IOP Conference Series: Materials Science and Engineering

PAPER • OPEN ACCESS

A satellite-based quantum key distribution using decoy-state protocol

To cite this article: A M Sofy *et al* 2021 *IOP Conf. Ser.: Mater. Sci. Eng.* **1172** 012010

A satellite-based quantum key distribution using decoy-state protocol

A M Sofy[1], M Y Shalaby[2] and H M Dahshan[1]

[1] Military Technical College, Department of Communication Engineering, Cairo, Egypt
[2] Ministry of Defence, Cairo, Egypt

E-mail: myousef73@hotmail.com

Abstract. An ideal QKD implementation that provides the promising unconditional security using single photon laser source is not practically easy, also sending these photons over a fiber channel affects the maximum distance of link up to few hundreds of kilometers because of the receiver's detectors losses. Therefore, the achievement of a global quantum network is not easy, and the need to use LEO satellites [1,2] for establishing quantum links makes the job easier as quantum free space link provides much less losses to the link than fiber links. Nowadays, a quantum communication link can be established by satellites through free space. in this paper, we propose an implementation [3] of a satellite-based quantum key distribution using decoy-state protocol [4], we then compare this protocol with the BB-84 protocol [3] against security and the key length of the generated shared key.

1. Introduction

Quantum key distribution protocols are protocols for distributing secure key privately between two sides to establish a secure channel between them, This field of study has a quick progress since the first proposed protocol in 1984 (BB-84) named after its inventors (Bennett and Brassard) [5],QKD security doesn't depend on the computational difficulty of mathematical problems solving (mainly factorizing a large prime number as in most current encryption systems), but depends on the uncertainty principle of the quantum mechanics.

Another advantage of quantum cryptography represented in QKD protocols, a property called forward security' as if a generated QKD key is secure now so it will remain secure in the future against computing power advances, on the other hand, in public-key encryption, the keys and secured messages be stored and being subjected to different kinds of cryptanalysis and can be easily affected by computing power advances in the future.

In case of talking about the optical techniques for QKD implementation, it can be classified into two types, discrete-variable QKD (DV-QKD) in which each bit of private information is encoded into a discrete degree of freedom of optical signals. Another technique called continuous-variable QKD (CV-QKD) in which the private information is encoded using coherent communication techniques. Both techniques have consumed a lot of research effort to increase the rate of key generation and make it more compatible with nowadays communication infrastructure. but both techniques have a difficulty when being implemented in a wide-scale of QKD as there is big exponentially increasing transmission losses on the physical communication channels with distance, which makes a great limitation on the achievable key rates on these channels on long distances.

In this paper, we focus on DV-QKD protocols which can be categorized into prepare and measure protocols and entanglement-based protocols.

Entanglement based protocols Link quantum states of two far away (separated) objects together in a way that you can't describe one of them alone but only as a combined quantum state. In other words, measuring one will affect the other, so a pair of entangled objects is shared between two users, this is called entanglement. if any object was intercepted, it will be detected by affecting the other, and hence any unofficial third party will be detected.

Prepare and measure protocols where, Alice prepares (encodes) each classical bit individually as an optical signal then transmit it to Bob, who makes some measurements on the incoming signal individually, so he can get the classical data back. In this paper, we focus on prepare and measure protocols.

1.1. BB-84 Protocol

It is considered the pioneer work in quantum key distribution and it is the most commonly used prepare and measure protocol in which classical bits are encoded individually as polarization of a single photon, as Alice prepares the photons to be sent to Bob by choosing randomly the operating basis either horizontal/vertical basis (with polarization 0°/90°, respectively) basis or diagonal basis (with polarization 45°/135°, respectively) and then, the state with polarization 0° for horizontal/vertical basis or polarization 45° for diagonal basis is encoded as bit 0, and the state with polarization 90° for horizontal/vertical basis or polarization 45° for diagonal basis is encoded as bit 1. Then Bob receives these photons and makes his measurement on them one by one using randomly selected bases. After that, both sides announce in public the used basis every time, signals with different bases will be discarded and the others with the same basis will be kept, from which they create a secret key between them. In practical, applying such a protocol requires a true quantum random number generator such as (Quantis AIS 31) for random seeds production to make basis selection, and a single photon laser source which is not practically applicable as each laser pulse has some probability of containing more than a single photon.

1.2. Decoy-State Protocol

To overcome the problem of single photon sources, decoy-state protocol [4] uses weak coherent state laser source, where the mean of the number of photons can be controlled by adjusting the intensity of the laser beam, so decoy-state protocol, a one-way quantum key distribution protocol, actually works the same way as BB84, however it adds a precedent step which adds another degree of freedom. This adds another choice taken by Alice when sending every signal pulse to Bob, as well as another level of complexity for the eavesdropper to analyze.

