Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/140518

The Entangling-Probe Attack On The Bennett-Brassard 1984 Protocol

H. F. Abdel-Hameed[1,2]

[1]Mathematics Department, Faculty of Science, Sohag University, Sohag, Egypt
[2]Mathematics Department, Khurma University College, Taif University, Al-Taif, Saudi Arabia

Received: 19 Jun. 2019, Revised: 8 Sep. 2019, Accepted: 13 Sep. 2019
Published online: 1 Sep. 2020

Abstract: In this paper, we introduce a generalization of the Fuchs-Peres-Brandt (FPB) attack which is the most powerful individual-photon attack against Bennett-Brassard 1984 (BB84) quantum key distribution protocol. We suppose that Eve sets up her C-NOT gate with its control-qubit computational basis $\{|0\rangle_C, |1\rangle_C\}$ given by an α rotation from the BB84 $(H-V)$ basis.

Keywords: Quantum key distribution (QKD),BB84 protocol, Polarization, FPB attack, C-NOT Gate, Single-photon

1 Introduction

Key distribution is the term applied techniques that allow two parties to acquire a random bit sequence (the key) with a high level of confidence that no one else knows or has significant partial information [1]. The best-known quantum key distribution (QKD) protocol (BB84) was published by Bennett and Brassard in 1984 [2], while its idea goes back to Stephen Wiesner in the 1970's [3]. In this protocol, the first party (the sender Alice) sends a sequence of signals (single-photon pulses) each randomly chosen from one of the four polarization states of the horizontal/vertical $(H-V)$ and ±45° diagonal/antidiagonal $(D-A)$ bases. For each signal, the second party (the receiver Bob) randomly chooses one of the two measurement devices to perform a measurement. Alice and Bob announce their polarization bases for each signal. They discard all events that are detected by Bob using different bases. Alice randomly chooses a fraction of all remaining events as test events. For those test events, she transmits the positions and the corresponding polarization data to Bob. Bob compares his polarization data with those of Alice and tells him whether their polarization for the test events agrees. In case of agreement, Alice and Bob convert the polarization data of the remaining set of events into binary form. Such a generated binary string is their secret key now.

Since then, the BB84 protocol has been implemented in free space [4] and in optical fibers [5]. Its security has been analyzed [6, 7], particularly for configurations that involve non-ideal operating conditions, such as the use of weak laser pulses instead of single photons [8]. An eavesdropper (Eve) may try to break the scheme to share or gain Alice and Bob's information. For quantum cryptography, the security of some QKD protocol in the presence of external noises [9, 10] as well as the robustness BB84 for distributing a QKD [11] are investigated. Papers of Fuchs and Peres [12], Slutsky *et al.* [13], and Brandt [14] show that the most powerful individual-photon attack can be accomplished with a controlled-NOT (C-NOT) gate. In this scheme, Eve supplies the target qubit to the C-NOT gate, which entangles it with the BB84 qubit that Alice is sending to Bob. Eve then makes her measurement of the target qubit to obtain information on the shared key bit at the expense of imposing detectable errors between Alice and Bob [14, 15]. It is shown that single-photon two-qubit (SPTQ) quantum logic can be used to implement [15] Fuchs-Peres-Brandt (FPB) entangling probe, in which a single photon carries two independent qubits: the polarization and the momentum (or spatial path) states of the photon [16].

It is interesting to report that, SPTQ gates are deterministic and can be efficiently implemented using only linear optical elements [17, 18]. Also, they are distinct from standard two-photon quantum gates.

Kim *et al.* [16] use SPTQ logic to implement the FPB probe as a complete physical simulation of the most

[*] Corresponding author e-mail: hf_elsheikh@yahoo.com

powerful individual-photon attack on the BB84 protocol, including physical errors. This is the first experiment on attacking the BB84 protocol, and its results are consistent with theoretical predictions. In the paper [16], they regard that Eve breaks the connection between Alice and Bob by setting up her C-NOT gate with its control-qubit computational basis $\{|0\rangle_C, |1\rangle_C\}$ given by a $\frac{\pi}{8}$ rotation from the BB84 $(H-V)$ basis. The SPTQ probe could become a true attack if quantum non-demolition measurements were available to Eve [8]. The present paper aims to show how Eve can share Alice and Bob's information without making any disturbance of Bob's measurements by setting up C-NOT gate of Eve. In Sec.2, Fuchs-Peres-Brandt (FPB) attack is investigated and discussion is presented in Sec 3.

