View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Universiti Putra Malaysia Institutional Repository

Malaysian Journal of Mathematical Sciences 13(S) August: 127–140 (2019)
Special Issue: The 6th International Cryptology and Information Security Conference (CRYPTOLOGY2018)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

QuCCs: An Experimental of Quantum Key Distribution using Quantum Cryptography and Communication Simulator

Zukarnain, Z.A.*[1], Buhari, A.[1], Harun, N.Z.[1,2], and Khalid, R.[1]

[1]*Department of Network, Faculty of Computer Science & Information Technology, University Putra Malaysia, Malaysia*
[2]*Department of Information Security, Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Malaysia*

E-mail: zuriati@upm.edu.my
Corresponding author *

ABSTRACT

The applications of quantum information science move towards bigger and better dimensions for the next generation technology. In the field of quantum cryptography and quantum computation, the world already witnessed various groundbreaking tangible products and promising results. Quantum cryptography is one of the mature fields of quantum mechanics and the devices are already available in the markets. In order to reach the heights of digital cryptography, the current state of quantum cryptography is still under various researches. However, the complexity of quantum cryptography is high due to combination of hardware and software. The lack of effective simulation tool to design and analyze the quantum cryptography experiments delays the reaching distance of the success. Therefore, in this paper, a framework to achieve an effective single photon based quantum cryptography simulation tool is proposed. The limitations of a commercial photonic simulation tool based experiments are also highlighted. Finally, the ideas for achieving one-stop simulation package for quantum based secure key distribution experiments

are discussed. The proposed modules of simulation framework have been analyzed from the programming perspective.

Keywords: quantum cryptography, quantum computation, quantum key distribution.

1. Introduction

Nowadays, data and information can be stolen during any kind of digital transaction, even with the current security measures. Nevertheless, secure key distribution problem is always a holy-grail research in the security world. As modern world moves completely towards digital, digital based transaction and communication are becoming the norm of the current society. As the same growth of usage, hacking, spying and phreaking becomes common critical threats to the society. The basic reason behind these threats is due to its vulnerable nature. In digital communication, any information can be copied without detection. Most of the popular current security mechanism provides only computational security which means bound towards the technology limit. Further, these security mechanisms are vulnerable to brute force attack. The smart phone and quantum computer is the toughest candidate, which can break the current security systems. Therefore, quantum security protocols have been researched for long time as a solution to provide unconditional security to the existing transaction of data in the network. Quantum security protocol uses the smallest particle of light to transfer information over fiber optics cables. Particularly, the principles of no-cloning theorem and Heisenberg's uncertainty principle culminate a new breed of cryptography so called quantum cryptography. Quantum cryptography has inbuilt properties to detect hacking activity, self-message destruction and cannot be replicated. Under the quantum cryptography, Quantum Key Distribution (QKD) is the matured field and real-time products are available in the market.

QKD history has already accomplished 30 years. From the ground-breaking protocol BB84 (Bennett and Brassard, 2014) to current QKD protocols have undergone various developments. The improvement of quantum hardware improves the quality of QKD based solution. The presence of noise in the channel and losses due to imperfect devices need QKD more rigorous research to achieve the heights of digital cryptography. However, there is an enormous growth in the field of QKD as compare to quantum computer. Currently, QKD researches are mostly based on experimental and mathematical. Mathematical modeling is inefficient due to unable to comprehend the real experiment issues. The later

research is expensive due to need of photonics components. At this stage, it is expensive and cost millions to setup and implement quantum security solutions. Further, QKD research lacks of effective simulation tool which is able to simulate the QKD's protocol and implementation. There is a complexity in developing the quantum based simulation. It is also very difficult to measure and quantify risk in using quantum security solutions. Current, simulation tools are able to simulate macroscopic elements very well due to its deterministic type. On the other hand, quantum is basically stochastic nature. Further classical theories have failed so far in describing absolutely about the microscopic level of elements. Before, we delve into further issues; a brief summary of quantum theory is summarized in order to understand the quantum world clearly.

