Journal of Quantum Information Science, 2015, 5, 103-108
Published Online September 2015 in SciRes. http://www.scirp.org/journal/jqis
http://dx.doi.org/10.4236/jqis.2015.53012

Analysis of Security of Quantum Key Distribution Based on Entangled Photon Pairs by Model Checking

Surapol Rochanapratishtha, Wanchai Pijitrojana

Department of Electrical and Computer Engineering, Faculty of Engineering, Thammasat University, Bangkok, Thailand
Email: r.surapol@gmail.com, pwanchai@engr.tu.ac.th

Received 14 July 2015; accepted 13 September 2015; published 16 September 2015

Abstract

Quantum key distribution is a technique to securely distribute a bit string between two parties by using the laws of quantum mechanics. The security of this technique depends on the basis of quantum mechanics rather than the difficulty of the mathematical calculation as in the classical encoding. Researches in this field have shown that the quantum key distribution will be fully functioning outside the laboratory in a few years. Due to the complexity and the high efficiency of the device, the verification is needed. In this article, we use PRISM to verify the security of the quantum key distribution protocol, which uses the entangled photon based on BB84 protocol.

Keywords

Cryptography, Quantum Cryptography, Quantum Key Distribution, Model Checking

1. Introduction

Security has currently become an important topic of research. Confidential information, e.g. financial and credit card information, requires the highest security. Therefore the cryptography has been used to protect the information. Nowadays the quantum cryptography is proposed as an alternative approach for security. The quantum cryptography is based on the quantum physics. The first protocol of the quantum key distribution was proposed in 1984 by Bennett and Brassard as BB84 protocol [1]. After that, so many quantum key distribution protocols have been proposed. However, BB84 protocol is still the most widely used protocol till date.

The mathematical verifications of the security of the quantum key distribution are currently not sufficient. Therefore computer science researcher developed a technique and a device for analyzing protocols. For example,

How to cite this paper: Rochanapratishtha, S. and Pijitrojana, W. (2015) Analysis of Security of Quantum Key Distribution Based on Entangled Photon Pairs by Model Checking. *Journal of Quantum Information Science*, **5**, 103-108.
http://dx.doi.org/10.4236/jqis.2015.53012

the model checker SPIN [2] can test the model for the compatibility with the temporal formula. However the model checker PRISM [3] is a probabilistic symbolic model checker which calculates the probability of compatibility using the formula. The reason that the quantum mechanics is used is due to its random nature.

Therefore, in this article, we proposed the analysis of the security of QKD using PRISM. This work is similar to [4]-[7]. The distinct difference is that we have collected the efficiency parameters of the quantum channel and the parameters of the rate of attack in [6] and applied to the quantum key distribution protocol with entangled photon pairs. The idea is similar to [8] but here we use the entangled photon pairs instead of the qubit pairs.

The structure of the article is as follows. Section 2 presents the details of the BB84 protocol with Qubit pairs. In Section 3, we propose the basic technique of model checking and show the needs of this technique for the analysis of QKD. In Section 4, we present the result of the security analysis of the EEBB84 protocol that uses the efficiency parameters and the rate of attack to analyze the eavesdropping detection function. Lastly, we discuss the conclusion in the Section 5.

2. Quantum Key Distribution: BB84 with Entangled Photon Pairs

Quantum Key Distribution (QKD) uses quantum mechanics to guarantee secure communication. It is only used to produce and distribute a key $K = \{0,1\}^n$, not to transmit any message data. This key can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can then be transmitted over a standard communication channel.

The protocol BB84 [1], named after its inventors and year of publication, uses four photon polarization states grouped together in two different non-orthogonal bases. It is based on the assumption that only one photon can be transmitted at a time.

In general the two non-orthogonal bases are:

a) Base + having horizontal polarization (0˚) and vertical polarization (90˚), and we represent the base states with intuitive notation: $|0\rangle$ and $|1\rangle$. So, we have $+ = \{|0\rangle, |1\rangle\}$.

b) Base × having diagonal polarizations (45˚) and (135˚). The two different base states are $|+\rangle$ and $|-\rangle$ with $|+\rangle = 1/\sqrt{2} \cdot (|0\rangle + |1\rangle)$ and $|-\rangle = 1/\sqrt{2} \cdot (|0\rangle - |1\rangle)$. So, we have $\times = \{|+\rangle, |-\rangle\}$.