In this case, Alice chooses randomly the intensity level of the sent state signal between two or more levels of intensity every time. Later, Alice announces publicly the used intensity level for sending every signal state (qubit). Since eavesdropper can't differentiate between signal and decoy pulses, any eavesdropping technique which depends on the number of photons (as Photon Number Splitting attack, PNS attack) has different impacts on the signal states and the decoy states and is therefore likely to be detected.

Decoy-state protocol has advantages over BB84 protocol, as in ideal BB84 protocol, only signals with single photon pulses sent from Alice are guaranteed to be secure, also using this would reduce losses in a comparison to BB84, moreover, using regular multi-photon sources leads to the ability of deploying these protocols using commercially available components.

1.3. Attacks and Security Proofs

Intercept and resend attack, Eve is going to quantify all the quantum states (photons) sent from Alice and then forward other states to Bob, prepared in the state she is estimating. It causes errors on the keys Alice and Bob share using BB84 protocol. Since, Eve has no idea the bases on which the states sent by Alice are encoded, she can only guess what bases to determine in the same way Bob does [6]. She estimates the correct state of photon polarization as sent by Alice when she chooses the same basis used by Alice, and sends the photon with the correct polarization to Bob. However, when she chooses the wrong basis, she estimates the state randomly and the state sent to Bob might not be the same as the state sent by Alice. If Bob then tests this state on the same basis that Alice sent, he gets a random outcome, with 50 percent he will get incorrect outcome (instead of the right outcome he would get without Eve being present).

Table I below gives an example of such an attack as the system uses two bases $|P\rangle$ and $|X\rangle$ of dimension d=2.

Table 1. Detecting Eve in Intercept and Resend Attack.

Randomly sent qubits	1	0	0	0	1	1	0	1	0
Qubits sent by Alice	$\|P; 1\rangle$	$\|X; 0\rangle$	$\|P; 0\rangle$	$\|P; 0\rangle$	$\|X; 1\rangle$	$\|X; 1\rangle$	$\|P; 0\rangle$	$\|X; 1\rangle$	$\|P; 0\rangle$
Eve's measuring basis	P	P	P	X	X	P	X	X	X
Qubits sent by Eve	$\|P; 1\rangle$	$\|P; 1\rangle$	$\|P; 0\rangle$	$\|X; 1\rangle$	$\|X; 1\rangle$	$\|P; 1\rangle$	$\|X; 0\rangle$	$\|X; 1\rangle$	$\|X; 1\rangle$
Bob's measuring basis	X	X	P	X	X	P	P	P	X
Qubits received by Bob	1	0	0	1	1	1	1	1	1
Shared key		0	0		1		**[1]**		

Photon number splitting attack, Alice in the BB84 protocol uses single photon to send the quantum state to Bob. In practical Implementations, laser pulses may have 2 or more Photons per pulse. When there are multiple photons in the pulse, then Eve can separate the excessive photons and Forward the remaining one photon to Bob. This is the concept of the splitting of photon number attack, where Eve uses a quantum memory to store those extra photons till Alice and Bob reveal the encoding basis. Eve then can calculate her photons in Right foundation and get crucial information without making detectable errors. this problem has many solutions. The most apparent is the use of a real single source of photons rather than an attenuated laser.

Although these sources are still in the developmental process, QKD was successfully carried out with them because current sources operate at low efficiency and frequency main levels and conveyance distances are restricted. Another option is replacing the BB84 Protocol with the Decoy states protocol, where Alice sends some randomly selected laser pulse's intensities with different average photon number of her laser pulses. You may use these decoy states to detect an PNS attack, since Eve has no way of knowing which pulses are signals and which are decoys. This concept was put into effect successfully, at the University of Toronto and in a number of QKD experiments, allowing high levels of security against known attacks.

Denial of service attack, which can be performed by simply cutting or blocking the line between two points connected by the quantum key distribution. This is one of the reasons why developing quantum key distribution networks must have alternative links in the case of interruption.

Security proofs, in case that Eve has unlimited resources, e.g. both classical and quantum computation abilities so she has a big chance to make a successful attack. BB84 protocol has been proved to be immune against any quantum mechanics-based attacks. Quantum mechanics allowed us to transmit information unconditionally safe using an ideal source of photons that emits just one photon at a time[7]. however, there are also other Necessary conditions to make the communication safe:

- Eve can't physically access Alice encoding equipment and Bob decoding equipment

- Using a true random generator for producing random seeds for both Alice's and Bob's selections.
- The classical channel of communication should be authenticated by the use of unconditionally secure Scheme for Authentication.
- One-time pad encryption scheme preferred to be used for encrypting the message.

