Quantum Information and Computation, Vol. 12, No. 7&8 (2012) 0620–0629

AN OPTICAL SCHEME FOR QUANTUM MULTI-SERVICE NETWORK

FÁBIO ALENCAR MENDONÇA
Lab. of Quantum Information Technology, Department of Teleinformatic Engineering
Federal University of Ceará, C.P. 6007 – Campus do Pici – 60455–970 Fortaleza–CE, Brazil

Federal Institute of Education, Science and Technology of Ceara, Fortaleza-Ce, Brazil

DANIEL BARBOSA DE BRITO
Lab. of Quantum Information Technology, Department of Teleinformatic Engineering
Federal University of Ceará, C.P. 6007 – Campus do Pici – 60455–970 Fortaleza–CE, Brazil

RUBENS VIANA RAMOS
Lab. of Quantum Information Technology, Department of Teleinformatic Engineering
Federal University of Ceará, C.P. 6007 – Campus do Pici – 60455–970 Fortaleza–CE, Brazil

Received May 13, 2011
Revised April 2, 2012

Several quantum protocols for data security having been proposed and, in general, they have different optical implementations. However, for the implementation of quantum protocols in optical networks, it is highly advantageous if the same optical setup can be used for running different quantum communication protocols. In this direction, here we show an optical scheme that can be used for quantum key distribution (QKD), quantum secure direct communication (QSDC) and quantum secret sharing (QSS). Additionally, it is naturally resistant to the attack based on single-photon detector blinding. At last, we show a proof-of-principle experiment in 1 km optical fiber link that shows the feasibility of the proposed scheme.

Keywords:
Communicated by: B Kane & G Milburn

1 Introduction

The field of secure quantum communication has been intensively investigated in recent decades. Although there are already several quantum protocols for data security [1–6], up to this moment only quantum key distribution became commercially available. Considering the implementation of different quantum communication protocols in optical networks, a highly desirable situation would be the development of an optical setup able to run different quantum protocols, integrating, in a simple way, different quantum services in the same optical network. In this direction, this work presents an optical scheme, based on thermal and coherent states, which can support quantum key distribution (QKD), quantum secure direct communication (QSDC) and quantum secret sharing (QSS). Furthermore, the proposed scheme can be easily implemented and it is resistant against several attacks including the external control of single-photon detectors [7].

Before explaining the proposed optical scheme, we give a brief review of coherent and thermal states. These states are described by the following density operators

$$\rho_\alpha = |\alpha\rangle\langle\alpha|, \qquad |\alpha\rangle = \sum_{n=0}^{\infty} exp\left(-\frac{|\alpha|^2}{2}\right)\frac{\alpha^n}{\sqrt{n!}}|n\rangle, \tag{1}$$

$$\rho_t = \frac{\mu_t^n}{(1+\mu_t)^{1+n}}|n\rangle\langle n|. \tag{2}$$

In (1) and (2), μ_t and $|\alpha|^2$ are, respectively, the mean photon number of the thermal and coherent states. Their overlap is given by

$$\langle\alpha|\rho_t|\alpha\rangle = exp\left[-\frac{|\alpha|^2}{1+\mu_t}\right]/(1+\mu_t). \tag{3}$$

Since they are not orthogonal for finite values of μ_t and $|\alpha|^2$, they cannot be perfectly distinguished. In particular, if $\mu_t = |\alpha|^2$ then the lower the mean photon number the worse is the distinguishability. However, if $\mu_t = |\alpha|^2 \neq 0$, the states ρ_α and ρ_t can be distinguished with high probability if one has a large enough number of samples of one of them. This task can be realized by a threshold single-photon detector. The probabilities of thermal and coherent states to fire an avalanche in a threshold single-photon detector are (neglecting the afterpulsing), respectively

$$P_t = 1 - \frac{1}{1+\eta\mu_t}(1-p_d), \tag{4}$$

$$P_c = 1 - exp(-\eta|\alpha|^2)(1-p_d). \tag{5}$$

In (4) and (5), η and p_d are, respectively, the single-photon detector quantum efficiency and dark count probability.

Measuring with a spectrum analyser, in a fixed frequency band, the electrical power of the signal produced by a threshold single-photon detector, a large sample of thermal states can be distinguished of a large sample of coherent states when both of them have the same low mean photon number. This happens because the electrical power in a fixed band is proportional to $(P - P^2)$ where P is the probability of an avalanche to be fired [8]. Since the probabilities in (4) and (5) are different when $\mu_t = |\alpha|^2$ ($P_c > P_t$), the electrical powers measured will also be different.