The association between the information bit and basis are described in the **Table 1**.

The protocol can be described as follows:

1) Quantum Transmissions (First Phase)

a) Sources of entangled photon pairs randomly to create a pair of photons, then separate the photon qubit partner forwarded to Alice and Bob. Alice chooses a random string of bases $b \in \{+,\times\}^n$, where $n > N$.

b) Alice prepares a photon in quantum state a_{ij} for each bit d_i in d and b_i in b as in **Table 1**, and sends it to Bob over the quantum channel.

c) With respect to either + or ×, chosen at random, Bob measures each a_{ij} received. Bob's measurements produce a string $d' \in \{0,1\}^n$, while his choices of bases form $b' \in \{0,1\}^n$.

2) Public Discussion (Second Phase)

a) For each bit d_i in d

i) Alice over the classical channel sends the value of b_i to Bob.

ii) Bob responds to Alice by stating whether he used the same basis for the measurement. Both d_i and d_i' are discarded if $b_i \neq b_i'$.

b) Alice chooses a random subset of the remaining bits in d and discloses their values to Bob over the classical channel. If the result of Bob's measurements for any of these bits does not match the values disclosed, eavesdropping is detected and communication is aborted.

c) The string of bits remaining in d once the bits disclosed in step 2b) are removed is the common secret key, $K = \{0,1\}^N$.

Measuring with the incorrect basis yields a random result, as predicted by quantum theory. Thus, if Bob

Table 1. Coding scheme for the BB84 protocol.

Table Head	+	×
0	$\|0\rangle = a_{00}$	$\|+\rangle = a_{10}$
1	$\|1\rangle = a_{01}$	$\|-\rangle = a_{11}$

chooses the × basis to measure a photon in state 1, the classical outcome will be either 0 or 1 with equal probability because $|1\rangle = 1/\sqrt{2} \cdot (|+\rangle - |-\rangle)$; if the + basis was chosen instead, the classical outcome would be 1 with certainty because $|1\rangle = 1|1\rangle + 0|0\rangle$.

To detect Eve, Alice and Bob perform a test for eavesdropping in step 2b) of the protocol. The idea is that, wherever Alice and Bob's bases are identical (*i.e.* $b_i = b_i'$), the corresponding bits should match (*i.e.* $d_i = d_i'$). If not, an external disturbance is produced or there is noise in the quantum channel, we suppose all that is caused by Eve. In our article we are interested in analyzing this important property assured by quantum mechanics: the enemy's presence is always made manifest to the legitimate users.

3. The Model Checking for Our Work

Designing the hardware and software for a complicated system requires a lot of time and effort to ensure the correctness. A technique that can help reduce the time and ensure the complete validity of a system is the formal verification. This technique can prove the correctness of the algorithm of the system required. The formal verification also includes the model checking.

Model checking is the technique of the brute-force verification of the system correctness. The model checking is used in the problem regarding the model that needs the automatic checking of the specification. We write the model checking using PRISM of model M with the specification pi as $M \vDash P_i$. The probability is calculated by

$$\Pr\{M \vDash P_i\} \tag{1}$$

By writing $M = M(x_1, x, \cdots, x_n)$, we can write the probability in Equation (1) for each of the x_i. The resulting plot will show the description of Equation (1).

The model in PRISM consists of modules. Each module has its own working process and variables. The working mechanisms of each module are shown as follower

$$[action] \to a_1 : (\text{var}_1 = \text{value}_1) + a_2 : (\text{var}_2 = \text{value}_2) + \cdots + a_n : (\text{var}_n = \text{value}_n); \tag{2}$$

In Equation (2), the variable var_i is defined by value_i with a probability equal to $a_i = 1$. In case of $n = 1$ we have a symbolic $a_1 : (\text{var}_1 = \text{value}_1) = (\text{var}_1 = \text{value}_1)$ with 1 and $a = 1$. The model checker PRISM allows for us defined a probability is an action. For instant: in case $n = 2$ we have modelling tends of protocol EEBB84 of Alice in choice of state of quantum by module as component the action:

$$[stateofAlice]true \to 0.7 : (EtatAlice = |1\rangle) + 0.3 : (EtatAlice = |0\rangle); \tag{3}$$

In Equation (3), Alice tends to choose one type of encoding data 1 in **Table 1**.

