NANOSYSTEMS: PHYSICS, CHEMISTRY, MATHEMATICS, 2019, 10 (4), P. 398–401

Analysis of the unambiguous state discrimination with unequal a priori probabilities

A. A. Gaidash, S. S. Medvedeva, G. P. Miroshnichenko

ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia

andrewdgk@gmail.com, mdvdv.svt@gmail.com

PACS 42.50.Dv **DOI 10.17586/2220-8054-2019-10-4-398-401**

In this paper, we study unambiguous state discrimination regarding advanced attack on phase-coded quantum key distribution protocol. We propose the method of optimal unambiguous state discrimination probability derivation as a function of *a priori* probabilities for signal states. The expression obtained as an example in case of two signal states explicitly demonstrates the additional term dependent on small deviations from equal *a priori* probabilities that may take place in real quantum key distribution implementations. Precise estimation of optimal unambiguous state discrimination probability is significant for complete evaluation of quantum key distribution security.

Keywords: quantum key distribution, unambiguous state discrimination.

Received: 13 May 2019

Revised: 28 June 2019

1. Introduction

Throughout the last few decades the field of quantum cryptography has been rapidly developing and advancing. It has emerged with the first papers [1, 2] dedicated to the descriptions of protocols which allow secure distribution of a finite bit sequence between legitimate partners, and it is still in the focus of research groups, for instance [3–5]. Not only the protocols are of special interest, but also different types of attacks are studied in order to find successful countermeasures.

In this work we would like to concentrate on zero-error unambiguous state discrimination (USD) attack that is a considerable threat for protocols utilizing weak coherent states. USD attack requires eavesdropper (Eve) tapping into quantum channel of legitimate parties (Alice and Bob), errorlessly measuring the states and resending the modified states to Bob in order to preserve detection statistics [6]. We explore the phase-coded protocol which utilizes several pairs weak coherent states sent with unequal *a priori* probability. Imperfect state preparation that can result in the sending probabilities' inequality is the immanent part of every practical set-up. For example, quantum random number generator may cause unequal probability of state preparation [7–9]. Hence we examine the influence of unequal *a priori* probability on the discrimination probability.

USD measurement is subject of research for almost three decades. General approach to discrimination between linearly independent states was introduced in [10, 12, 13]. The solution for minimum achievable probability of inconclusive outcome for three states was given by [11]. The method of minimizing the probability for N symmetric states was considered in [12]. The special case of equal *a priori* probabilities for N states was discussed in [13]. Bounds of unambiguous state discrimination probabilities have been studied for the case of N linearly independent states in [14–16]. Several approaches to numerical optimization were proposed as well in [16, 17]. Implementations of USD in field of quantum computations also take place, e.g. for purpose of quantum cloning operation [18] or USD between oracle operators [19].

2. Method description

To perform unambiguous discrimination of the N signal states $|f_i\rangle$ Eve determines special positive-operator valued measure (POVM). It consists of projection operators $\hat{A}_i$ which are related to probabilities of successful state discrimination P_i (for each state) and operator $\hat{A}_0$ that is related to obtaining inconclusive result which is always present due to the nonorthogonality of the states and introduced in order to make the sum of the projection operators satisfy the decomposition of the identity:

$$\sum_{i=0}^{N} \hat{A}_i = \hat{I}. \tag{1}$$

Extracted from (1) the operator $\hat{A}_0$ is expressed as:

$$\hat{A}_0 = \hat{I} - \sum_{i=1}^{N} \hat{A}_i, \tag{2}$$

and according to [11] $\hat{A}_0$ is subject to condition:

$$\det[\hat{A}_0] = 0. \tag{3}$$

The latter provides maximal allowed values for probabilities P_i. We specify operators $\hat{A}_i$ as follows:

$$\hat{A}_i = P_i \left|v_i\right\rangle \left\langle v_1\right|, \tag{4}$$

where $|v_i\rangle$ is state that forms biorthogonal basis with the signal states $|f_i\rangle$ (i.e. $\langle v_i|f_j\rangle = \delta_{ij}$, where δ_{ij} is Kronecker delta).

Thus one needs to optimize the average probability of USD:

$$P = \sum_{i=1}^{N} p_i P_i, \tag{5}$$

where p_i is *a priori* probability of sending each state. One may use Lagrange multiplier method in order to do so. Hence, the function to be optimized is P from expression (5) and the following expression is bound [11]:

$$\det \hat{A}_0 = \det \left(\hat{I} - \sum_{i=1}^{2N} P_i |v_i\rangle\langle v_i| \right) = 0. \tag{6}$$

Let us introduce orthogonal basis $|u_i\rangle$ obtained by, for instance, Gram–Schmidt process. For simplicity let us denote matrix of the operator $\hat{A}_0$ (inconclusive result) as A in this orthonormal basis, and operators $|v_k\rangle\langle v_k|$ as $V^{(k)}$ respectively.

