RESEARCH ARTICLE | JANUARY 08 2020

Security of B92 protocol with uninformative states in asymptotic limit with composable security

N. Ali ✉; N. A. N. Mat Radzi; S. A. Aljunid; R. Endut

AIP Conf. Proc. 2203, 020049 (2020)
https://doi.org/10.1063/1.5142141

Security of B92 protocol with uninformative states in asymptotic limit with composable security

N. Ali[2, a)], N.A.N. Mat Radzi [1, b)], S. A. Aljunid[2], R. Endut[2]

[1] *School of Microelectronic Engineering, Universiti Malaysia Perlis, 02000 Arau, Perlis, Malaysia*
2Advanced Communication Engineering, Centre of Excellence, Universiti Malaysia Perlis, 02600 Arau, Perlis, Malaysia.

[a)] Corresponding author: norshamsuri@unimap.edu.my
[b)]nainaradzi@gmail.com.my

Abstract. The security of the Quantum Key Distribution (QKD) is coming from the fundamental principle of quantum physic where any action on the quantum system that tries to extract the information will be considered generally as a measurement which basically will modify the system. The protocol of B92 has been proven unconditionally secure by various of study based on the entanglement distillation protocol (EDP) technique. However, based on this technique it does not prove composable security which is actually important in privacy amplification in order to guarantee the partial key shared cannot revoke the security of the system. We review the security analysis of this system and its implementation in this work.

INTRODUCTION

Quantum Cryptography is one of the vast disciplined fields in Quantum Information which actually one of the techniques being used to reduce the vulnerability of the emergence quantum computer. Even it is long to see the quantum computer for really solve the encryption problems, as for example RSA cryptography. RSA is based on factorizing problems whereas updated no classical system can solve polynomial speed up unless it is exponential which is untraceable. This is because in 1994 Peter Shor's [3] introduce the quantum algorithm which can solve the factoring and discrete logarithm problem in polynomial of time. This rebukes the security of classical cryptography even its implementation is way far as technologies go on. The RSA cryptography is based on the public key cryptography which the factoring number is being exposed publicly and the hidden only private key that can unlock back the encrypted message. However, this security is only valid if the large prime number cannot be calculated by the classical computer in polynomial time. Thus, the security is vulnerable if exist computer power which can compute very fast this problem. The most famous method of the encryption system is one-time pad that previously being used in the World War 2 and Enigma is one of the examples of the implementation one-time pad cryptography. The security of Enigma is unbreakable until World War 2 finishes since the encryption is based on the mechanical machine which produces random events for the encrypted. As in the quantum cryptography the randomness is given by the quantum effect which naturally random in nature.

The first idea of implementation quantum cryptography was in 1984 which was proposed by Bennett and Brassad [4] where thery used two orthogonal states to decode the digital classical data. The keys are generated based on the protocol called BB84. In the protocol, they produce four types of states to represent the digital coded which correspond to a key that can be generated based on the protocol. The state of this protocol can be any quantum state. One basis

The 2nd International Conference on Applied Photonics and Electronics 2019 (InCAPE 2019)
AIP Conf. Proc. 2203, 020049-1–020049-7; https://doi.org/10.1063/1.5142141
Published by AIP Publishing. 978-0-7354-1954-4/$30.00

can consist two polarization states, for example, $|H>,\ |V>, |45^{\circ}>, |135°>$. The protocol of the system encoded as below:
Horizontal basis

$$|H> \Rightarrow \text{"0"} \tag{1}$$

$$|V> \Rightarrow \text{"1"} \tag{2}$$

Diagonal basis

$$|D> \Rightarrow \text{"0"} \tag{3}$$

$$|A> \Rightarrow "1" \tag{4}$$

$$|D> = \frac{1}{\sqrt{2}}[|V> + |H>] \tag{5}$$

$$|A> = \frac{1}{\sqrt{2}}[|V> - |H>] \tag{6}$$

These four states satisfy the following relationship

$$< H|V> = < A|D> = 0 \tag{7}$$

$$< H|H> = < V|V> = < A|A> = < D|D> = 1 \tag{8}$$

$$[< H|A >]^2 = [< H|D >]^2 = [< V|A >]^2 = [< V|D >]^2 = \frac{1}{2} \tag{9}$$

The main security on the quantum system relies on the physical properties of the quantum system but in classical cryptography the security relies on the complexity which currently still in class of NP problem [5] that intractable for classical computer. Thus, quantum cryptographic gives advanced security protection which in nature cannot be hacked.