Therefore, the quantum simulator offers an easy way to manipulate desired component parameters while setting other parameters fixed. It is also provides a simpler way of conducting experiments, with a further cost reduction in relation to the practical real experiment. This article aims to emphasize the modeling issues of the quantum world and details that need to be considered during computer simulation. We describe the design of a proposed Quantum Cryptography and Communication Simulator (QuCCs) which was implemented in Java programming language as an interface, MatLab/Mathematica for calculation, and MySQL as a database. QuCCs is a simulator aimed as software designing tools for implementing secure key exchange solutions based on quantum principles. Moreover, QuCCs is designed as an online simulation tool with various interactive features such as online collaboration, virtual lab, cost estimation and budget planning which align with quantum communication experimental models.

This paper also aims to emphasize the modeling issues of the quantum world and details need to be considered during computer simulation. We would like to describe briefly about the modeling issues of macroscopic devices in the quantum world. For example, the detectors are macroscopic devices used to measure microscopic quantities. Macroscopic measuring devices have an enormous number of quantum states. Due to decoherence effect, wave function of the neutron in the detector is lost some information. The detector registers the remaining information with relative probability. Simulation of quantum world consists of stochastic process. The random number generator plays a vital role in the computer simulation program for quantum world. This article is organized as follows: Section 2 outlines the background works on Quantum Cryptography simulator. Section 3 describes the quantum theories. Section 4 introduces the design of QuCCs's Model. Section 5 provides the methodology to conduct the simulation. Section 6 discusses about the experiment's result while Section 7 concludes this article and outlines the future work.

2. Quantum Cryptography Simulator

This section reviews several quantum cryptography simulator for conducting quantum experiment. Attila Pereszlényi's (Pereszlényi, 2005) circuit which studies the QKD protocols by means quantum circuit level. Qcircuit has the quantum circuit interface with various objects to denote the OKD elements and analyze quantum bit error rate. Later, Object oriented simulation for QKD was proposed by Zhang et al. (2007). Zhao and De Raedt (2008) proposed an event-by-event simulation model and polarizer as the simulated component for QKD protocols i.e. BB84 protocol by Bennet and Brassard and Ekert's (Ekert, 1991) protocol with presence of Eve and misalignment measurement as scenarios. Niemiec et al. (2011) presented a C++ application to evaluate and test quantum cryptography protocols. This application has elegant user-friendly interface and many modules which complete entire QKD operations. It includes BB84 and B92 as a protocol option; two modules for eavesdropping; a noise level module; and privacy amplification. This simulation is suited for understanding overall QKD operations.

In contrast to above works, our previous work proposed simulation framework concentrates more on experimental elements (Buhari, 2012, Buhari et al., 2012a,b,c). Further, scalability of our module is better. One can extend to other encoding i.e. phase, amplitude and deployment of decoy states. However entangled based QKD and correlation of simulation output statistics with published experimental results are still upcoming challenges. Moreover, QKD field is conversely lacking of efficient simulation to study and evaluate the hardware performances. In our previous work, we proposed polarized based QKD based on discrete event simulation using commercial photonic simulation software called OptiSystem. OptiSystem is basically for photonic based telecommunication design and analysis tool. However, due to the presence of various photonic components, we can model QKD experiments. OptiSystem offers drag and drop solution with various inbuilt components.

Due to lack of real detector setup and missing of important components in our previous research based on OptiSystem, the experimental results are less accuracy even though closeness to real experiments. Precisely, in the source module, lack of polarization beam splitter (PBS) and lack of detector in receiver module made simulation less significant. Therefore, these limitations are the core motivation for this current research. In this paper, the required building blocks and systematic workflow for the experimental quantum cryptography protocols is proposed and defined.