2 Optical setup for quantum multi-service network

The proposed optical scheme is shown in Fig. 1. The goal of this setup is to use the thermal states to protect the coherent states emitted by Alice and phase modulated by Bob.

Basically, Alice produces optical pulses having a coherent state at the horizontal mode and a thermal state at the vertical mode, both of them having the same (low) mean photon number. Following, Alice, randomly, sets her polarisation rotator $R(\theta_1)$ in 0 or $\pi/2$. Thus, for each optical pulse at Alice's output, the quantum state entering the optical channel is $1/2(\rho_\alpha \bigotimes \rho_t)_{HV} + 1/2(\rho_t \bigotimes \rho_\alpha)_{HV}$. Bob, by its turn, has a polarisation insensitive phase modulator [9]. Bob's phase modulation does not change the thermal state but it adds the phase ϕ_B to the coherent state. Leaving Bob's place, the optical pulses are sent back to Alice.

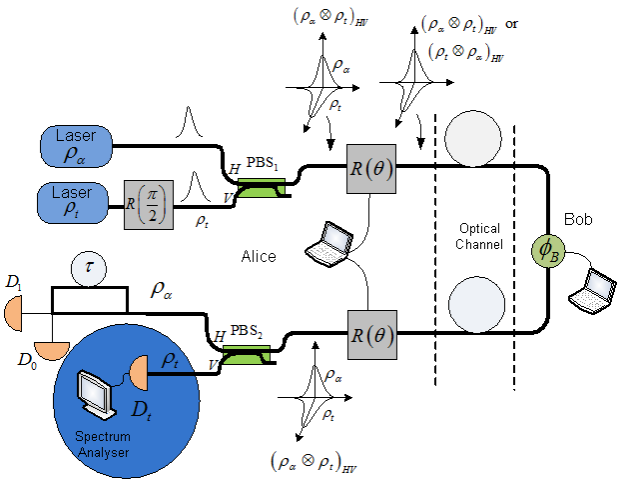

Fig. 1. Optical setup for implementation of a multi-service quantum network. PBS – polarizing beam splitter; R – polarization rotator; ϕ_B – phase modulator.

For each pulse arriving, she applies the same polarisation rotation she had applied when the pulse was leaving her place. Thus, before PBS_2, all pulses will have the coherent state at H-mode and thermal state at V-mode. These modes are separated by PBS_2 and the thermal state at the V-mode is monitored by a single-photon detector plugged to a spectrum analyser that will measure the electrical power in a fixed band. On the other hand, the coherent state at H-mode is sent to a fibre interferometer whose time difference between upper and lower arms, τ, is equal to the time separation between two consecutive pulses.

3 Security analysis

The security of the proposed optical setup can be explained as follows: Alice has two secrets: the mean photon number used and the polarisation rotations applied. During the communication, only one mean photon number value is used, but only Alice knows its value. As explained before, the coherent and thermal states with the same mean photon number can be distinguished if one has a large number of samples. With the setup shown in Fig. 1, only Alice can have a large amount of samples (pulses) because she is the only one able to separate with 100% of certainty the coherent and thermal states. Thus, Alice knows exactly the electrical power value she has to measure at the thermal state output. If she measures a different value, she will know that at thermal state output there is another type of quantum state or the mean photon number of the thermal state was changed.

In order to gain some information, the eavesdropper, Eve, has to attack the coherent state after Bob's phase modulation. However, Eve does not know in which polarisation mode it is, hence, she has to attack both modes. In the intercept-resend attack, having only one pulse to make correctly the distinguishability, sometimes the eavesdropper will be confused and, during the state reconstruction, with some probability (depending on the method used to determine in which mode is the coherent state), she may change ρ_α and ρ_t positions. In this case, Alice

will receive some coherent states at the thermal state output and some thermal states at the coherent state output. Alice will notice this attack because the electrical power value measured at thermal state output will be different from the expected value. Moreover, the thermal states at coherent state output will increase the error rate of the quantum communication protocol.