A. Bennett 1992 (B92) protocol

The Bennett 1992 [6] or B92 protocol is a Quantum Key Distribution (QKD) protocol basically the simplest version of BB84 protocol which using two nonorthogonal states. The protocol utilizes the Heisenberg uncertainty which used two nonorthogonal states. The protocol used the state $|H>$ in equation (1) as digital bit 1 and the state $|D>$ in equation (3) as digital bit 0. The state of the $|H>$ can also be represented as $|0>$ and state $|D>$ represented as $|+>$. Both of the states are on different bases which state $|0>$ is in rectilinear and $|+>$ on diagonal basis. Alice will send these two states and Bob will randomly measure the two bases. Bob will announce either conclusive or inconclusive outcomes after the measurement. The conclusive outcomes represent the measurement result which is orthogonal to the sending states since it is deterministically known.

As for general we can represent the qubit of B92 protocol as [7], [11]

$$|\varphi_j> = \beta|0_x> + (-1)^j \alpha|1_x> \tag{10}$$

Where $j = \{0,1\}, \{|0_x>, |1_x>\}$ are the eigenstates of the X basis and

$$\beta = cos\frac{\theta}{2}, \alpha = sin\frac{\theta}{2} \tag{11}$$

The B92 states are nonorthogonal states which $0 < \theta < \pi/2$. The X basis in the equation (11) is related to Z basis by $|j_z \geq = 1/\sqrt{2}[|0_x > +(-1)^j|1_x >]$. As mentioned previously the conclusive outcomes are represented by the orthogonal states that prepared by Alice thus the orthogonal state is $|\varphi_j >$ as in equation (10) is:

$$\left|\overline{\varphi_j}\right> = \beta\left|0_x\right> - (-1)^j \alpha |1_x > \tag{12}$$

The states prepared by Alice can also be represented by a density matrix ρ_A as below [11]:

$$\rho_A = \frac{|\varphi_0 >< \varphi_0| + |\varphi_1 >< \varphi_1|}{2} \tag{13}$$

$$= \beta^2 |0_x >< 0_x| + \alpha^2 |1_x >< 1_x| \tag{14}$$

Information decoded by Bob in the basis of $B_k = \{\varphi_k, \overline{\varphi_k}\}$, where $k = \{0,1\}$ and the outcome of the measurement either $|\varphi_k >$ or $|\overline{\varphi_k} >$. Moreover, if we consider straight nonorthogonal, we can show that $|\varphi_0 >$ in diagonal basis and $|\varphi_1 >$ in a rectilinear basis. Bob's message will encode as $j = k \oplus 1$ where "$\oplus$" is addition modular 2 and the conclusive outcome if the Bob result is $|\overline{\varphi_k} >$.

I. B92 Security

The B92 protocol QKD system has been proven "unconditional security" by Kiyoshi [1] over the lossy channel and noisy channel and also in the loss-free channel [2]. These papers have proven technique of entanglement distillation protocol (EDP). In addition, it was shown that the EDP has to be reduced to the B92 protocol which then followed by showing that EDP is successful proven unconditional security. As simplification, the preparation of the state by Alice in B92 protocol is considered as measurement of Alice on entanglement state on Z basis after she prepared. The measurement of the Bob in the B92 protocol can be shown as the local filtering and immediately Z basis measurement after that. Another important point in the security is the number of errors and number of filter pairs pass the filtering process is using to calculate the bit errors and phase errors respectively[1,2]. The details of security in [1] and [2] were used as the references in this study.

