




Optimal individual and collective measurements for nonorthogonal quantum key distribution signals

Isabella Cerutti  and Petra F. Scudo ^{*}

European Commission Joint Research Centre, 21027 Ispra, Italy

 (Received 15 December 2023; revised 20 February 2024; accepted 27 February 2024; published 20 March 2024)

We consider how the theory of optimal quantum measurements determines the maximum information available to the receiving party of a quantum key distribution (QKD) system employing linearly independent but nonorthogonal quantum states. Such a setting is characteristic of several practical QKD protocols. Due to nonorthogonality, the receiver is not able to discriminate unambiguously between the signals. To understand the fundamental limits that this imposes, the quantity of interest is the maximum mutual information between the transmitter (Alice) and the receiver, whether legitimate (Bob) or an eavesdropper (Eve). To find the optimal measurement—taken individually or collectively—we use a framework based on operator algebra and general results derived from singular-value decomposition, achieving optimal solutions for von Neumann measurements and positive operator-valued measures (POVMs). The formal proof and quantitative analysis elaborated for two signals allow us to conclude that optimal von Neumann measurements are uniquely defined and provide a higher information gain compared to POVMs. Interestingly, collective measurements not only do not provide additional information gain with respect to individual ones but also suffer from a gain reduction in the case of POVMs.

DOI: [10.1103/PhysRevA.109.032615](https://doi.org/10.1103/PhysRevA.109.032615)

I. INTRODUCTION

In this paper, we consider a general quantum key distribution (QKD) scheme in which the sender transmits nonorthogonal quantum bits and operates with a given choice of the basis. The aim is to address the issue of optimal detection of N qubits encoded in signal states $|\Psi_i\rangle$, with $i = 1, 2, \dots, N$. The optimal detection strategy may be equivalently seen as an optimal interception strategy by an eavesdropper as well as an optimal measurement strategy at the receiver's end. We denote the receiver as Bob whether he is the intended party or an eavesdropper.

The importance of the result is that collective attacks will be more practical when quantum computing technology has developed beyond the current level, which is exactly the circumstances for which QKD is advocated. The topic is of general interest in quantum cryptography, including time-bin encoded QKD protocols such as coherent one way [1] and differential phase shift [2].

We assume a quantum key encoding scheme in which the sender, Alice, prepares signal states represented as $|\Psi_i\rangle_k$, which identifies the k th logical qubit of signal i . Moreover, we assume that the signal states form a set of nonorthogonal linearly independent quantum states in the vector space of the signals. Nonorthogonal signal states are typical of QKD protocols based on coherent pulses.

In order to optimally determine the state sent by Alice, the receiver (Bob) may choose to perform an unambiguous-state-discrimination positive operator-valued measure (POVM) [3] or a von Neumann projective measurement [4]. The first

strategy is generally adopted in quantum cryptography and allows for the discrimination of two signal states with certainty, leaving Bob with a finite margin of error, referred to as an “inconclusive answer.” The second strategy consists in abandoning certainties in favor of probabilities by performing a projective measurement. The latter strategy generally increases the mutual information gain of the process and is adopted by information theorists.

In the following sections we address the main question of the paper: Can optimal collective measurements outperform individual ones when discriminating among nonorthogonal QKD states? To answer this question, we compare the use of *individual measurements* with *collective measurements*, where two (or potentially more) signal states are measured jointly. To this end, we consider both collective projective (von Neumann) measurements and POVMs. The comparison is based on the optimization of mutual information gain. Finally, we discuss the use of entanglement in optimizing collective measurements.

The solution to this problem is inspired by the seminal work by Peres and Wootters on optimal detection of quantum information [5], suggesting that combined entangled measurements perform better than individual measurements in the detection of pairs of nonorthogonal tensor-product quantum states. In their work, Peres and Wootters analyze the optimal detection of pairs of spin particles aligned along three nonorthogonal directions (along the z axis and tilted by 120° in opposite directions). Note that even though each signal state is a separable state of the two particles, their optimal detection was found to be represented by an entangled operator on the state space of the two systems. In a subsequent work [6], Wootters found a joint yet separable (nonentangled) measurement that could attain the same optimal information gain.

^{*}petra.scudo@ec.europa.eu

The problem was solved for specific signal states, leaving open the question about the generalization of their results to arbitrary pairs of product states. Note that, analogous to Refs. [5,6], the property we wish to investigate is whether *collective* and, specifically, *entangled* measurements outperform individual measurements when applied to separable, nonentangled signal states and whether this property holds also in the case of states like the time-bin ones that do not rely on an additive-group-structure property (e.g., the spin coupling and Clebsch-Gordan decomposition for quantum angular momentum states).

Based on the seminal works by Eldar and Forney [7,8], we address these questions by deriving the optimal measurements using both a von Neumann projective approach and POVM operators. The optimization exploits the properties of singular-value decomposition (SVD) and, in particular, its derivation, known as the Eckart-Young theorem [9]. Different from the previous works by Eldar and Forney, we focus on the maximization of the average information gain, for which we provide the demonstration of uniqueness and optimality of von Neumann measurements. Moreover, our results apply to practical QKD systems, allowing us to answer the question on whether collective measurements can be more beneficial than the individual ones. We conclude our study by analyzing the effects of both von Neumann and POVM measurements on the initial quantum signals and comparing the use of Shannon and von Neumann entropies as a measure of disturbance.

II. OPTIMAL VON NEUMANN MEASUREMENTS

A. Optimizing the information gain

We quantify the information gained by the measurement in terms of *average information gain*, defined as the difference between the Shannon entropy of Alice's initial preparation H_{in} and the average final entropy after performing the measurement H_{fin} [3,5]:

$$I_{\text{av}} = H_{\text{in}} - H_{\text{fin}}. \quad (1)$$

For N equiprobable signal states $|\Psi_i\rangle$, $r_i = 1/N$ ($1 \leq i \leq N$), the initial entropy is

$$H_{\text{in}} = - \sum_i r_i \log_2(r_i) = \log_2(N). \quad (2)$$

The assumption of equiprobable signals sent by Alice is important for maximizing the entropy of the source and thus determining the maximum possible information gain of the receiver. The optimization of the information gain equally applies to the intended party or to an eavesdropper.

On the other side, the average final entropy at Bob's (Eve's) end depends on the measurement results $\{\mu\}$ and on the specific measurement strategy. We shall later compare the optimal information gain of projective von Neumann measurements with that obtained by applying a POVM.

