VERIFICATION OF QUANTUM CRYPTOGRAPHY PROTOCOLS BY MODEL CHECKING

Mohamed Elboukhari[1], Mostafa Azizi[2] and Abdelmalek Azizi[1,3]

[1]dept. Mathematics & Computer Science, FSO, University Mohamed I[st], Morocco
[2] dept. Applied Engineering, ESTO, University Mohamed I[st], Oujda, Morocco
elboukharimohamed@gmail.com , azizi.mos@gmail.com
[3]Academy Hassan II of Sciences & Technology, Rabat, Morocco
abdelmalekazizi@yahoo.fr

ABSTRACT

Unlike classical cryptography which is based on mathematical functions, Quantum Cryptography or Quantum Key Distribution (QKD) exploits the laws of quantum physics to offer unconditionally secure communication. The progress of research in this field allows the anticipation of QKD to be available outside of laboratories within the next few years and efforts are made to improve the performance and reliability of the implemented technologies. But despite this big progress, several challenges remain. For example the task of how to test the devices of QKD did not yet receive enough attention. These apparatuses become heterogeneous, complex and so demand a big verification effort. In this paper we propose to study quantum cryptography protocols by applying the technique of probabilistic model checking. Using PRISM tool, we analyze the security of BB84 protocol and we are focused on the specific security property of eavesdropper's information gain on the key derived from the implementation of this protocol. We show that this property is affected by the parameters of the eavesdropper's power and the quantum channel.

KEYWORDS

Quantum Cryptography, Model Checking, BB84 Protocol, Verification

1. INTRODUCTION

Classical cryptography algorithms are based on mathematical functions. The robustness of a given cryptosystem is based essentially on the secrecy of its private key and the difficulty with which the inverse of its one-way functions can be computed. The problem is that there is no mathematical proof that will establish whether it is not possible to find the inverse of a given one-way function. On the contrary, Quantum Cryptography is a method for sharing secret keys, whose security can be formally demonstrated.

Quantum Cryptography uses the laws of quantum physics in order to carry out a cryptographic task. At first, the idea of Quantum Cryptography did not attract much attention but research efforts have increased since the 1990s when it was proved that quantum computers could break the public-key cryptosystems commonly used in modern cryptography. A more interest also has been generated after the first practical demonstration over 30 cm of free space employing polarization coding [1]. Various experimental and theoretical studies have been undertaken, and prototype products are now commercially available.

The security of Quantum Cryptography or Quantum Key Distribution (QKD) protocols is guaranteed by the laws of quantum physics. The BB84 protocol is the first quantum cryptography protocol, which was proposed by Bennett and Brassard in 1984 [1]. The security proof of this protocol against arbitrary eavesdropping strategies was first proved by Mayers [2], and a simple proof was later shown by Shor and Preskill [3].

DOI : 10.5121/ijnsa.2010.2404

In general, the mathematical proof of security of quantum cryptography protocols is not enough to assure that the implementation of a system related to certain quantum cryptography protocol is secure. As shown in traditional cryptography, during the progress from an ideal protocol to an implementation, several flaws of security can appear. So, even extensive research has been initiated for sophisticated implementation of Quantum Cryptography in practical communication networks, these systems are difficult to design; for that it is very important to analyze and verify such systems with more details related to their practical implementation.

Through our article we provide an analysis using PRISM [4], a tool of the technique of probabilistic model checking, to analyze certain security property of the BB84 protocol. Our work is done in the same manner as [5]-[6]-[7]-[8], but our effort is focused on the property of obtaining information on the key by the eavesdropper. The key is generated by the BB84 protocol. We introduce the parameters of quantum channel's efficiency and the parameter of the eavesdropper's power to show that these parameters affect the amount of information obtained by the eavesdropper.

Our paper is organized as follows. In section 2, the related works is introduced. In Section 3 we present a detailed description of the BB84 protocol. We give a simple presentation of the technique of model checking in Section 4 and we show also why this technique is desired to analyze quantum cryptography protocols. In section 5 we describe our analysis of BB84's security by introducing parameters of the channel and the eavesdropper in order to study the property of the information on the key owned by the eavesdropper. We conclude our work by giving the main results in section 6.

