# Equiprobable unambiguous discrimination of quantum states by symmetric orthogonalisation

D.B. Horoshko, M.M. Eskandari, S.Ya. Kilin

# Equiprobable unambiguous discrimination of quantum states by symmetric orthogonalisation

D. B. Horoshko[a,b,*], M. M. Eskandari[b], S. Ya. Kilin[b]

[a] *Univ. Lille, CNRS, UMR 8523 - PhLAM - Physique des Lasers Atomes et Molécules, F-59000 Lille, France*
[b] *B. I. Stepanov Institute of Physics, NASB, Nezavisimosti Ave. 68, Minsk 220072 Belarus*

**Abstract**

We show that the maximal probability of equiprobable unambiguous discrimination of a set of pure quantum states is given by the minimal eigenvalue of the Gram matrix of this set. We illustrate this result with several examples important for the protocols of quantum key distribution realized with weak coherent states of light.

*Keywords:* unambiguous state discrimination, quantum key distribution, quantum measurement theory, coherent states

## 1. Introduction

If a quantum system is prepared in one state $|\psi\rangle$ of a given set $\{|\psi_k\rangle, k = 1, ..., N\}$, its state can be determined with certainty by a measurement only when all the states of this set are mutually orthogonal [1]. If at least two states of the set are non-orthogonal, the procedure of determining the state $|\psi\rangle$, called quantum state discrimination, cannot give the true answer in each trial. There are two different approaches to treating this problem in the quantum measurement theory. The first approach consists in allowing errors in the measurement outcomes. Different strategies can be pursued in designing the optimal measurement: minimizing the average error in one measurement [2] or maximizing the retrieved information in measurements of long blocks [3]. The second approach consists in allowing the failure of the discrimination procedure [4, 5, 6, 7, 8]. If the discrimination succeeds, which happens with some probability $P_D < 1$, then the state is determined with certainty. Otherwise, the discrimination fails. The failure is known to the experimentalist and represents thus an additional measurement outcome. In the case of failure no information on the state is available and this state can only be randomly guessed, which results inevitably in an error. In a long series of trials such errors are more frequent than the errors of the minimal-error measurement of the first approach, however the positions of the erroneous outcomes are known with much higher precision, which is crucial for some applications. Such an unambiguous state discrimination (USD) procedure realizes a quantum measurement with $N + 1$ outcomes: one outcome for each state and one more outcome for the failure (inconclusive outcome). The measurements of this type are especially important for the analysis of security of quantum key distribution (QKD) systems [9, 10], where USD can be used by the adversary for monitoring the communication of the legitimate users and blocking it in the case of an inconclusive outcome [11]. Experimental schemes for USD of coherent states of light have been developed on the basis of linear optics and photon counting [12, 13].

USD with two equiprobable states has been analyzed by Ivanovic [4], Dieks [5] and Peres [6], who have found that the success probability in this case is $P_D = 1 - |\langle\psi_1|\psi_2\rangle|$. The case of different a priori probabilities has been studied by Jaeger and Shimony [7]. The general case of $N$ states with arbitrary a priori probabilities $\{\eta_k\}$ has been treated by Chefles [8], who has shown that the USD is possible if and only if the states of the set are linearly independent. In the same paper the positive operator-values measure (POVM) realising the USD is constructed and the average probability of success is written as $P_D = \sum_k \eta_k P_k$, where $P_k$ is the conditional probability of the true outcome when the state $|\psi_k\rangle$ is prepared. The problem of maximizing $P_D$ for a given set of states and a priori probabilities attracted much attention [14, 15, 16, 17, 18], and efficient numerical algorithms have been found. Analytical expressions for the POVM and the average success probability for $N > 2$ are known only for the special case of a symmetric set of states, where each state is produced in a cyclic manner from the previous one by means of a unitary rotation, and equiprobable measurements, where all conditional probabilities are the same $P_k = P_D$ [19]. Equiprobable measurements are highly likely to be optimal in the case of equiprobable a priori probabilities, which is a typical situation in quantum communications. However, the states used for quantum encoding not always belong to the class of symmetric ones.

