The Simulation of one-time-pad quantum key distribution

M Delina\textsuperscript{1,*}, B H Iswanto\textsuperscript{1}, H Permana\textsuperscript{2} and S Muhasyah\textsuperscript{3}

\textsuperscript{1}Physics Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. Jl. Rawamangun Muka No 1, Jakarta Timur 13220, Indonesia
\textsuperscript{2}Educational Physics Department, Faculty of Mathematics and Natural Sciences, Universitas Negeri Jakarta. Jl. Rawamangun Muka No 1, Jakarta Timur 13220, Indonesia
\textsuperscript{3}Ministry of Foreign Affair Republic Indonesia, Jl. Taman Pejambon No 6, Jakarta Pusat, Indonesia

*mutia_delina@unj.ac.id

Abstract. The quantum key distribution provides a secure information exchange. The system employed a single photon as the messenger. In this study one-time-pad (OTP) quantum key distribution provide a key which is use securely. For example, in a war. Therefore, it is not possible to share the secreete key in this condition, but the OTP can be generated several times as long as there is no eavesdropped detected. This paper discusses the simulation of a one-time pad quantum key distribution with event-by-event method.

1. Introduction
Cryptography is needed to produce a secure information transmission from sender to the recipient [1]. A long time ago, Julius Caesar used this technique to send a classified message by shift the alphabet. For examples with shift 3 then A is replaced by D, B is replaced by E, C is replaced by F and so on. With this technique message SAVE THE CITY become VDYH WKH FLWB. This technique is known formally as Caesar cipher [2]. Subsequently, some other techniques arise and become more complex, such as Vigenere cipher [3], Jingsaw cipher [4], two letters cipher [5] and Quantum Key Distribution [6].

Vigenere cipher, which is proposed by Giovan Battista Bellasoin 1553 is the expansion of Caesar cipher. The technique uses several Caesar ciphers in a sequence which consist of several shifts. An alphabet table: tabula recta, Vigenere square and Vigenere table can be employed to encrypt a message. For example, the original information is THE, and the secret key is ABC. A is shift 0, B is shift 1 and C is shift 2. By adding ABC to THE and then the word is changed to be TIG.

Jigsaw cipher is more interesting than the previous one. This technique uses a simple, transposition system. The message is written into a rectangle box which consists of horizontal dan vertical lines. The length of horizontal lines is determined by the key’s number, while the dimension of the message forms the length of vertical lines. The message is written line by line from to the button of rectangle box. The example is shown in table 1. The message uses four digits key to write ATTACK THE CITY NOW. Then the message is written as follow TTYO TKCN ACEY AHTW. Table 1. The rectangle box with 3 digits key.
The next technique is two letter cipher. The name came from the procedure which replace the original letter into two letters. The replacement does base on table 2.

Table 1. Example the button of rectangle box.

| 3 | 2 | 1 | 4 |
|---|---|---|---|
| A | T | T | A |
| C | K | T | H |
| E | C | Y | T |
| Y | N | O | W |

Table 2. The rectangle box with 3 digits key.

|   | A | B | C | D | E |
|---|---|---|---|---|---|
| A | A | B | C | D | E |
| B | F | G | H | I | K |
| C | L | M | N | O | P |
| D | Q | R | S | T | U |
| E | V | W | X | Y | Z |

The alphabet replaced by two letters from the horizontal and vertical line which parallel with it. Alphabet A replaced by AA, B replaced by AB, L replaced by CA, P replaced by CE etc. For example, message HELP ME become BCAEC ACECB AE. This technique omitted J, which replace by I.

There are many other techniques, and the famous one is Quantum key distribution (QKD) which developed by Bennet and Brassard [7]. This technique offered modern cryptography by employs a single photon as the messenger and gives a secure key solution based on the theory of quantum mechanics. The predominance of this technique is that the message will break when an eavesdrops intercept it. The broken message is a signal of an eavesdropper presence. The quantum key distribution is built from two components; the algorithm and the key. The algorithm gives the mathematical process to change or transform the original file, while the key locks and unlocks the file. There are two kinds of key to lock and unlock the file; symmetric and asymmetric. The symmetric key uses a similar key to encrypt and descript the message. Otherwise, the asymmetric key uses two different keys to each encrypt and descript the message. There is a specific condition which needs a special key. The key is used only once: for example, in a war. This key well is known as the one-time pad key (OTP). In this study, we use the event-by-event method to simulate the one-time-pad quantum key distribution.