To maximize the average information gain, the measurement strategy should aim at minimizing the final entropy H_{fin} . Having found a specific result μ , Bob's posterior conditional probability for state i is given by Bayes's theorem [10]:

$$Q_{i,\mu} = \frac{P_{\mu,i} r_i}{q_\mu} \quad \forall i, \mu = 1, \dots, N, \quad (3)$$

where $P_{\mu,i}$ is the probability of detecting state μ if the input state is i and

$$q_\mu = \sum_j P_{\mu,j} r_j \quad \forall \mu = 1, \dots, N \quad (4)$$

is the total probability for result μ . For equiprobable signals $r_i = 1/N$ ($1 \leq i \leq N$), Eq. (3) becomes

$$Q_{i,\mu} = \frac{P_{\mu,i}}{\sum_j P_{\mu,j}} \quad \forall i, \mu = 1, \dots, N. \quad (5)$$

After result μ is obtained, the associated entropy relative to μ is

$$H_\mu = - \sum_i Q_{i,\mu} \log_2(Q_{i,\mu}) \quad \forall \mu = 1, \dots, N, \quad (6)$$

while the average final entropy over all possible results is

$$\langle H_{\text{fin}} \rangle = \sum_\mu q_\mu H_\mu. \quad (7)$$

The information gain (1) is maximized when the initial entropy is maximized while the average final entropy (7) is minimized. The maximum initial entropy is achieved when the signal states are equiprobable, as assumed in Eq. (2). The average final entropy is minimized when the terms $Q_{i,\mu}$ in Eq. (6) take either of the extreme values of the probability range, i.e., 0 or 1 (see the Appendix). In the specific case of orthonormal signals by Alice, this corresponds at the receiver's end to performing a von Neumann measurement using the same orthonormal basis as the transmitter.

B. Determining optimal von Neumann measurements for a given set of input states

In order to translate the above observation into a quantitative condition on Bob's measurement, it is convenient to express both Alice's input states and Bob's measurement projectors in matrix form.

Let $|\Psi_i\rangle$, $i = 1, 2, \dots, N$, be Alice's input vector states with real elements, and define \mathbf{A} to be the matrix having as columns these vectors expressed with respect to a given basis in the Hilbert space \mathcal{H}_A :

$$\mathbf{A} = \begin{pmatrix} \Psi_{11} & \Psi_{21} & \cdots & \Psi_{N1} \\ \Psi_{12} & \Psi_{22} & \cdots & \Psi_{N2} \\ \cdots & \cdots & \cdots & \cdots \\ \Psi_{1N} & \Psi_{2N} & \cdots & \Psi_{NN} \end{pmatrix}. \quad (8)$$

Let $\{\Pi_i = |\Phi_i\rangle\langle\Phi_i|\}_i$ be a complete set of orthonormal projectors on \mathcal{H}_A corresponding to Bob's von Neumann measurement. Analogously to (8), let us define \mathbf{B} to be the matrix having as columns the vectors $|\Phi_i\rangle$, $i = 1, 2, \dots, N$, in the same basis with $\langle\Phi_i|\Phi_j\rangle = \delta_{i,j}$:

$$\mathbf{B} = \begin{pmatrix} \Phi_{11} & \Phi_{21} & \cdots & \Phi_{N1} \\ \Phi_{12} & \Phi_{22} & \cdots & \Phi_{N2} \\ \cdots & \cdots & \cdots & \cdots \\ \Phi_{1N} & \Phi_{2N} & \cdots & \Phi_{NN} \end{pmatrix}. \quad (9)$$

Correspondingly, the elements $P_{\mu,i}$ in (5), which are given by

$$P_{\mu,i} = |\langle\Phi_\mu|\Psi_i\rangle|^2, \quad (10)$$

can be collected in a *probability matrix* \mathbf{P} :

$$\mathbf{P} = (\mathbf{B}^T \mathbf{A}) \circ (\mathbf{B}^T \mathbf{A})^*, \quad (11)$$

where the symbol \circ indicates the Hadamard product between matrices and the symbol $*$ denotes the entrywise complex conjugate of the matrix.

Matrix \mathbf{P} is normalized on the columns, i.e.,

$$\sum_{\mu} P_{\mu,i} = 1 \quad \forall i, \quad (12)$$

since each input i is mapped with a certain probability onto one of the possible N measurement outcomes, so that the total probability sums to 1. This follows from the measurement completeness condition and holds both for von Neumann measurements and for POVMs. If also

$$\sum_i P_{\mu,i} = 1 \quad \forall \mu, \quad (13)$$

then matrix \mathbf{P} is normalized on both columns and rows and thus is called *doubly stochastic*. As we show below that the double stochasticity of \mathbf{P} is a necessary and sufficient condition for the determination of a unique orthogonal measurement minimizing the average final entropy in (7).

We recall here the main properties of doubly stochastic matrices [11].

Theorem 1. Birkhoff's theorem. The set of $n \times n$ doubly stochastic matrices is a convex set whose extreme points are the permutation matrices.

A very useful corollary to Birkhoff's theorem is the following:

Corollary 1. The maximum (minimum) of a convex (concave) real-valued function on the set of doubly stochastic $n \times n$ matrices is attained at a permutation matrix.

Given the convexity of the entropy function to minimize, we may apply the above corollary to (1) to derive that the average final entropy is minimum when \mathbf{P} is a permutation matrix (i.e., with a single element equal to 1 for each row and column and null otherwise). This corresponds, as observed earlier, to each row of \mathbf{Q} having just one element equal to 1 and the others equal to 0, $Q_{i,\mu} \in \{0; 1\}$.

Without loss of generality (and optimality), we can restrict the class of permutation matrices to the identity matrix $\mathbb{1}$ since any other permutation matrix may be obtained by applying a permutation \mathbf{R} to the identity.

Thus, the objective is to find the coefficients of \mathbf{B} such that

$$\mathbf{B}^T \mathbf{A} \rightarrow \mathbb{1}. \quad (14)$$

By multiplying the left side by a permutation matrix \mathbf{R} ,

$$\mathbf{R} \mathbf{B}^T \mathbf{A} \rightarrow \mathbf{R} \mathbb{1} = \mathbf{R}, \quad (15)$$

it is possible to explore all the other possible optimal solutions with swapped rows and columns, leading to the same value of minimal entropy. Relation (14) is realized with equality only when \mathbf{A} is also orthonormal, i.e., Alice sends orthogonal signals. For nonorthogonal signals, the optimal matrix \mathbf{B} realizing (14) is the closest orthonormal matrix which approximates \mathbf{A} in the least-squares sense.

In order to solve matrix equation (14) for unknown \mathbf{B} (matrix \mathbf{A} is given by Alice's choice of signal states), we make use of the Eckart-Young [9] and Mirsky [12] theorems of linear

algebra in the “minimal transformation to orthonormality” formulation derived by Johnson [13]. We briefly recall the main statement and proof of this theorem.

Theorem 2. Johnson's theorem. Let \mathbf{X} be an $n \times n$ complex full-rank matrix. Then the *minimal transformation to orthonormality* approximating \mathbf{X} is given by \mathbf{Z} such that

$$\text{Objective function: } \min \text{Tr}\{(\mathbf{X} - \mathbf{Z})^T (\mathbf{X} - \mathbf{Z})\}, \quad (16)$$

$$\text{Constraint: } \mathbf{Z}^T \mathbf{Z} = \mathbb{1}, \quad (17)$$

where Tr indicates the trace of the matrix.