2. DESCRIPTION OF RELATED WORKS

The issue of analyzing quantum protocols by model checking is already introduced in the literature. More specially, using the approach of model checking for studying quantum cryptography protocols has been also introduced.

The authors Rajagopal Nagarajan and Simon Gay in the article [9] propose to analyze quantum protocols by the techniques of formal verification which was applied and developed in classical computing for the analysis of communicating concurrent systems. The first step in formal verification is to define a model of the system to be analyzed, in a well-founded mathematical notation and based on the same underlying theory, an automated analysis tool is used to reason about the system.

In their article [10], the authors Rajagopal Nagarajan, Simon Gay and Nikolaos Papanikolaou introduce fundamental and general techniques for formal verification of quantum protocols. Knowing that current analyses of quantum protocols use a traditional mathematical approach and require considerable understanding of the underlying physics, the authors argue that automated verification techniques present an elegant alternative. To show the feasibility of these techniques, they use PRISM, a probabilistic model-checking tool. For the automated analysis of quantum information protocols the authors establish model-checking techniques in the articles [11]-[12]. Precisely they have introduced QMC, a model-checking tool for quantum protocols. As opposed to simulation systems, QMC is proposed as the first dedicated verification tool for quantum protocols. QMC enables the verification and modeling of properties of quantum protocols expressible in the quantum formalism.

In the article [13] the authors Rajagopal Nagarajan, Nikolaos Papanikolaou, Garry Bowen and Simon Gay introduce the use of computer–aided verification as a practical means for analyzing the QKD protocol BB84. Using the probabilistic model–checking approach, they have used the PRISM model–checker to show that, the equivocation of the eavesdropper with respect to the channel decreases exponentially as the number of qubits transmitted in BB84 is increased. They

showed also that the probability of detecting the presence of an eavesdropper increases exponentially as the number of qubits increases.

The authors Mohamed Elboukhari, Mostafa Azizi, and Abdelmalek Azizi in the article [6] describe a methodology based on model checking in order to analyze quantum information systems. They are interested in the QKD protocol B92. By using the PRISM tool as a probabilistic model checker, they show that the protocol B92 fulfilled specific security properties. The authors in the article [8] use the same technique to analyze certain security's properties of B92 protocol; they are interested in the specific security property of eavesdropping detection. They have demonstrated that this property is affected by the power of eavesdropper and the parameters of quantum channel. The same study has been done by the authors to the BB84 protocol [7].

3. PROTOCOL OF QUANTUM CRYPTOGRAPHY: BB84

Quantum Key Distribution has a unique and important properly; it is the ability of the two communicating users (traditionally referred to as Alice and Bob) to detect the presence of any third party (referred to as Eve) trying to gain some information of the key. Eve trying to eavesdrop on the key must in some way measure it, thus introducing detectable anomalies. By using quantum entanglement or quantum superpositions and transmitting information in quantum states over a quantum channel (such as an optical fiber or free air), a communication system can be implemented which detects eavesdropping.

BB84 protocol is surely the most famous and most realized quantum cryptography protocol. This protocol uses the transmission of single polarized photons. The polarizations of the photons are four states, and are grouped together in two different non orthogonal basis.

Generally the two non orthogonal basis are:
-base $\oplus$ of the horizontal (0°) and vertical polarization (+90°), and we represent the base states with the intuitive notation: $|0\rangle$ and $|1\rangle$. We have $\oplus = \{|0\rangle, |1\rangle\}$.

-base $\otimes$ of the diagonal polarizations (+45°) and (+135°). The two different base states are $|+\rangle$ and $|-\rangle$ with $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. We have $\otimes = \{|+\rangle, |-\rangle\}$.

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

Table 1. Information bit and the basis in the BB84 protocol.