2 FPB Attack

In the paper by Kim *et al.* [16], Eve sets up her C-NOT gate with its control-qubit computational basis $\{|0\rangle_C, |1\rangle_C\}$ given by a $\frac{\pi}{8}$ rotation from the BB84 $(H-V)$ basis. But in this work, we assume that Eve sets up her C-NOT gate with any rotation angle of α, s.t. $\pi \geq \alpha \geq 0$, from the BB84 $(H-V)$ basis, as shown in Fig. 1,

$$|H\rangle = \cos\alpha|0\rangle_C - \sin\alpha|1\rangle_C, \tag{1}$$

$$|V\rangle = \sin\alpha|0\rangle_C + \cos\alpha|1\rangle_C, \tag{2}$$

$$|D\rangle = \cos(\frac{\pi}{4}-\alpha)|0\rangle_C + \sin(\frac{\pi}{4}-\alpha)|1\rangle_C, \tag{3}$$

$$|A\rangle = -\sin(\frac{\pi}{4}-\alpha)|0\rangle_C + \cos(\frac{\pi}{4}-\alpha)|1\rangle_C. \tag{4}$$

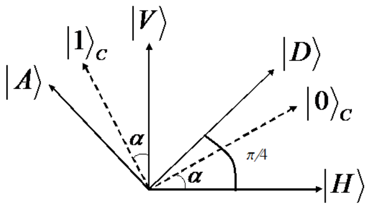

Fig. 1: Relations between control-qubit computational basis for Eve's C-NOT gate and BB84 polarization states

We suppose that Eve prepares her probe qubit to creat an error probability P_E in the initial state

$$|T_{\text{in}}\rangle = \frac{1}{\sqrt{2}}\{(C+S)|0\rangle_T + (C-S)|1\rangle_T\} \tag{5}$$

where $C = \sqrt{1-2P_E}$, $C^2+S^2=1$, and $\{|0\rangle_T, |1\rangle_T\}$ is the target qubit's computational basis.

Now, when Eve applies the C-NOT gate which entangles with Alice's photon states, we can get four possible outputs of the C-NOT gate in the form

$$|H_{\text{out}}\rangle \equiv |H\rangle|T_1\rangle + |V\rangle|T_{E1}\rangle, \tag{6}$$

$$|V_{\text{out}}\rangle \equiv |V\rangle|T_2\rangle + |H\rangle|T_{E1}\rangle, \tag{7}$$

$$|D_{\text{out}}\rangle \equiv |D\rangle|T_3\rangle - |A\rangle|T_{E2}\rangle, \tag{8}$$

$$|A_{\text{out}}\rangle \equiv |A\rangle|T_4\rangle - |D\rangle|T_{E2}\rangle, \tag{9}$$

where $|T_1\rangle$, $|T_2\rangle$, $|T_3\rangle$, $|T_4\rangle$, $|T_{E1}\rangle$, and $|T_{E2}\rangle$ are given by

$$|T_1\rangle = \frac{1}{\sqrt{2}}\Big(\big(C+S\cos 2\alpha\big)|0\rangle_T + \big(C-S\cos 2\alpha\big)|1\rangle_T\Big) \tag{10}$$

$$|T_2\rangle = \frac{1}{\sqrt{2}}\Big(\big(C-S\cos 2\alpha\big)|0\rangle_T + \big(C+S\cos 2\alpha\big)|1\rangle_T\Big) \tag{11}$$

$$|T_3\rangle = \frac{1}{\sqrt{2}}\Big(\big(C+S\sin 2\alpha\big)|0\rangle_T + \big(C-S\sin 2\alpha\big)|1\rangle_T\Big) \tag{12}$$

$$|T_4\rangle = \frac{1}{\sqrt{2}}\Big(\big(C-S\sin 2\alpha\big)|0\rangle_T + \big(C+S\sin 2\alpha\big)|1\rangle_T\Big) \tag{13}$$

$$|T_{E1}\rangle = \frac{S}{\sqrt{2}}\sin 2\alpha\big(|0\rangle_T - |1\rangle_T\big) \tag{14}$$

$$|T_{E2}\rangle = \frac{S}{\sqrt{2}}\cos 2\alpha\big(|0\rangle_T - |1\rangle_T\big) \tag{15}$$