3. Quantum Theory

Quantum theory is a theory to describe physics on a microscopic scale, such as on the scale of atoms, molecules, electrons, protons, etc. Both Newton's mechanical motion of object and Maxwell's light as a wave are unfit to describe precision of microscopic elements. The quantum theory is supported by the unconditional security as verified by the Heisenberg Uncertainty and no-cloning theorem. Heisenberg Uncertainty theory describes that the intruder cannot distinguish the properties of the quantum states without disturbing it while no-cloning theorem defined that the unknown quantum states cannot be copied. The following subsections explain briefly about various building blocks of quantum mechanics principles taken from Howard (1985), Pereszlényi (2005), Zhang et al. (2007).

3.1 Photon

Quantum theory describes light as a particle called a photon. In 1922, Nobel proposed light is made of quanta, later named photons, which have well defined energy and momentum. DeBroglie also proposed that a photon not only carries energy, but also carries momentum. Energy is a scalar and momentum is a vector quantity. Photons can be treated as the packets of light which behave as a particle. To describe interactions of light with matter, need particle (quantum) description of light. A single photon has an energy given by

$$\mathrm{E} = \frac{hc}{\lambda'} \tag{1}$$

where h is the planck constant with the value of 6.6×10^{-34} J/s, c is the speed of light with the value of 3×108 m/s and λ is the length of light in meter. Photons also carry momentum. The momentum is related to the energy by:

$$\mathrm{p} = \frac{e}{c} = \frac{h}{\lambda'} \tag{2}$$

In QKD, the process of sharing a sensitive information securely between parties in the network can be realized with the support key exchanged using photon for the encryption purposes. The transmission of a photon happens through the quantum channel while the transmission of the data is carried out through public channels such as radio frequency channels and the Internet.

3.2 Quantum Superposition

A quantum system can take on two states at once. For example, each quantum bit (qubit) can encode both a 1 and a 0 at the same time. The superposition states can be defined as:

$$|\Psi \equiv \alpha|0> +\beta|1> = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} \tag{3}$$

where Ψ is the superposition states,$|0>$ and $|1>$ are qubits states, and α and β are the complex numbers. The $\begin{bmatrix}\alpha\\ \beta\end{bmatrix}$ is a two dimensional vector, where $|0>$ equals to $\begin{bmatrix}1\\ 0\end{bmatrix}$ and $|1>$ equals to $\begin{bmatrix}0\\ 1\end{bmatrix}$. The probability of α and β coefficients can be satisfied by

$$|\alpha|^2 + |\beta|^2 = 1 \tag{4}$$

where $|\alpha|^2$ is the probability of obtaining $|\Psi>$ in $|0>$ and $|\beta|^2$ is the probability of obtaining $|\Psi>$ in $|1>$.

3.3 Quantum Phase Transition

Phase transition is a change in the collective properties of a macroscopic number of atoms and quantum phase describe about change in the nature of quantum superposition in a macroscopic quantum system.

3.4 Quantum Dehorence

The loss of coherence or ordering of the phase angles between the components of a system in a quantum superposition. Decoherence increases with the number of quantum logic gates (qubits). Research is going into decreasing decoherence by limiting the amount of macroscopic devices involved in the process.

3.5 Quantum Entanglement

Entanglement is one of the quantum mechanics fields that can be defined as the correlation between particles that cannot be separated even though separated by the distance between them. Two qubits are assumed to be entangled when the measurement of one qubit has affected the state of the other qubit. The disturbance by the eavesdropper to the entangled qubits may break the

correlation between them (Verma et al., 2019). The simplest entangled state is Bell state; consist of two entangled particles called Einstein-Podolsky-Rosen (EPR) pairs. In quantum entanglement, the measurement is important to determine whether the state is entangled or separable. There are two types of entanglement state which is the qubit spinning in the same direction and different direction (Chen et al., 2015). In QKD, the entangled state is utilized to establish secure key and detect the presence of eavesdropper. However, it is hard to adopt the entangled state in the current communication system due to the difficulties of generating, transmitting and storing the entangled state efficiently. Besides, a comparative study conducted by Sharma et al. (2016) found that the quantum cryptography using entanglement is physically more expensive compared to single qubit.