Bit	$\oplus$	$\otimes$
0	$\|0\rangle = a_{00}$	$\|+\rangle = a_{10}$
1	$\|1\rangle = a_{01}$	$\|-\rangle = a_{11}$

The BB84 can be introduced as follows [17]:

1) Quantum Transmissions (First Phase)

a) Alice selects a random string of bits $d \in \{0,1\}^n$, and a random string of bases $b \in \{\oplus, \otimes\}^n$, where $n > N$ (N is the length of the final key).

b) Alice prepares a photon in quantum state a_{ij} for each bit d_j 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 $\oplus$ or $\otimes$ selected 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) Over the classical channel Alice sends the value of b_i to Bob.

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

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

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

In step 2b), Alice and Bob perform a test for eavesdropping. If 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 a noise in the quantum channel. By need of security, we suppose all disturbances are caused by Eve.

4. MODEL CHECKING AND QUANTUM CRYPTOGRAPHY PROTOCOLS

More time and effort are spent on verification than on construction in design of complex systems in software and hardware. The techniques are sought to reduce and ease the verification efforts while increasing their coverage. In this spirit, formal verification is the act of proving or disproving the correctness of intended algorithms underlying a system with respect to a certain formal specification or property, using formal methods of mathematics. The technique of model checking is an approach of formal verification. It is a verification technique that explores all possible system states in a brute-force manner. In the field of computer science, model checking refers to the following problem: Given a model of a system, test automatically whether this model meets a given specification. By using a specialized software tool (called a model–checker), a system implementor can mechanically prove that the system satisfies a certain set of requirements.

We meet in the literature several Proofs of unconditional security of the BB84 protocol [2]-[3], but as Gottesman and Lo [18] point out that "the proof of security of QKD is a fine theoretical result, but it does not mean that a real QKD system would be secure". So, more flexible approach to analyzing the security of quantum cryptographic protocols is clearly desirable. Thus, in practice a component of a system may be quantum, but others could still be classical. So, manufacturers of commercial quantum cryptographic systems [19], require efficient and rigorous methods for design and testing.

In our paper we propose to analyze the security of BB84 protocol by model checking. To realize this, first we build an abstract model, noted M and we express it in a description language. Next, we describe the desired behavior of the system in a set of temporal formulae p_i. Both the model and the formulae are the input of the model–checker.

If the systems have a probabilistic behavior, a variation of this technique is used; a probabilistic model–checker, such as PRISM [20]. PRISM models are illustrated by probabilistic transition

systems. The properties for PRISM models are written in Probabilistic Computation Tree Logic (PCTL).

We verify in PRISM if the model M satisfy the property defined by p_i (i.e. whether for each property p_i M ‘ p_i), and PRISM computes the followig probability:

$$P_r\{M \text{ ‘ } p_i\} \tag{1}$$

We can also, parameterize the model M by writing $M = M(x_1, x_2, x_3, \ldots, x_n)$ and the probability (1) can be calculated for different value of x_i , this enables us to have a meaningful plot of the variation of (1).

A model in PRISM is formed by components called modules. Each module has a sequence of actions to be achieved and also its own local variables. The actions take the form:

$$[action] \rightarrow a_1 : (\text{var}_1 = value_1) + a_2 : (\text{var}_2 = value_2) + \ldots\ldots + a_n : (\text{var}_n = value_n) \tag{2}$$

The variable var_i in this equation is assigned by $value_i$ with probability a_i ($\sum_{i=1}^{i=n} a_i = 1$). If $n = 1$ we have the notation: $a_1 : (\text{var}_1 = value_1) = (\text{var}_1 = value_1)$ with $a_1 = 1$. PRISM permits us to specify arbitrarily probabilities for actions, for example in case $n = 2$ we can model a tendency in BB84 protocol of Alice in the choice of the quantum states by a module containing the following action:

$$[EtatOfAlice]\, true \rightarrow 0.8 : (EtatAlice = |1\rangle) + 0.2 : (EtatAlice = |0\rangle); \tag{3}$$

In this equation, Alice is biased towards choosing the state $|1\rangle$ to encode the data 1 according to the Table 1.