If Eve sets up her C-NOT gate with a rotation $\alpha = \frac{\pi}{8}$ from the $(H-V)$ basis, she has to wait Alice and Bob's comparison for their basis selections over a classical channel [13] to know exactly which state she has gotten $|H\rangle$ $(|V\rangle)$ or $|D\rangle$ $(|A\rangle)$. Whereas, for any rotation angle $\alpha \neq \frac{\pi}{8}$, using Eqs (6)-(9), Eve can share Alice and Bob in the same qubits without waiting the comparison will occur between them for their basis selections, but she can directly get the share qubits from her measurements using the distinguishing between $|T_1\rangle$, $|T_2\rangle$, $|T_3\rangle$, and $(|T_4\rangle)$ to obtain $|H\rangle$, $|V\rangle$, $|D\rangle$, or $(|A\rangle)$, respectively. Eve's information gain may cause an error whenever Alice and Bob choose a common basis and Eve's probe output states are $|T_{Ei}\rangle$, where $i=1,2$. For instance, if Alice sends Bob a state $|H\rangle$ and Bob uses the $(H-V)$ basis to measure, Eq. (6) will show that Alice and Bob get an error event when the measured output state is $|V\rangle|T_{E1}\rangle$. The probability that this will occur is $\langle|T_{E1}|T_{E1}\rangle = \frac{S^2}{2}\sin^2 2\alpha$

Now, we consider two special cases for the rotation angle α. In the first one, we assume that Eve sets up her

C-NOT gate in the same direction of the state $|H\rangle$ ($\alpha = 0$). In this case, $|T_{E1}\rangle = 0$, which means that when Alice sends Bob one of the states $|H\rangle$ or $|V\rangle$, Eve can break their connection to gain the same state, without making any perturbation for their measurements. Thus, for the rotation angle $\alpha = 0$, the probability for Eve to cause an error event whenever Alice and Bob choose the basis $(H-V)$ is zero. To do so, she just distinguishes between $|T_1\rangle$ and $|T_2\rangle$ by performing a projective measurements along $|0\rangle_T$ and $|1\rangle_T$, then Eve can correlate the measurement of $|0\rangle_T$ with $|T_1\rangle$ and $|1\rangle_T$ with $|T_2\rangle$. Hence, Eve needs only to distinguish between $|0\rangle_T$ and $|1\rangle_T$ which means that she does not need any quantum memory to measure her probe qubit. Unfortunately, in this case, we have gotten $|T_3\rangle = |T_4\rangle$. That means Eve can not distinguish between the states $|D\rangle$ and $|A\rangle$ as well as she makes error event for Alice and Bob if the measured out state is $|A\rangle|T_{E2}\rangle$ or $|D\rangle|T_{E2}\rangle$, i.e. Eve can not gain any information when Alice sends Bob using $(D-A)$ basis. In the second one, Eve sets up her C-NOT gate in the same direction of the state $|D\rangle$ ($\alpha = \frac{\pi}{4}$). In this case, we get $|T_{E2}\rangle = 0$ which means that Eve can share Alice and Bob for both states $|D\rangle$ and $|A\rangle$ without making any error event for the measurements of Alice and Bob. Eve can benefit from these two cases by comparing between them. Eve needs a device to tell her which basis is used by Alice to send Bob a photon. Then, Eve can define in which angle ($\alpha = 0$ or $\alpha = \frac{\pi}{4}$) she needs to set up her C-NOT gate. If Alice sends Bob using $(H-V)$ basis, Eve will set up her C-NOT gate in the same direction of $|H\rangle$ ($\alpha = 0$). Similarly, if Alice uses $(D-A)$ basis, Eve will set up her C-NOT gate in the direction of the state $|D\rangle$ ($\alpha = \frac{\pi}{4}$). Here, the most powerful point is that Eve can share Alice and Bob without making any disturbance, which means that Alice and Bob do not feel that Eve is eavesdropping.

