Formal Verification of the Security of a Free-Space Quantum Key Distribution System

Verónica Fernández, María-José García-Martínez, Luis Hernández-Encinas, and Agustín Martín*

Department of Information Processing and Coding
Instituto de Física Aplicada, (IFA-CSIC), Serrano 144, 28006- Madrid, Spain
Phone: +34915618806 (ext. 406), Fax: +34914117651
E-mail: {veronica.fernandez, mariajose.garcia, luis, agustin}@iec.csic.es

***Abstract*— The security of a free-space Quantum Key Distribution (QKD) system is analyzed by using PRISM, a probabilistic model checker. Disturbances and misalignments causing an imperfect channel are considered. The security of the system is formally demonstrated against intercept-resend and random substitution eavesdropping attacks for a particular range of transmitted photons.**

***Index Terms*— Cryptography, formal verification, probabilistic model checking, quantum key distribution.**

I. Introduction

Security protocols are specifications of communication patterns which are intended to let agents share secrets over a public network. They are required to perform correctly even in the presence of malicious intruders who listen to the message exchanges over the network and also manipulate the system (by blocking or forging messages, for instance). Obvious desirable requirements include secrecy and authenticity. The presence of possible intruders imposes the use of symmetric and asymmetric cryptographic primitives to encrypt the communications [1].

Nevertheless, it has been widely acknowledged that even the use of the most perfect cryptographic tools does not always ensure the desired security goals. This could be either for efficiency reasons or because frequent use of certain long-term keys might increase the chance of those keys being broken by means of cryptanalysis.

Secure key agreement where the output key is entirely independent from any input value is offered by Quantum Key Distribution (QKD). Although this technique does not eliminate the need for other cryptographic protocols, such as authentication, it can be used to build systems with new security properties.

The aim of this work is to analyze the security of BB84 protocol [2] against two kinds of eavesdropping attacks (intercept-resend and random substitution attacks) when implemented in an experimental QKD system. We will consider the influence of possible disturbances in the free-space between Alice and Bob, and misalignments in the optics to calculate the probability of detection of the eavesdropper as a function of the number of photons transmitted (or equivalently, the length of the bit sequence generated by Alice).

The rest of the paper is organized as follows. Section II includes some preliminaries and definitions. Section III briefly outlines the BB84 protocol, describes the actual free-space QKD system under development in our labs, and exposes the model checking methodology used to analyze its security. The calculated results are presented and discussed in section IV and, finally, conclusions are derived in section V.

II. Preliminaries

In this section, we include a short explanation about the security of QKD systems and the usefulness of formal methods to verify its security, and a description of the verification software used in this work.

A. Quantum Key Distribution security

QKD protocols provide a way for two parties, a sender, Alice, and a receiver, Bob, to share a key through a quantum communication channel (by means of optical fiber or free-space links), and detect the presence of an eavesdropper, Eve. The first complete protocol for QKD, widely used today, was BB84, which uses two non-orthogonal bases, each one with two orthogonal and linearly polarized states (0º/90º and 45º/–45º, respectively) that encrypt each photon to be transmitted [2]. Later on, a simplified version, the B92 protocol, was also introduced [3].

QKD allows two distant partners to communicate with absolute security. Unlike conventional cryptography, QKD promises perfect, unconditional security based on the fundamental laws of physics, the non-cloning theorem and the uncertainty principle. The security of QKD has been rigorously proven in several papers [4]–[6], given some assumptions as can be the physical security of encoding/decoding devices, a true source of random bits, authenticated classical channel to compare bits, and reliable single photon emitters and detectors.

*Contact Author: Agustín Martín.

Manuscript received March 30, 2011. This work was supported in part by the Ministerio de Ciencia e Innovación (Spain), project no. MTM2008-02194.

Unfortunately, building a practical QKD system that is absolutely secure is a substantial research challenge. The first prototype of a QKD system leaked key information over a side channel (it made different noises depending on the photon polarization) [7], and more sophisticated side channel attacks continue to be proposed against particular implementations of existing systems [8]. Furthermore, experiments can be insecure because QKD systems in real life are generally based on attenuated laser pulses, which occasionally give out more than one photon [9].