In this Letter we derive a simple formula for the prob-

*Corresponding author. Tel.: +33640108808, Fax: +33320337020.
*Email address:* dmitri.horoshko@univ-lille.fr (D. B. Horoshko)

ability of success of a USD restricted to equiprobable measurements, we show that $P_D$ in this case is given by the minimal eigenvalue of the Gram matrix of the set of quantum states, $G_{kl} = \langle\psi_k|\psi_l\rangle$. This result includes naturally the well-known properties of equiprobable USD: In the case of linearly dependent states $P_D = 0$, since $G_{kl}$ is degenerate and its minimal eigenvalue is zero, and in the case of two states it gives the Ivanovic-Dieks-Peres probability as a solution of the second-order characteristic equation. This result is important for calculating the efficiency of the USD attack on a QKD system, where the exact description of the measurement is not necessary, but only the value of the probability of success.

In Section 2 we review briefly the USD theory of Ref. [8] and formulate its main results as two lemmas. In Section 3 we discuss the symmetric (Löwdin) orthogonalisation of a set of linearly independent states. Writing quantum operators in the Löwdin basis and applying the lemmas we prove the theorem containing the main result of this Letter. In Section 4 we consider several examples where the minimal eigenvalue of the Gram matrix can be rather easily calculated analytically. Section 5 concludes the Letter.

## 2. Unambiguous state discrimination

We start with a definition of USD measurement, which includes the trivial case of zero discrimination probability.

**Definition.** *USD of a set of $N \geq 2$ states $\{|\psi_k\rangle, k = 1, ..., N\}$ is a generalized measurement characterized by a POVM including $N$ positive operators $\left\{\hat{\Pi}_k, k = 1, ..., N\right\}$ for conclusive outcomes, satisfying the zero-error condition*

$$\langle\psi_l|\hat{\Pi}_k|\psi_l\rangle = P_k\delta_{kl},\ 0 \leq P_k \leq 1, \tag{1}$$

*and one more positive operator $\hat{\Pi}_0$ for the inconclusive outcome (failure), such that together these operators represent a resolution of identity*

$$\sum_{k=1}^{N} \hat{\Pi}_k + \hat{\Pi}_0 = \hat{I}, \tag{2}$$

*where $\hat{I}$ is the identity operator on the space $\mathcal{S}$ spanned by the states of the considered set.*

When a quantum system in some state $|\psi\rangle$ is measured, the probability of the $k$th outcome is $\langle\psi|\hat{\Pi}_k|\psi\rangle$ and is equal to $P_k$ if $|\psi\rangle = |\psi_k\rangle$ and to zero if $|\psi\rangle$ is some other state of the set. The probability of the inconclusive outcome for $|\psi\rangle = |\psi_k\rangle$ is $\langle\psi_k|\hat{\Pi}_0|\psi_k\rangle = 1 - P_k$. Note also that from the Cauchy-Schwarz inequality for the states $\hat{\Pi}_k^{1/2}|\psi_l\rangle$ and $\hat{\Pi}_k^{1/2}|\psi_m\rangle$ we obtain

$$\begin{aligned} |\langle\psi_l|\hat{\Pi}_k|\psi_m\rangle|^2 &\leq \langle\psi_l|\hat{\Pi}_k|\psi_l\rangle\langle\psi_m|\hat{\Pi}_k|\psi_m\rangle \\ &= P_k^2\delta_{kl}\delta_{km}, \end{aligned} \tag{3}$$

wherefrom

$$\langle\psi_l|\hat{\Pi}_k|\psi_m\rangle = P_k\delta_{kl}\delta_{km}, \tag{4}$$

i.e. the operators of conclusive events are diagonal in the basis of the discriminated states.

By the above definition we accept the possibility of a zero discrimination probability for some states. It is easy to see that in the case of a linearly dependent set of states this is always the case.

**Lemma 1.** *USD of a linearly dependent set of states is characterized by al least one zero probability $P_k$.*

*Proof.* In the case of linear dependence we can write

$$|\psi_l\rangle = \sum_{m=1}^{N} f_{lm}|\psi_m\rangle \tag{5}$$

with at least one non-zero off-diagonal element $f_{lm} \neq 0$, $l \neq m$. Substituting Eq. (5) into the zero-error condition (1) and applying Eq. (4) we obtain

$$|f_{lm}|^2 P_k\delta_{km} = P_k\delta_{kl}. \tag{6}$$

Since the matrix $f_{lm}$ for linearly dependent states can be non-diagonal, there should be at least one $P_k = 0$. □

For linearly independent set of states the POVM can be built as follows [8]. The operators of conclusive outcomes are $\hat{\Pi}_k = q_k P_k|\psi_k^\perp\rangle\langle\psi_k^\perp|$, where the state $|\psi_k^\perp\rangle$ is "reciprocal" to $|\psi_k\rangle$, i.e. it belongs to the space $\mathcal{S}$ and satisfies $\langle\psi_i|\psi_k^\perp\rangle = c_k\delta_{ik}$, with some non-zero $c_k$, while $q_k = |c_k|^{-2}$. In practical calculations, the state $|\psi_k^\perp\rangle$, reciprocal to $|\psi_k\rangle$, can be found at the end of the Gram-Schmidt orthogonalization procedure, applied to the initial set of state with the state $|\psi_k\rangle$ put to the end. The operator of the inconclusive outcome $\hat{\Pi}_0$ is determined from Eq. (2) as the complement to the identity for the operators of conclusive outcomes.