The proof of Johnson's theorem is based on the Eckart-Young formulation of the SVD, allowing the derivation of the orthonormal matrix \mathbf{Z} minimizing (16). Note that the objective function (16) is equivalent to

$$\min \text{Tr}\{(\mathbf{Z}^T \mathbf{X} - \mathbb{1})^T (\mathbf{Z}^T \mathbf{X} - \mathbb{1})\}, \quad (18)$$

thus translating into the closest approximation to the identity of matrix $\mathbf{Z}^T \mathbf{X}$. In our notation, Johnson's \mathbf{X} matrix corresponds to Alice's \mathbf{A} , while \mathbf{Z} is Bob's \mathbf{B} . Matrix \mathbf{A} can be decomposed into the product of matrix \mathbf{U} , having as columns the eigenvectors of $\mathbf{A} \mathbf{A}^T$; the diagonal singular-value matrix $\mathbf{\Sigma}$; and matrix \mathbf{V} , having as columns the eigenvectors of $\mathbf{A}^T \mathbf{A}$:

$$\mathbf{A} = \mathbf{U} \mathbf{\Sigma} \mathbf{V}^T, \quad (19)$$

where $\mathbf{U} \mathbf{U}^T = \mathbb{1}$ and $\mathbf{V} \mathbf{V}^T = \mathbb{1}$. The orthonormal matrix \mathbf{B} that best approximates \mathbf{A} ,

$$\min \text{Tr}(\mathbf{B} - \mathbf{A})^T (\mathbf{B} - \mathbf{A}), \quad (20)$$

is given by

$$\mathbf{B} = \mathbf{U} \mathbf{V}^T, \quad (21)$$

which is the product of the two orthonormal matrices derived from the SVD decomposition of \mathbf{A} . Note that whenever \mathbf{A} admits distinct singular values, the solution defined by (21) is unique up to column permutations and yields

$$\mathbf{B}^T \mathbf{A} = \mathbf{V} \mathbf{\Sigma} \mathbf{V}^T, \quad (22)$$

which defines a symmetric matrix (as the right-side and left-side orthonormal matrices are identical).

Being symmetric, \mathbf{P} resulting from (11) is a doubly stochastic matrix. Thus, if \mathbf{P} is a doubly stochastic matrix, the optimal measurement matrix \mathbf{B} maximizing the average information gain (1) is derived by virtue of Birkhoff's theorem by (15) and *uniquely defined* by (21).

Conversely, assuming that $\mathbf{B} = \mathbf{U} \mathbf{V}^T$ is the optimal solution to maximizing the average information gain, substituting (22) into (11), we obtain a doubly stochastic matrix. The proof of the latter implication is a straightforward consequence of the symmetry of the matrix product (22). We are able, therefore, to state that double stochasticity is a *necessary and sufficient condition* for the determination of a unique optimal orthonormal \mathbf{B} of the form $\mathbf{B} = \mathbf{U} \mathbf{V}^T$.

So far, the search for Bob's optimal measurement assumed a doubly stochastic matrix \mathbf{P} . We wish now to explore optimality while relaxing this initial condition. By definition \mathbf{P} is positive semidefinite because its elements correspond to the transition probabilities between Alice's states and Bob's measurement vectors. In probabilistic terms, \mathbf{P} is a stochastic

matrix describing the transitions of a Markov chain [14]. When Alice's states are linearly independent, \mathbf{P} is, in fact, strictly positive. We recall here the following set of results for strictly positive $n \times n$ matrices derived by Marcus and Newman [15] and Sinkhorn and Knopp [16].

Theorem 3. Sinkhorn's theorem. Let \mathbf{X} be a strictly positive $n \times n$ matrix. Then to \mathbf{X} there corresponds a unique doubly stochastic matrix \mathbf{T}_X which can be expressed in the form

$$\mathbf{T}_X = \mathbf{D}_1 \mathbf{X} \mathbf{D}_2, \quad (23)$$

where \mathbf{D}_1 and \mathbf{D}_2 are diagonal matrices with positive entries. \mathbf{D}_1 and \mathbf{D}_2 are unique themselves up to a scalar factor.

The doubly stochastic matrix \mathbf{T}_X is derived as a limit of the sequence of matrices generated by alternately normalizing the rows and the columns of \mathbf{X} until convergence. A sufficient condition for this scaling process to converge is provided by the following.

Corollary 2. Marcus and Newman corollary. If \mathbf{X} is strictly positive and symmetric, there exists a diagonal matrix \mathbf{D} with positive main diagonal entries such that

$$\mathbf{T}_X = \mathbf{D} \mathbf{X} \mathbf{D} \quad (24)$$

is doubly stochastic.

Sinkhorn and Knopp [16] later showed that the sequence of matrices generated by alternately normalizing the rows and the columns of \mathbf{X} converges to the doubly stochastic limit $\mathbf{T}_X = \mathbf{D}_1 \mathbf{X} \mathbf{D}_2$ if and only if $\mathbf{X} \neq 0$ and each positive entry of \mathbf{X} is contained in a positive diagonal.

Matrices for which the normalizing sequence converges are called *scalable*. For such matrices, the best-known scaling algorithm consists of applying a ‘‘coordinate-descending’’ method known as *RAS* or *biproportional fitting* algorithm [17,18]. Note that in all cases in which the algorithm converges to a doubly stochastic matrix, we return to the same initial assumptions enabling the implementation of Johnson's theorem and thus to the same optimal solution (21). The latter consideration also provides an answer to the question raised long ago in the seminal work by Hausladen and Wootters discussing the optimality of their ‘‘pretty good measurement’’ with respect to maximizing average information gain [19]. Their density operator ρ corresponds to

$$\rho = \mathbf{A}^T \mathbf{A} \quad (25)$$

and thus the pretty-good-measurement matrix to $\mathbf{M} = \mathbf{A}(\mathbf{A}^T \mathbf{A})^{-\frac{1}{2}}$. By substituting the SVD expression $\mathbf{A} = \mathbf{U} \mathbf{\Sigma} \mathbf{V}^T$ and taking into account the unitarity of \mathbf{U} and \mathbf{V} , it is straightforward to check that $\mathbf{M} = \mathbf{U} \mathbf{V}^T$ coincides with the optimal \mathbf{B} . This provides a rigorous demonstration of the optimality of their pretty good measurement by virtue of the scaling properties of the probability.

We summarize our findings in the following theorem.

Theorem 4. Optimal detection of nonorthogonal signals. Let $|\psi_i\rangle$, $i = 1, 2, \dots, N$, be a set of nonorthogonal linearly independent signal states on Alice's Hilbert space \mathcal{H}_A and $|\Phi_\mu\rangle$, $\mu = 1, 2, \dots, N$, be a set of orthonormal states on Bob's \mathcal{H}_B , with $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = N$. Let \mathbf{A} and \mathbf{B} be the matrices with these states as column vectors and $\mathbf{P} = (\mathbf{B}^T \mathbf{A}) \circ (\mathbf{B}^T \mathbf{A})^*$ be the corresponding stochastic matrix of transition probabilities. The following propositions hold: If

(1) \mathbf{P} is doubly stochastic, (2) \mathbf{P} is strictly positive and symmetric, or (3) \mathbf{P} is *scalable* to a doubly stochastic limit matrix, then the optimal von Neumann measurement \mathbf{B} maximizing the average information gain defined in (1) is uniquely determined by $\mathbf{B} = \mathbf{U} \mathbf{V}^T$, where \mathbf{U} and \mathbf{V} are unitary operators diagonalizing $\mathbf{A} \mathbf{A}^T$ and $\mathbf{A}^T \mathbf{A}$, respectively.