Those multi-photon pulses enable powerful eavesdropping attacks including the Beam-Splitting (BS) attack [10], or the Photon Number Splitting (PNS) attack [11], [12]. Information leakage caused by BS attacks can be extinguished by privacy amplification [13]. To counter the PNS attack several schemes have been proposed: The non-orthogonal encoding protocol SARG04 [14], the decoy state method [15], [16], or the differential phase shift QKD [17]. Other device-independent security proofs aim to minimize the security assumptions on physical devices [18]–[20]. Very recently, several methods have been presented to blind or control the detection events in QKD distribution systems that use gated single-photon detectors [21], [22], allowing for attacks eavesdropping the full raw and secret key without increasing the Quantum Bit Error Rate (QBER).

B. Formal methods

Thus, despite the existence of a mathematical proof of the security of a given protocol, it is necessary to verify that the implementation of that protocol in a real system is secure. *Formal methods* allow this task to be developed.

Formal methods provide a mathematical representation of the security functions and the expected behavior of a given protocol or system. The two main aspects of formal methods are the language that is used to formally express the characteristics of the protocol or system (specification language), and the way to proof the correct behavior of the system according to the formal specification (formal verification). The most widely used technique to verify security protocols is *model checking* [23].

The basic idea of model checking security protocols is to build a relatively small model of a system running the protocol of interest together with a general intruder model that interacts with the protocol [24]. The model checking technique explores all possible system states to automatically test whether the system model meets the specification. The automated software tool is called a model checker.

Since quantum phenomena are inherently described by random processes, an entirely appropriate technique for verification of quantum protocols is *probabilistic* model checking [25]. Probabilistic model checking is a formal verification technique for the modeling and analysis of systems that exhibit stochastic behavior. It can be applied to several different types of probabilistic models. The three most commonly used are: Discrete Time Markov Chains (DTMCs), in which time is modeled as discrete steps, and randomness as discrete probabilistic choices; Markov Decision Processes (MDPs), which extend DTMCs with the ability to represent nondeterministic behavior; and Continuous Time Markov Chains (CTMCs) which does not permit nondeterminism but allows specification of real (continuous) time behavior, through the use of exponential distributions [26].

C. PRISM model checker

In this work we use PRISM [27], [28] to verify the security of a free-space QKD system under development in our labs [29]. PRISM is a free and open source probabilistic model checker for formal modeling and analysis of systems which exhibit random or probabilistic behavior. It was initially developed at the University of Birmingham and now at the University of Oxford, and supports the three types of probabilistic models mentioned above, DTMCs, CTMCs, and MDPs, plus extensions of these models with costs and rewards. Models are described using the PRISM language, a simple, state-based language which subsumes several well-known probabilistic temporal logics, including Probabilistic Computational Tree Logic (PCTL), used for specifying properties of DTMCs and MDPs, and Continuous Stochastic Logic (CSL), an extension of PCTL for CTMCs. The model checker provides support for automated analysis of a wide range of quantitative properties of these models, as can be, for example, the calculation of the worst-case probability of a given protocol terminating in error, over all possible initial configurations or the probability that an enemy obtains information data on a key in a QKD protocol as a function of several parameters. It incorporates state-of-the art symbolic data structures and algorithms, based on Binary Decision Diagrams (BDDs) and Multi-Terminal Binary Decision Diagrams (MTBDDs) [30], [31]. It also features discrete-event simulation functionality for generating approximate results to quantitative analysis.