Thus system of equations is as follows:

$$\begin{gathered} \frac{d}{dP_n} \sum_{k=1}^{N} p_k P_k - \lambda \frac{d}{dP_n} \det A = 0, \\ \det A = 0, \end{gathered} \tag{7}$$

where λ is Lagrange multiplier. Insofar as

$$\frac{d}{dP_n} \det(A) = \operatorname{Tr}\left(\operatorname{adj}(A) \frac{d}{dP_n} \left(I - \sum_{k=1}^{N} P_k V^{(k)} \right) \right) = \operatorname{Tr}\left(- \operatorname{adj}(A) V^{(n)} \right), \tag{8}$$

where, $\operatorname{Tr}(X) = \sum_i X_{ii}$ is trace of arbitrary matrix X, $\operatorname{adj}(A)$ is adjoint matrix of matrix A, I is identity matrix, hence

$$\begin{gathered} p_n + \lambda \operatorname{Tr}\left(\operatorname{adj}(A) V^{(n)} \right) = 0, \\ \det A = 0. \end{gathered} \tag{9}$$

Since sum of p_i is equal to unit than Lagrange multiplier is as follows:

$$\lambda = - \frac{1}{\operatorname{Tr}\left(\operatorname{adj}(A) \sum_k V^{(k)} \right)}, \tag{10}$$

and consequently p_i is expressed as

$$p_i = \frac{\operatorname{Tr}\left(\operatorname{adj}(A) V^{(i)} \right)}{\operatorname{Tr}\left(\operatorname{adj}(A) \sum_k V^{(k)} \right)}. \tag{11}$$

One needs to derive P_i as function p_i in order to obtain expression of optimal USD as function of p_i.

3. Example

As an example let us consider two signal states. Their overlapping is denoted as B. Thus signal states can be described in terms of orthonormal basis (obtained by Gram–Schmidt process) as follows:

$$|f_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |f_2\rangle = \begin{pmatrix} \dfrac{-B}{\sqrt{1-B^2}} \\ \dfrac{1}{\sqrt{1-B^2}} \end{pmatrix}. \tag{12}$$

Considering

$$|v_1\rangle = \begin{pmatrix} 1 \\ \dfrac{-B}{\sqrt{1-B^2}} \end{pmatrix}, \quad |v_2\rangle = \begin{pmatrix} 0 \\ \dfrac{1}{\sqrt{1-B^2}} \end{pmatrix}, \tag{13}$$

condition (6) may be derived in the following form:

$$\det \hat{A}_0 = \det \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 1 & \dfrac{-B}{\sqrt{1-B^2}} \\ \dfrac{-B}{\sqrt{1-B^2}} & \dfrac{B^2}{1-B^2} \end{bmatrix} P_1 - \begin{bmatrix} 0 & 0 \\ 0 & \dfrac{1}{1-B^2} \end{bmatrix} P_2 \right)$$

$$= \det \begin{bmatrix} 1-P_1 & \dfrac{BP_1}{\sqrt{1-B^2}} \\ \dfrac{BP_1}{\sqrt{1-B^2}} & \dfrac{1-B^2-B^2P_1-P_2}{1-B^2} \end{bmatrix} = \frac{1-B^2-P_1-P_2+P_1P_2}{1-B^2} = 0, \tag{14}$$

thereby the probability P_1 can be denoted as

$$P_1 = \frac{1-B^2-P_2}{1-P_2}. \tag{15}$$

Lagrange multiplier is as follows:

$$\lambda = \frac{1-B^2}{(P_1+P_2)-2}, \tag{16}$$

and probabilities p_1 and p_2 are as

$$p_1 = \frac{1-P_2}{2-(P_1+P_2)}, \tag{17}$$

$$p_2 = \frac{1-P_1}{2-(P_1+P_2)}. \tag{18}$$

By substituting expression (15) in expression (17) we find

$$p_1 = \frac{(1-P_2)^2}{(1-P_2)^2+B^2}, \tag{19}$$

and consequently:

$$P_2 = 1 - B\sqrt{\frac{p_1}{1-p_1}} = 1 - B\sqrt{\frac{p_1}{p_2}}. \tag{20}$$

Taking into account symmetry of expressions (15), (17), (18) with respect to P_1 and P_2 following expression for P_1 is derived analogously:

$$P_1 = 1 - B\sqrt{\frac{p_2}{p_1}}. \tag{21}$$

By substituting expressions (20) and (21) in (5) we obtain optimized USD probability:

$$P = p_1\left(1 - B\sqrt{\frac{p_2}{p_1}}\right) + p_2\left(1 - B\sqrt{\frac{p_1}{p_2}}\right) = 1 - 2B\sqrt{p_1p_2}. \tag{22}$$

This result has well-known form [11] if $p = p_1 = p_2 = \dfrac{1}{2}$. Defining $p_1 = \dfrac{1}{2} + \Delta p$ and $p_2 = \dfrac{1}{2} - \Delta p$, where Δp is considerably small deviation from equal *a priori* probabilities, we get

$$P = 1 - 2B\sqrt{\left(\frac{1}{2} + \Delta p\right)\left(\frac{1}{2} - \Delta p\right)} \approx 1 - B + 2B(\Delta p)^2. \tag{23}$$

Therefore, the value of P has quadratic term dependent on small deviations from equal *a priori* probabilities.