Since the reciprocal states and the numbers $q_k$ are uniquely determined by the initial set of states, the only degree of freedom in the definition of the POVM is connected to the conditional probabilities $P_k$. Positivity of $\hat{\Pi}_0$ imposes a restriction on the possible values of $P_k$. Optimisation strategies have been developed for finding a POVM maximizing the average success probability $P_D$ [14, 15, 16, 17, 18]. In this work we restrict our consideration to equiprobable measurements with $P_k = P_D$, playing an important role in the security analysis of QKD protocols. In this particular case, which we call "equiprobable USD", the optimal POVM, maximizing $P_D$ can be determined from the structure of the set of reciprocal states, as formulated by the following lemma [8].

**Lemma 2.** *The maximal success probability $P_D$ for an equiprobable USD of a set of linearly independent states $\{|\psi_k\rangle, k = 1, ..., N\}$ is given by $P_D = \lambda_{\max}^{-1}$, where $\lambda_{\max}$ is the maximal eigenvalue of the operator*

$$\hat{\Lambda} = \sum_{k=1}^{N} \frac{|\psi_k^\perp\rangle\langle\psi_k^\perp|}{|\langle\psi_k^\perp|\psi_k\rangle|^2}. \tag{7}$$

*Proof.* The positivity of $\hat{\Pi}_0$ together with Eq. (2) require that the eigenvalues of $\sum_k \hat{\Pi}_k = P_D\hat{\Lambda}$ are not greater than 1. It means that the set of possible POVM corresponds to $P_D \in \left[0, \lambda_{\max}^{-1}\right]$, hence the maximal probability of success. □

Lemma 2 allows one to calculate the maximal success probability for any initial set of linearly independent states. However, this task requires building a set of reciprocal states by a tedious Gram-Schmidt orthogonalisation algorithm, whose length increases with the growth of dimensionality of the initial set of states. In the next section we will see that another orthogonalisation procedure, the Löwdin or symmetric orthogonalisation, is much better suited to the considered problem.

## 3. Löwdin orthogonalisation

Let us write the states of the initial set of linearly independent states in a form of row vector and express them via the states of some orthonormal basis $\{|v_1\rangle, ..., |v_N\rangle\}$ on $\mathcal{S}$:

$$\left( \begin{array}{cccc} |\psi_1\rangle & ... & |\psi_N\rangle \end{array} \right) = \left( \begin{array}{cccc} |v_1\rangle & ... & |v_N\rangle \end{array} \right) \mathbf{L}, \qquad (8)$$

where $\mathbf{L}$ is a complex $N \times N$ matrix. This matrix is non-unitary in general and satisfies

$$\mathbf{L}^\dagger\mathbf{L} = \begin{pmatrix} \langle\psi_1| \\ ... \\ \langle\psi_N| \end{pmatrix} \left( \begin{array}{cccc} |\psi_1\rangle & ... & |\psi_N\rangle \end{array} \right) = \mathbf{G}, \qquad (9)$$

where $\mathbf{G}$ is the Gram matrix of the initial set of states.

Among various bases on $\mathcal{S}$ there is one whose transform matrix is Hermitian and is given by $\mathbf{L} = \mathbf{L}^\dagger = \mathbf{G}^{\frac{1}{2}}$. The orthonormal basis obtained in this way was first introduced by Löwdin [20] and is characterized by minimal distance from the non-orthogonal set [21]. Moreover, the whole orthogonalization procedure is symmetric with respect to the initial set. The Löwdin basis has proven to be highly efficient for the analysis of entanglement of two-mode Schrödinger cat states [22].