PRISM has been used to analyze systems from a wide range of application domains, including quantum protocols. BB84, assuming a perfect quantum channel, was examined using this method in [32] and [33]. Very recently the security of B92 and BB84 quantum protocols have been analyzed in [34] and [35], respectively, by considering an intercept-resend attack and by calculating the probability that an eavesdropper measures more than half the photons transmitted from Alice to Bob, taking into account the influence of quantum channel efficiency and Eve’s power on the information obtained about the key. Similar approaches are presented in [36] and [37] for a standard man in the middle attack, showing results about the probability to detect the eavesdropper. The same tool has been used in [38] to study the security of BB84 protocol in the same attacking scenarios analyzed in present paper but calculating, for different key lengths, the probability of detection of the eavesdropper as a function of a parameter which represents the probability of flipping the transmitted bit in its own basis. The results of this work predict a lower chance to detect the eavesdropper in a noisy channel.

III. System description and methodology

The aim of this work is to verify the security of BB84 QKD protocol when implemented in a practical system. In this section we first outline the basics of the protocol. Then we describe the experimental setup and the formal models used to simulate it.

A. BB84 protocol description

The basic BB84 protocol consists in a first phase, where quantum transmissions take place over a quantum channel and a second one, where Alice and Bob discuss over a classical channel, assumed public, which may be passively monitored (but not tampered with) by an enemy [2]. QKD uses polarized photons as information carriers. BB84 protocol uses four polarizations for the photons: $|0\rangle, |1\rangle, |+\rangle$, and $|-\rangle$, grouped in two non-orthogonal basis, $\oplus$ for horizontal and vertical polarizations, and $\otimes$, also known as *Hadamard* basis, for diagonal polarizations. The first state of each base corresponds to the 0 classical bit value, while the second one corresponds to the 1.

During the first phase:

a) Alice generates a random string of bits $\boldsymbol{d} \in \{0,1\}^n$, where n is the number of transmitted photons, and a random string of bases $\boldsymbol{b} \in \{\oplus,\otimes\}^n$, with $n > K$, where K is the length of the key.

b) Alice sends, over the quantum channel, a photon to Bob for each bit d_i in $\boldsymbol{d}$. For each photon she randomly selects a basis b_i in $\boldsymbol{b}$ with equal probability so that those photons are codified in one of the four above mentioned polarizations.

c) Bob measures each quantum state received with respect of each one of the orthogonal basis, chosen at random. The choices of bases generate a string $\boldsymbol{b'} \in \{\oplus,\otimes\}^n$ and the measurements generate the string $\boldsymbol{d'} \in \{0,1\}^n$.

During the second phase:

a) For each bit d_i in $\boldsymbol{d}$:

i. Alice sends the value of b_i to Bob over a public classical channel (an asymmetric channel, for example).

ii. Bob responds by stating whether he used the same basis for measurements. If $b_i' \neq b_i$, both d_i and d_i' are discarded.

b) Alice chooses a subset of the remaining bits in $\boldsymbol{d}$ and discloses their values to Bob over the classic channel. If the results of Bob's measurements for any of these bits do not match the values disclosed, eavesdropping is detected and communication is aborted.

c) Once the bits disclosed in previous step are removed, the remaining bits in $\boldsymbol{d}$ form the final secret key.

B. Description of our QKD system

Our experimental free-space QKD setup is currently designed to implement B92 protocol at 1 GHz clock rate, and we are improving the system to also implement BB84 protocol. The transmitter in Alice's module (Fig. 1) is mounted on an aluminium base plate. It has two 850nm channels, used for the transmission of the key, and a 1550nm channel for the synchronizing signal. Those channels are combined by means of two pellicles, and the resulting beam is expanded with an output telescope, formed by lenses L_1 and L_2, so that it produces a 40mm-diameter diffraction limited spot. The expansion of the beam is made to allow a long-distance transmission without large beam divergences.

