set the specific value of the parameters of the physical components, therefore, solution can be deployed in different QKD physical systems.

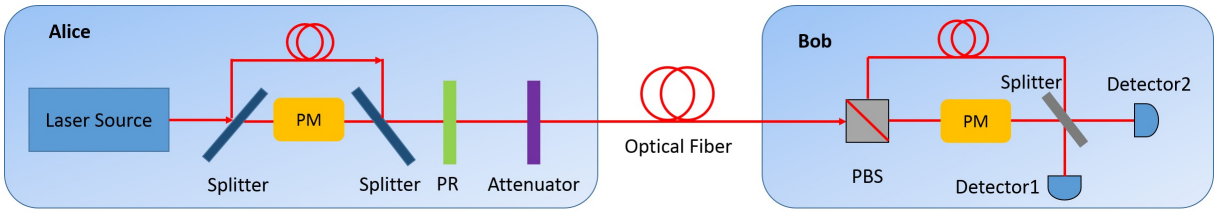


Figure 1: Physical components in a typical QKD system

## 3 Software simulation and Preliminary results

SSPC consists of two part, Alice and Bob. Both of them are composed of 3 modules, integrated physical components simulation module, data generation module and data transmission module. The function of the data generation module and the data transmission at Alice side and Bob side are the same. Random number is generated in the data generation module and is used to generate the codewords. The TCP protocol is adopted in the module of data transmission to transmit the codewords.

At Alice side, the integrated physical components simulation module consists of single photon source simulation sub-module and quantum states production sub-module, which are designed to simulate the preparation of single photon stream. At Bob side, we simulated the single photon detector and quantum channel in the integrated physical components simulation module.

We use the code word to express the information carried by the photon. The code word of Alice and Bob both are consist of 8 bits.In the codeword of Alice, the eighth bit means the base used to generate the photon, which has two types, 0 and 1; the seventh bit means the key to be carried by the photon, which has two value, 0 and 1; the sixth and fifth bits means the type of state of the photon, which has three values, 00, 01, 10, stand for vacuum state, signal state and decoy state respectively; the fourth bit to the first bit are padding. Therefore, there are 12 different code words at Alice side. In the codeword of Bob, the eighth bit to the fourth bit are padding; the third and the second bits stand for the results of the detection of the photon which has three value, 00, 01, 10; the first bit stands for the base used to detect the photon, which has two types, 0 and 1.

## 4 Conclusion

In this paper, we propose a method to simulate the physical sub-system of QKD. Which could simulate the procedure of the production, transformation and detection of quantum states. Using this simulation system, we could get the data flow extremely ensemble to the data generated by real physical system. We could change the value of the parameters according to different physical system in our simulating system. Therefore, solution can be deployed in different QKD physical systems.

## 5 Acknowledgement

This work was supported in part by National Science Foundation of China under grant No.61202488, and the outstanding young scholar funding of NUDT.

# References


[1] Charles H Bennett. Quantum cryptography: Public key distribution and coin tossing. In *International Conference on Computer System and Signal Processing, IEEE, 1984*, pages 175–179, December 1984.

[2] Teng-Yun Chen, Jian Wang, Hao Liang, Wei-Yue Liu, Yang Liu, Xiao Jiang, Yuan Wang, Xu Wan, Wen-Qi Cai, Lei Ju, et al. Metropolitan all-pass and inter-city quantum communication network. *Optics Express*, 18(26):27217–27225, 2010.

[3] Shuang Wang, Wei Chen, Zhen-Qiang Yin, Yang Zhang, Tao Zhang, Hong-Wei Li, Fang-Xing Xu, Zheng Zhou, Yang Yang, Da-Jun Huang, et al. Field test of wavelength-saving quantum key distribution network. *Optics letters*, 35(14):2454–2456, 2010.

[4] Masahide Sasaki, M Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics Express*, 19(11):10387–10409, 2011.

[5] Damien Stucki, Matthieu Legre, F Buntschu, B Clausen, Nadine Felber, Nicolas Gisin, L Henzen, Pascal Junod, G Litzistorf, Patrick Monbaron, et al. Long-term performance of the swissquantum quantum key distribution network in a field environment. *New Journal of Physics*, 13(12):123001, 2011.

[6] Bernd Fröhlich, James F Dynes, Marco Lucamarini, Andrew W Sharpe, Zhiliang Yuan, and Andrew J Shields. A quantum access network. *Nature*, 501(7465):69–72, 2013.

[7] Ke Cui, Jian Wang, Hong-Fei Zhang, Chun-Li Luo, Ge Jin, and Teng-Yun Chen. A real-time design based on fpga for expeditious error reconciliation in qkd system. *Information Forensics and Security, IEEE Transactions on*, 8(1):184–190, 2013.

[8] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[9] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Physical review letters*, 90(5):057902, 2003.

[10] Ryan DL Engle, Douglas D Hodson, Michael R Grimaila, Logan O Mailloux, Colin V McLaughlin, and Gerald Baumgartner. Modeling quantum optical components, pulses and fiber channels using omnet++. *arXiv preprint arXiv:1509.03091*, 2015.

[11] LO Mailloux, RD Engle, MR Grimaila, DD Hodson, JM Colombi, and CV McLaughlin. Modeling decoy state quantum key distribution systems. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 12(4):489–506, 2015.

[12] LO Mailloux, MR Grimaila, DD Hodson, RD Engle, CV McLaughlin, and GB Baumgartner. A model and simulation framework for studying implementation non-idealities in quantum key distribution systems. September 2015.

[13] Logan O Mailloux, Jeffrey D Morris, Michael R Grimaila, Douglas D Hodson, David R Jacques, John M Colombi, Colin V McLaughlin, and Jennifer A Holes. A modeling framework for studying quantum key distribution system implementation nonidealities. *Access, IEEE*, 3:110–130, 2015.

[14] Logan O Mailloux, Michael R Grimaila, Douglas D Hodson, L Elaine Dazzio-Cornn, and Colin McLaughlin. Modeling continuous time optical pulses in a quantum key distribution discrete event simulation. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2014.

[15] Jeffrey D Morris. *Conceptual modeling of a quantum key distribution simulation framework using the discrete event system specification*. PhD thesis, AIR FORCE INSTITUTE OF TECHNOLOGY, 2014.

[16] Jeffrey D Morris, Michael R Grimaila, Douglas D Hodson, Colin V McLaughlin, and David R Jacques. Using the discrete event system specification to model quantum key distribution system components. *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 12(4):457–480, 2015.