A Generic Simulation Framework for Non-Entangled based Experimental Quantum Cryptography and Communication: Quantum Cryptography and Communication Simulator (QuCCs)

Abudhahir Buhari¹, Zuriati Ahmad Zukarnain², Roszelinda Khalid², Ahmad Zakir Dato` Wira Jaafar³

¹ FCMIT, Infrastructure University Kuala Lumpur (IUKL), Kajang, Malaysia; ²FSKTM, University Putra Malaysia, Serdang, Malaysia; ³ Putra Science Park, University Putra Malaysia, Serdang, Malaysia.

abudhahir@iukl.edu.my, zuriati@upm.edu.my, roszelinda@gmail.com, zakir.jaafar@gmail.com.

Abstract. The applications of quantum information science move towards bigger and better heights for the next generation technology. Especially, in the field of quantum cryptography and quantum computation, the world already witnessed various ground-breaking tangible product and promising results. Quantum cryptography is one of the mature field from quantum mechanics and already available in the markets. The current state of quantum cryptography is still under various researches in order to reach the heights of digital cryptography. The complexity of quantum cryptography is higher 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. In this paper, we propose a framework to achieve an effective non-entanglement based quantum cryptography simulation tool. We applied hybrid simulation technique i.e. discrete event, continuous event and system dynamics. We also highlight the limitations of a commercial photonic simulation tool based experiments. Finally, we discuss ideas for achieving one-stop simulation package for quantum based secure key distribution experiments. All the modules of simulation framework are viewed from the computer science perspective.

1. INTRODUCTION

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 become the norm of the current society. As the same growth of usage, hacking, spying and phreaking become common critical threats to the society. The basic reason behind this threat 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 technology limit. Further, these security mechanisms are vulnerable to brute force attack. Both smart phone and quantum computer is the toughest candidate to break the current security systems. However, security based on quantum principle provides unconditional security. Especially, the principles of no-cloning theorem and Heisenberg’s uncertainty principle culminate a new breed of
cryptography so called quantum cryptography. Under the quantum cryptography, quantum key
distribution (QKD) is the matured field and already available in the market.

QKD is a jargon of digital’s secure key distribution technique based on quantum principles. QKD
offers unconditional security which means not bounded by technology limit and only bounded
quantum law. Further, detection of attacker or eavesdropper is an intrinsic property of QKD
mechanism. Thus QKD paves the way for the next-generation security.

QKD history has already accomplished 30 years. From the ground-breaking protocol BB84 to
current QKD protocols have undergone various developments. The improvement of quantum
hardware improves the quality of QKD based solution. The presence of noise, loss and imperfect
devices make QKD need 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. 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 [1-3]. 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.

Quantum theory is a theory needed 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 following
subsections explain briefly about various building blocks of quantum mechanics principles taken from
[4-6].

1.1. 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. Nobel 1922.

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 “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

\[ E = \frac{hc}{\lambda} \]  

(1)

where

\[ h = \text{Planck’s constant} = 6.6x10^{-34} [\text{J s}] \]
\[ c = \text{speed of light} = 3x10^8 [\text{m/s}] \]
\[ \lambda = \text{wavelength of the light (in [m])} \]

Photons also carry momentum. The momentum is related to the energy by:

\[ p = \frac{E}{c} = \frac{h}{\lambda} \]
1.2. 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.

1.3. 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.

1.4. 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.

1.5. Quantum Entanglement
Our proposed simulation model has no scope for quantum entanglement oriented experiments. However, we would like to highlight the properties and developments in that area. Moreover, quantum entanglement is going to play a vital role for an effective quantum communication, computation and cryptography. Thus, quantum entanglement based research gains more important. Table 1 lists various progresses in the quantum entanglement field.

In 1935, Einstein, Podolsky and Rosen published a paper and so called EPR paradox. They disagreed the violation of relativistic locality by quantum mechanics (QM). In following year, Schrodinger published an extension of the EPR paper, coining the term “entanglement” to describe the phenomenon that particles that are arbitrary distances apart can influence one another instantaneously. Thus quantum states are not independent of observation and further it’s impossible to observe a quantum state without changing it. In other words, superposition of two electron states leads to non-local correlations between spins. For example, classical register needs 3 bits encodes one symbol of eight combinations. But, quantum register 3 qubits can encode all eight combinations at once.