2. Related Work

Nowadays usage of satellite QKD became applicable as it is moving so fast from the experimental phase to the practical one. An example, is the Chinese project carrying the name of (Micius) [8] a sun-synchronous satellite in a low-earth orbit at 500 KM altitude, which is a common project between Chinese Academy of Sciences (CAS), Austrian Academy of Sciences (AAS) and University of Vienna. It uses an optical transmitter to operate a Decoy-state QKD, as the Chinese quantum satellite works as a trusted relay between three nodes for key distribution.

Satellite optical links can be categorized into uplink and downlink. The downlink is more reliable than uplink as it is subjected to lower atmospheric loss than the uplink, because atmospheric properties like turbulence causes wandering of the optical beam which translates into a less accurate land transmitter than a space transmitter. But the uplink has an advantage that we don't have to place an accurate optical laser source in space which is somehow complex, instead we need to place a simple receiver onboard the satellite.

The most significant scenario of applying QKD in space is by using the satellite as a flying trusted node or it can be called (Key Relay Protocol), that the satellite makes QKD process with every ground station individually after all the satellite will store a shared secret key between it and each ground station. So for making a secure link between any two ground stations that have secret keys, (key 1) and (key 2) respectively, we need to provide each one with the key of the other, this is simply done by the satellite that sends the XOR combination of the two keys (key1, key2) to both stations, from which each station can retrieve the key of the other by XORing its own key to this combination, key1 $\oplus$ (key1$\oplus$ key2) = key2, key2 $\oplus$ (key1 $\oplus$ key2) = key1, this process is illustrated in Figure 1.

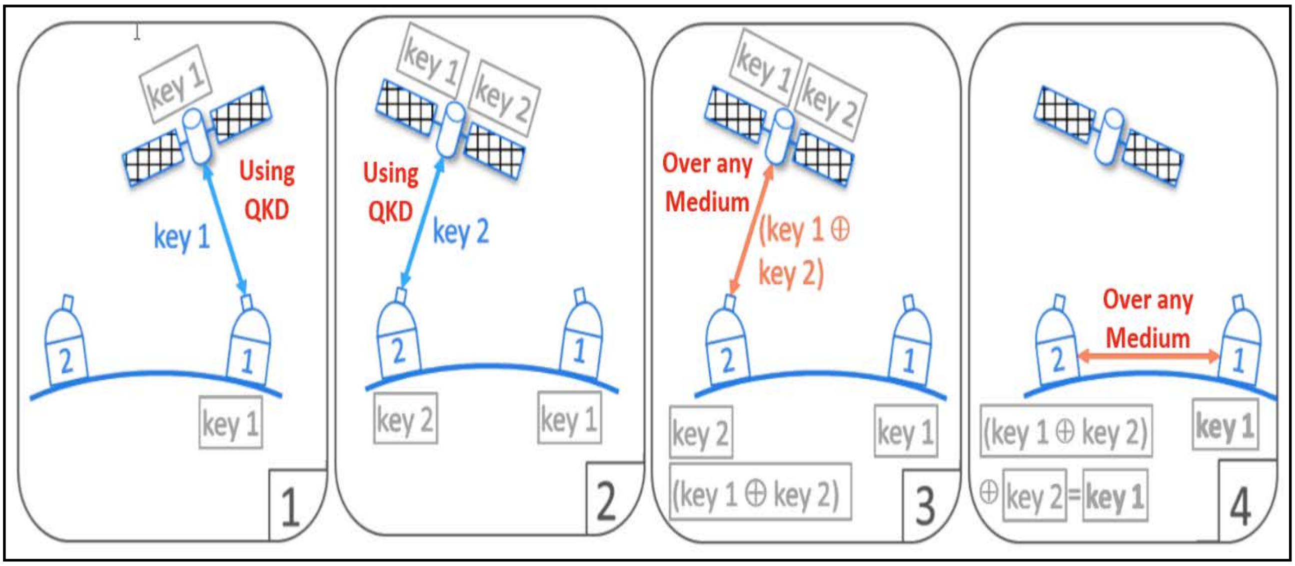

Figure 1. The use of a satellite for QKD.

The key relay protocol is implemented practically in the Chinese quantum satellite "Micius" that deploys a Decoy-state QKD protocol through a quantum downlink. The trusted node network principal may be used in fiber network, however using a ground trusted node makes it easily be subjected to surveillance, probes and other kinds of attacks that can't affect a flying node (satellite) as it is a fast-moving target.

3. THE PROPOSED SIMULATION FRAMEWORK

We simulate the implementation of Decoy-state protocol using Optisystem v7.0 software package. It is an optical communication system simulator that provides a wide variety of QKD components. Most of the components used in simulation and their properties are exploited for the experimental use to setup QKD. In our experiment, a two-dimensional quantum system (d=2) is proposed with two orthogonal bases the rectilinear basis and the diagonal bases which are as presented in Table 2.