II. Unambiguous State Discrimination (USD)

Unambiguous state discrimination (USD) is one of the vulnerable attacks to the B92 protocol [7,8]. This attack is purposely for the weak coherent states in which the number of photons is distributed according to Poison distribution, as we can see the state equation can be described by the density matrix [9].

$$\rho = e^{-\mu} \sum_n \frac{\mu^n}{n!} |n >< n| \tag{15}$$

There are a few parameters which can be said the USD attacked is failed to acquire the information [9]. This is the parameter that QKD system is secured where the value of the transmission efficiency and also the detector efficiency should be $\eta_L \eta_B \geq 1 - 2^{-1/2}$ and the $\mu < \mu_2$ where μ_2 mention as below

$$\mu_2 = \frac{-2}{\eta_L \eta_B} \ln\left(\frac{4 - 3\eta_B}{4 - \eta_B}\right) \tag{16}$$

At the event of the more loss in the system, QKD system can be secured from USD attacked where the value $F > 0$ and μ value should maintain as $\mu < \mu_2$ and F is given as:

$$F \approx \eta_B^2 \left(\eta_L \mu - \frac{1}{2}\eta_L^2 \mu^2 - P_D\right) \tag{17}$$

where P_D discrimination probability is given as below:

$$P_D = 1 - e^{-\mu}\left(\sqrt{2}sinh\frac{\mu}{\sqrt{2}} + 2cosh\frac{\mu}{\sqrt{2}} - 1\right) \tag{18}$$

The μ_2 is normal practical value is always $\mu \geq 1$ which if we compare to some of the other attacks such as Photon Number Splitting (PNS) attack [10] that give μ value as $\mu = \eta_L/g_2$ where η_L is the transmission of the system given by equation (19) and $g = 1$ for Poisson source and $g < 1$ for sub-Poisson source,

$$\eta_L = 10^{-\alpha d/10} \tag{19}$$

where α is the attenuation coefficient and d is transmission distance. The value of μ is only secured when the visibility $V > 0.8$. The other practical attacked regarding the detector blinding has been reported previously [11].

III. B92 with two nonorthogonal states and uninformative states

The modification of B92 protocol made by Lucamarini *et al.* [12] increased the performance of the protocol which previously known as susceptible to the noises especially for the B92 single photon states. B92 protocol has few other variations which utilize the proposed method [6]. However, we only go through two protocols which are SARG04 protocol [13] which proposed to countermeasure the PNS attack and $4 + 2$ protocol [14] which is the old protocol that proposed to increase the security protocol against the same PNS attack but maintain the strong reference pulse for intercept resend attacks [16]. The interesting part is the $4 + 2$ protocol giving the link to most of the other modified B92 protocols [8], [9], [12].

The implementation of two uninformative states differs from the $4 + 2$ protocol which the two uninformative states are orthogonal to each other [8], [15]. The protocol for the two nonorthogonal and uninformative can be represented as below:

The protocol consists of seven steps as following:

i. Alice prepares signal states $|\varphi_j>$ which $j = \{0,1\}$ is randomly and uniformly for $2N$ signal qubits. She also prepares uninformative states as $|\varphi_d>$ for $\alpha^2 N$ qubits and $|\varphi'_d>$ for $\beta^2 N$ qubits.

ii. Bob executes randomly the measurement $\mathcal{M}_{B92}^{\beta}$ with probability $1/2$ and another $1/2$ probability for the X basis and the outcomes are recorded. In the case of $|v>$ is obtain then vacuum is recorded, if $|\varphi_0>$ or $|\varphi_1>$ is obtain then inconclusive outcome is recorded and if $|\overline{\varphi_0}>$ or $|\overline{\varphi_1}>$ is obtain then "1" and "0" is recorded respectively for the measurement $\mathcal{M}_{B92}^{\beta}$ basis. As for the X basis measurement $|0_x>$ or $|1_x>$ is recorded.