III. COLLECTIVE VERSUS INDIVIDUAL MEASUREMENTS

In this section, we use the results derived above to compare individual and collective von Neumann measurements. The question is motivated by considering a general QKD scenario in which Alice transmits a sequence of K ($K \geq 2$) signals. Instead of measuring each signal individually, Bob may decide to store the K signals in a quantum memory and perform a collective measurement. We will consider the case with $K = 2$ independent signals because the result can then be trivially extended to any $K > 2$. We may think of them as states belonging to consecutive time slots (i.e., generated by QKD systems operating in time-division multiplexing). If each of the signals is represented as before by $|\Psi_i\rangle$, $i = 1, 2, \dots, N$, the possible pairs are represented by $|\Psi_{i,j}\rangle$, $i, j = 1, 2, \dots, N$, in the Hilbert space of dimension $N^2 \mathcal{H}_A \otimes \mathcal{H}_A$:

$$|\Psi_{i,j}\rangle = |\Psi_i\rangle \otimes |\Psi_j\rangle \quad \forall i, j = 1, 2, \dots, N, \quad (26)$$

where \otimes is the tensor or Kronecker product. Let \mathbf{A}_2 be the matrix with the vectors $|\Psi_{i,j}\rangle$ as columns, or, equivalently,

$$\mathbf{A}_2 = \mathbf{A} \otimes \mathbf{A}. \quad (27)$$

Among Bob's joint measurements we may further distinguish between collective (or joint) uncorrelated measurements described by tensor-product states or collective *entangled* measurements. For example, Ref. [5] showed that for the so-called *double-trine* states the optimal measurement was global and entangled. Later, Wootters [6] determined a global yet unentangled measurement that performed equally well in obtaining the same optimal mutual information gain. Analogously, in our case Bob may consider collective von Neumann measurements defined by product states

$$|\Phi_{\mu,\nu}\rangle = |\Phi_\mu\rangle \otimes |\Phi_\nu\rangle \quad \forall \mu, \nu = 1, 2, \dots, N \quad (28)$$

or by general superpositions of such states (including entangled ones)

$$|\Phi_{M,N}\rangle = \sum_{\mu,\nu} B_{\mu,\nu;M,N} |\Phi_\mu\rangle \otimes |\Phi_\nu\rangle. \quad (29)$$

The corresponding elements of the probability matrix \mathbf{P} are labeled by a double-index measurement result and a double-index input signal:

$$P_{M,N;i,j} = |\langle \Phi_{M,N} | \Psi_{i,j} \rangle|^2 \quad (30)$$

$$= \left| \sum_{\mu,\nu} B_{\mu,\nu;M,N} \langle \Phi_\mu | \Psi_i \rangle \langle \Phi_\nu | \Psi_j \rangle \right|^2. \quad (31)$$

For product states, the matrix \mathbf{B}_2 , having the set of orthonormal vectors $|\Phi_{i,j}\rangle = |\Phi_i\rangle |\Phi_j\rangle$ as columns, can be written as

$$\mathbf{B}_2 = \mathbf{B} \otimes \mathbf{B}. \quad (32)$$

Analogously, for general superposition including entangled measurements, \mathbf{B}_2 corresponds to linear combinations of such products,

$$\mathbf{B}_2 = \sum_{\mu,v} B_{\mu,v} \mathbf{B}_\mu \otimes \mathbf{B}_v, \quad (33)$$

where the multi-index μ in matrix \mathbf{B}_μ defines a specific permutation of the column vectors $|\Phi_i\rangle$, $i = 1, 2, \dots, N$, and the superposition coefficients $B_{\mu,v} \in \mathbb{C}$ are normalized in the square modulus $\sum_{\mu,v} |B_{\mu,v}|^2 = 1$.

The optimal von Neumann product measurement leads to the probability matrix \mathbf{P}_2 as

$$\begin{aligned} \mathbf{P}_2 &= (\mathbf{B}_2^T \cdot \mathbf{A}_2) \circ (\mathbf{B}_2^T \cdot \mathbf{A}_2)^* \\ &= [(\mathbf{B} \otimes \mathbf{B})^T \cdot (\mathbf{A} \otimes \mathbf{A})] \circ [(\mathbf{B} \otimes \mathbf{B})^T \cdot (\mathbf{A} \otimes \mathbf{A})]^* \\ &= [(\mathbf{B}^T \cdot \mathbf{A}) \otimes (\mathbf{B}^T \cdot \mathbf{A})] \circ [(\mathbf{B}^T \cdot \mathbf{A}) \otimes (\mathbf{B}^T \cdot \mathbf{A})]^* \\ &= [(\mathbf{B}^T \cdot \mathbf{A}) \circ (\mathbf{B}^T \cdot \mathbf{A})^*] \otimes [(\mathbf{B}^T \cdot \mathbf{A}) \circ (\mathbf{B}^T \cdot \mathbf{A})^*] \\ &= \mathbf{P} \otimes \mathbf{P}, \end{aligned} \quad (34)$$

where the mixed-product property for Kronecker and Hadamard products was used, along with Eqs. (11), (27), and (32). For general superposition measurements, each term in (34) ($\mathbf{B}_2^T \cdot \mathbf{A}_2$) becomes

$$\left(\sum_{\mu,v} B_{\mu,v} \mathbf{B}_\mu \otimes \mathbf{B}_v \right)^T \cdot (\mathbf{A} \otimes \mathbf{A}). \quad (35)$$

To derive the optimal superposition measurement, we use the optimization for the optimal \mathbf{B} in (16),

$$\begin{aligned} \min \operatorname{Tr} \left\{ \left[(\mathbf{A} \otimes \mathbf{A}) - \left(\sum_{\mu,v} B_{\mu,v} \mathbf{B}_\mu \otimes \mathbf{B}_v \right) \right]^T \right. \\ \left. \times \left[(\mathbf{A} \otimes \mathbf{A}) - \left(\sum_{\mu',v'} B_{\mu',v'} \mathbf{B}_{\mu'} \otimes \mathbf{B}_{v'} \right) \right] \right\}, \end{aligned} \quad (36)$$

which leads to the following equivalent condition, after the products within the trace are developed:

$$\begin{aligned} \max \operatorname{Tr} \left(\sum_{\mu,v} B_{\mu,v} (\mathbf{B}_\mu^T \mathbf{A}) \otimes (\mathbf{B}_v^T \mathbf{A}) \right) \\ = \max \sum_{\mu,v} B_{\mu,v} \operatorname{Tr}(\mathbf{B}_\mu^T \mathbf{A}) \operatorname{Tr}(\mathbf{B}_v^T \mathbf{A}) \\ \leq \max \sum_{\mu,v} |B_{\mu,v}| \operatorname{Tr}(\mathbf{B}_\mu^T \mathbf{A}) \operatorname{Tr}(\mathbf{B}_v^T \mathbf{A}) \\ \leq \max [\operatorname{Tr}(\mathbf{B}_\mu^T \mathbf{A}) \operatorname{Tr}(\mathbf{B}_v^T \mathbf{A})], \end{aligned} \quad (37)$$

under the orthogonality condition for matrices \mathbf{B}_μ and \mathbf{B}_v .