4. Analysis of the Entangled Photon Based on the BB84 Protocol by PRISM

4.1. The Detailed of the Model EEBB8 in PRISM

The tool PRISM is the device for checking the probability. It was developed at the University of Birmingham. The characteristic of the model checker is that the input of the module represents the state change of the system and the general rule is in the form of temporal logic. The answer can be "yes" and "no" which shows the compatibility with the specification.

The testing of the probability model refers to the analysis of the probability arises from the transition of states and the analysis with the analytical method.

We setup the model of BB84 in PRISM started by setting the source to be an entangled photon using M_{EEBB84} symbol.

This model consists of the following modules: a quantum channel's module, Alice's module, Bob's module and Eve's module. This is consistent with quantum key distribution. We want to study the properties of security protocols EEBB84 with PRISM. We define the models that the model has to detect intercept them. So if Alice and Bob know that Eve was eavesdropping attempts. They have agreed to stop the process of creating a secret key code immediately. By using our model of EEBB84 calculate the probability as follows:

$$\Pr\{M_{EEBB84} \vDash P_{\text{det}}\} \tag{4}$$

where P_{det} represents a formula PCTL which its Boolean value is TRUE if the eavesdropper is detected. We

can adjust the value of n to change the number of photons transmitted to the communication channel between Alice and Bob. So in our PRISM model this probability is a function of n. We write the probability of detecting the eavesdropper as follows:

$$P_{\text{det}}(n) = \Pr\{M_{EEBB84} \vDash P_{\text{det}}\} \tag{5}$$

We can see that PRISM will calculate the exact value of the probability of detecting an eavesdropper Eve. But we need to set definitions for P_{det}. In order to determine the precise detection Eve, will allow us to write P_{det} similar to the traditional values of a probability $P_r(\varphi)$.

4.2. The Detailed of P_{det}

The model M_{EEBB84}, we assume that Eve is a type of attack "intercept-resend". So, Eve to trap photons passed in quantum communication channel. Eve will measure the photon with basis vectors (+ or x), and Eve to have measurable results given by T_i^{eve}. Then Eve sends photons to Bob with the same type of basis vectors. When Bob receives the photons by Eve and then Bob will be measured by a vector based on the measurement results is set by T_i.

In order to detect Eve, it is necessary to compare the bits of Alice and Bob (which are respectively A_i and B_i) when the test of Bob is $T_i = 1$; if in such case $(A_i \neq 1 - B_i)$ then we are sure that a disturbance take place and it be caused certainly by the enemy, Eve. Let us note here that we suppose that the quantum channel is perfect; an imperfect channel can cause additional disturbances. In such case, for the need of the security we suppose all noise is due to Eve.

So, Eve's presence is made manifest as soon as the following event φ occurs:

$$\varphi = (T_i = 1) \wedge (A_i \neq 1 - B_i) \text{ for some } i \leq n \tag{6}$$

$$\varphi = (T_i = 1) \wedge (A_i = B_i) \text{ for some } i \leq n \tag{7}$$

Therefore, we can give the expression of $P_{\text{det}}(n)$ as a classical probability:

$$P_{\text{det}}(n) = \Pr\{(T_i = 1) \wedge (A_i = B_i)\} \text{ for some } i \leq n \tag{8}$$

Finally, the PCTL formula P_{det} corresponding to this formula is:

$$P_{\text{det}} = \{TRUE \cup (T_i = 1) \wedge (A_i = B_i)\} \tag{9}$$

4.3. The Probability of Detection of the Eavesdropper

Here it is based on the assumption that the channel can store only one photon at a time and the quantum channel is ideal. We model this in the quantum channel module by the line:

$$[\text{aliceput}](\text{ch\_state} = 0) \rightarrow (\text{ch\_state}' = 1) \& (\text{ch\_bas}' = \text{al\_bas}) \& (\text{ch\_bit}' = \text{al\_bit}); \tag{10}$$

But, the eavesdropper intercepts all the photons passing through the channel. We model this in the quantum channel module by the line:

$$[\text{eveput}](\text{ch\_state} = 3) \rightarrow (\text{ch\_state}' = 4) \& (\text{ch\_bas}' = \text{eve\_bas}) \& (\text{ch\_bit}' = \text{eve\_bit}); \tag{11}$$

We use ch_state, ch_bas, ch_bit, al_bas, al_bit for respectively state, base and bit of the channel and base and bit of Alice. This line shows that the information sent by Alice (base and bit) remain unchanged before it received by Eve.