Table 2. Representation of Basis

Basis	Notation	Bit 0	Bit 1
Rectilinear Basis	+	0^{O} →	90^{O} ↑
Diagonal basis	X	45^{O} ↗	135^{O} ↖

3.1. Dataset

A hardware true quantum random numbers generator (Quantis AIS 31) shown in Figure 2 was used to generate the used random seeds that were used in the simulation work.

IDQ
Quantum Random Number Generator
Made in Switzerland
www.idquantique.com
QUANTIS
QUANTUM RANDOM NUMBER GENERATOR
IDQ

Figure 2. RNG used in simulation (Quantis AIS 31).

The generated random seeds were used for making the selection of the following:

- The basis of each iteration used by Alice
- Bob's basis for each iteration

- The basis for each iteration used by Eve
- Alice's intensity level of the sent state signal (from two levels of intensity)

A previous work was done by the Authors for modelling BB84 [3] on which this work is based. To make a fare comparison between the two protocols, this simulation is done with and without the presence of a third party (Eve).

3.2. *IMPLEMENTATION SETUP FOR DECOY-STATE PROTOCOL*

There are three basic functional blocks in this model as follows:

- Alice's side: where the laser source can emit a pulse with two intensities. The pulse is then encoded as a random state in random basis for each pulse
- Bob's side: where a random selection of the used basis for measurement is done with every received pulse from Alice
- Eve's side (if exist): where also a random measurement is done on the pulses passing through the quantum channel as Eve is supposed to have a full access to the quantum channel and can perform Intercept and resend attack. ,a more detailed description for the internal components of the model's blocks was previously illustrated in our previous work [3] of modelling the BB84 and The Two-Way QKD
  protocols.

The modelling diagram of Decoy state without Eve is shown in Figure 3, and the modelling diagram of Decoy state with Eve is shown in Figure 4.