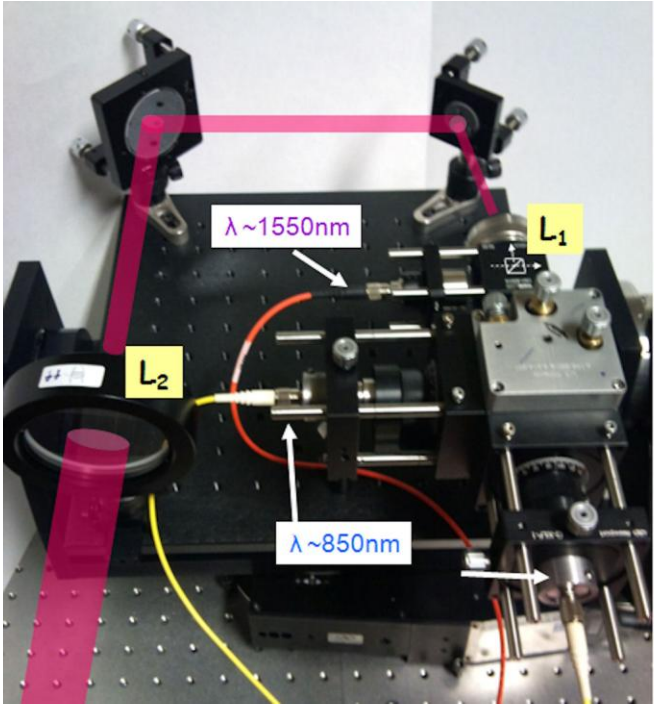

Fig. 1. Current Alice's setup (implementing B92).

The receiver module, Bob, is placed at a distance of 40 m from Alice during the preliminary tests (3 km in the final system is expected) and, therefore, it receives a diverging beam. To efficiently detect the beam a Schmidt-Cassegrain telescope of 25.4 cm diameter, 2.5 m equivalent focal distance and fine-pointing capability is used. Bob's optics has been designed to be coupled to the output of the telescope by using lightweight and compact mounts (see Fig. 2). The output of the telescope is connected to Bob's optics and the outputs of Bob's channels are connected to two single-photon detectors by using optical fiber. The optical synchronization pulse is detected by an avalanche photodiode. The outputs of all three detectors are connected to an electronic card which is able to measure the time of arrival of the photons with high temporal precision. This information is then sent to Alice from which she can infer which key bits have been received by Bob.

Especial care must be paid to one of the most critical parts of the system, the filtering of the solar background radiation. For this purpose, a combination of spectral, spatial, and software filtering are used. The spatial filtering is carried out by optical fiber (Fig. 2). A good compromise of the diameter of this fiber must be found, as small diameters improve the filtering of the solar radiation at the expense of higher signal losses. In addition, if the diameter is too small the signal could be lost due to the beam wandering caused by the fluctuations of the index of refraction of the air.

A non-optimal filtering of the solar radiation can be a typical source of noise. In addition, a not optimal alignment between Alice and Bob, variations in the atmospheric conditions and/or difficulties in the coupling losses can make the channel imperfect, and should be considered in order to formally verify the security of the whole system.

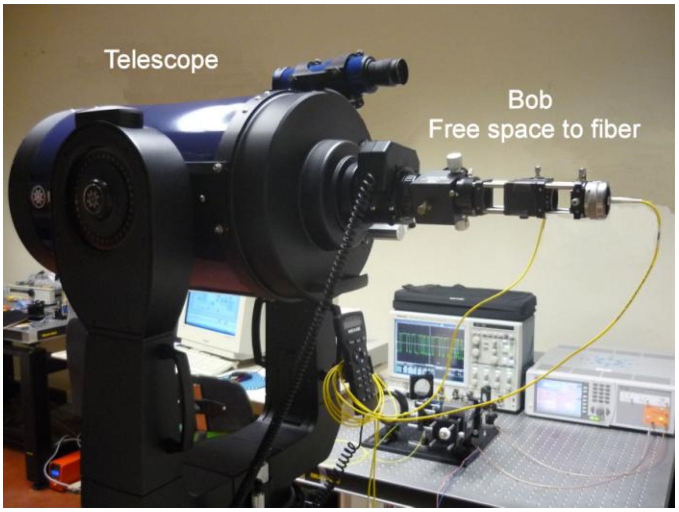

Fig. 2. Bob's optics at the output of the receiver telescope, coupling input beam to optical fiber.

