Security Verification of BB84 Protocol Using PRISM Model-Checker

Amir M. Tavala[1], Sorush Nazem[1], and Ali A. Babaei Brojeny[2]

[1] Department of Electrical Engineering, Isfahan University of Tech., Isfahan 84156, Iran [2] Department of Physics, Isfahan University of Tech., Isfahan 84156, Iran

Abstract

The fast developing theory of Quantum Communications describes the Quantum Mechanical based concepts. Considering their classical counterparts for information transmission securely through the Quantum Channel, we have to deal with Quantum Cryptography. Quantum key distribution is the most well-known application of quantum cryptography. While current analysis of quantum protocols use a traditional mathematical approach and require considerable understanding of the underlying physics, a simpler probabilistic model checking is used to some extent which is compatible with classical implementation as an alternative. In this presentation the PRISM model checking tool – by Birmingham group - is employed inasmuch as details to measure the security of the full BB84 protocol when the presence of some additional parameters are taken into account while considering two eavesdropper's attacks

1– Introduction

In this presentation, we study one of the well-known protocols of Quantum Key Distribution using a probabilistic model checker to compare the security in various q-channel conditions. The PRISM tool is the one developed by Birmingham University team. With the aid of some available coding in [1] we apply the channel noise model to the BB84 protocol.

1–1- Quantum Cryptography

Cryptography talks about how two parties can have safe communication with respect to the possible amount of valid information which can be tapped by eavesdropper (Eve). Invented by C. Bennet and G. Brassard in 1982, QKD begins with a radically different premise from the previous Cryptographic theories: we should base security on known physical laws rather than on mathematical complexities of complicated non-proven algorithms. QKD lets two parties—for example, Alice and Bob—agree on secret key which is formed in three steps: raw quantum transmission- which uses both the quantum and public channel simultaneously-,error correction and privacy amplification-that make use of only the public channel-.

1–2- Protocol Security Verification

The detection probability of Eve – which is our model criterion for security – and the ratio of valid tapped to the total transmitted information are two important security criteria which always have to be considered. [2] We want to have a measure of security for a set of particular channel circumstances using a model checker tool. The model checking procedure involves three main steps: (i) system specification, (ii) property specification, (iii) verification. A model checker then employs its built-in algorithms to simulate the possibilities and give the probabilities as the result.

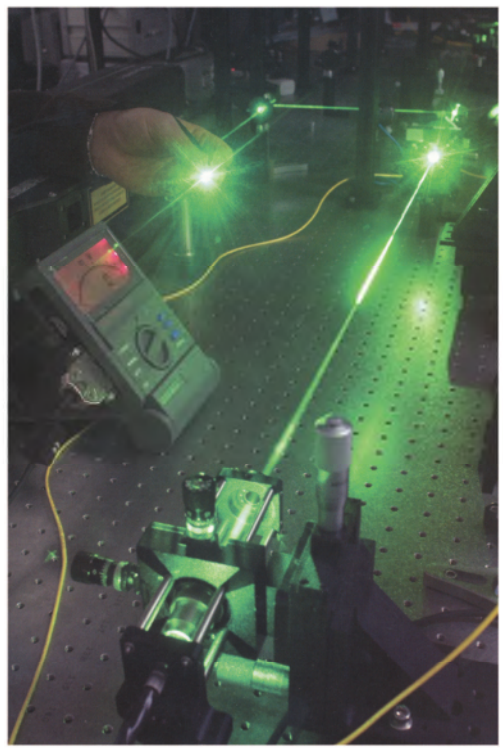

Figure1- A Quantum Cryptography implementation

2 - 1 Software Tools

Nowadays there exist different QPLs (Quantum Programming Language) available. Among them, the PRISM model checker has some advantages especially for BB84 analysis as the protocol developers also used it for this purpose [3]. PRISM uses three probabilistic models. In our program we use DTMC (Discrete Time Marcov Chain) model[4].

2 – 2 Building the Model

The designated model measures $P_{def}(N)$ which means the probability that Eve is tampering in a noisy channel for a transmission of N qbits. First of all, we define $P_E = P_0(N)/N$ for one transmission where [5]:

$$P_0(N) = 1-\exp(-0.134*N) = P_{def}(N)\big|_{np=0}, \quad \text{(noiseless channel)}$$

np is the noise probability. Then we suppose the total noise, either between Alice and Eve or between Eve and Alice, as a single random variable such that bit change occurs with the probability of *np* independent from the presence of Eve. In this method we have considered both possible types of noise: Bit flip and Phase flip. Assuming equal probability in the selection of bases (diagonal and off-diagonal), the presence of bit flip will no longer affect a qbit in the diagonal bases and neither will the phase flip and off-diagonal bases. A clever Eve might try to regenerate a demolished photon and send a copy of her received bit (Intercept-Resend attack) or a random bit (Random Substitution attack). We calculate numerically $P_{def}(N)$ for both circumstances. There exist some other attacks like *Beam Splitting Attack* which we do not investigate them here; as we can usually prevent them by some implementation considerations [6].