4. Discussion and conclusion

In this work we analyze the probability of unambiguous discrimination for arbitrary number of states with unequal *a priori* probabilities. The proposed method provides system of equations (expressions (11) and (3)) that can be solved in order to find optimized USD probability as function of *a priori* probabilities. We consider rather simple and well-studied example for two states; the result is the same as in [20]. However, the authors of that paper obtain result only for two states. Concerning the method described in this paper it is unfortunate that the amount of calculations for higher number of states grows rapidly so it might be rather difficult to obtain analytical expressions similar to expression (22).

The results are important mostly in the field of quantum key distribution. In order to achieve certain level of security, one should consider various attacks, estimate probabilities of their success, and apply corresponding countermeasures to them. Thus estimation of optimal USD probability is crucial for bounding Eve's information during, for instance, advanced USD attack [6]. However consideration of an ideal case is not enough in this instance since there is an additional quadratic term related to slightly unequal (e.g. due to the bias in quantum random number generator) *a priori* probabilities in expression (23) that might provide additional information to Eve. Precise estimation of optimal USD probability is a significant step towards complete evaluation of quantum key distribution security.

Acknowledgements

This work was financially supported by the Ministry of Education and Science of Russian Federation (contract No. 03.G25.31.0229).

References

[1] Bennett C.H., Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of "International Conference on Computers, Systems and Signal Processing"*, Bangalore, India, 09.12.1984, P. 17.
[2] Ekert A. Quantum cryptography based on Bell's theorem. *Physical review letters*, 1991, **67** (6), P. 661–663.
[3] Vazirani U., Vidick T. Fully device independent quantum key distribution. *Communications of the ACM*, 2019, **62** (4), P. 133–133.
[4] Minder M., Pittaluga M., et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics*, 2019, **13**, P. 334–338.
[5] Razavi M., Leverrier A., et al. Quantum key distribution and beyond: introduction. *JOSA B*, 2019, **36** (3), P. QKD1–QKD2.
[6] Ko H., Choi B.S., Choe J.S., Youn C.J. Advanced unambiguous state discrimination attack and countermeasure strategy in a practical B92 QKD system. *Quantum Information Processing*, 2018, **17** (17), P. 1–14.
[7] Ivanova A.E., Chivilikhin S.A., Gleim A.V. Quantum random number generator based on homodyne detection. *Nanosystems: Physics, Chemistry, Mathematics*, 2017, **8** (2), P. 239–242.
[8] Ivanova A.E., Chivilikhin S.A., Gleim A.V. The use of beam and fiber splitters in quantum random number generators based on vacuum fluctuations. *Nanosystems: Physics, Chemistry, Mathematics*, 2016, **7** (2), P. 378–383.
[9] Ivanova A.E., Egorov V.I., Chivilikhin S.A., Gleim A.V. Investigation of quantum random number generation based on space-time division of photons. *Nanosystems: Physics, Chemistry, Mathematics*, 2013, **4** (4), P. 550–554.
[10] Barnett S.M., Croke S. Quantum state discrimination. *Advances in Optics and Photonics*, 2009, **1** (2), P. 238–278.
[11] Peres A., Terno D.R. Optimal distinction between non-orthogonal quantum states. *Journal of Physics A: Mathematical and General*, 1998, **31** (34), P. 7105–7111.
[12] Chefles A., Barnett S.M. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics letters A*, 1998, **250** (4–6), P. 223–229.
[13] Chefles A. Unambiguous discrimination between linearly independent quantum states. *Physics Letters A*, 1998, **239** (6), P. 339–347.
[14] Zhang S., Feng Y., Sun X., Ying M. Upper bound for the success probability of unambiguous discrimination among quantum states. *Physical Review A*, 2001, **64** (6), 062103, P. 1–3.
[15] Duan L.M., Guo G.C. Probabilistic cloning and identification of linearly independent quantum states. *Physical review letters*, 1998, **80** (22), P. 4999–5002.
[16] Sun X., Zhang S., Feng Y., Ying M. Mathematical nature of and a family of lower bounds for the success probability of unambiguous discrimination. *Physical Review A*, 2002, **65** (4), 044306, P. 1–3.
[17] Eldar Y.C. A semidefinite programming approach to optimal unambiguous discrimination of quantum states. *IEEE Transactions on information theory*, 2003, **49** (2), P. 446–456.
[18] Galvao E.F., Hardy L. Cloning and quantum computation. *Physical Review A*, 2000, **62** (2), 022301, P. 1–5.
[19] Chefles A., Kitagawa A., et al. Unambiguous discrimination among oracle operators. *Journal of Physics A: Mathematical and Theoretical*, 2007, **40** (33), P. 10183–10213.
[20] Jaeger G., Shimony A. Optimal distinction between two non-orthogonal quantum states. *Physics Letters A*, 1995, **197** (2), P. 83–87.