Although Fig. 1 and Fig. 2 show our current experimental setup implementing the B92 protocol, all comments in previous paragraph about sources of noise and imperfections are also valid for the BB84 protocol which will also be implemented as an improvement to our system. For this reason this is the protocol we simulate in this work.

C. Formal models

In order to verify the security of the system described above we have to model it in a description language and express its desired properties by means of a formula written in a given logic. The model and the formula are the input to PRISM, that will compute the probability with which that particular formula is satisfied by the simulated model.

According to the experimental setup and the protocol described previously in subsection *B*, we have simulated the QKD system in PRISM language. The modeling is probabilistic, DTMC, and we have analyzed the probability to detect Eve as a function of the channel efficiency and the number of transmitted photons (which are assumed to be linearly related to the length of the key).

1) System model (M): Four modules have been built to consider Alice, Bob, Eve, and a communication channel which can be imperfect due to disturbances and misalignment losses. All those modules have three local variables, corresponding respectively to the computational state, the basis with respect to which a photon is encoded, and the bit value which is being encoded. A fourth variable is added to Alice module to simulate the transmission of *N* photons (each one encoding a bit value) as the iteration for *N* times of the transmission of a single photon in a given state.

2) Desired property: The presence of an eavesdropper must be detected by the protocol users. If Φ is a formula corresponding to the event that an eavesdropper is detected, the probability of this event in our model *M* is:

$$P_{detection} = \boldsymbol{P_r}\ \{M\ (N{,}P_C)\ \ satisfy\ \ \Phi\}$$

where P_C is the probability that Eve obtains the correct bit value although an incorrect basis is chosen for her measurement, and $\Phi = \boldsymbol{true} \cup Bobstate = V$, V being the value assigned in the program to the state of Bob when Eve is detected.

3) Attacks: Two different attacks are considered: A typical intercept-resend attack [32] and a random substitution attack [33]. In the first one, which is the most widely simulated eavesdropping attack, we have introduced nondeterminism for Alice, Bob and Eve, and we have simulated Bob's behavior so that a comparison is made between his variable of basis and that of the channel before Alice reveals her basis; if both values are different, then the value of the bit variable in Bob module is updated with the value of the bit variable in channel module (0 or 1) with a probability P_C, and with the other bit value (1 or 0) with a probability $1-P_C$. In the same way, Eve's behavior is simulated so that if the value of her variable of basis coincides with that of the channel, she gets the right bit. Otherwise the result she gets is random, as predicted by quantum theory.

In the random substitution attack, the eavesdropper chooses a basis b_i" at random, and also a random data bit d_i"; she substitutes the *i*-th photon (which encodes bit d_i in b_i basis) with a new photon which represents d_i" bit in b_i" basis. In our program, Eve replaces a 0 bit on the channel with a probability defined by a variable called SUBS, and a 1 bit with a probability 1−SUBS. The same probabilities are used to replace channel bases.

IV. Results

We have computed the probability of detection of an eavesdropping while performing the two above mentioned attacks. For each one, we have studied the variation of $P_{detection}$ as a function of the number of transmitted photons. Several calculations have been made, varying the value of P_C (we have considered values from $P_C = 0$ to $P_C = 0.9$ in steps of 0.15), and simulating possible channel inefficiencies by the inclusion of a noise parameter in the channel module.

A. Intercept-resend attack

Fig. 3 shows the probability of detection of an eavesdropper in the BB84 protocol as a function of the number of photons transmitted. The channel is assumed without noise and a comparison is made between the plots obtained for different values of the parameter P_C.

As can be observed, the value of P_C highly influences the probability of detection of the eavesdropper when there is no noise in the channel. In fact, if the number of photons transmitted is greater than 25, the probability of detecting the eavesdropper is higher than 0.9, except if $P_C = 0.9$.

Channel module in PRISM is modified in order to simulate a noisy channel so that the probability of the information sent by Alice (base and bit) remain unchanged before being received by Eve is 40%. Calculations are repeated and results are shown in Fig. 4.

