Available online at www.sciencedirect.com
ScienceDirect
Electronic Notes in Theoretical Computer Science
ELSEVIER
Electronic Notes in Theoretical Computer Science 270 (1) (2011) 175–182
www.elsevier.com/locate/entcs

Verification of Quantum Protocols with a Probabilistic Model-Checker

Amir M. Tavala [1,2] Soroosh Nazem[3]

Department of Electrical and Computer Engineering
Isfahan University of Technology
Isfahan 84156-83111, Iran

Ali A. Babaei-Brojeny[4]

Department of Physics
Isfahan University of Technology
Isfahan 84156-83111, Iran

Abstract

Channel modeling is crucial for studying the behavior of quantum channels in order to build an efficient error correction scheme in addition to security verification of different protocols. While most current analyses of quantum protocols use a traditional mathematical approach, we employ a simpler probabilistic model checking which is more compatible with classical implementations to investigate the dependency of the security on the quantum channel noise. We also compare a couple of eavesdropping strategies from the security point of view.

Keywords: Probabilistic modeling, Quantum protocol verification, Quantum key distribution

1 Introduction

The field of quantum information theory has brought the potential to accomplish feats considered impossible by purely classical methods. One of these is the ability to transmit an unconditionally secure message between two parties, known as quantum cryptography. Quantum cryptography is one of the earliest practical results among the various theories which are tied with quantum mechanics and are not yet fulfilled by present technologies.

On the one hand, quantum mechanics postulates put some constraints on all

[1] The authors would like to thank Ms. Farnaz Pirasteh for the help in preparation of the LATEX version.
[2] Email: a.tavala@ec.iut.ac.ir
[3] Email: sorush.nazem@gmail.com
[4] Email: brojeny@cc.iut.ac.ir

doi:10.1016/j.entcs.2011.01.016

logic that governs classical communication. On the other hand, those postulates enhance security beyond computational security. It should be noted that the quantum channel and quantum bits are utilized for transmitting classical bits of the key. The complete communication either involves a classical medium in parallel or the classical data can be sent through the same quantum channel [1].

Quantum key distribution (QKD) establishes a string of random bits shared by two spatially separated parties, say Alice and Bob, in an information-theoretically secure manner [2]. Later, Bob performs a sifting transaction or secret key reconciliation (through the public channel) to discard all cases where he reads the wrong basis.

The BB84 and B92 protocols are among the first and best-known ones which are proved to be unconditionally secure even with some assumptions of imperfections in the channel and devices [3, 4]. There have been several recent methods, some of which are based on teleportation and entanglement, such as the six-state scheme, which have relatively enhanced the security bound and tolerate more errors [12]. There have been numerous theoretical investigations done by computer scientists on channel modeling in QKD protocols, most of which concentrate on the ideal conditions; in the worst case, they model the channel noise equivalent to the eavesdropper (Eve)'s effect. To have a more realistic description of the channel for a particular protocol, one has to consider different tapping schemes, the detection efficiency of measurement devices [9, 10] and statistical parameters of channel imperfections such as noise, damping factor (for dissipating channels), decoherence [7], etc.

In this paper, we have measured the security of the BB84 protocol using a probabilistic modeling approach and built a simple model for channel noise and imperfections which have been verified by PRISM programming. The results are shown to tend to those of the noiseless channel cases and the comparison of different tapping scenarios is consistent with the other works [13]. The rest of the paper is organized as follows: The model of quantum channels is described in section 2. The PRISM model checker, simulation details and experimental results are given in section 3. The paper is concluded in section 4.

2 Building the Model

Model checking is a procedure involving three main steps: (i) constructing an abstract model of a given system (system specification); (ii) defining the properties desired of the system in a form that can be checked automatically (property specification); and (iii) feeding the model into an appropriate software tool (verification, which will be covered in the next section). A model checker then employs its built-in algorithms to simulate the possibilities and give the result in the form of probabilities [8].

Probabilistic simulations are based on different probabilistic models like CTMC, MDP, DTMC, etc. In our experiment, the Discrete Time Markov Chain (DTMC) model is used for security verification of BB84 in a noisy channel. We concentrate

on *Intercept-Resend* attacks as eavesdropper's strategy, but a security comparison with *Random Substitution* attacks is also investigated [8].