5. VERIFICATION OF BB84 USING THE MODEL CHECKER PRISM

5.1 The Model BB84 in PRISM Tool

Classical model checkers input a description of a model, represented as a state transition system, and a specification, typically a formula in some temporal logic, and return “yes” or “no”, indicating whether or not the model satisfies the specification. When using a probabilistic model checking, the models are probabilistic, in the sense that they encode the probability of making a transition between states instead of simply the existence of such a transition, and analysis normally entails calculation of the actual likelihoods through appropriate numerical or analytical methods.

To begin our verification, we have elaborated a model of BB84 in PRISM noted M_{BB84}. It is done within a file including modules that represent the components of the system. So, in M_{BB84}, there is a module corresponding to each party involved in the protocol (Alice, Bob and Eve), plus a module representing the quantum channel.

In our work, we are interested to the important security’s property that the protocol must ensure: an enemy could never be able to obtain the value of the key. Even if an enemy succeeds to obtain a certain quantity of information by trying to monitor the classical channel, this quantity has to be minimal.

By using our model of BB84, we can calculate the probability:

$$P_r\{M_{BB84} \text{ ‘ } p_{data}\} \tag{4}$$

Here p_{data} represents a formula PCTL, its Boolean value is $TRUE$ if the enemy obtataind the information data on the key. Let n is the number of photons transmitted by Alice to Bob. So, we can vary n and in our PRISM model this probability is a function of n . We write the probability that Eve gain the knowledge of data on the key as:

$$P_{data}(n) = P_r\{M_{BB84} \text{ ‘ } p_{data}\} \tag{5}$$

In our paper, we will analyse the correct measurements that Eve does when she intercepts the photons transmitted by Alice. Let β_i denote the event in which Eve makes a correct measurement to the i-th photons transmitted. Eve is able to obtain the secret key if she measures all photons correctly, this event occurs with the probability:

$$P_{all} = \prod_{i=1}^{i=n} P_r(\beta_i) \tag{6}$$

We want to examine a variation of a probability proportionel to P_{all} noted $P_{>\frac{1}{2}}$ when Eve measures more than half the photon transmitted. This property is noted as $\phi_{>\frac{1}{2}}$ .we will study the variation of the probability:

$$P_{>\frac{1}{2}}(n) = P_r\{M_{BB84} \text{ ‘ } \phi_{>\frac{1}{2}}\} \tag{7}$$

The PRISM tool calculates exactly the probability that Eve measures correctly more than half the photons sent by Alice to Bob. We give in the next paragraph the definition of $\phi_{>\frac{1}{2}}$ according to our model of BB84.

5.2 The expression o f $\phi_{>\frac{1}{2}}$

Eve in our model M_{BB84} performs the “intercept-resend” attack; Eve receives each photon on the quantum channel, measures it with her basis denoted $b_i^{"}$, obtaining a bit value $d_i^{"}$, and then transmits to Bob a new photon, representing $d_i^{"}$ in the $b_i^{"}$ basis. Eve must make a random choice of basis, denoted $b_i^{"}$, which may or may not match Alice’s original choice, b_i . If $b_i^{"} = b_i$, Eve is sure that she measured the i-th photon correctly; otherwise, quantum theory predicts that her measurement result will be correct with the probability of $1/2$.

Our PRISM model M_{BB84} has a module called Eve includes a variable nc by which we calculate the number of time that Eve makes a correct measurement. nc is shown in our M_{BB84} by the code lines with LUCKY=0.5:

```
[evemeasure] (eve_state=1)&(eve_bas=ch_bas)&(nc<n) → (eve_state'=2)&(eve_bit'=ch_bit)&(nc'=nc+1);
[evemeasure] (eve_state=1)&(eve_bas!=ch_bas)&(nc<n) → LUCKY : (eve_state'=2)&(eve_bit'=ch_bit)&(nc'=nc+1)
                                                    +(1-LUCKY) : (eve_state'=2)&(eve_bit'= 1-ch_bit);   (8)
```

In lines (8), eve_state, eve_bas and eve_bit denotes state, base and bit of Eve and ch_bas and ch_bit represent base and bit of the quantum channel.