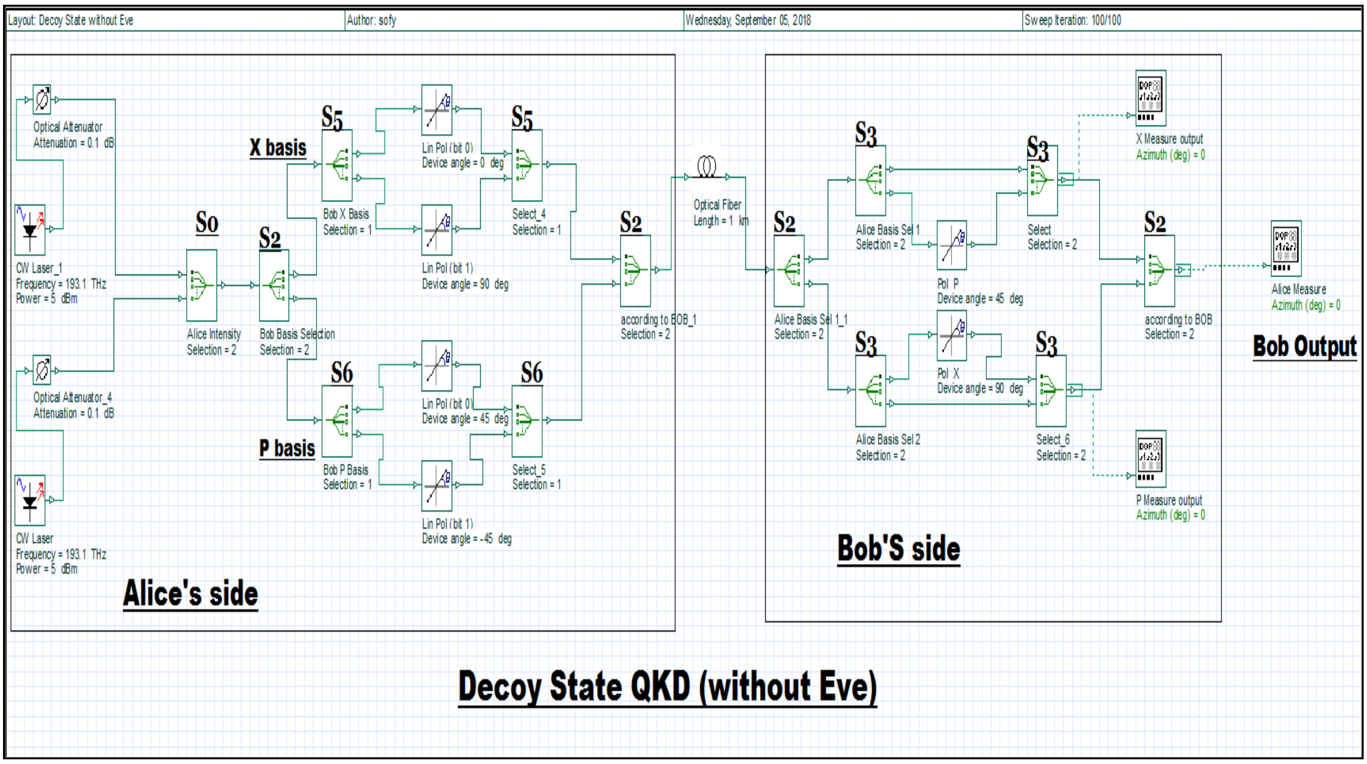

Figure 3. Model of Decoy-State QKD without Eve.

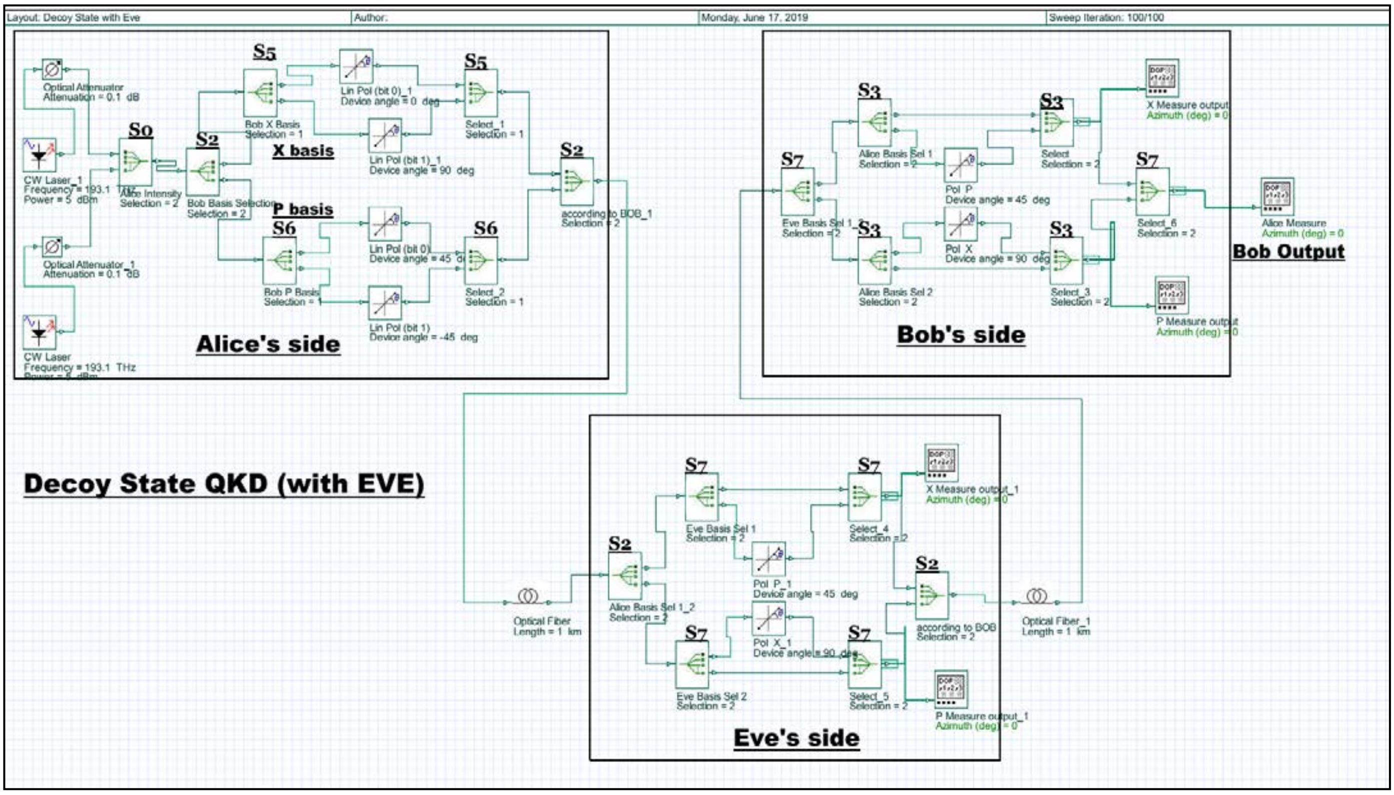

Figure 4. Model of Decoy-State QKD with Eve.