In the following subsections, we first briefly introduce the basic concepts of DTMC which are useful for better understanding of the model-checking procedure. Then, we present a simple form of channel noise applied in protocol analysis.

2.1 Discrete Time Markov Chains

A Markov chain is a stochastic process whose state space I is discrete (finite or countably infinite) and such that the probability distributions for its future development depend only on the present state and not on the path (consisting of past states) that was followed to reach this state. If we further assume that the parameter space T is also discrete, then we have a discrete time Markov chain. We can state the Markov property as

$$P(X_n = i_n | X_0 = i_0, X_1 = i_1, ..., X_{n-1} = i_{n-1}) = P(X_n = i_n | X_{n-1} = i_{n-1}) \tag{1}$$

where the X_i's are random variables at time step $i = \{0, 1, 2, ...\}$ and if $X_n = j$, then the state of the system at time step n is j, X_0 being the initial state of the system. So the transition probability of the Markov Chain is given by

$$p_{jk}(m, n) = P(X_n = k | X_m = j), \quad 0 \leq m \leq n \tag{2}$$

and if its value depends only on the difference $n - m$, i.e., the number of steps, then such chains are called homogeneous Markov chains. In such a case:

$$p_{jk}(n) = P(X_{m+n} = k | X_m = j) \tag{3}$$

denotes the n-step transition probabilities. The one step transition probabilities of a DTMC could be specified in the form of a transition probability matrix. The row sums of this square matrix are equal to unity. It plays an important role in the analysis based on DTMC. The n-step transition probabilities can be computed by one form of the Chapman-Kolmogorov equation:

$$p_{ij}(m + n) = \sum_k p_{ik}(m) p_{kj}(n) \tag{4}$$

Let $P(n)$ be the n-step transition probability matrix, then we can write the above equation as:

$$P(n) = P.P(n - 1) = P^n \tag{5}$$

Hence, the one step transition probability matrix could be multiplied $(n - 1)$ times by itself to get the n-step transition probability matrix. Also using the theorem of total probability we have:

$$p_j(n) = P(X_n = j) = \sum_i p_i(0) p_{ij}(n) \tag{6}$$

Hence, the step-dependent probability vector of, denoting by $p(n)$ of Xn at time n could be expressed as

$$p(n) = [p_0(n), p_1(n), ..., p_j(n), ...] = p(0)P^n \tag{7}$$

2.2 Quantum Channel Noise Modeling

There are various noise forms which can be described as a stochastic process by giving the power density, probability distribution, etc. We here consider a simple model which is expressed with a single parameter, say P_N, which represents the probability of flipping the transmitted qubit in its own basis. The protocol security is expected to diminish as the entropy of the received qubit increases which corresponds to greater values of P_N up to $\frac{1}{2}$. We can define this parameter for every part of the channel. In our discussion, the channel has two sections. We assume that all imperfections in the transmitting device of Alice, the quantum channel between Alice and Eve and the receiver device of Eve can be modeled by P_{N1} and the imperfections in Eve's transmitter, the channel between Eve and Bob and Bob's receiver are modeled by P_{N2}.

Although the existence of noise is a desirable fact for the eavesdropper, passive attacks are still unattainable. In other words, Eve cannot hide her modifications completely in the channel noise and her presence is detectable, but with a relatively lower chance. It should be noted that Eve is assumed to have ultimate computational power and unlimited technology for state preparation.

The detection probability of Eve is our model criterion for security [11] which is denoted by P_{det}. This probability is only well-defined when the selected bases by both Alice and Bob are the same, so they are able to check if there is any evidence of tapping. Therefore, we focus on the two cases when the transmitted qubit by Alice and received qubit by Bob are either equal or non-equal, where $P(A = B)$ and $P(A \neq B)$ are the probabilities of each of the mentioned cases and the bases are supposed to be identical. Then, we have:

$$P_{det} = P_{det}|(A = B).P(A = B) + P_{det}|(A \neq B).P(A \neq B) \tag{8}$$

In a noiseless channel, $P(A = B) = 1 - P(A \neq B) = \frac{3}{4}$; For nonzero values of P_{N1} and P_{N2}, this statement is, however, no longer correct. Also, let

$$P_0(N) = [1 - exp(-0.134N)]/N \tag{9}$$

where $P_0(N)$ represents the probability of detection of Eve per qubit in a noiseless channel for an intercept-resend attack [13]. It can be shown that the detection probabilities can be derived as follows:

$P_{det}|(A = B) =$

$$\frac{P_0[P_{N1}(1 - P_{N2}) + P_{N2}(1 - P_{N1})]}{P_0[P_{N1}(1 - P_{N2}) + P_{N2}(1 - P_{N1})] + (1 - P_0)[(1 - P_{N1})(1 - P_{N2}) + P_{N1}P_{N2}]} \quad (10)$$

and
$P_{det}|(A \neq B) =$

$$\frac{P_0[(1 - P_{N1})(1 - P_{N2}) + P_{N1}P_{N2}]}{P_0[(1 - P_{N1})(1 - P_{N2}) + P_{N1}P_{N2}] + (1 - P_0)[P_{N1}(1 - P_{N2}) + P_{N2}(1 - P_{N1})]} \quad (11)$$

It may sound reasonable to think of identical stochastic characteristics in the two mentioned parts of the channel for simplification which means $P_{N1} = P_{N2} = P_N$. Then, if we define:

$$H = 2P_N(1-P_N) \quad (12)$$

which is proportional to the variance of a Bernoulli random variable, peaked at $P_N = \frac{1}{2}$. The above formula can be reduced to:

$$P_{det}|(A = B) = \frac{P_0 H}{(1 - P0)(1 - H) + P_0 H} \quad (13)$$

$$P_{det}|(A \neq B) = \frac{P_0(1 - H)}{P_0(1 - H) + (1 - P_0)H} \quad (14)$$

3 Applying the model in PRISM

3.1 Simulation Details

Because of the random behavior of quantum phenomena, it has been suggested to use an appropriate probabilistic tool for verifying quantum protocols instead of logical model-checkers like SPIN [6, 14]. Among them, PRISM (probabilistic symbolic model-checker) has some advantages especially for BB84 analysis as the protocol developers also used it for this purpose [7]. Papanikolaou proposed an analysis of BB84 for two possible attacks where the channel is considered noiseless and all the device imperfections are neglected [14].

Here, each DTMC state corresponds to a unique event which is possible according to the protocol flowchart and the transition probabilities are determined by our assumptions. For example, it is logical to consider a 50-50 chance for both Bob and Eve to get the correct qubit providing that their measurement basis is not the same as that of the received qubit.

In transmission of a stream of qubits, the security criterion and simulation time

highly depend on the size of the stream or number of transmitted qubits, say N. Larger numbers of qubits provide more security but need more complex systems to be implemented.

3.2 Experimental Results

The following 3 figures show the security criterion for an intercept-resend attack in a noisy channel. They are plotted by exporting the result into MATLAB software. In figure 1, the role of channel noise is illustrated which reduces the curvature of the graph when it goes up. Thus, Eve is more likely to be detected. Note that the noiseless condition is shown at the top of other graphs.

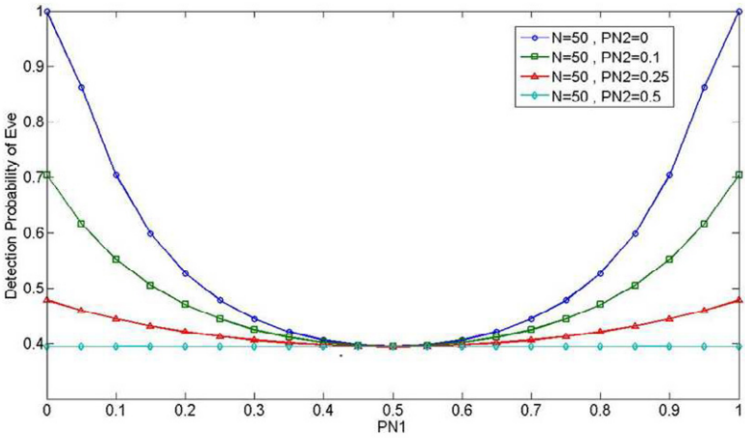

Fig. 1. Security criterion vs. P_{N1} for $N = 50$ for different values of P_{N2}.