The fomulae of $\phi_{>\frac{1}{2}}$ can be written in terms of nc as:

$$\phi_{>\frac{1}{2}} = \{ TRUE \cup (nc > \frac{n}{2}) \} \tag{9}$$

5.3 Influence of Quantum Channel's Efficiency on the Eve's Obtained Information on the Key

In our model BB84 the quantum channel is written in a module called *Quantum Channel*. In practice, quantum channel can be an optical fiber or free air. In this section, we present a simulation of the influence of the channel's efficiency on the information gain of Eve on the key. This is done by elaborating three curves: curve when the quantum channel is perfect and if it is noisy and if it produces a lot of noise. We expect if the channel becomes very noisy the amount of information obtained by Eve on the key decreases. We consider in this paragraph that Eve is powerful; Eve intercepts all photons sent by Alice to Bob.

There is no noise in the perfect quantum channel, we model this in the module *Quantum Channel* by the line:

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

Here, ch_state represets the state of the quantum channel and al_bas and al_bit denote base and bit of Alice. The line (10) shows that the information sent by Alice (base and bit) remain unchanged before it received by Eve.

For $1 \le n \le 60$, PRISM calculates $P_{>\frac{1}{2}}(n)$ which described in 5.1) this produces the curve of $P_{>\frac{1}{2}}$ (noted $P^{Ch(2)}_{>\frac{1}{2}}$) as illustrated in Fig. 1.

To draw a curve of $P_{>\frac{1}{2}}$ (noted $P^{Ch(1)}_{>\frac{1}{2}}$) where there is a bit noise in the channel; we change the line (10) by the following code lines:

$$\begin{aligned} [aliceput](ch\_state = 0) \rightarrow\ & c0 : (ch\_state' = 1) \,\&\, (ch\_bas' = al\_bas) \,\&\, (ch\_bit' = al\_bit) \\ & + c1 : (ch\_state' = 1) \,\&\, (ch\_bas' = 1 - al\_bas) \,\&\, (ch\_bit' = al\_bit) \\ & + c2 : (ch\_state' = 1) \,\&\, (ch\_bas' = al\_bas) \,\&\, (ch\_bit' = 1 - al\_bit) \\ & + c3 : (ch\_state' = 1) \,\&\, (ch\_bas' = 1 - al\_bas) \,\&\, (ch\_bit' = 1 - al\_bit); \end{aligned} \tag{11}$$

We give the values to the number c0, c1, c2 and c3 as: c0=0.7, c1=c2=c3=0.1. We remark from these lines that the information of Alice has been changed in little way. if we modify these lines by giving new values like c0=0.4, c1=c2=c3=0.2 we simulate a channel very noisy. This permits us to elaborate a curve of $P_{>\frac{1}{2}}$ (noted $P^{Ch(0)}_{>\frac{1}{2}}$). All curves $(P^{Ch(i)}_{>\frac{1}{2}})_{0 \le i \le 2}$ are shown in Fig. 1.