For the photon number splitting (PNS) attack, Eve will have to count the photon number of both modes. If each mode has at least two photons, a single-photon from each mode is captured and the rest of the photons are sent to Alice through a lossless fibre. If at least one of the modes has only one or zero photons, the optical pulse is absorbed and a vacuum state is sent to Alice. As can be seen, in this attack Eve's action does not cause the appearance of coherent states at the thermal output, but it changes the photon number distribution of the pulses arriving at the single-photon detector at thermal output and, hence, the electrical power value measured at thermal state output once more will be different from the expected value. In order to see this clearly, let $p^{\alpha}_{0(1)}$ and $p^{t}_{0(1)}$ be, respectively, the probabilities of the coherent and thermal states sent by Alice having zero (one) photon. Thus, the quantum state of the light arriving at Alice's place in the V-mode is, approximately, $(1-q)|0\rangle\langle 0| + q|1\rangle\langle 1|$, where $q = [1 - p^{\alpha}_0 - p^{\alpha}_1] \cdot [1 - p^{t}_0 - p^{t}_1]$. As can be noted, for simplification, the situations where the pulses sent by Alice have more than two photons were not considered since the mean photon number used is much lower than 1. Thus, the probability of detection caused by that state is $1 - (1 - q\eta)(1 - p_d)$. In order to do not disturb the electrical power value measured by Alice, the condition $1-(1-q\eta)(1-p_d) = 1-(1-p_d)/(1+\eta\mu_t)$ must be obeyed. However, for $\mu_t < 10$ this condition is never satisfied for any value of η, hence the PNS attack will cause an error in Alice.

The beam splitter attack can be realized without disturbing Alice's measurement if the beam splitter used has reflectance equal to the channel losses and Eve provides a lossless channel between her place and Bob's place. However, since Eve cannot attack all pulses, the amount of information obtained by Eve is limited. As happens in the PNS attack, she has to obtain at least one photon from each mode.

At last, the optical setup shown in Fig. 1 is naturally resistant to the attack in which the single-photon detectors are externally controlled by Eve by using strong light [7]. If Eve tries to control Alice's single-photon detectors the strong light will change the electrical power measured by Alice at the thermal state output, indicating that an attack is happening.

For all attacks discussed up to now we were concerned only with the probability of Eve to cause an alert signal in Alice by changing the electrical power value measured. However, even when this is not the case, Eve still has a hard problem to solve: she does not know which mode (H or V) contains the useful information, hence, she has to measure both of them and try to discover what is the useful information. For example, if the information is coded in the difference of phase between two consecutives coherent states (as it will be discussed latter), and Eve has success in her attack getting four photons from the two consecutive pulses, namely ph_{1c}, ph_{1t}, ph_{2c} and ph_{2t}, she has to measure the phase difference between $ph_{2c}-ph_{1c}$, $ph_{2c}-ph_{1t}$, $ph_{2t}-ph_{1c}$, and $ph_{2t}-ph_{1t}$. Thus, even if Eve can measure the phase difference without destroying the individuals phase information, she has four phase difference values and she has to guess which of them represents the correct information.

4 Quantum protocols

The first application of the scheme shown in Fig. 1 is quantum key distribution. The DPS-QKD protocol [10] can be readily implemented if Bob and Alice play the opposite roles as happens in traditional DPS-QKD. Thus, Bob modulates randomly each pulse that arrives at his place applying the phases 0 or π. Alice, by its turn, is the one who has the interferometer placed at the coherent state output. The protocol rules are the same and its security is increased by the use of thermal states as explained before.

The second application is quantum secure direct communication in which Bob sends to Alice in a secure way the bit string he wants. This is just a slight modification of the DPS-QKD protocol. Since the thermal states protect the coherent states, Bob and Alice can divide the pulse sequence (emitted by Alice) in time slots having two pulses and code a bit in the phase difference of two consecutive coherent pulses. For example, if the phase difference is 0, a bit 0 is obtained and if the phase difference is π, the bit 1 is obtained. Furthermore, the time interval between two time slots is larger than the time interval between the pulses inside a time slot (τ), hence, differently of the DPS-QKD, there is no useful information between the second coherente pulse of the n-th time slot and the first coherent pulse of the $(n+1)$-th coherent pulse. Every time Alice gets detection, she will obtain, very likely, the bit encoded by Bob. Since weak coherent states are being used, in several times Alice will not have detection. She must inform these situations to Bob. In these cases, Alice sends a new sequence of pulses with a new polarisation codification and Bob, by its turn, retransmits the bits not obtained in the first round of the protocol. The process is repeated until Alice gets the complete information.