3 Conclusion

Accordingly, when Eve sets up her C-NOT gate in the same direction of a basis, she can share Alice and Bob in qubits of this basis without making any error event for Bob's measurements, but she can not get any information about the other basis.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article

References

[1] C. H. Bennett. Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.*, **68**, 3121-3124, (1992)

[2] C. H. Bennett and G. Bassard. *Quantum Cryptography: Public key distribution and coin tossing*, Proc. of IEEE International Conference on Computers, Systems, and Signal Processing, Banglore, India, 175–179, (1984)

[3] S. Wiesner. Conjugate Coding, *ACM SIGACT News*, **15**, 78-88 (1983)

[4] B. C. Jacobs and J. D. Franson. Quantum cryptography in free space, *Opt. Lett.*, **21**, 1854-1856, (1996); W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. Peterson. Daylight Quantum Key Distribution over 1.6 km, *Phys. Rev. Lett.*, **84**, 5652-5655, (2000); R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night, *New J. Phys.*, **4**, 43.1-43.14, (2002); C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster and J. G. Rarity. A step towards global key distribution, *Nature*, **419**, 450-451, (2002)

[5] J. D. Franson and H. Ilves. Quantum cryptography using optical fibers, *Appl. Optics*, **33**, 2949-2954, (1994); C. Marand and P. D. Townsend. Quantum key distribution over distances as long as 30 km, *Opt. Lett.*, **20**, 1695-1697, (1995); R. J. Hughes, G. L. Morgan and C. G. Petrson. Quantum key distribution over a 48 km optical fibre network, *J. Mod. Opt.*, **47**, 533-547, (2000)

[6] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Phys. Rev. Lett.*, **85**, 441-444, (2000); D. Mayers. Unconditional security in quantum cryptography, *J. ACM*, **48**, 351-356, (2001); H.-K. Lo. A simple proof of the unconditional security of quantum key distribution, *J. Phys.* A, **34**, 6957-6967, (2001)

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. Experimental quantum cryptography, *Journal of Cryptology*, **5**, 3–28, (1992); C.H. Bennett, G. Brassard, C. Crepeau and U.M. Maurer. Generalized privacy amplification, *IEEE Trans. Inf. Theory*, **41**, 1915-1923, (1995)

[8] B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao and Y. Fainman. Effect of channel imperfection on the secrecy capacity of a quantum cryptographic system, *J. Mod. Opt.*, **44**, 953-961, (1997); G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders Limitations on Practical Quantum Cryptography, *Phys. Rev. Lett.*, **85**, 1330-1333, (2000); V. Makarov and D. R. Hjelme. Faked states attack on quantum cryptosystems, *J. Mod. Opt.*, **52**, 691-705, (2005).

[9] Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim. Effects of depolarizing quantum channels on BB84 and SARG04 quantum cryptography protocols, *Laser Physics*, **21**, 1438-1442, (2011)

[10] R. Loura, A. J. Almeida, P. Andre, A. N. Pinto, P. Meteus, and C. N. Paunkovic. Noise and measurement errors in a practical two-state quantum bit commitment protocol, *Phys. Rev.* A, ' **89**, 052336(1-15), (2014)

[11] H. Abdel-Hameed, N. Zidan, and M. R. Wahiddin. The Probe Attack on the Bennett-Brassard 1984 Protocol in the Presences of Noisy Amplitude Damping Channel, *Int. J. Theor. Phys.*, **56**, 2231-2242, (2017)

[12] C. A. Fuchs and A. Peres. Quantum-state disturbance versus information gain: Uncertainty relations for quantum information, *Phys. Rev.* A, **53**, 2038-2045, (1996)

[13] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman. Security of quantum cryptography against individual attacks, *Phys. Rev.* A, **57**, 2383-2398, (1998)

[14] H. E. Brandt. Quantum-cryptographic entangling probe, *Phys. Rev.* A, **71**, 042312(1-14), (2005)

[15] J. H. Shapiro and F. N. C. Wong. Attacking quantum key distribution with single-photon two-qubit quantum logic, *Phys. Rev.* A, **73**, 012315(1-7), (2006)

[16] T. Kim, I. S. Wersborg, F. N. C. Wong, and J. H. Shapiro. Complete physical simulation of the entangling-probe attack on the Bennett-Brassard 1984 protocol, *Phy. Rev.* A, **75**, 042327(1-5), (2007)

[17] M. Fiorentino and F. N. C. Wong. Deterministic Controlled-NOT Gate For Single-Photon Two-Qubit Quantum Logic, *Phys. Rev. Lett.*, **93**, 070502(1-4), (2004)

[18] M. Fiorentino, T. Kim, and F. N. C. Wong. Single-photon two-qubit SWAP gate for entanglement manipulation, *Phys. Rev.* A, **72**. 012318(1-4), (2005)

H. F. Abdel-Hameed received the PhD degree in Quantum Mechanics at Sohag University. His research interests are in the areas of Quantum Mechanics, Quantum information and quantum optics. He has published research articles in reputed international journals of mathematical and theoretical physics.