iii. After Alice finishes sending the $2N$ signal qubits for $|\varphi_j>$, $\alpha^2 N$ qubits for $|\varphi_d>$ and $\beta^2 N$ qubits for $|\varphi'_d>$; Bob will announce the vacuum, conclusive, inconclusive and X basis measurement. Then, Alice announced the measurement of Bob X basis which corresponding and not corresponding to her preparation. That preparation which not correspondent to Alice preparation and Bob measurement in X basis is discarded. The other bits with correspondent to Bob measurement $\mathcal{M}_{B92}^{\beta}$ basis; value n_{kv} of joint occurrences $\{|\overline{\varphi_k}>, |v>\}$ $(k = \{0,1,d,d'\})$ is estimated by Alice and announced to the Bob. Data for the inconclusive outcomes are removed.

iv. Bob estimates the number of phase errors n_{ph} for the uninformative qubits sending by Alice where she prepared $|0_x>$ or $|1_x>$ and he measured $|1_x>$ or $|0_x>$ respectively.

v. The first half of remaining bits on the measurement $\mathcal{M}_{B92}^{\beta}$basis is used for estimating the number of bits errors n_{err} in which Alice prepare $|\varphi_0>$ or $|\varphi_1>$ and Bob decoded as "1" or "0" respectively.

vi. From the n_{err}user estimate the number of bits errors n_{bits}.

vii. The user performs the error correction and privacy amplification on data bits according to the value of n_{bits} and obtaining the shared secret key n_{key} for both parties.

IV. The security for two nonorthogonal and uninformative states

The security of the nonorthogonal and uninformative states [1,2] was employed followed with some addition on two uninformative qubits. The value of n_{1v} of joint occurrence $\{|1_x>, F_v\}$ for phase estimation is given below [12]:

$$n_{ph} = \beta^2 n_{01} + \alpha^2 n_{10} \tag{20}$$

$$\alpha^2 N = n_{10} + n_{11} + n_{1v} \tag{21}$$

This n_{1v} is shown in EDP with actually similar to the n_{dv}in the prepared and measured (PM) technique for two nonorthogonal and uninformative states. By showing the EDP is successfully proven unconditionally secure then the technique is said unconditional security [12]. n_{1v} also, being used to improved further the phase error estimation and thus improved the working distance of the system. We refer the detailed security [16] and numerical analysis of the improved version utilizing the $\{|0_x>, |1_x>\}$ as uninformative qubits.

RESULTS AND DISCUSSION

As we refer back to the initial state of B92 protocol given by equation (10) and density matrix in equation (14), we can deduce the state that sent by Alice and received by Bob. Based on [2], we can estimate the error rate base on the bit error where N bits are used to compare the measurement of the Alice on Z basis and Bob measurement on $\mathcal{M}_{B92}^{\beta}$ basis. Based on equation (20) and equation (21), if we consider the lossless environment, then n_{1v} can be considered 0 and equation (21) can refer the value determined the nonorthogonality where $n_{10} + n_{11}$ is equal to $\alpha^2 N$. This value actually shows that Alice has full access to her qubits send. In case of lossless channel, the probability is measured based on the paper [2]. As shown in equation (14), for the lossless channel the states are measured based on positive operator value measure (POVM) as below:

$$\mathcal{F}_0 = \frac{|\overline{\varphi_1}><\overline{\varphi_1}|}{2} \tag{22}$$

$$\mathcal{F}_1 = \frac{|\overline{\varphi_0}><\overline{\varphi_0}|}{2} \tag{23}$$

$$<\varphi_0|\mathcal{F}_0|\varphi_0> = 2\alpha^2\beta^2 \tag{24}$$

$$<\varphi_0|\mathcal{F}_1|\varphi_0> = 0 \tag{25}$$

$$<\varphi_1|\mathcal{F}_0|\varphi_1> = 0 \tag{26}$$

$$<\varphi_1|\mathcal{F}_1|\varphi_1> = 2\alpha^2\beta^2 \tag{27}$$

$$\mathbb{A}_{PM} = \frac{1}{2}\left(<\varphi_j|\mathcal{F}_0|\varphi_j> + <\varphi_j|\mathcal{F}_1|\varphi_j>\right) \tag{28}$$

$$= 2\alpha^2\beta^2 \tag{29}$$

As for the noiseless channel, we consider the reduction argument from the EDP and by referring to the paper [2], the main operator in the EDP which is $\mathcal{F}_{fill}$ was introduced as below. By applying the trace on the measurement, we can get the probability of states after applying the filter.