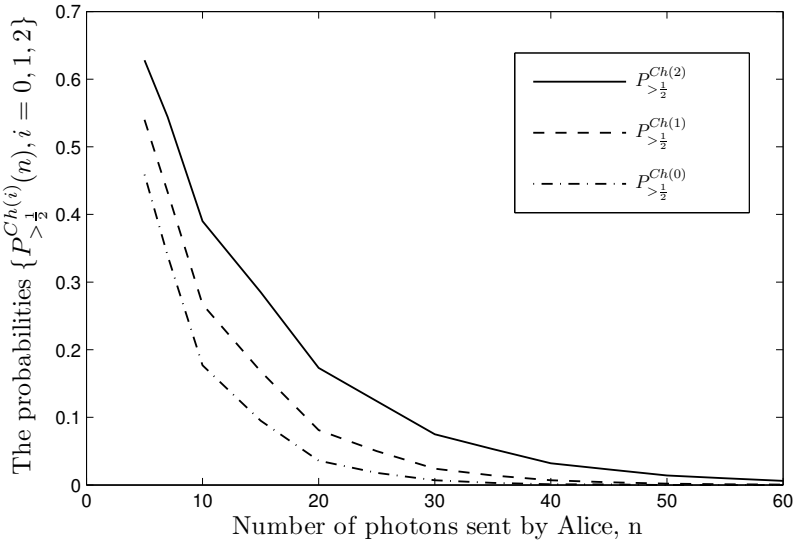

Figure 1. The probabilities $\{P_{>\frac{1}{2}}^{Ch(i)}(n), i = 0, 1, 2\}$ that Eve measures more than half the photons transmitted by Alice to Bob when we change the canal's efficency.

We note from these curves, that if we increase the number of photons emitted by Alice (n), the probability that Eve measures more than half the photons decreases and tends towards 0 and we note $\lim_{n\to\infty} P_{>\frac{1}{2}}^{Ch(i)}(n) = 0$ for $0 \le i \le 2$. Also, as the channel becomes noisy the probability that the amount of information on the key owned by Eve becomes smaller as expected and we have the following inequality for $5 \le n \le 60$:

$$P_{>\frac{1}{2}}^{Ch(0)}(n) \le P_{>\frac{1}{2}}^{Ch(1)}(n) \le P_{>\frac{1}{2}}^{Ch(2)}(n) \quad (12)$$

5.4 Influence of Eve's Power on the Information Obtained on the Key

We want to simulate as in paragraph 5.3) the influence of the power of Eve on its information obtained on the key. We expect that if the power is lower, the information which gained by Eve on the key is lower too. We suppose in this paragraph that the quantum channel is perfect.

The curve $P_{>\frac{1}{2}}$ (noted also $P_{>\frac{1}{2}}^{Eve(2)}$) represents the function $n \to P_{>\frac{1}{2}}(n)$ if Eve is powerful; Eve performs the intercept-resend attack to all photons emitted by Alice to Bob. So, Eve measures all photons. This appears firstly in the previous lines (8) and in the following line included in the module *Quantum Channel*:

[eveput] (ch_state=2) -> (ch_state'=3)&(ch_bas'=eve_bas)&(ch_bit'=eve_bit); (13)

Now, we modify the lines (8) by the following with $d1 = 0.7$ and $d2 = 0.3$:

[evemeasure] (eve_state=1)&(eve_bas=ch_bas)&(nc<n) → d1:(eve_state'=2)&(eve_bit'=ch_bit)&(nc'=nc+1)+
d2:(eve_state'=2)&(eve_bit'=ch_bit)&(nc'=nc) ; (14)
[evemeasure] (eve_state=1)&(eve_bas!=ch_bas)&(nc<n) → LUCKY*d1 : (eve_state'=2)&(eve_bit'=ch_bit)&(nc'=nc+1)+
LUCKY*d2 : (eve_state'=2)&(eve_bas'=ch_bas)&(eve_bit'=ch_bit)&(nc'=nc)+
(1-LUCKY)*d1 : (eve_state'=2)&(eve_bit'= 1-ch_bit)+
(1-LUCKY)*d2 : (eve_state'=2)&(eve_bas'=ch_bas)&(eve_bit'=ch_bit);

Here, the lines (14) in which appears the number d2 Eve doesn't measure the photon intercepted, so she doesn't alter its state (base and bit). So the lines (14) and (13) model a weak attack of Eve because for several photons Eve doesn't measure. By varying n in the interval [5, 60], we realise the curve $P_{>\frac{1}{2}}$; we note it by $P^{Eve(1)}_{>\frac{1}{2}}$.

When Eve measures a lot of photons, we simulate a medium attack of Eve; this is done by changing the number d1 and d2 in the lines (13) as $d1 = 0.4$ and $d2 = 0.6$. So, the new form of lines (14) and the line (13) illustrate a medium attack.