1.6. Quantum Criticality
There is a complex and non-local entanglement at the critical point between two quantum phases. There is entanglement between electrons/atoms at all distance scales. Further, there is a presence of entanglement between inside and outside of a black hole. This leads to Hawking temperature or black hole temperature and Bekenstein entropy or black hole entropy.
Table 1. Quantum Entanglement Progress

| Year | Achievement |
|------|-------------|
| 2003 | Three electrons are entangled using an ultrafast laser pulse and a magnetic quantum. |
|      | Quantum synchronization of atomic clocks over long distances with unprecedented accuracy |
| 2004 | Transmission of quantum cryptographic keys over a 730 meter distance @ 1Mbps |
|      | Quantum Interferometry: Dramatic noise reduction and sensitivity improvements in quantum measurement |
|      | Quantum Teleportation: Quantum Optical lithography: quantum peak is narrower and spacing is halved |

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.

2. LITERATURE REVIEW

This section briefly recaps the related literature and explains the deficiency of our previous work on quantum cryptography simulation.

Attila Pereszlényi’s [7] Qcircuit which studies the QKD protocols by means quantum circuit level. Qcircuit has the quantum circuit interface with various objects to denote the QKD elements and analyze quantum bit error rate. Object oriented simulation for QKD was proposed by Zhang et al. [8]. Shuang and Hans [9] proposed an event-by-event simulation model and polarizer as the simulated component for QKD protocols i.e. BB84 protocol by Bennet and Brassard [10] and Ekert’s [11] protocol with presence of Eve and misalignment measurement as scenarios. Niemiec et al. [12] 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, Abudhahir et al. [13], as our previous work proposed simulation framework concentrates more on experimental elements. 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.
Our previous work, we proposed polarized based QKD based on discrete event simulation using commercial photonic simulation software called OptiSystem[14, 15] [16].

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. The polarized based QKD simulation setups using OptiSytem is presented in Appendix.

Due to lack of real detector setup and missing of important components in our previous research based on OptiSystem, cause less accuracy and 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. However, 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. METHODOLOGY
In this section, we describe elaborately our proposed simulation framework called QuCCs. As we mentioned already, quantum is all about microscopic and devices i.e. transmitters, channels and receiver components are considered as macroscopic. 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. Specifically, property referred as members or variables of a computer program. Microscopic or qubit also list of properties. The mesoscopic features are considered as function or behavior and 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. [17]. From the various QKD research, we have listed the macroscopic properties in the Appendix. Fig. 1 illustrates the qubit properties. Table 2 describes the features of each simulation and flow of simulation is viewed as 3D and represented in Figure 2.

![Figure 1. Qubit's Properties / Microscopic Features](image-url)
Table 2. Types of Simulation

| Macro Sim | Meso Sim | Micro Sim |
|-----------|----------|-----------|
| Standard Properties Default Properties | Effects Functions. | Qubit Properties |

Figure 2. 3Dimensional View of Simulation Flow

Figure 3 classifies the meso simulation features. 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 meso simulation carried out by system dynamics. The following section briefly describes the modeling of few optical components.

3.1. Modeling a Coherent Wave (CW) Laser

One of the important components in the source module is laser. There are various types of laser available. Here, we describe coherent wave type laser.
\[ |\sqrt{\mu} e^{i\theta} > \equiv |\alpha > = e^{\frac{\alpha}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n > \] 

(2)

The equation 2 describes the intrinsic property of CW laser. Table 3 represents the parameter and generation method for the equation. The column ‘generation’ represents type of calculation has been applied. The option ‘random’ choose a value at the time of simulation run. The option ‘manual’ represents the value feed from user input. The option ‘auto’ represents calculation based on user inputs.

| Property | Explanation | Generation |
|----------|-------------|------------|
| \(\alpha\) | Avg. photon number or intensity in a pulse | Random |
| \(\mu\) | \(\alpha^2\) | Auto |
| \(\theta\) | Phase factor | Random |

### Table 3. Intrinsic Property of CW Laser

3.2. Modeling of Fiber Channel

\[ t = 10^{-\frac{\alpha l}{10}} \]

(3)