3.3. *Results*

In this model 1000 qubits were generated and sent from Alice to Bob. In the case that Eve is not present, the shared key size is 297 qubits, in the case of Eve presence, the shared key size is 213 qubits, as shown in Figure 6, taking into consideration that in both cases the same random seeds were used as various inputs for the modelling software for selecting Alice's encoding basis , Bob's measuring basis and also Eve's measuring basis, after analyzing the results and comparing the shared key size between the two cases of presence and absence of Eve we found that the presence of Eve affected 84 qubits which was detected as errors after the final announcement between the two parties out of 297 qubits (the shared key size in case of Eve's absence) leading to make the key size up to 213 qubits in case of exchanging 1000 qubits between the two parties.

To make a fare comparison between the proposed implementation of decoy-state protocol and the implementation of BB84 protocol[3,9], we select the same random seeds for both implementations at every iteration. The comparison results are shown below:

- without Eve's presence, the total shared key size decreased from 534 qubits in the case of BB84 [3] to 297 qubits in the case of our Decoy-state implementation.
- with Eve's presence, the total shared key size decreased from 412 qubits in the case of BB84 [3] to 213 qubits in the case of our Decoy-state implementation.

So, the probability of detecting Eve of BB-84 and Decoy state protocols can be calculated as shown in equation (1) and equation (2) sequentially.

$$P_d = \frac{\text{number of wrongly received qubits due to Eve's Measure}}{\text{Shared key size without Eve}} = \frac{122}{534} = 0.228 \qquad (1)$$

$$P_d = \frac{\text{number of wrongly received qubits due to Eve's Measure}}{\text{Shared key size without Eve}} = \frac{84}{297} = 0.28 \quad (2)$$

Figure 5 shows the results of One-Way protocol that was previously obtained in our previous work [3], and Figure 7 shows the comparison between the two protocols.

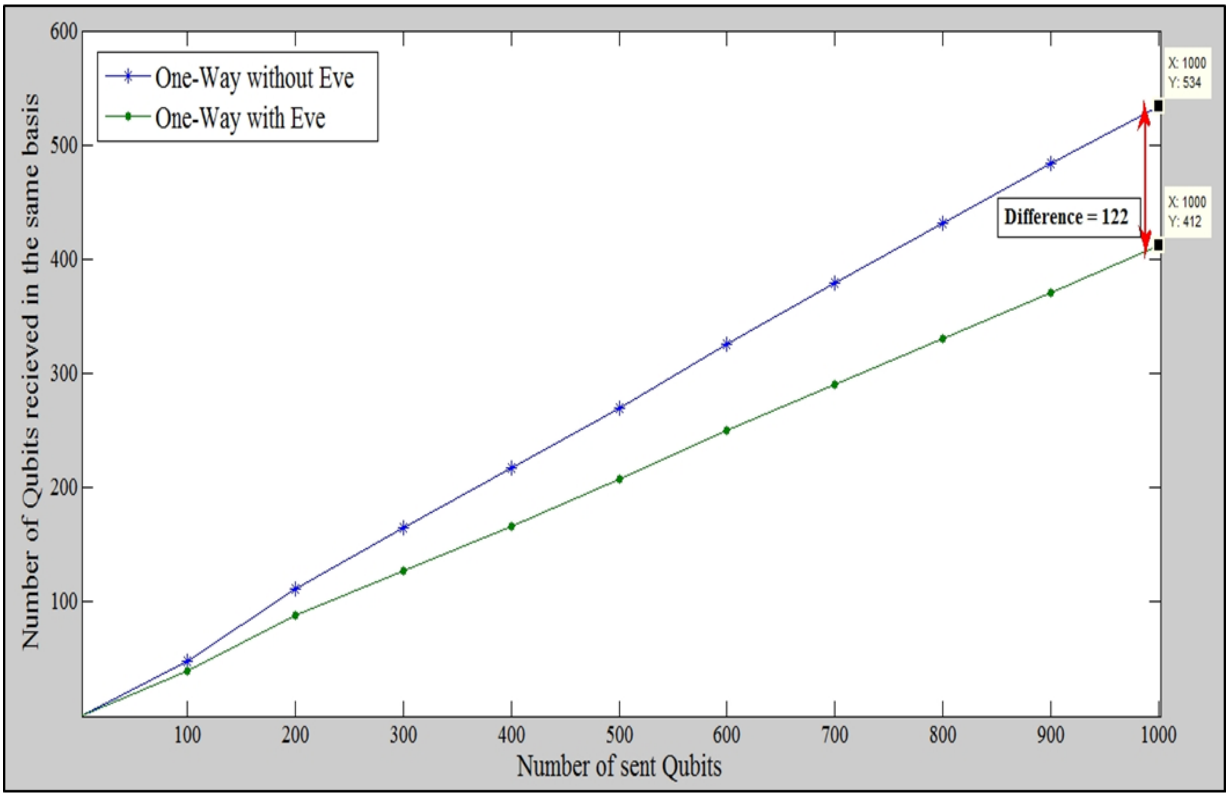

Figure 5. The number of qubits in the shared key between Alice and Bob in the presence and absence of EVE in One-Way protocol.