In the above relations we used the linearity of the trace operator, the property $\operatorname{Tr}(\mathbf{X} \otimes \mathbf{Y}) = \operatorname{Tr}(\mathbf{X})\operatorname{Tr}(\mathbf{Y})$, and the fact that the maximum of a convex combination is in one of the extreme points. Recalling the derivation in Johnson's theorem in [13], determining $\max \operatorname{Tr}(\mathbf{B}_\mu^T \mathbf{A})$ leads to a unique optimal solution \mathbf{B} up to column permutations.

The result indicates that the matrix of the collective measurement probability \mathbf{P}_2 can be written as a Kronecker product of the matrices representing the individual measurement probabilities \mathbf{P} for both product and superposition measurements.

Thus, there is no information gain in performing a collective measurement—either uncorrelated or entangled—over two (or more) nonorthogonal signals when using a von Neumann projection.

IV. OPTIMAL UNAMBIGUOUS STATE DISCRIMINATION

Optimal unambiguous state discrimination (USD) was first solved for the case of two signals by Ivanovic [20], Dieks [21], and Peres [22] and for three signals by Peres and Terno [23]. Partial results for N nonorthogonal linearly independent signals were provided by Chefles [24], while a complete solution in terms of semidefinite programming was found by Eldar [8] and improved recently by Karimi [25].

Optimal USD is based on POVMs. Whereas a projective or von Neumann measurement generates probabilities, a USD POVM either identifies the correct state with certainty or generates an inconclusive answer. Referring to the above definition of $Q_{i,\mu}$ (3), applying a USD POVM, we have

$$Q_{i,\mu} = \delta_{i\mu} \quad \forall i, \mu = 1, \dots, N, \quad (38)$$

where $\delta_{i\mu}$ is the Kronecker delta, and thus, (6) becomes

$$H_\mu = 0 \quad \forall \mu = 1, \dots, N. \quad (39)$$

Therefore, the only non-null term contributing to the final entropy is the one associated with the inconclusive answer $\mu = 0$:

$$Q_{i,0} = \frac{P_{0,i} r_i}{q_0} \quad \forall i = 1, \dots, N, \quad (40)$$

and correspondingly,

$$H_0 = - \sum_i Q_{i,0} \log_2(Q_{i,0}), \quad (41)$$

$$\langle H_{\text{fin}} \rangle = q_0 H_0 = - \sum_i P_{0,i} \log_2 \left(\frac{P_{0,i}}{\sum_j P_{0,j}} \right). \quad (42)$$

In the following the final entropy is optimized by minimizing the probability of an inconclusive result. Indeed, by setting $P_{0,i} = p_{\text{inc}}$, $i = 1, \dots, N$, we obtain

$$\langle H_{\text{fin}} \rangle = p_{\text{inc}} \log_2(N), \quad (43)$$

where we also used equal probabilities for Alice's input states $|\Psi_i\rangle$.

The optimal POVM operators $\{\Pi_i\}_{i=0,1,\dots,N}$ such that

$$\sum_{i=0}^N \Pi_i = \mathbb{1}, \quad \sum_{i=1}^N \Pi_i \leq \mathbb{1} \quad (44)$$

can be derived following the demonstration in [8]. Let $|\tilde{\Psi}\rangle$ be the reciprocal states associated with Alice's states $|\Psi\rangle$, such that $\langle \Psi_h | \tilde{\Psi}_k \rangle = \delta_{hk}$ ($1 \leq h, k \leq N$); i.e., the reciprocal states are orthogonal to Alice's states. Define

$$\Pi_i = (1 - p_{\text{inc}}) |\tilde{\Psi}_i\rangle \langle \tilde{\Psi}_i| \quad (45)$$

and $\tilde{\mathbf{A}}$ as the matrix whose columns are the reciprocal states $|\tilde{\Psi}_i\rangle$, $i = 1, \dots, N$. The matrix $\tilde{\mathbf{A}}$ is orthogonal to \mathbf{A} , i.e.,

$$\tilde{\mathbf{A}}^T \cdot \mathbf{A} = \mathbb{1}, \quad (46)$$

showing similarity to Eq. (14) for the von Neumann case. The solution can be found by resorting to the Moore-Penrose

pseudoinverse [26], i.e.,

$$\tilde{\mathbf{A}}^T = (\mathbf{A}^T \mathbf{A})^{-1} \mathbf{A}^T. \quad (47)$$

By applying the SVD to $\mathbf{A} = \mathbf{A} \mathbf{\Sigma} \mathbf{V}^T$, we find that the matrix of the reciprocal states is given by

$$\tilde{\mathbf{A}} = \mathbf{U} \mathbf{\Sigma}^{-1} \mathbf{V}^T; \quad (48)$$

i.e., its singular values are the inverse of those of \mathbf{A} but with the same eigenvector matrices \mathbf{U} and \mathbf{V} .

For equiprobable signals, the summation in (44) is equal to

$$(1 - p_{\text{inc}}) \sum_{i=1}^N |\tilde{\Psi}_i\rangle \langle \tilde{\Psi}_i| = \tilde{\mathbf{A}} \tilde{\mathbf{A}}^T = \mathbf{U} \mathbf{\Sigma}^{-2} \mathbf{U}^T, \quad (49)$$

and the probability of a conclusive result (i.e., $1 - p_{\text{inc}}$) is maximized when it is equal to the inverse of the maximum eigenvalue of $\sum_i |\tilde{\Psi}_i\rangle \langle \tilde{\Psi}_i|$ or, equivalently, to the minimum singular value of $\mathbf{\Sigma}^2$.

V. PAIRS OF NONORTHOGONAL SIGNALS

We examine first the application of the present framework to the case of a single qubit in two equally likely nonorthogonal states. Such states are representative of the nonorthogonal signals used in some QKD protocols [27,28]. The angle between them is identified as $\theta \in (0, \pi/2]$. When $\theta = \pi/2$, the two signals become orthogonal and thus perfectly distinguishable by a standard von Neumann measurement in the same basis. The signals can be generally expressed as

$$\Psi_1 = \begin{pmatrix} \cos(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) \end{pmatrix}, \quad \Psi_2 = \begin{pmatrix} \cos(\frac{\theta}{2}) \\ -\sin(\frac{\theta}{2}) \end{pmatrix}, \quad (50)$$

which correspond to Bennett *et al.*'s "parity bits" [29].

By replacing $c = \cos(\frac{\theta}{2})$ and $s = \sin(\frac{\theta}{2})$, the corresponding matrix \mathbf{A} is given by

$$\mathbf{A} = \begin{pmatrix} \cos(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \\ \sin(\frac{\theta}{2}) & -\sin(\frac{\theta}{2}) \end{pmatrix} = \begin{pmatrix} c & c \\ s & -s \end{pmatrix} \quad (51)$$

and can be SVD decomposed into

$$\begin{aligned} \mathbf{A} &= \mathbf{U} \mathbf{\Sigma} \mathbf{V}^T \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{2}c & 0 \\ 0 & \sqrt{2}s \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}. \end{aligned} \quad (52)$$

Based on (21), the optimal von Neumann measurement is thus

$$\mathbf{B} = \mathbf{U} \mathbf{V}^T = \mathbf{V}^T = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (53)$$

i.e., a rotation by $\pi/4$ of Alice's basis, followed by a reflection.