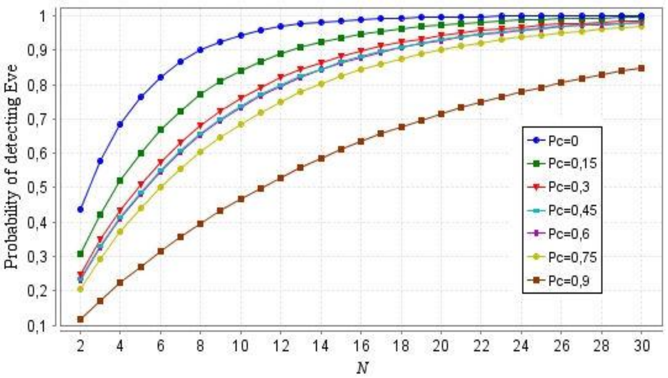

Fig. 3. Probability of detection of Eve as a function of the number of photons emitted for different values of P_C, when a noiseless channel is considered.

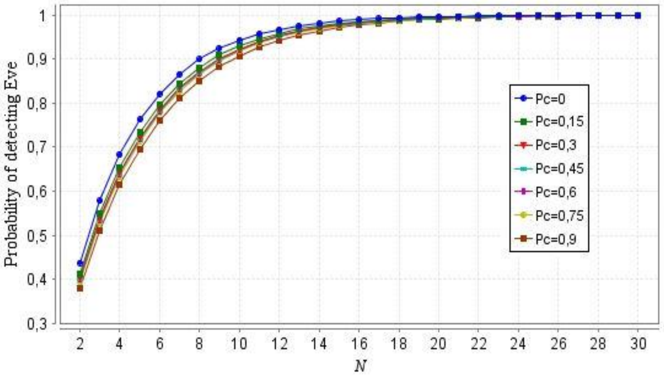

Fig. 4. Probability of detection of Eve as a function of the number of photons emitted for different values of P_C, when a noisy channel is considered.

In this case, i.e., if the channel is noisy, the eavesdropper is detected with a probability higher than 0.9 if only 10 photons are transmitted, for all values of P_C.

A comparison of Fig. 3 and Fig. 4 reveals that in a noisy channel the value of the probability that Eve obtains the correct bit value although an incorrect basis is chosen for her measurement has almost negligible influence in the probability of detection of the attack. Moreover, in the presence of noise the probability of detection of Eve increases. This result is similar to that presented in [37], although it differs from what is concluded in a very recent paper [38].

B. Random substitution attack

As for the previous attack, the probability of detection of Eve as a function of the number of photons transmitted in a channel without noise is shown in Fig. 5 for different values of the P_C parameter.

It can be noted that, in this case, there is almost no difference between the calculated probabilities for different values of P_C. When calculations were repeated considering a noisy channel the values obtained were the same (shown as a wide green line in Fig. 5). In this simulation, if the number of transmitted photons is greater than 10, the probability that Eve is detected is higher than 0.9, for each value of P_C considered.

This result indicates that the random substitution attack produces a high probability of Eve's detection regardless the channel noise (as could be expected, because in this scenario Eve's behavior is similar to the way how noise, at random, modifies the transmitted bits).

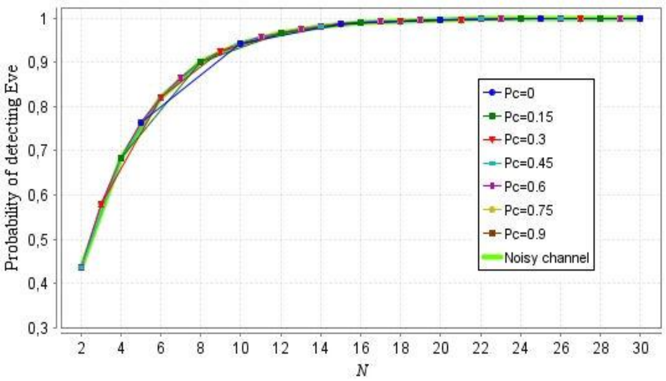

Fig. 5. Probability of detection of Eve as a function of the number of photons emitted for different values of P_C in a channel without noise. Results for a noisy channel are also shown.