The third and last application is quantum secret sharing. Here, once more, a slot time of two consecutive pulses defines the bit value and, hence, there is no information between pulses of different time slots. The same setup shown in Fig. 1 is used but now there are several Bobs, each one having its own phase modulator and a secret bit sequence that defines the phase-shift values that each Bob must apply in the pulses sent by Alice. The individual Bob's sequences are built in such way that the difference of phase between the two pulses in a time slot is always 0 or π. At the end of the protocol, Alice is going to obtain a bit sequence that will allow her to perform a useful task. On the other hand, if any Bob does not use the correct phase-shifts, the phase difference between pulses in a time slot may be different of 0 and π or, maybe 0 when it should be π or vice-versa. In this case, very likely, Alice will not get the correct final bit sequence. Hence, in order to Alice to achieve the correct bit string, all Bobs must collaborate using correctly their phase modulators according to their secrets.

5 Experimental results

In order to show to feasibility of the optical setup proposed, we realized a proof-of-principle experiment, implementing the optical setup shown in Fig. 1 without Bob's phase modulator and using CW light. Our goal is to check the security of the proposed scheme. The optical channel used was a 1 km single-mode optical fibre. We used a home-made single-photon detector based on the avalanche photodiode PGA-400, from Princenton Lightwave Inc. The output signal of the single-photon detector was directly plugged in a spectrum analyzer and the electrical power was measured. Two laser diodes operating at 1550 nm were used. The thermal light was produced operating one of the lasers well below the threshold while the

coherent state was produced operating the other laser well above the threshold. The mean photon number used for both quantum states was $\mu \sim 0.1$. The electrical power in a fixed band (central frequency = 70 MHz and RBW = 2 MHz) was measured in four situations: I) Complete absence of light. II) θ_1=θ_2=$\pi/2$. III) θ_1=0 and $\theta_2 = \pi/4$. IV) θ_1=θ_2=0. The cases II and IV show the expected measured power value when there are not attacks. The case III simulates an intercept-resend attack in which Eve changes the coherent and thermal modes with probability 50%. At last, in case I the power measured is produced by avalanches caused by dark counts. These results can be seen in Fig. 2.

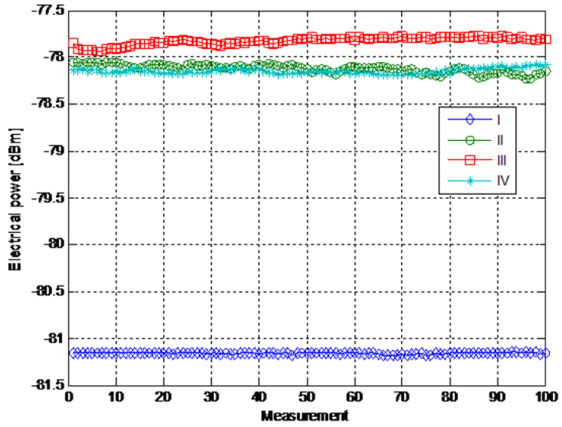

Fig. 2. Electrical power measured by a spectrum analyzer. A hundred values were measured in order to show the stability of the measurement along the time. I) Complete absence of light. II) θ_1=θ_2=$\pi/2$. III) θ_1=0 and $\theta_2 = \pi/4$. IV) θ_1=θ_2=0.

As can be observed in Fig. 2, when there are coherent and thermal states at the thermal output (case III), what happens in the intercept-resend attack, Alice clearly measures a power value different from the expected value (cases II and IV).

6 Conclusions

We proposed an optical setup able to run three different quantum protocols: QKD, QSDC and QSS. The quantum property that guarantees the security of these protocols is the non-perfect distinguishability between coherent and thermal states with the same (low) mean photon number. Some important considerations are:

1. In a first glance, one may think that our QKD protocol, hereafter named CT-DPS-QKD, is a kind of decoy-state protocol [11-14], being the thermal state the decoy state. This happens because like a decoy-state protocol, the CT-DPS-QKD also uses an extra quantum state with different photon number statistics aiming to increase the probability of Eve's detection. However, there are some important differences when the CT-DPS-QKD protocol is compared with commonly used decoy-state protocols:

1.1 Decoy-state protocols were designed aiming to prevent the photon number splitting (PNS) attack and they are not robust against attacks based on the external control of single-photon detectors [7]. For these decoy-state protocols, the single-photon detector had to be changed in order to detect an external control, hence more complex single-photon detectors are required. The CT-DPS-QKD protocol is naturally robust against PNS attack, external control of single-photon detectors, sequential attack using an unambiguous discrimination, among others.