The associated probability matrix for individual measurements is

$$\begin{aligned} \mathbf{P} &= (\mathbf{V} \mathbf{\Sigma} \mathbf{V}^T) \circ (\mathbf{V} \mathbf{\Sigma} \mathbf{V}^T)^* = \frac{1}{2} \begin{pmatrix} (c+s)^2 & (c-s)^2 \\ (c-s)^2 & (c+s)^2 \end{pmatrix} \\ &= \frac{1}{2} \begin{pmatrix} 1 + \sin(\theta) & 1 - \sin(\theta) \\ 1 - \sin(\theta) & 1 + \sin(\theta) \end{pmatrix}. \end{aligned} \quad (54)$$

Note that \mathbf{P} is doubly stochastic since the sum of the elements in each row is equal to 1, as is the sum of the elements in each column. Indeed, each element of \mathbf{V} has a square value of $1/2$, which is a sufficient condition for the doubly stochasticity of \mathbf{P} . When $\theta = \pi/2$ (i.e., the two signals are orthogonal), $\mathbf{P} = \mathbb{1}$ and reaches the maximum possible entropy.

The average information gain for von Neumann measurements computed from (1)–(7) is

$$I_{\text{av}} = 1 + \frac{(c+s)^2}{2} \log_2 \frac{(c+s)^2}{2} + \frac{(c-s)^2}{2} \log_2 \frac{(c-s)^2}{2}. \quad (55)$$

With POVM measurements, the probability of an inconclusive result is derived from the smallest singular value of $\mathbf{\Sigma}$ (i.e., $\sqrt{2}s$), leading to $p_{\text{inc}} = 1 - (\sqrt{2}s)^2$. The average information gain is obtained by applying (1) and (43), leading to $I_{\text{av}} = 2s^2$.

For the case of two nonorthogonal signals, a generic SO(2) rotation matrix can be written as

$$\mathbf{B}_{\text{SO}(2)} = \begin{pmatrix} \cos(\phi) & -\sin(\phi) \\ \sin(\phi) & \cos(\phi) \end{pmatrix}, \quad (56)$$

with $\phi \in (0, 2\pi]$. In this case it is easily seen that the generic $\mathbf{B}_{\text{SO}(2)}$ matrix leads to a scalable $\mathbf{P}_{\text{SO}(2)}$ in the sense of Theorem 4 since

$$\begin{aligned} \mathbf{P}_{\text{SO}(2)} &= (\mathbf{B}_{\text{SO}(2)}^T \mathbf{A}) \circ (\mathbf{B}_{\text{SO}(2)}^T \mathbf{A})^* \\ &= \begin{pmatrix} [c \cos(\phi) + s \sin(\phi)]^2 & [c \cos(\phi) - s \sin(\phi)]^2 \\ [c \sin(\phi) - s \cos(\phi)]^2 & [c \sin(\phi) + s \cos(\phi)]^2 \end{pmatrix} \end{aligned} \quad (57)$$

is doubly stochastic $\forall \theta \in (0, \pi/2]$ if and only if

$$\sin^2(\phi) = \cos^2(\phi) \Rightarrow \sin(\phi) = \pm \cos(\phi), \quad (58)$$

leading to the same optimal \mathbf{B} derived in Eq. (53) and demonstrating the uniqueness of the optimal solution and its convergence.

For collective measurements on pairs of two signals $\Psi_i \otimes \Psi_j$ ($i, j = 1, 2$), the resulting matrix \mathbf{A} is

$$\begin{aligned} \mathbf{A}_2 &= \begin{pmatrix} c^2 & c^2 & c^2 & c^2 \\ cs & -cs & cs & -cs \\ cs & cs & -cs & -cs \\ s^2 & -s^2 & -s^2 & s^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1/\sqrt{2} & 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \begin{pmatrix} 2c^2 & 0 & 0 & 0 \\ 0 & 2cs & 0 & 0 \\ 0 & 0 & 2cs & 0 \\ 0 & 0 & 0 & 2s^2 \end{pmatrix} \\ &\times \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ \sqrt{2} & 0 & 0 & -\sqrt{2} \\ 0 & -\sqrt{2} & \sqrt{2} & 0 \\ -1 & 1 & 1 & -1 \end{pmatrix}, \end{aligned} \quad (59)$$

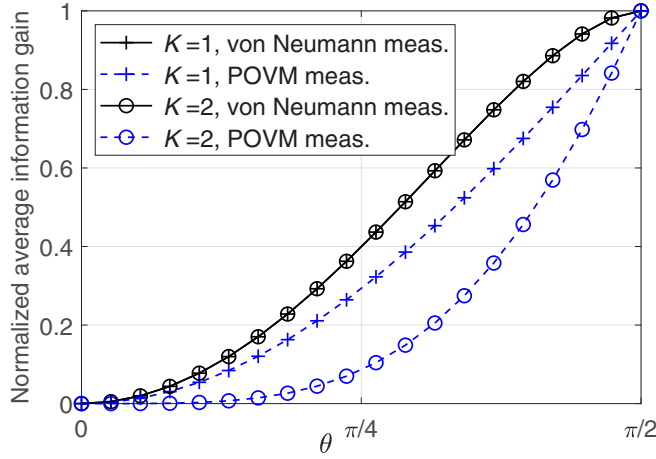


FIG. 1. Average information gain vs the angle between the two nonorthogonal signals θ for individual ($K = 1$) and collective ($K = 2$) measures normalized to K .

whereas the optimal von Neumann measurement is

$$\mathbf{B}_2 = \mathbf{U}_2 \mathbf{V}_2^T = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \mathbf{B} \otimes \mathbf{B}, \quad (60)$$

leading to the probability matrix

$$\mathbf{P}_2 = \frac{1}{4} \begin{pmatrix} (c+s)^4 & (c^2-s^2)^2 & (c^2-s^2)^2 & (c-s)^4 \\ (c^2-s^2)^2 & (c+s)^4 & (c-s)^4 & (c^2-s^2)^2 \\ (c^2-s^2)^2 & (c-s)^4 & (c+s)^4 & (c^2-s^2)^2 \\ (c-s)^4 & (c^2-s^2)^2 & (c^2-s^2)^2 & (c+s)^4 \end{pmatrix} = \mathbf{P} \otimes \mathbf{P}. \quad (61)$$

With POVM measurements, the probability of an inconclusive result is derived from the square of the smallest singular value of Σ (i.e., $2s^2$), leading to $p_{\text{inc}} = 1 - (2s^2)^2$. The average information gain obtained from (1), (2), and (43) is thus

$$I_{\text{av}} = \log_2(4) - [1 - (2s^2)^2] \log_2(4) = 8s^4. \quad (62)$$

The quantitative results presented in this section are represented in Fig. 1, which shows the average information gain for optimal von Neumann and POVM measurements. Individual ($K = 1$) and collective ($K = 2$) measurements are compared, and thus, the average information gain is normalized to K . The maximum information gain is achieved with the von Neumann measurements independently of the type of measurement (i.e., individual or collective). The I_{av} advantage of von Neumann with respect to POVM measurements is plotted in Fig. 2, which shows that performing collective POVM measurements reduces the information gain. This behavior is possibly attributable to the fact that the entropy of inconclusive results is spread over a larger number of signals and increases with the dimension of the spanned Hilbert space.