4. QuCCs's Model Design

This section describes and elaborates the proposed simulation framework called QuCCs. As mentioned earlier, quantum is considered as microscopic i.e. qubit and macroscopic i.e. devices transmitters, channels and receiver components. The relation between micro and macro is defined as mesoscopic simulation.

From the computer program view, devices are defined as a list of properties or characteristics. Property is referred as members or variables of a computer program, while the properties are referred to microscopic or qubit. The mesoscopic features are considered as function or behavior that is responsible for changes in the qubit properties according to the device properties. A complete mathematical description of macroscopic devices is reviewed by Scarani et al. (2009). Figure 1 classifies the mesoscopic simulation features. The following section briefly describes the modeling of few optical components.

4.1 Coherent Wave (CW) Laser

Laser is the one of the important components in the source module. There are various types of laser available in the market. This section will present coherent wave type laser. The equation of intrinsic property of CW laser can be described as

$$|\sqrt{\mu}e^{i\theta}\rangle \equiv |\alpha\rangle = e^{-\frac{\mu}{2}} \sum_{n=0}^{\infty} \frac{a^n}{\sqrt{n!}} |n\rangle \tag{5}$$

where α is the average number of photon or intensity of a pulse, μ is equal to α^2 and θ is the phase factor. It can be noted that α and θ is randomly generated

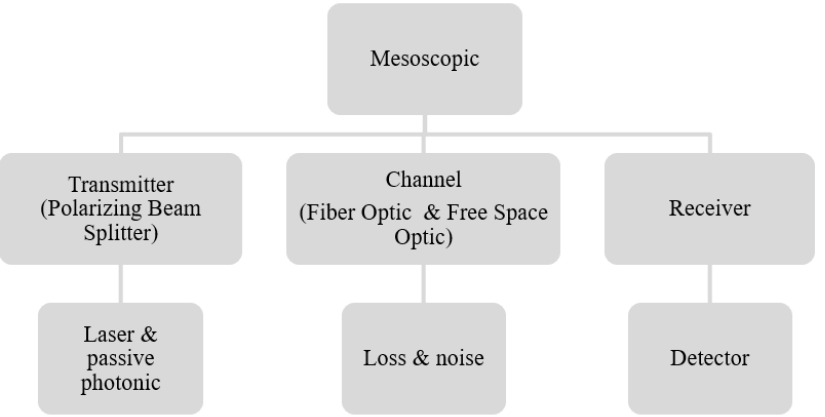


Figure 1: Classification of Mesoscopic Simulation

at the time of simulation run, while μ is calculated based on user input.

4.2 Fiber Optic Channel

The fiber channel's loss intrinsic property can be represented as

$$t = 10^{-\frac{\alpha l}{10}} \tag{6}$$

where α is the attenuation coefficient and l is the fiber optic distance. In the fiber optic network, the standard attenuation can be setup based on the operating wavelengths; 1550nm, 1300nm and 800nm for short, medium and long range applications. The attenuation coefficients are 0.25, 0.35 and 2dB/km correspondingly. The value of α and l is gathered from the user input.

4.3 Polarization Beam Splitter (PBS)

The component PBS plays a vital role in the polarized based QKD experiments. PBS is responsible to choose the encoding scheme randomly. In other words, the whole random mechanism of QKD depends on this component.

Table 1: Parameter value of the experiment

Property	**Polarization**	**Photon generation**
Rectilinear Diagonal	90°or 0° +45°or -45°	Random

4.4 Detector

Detector is the vital component in the receiver module. The function of a detector is to convert the light into electrical signal. Nevertheless, quantum cryptography still lacks of perfect detector. Supposedly, a good detector must able to achieve high detection rate. The analysis by Harun et al. (2018) proved that there are many important criterion need to be fulfilled in order to choose the best detector including low dark count rate and high detector efficiency.