Representing the operator $\hat{\Lambda}$ as a matrix in the Löwdin basis we obtain

$$\begin{aligned} \mathbf{\Lambda} &= \begin{pmatrix} \langle v_1| \\ ... \\ \langle v_N| \end{pmatrix} \hat{\Lambda} \left( \begin{array}{cccc} |v_1\rangle & ... & |v_N\rangle \end{array} \right) \qquad (10) \\ &= \mathbf{G}^{-\frac{1}{2}} \begin{pmatrix} \langle\psi_1| \\ ... \\ \langle\psi_N| \end{pmatrix} \hat{\Lambda} \left( \begin{array}{cccc} |\psi_1\rangle & ... & |\psi_N\rangle \end{array} \right) \mathbf{G}^{-\frac{1}{2}} \\ &= \mathbf{G}^{-\frac{1}{2}}\mathbf{I}\mathbf{G}^{-\frac{1}{2}} = \mathbf{G}^{-1}, \end{aligned}$$

where $\mathbf{I}$ is the $N \times N$ identity matrix. We see that in the Löwdin basis the matrix of the operator $\hat{\Lambda}$ is the inverse of the Gram matrix $\mathbf{G}$. Thus, its maximal eigenvalue is equal to the inverse of the minimal eigenvalue of the Gram matrix and we arrive to the following theorem.

**Theorem.** *The maximal success probability $P_D$ for an equiprobable USD of a set of any states $\{|\psi_k\rangle, k = 1, ..., N\}$ is given by the minimal eigenvalue of its Gram matrix $G_{kl} = \langle\psi_k|\psi_l\rangle$.*

*Proof.* In the case of linearly independent states the proof follows from Lemma 2 and Eq. 10. In the case of linearly dependent states the minimal eigenvalue of the Gram matrix is zero, and so is the probability of success $P_D$ by Lemma 1. □

Note, that in the case of equiprobable USD of a linearly dependent set the only possible POVM, by Lemma 1, is the trivial one, composed of $\hat{\Pi}_0 = \hat{I}$ and all other operators zero.

The Löwdin basis allows one to find also the POVM of the equiprobable USD. Consider the states

$$\left( \begin{array}{cccc} |\tilde{\psi}_1\rangle & ... & |\tilde{\psi}_N\rangle \end{array} \right) = \left( \begin{array}{cccc} |v_1\rangle & ... & |v_N\rangle \end{array} \right) \mathbf{G}^{-\frac{1}{2}}. \qquad (11)$$

It is easy to see that

$$\begin{pmatrix} \langle\tilde{\psi}_1| \\ ... \\ \langle\tilde{\psi}_N| \end{pmatrix} \left( \begin{array}{cccc} |\psi_1\rangle & ... & |\psi_N\rangle \end{array} \right) = \mathbf{G}^{-\frac{1}{2}}\mathbf{I}\mathbf{G}^{\frac{1}{2}} = \mathbf{I}, \qquad (12)$$

which means that the reciprocal states are given by $|\psi_k^\perp\rangle = c_k|\tilde{\psi}_k\rangle$ and the operators of the POVM are $\hat{\Pi}_k = P_D|\tilde{\psi}_k\rangle\langle\tilde{\psi}_k|$.

## 4. Examples

In this section we consider several examples, where the maximal probability of equiprobable USD can be easily obtained. The first example is the case of two states $|\psi_1\rangle$ and $|\psi_2\rangle$. The eigenvalues of the Gram matrix

$$\mathbf{G} = \begin{pmatrix} 1 & \langle\psi_1|\psi_2\rangle \\ \langle\psi_2|\psi_1\rangle & 1 \end{pmatrix} \qquad (13)$$

are easily obtained from the quadratic characteristic equation in the form $g_{1,2} = 1 \pm |\langle\psi_1|\psi_2\rangle|$. The minimal eigenvalue is obviously $g_2 = 1 - |\langle\psi_1|\psi_2\rangle|$, which corresponds to the Ivanovic-Dieks-Peres probability [4, 5, 6].

The second example is the case of $N$ symmetric states such that $|\psi_k\rangle = \hat{U}^{k-1}|\psi_1\rangle$, where $\hat{U}$ is a unitary operator satisfying $\hat{U}^N = \hat{I}$ [19, 22]. In this case the Gram matrix depends only on the difference modulo $N$ of its indices, $G_{kl} = \langle\psi_1|\hat{U}^{l-k}|\psi_1\rangle$, and is therefore a circulant matrix, whose $k$th row is a circularly right-shifted $(k-1)$th row. The circulant matrix eigenvalues are given by the discrete Fourier transform of the first row [23]:

$$g_j = \sum_{k=1}^{N} \langle\psi_1|\psi_k\rangle e^{i2\pi jk/N}, \qquad (14)$$

and to obtain the maximal success probability one needs to find the minimum of this expression. The same expression was obtained by Chefles and Barnett [19] from

an explicit construction of reciprocal states. The case of $N = 4$ corresponds to the states used in realisations of the BB84 protocol of QKD by means of weak coherent states. Indeed, in the polarization encoding there are two modes, right and left polarized ones, and the four code states can be written as [24, 25]

$$\begin{aligned} |0_+\rangle &= |\alpha\rangle_R \otimes |\alpha\rangle_L, \\ |0_\times\rangle &= |\alpha\rangle_R \otimes |i\alpha\rangle_L, \\ |1_+\rangle &= |\alpha\rangle_R \otimes |-\alpha\rangle_L, \\ |1_\times\rangle &= |\alpha\rangle_R \otimes |-i\alpha\rangle_L, \end{aligned} \tag{15}$$

where the ket index denotes the right (R) or left (L) polarization. The states $|0_+\rangle$ and $|1_+\rangle$ create the rectilinear basis, while the states $|0_\times\rangle$ and $|1_\times\rangle$ create the diagonal one. We see, that the state of the right-polarized mode is the same for all four code states. Thus, the task of state discrimination can be limited to the left-polarized mode only, whose states are four coherent states $\{|\alpha\rangle, |i\alpha\rangle, |-\alpha\rangle, |-i\alpha\rangle\}$. The four eigenvalues of their Gram matrix can be obtained from Eq. (14) as functions of the average photon number in one mode $\nu = |\alpha|^2$. In the range of practical values $0 < \nu \leq 2$ the minimal eigenvalue is

$$g_{\min}^{\mathrm{BB84}} = 2e^{-\nu}\left(\sinh\nu - \sin\nu\right), \tag{16}$$

which corresponds to the result of Ref. [11].

The third example is the set of two-mode states used in the realizations of the BB84 protocol by subcarrier wave modulation [26, 27, 28, 29]. At low modulation index these states can be written as [30, 31]

$$\begin{aligned} |\psi_1\rangle &= |\alpha\rangle_U \otimes |\alpha\rangle_L, \\ |\psi_2\rangle &= |-i\alpha\rangle_U \otimes |i\alpha\rangle_L, \\ |\psi_3\rangle &= |-\alpha\rangle_U \otimes |-\alpha\rangle_L, \\ |\psi_4\rangle &= |i\alpha\rangle_U \otimes |-i\alpha\rangle_L, \end{aligned} \tag{17}$$

where the ket index denotes the upper (U) or lower (L) sideband of the carrier wave. These states belong to the class of symmetric states and the four eigenvalues of the Gram matrix are easily obtained from Eq. (14). The minimal one is

$$g_{\min}^{\mathrm{SCW}} = (1 - e^{-2\nu})^2, \tag{18}$$

where $\nu = |\alpha|^2$, as above, is the average photon number in one polarisation mode.

The fourth and the last example corresponds to the case of the BB84 protocol with polarization encoding and decoy states. Decoy states are different from the signal ones only by their coherent amplitude $\beta$ with $|\beta| \neq |\alpha|$. Here we consider only the case of one decoy level, as initially proposed by Hwang [32]. This case can be easily generalized to two levels, usually applied in practice [33], or any other number of levels. Our task is to discriminate the set of eight states, composed of four signal states, defined by Eq. (15) and four decoy states obtained from this equation by the substitution $\alpha \to \beta$. These eight states are shown schematically in Fig. 1.

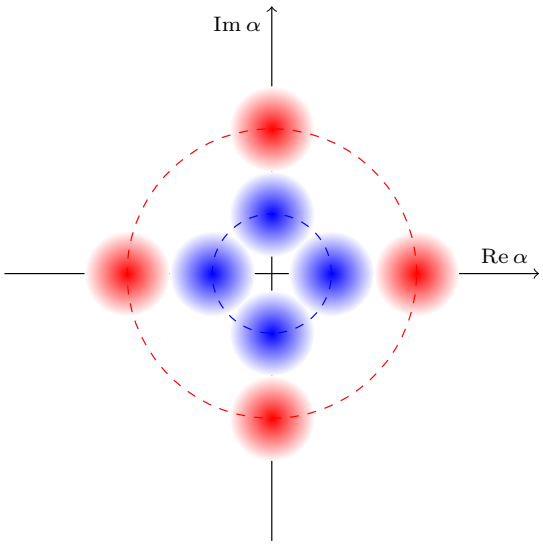


Figure 1: Eight states of the left-polarized mode in a realisation of the decoy-state enhanced BB84 protocol with weak coherent states. Each state is a coherent states and is represented by the $\sigma$-area of its Wigner function. Four states of the inner (blue) circle are the four signal states. Four states of the outer (red) circle are the four decoy states. Decoy states have higher mean photon number in this drawing, as in the original proposal by Hwang [32], though the analytical treatment admits any values of the mean photon number of the signal and the decoy states.