2. Event-by-event method

Event by event is a new computer simulation method developed by De Raedt et al [8]. The method has several advantages: it simulates the quantum phenomenon event-by-event, the contribution of each photon influences simulation result. It reproduces the results of quantum theory; and it does not need to solve the Schrodinger equation. The simulation uses classical wave theory and quantum particle concept only [7]. This method also capable in simulating the quantum cryptography distribution [9].

Quantum key distribution allows two parties (Alice and Bob) to do a message transmission throughout photon securely. A single photon is the messenger which carries polarization information. The quantum key distribution uses two sets of non-orthogonal system based on 45° rotation. Therefore, the single photon polarized in the horizontal 0° or in the vertical 90° state. The photon can also be polarized in diagonal 45° or anti diagonal 135°. The message which was sent by Alice to Bob are in bit mode, 0 or 1. Then output bit 0 and 1 has intensity.
\[ I_0 = \cos 2(\psi - \phi), \]
\[ I_1 = \sin 2(\psi - \phi). \]  

(1)

where \( \psi \) polarization of incident beam and \( \phi \) is polarization orientation. The output 0 is represented by \( \phi \) while output 1 is represented by \( \phi + 90^\circ \).

3. One-Time Pad (OTP)
One-time pad is a secure key to protect classified information also called Vernam cipher. This technique proposed by Frank Miller and Gilbert Vernam. In this technique the length of secret key (pad) and plaintext message is equal. Previously OTP is used only once and random. One-time-pad quantum key cannot be copied, or eaves dropped. But in quantum era, random OTP can be use repeatedly as long as there is no eavesdropped [8].

4. The simulation
Following is a sequence of the simulation program. Alice and Bob transmitted a secret message. The first step, Alice set classical one-time pad secret key for Alice and Bob. The key should be a sequence random binary number. The second step, Alice formulated the classical message, event-by-event — each message represented by sequences binary numbers randomly. The position and value of each binary number have to be recorded by Alice. The third step, Bob encrypted the message with classical one-time pad key. Alice prepared a sequence of N single photon according to the value of the key and sent the message to Bob. The single photon or the messenger carried the ciphertext.

The fourth step, Bob receipted message from Alice. Bob decrypt the message by measuring each photon. After getting the key from measurement, Bob encrypts the message. Both partied; Alice and Bob have to make sure there is no eavesdropped. The present of eavesdropped will give an error. A big error show there was eavesdropped in the message transmission. No error means the absence of an eavesdropper. The fifth step is after checking the message, Alice and Bob able to reuse the key when there is no error in the measurement.

5. Conclusion
Using particle only, event-by-event simulate the one-time-pad quantum key distribution. One-time pad quantum key distribution can transmit the classified message securely. The key can be used repeatedly as long as there is no error in the measurement.

References
[1] A E Omolara, A Jantan, O I Abiodun and H Arshad 2018 An Enhanced Practical Difficulty of One-Time Pad Algorithm Resolving the Key Management and Distribution Problem Proceedings of the International MultiConference of Engineers and Computer Scientists 1
[2] A Jain, R Dedhia and A Pathil 2015 Enhancing the Security of Caesar Cipher Substitution Method using a Randomized Approach for more Secure Communication International Journal of Computer Applications 129(6)
[3] A Bhateja, S Kumar and A K Bhateja 2013 Cryptanalysis of Vigenere Cipher Using Particle Swarm Optimization with Markov Chain Random Walk IJCSE 5(422)
[4] V Kodaganallur 2006 Secure E-Commerce: Understanding the Public Key Cryptography Jigsaw Puzzle Information Systems Security 14 (6)
[5] R Curchhouse 2004 Codes and Ciphers Cambridge University Press
[6] Zhi-Hao Liu and Han-Wu Chen 2016 Cryptanalysis and improvement of quantum broadcast communication and authentication protocol with a quantum one-time pad Chin. Phys. B 25(1)
[7] M Elboukhari, M Azizi and A Azizi 2010 Quantum Key Distribution Protocols: a Survey International Journal of Universal Computer Sciences 1(59)
[8] H De Raedt, K De Raedt and K Michielsen 2005 Event-based simulation of single-photon beam splitters and Mach-Zehnder interferometers Europhysics Letter 69(6)
[9] H De Raedt, M Delina, F Jin and K Michielsen 2012 Corpuscular Event-by-Event Simulation of Quantum Optics Experiments: Application to a Quantum-Controlled Delayed-Choice Experiment *Physica Scripta* (T121)