VI. QUANTUM STATE AFTER THE MEASUREMENT AND VON NEUMANN ENTROPY

Bob's measurement and its related information gain generate a disturbance of the initial quantum state sent by Alice.

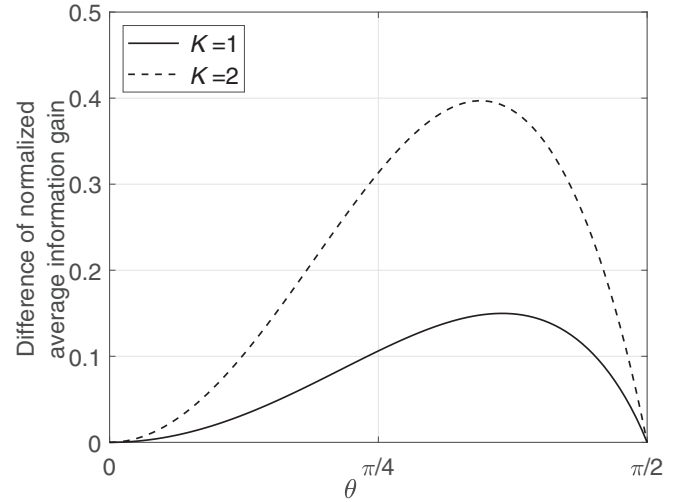


FIG. 2. Difference of normalized average information gain (between von Neumann and POVM measurements) as a function of θ for individual ($K = 1$) and collective ($K = 2$) measures.

The trade-off between information gained during a measurement and quantum state disturbance is an important factor in a cryptographic protocol and was first analyzed for nonorthogonal signals by Fuchs and Peres [30]. In their work, the disturbance (discrepancy rate) on each of Alice's n signals $\{|\Psi_i\rangle\}$ was defined as

$$D = 1 - \langle \Psi_i | \rho_{\text{fin},i} | \Psi_i \rangle, \quad (63)$$

where $\langle \Psi_i | \rho_{\text{fin},i} | \Psi_i \rangle = F$ denotes the fidelity between the initial state $|\Psi_i\rangle$ and the final state after the measurement $\rho_{\text{fin},i}$.

For initial and final mixed states, the definition can be modified using Jozsa's approach for density matrices' fidelity [31]

$$D = 1 - F(\rho_{\text{in}}, \rho_{\text{fin}}) = [Tr(\sqrt{\sqrt{\rho_{\text{in}}}\rho_{\text{fin}}\sqrt{\rho_{\text{in}}}})]^2, \quad (64)$$

where $\rho_{\text{in}} = \sum_i r_i |\Psi_i\rangle \langle \Psi_i|$ is the statistical mixture of Alice's input states, while the state after the measurement becomes

$$\rho_{\text{fin}}^{\text{vN}} = \sum_{\mu} P_{\mu} \rho_{\text{in}} P_{\mu} \quad (65)$$

for a von Neumann projective measurement with $P_{\mu} = |\Phi_{\mu}\rangle \langle \Phi_{\mu}|$ and

$$\rho_{\text{fin}}^{\text{POVM}} = \sum_{\mu} \sqrt{\Pi_{\mu}} \rho_{\text{in}} \sqrt{\Pi_{\mu}} \quad (66)$$

for a POVM $\{\Pi_{\mu}\}_{\mu=0,1,\dots,N}$, as defined in (44) [32].

In our case, assuming an initial density operator given by an equal distribution over Alice's input states $|\Psi_i\rangle$, the final density operator resulting from the measurement is

$$\rho_{\text{fin}}^{\text{vN}} = \sum_{\mu} \sum_i \frac{1}{N} |\langle \Phi_{\mu} | \Psi_i \rangle|^2 |\Phi_{\mu}\rangle \langle \Phi_{\mu}| \quad (67)$$

for a von Neumann measurement and

$$\rho_{\text{fin}}^{\text{POVM}} = \sum_{\mu} \sum_i \frac{(1 - p_{\text{inc}})}{N} |\langle \tilde{\Psi}_{\mu} | \Psi_i \rangle|^2 |\tilde{\Psi}_{\mu}\rangle \langle \tilde{\Psi}_{\mu}| \quad (68)$$

for a POVM. In both cases we may compare the disturbance produced on the state with the information gained by the measurement.

Another way to evaluate the impact of the measurement on the quantum state transmitted by Alice is to compute the von Neumann entropy of the density operator before and after the measurement.

Analogously to the disturbance factor, the change in von Neumann entropy also provides a measure of the modification produced by Bob's measurement. However, rather than being directly associated with the state fidelity, the von Neumann entropy is associated with the increase of disorder in the statistical mixture of states composing ρ_{in} .

We consider, for $\rho = \rho_{\text{in}}, \rho_{\text{fin}}$, the von Neumann entropy to be defined as [32,33]

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho) \quad (69)$$

and compare the entropy of the initial state with the entropy after the measurement. We refer to the case of the two equiprobable signals defined in (50) and use

$$\rho_{\text{in}} = \begin{pmatrix} c^2 & 0 \\ 0 & s^2 \end{pmatrix} \quad (70)$$

for the initial state. The state after the measurement can be computed by means of equations (65) and (66) and considering the optimal von Neumann and POVM measurements for two nonorthogonal signals analyzed in the previous section. The optimal von Neumann projectors are given by (53)

$$P_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad (71)$$

while the optimal USD POVM operators may be written as

$$\Pi_1 = \alpha(\mathbb{1} - |\Psi_2\rangle\langle\Psi_2|), \quad (72)$$

$$\Pi_2 = \alpha(\mathbb{1} - |\Psi_1\rangle\langle\Psi_1|), \quad (73)$$

$$\Pi_0 = \mathbb{1} - \Pi_1 - \Pi_2, \quad (74)$$

where the coefficient α is obtained by minimizing the probability of an inconclusive answer and can be expressed as $\alpha = (2c^2)^{-1}$. The optimal USD POVM operators for the states (50) are explicitly given by

$$\Pi_1 = \alpha \begin{pmatrix} s^2 & cs \\ cs & c^2 \end{pmatrix}, \quad (75)$$

$$\Pi_2 = \alpha \begin{pmatrix} s^2 & -cs \\ -cs & c^2 \end{pmatrix}, \quad (76)$$

$$\Pi_0 = \begin{pmatrix} c^2 - s^2 & 0 \\ 0 & 0 \end{pmatrix}, \quad (77)$$

where $c = \cos(\frac{\theta}{2})$ and $s = \sin(\frac{\theta}{2})$. Using the above expressions, by means of (65) and (66), we derive the density matrices after the measurement

$$\rho_{\text{fin}}^{\text{vN}} = \frac{1}{2} \mathbb{1} \quad (78)$$

and

$$\rho_{\text{fin}}^{\text{POVM}} = \frac{1}{2} \begin{pmatrix} 1 + \cos^2(\theta) & 0 \\ 0 & \sin^2(\theta) \end{pmatrix}. \quad (79)$$