1.2 Decoy-state protocols can use any number of decoy states and all of them are of the same type, for example, coherent states with different amplitudes chosen randomly. The CT-DPS-QKD protocol uses two different types of quantum state, coherent and thermal states, with the same optical power.

1.3 The current decoy-state protocols require parameter estimation from the data exchanged by Alice and Bob in order to infer Eve's presence, while the CT-DPS-QKD protocol infers Eve's presence from a parameter (error) estimation and/or the measurement of an electrical power.

1.4 When used in QKD, decoy states are optional states used to increase the security. If they are not used, the QKD protocol may still have some security depending on the parameters of the optical implementation like the mean photon number (that must be low in order to prevent multi-photon pulses) and the distance between Alice and Bob. On the other hand, in the QSDC and QSS protocols the information coded in the coherent states is classical (phase difference of 0 or π between two pulses that belong to the same time slot), hence in those cases the usage of thermal states is mandatory.

From the above, we have a different point of view. Our protocol with coherent and thermal states is a two-state protocol, like the protocol B92, that can be used alone (QSDC and QSS protocols) or can it be used together with others protocols aiming to increase the security (CT-DPS-QKD).

2. Since Bob has to modulate both polarization modes sent by Alice with the same information (he does not know which one is the coherent state) one of the quantum states used must not be affected by phase-modulation, otherwise, an eavesdropper would have two pulses containing the same information and the scheme would not be secure. Hence, one of the states used must be a state whose density matrix is a diagonal matrix in the Fock basis, that is $\sum_n p_n|n\rangle\langle n|$, like thermal states.

3. We described a situation where only Alice knows the mean photon number used (that is equal for both coherent and thermal states). However, our scheme may still be secure if Eve knows in advance the mean photon number used. If Eve knows the value of Eq. (4), she can produce a different quantum state that will produce the expected electrical power value at Alice's spectrum analyzer (for example, producing a coherent state with a suitable mean photon number polarized in $\pi/4$). In this case, Alice's Eavesdropper's detector, composed by threshold single-photon detector and spectrum analyzer, will not detect Eve's presence. However, in order to know the value of Eq. (4), Eve has to know the mean photon number of the light pulses sent by Alice and

the characteristics (quantum efficiency, dark count and afterpulsing probabilities) of the single-photon detector plugged in the spectrum analyzer. If Alice is sure that Eve does not know those parameters values, then she can divulgate the mean photon number used and the proposed scheme still remains secure.

4. The QKD protocol in our scheme is more secure than the original DPS-QKD protocol regardless the attack considered. This occurs because our QKD protocol is the DPS-QKD protocol protected by a second quantum security layer: the non-perfect distinguishability between coherent and thermal states. Hence, before applying any kind of attack to the DPS-QKD protocol, Eve has firstly to break the quantum security layer formed by the coherent and thermal states.

5. Since the DPS-QKD scheme is used, a brief security analysis for a sequential attack using an unambiguous discrimination can be realized. Let us assume that Eve knows the mean photon number used (but she does not know Alice's single-photon detector) and she uses unambiguous state discrimination in order to identify the coherent states sent by Alice. Eve's machine has three possible outcomes: $|\alpha\rangle$, $|-\alpha\rangle$ and '?', where the last implies in a inconclusive result. For each pulse sent by Alice, Eve applies the unambiguous discrimination to both polarization modes. Four situations are possible: I)'$\{?,?\}_{HV}$' (inconclusive in H and V modes) – in this case Eve should send a vacuum state to Alice. Note that Eve has to keep the electrical power value measured by Alice at thermal output in the correct value (or range), hence, it may not be possible to Eve always to send a vacuum state when she gets $\{?,?\}_{HV}$. If this is not possible, Eve will have to guess the coherent state sent by Alice running the risk of causing an error in the quantum communication. II) $\{|\pm\alpha\rangle,?\}_{HV}$ – in this case Eve sends the state$|\pm\alpha,\pm\alpha\rangle_{HV}$ to Alice. If the $|\pm\alpha\rangle$ comes from the measurement of the coherent state, Eve does not introduce an error in the quantum communication, if it comes from the measurement of the thermal state, there is some probability of Eve sending the wrong state and to cause an error in the quantum communication. This probability depends on the probability of Eve's machine to give the result '?' when a thermal state is measured. III) $\{?,|\pm\alpha\rangle\}_{HV}$ – the same as II. IV) $\{|\pm\alpha\rangle,|\pm\alpha\rangle\}_{HV}$ – when both results are the same, Eve does not introduce an error in the quantum communication. On the other hand, when she obtains different results, she will have to choose randomly one of them to send to Alice. Hence, there will be some probability of Eve sending the wrong state. In all cases she introduces an error in Alice's eavesdropper's detector, since a coherent state with mean photon number equal to '0' or $|\alpha|^2$ will not produce the same electrical power than a thermal state with mean photon number equal to $|\alpha|^2$.