In this case PRISM provides a curve of $P_{>\frac{1}{2}}$ noted $P^{Eve(0)}_{>\frac{1}{2}}$. The curves $(P^{Eve(i)}_{>\frac{1}{2}})_{0\le i\le 2}$ are shown in Fig. 2.

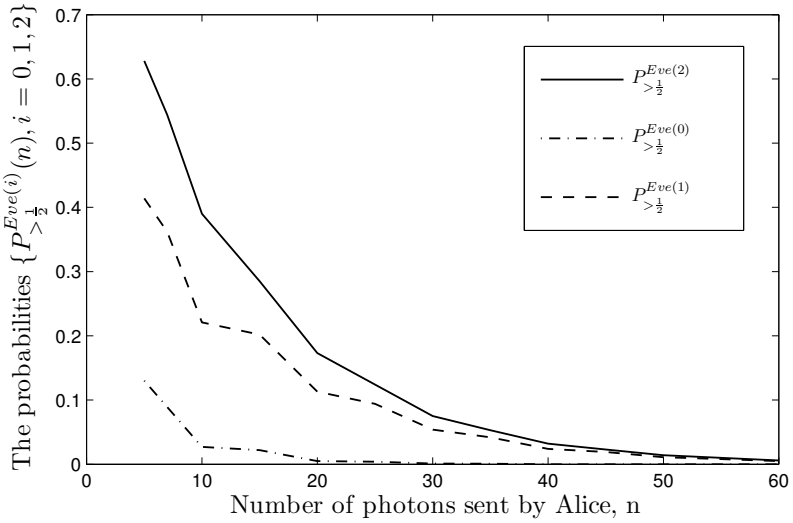

Figure 2. The probabilities $\{P^{Eve(i)}_{>\frac{1}{2}}(n), i = 0, 1, 2\}$ that Eve measures more than half the photons transmitted by Alice to Bob when we change the Eve's power.

We remark from this figure if we increase n, the number of photons transmitted by Alice, the probability that Eve measures more than half the photons correctly decreases too and we have $\lim_{n\to+\infty} P^{Eve(i)}_{>\frac{1}{2}}(n) = 0$, $i = 0, 1, 2$.

More interesting, if the power of Eve become lower, the probability that Eve measures correctly more than half the photons becomes smaller. This is clearly illustrated by the inequality for $5 \le n \le 60$:

$$P^{Eve(0)}_{>\frac{1}{2}}(n) \le P^{Eve(1)}_{>\frac{1}{2}}(n) \le P^{Eve(2)}_{>\frac{1}{2}}(n) \quad (15)$$

6. Conclusion

Classical cryptography such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. Unfortunately all cryptographic techniques will be ineffective if the key distribution mechanism is weak. The security of these actual mechanisms of key distribution mechanism is based on computational complexity and the extraordinary time needed to break the code. Quantum Cryptography is attracting much attention as a solution of the problem of key distribution; QKD offers unconditionally secure communication based on quantum mechanics. And Quantum Cryptography could well be the first application of quantum mechanics at the single quanta level. Now, many experiments have demonstrated that keys can be exchanged over distances of a few tens of kilometers at rates at least of the order of a thousand bits per second and there is no doubt that the technology can be mastered and will find commercial applications.

So, Quantum Cryptography cryptosystems are very promising and the technology is improving more and more to fulfill requirements. But there is a big need of testing and analysis such systems due to their complexity.
In this context, we have applied the technique of model checking to analyze the security of the BB84 protocol. We have concentrated our effort on studying the property of the amount of information on the key obtained by an eavesdropper. Using the model checker PRISM we have obtained the following results:
- To decrease the probability that Eve measures more than half the photons sent by Alice, it is necessary to increase the number of the photons transmitted,
- If the quantum channel is noisy than the probability that Eve obtained some information on the key decreases too,
- If the power of Eve becomes stronger, the probability that Eve measures more than half the photon sent is higher.