Figure 2 depicts the best and worst cases with respect to the presence of noise in the second part of the channel, i.e., between Eve and Bob.

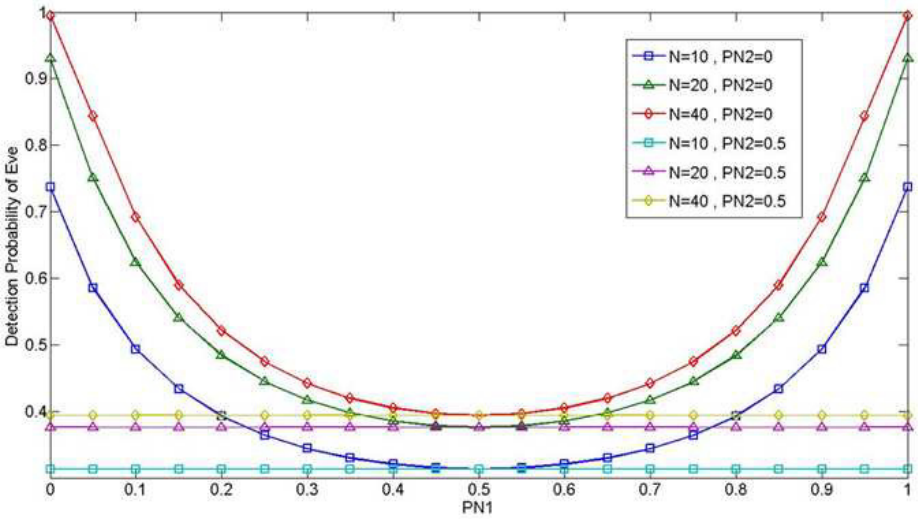

Fig.2. Security vs. P_{N1} for three pairs of graphs
when the second part of the channel is either noiseless or random.

In the next figure we suppose identical statistical conditions for both parts of the channel which means $P_{N1} = P_{N2} = P_N$. It shows the security dependency on the number of transmitted qubits (N) as it was expected.

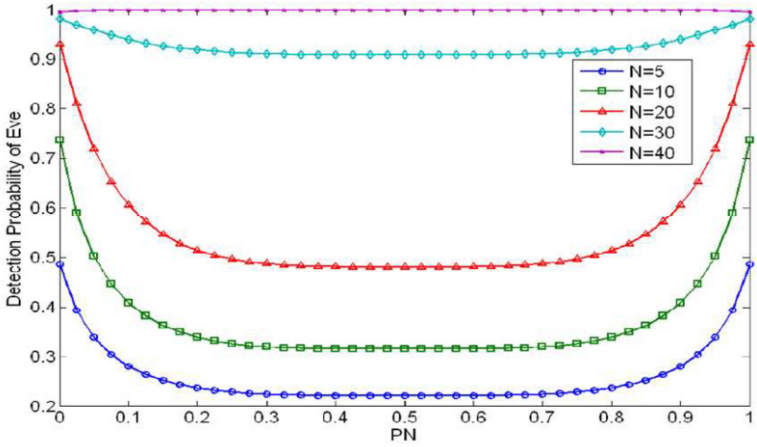

Fig. 3. Security vs. P_N for different values of N

Figure 4 is inserted directly from the PRISM environment and shows that it is not a clever idea for Eve to choose random substitution as the detection probability would be considerably higher. That is why it is preferred not to repeat the previous analysis for random substitution attack [5].