We group the signal state together with the corresponding decoy one in a two-component row vector

$$\mathbf{W}_k = \left(|\alpha\rangle_R \otimes |\alpha_k\rangle_L, |\beta\rangle_R \otimes |\beta_k\rangle_L\right), \tag{19}$$

where $\alpha_k = (-i)^{k-1}\alpha$ and $\beta_k = (-i)^{k-1}\beta$. We concatenate all four such vectors in one eight-component vector $\mathbf{W} = (\mathbf{W}_1\mathbf{W}_2\mathbf{W}_3\mathbf{W}_4)$. Now the Gram matrix is $\mathbf{G} = \mathbf{W}^\dagger\mathbf{W}$. This matrix can be written in a block form with the blocks represented by $2 \times 2$ matrices

$$\begin{aligned} \mathbf{G}_{kl} &= \mathbf{W}_k^\dagger \mathbf{W}_l \\ &= \begin{pmatrix} \langle\alpha_k|\alpha_l\rangle & \langle\alpha|\beta\rangle\langle\alpha_k|\beta_l\rangle \\ \langle\beta|\alpha\rangle\langle\beta_k|\alpha_l\rangle & \langle\beta_k|\beta_l\rangle \end{pmatrix}. \end{aligned} \tag{20}$$

It is easy to see that these blocks depend on the index difference $k - l$ only, so that the Gram matrix is block-circulant. This is a consequence of the fact that the state pairs are symmetric with respect to the operator $\hat{U} = \exp\{i\pi a^\dagger a/2\}$ where $a$ is the photon annihilation operator of the left-polarized mode, i.e. $\mathbf{W}_k = \hat{U}^{k-1}\mathbf{W}_1$. The eigenvalues of a block-circulant matrix are given by the set of eigenvalues of all elements of a discrete Fourier transform of its first block row [34], which in our case are

$$\begin{aligned} \mathbf{F}_k &= \sum_{l=1}^{4} i^{(k-1)(l-1)}\mathbf{G}_{1l} \\ &= \begin{pmatrix} \langle\alpha|\tilde{\mathrm{c}}_k^\alpha\rangle & \langle\alpha|\beta\rangle\langle\alpha|\tilde{\mathrm{c}}_k^\beta\rangle \\ \langle\alpha|\beta\rangle\langle\beta|\tilde{\mathrm{c}}_k^\alpha\rangle & \langle\beta|\tilde{\mathrm{c}}_k^\beta\rangle \end{pmatrix}, \end{aligned} \tag{21}$$

where

$$|\tilde{c}_k^{\alpha}\rangle = \sum_{j=0}^{3} e^{i\pi(k-1)j/2}|\alpha e^{-i\pi j/2}\rangle \qquad (22)$$

is the unnormalized discrete Fourier transform of the four coherent states equidistant on the circle, which is known as rotationally-invariant circular state [22].

$\mathbf{F}_k$ is a Hermitian $2 \times 2$ matrix. Its smaller eigenvalue is

$$\lambda_k^{(-)} = \frac{1}{2}\left(\mathrm{Tr}\,\mathbf{F}_k - \sqrt{(\mathrm{Tr}\,\mathbf{F}_k)^2 - 4\det\mathbf{F}_k}\right), \qquad (23)$$

and the minimal eigenvalue of $\mathbf{G}$ is given by the smallest eigenvalue of all four matrices

$$g_{\min}^{\mathrm{BB84+decoy}} = \min_k \lambda_k^{(-)}. \qquad (24)$$

In Fig. 2 we show the four smaller eigenvalues of the matrices $\mathbf{F}_k$ in the case where the decoy states contain $2|\beta|^2 = 1$ photon on average, as initially proposed by Hwang [32].