By comparing Fig. 3 with Fig. 5 it can be observed that, in a perfect channel, Eve is more likely to be detected if she uses a random substitution attack, even with small values of N. In presence of noise or imperfections in the operating devices the probability of detecting the eavesdropper is quite similar for both attacks.

V. Conclusions

In this work, the interest of formally verifying the security of an experimental QKD system, by describing possible problems which can cause imperfections in the quantum channel, has been pointed out. By using a probabilistic model checker, the probability of detecting an eavesdropper is calculated for both an intercept-resend attack and a random substitution attack. Results show that as the channel becomes noisier the probability of Eve's detection increases.

References

[1] A. S. Khan, M. Mukund, and S. P. Suresh, "Generic verification of security protocols," *Lecture Notes in Comput. Sci.*, vol. 3639, pp. 221–235, 2005.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput. Syst. Signal Process*, pp. 175–179, 1984.

[3] C. H. Bennet, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett*., vol. 68, pp. 3121–3124, 1992.

[4] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.*, vol. 85, pp.441–444, 2000.

[5] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, pp. 351–406, 2001.

[6] H. K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999. Available: doi:10.1126/science.283.5410.2050. eprint arXiv:quant-ph/9803006.

[7] G. Brassard, "Brief history of quantum cryptography: A personal perspective," eprint arXiv:quant-ph/0604072, 2006.

[8] Y. Zhao, C. H. F. Fung, B. Qi, Ch. Chen, and H.K. Lo, "Experimental demonstration of time-shift attack against practical quantum key distribution systems," eprint arXiv:0704.3253v2, March 2008.

[9] M. Jing-Long, W. Fa-Qiang, L. Qing-Qun, and L. Rui-Sheng, "Practical non-orthogonal decoy state quantum key distribution with heralded single photon source," *Chinese Physics B*, vol. 17, no. 4, pp. 1178–06, April 2008.

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, pp. 3–28, 1992.

[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," *Phys. Rev. Lett.*, vol. 85, no. 6, pp. 1330–1333, 2000.

[12] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New J. Phys*, vol. 4, pp: 44-1–44-9, 2002.

[13] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, part 2, pp. 1915–1923, November 1995.

[14] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks For Weak Laser Pulse Implementations," *Phys. Rev. Lett*., vol. 92, no. 5, 057901, 2004.

[15] W. Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, no. 5, 057901, 2003. eprint arXiv:quant-ph/0211153.

[16] J. W. Harrington, J. M Ettinger, R. J. Hughes, and J. E. Nordholt, "Enhancing practical security of quantum key distribution with a few decoy states," 2005. eprint arXiv: quant-ph/0503002.

[17] Z. Feng, F. Ming-Xing, L. Yi-Qun and L. Song-Hao, "Differential-phase-shift quantum key distribution," *Chinese Physics*, vol. 16, pp. 3402–3406, November 2007.

[18] D. Mayers and A. C. Yao, "Quantum cryptography with imperfect Apparatus," in *Proc. 39th Ann. IEEE Symp. Foundations of Comp. Sci.*, pp. 503–509. IEEE Press, 1998. Available: doi:10.1109/SFCS.1998.743501. eprint arXiv:quant-ph/9809039.

[19] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, no. 2, 230501, 2007. Available: doi:10.1103/PhysRevLett.98.230501. eprint arXiv:quant-ph/0702152.

[20] D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inform. Comput.*, vol. 4, no. 5, pp. 325–360, September 2004. Available: http://www.rinton.net/xqic4/qic-4-5/325-360.pdf. eprint arXiv:quant-ph/0212066.

[21] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, "Thermal blinding of gated detectors in quantum cryptography," *Opt. Exp*., vol. 18, no. 26, pp. 27938–27954, 2010.