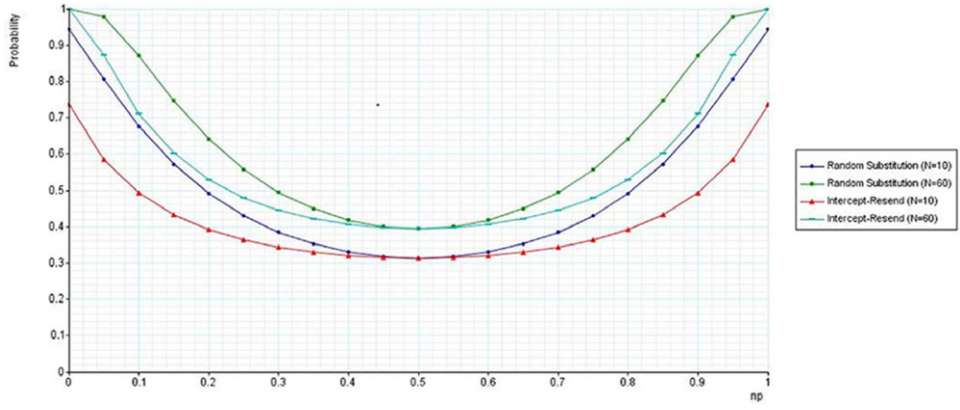

Fig. 4. Security criterion vs. noise probabilities for different numbers of qubit stream lengths (10 and 60) for the two attacks. Note that when the channel behavior is completely random, the security has its minimum value and the corresponding values for both attacks become equal. Again, we have $P_{N1} = P_{N2} = P_N$ (which is denoted by np in here [5]).

4 Conclusion and Future Directions

In this presentation, we employ PRISM for analyzing BB84 with different tapping scenarios which are also focused on in [14]. The outcomes for noiseless and noisy channel are compared and it is shown that it confirms and satisfies the expected results and formula [13]. Further investigations can be done by building a more

complicated model of the noise or considering other imperfection factors. Also, the same verification can be done for other protocols or security criteria.

References

[1] Mitra, A., *Complete Quantum Communication with Security*, (1995), URL: http://arxiv.org/abs/quant-ph/9812087v7.

[2] Dobsi ek, M., J. Kola, and R. Lorencz, *A Theoretic-framework for Quantum Steganography*, Proc. of CTU Workshop (2006), 124–125.

[3] Hupkes, H. J., *Unconditional Security of Practical Quantum Key Distribution*, URL: arXiv:quant-ph/0402170v1.

[4] Tamaki, K. et al., *Unconditional Security of the Bennett 1992 Quantum Key Distribution Protocol over a Lossy and Noisy Channel*, Physical Review A (2004).

[5] Tavala, Amir M., Soroosh Nazem, and Ali A. Babaei-Brojeny, *Security Verification of BB84 Protocol Using PRISM Model-Checker*, Proc. of International Iran Conference on Quantum Information (2007).

[6] Gay, S., R. Nagarajan, and N. Papanikolaou, *Probabilistic Model-Checking of Quantum Protocols*, URL: arXiv: quant-ph/0504007v2 (2005).

[7] Barenco, A., T. A. Brun, R. Schack, and T. P. Spiller, *Effects of noise on quantum error correction algorithms*, URL: arXiv:quant-ph/9612047v1 (1996).

[8] Wu, L., and D. A. Lidar *Overcoming quantum noise in optical fibers*, Physical Review A (2004).

[9] Gottesman, D., Lo, H. K., Lutkenhaus, N., and Preskill, J. *Security of quantum key distribution with imperfect devices*, Proc. of International Symposium on Information Theory (2004).

[10] Guerreau, O. L., F. J. Malassenet, S. W. McLaughlin, and J. M. Merolla, *Quantum Key Distribution without a Single-Photon Source Using a Strong Reference*, IEEE Photonics Technology Letters **178** (2005).

[11] Mayer, D., *Unconditional Security in Quantum Cryptography*, Journal of ACM**483** (2001).

[12] Gottesman, D., and H. K. Lo, *Proof of Security of Quantum Key Distribution With Two-Way Classical Communications*, IEEE Trans. Information Theory **492** (2003).

[13] Nagarajan, R., N. Papanikolaou, G. Bowen, and S. Gay *An Automated Analysis of the Security of Quantum Key Distribution*, URL: arXiv:cs.CR/0502048 v1 (2005).

[14] Papanikolaou, N., *Techniques for design and validation of quantum protocols*, M.Sc. Thesis, URL: http://www.dcs.warwick.ac.uk/ nikos/.