For $1 \leq N \leq 30$, PRISM calculates $P_{\text{det}}(N)$, this produces the curve of P_{det} (noted as $P_{\text{det}}(N)$) as in **Figure 1**.

We note from the above curve, if we increase the number of photons emitted by Alice over the quantum channel, the probability of Eve's detection increases and tends towards 1.

4.4. The Effect on Quantum Channel's Performance and Rate of Attack

In our model MBB84, the quantum channel is represented by a module called Quantum Channel which can be in

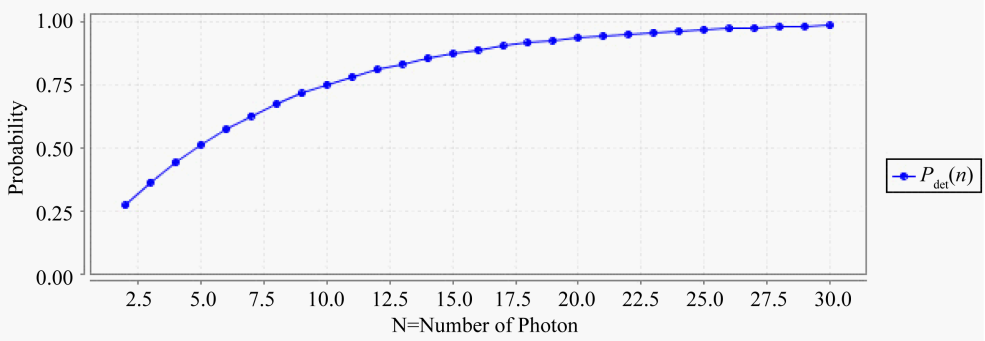

Figure 1. The probability to detect Eve where the no of photons transmitted by Alice.

reality optical fiber or free air. We expect that the probability of detecting Eve increases when the quantum channel becomes noisy and also the probability of detecting Eve increases when the rate of attack increases. To achieve this we have consider 3 cases.

1) channel(no noise) and weak attack

As the channel is ideal channel we can model this in module quantum channel as Equation (9). When Eve doesn't intercept most of the photons, we simulate a weak attack. We can write this line as:

$$[eveput](\text{ch\_state}=3)\rightarrow(\text{ch\_state}'=4)\&(\text{ch\_bas}'=\text{al\_}bas)\&(\text{ch\_bit}'=\text{al\_bit}); \quad (12)$$

2) Little noisy channel and medium attack

When there is little noise in the channel we can model this in the module quantum channel as:

```
[aliceput]  (ch_state=0) → 0.7:(ch_state'=1) & (ch_bas'=al_bas) & (ch_bit'=al_bit)
                          +0.1:(ch_state'=1) & (ch_bas'=1-al_bas) & (ch_bit'=1-al_bit)
                          +0.1:(ch_state'=1) & (ch_bas'=al_bas) & (ch_bit'=1-al_bit)
                           +0.1:(ch_state'=1)  &  (ch_bas'=1-al_bas)  &  (ch_bit'=al_bit);   (13)
```

As Eve performs a medium attack here we can model this line as:

```
[eveput]   (ch_state=3) → 0.5:(ch_state'=4) & (ch_bas'=eve_bas) & (ch_bit'=eve_bit)
                          +0.5:(ch_state'=4) & (ch_bas'=al_bas) & (ch_bit'=al_bit);   (14)
```

3) Much noisy channel and strong attack

When there are very much noise in the channel we can model this in the quantum channel as:

```
[aliceput] (ch_state=0) →0.1:(ch_state'=1) & (ch_bas'=al_bas) & (ch_bit'=al_bit)
    +0.3:(ch_state'=1) & (ch_bas'=1-al_bas) & (ch_bit' '=1-al_bit)
    +0.3:(ch_state'=1) & (ch_bas'=al_bas) & (ch_bit'=1-al_bit)
                          +0.3:(ch_state'=1) & (ch_bas'=1-al_bas) & (ch_bit'=al_bit);  (15)
```

As Eve intercepts all the photons passing through the channel we can model this in quantum channel as Equation (11).

In the above situations PRISM provides a curve of P_{det} noted $P_{det}ch(i)Eve(i)$. The curves $P_{det}ch(i)Eve(i)$, for $i = 0, 1, 2$ are illustrated in **Figure 2**.