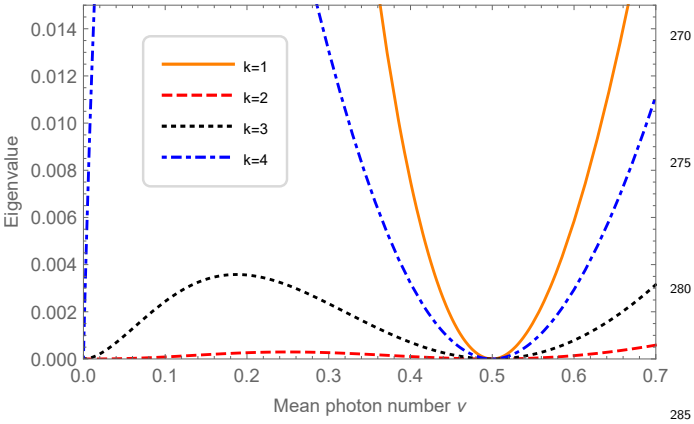


Figure 2: Four eigenvalues $\lambda_k^{(-)}$ as functions of the mean photon number in one mode $\nu = |\alpha|^2$ for the BB84 protocol with one level of decoy states. The decoy states contain $\nu' = |\beta|^2 = 0.5$ photons in each mode. The minimal eigenvalue, $\lambda_2^{(-)}$, gives the USD probability for the states depicted in Fig. 1. At the point $\nu = \nu'$ all four eigenvalues are zeros. At this point $\alpha = \beta$ and the set of considered states is linearly dependent, which means that the USD probability is zero.

The discrimination probability $P_D$ is given by the smaller eigenvalue of $\mathbf{F}_2$ and for $\nu = |\alpha|^2 = 0.15$ is equal to $P_D = 1.8 \times 10^{-4}$, which corresponds to 37 dB of loss. Note, that a satellite communication line is expected to have about 40 dB of loss in the down-link configuration and about 50 dB in the up-link one [35]. It means that the USD attack on the BB84 protocol in this case should be countered either by decreasing the decoy state level, which is a common practice presently [33], or by randomizing the phase of the states in the quantum channel [11].

## 5. Conclusions

In this Letter we have shown that the maximal probability of an equiprobable USD of a set of quantum states is given by the minimal eigenvalue of the Gram matrix of the set. This result allows one to calculate this probability directly, avoiding a construction of the set of reciprocal states. We have shown that in several special cases analytical expressions for the discrimination probability can be rather easily found. We believe that these results deepen the understanding of the USD technique and can find numerous applications in the analysis of protocols of QKD realized with weak coherent states of light.

## Acknowledgments

This work was supported by Belarus State Program of Scientific Research "Convergence-2020" (grant 3.1.01) and by Belarusian Republican Foundation for Fundamental Research (grant F18R-118).

## References

[1] J. von Neumann, Mathematical Foundations of Quantum Mechanics, Princeton University Press (1955). DOI:10.2307/j.ctt1wq8zhp

[2] C. W. Helstrom, Quantum Detection and Estimation Theory, Academic Press, New York (1976).

[3] A. S. Holevo, The Capacity of the Quantum Channel with General Signal States, IEEE Trans. Inf. Theory, 44, 269 (1998). DOI:10.1109/18.651037

[4] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987). DOI:10.1016/0375-9601(87)90222-2

[5] D. Dieks, Overlap and distinguishability of quantum states, Phys. Lett. A **126**, 303 (1988). DOI:10.1016/0375-9601(88)90840-7

[6] A. Peres, How to differentiate between non-orthogonal states, Phys. Lett. A **128**, 19 (1988). DOI:10.1016/0375-9601(88)91034-1

[7] G. Jaeger and A. Shimony, Optimal distinction between two non-orthogonal quantum states, Phys. Lett. A **197**, 83 (1995). DOI:10.1016/0375-9601(94)00919-G

[8] A. Chefles, Unambiguous Discrimination Between Linearly-Independent Quantum States, Phys. Lett. A **239**, 339 (1998). DOI:10.1016/S0375-9601(98)00064-4

[9] S. Ya. Kilin, in Progress in Optics, Chapter 1: Quanta and information. Ed. E. Wolf, **42**, 1 (2001).