In the end, the automatic model checker PRISM enables us to analyze BB84 protocol and this approach is adaptable to other protocol of Quantum Cryptography. Also this approach is adequate to analyze heterogonous cryptographic systems containing quantum and classical components.

REFERENCES

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, New York, Bangalore, India, 1984, pp. 175–179.

[2] D. Mayers, ”Unconditional security in quantum cryptography,” Journal of the ACM, vol. 48, no. 3, pp. 351–406, May 2001.

[3] P. W. Shor and J. Preskill, ”Simple proof of security of the BB84 quantum key distribution protocol,” Phys. Rev. Lett, vol. 85, no. 2, pp. 441–444, July 2000.

[4] D. Parker, G. Norman, and M. Kwiatkowska, “PRISM 2.0 users’ guide,”February 2008. http://www.prismmodelchecker.org/doc/manual.pdf

[5] Nikolaos K. Papanikolaou ”Techniques for Design and Validation of Quantum Protocols”, Coventry, September 2004, University of Warwick.

[6] M. Elboukhari, M. Azizi, A. Azizi, “Security Oriented Analysis of B92 by Model Checking”, in Proc. IEEE Int. Conf. new technology, mobility and security (NTMS), page 454-458, 2008.

[7] Elboukhari, M. Azizi, A. Azizi, “Analysis of the Security of BB84 by Model Checking”, IJNSA, Vol 2, Number 2, pp. 87-98, April 2010. http://airccse.org/journal/nsa/0410ijnsa7.pdf

[8] M. Elboukhari, M. Azizi, A. Azizi, “Analysis of Quantum Cryptography Protocols by Model Checking”, IJUCS, Vol 1, pp. 34-40, 2010. http://www.hypersciences.org/IJUCS/Iss.1-2010/IJUCS-4-1-2010.pdf

[9] R. Nagarajan and S. J. Gay. Formal Verification of Quantum Protocols. arXiv:quant-ph/0203086, March 2002.

[10] S. J. Gay, R. Nagarajan and N. Papanikolaou. Probabilistic Model-Checking of Quantum Protocols. arXiv:quant-ph/0504007, April 2005.

[11] S. J. Gay, N. Papanikolaou and R. Nagarajan. Model-Checking Quantum Protocols. August 2008.

[12] S. J. Gay, N. Papanikolaou and R. Nagarajan. QMC: a model checker for quantum systems. In: Proceedings of the 20th International Conference on Computer Aided Verification (CAV). Springer LNCS series, volume 5123, pages 543-547, 2008.

[13] R. Nagarajan, N. Papanikolaou, G. Bowen and S. J. Gay. An Automated Analysis of the Security of Quantum Key Distribution. arXiv:cs.CR/0502048, February 2005.

[14] S. J. Gay, R. Nagarajan and N. Papanikolaou. Specification and Verification of Quantum Protocols. In: Semantic Techniques in Quantum Computation (S. J. Gay and I. C. Mackie, eds.). Cambridge University Press, 2010.

[15] Nick Papanikolaou, 'Reasoning Formally About Quantum Systems: An Overview', ACM SIGACT News, 36(3), pp. 51-66, 2005.

[16] N. Papanikolaou, 'Model Checking Quantum Protocols', Ph.D. Thesis, Department of Computer Science, University of Warwick, 2009.

[17] M. Elboukhari, M. Azizi, A. Azizi, “Implementation of secure key distribution based on quantum cryptography”, in Proc. IEEE Int. Conf Multimedia Computing and Systems (ICMCS’09), page 361 - 365, 2009.

[18] D. Gottesman and H-K. Lo. From Quantum Cheating to Quantum Security. Physics Today, 53(11),November 2000. quant-ph/0111100.

[19] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “‘Plug and Play’ systems for quantum cryptography,” App. Phys. Lett., vol. 70, no. 7, 1997, see also http://www.idquantique.com.

[20] D. Parker, G. Norman, and M. Kwiatkowska, “PRISM 2.0 users’ guide,” February 2004.