6. Considering the QKD proposed, although there is useful information only in the quantum communication with coherent states, our scheme consists of two quantum protocols running at the same time, the DPS-QKD and the protocol with coherent and thermal states. They are linked in such way that attacking one of them produces errors in both when the value of (4) is not known by Eve.

7. Since our scheme uses a polarization codification, the main problem in long distance networks is the fiber depolarization. Hence, our scheme requires a (passive or active)

polarization controller in order to have a stable operation during long time intervals. However, this can be achieved using, for example, the scheme proposed in [15].

8. In order to avoid some side-channel attacks, optical filters should be used to let the coherent and thermal states inside the same spectrum range. On the other hand, aiming to avoid a Trojan horse attack in which Eve sends optical pulses to Bob's phase modulator, some counter-measures have to be implemented by Bob. He can, for example, to use an optical circulator before the phase modulator (to avoid a bidirectional path) and a beam splitter with a detector after the phase modulator in order to detect pulses sent by Eve.

Although we have discussed only QKD, QSDC and QSS protocols, our setup can be used in any quantum protocol where the secure transmission of coherent states is required. At last, since our optical scheme is secure, easily implementable and it can support different quantum protocols, we believe that it is a step-forward in the implementation of multi-service quantum networks.

Acknowledgements

This work was supported by the Brazilian agencies CAPES and CNPq via Grant no. 303514/2008-6. The experimental work was realized at LATIQ and NUCEMA/NUTEC(SECITECE) laboratories. Also, this work was performed as part of the Brazilian National Institute of Science and Technology for Quantum Information.

References

1. C. H. Bennet, G. Brassard (1984), *Quantum cryptography: public key distribution and coin tossing*, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 175-179.
2. D. Stucki et al. (2009), *High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres*, New. J. Phys. 11, 075003.
3. K. Shimizu, N. Imoto (2000), *Single-photon-interference communication equivalent to Bell-state-basis cryptography quantum communication*, Phys. Rev. A 62, 054303.
4. M. Hillery, V. Buzek and A. Berthiaume (1999), *Quantum Secret Sharing*, Phys. Rev. A 59, 1829.
5. X. Wen, Y. Liu, and N. Zhou (2007), *Secure quantum telephone*, Opt. Comm. 275, 278-282.
6. W. Brito, and R. V. Ramos (2008), *Quantum information technology with Sagnac interferometer: interaction-free measurement, quantum key distribution and quantum secret sharing*, J. of Mod. Opt. 55, 1231-124.
7. L. Lydersen et al (2010), *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nature Photonics 4, 686-689.
8. M. D. S. Cavalcanti (2011), *Spectral Method for characterization of avalanche photodiode working in the Geiger mode*, Master thesis, Department of Teleinformatic Engineering, Federal University of Ceara, Brazil (2011). Also in: M. D. S. Cavalcanti, F. A. Mendona and R. V. Ramos (2011), Spectral method for characterization of avalanche photodiode working as single-photon detector, Opt. Letts., 36, 17, 3446-3448.
9. B. Qi, L.-L. Huang, H.-K. Lo, and L. Qian (2006), *Polarization insensitive phase modulator for quantum cryptosystems*, Opt. Express 14, 4264-4269.
10. H. Takesue et al (2005), *Differential phase shift quantum key distribution over 105 km fibre*, New J. Phys. 7, 232.

11. H.-K. Lo, X. Ma, and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., 94, 23, 230504.
12. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo (2005), *Practical decoy state for quantum key distribution*, Phys. Rev. A, 72, 1, 012326.
13. M. Curty, X. Ma, B. Qi, and T. Moroder (2010), *Passive decoy-state quantum key distribution with practical light sources*, Phys. Rev. A, 81, 2, 022310.
14. Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto (2007), *Simple and efficient quantum key distribution with parametric down-conversion*, Phys. Rev. Lett., 99, 180503.
15. G. B. Xavier, G. Vilela de Faria, G. Temporao and J. P. von der Weid (2008), *Full polarization control for fiber optical quantum communication systems using polarization encoding*, Opt. Express 16, 1867-1873. 3.1.