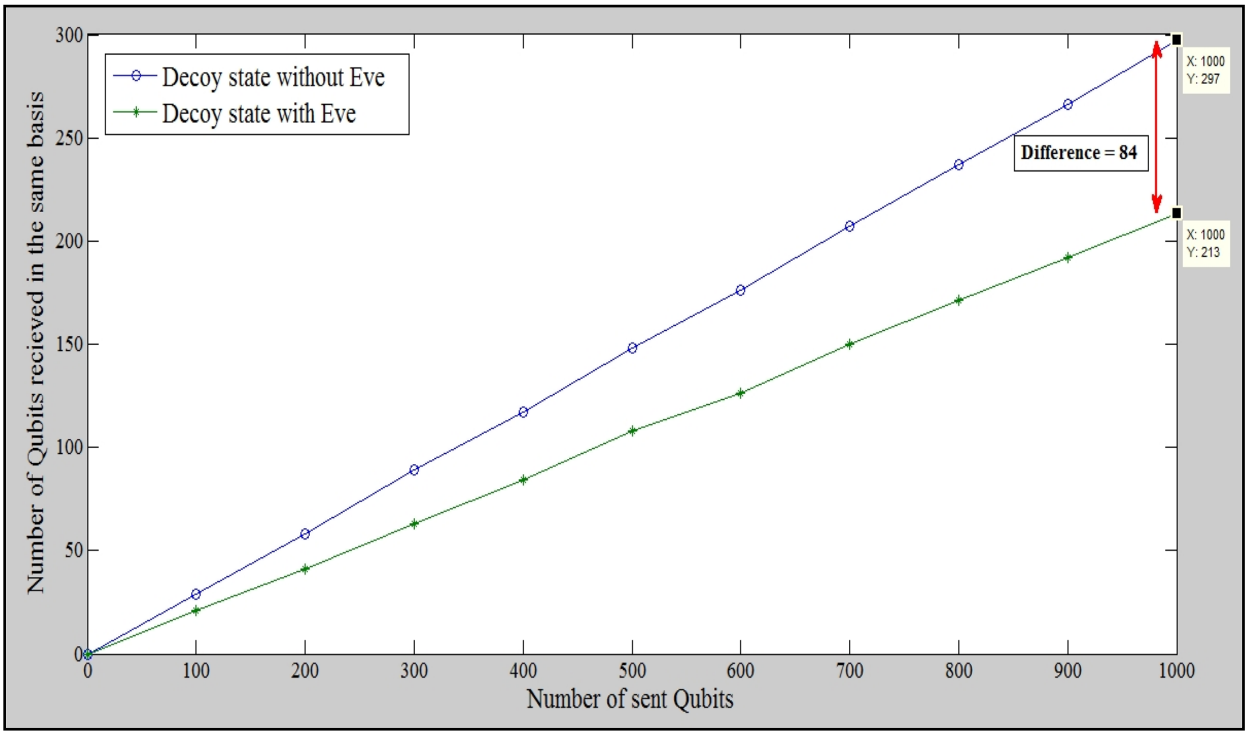

Figure 6. The number of qubits in the shared key between Alice and Bob in the presence and absence of EVE in Decoy-state protocol.