Table 2: Intrinsic Property of Detectors

	APD	**InGaAs**	**VLPC**	**SSPD**	**TES**
Detected Wavelength	600	600	600	600	600
Quantum Efficiency	50%	10%	58%-85%	0.9%	65%
Fractions of dark count rate	100Hz	10^{-5}/gate	20KHz	100Hz	10Hz
Repetition Rate	CW	CW	CW	CW	CW
Maximum Count Rate	15	0.1	0.015	N/A	0.001
Jitter [ps]	50-200	500	N/A	68	9×10^4
Temperature of Operation [K]	250	220	6	2.9	0.1
Distinguishing Photon Number	N	N	Y	N	Y

5. Methodology

This section describes and elaborates the proposed simulation framework called QuCCs. As mentioned earlier, quantum is about microscopic such as qubit and macroscopic such as transmitters, channels and receiver components. The relation between micro and macro is defined as mesoscopic simulation.

The QuCCs model is a combination of discrete event simulation (DES), system dynamics and continuous simulation techniques. DES is the overall workflow of the simulation. Continuous event simulation is responsible for qubit operation and mesoscopic simulation carried out by system dynamics. As shown in Figure 2, the approach to operate the experiment is discrete event where the events describe the flow of experiment to produce qubits based on the polarization. The QuCCs enables users to input the value of the properties according to

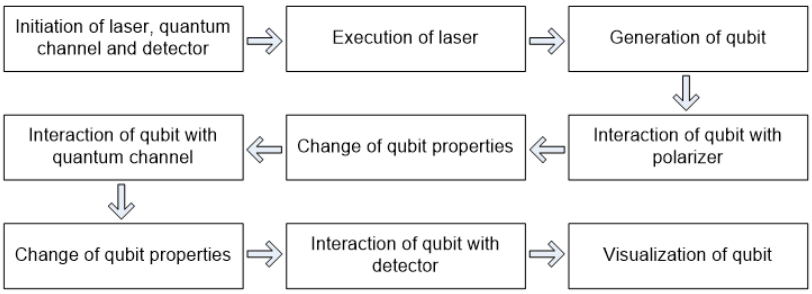


Figure 2: The simulation's flow of event

their experiment's requirement. Table 1 presents the parameters and the value range of the components in the QuCCs simulator.

Table 3: Parameter value of the experiment

Component	**Properties**	**Value range**	**Function**
Standard Laser	Frequency	0 to infinity	CalculateEnergy() CalculatePhoto-electricEffect() GenerateNoOfPhotons() CalculateMomentum() CalculateCompotonEffect()
Polarizer	Set of polarization	H, V, LD, RD	SetPolarization()
Standard Attenuator	Attenuation	Between 0 and 1	ReduceEnergyValue() ReduceNoOfPhoton() Loss(dBm)
Fibre Optic	Channel length	Between 0 and 100000	ReduceEnergyValue() CurrentEnergy(Joule)
Detector	No. of incident photon No. of electron	H, V, LD, RD	RetrievePolarization()

To conduct the QKD's experiment, we set up quantum components using QuCCs. The simulator provides an easy way to manipulate desired parameters of each component and it is very efficient to simulate the experiment with low cost compared to the practical testbed. Figure 3 presents the GUI of QuCCs consisting the component library on the left side and its properties on the left side, allows user to define parameters based on the precise component specification with varying configurations such as the frequency of laser and incoming photon polarization.