In the above figure we mark that

1) When the quantum channel is ideal and the rate of attack is weak the probability of detection of eavesdropper increases as we increase the number of photons,

2) When the quantum channel is little noisy and the rate of attack is medium the probability of detection of eavesdropper increases more rapidly as we increase the number of photons,

3) When the quantum channel is very noisy and the rate of attack is strong the probability of detection of eavesdropper increases even more rapidly as we increase the number of photons.

5. Conclusions

As the need of Quantum cryptography is raised, it is very much necessary to test and analyze such systems with more effort. In this article we chose a model-based technique for security analysis of the most widely used protocol

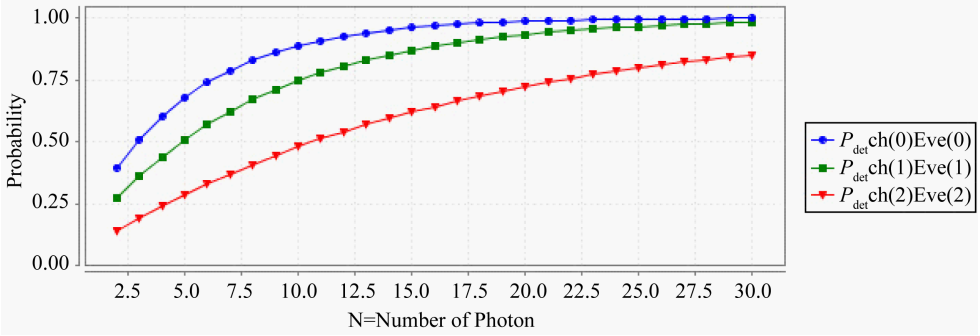

Figure 2. The probability $\{P_{det}\ \mathrm{ch}(i);\ i = 0, 1, 2\}$ to detect Eve where the no of photons transmitted by Alice.

BB84. We are interested in studying the property of eavesdropper. By using the PRISM tool, we get the following four results:

First, if we want to increase the probability of the detection of eavesdropper, it is necessary to increase the number of transmitted photons.

Second, in the case when the quantum channel becomes noisy then the probability of detecting the eavesdropper increases too.

Third, when the power of Eve becomes much stronger, the probability of her detection is higher.

Fourth, when comparing the results of the graph in **Figure 2** with the [9] I can see that if the source of entangled photon pairs photons, the system has the probability to detect the eavesdropper higher.

So, from the above results, we have seen a trend of security quantum key distribution protocols, and have detected the eavesdropper is highly effective, according to the theory. And, when we change the source photons, they are entangled photon pairs. It showed that the rate of detecting Eve was with even higher rates. This article is just presenting the analysis, model checking techniques for protocol EEBB84 (the source of photons with entangled photon pairs). And we hope that the information in this article is a guide to the application of this technique to analyze other quantum protocols and so on.

References

[1] Bennett, C.H. and Brassard, G. (1984) Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, 10-12 dEcember 1984, 175-179.

[2] Gerard, J.H. (1997) The Model Checker SPIN. *IEEE Transactions on Software Engineering*, **23**, 279-295.

[3] prismmodelchecker. http://www.prismmodelchecker.org/

[4] Elboukhari, M., Azizi, M. and Azizi, A. (2009) Implementation of Secure Key Distribution Based on Quantum Cryptography. *Proceedings of IEEE International Conference on Multimedia Computing and Systems* (*ICMCS*'09), Ouarzazate, 2-4 April 2009, 361-365.

[5] Elboukhari, M., Azizi, M. and Azizi, A. (2010) Analysis of Quantum Cryptography Protocols by Model Checking. *IJUCS*, **1**, 34-40.

[6] Elboukhari, M., Azizi, M. and Azizi, A. (2010) Analysis of the Security of BB84 by Model Checking. *International Journal of Network Security & Its Applications* (*IJNSA*), **2**, 87-97.

[7] Papanikolaou, N.K. (2004) Techniques for Design and Validation of Quantum Protocols. University of Warwick, Coventry.

[8] Siddiqui, M.A. and Qureshi, T. (2014) Quantum Key Distribution with Qubit Pairs. *Journal of Quantum Information Science*, **4**, 129-132. http://dx.doi.org/10.4236/jqis.2014.43014

[9] Sahoo, J.R. and Satapathy, S. (2011) Simulation and Analysis of BB84 Protocol by Model Checking. *International Journal of Engineering Science and Technology*, **3**, 5695.