$$\mathcal{F}_{fill} \equiv \alpha|0_x>_B<0_x| + \beta|1_x>_B<1_x| \tag{30}$$

$$Tr\left[\left(I_A \otimes \mathcal{F}_{fill}\right)\rho_{AB}\left(I_A \otimes \mathcal{F}_{fill}\right)\right] = 2\alpha^2\beta^2 \tag{31}$$

In case the state has depolarization channel as mention in [2] where $\rho \to \varepsilon(\rho) = (1-p)\rho + p/3\sum_{a=x,y,z}\sigma_a\rho\sigma_a$ then the probability of getting the state change to become $2\alpha^2\beta^2 - 2\alpha^2\beta^2 + \frac{p}{2}$. Then if we consider individual errors such bit errors and phase errors, which are given by $n_{err} = \alpha^4 + \beta^4 - 2\alpha^2\beta^2$ and $n_{ph} = 4\alpha^4 + 4\beta^4$respectively actually reduce the bits successful sending to Bob. The bits errors can be determined when the Alice measure in the Z basis and Bob measure in the $\mathcal{M}_{B92}^{\beta}$ in PM protocol which actually similar to Z basis measurement followed by the filtering operation in EDP [1, 2, 12]. In order to determine the phase errors in the normal B92 protocol it is not measurable since there is no measurable basis is done on the X basis which corresponds to the phase errors. The strategy by assuming the Gedanken measurement in which not available in protocol but able to generate the value of phase error. The number of phase errors could be determined if Alice and Bob measure in X basis measurement just after done the local filtering $\mathcal{F}_{fill}$ for N pairs qubits that share by Alice to Bob.

CONCLUSION

In this paper, we have reviewed the security analysis by previous works [1], [2] and [12] with the implementation of uninformative states into the protocol. As depicted in Fig. 1, we show the error rate with normalized to the n_{fill} and the effect with the nonorthogonal states between two signal states.

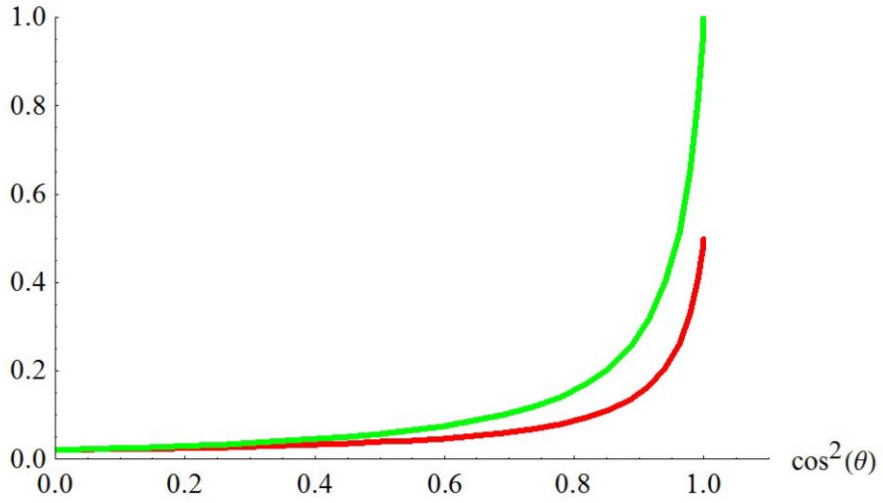

FIGURE 1. The error rate with normalized to the n_{fill} with respect to the nonorthogonal of two states. The value of p is fixed into p = 0.03. (Green line) The phase errors as in the nonorthogonal value $\frac{p}{6}(3 + \cos 2\theta)$ solving from the equation n_{ph} phase and (Redline), the bit errors as in nonorthogonal value is $p/3$ solving from the equation n_{err}.