[22] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, Ch. Marquardt, V. Makarov, and G. Leuchs, "After-gate attack on a quantum cryptosystem," *New Journal of Physics*, vol. 13, 013043, 14 pp. 2011.

[23] C. Baier and J. P. Katoen, *Principles of model checking*. The MIT Press, Cambridge, MA, USA, 2008.

[24] S. Basagiannis, P. Katsaros and A. Pombortsis, "Synthesis of attack actions using model checking for the verification of security protocols," *Secur. Comm. Networks*, vol. 4, no. 2, pp. 147–161, February 2011.

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

[26] M. Duflot, M. Kwiatkowska, G. Norman, D. Parker, S. Peyronnet, C. Picaronny, and J. Sproston, "Practical Applications of Probabilistic Model Checking to Communication Protocols," In S. Gnesi and T. Margaria (eds.), *FMICS Handbook on Industrial Critical Systems*, IEEE Computer Society Press. Ch. 7, 2010. Available: http://eprints.gla.ac.uk/39594/1/fmics-chapter.pdf

[27] A. Hinton, M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: A tool for automatic verification of probabilistic systems," Lecture Notes in Comput. Sci., vol 3920, pp 441–444, 2006.

[28] PRISM web site. www.prismmodelchecker.org.

[29] M. J. García Martínez, D. Arroyo, N. Denisenko, D. Soto, A. Orúe , and V. Fernández, "High-speed free-space quantum key distribution system for urban applications," in *Proceedings of Photon10*, pp. 276, Southampton, UK, August, 2010.

[30] M. Kwiatkowska, G. Norman, and D. Parker, "Probabilistic Symbolic Model Checking with PRISM: A Hybrid Approach," *Int. J. Soft. Tools Techn. Transfer*, vol. 6, no. 2, pp. 128–142, September 2004

[31] D. Parker, "Implementation of Symbolic Model Checking for Probabilistic Systems", Ph.D. thesis, University of Birmingham. August 2002. Available: http://www.prismmodelchecker.org/papers/davesthesis.pdf

[32] R. Nagarajan, N. Papanikolaou, G. Bowen, and S. Gay. "An automated analysis of the security of quantum key distribution," In *Proc. Third International Workshop on Security Issues in Concurrency (SECCO'05)*, San Francisco, USA, August, 2005. Available: http://www.dcs.warwick.ac.uk/~nikos/downloads/nrgsecco05.pdf

[33] N. Papanikolaou, *Techniques for design and validation of quantum protocols*, M. Sc. Thesis, University of Warwick (UK), 2004. Available: http://www.dcs.warwick.ac.uk/~nikos/downloads/npmscthesis.pdf.

[34] M. Elboukhari, M. Azizi, and A. Azizi, "Applying Model Checking Technique for the Analysis of B92 Security," *J. Computing*, vol. 2, no. 9, pp. 50–56, September 2010.

[35] M. Elboukhari, M. Azizi, and A. Azizi, "Verification of Quantum Cryptography Protocols by Model Checking," *Int. J. Network Security & Appl.*, vol 2, no 4, pp. 43–53, October 2010. Available: http://airccse.org/journal/nsa/1010ijnsa04.pdf

[36] M. Elboukhari, M. Azizi, and A. Azizi, "Analysis of Quantum Cryptography Protocols by Model Checking," *Int. J. Universal Comput. Sci.*, vol 1, pp. 34–40, 2010. Available: http://www.hypersciences.org/IJUCS/Iss.1-2010/IJUCS-4-1-2010.pdf

[37] M. Elboukhari, M. Azizi, and A. Azizi, "Analysis of the Security of BB84 by Model Checking," *Int. J. Network Security & Appl.*, vol 2, no 2, pp. 87–98, April 2010. Available: http://airccse.org/journal/nsa/0410ijnsa7.pdf.

[38] A. M. Tavala, S. Nazem, and A. A. Babaei-Brojeny, "Verification of Quantum Protocols with a Probabilistic Model-Checker," *Elect. Notes Theor. Comput. Sci.*, vol. 270, no 1, pp. 175–182, 2011.