The equation 3 represents the fiber channel ‘s loss intrinsic property. Table 4 shows the generation of values for fiber channel during simulation.

| Property         | Meaning                   | Generation |
|------------------|---------------------------|------------|
| \(L\)            | Length                    | Manual     |
| \(\alpha\)       | 1330nm (\(\alpha \approx 0.34\)dB/km) and 1550nm (\(\alpha \approx 0.2\)dB/km) | Manual     |
| Chromatic dispersion | -                        | Auto       |
| Polarization Mode Dispersion | Random              |             |

### Table 4. Intrinsic Property of Fiber Channel

3.3. Modelling of Free-Space Optics Channel

\[ t \approx \left( \frac{d_\tau}{d_\alpha + D l} \right)^2 10^{-\frac{\alpha l}{10}} \]

(4)
The equation 4 represents the losses in the telescope communication. In quantum jargon, telescope/communication refers as free-space optics. Table 5 shows the generation techniques for the free-space optics.

**Table 5. Intrinsic Property of Free Space Optics**

| Property | Meaning                                      | Generation |
|----------|----------------------------------------------|------------|
| $d_r$    | Geometric losses in receiving telescopes     | Auto       |
| $d_s$    | Geometric losses in sending telescopes       | Auto       |

3.4. Intrinsic Properties of Detector

Detector is the vital component in the receiver module. Detector function is to convert to the light into electrical signal. However, quantum cryptography still lacks of perfect detector. Table 6 represents various detector types with their intrinsic property.

**Table 6. Intrinsic Property of Detectors**

| Name                          | Avalanche Photo Diode: Silicon | InGaAs | VLP C | SSPD | TES |
|-------------------------------|--------------------------------|--------|-------|------|-----|
| Detected wavelength           | 600                            | 1550   | 650   | 1550 | 1550|
| Quantum Efficiency            | 50%                            | 10%    | 58%-85% | 0.9% | 65% |
| Fractions of dark count rate  | 100Hz                          | $10^3$/gate | 20KHz | 100Hz | 10Hz |
| Repetition Rate               | Coherent Wave (CW)             | 10     | 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   |

3.5. Modelling of Polarization Beam Splitter (PBS)
The component PBS plays a vital role in the polarized based QKD experiments. PBS is responsible of choosing randomly the encoding scheme. In other words, the whole random mechanism of QKD depends on this component. Table 7 presents the intrinsic property of PBS.

| Property | Meaning          | Generation     |
|----------|-----------------|----------------|
| Rectilinear | 90 degree or 0 degree | Random Selection |
| Diagonal       | +45 or -45 degree   | Random Selection |

3.6. Calculation of Raw Data Rate

\[ R = q \mu \nu (1 - L) \eta \]  \hfill (5)

The equation 5 represents the mathematical modeling of simple raw data rate calculation. This is prior to sifting in the QKD mechanism. Table 8 represents the calculation technique in the simulation.

| Meaning                  | Generation |
|--------------------------|------------|
| Raw data rate           |            |
| \( q \) – Polarization Selection | Random     |
| \( \mu \) – Avg. photon number | Auto       |
| \( \nu \) – Pulse rate of the laser | Auto       |
| \( L \) – Losses in the Fiber link | Auto       |
| \( \eta \) – Quantum efficiency | Auto       |

3.7. Simulation Flow.

The overall operation of experiment is a discrete event approach. For example, the following events describe the flow of operation to produce polarized based qubit.

1. Initiation of LASER, Channel, and Detector  
2. Execution of LASER  
3. Generation of Qubit  
4. Qubit interact with Polarizer  
5. Change of Qubit Properties  
6. Qubit interact with Channel  
7. Change of Qubit Properties  
8. Qubit interact with Detector  
9. Change of Qubit  
10. Visualization of Qubit
However, to simulate channel, continuous event simulation has been used and for the detector, system dynamics has been applied.

QuCCs is intent to design as online simulation tool with various interactive features like online collaboration, virtual lab, cost estimation and budget planning. QuCCS is aimed to one-stop solution for secure key exchange solutions based on quantum principles.

4. DISCUSSION
In this section, the key challenges and benefits of the QuCCs are discussed briefly. As mentioned already, quantum world is a stochastic nature. To model stochastic or random nature, a random number generator with big size of seed is needed. However, Pseudo RNG (PRNG) based on computer program has vulnerability. A true random number generation can be achieved by external resources. Random is the key factor for superposition.