3 – Simulation Results

First, we investigate the security measure of the protocol for attacks in comparison with each other in a noiseless channel (Fig. 2)
In plots of $P_{def}(N)$ vs. np for np between 0 and 1, we expect to have the lowest $P_{def}(N)$ for np = 0.5 and the curve should be symmetric, because changing np to 1, the noise probability should not affect the result. Also the relative P_{def} (N) of Random Substitution should be higher than Intercept-Resend attack as the former is obviously more easily detectable than the other. The figures 4 and 3 meet our expectations. As is seen from figures 4 and 3, when noise approaches to 0.5, the probability of detection will decrease and by increasing the number of bits, the probability will increase in both attacks.

The last graph depicts the result for both attacks and for two constants N at the same time which shows the security measures of the attacks relatively. Notice that for a constant N, the P_{def} should be equal for np=0.5. The reason is that at this point the received bit by Bob is completely random, or with the maximum *Entropy* or ambiguity so the result would be independent from the type of attack (Figure 5).

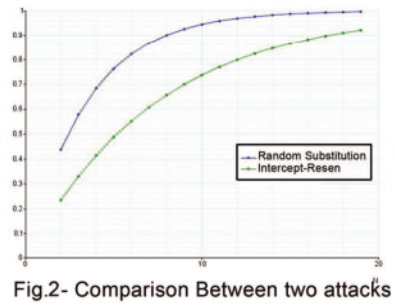

Fig.2- Comparison Between two attacks

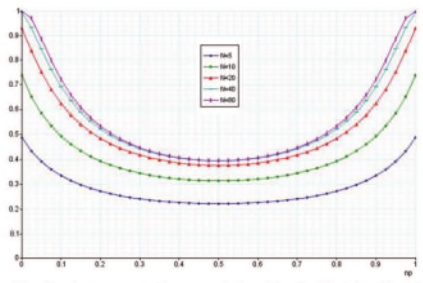

Fig.3- Intecept-Resend for N=5,10,20,40,80

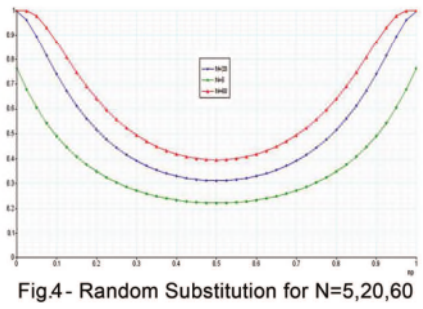

Fig.4- Random Substitution for N=5,20,60

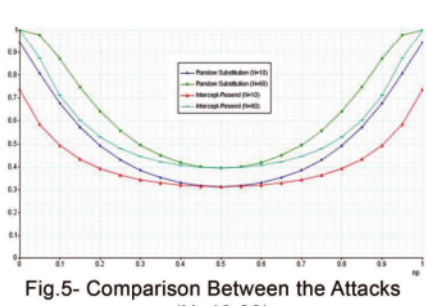

Fig.5- Comparison Between the Attacks (N=10,60)

4 – Summary and Future Direction

This study was dealt with a BB84 analysis including channel noise modeling using a probabilistic computer programming and simulation. A security measure was described and verified in two different attacks. Further studies and simulations can be done to change the probabilistic model of the noise or to investigate other protocols and/or attacks. The results of these investigations will be appeared elsewhere.

The authors would like to thank the Vice-chancellor for Research Affairs of IUT whom this undergraduate study was supported by them.

References

[1] http://www.dcs.warwick.ac.uk/~nikos/ research/01be2d960f0c23302/index.html
[2] Unconditional Security in Quantum Cryptography.
[3] Bennett, C. H., Brassard, G., Breidbart, S. and Wiesner, S., Quantum cryptography, or unforgetable subway tokens, Proceedings of Crypto '82 , August 1982, Plenum Press, pp. 267—275.
[4] PRISM manual – Version 3.1.1.
[5] Nagarajan R., Papanikolaou N., Bowen G., Gay S.,An Automated Analysis of the Security of Quantum Key Distribution.
[6] Quantum Key Distribution Technologies, IEEE Journal of Selected Topics in Quantum Electronics, Vol. 12, No. 4, July/August 2006.