The error estimation increases as the angle between the two nonorthogonal states increase with show that signal states is more vulnerable to the noise. The bit errors should be increased to maximum probability 0.5 where the state is orthogonal each other. This actually shows that phase error estimation will become worse in the large angle of nonorthogonality. This gives advantage to the two uninformative states which can estimate the phase errors directly.

ACKNOWLEDGMENTS

The authors acknowledge financial support by the School of Microelectronic Engineering, Universiti Malaysia Perlis (UniMAP. NA also acknowledges financial support by Universiti Malaysia Perlis Internal Grant 9007-00186.

REFERENCES

1. Kiyoshi Tamaki and Nobert Ltkenhaus; Unconditionally Security of the Bennett 1992 quan- tum key-distribution over lossy and noisy channel; Phys. Rev. A 69, 032316 (2004).
2. K. Tamaki, M. Koashi, and N. Imoto; Unconditionally Secure Key Distribution Based on Two Nonorthogonal States; Phys. Rev. Lett. 90, 167904 (2003).
3. Peter W. Shor; Polynomial-Time Algorithm for Prime Factorization and Discreate Logarithms on a Quantum Computer; Proc. of 35th Anual Symposium on the Foundations of Computer Science, (IEEE Computer Society Los Alamitos), p.124,1996.
4. Bennett, C.H., and Brassard, G., Quantum cryptography: Public key distribution and coin tossing, Proc. Int. Conf. Comput. Syst. Signal Process, Bangalore, 1984, pp. 175-179.
5. Micheal A. Nielsen and Issac L. Chuang; Quantum Computation and Quantum Information; Cambridge University Press; 2000.
6. Charles H. Bennett; Quantum crytography using two any two nonorthoganal states; Physical Rev. Letters. vol 68. 3121 (1992).
7. M. Dusek, N. Lutkenhaus, M. Hendrych; Quantum Crytography; Progress in Optics, vol. 49, Edt. E. Wolf (Elsevier, 2006), pp. 381-454.
8. K. Tamaki, N. Ltkenhaus, M. Koashi, J. Batuwantudawe; Unconditional security of the Bennett 1992 quantum key-distribution scheme with strong reference pulse; Phys. Rev. A 80 032302 (2009).
9. M. Dusek, M. Jahma, N. Ltkenhaus; Unambiguous state discrimination in quantum cryptography with weak coherent states. Physical Review A, Vol. 62, 022306 (2000).
10. A. Niederberger, V. Scarani, and N. Gisin; Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography; Phys. Rev. A 71, 042316 (2005).
11. Norshamsuri Ali; "Avoiding Vadim Makarov attack on the Single Photon Detector", arXiv preprint arXiv:1909.04805 (2019).
12. M. Lucamarini; G. D. Giuseppe, K. Tamaki; Robust unconditionally secure quantum key distribution with two nonorthogoanl and unimformative states; Physical Review A 80,032327 (2009).
13. V. Scarani, A. Acn, G. Ribordy, and N. Gisin; Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations; Phys. Rev. Lett. 92, 057901 (2004).; A. Acn, N. Gisin, and V. Scarani; Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks; Phys. Rev. A 69, 012309 (2004).
14. B. Huttner, N. Imoto, N. Gisin, T. Mor; Quantum cryptography with coherent states; Phys. Rev. A 51, 18631869 (1995).
15. M. Lucamarini, G. Vallone, I. Gianani, G. Di Giuseppe, P. Mataloni; Device-independent entanglement-based Bennett 1992 protocol; arXiv:1111.1997v2 (2011).
16. Kiyoshi Tamaki; Unconditionally secure quantum key distribution with relatively strong signal pulse; Phys. Rev. A 77, 032341 (2008).