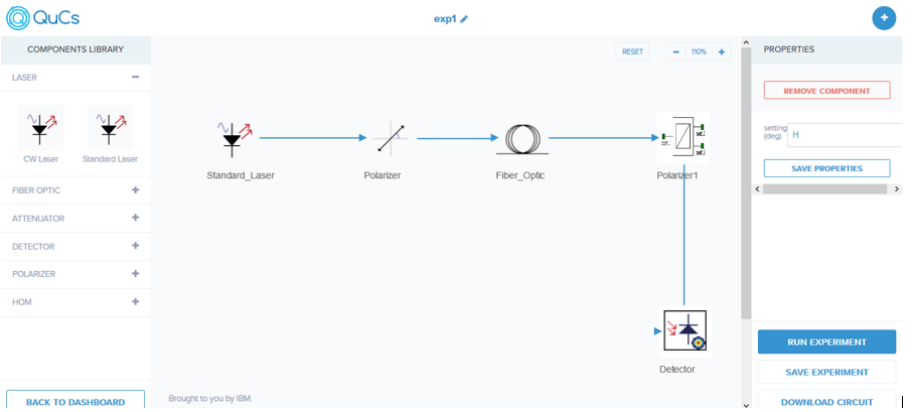
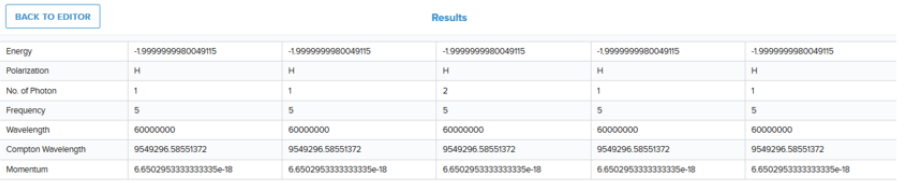


Figure 3: The Graphical User Interface of QuCCs

6. Results and Discussions

In this section, the result of experimental through QuCCs is shown and explained. Furthermore, the key challenges and benefits of the QuCCs are discussed briefly. The experiment's result presented in the Figure 4 after user click at the "run experimen" button, where user is able to view the obtain information after successful simulation. The results present the energy of the laser, polarization of photon, number of photon, frequency, compton wavelength and momentum value.

Quantum world is a stochastic nature; therefore, to model stochastic or random nature, a random number generator with big size of seed is needed. Random is the key factor for superposition. However, pseudo RNG (PRNG) based on computer program has vulnerability due to the true random number generation can be achieved by external resources. Moreover, due to limitation


BACK TO EDITOR

Results

Energy	-1.9999999980049115	-1.9999999980049115	-1.9999999980049115	-1.9999999980049115	-1.9999999980049115
Polarization	H	H	H	H	H
No. of Photon	1	1	2	1	1
Frequency	5	5	5	5	5
Wavelength	60000000	60000000	60000000	60000000	60000000
Compton Wavelength	9549296.58551372	9549296.58551372	9549296.58551372	9549296.58551372	9549296.58551372
Momentum	6.650295333333335e-18	6.650295333333335e-18	6.650295333333335e-18	6.650295333333335e-18	6.650295333333335e-18

Figure 4: The result of the experiments

of experimental data, the validation and verification of results are difficult. Another limitation is most of the quantum experimental devices are imperfect, thus reduces the quality of result.

Therefore, QuCCs is optimized to achieve correlate with theoretical result as well as available experimental result. To achieve the highly significant results, QuCCs is designed to exactly replicate the parameters and functions of quantum devices. QuCCs is a GUI based simulation with drag and drop solution, which is also contain inbuilt experimental model for fast processing. QuCCs also provides the information about the vendor details such as the specification for the component. Furthermore, QuCCs is equipped with the availability of data and results' export feature to ease the user work. Moreover, QuCCs is designed as an online program which supports other interactive features like collaboration and virtual lab. Thus QuCCs can support from novice to expert of quantum information science.