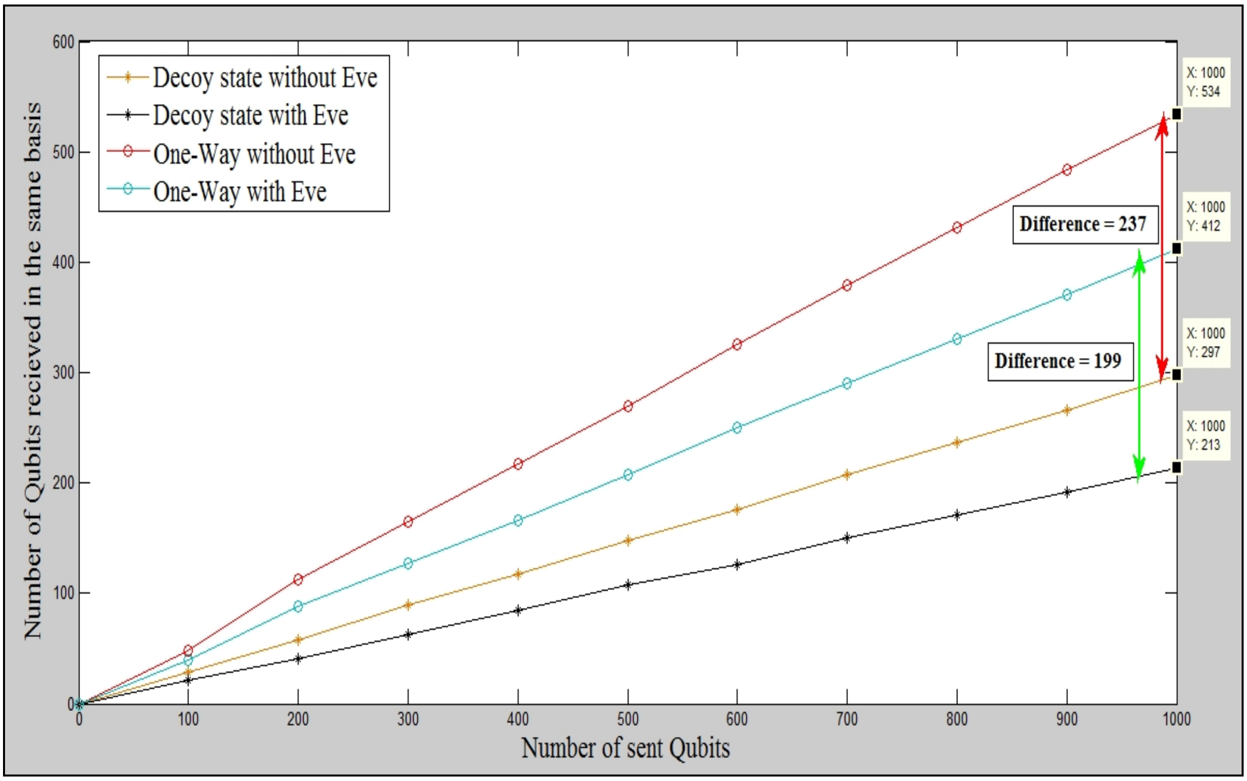

Figure 7. Comparison between the shared key size the presence and absence of EVE in One-Way protocol and Decoy-state protocol.

4. Conclusion

We have discussed the decoy-state protocol which is widely used for satellite quantum key distribution. Comparing the simulation of decoy-state protocol with BB84 protocol and according to the experimental results, the probability of detecting the presence of Eve, in the case of decoy-state implementation (Pd),equals 84/297 = 0.28, the probability of detecting the presence of Eve, in the case of implementing BB84 was 0.228 [3] in our previous work for a 1000 qubits sample.

we found out that decoy-state protocol is more secure against PNS attacks, and the experimental results of applying both protocol using Optiwave v7.0 software package shows that the probability of detecting Eve in the case of decoy-state protocol outperforms its counterpart in the case of BB84 protocol (0.28 versus 0.228) [10]. However, the number of shared qubits in the case of decoy-state protocol is less than its counterpart in the case of BB84 protocol.

References

[1] Liao S K, Cai W Q, Liu W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J C, Jiang X J, Wang J F, Huang Y M, Wang Q, Zhou Y L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y A, Liu N Le, Wang X Bin, Zhu Z C, Lu C Y, Shu R, Peng C Z, Wang J Y and Pan J W 2017 Satellite-to-ground quantum key distribution *Nature* **549** 43–7

[2] Scheidl T, Handsteiner J, Rauch D and Ursin R 2019 Space-to-ground quantum key distribution **11180** 67

[3] Sofy A M, Shalaby M, Dahshan H M and Rohiem A 2019 Modeling One-way and Two-way quantum key distribution protocols *Proc. - 2019 IEEE 9th Int. Conf. Intell. Comput. Inf. Syst. ICICIS 2019* 239–44

[4] Lo H K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 1–5

[5] Bedington R, Arrazola J M and Ling A 2017 Progress in satellite quantum key distribution *npj Quantum Inf.* **3** 1–12

[6] Fröhlich B, Lucamarini M, Dynes J F, Comandar L C, Tam W W-S, Plews A, Sharpe A W, Yuan Z and Shields A J 2017 Long-distance quantum key distribution secure against coherent attacks *Optica* **4** 163

[7] Alléaume R, Roueff F, Diamanti E and Lütkenhaus N 2009 Topological optimization of quantum key distribution networks *New J. Phys.* **11**

[8] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A and Weinfurter H 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98**

[9] Buhari A, Zukarnain Z A, Subramaniam S K, Zainuddin H and Saharudin S 2012 An efficient modeling and simulation of quantum key distribution protocols using OptiSystem^{TM} *ISIEA 2012 - 2012 IEEE Symp. Ind. Electron. Appl.* 84–9

[10] Verma P K, El Rifai M and Chan K W C 2019 Quantum Key Distribution *Signals and Communication Technology* (Springer) pp 59–84