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002). DOI:10.1103/RevModPhys.74.145

[11] M. Dušek, M. Jahma, and N. Lütkenhaus, Unambiguous state discrimination in quantum cryptography with weak coherent states, Phys. Rev. A **62**, 022306 (2000). DOI:10.1103/PhysRevA.62.022306

[12] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, N. Gisin, Unambiguous quantum measurement of nonorthogonal states, Phys. Rev. A **54**, 3783 (1996). DOI:10.1103/PhysRevA.54.3783

[13] F. E. Becerra, J. Fan, and A. Migdall, Unambiguous quantum measurement of nonorthogonal states, Nat. Comm. **4**, 2028 (2013). DOI:10.1038/ncomms3028

[14] Y. Sun, M. Hillery, and J.A. Bergou, Optimum unambiguous discrimination between linearly independent nonorthogonal quantum states and its optical realization, Phys. Rev. A **64**, 022311 (2001). DOI:10.1103/PhysRevA.64.022311

[15] Y. Eldar, A semidefinite programming approach to optimal unambiguous discrimination of quantum states, IEEE Trans. Inf. Theory **49**, 446 (2003). DOI:10.1109/TIT.2002.807291

[16] M. A. Jafarizadeh, M. Rezaei, N. Karimi, and A. R. Amiri, Optimal unambiguous discrimination of quantum states, Phys. Rev. A **77**, 042314 (2008). DOI:10.1103/PhysRevA.77.042314

[17] L. Roa, C. Hermann-Avigliano, R. Salazar, and A.B. Klimov, Conclusive discrimination among N equidistant pure states, Phys. Rev. A **84**, 014302 (2011). DOI:10.1103/PhysRevA.84.014302

[18] J. A. Bergou, U. Futschik, and E. Feldman, Optimal Unambiguous Discrimination of Pure Quantum States, Phys. Rev. Lett. **108**, 250502 (2012). DOI:10.1103/PhysRevLett.108.250502

[19] A. Chefles, S. M. Barnett, Optimum unambiguous discrimination between linearly independent symmetric states, Phys. Lett. A **250**, 223 (1999). DOI:10.1016/S0375-9601(98)00827-5

[20] P.-O. Löwdin, On the Non-Orthogonality Problem Connected with the Use of Atomic Wave Functions in the Theory of Molecules and Crystals, J. Chem. Phys. **18**, 365 (1950). DOI:10.1063/1.1747632

[21] I. Mayer, On Löwdin's method of symmetric orthogonalization, Int. J. Quantum Chem. **90**, 63 (2002). DOI:10.1002/qua.981

[22] D. B. Horoshko, S. De Bièvre, M. I. Kolobov, and G. Patera, Entanglement of quantum circular states of light, Phys. Rev. A **93**, 062323 (2016). DOI: 10.1103/PhysRevA.93.062323

[23] H. Lütkepohl, Handbook of Matrices, Wiley, New-York (1996).

[24] C. H. Bennett, F. Bessette, G. Brassard, and L. Savail, Experimental quantum cryptography, J. Cryptology **5**, 3 (1992). DOI:10.1007/BF00191318

[25] H. P. Yuen, Quantum amplifiers, quantum duplicators and quantum cryptography, Quantum Semiclassic. Opt. **8**, 939 (1996). DOI:10.1088/1355-5111/8/4/015

[26] J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography, Phys. Rev. Lett. **82**, 1656 (1999). DOI:10.1103/PhysRevLett.82.1656

[27] A. Ortigosa-Blanch and J. Capmany, Subcarrier multiplexing optical quantum key distribution, Phys. Rev. A **73**, 024305 (2006). DOI:10.1103/PhysRevA.73.024305

[28] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference, Opt. Expr. **24**, 2619 (2016). DOI:10.1364/OE.24.002619

[29] G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, Security of subcarrier wave quantum key distribution against the collective beam-splitting attack, Opt. Express **26**, 11292 (2018). DOI:10.1364/OE.26.011292

[30] P. Kumar and A. Prabhakar, Evolution of quantum states in an electro-optic phase modulator, IEEE J. Quantum Electron. **45**, 149–156 (2009). DOI:10.1109/JQE.2008.2002673

[31] D. B. Horoshko, M. M. Eskandary, and S. Ya. Kilin, Quantum model for traveling-wave electro-optical phase modulator, J. Opt. Soc. Am. B **35**, 2744 (2018). DOI:10.1364/JOSAB.35.002744

[32] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003). DOI:10.1103/PhysRevLett.91.057901

[33] C. C.-W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014). DOI:10.1103/PhysRevA.89.022307

[34] G. J. Tee, Eigenvectors of block circulant and alternating circulant matrices, Res. Lett. Inf. Math. Sci. **8**, 123 (2005).

[35] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Hübel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein, A comprehensive design and performance analysis of low Earth orbit satellite quantum communication, New J. Phys. **15**, 023006 (2013). DOI:10.1088/1367-2630/15/2/023006