7. Conclusion

This article deals with the practical realization of quantum cryptography and communication simulator from an experimental point of view. The work summarizes the basic characteristics of the quantum component and describes ways of implementing quantum simulator. The main part of this article deals with the QuCCs simulation environment which is primarily intended as an economical way to simulate quantum communication experiments via online components with instant and reliable results. An example QuCCs implementation described in this article indicates that the quantum communication experiments results relies on the variable set up for each quantum component. The classification of simulation i.e. micro, meso and macro is important to achieve the proximity of real world experiments. Further, mesoscopic simulation is bridge between devices and qubit. We also highlight the software requirement to achieve the highly interactive GUI based simulation tool. As

a conclusion, QuCCs may give benefit the researchers from digital security, high-speed network and quantum computation to model and simulate the real quantum experiment and quantum communication. In the future, this work can be easily extended to entanglement based research. Due to QuCCs software architecture is based on object oriented programming, thefore, it is easy to enhance or add new simulation elements.

References

Bennett, C. H. and Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11.

Buhari, A. (2012). An efficient modeling and simulation of quantum key distribution protocols using OptiSystem^{TM}. In *2012 IEEE Symposium on Industrial Electronics and Applications*, pages 84–89. IEEE.

Buhari, A., Zukarnai, Z. A., Subramaniam, S. K., Zainuddin, H., and Saharudin, S. (2012a). BB84 and noise immune quantum key distribution protocols simulation: An approach using photonic simulator. In *Proc. Int. Conf. Comput. Intell. Syst., Int. Conf. Elect., Electron.(ICCIS)*, pages 30–36.

Buhari, A., Zukarnain, Z. A., Subramaniam, S. K., Zainuddin, H., and Saharudin, S. (2012b). A Discrete Event Simulation Approach on Polarized based Quantum Key Distribution Protocols using OptiSystem^{TM}. *International Journal of Computer Science and Information Security*, 10(12):42–48.

Buhari, A., Zukarnain, Z. A., Subramaniam, S. K., Zainuddin, H., and Saharudin, S. (2012c). An Efficient Modeling and Simulation of Quantum Key Distribution Protocols Using OptiSystem^{TM}. *International Journal of Computer Science and Information Security*, 10(12):8–14.

Chen, C.-Y., Zeng, G.-J., Lin, F.-J., Chou, Y.-H., and Chao, H.-C. (2015). Quantum cryptography and its applications over the internet. *IEEE Network*, 29(5):64–69.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661.

Harun, N. Z., Zukarnain, Z. A., Hanapi, Z. M., and Ahmad, I. (2018). Evaluation of parameters effect in multiphoton quantum key distribution over fiber optic. *IEEE Access*, 6:47699–47706.

Howard, D. (1985). Einstein on locality and separability. *Studies in History and Philosophy of Science Part A*, 16(3):171–201.

Niemiec, M., Romański, Ł., and Święty, M. (2011). Quantum cryptography protocol simulator. In *International Conference on Multimedia Communications, Services and Security*, pages 286–292. Springer.

Pereszlényi, A. (2005). Simulation of quantum key distribution with noisy channels. In *Proceedings of the 8th International Conference on Telecommunications, 2005. ConTEL 2005.*, volume 1, pages 203–210. IEEE.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301.

Sharma, V., Thapliyal, K., Pathak, A., and Banerjee, S. (2016). A comparative study of protocols for secure quantum communication under noisy environment: single-qubit-based protocols versus entangled-state-based protocols. *Quantum Information Processing*, 15(11):4681–4710.

Verma, P. K., El Rifai, M., and Chan, K. W. C. (2019). *Multi-photon Quantum Secure Communication*. Springer.

Zhang, X., Wen, Q., and Zhu, F. (2007). Object-oriented quantum cryptography simulation model. In *Third International Conference on Natural Computation (ICNC 2007)*, volume 4, pages 599–602. IEEE.

Zhao, S. and De Raedt, H. (2008). Event-by-event simulation of quantum cryptography protocols. *Journal of Computational and Theoretical Nanoscience*, 5(4):490–504.