Further, due to limitation of experimental data, the validation and verification of result is quite challenging. However, the QuCCs is optimized to achieve correlate with theoretical result as well as available experimental result.

To achieve the highly significant results, exact replica of devices parameters and functions are needed. Nevertheless, the most of quantum experimental devices are imperfect. Thus this factor reduces the quality of result.

On the other hand, QuCCs is a GUI based simulation with drag and drop solution. QuCCs also contains inbuilt experimental model for fast process. QuCCs also provides the information about the vendor details i.e. price and specification for the component. Further, availability of data and results’ export feature ease the user work. Moreover, QuCCs is designed as online program which supports other interactive feature like collaboration and virtual lab. Thus QuCCs can support from novice to expert of quantum information science.
5. CONCLUSION
In this paper, we overviewed the proposed framework of QuCCs. 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. This work can be easily extended to entanglement based research. QuCCs software architecture based on object oriented programming. Thus, easy to enhance or add new simulation elements.

6. ACKNOWLEDGMENT
This project is developed under and support from UPM’s InnoHub program. We would like to thank Assoc. Prof. Dr. Samsilah Roslan for their wonderful effort and support.

References

1. Engle, R.D., et al., *A module-based simulation framework to facilitate the modeling of Quantum Key Distribution system post-processing functionalities*. The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, 2016: p. 1548512916666740.

2. Kabir, K.S., T. Chakraborty, and A.A. Al Islam. *Supercrypt: a technique for quantum cryptography through simultaneously improving both security level and data rate*. in 2016 International Conference on Networking Systems and Security (NSysS). 2016: IEEE.

3. Schranz, Á., E. Udvary, and Z. Kis. *Photon statistics determination for single photon based quantum key distribution*. in Transparent Optical Networks (ICTON), 2016 18th International Conference on. 2016: IEEE.

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

5. Ballentine, L.E., *Quantum mechanics*. Vol. 280. 1990: Prentice Hall Englewood Cliffs.

6. Horodecki, R., et al., *Quantum entanglement*. Reviews of Modern Physics, 2009. 81(2): p. 865.

7. Pereszlenyi, A. *Simulation of quantum key distribution with noisy channels*. 2005.

8. Zhang, X., Q. Wen, and F. Zhu. *Object-Oriented Quantum Cryptography Simulation Model*. 2007: IEEE.

9. Zhao, S. and H. De Raedt, *Event-by-event Simulation of Quantum Cryptography Protocols*. Journal of Computational and Theoretical Nanoscience, 2008. 5(4): p. 490-504.

10. Bennett, C.H. and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*. in IEEE International Conference Computer Systems and Signal Processing. 1984. Bangalore, India.

11. Ekert, A.K., *Quantum cryptography based on Bell's theorem*. Physical Review Letters, 1991. 67(6): p. 661-663.

12. Niemiec, M., Ł. Romański, and M. Święty. *Quantum Cryptography Protocol Simulator*. Multimedia Communications, Services and Security, 2011: p. 286-292.

13. Buhari, A., et al. *An efficient modeling and simulation of quantum key distribution protocols using OptiSystem™*. in Industrial Electronics and Applications (ISIEA), 2012 IEEE Symposium on. 2012: IEEE.

14. Buhari, A., et al., *BB84 and Noise Immune Quantum Key Distribution Protocols Simulation: An Approach Using Photonic Simulator*, in International Conference on Computer and Intelligent Systems (ICCCIS’2012) & International Conference of Electrical, Electronics, Instrumentation and Biomedical Engineering (ICEEIB’2012) Dec. 28-29, 2012. 2012: Bangkok (Thailand).
15. Buhari, A., et al., *A Discrete Event Simulation Approach on Polarized based Quantum Key Distribution Protocols using OptiSystem™*. International Journal of Computer Science and Information Security (IJCSIS), 2012. **Vol.10**(12): p. 42-48.

16. OptiSystem. Available from: [www.optiwave.com](http://www.optiwave.com).

17. Scarani, V., et al., *The security of practical quantum key distribution*. Reviews of Modern Physics, 2009. **81**(3): p. 1301.