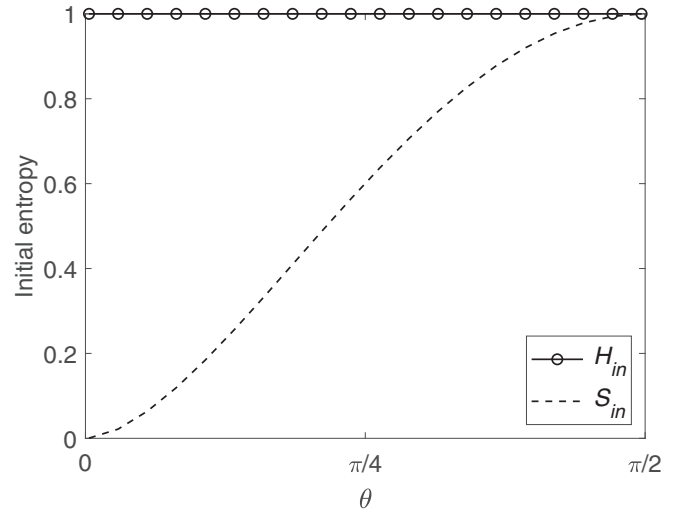


FIG. 3. Initial Shannon entropy H_{in} and von Neumann entropy S_{in} vs θ for individual von Neumann and POVM measures.

Figure 3 shows the initial Shannon entropy and von Neumann entropy as the angle between the two nonorthogonal signals defined in (77) increases. The corresponding final entropies for von Neumann and POVM measurements are represented in Fig. 4.

We observe that the initial von Neumann entropy is always increased by projective measurements, while POVMs may decrease it since the initial set of states is not forced into an equal distribution of perfectly distinguishable outcomes. Instead, for the same reason, the final Shannon entropy is lower than the von Neumann entropy, leading to a higher average information gain.

The von Neumann and Shannon entropies provide a complementary view of the disturbance on the state resulting from the measurement process, as shown in Fig. 5 for the two nonorthogonal signals. Indeed, the von Neumann entropy measures the closeness to a completely mixed state in the

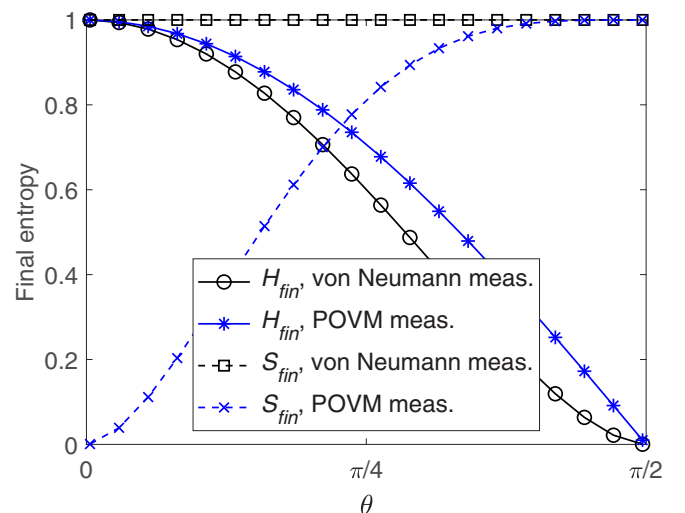


FIG. 4. Final Shannon entropy H_{fin} and von Neumann entropy S_{fin} vs θ for individual von Neumann and POVM measures.

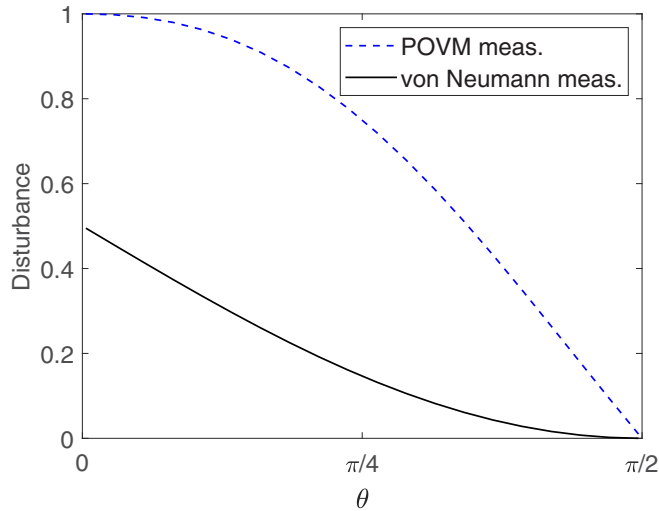


FIG. 5. Disturbance vs θ for individual von Neumann and POVM measures.

signal's Hilbert space. On the other hand, the Shannon entropy provides a view of the receiver's conditional probability distribution.

VII. CONCLUSIONS

The matrix-based formulation of the entropy optimization problem can be optimally solved for nonorthogonal signals by leveraging operator algebra and well-known theorems. We demonstrated that the optimal von Neumann measurements are unique and achieve the same information gain for individual and collective measurements regardless of whether they are uncorrelated or entangled. By contrast, not only is the information gain of POVMs lower than that for projective von Neumann measurements, but it also decreases when the number of signals collectively measured increases. We provided a comparative analysis of von Neumann and Shannon entropies to analyze the disturbance of the initial signal produced by the quantum measurement.

The present approach finds direct application in several QKD protocols based on weak coherent states. Such systems are also used to implement the Bennett-Brassard 1984 (BB84) protocol, in which each basis consists of two orthogonal signals. However, signal generation using weak coherent states and the effect of the transmission medium may affect the orthogonality of the signals received by Bob (or Eve). As such, the presented results can be applied to a given basis of the BB84 protocol to compute and optimize the average information gain in the considered basis.

ACKNOWLEDGMENTS

The authors wish to thank M. Travagnin, D. Bacco, C. De Lazzari, and T. Osborne for fruitful discussions on the topic and, in particular, A. Lewis for the accurate revision

of the manuscript. This work was funded by the European Commission as part of the JRC work program, Project No. 31920 SatCom4EU.

APPENDIX: MINIMIZING THE FINAL ENTROPY

The problem of minimizing the final entropy, i.e.,

$$\text{Min } H_\mu = \text{Min} \left(- \sum_{i=1}^N Q_{i,\mu} \log_2(Q_{i,\mu}) \right) \quad (\text{A1})$$

with the constraint that

$$\sum_{i=1}^N Q_{i,\mu} = 1, \quad (\text{A2})$$

can be solved using the method of Lagrange multipliers.

Let the Lagrange function be defined as

$$\begin{aligned} \mathcal{L}(Q_{1,\mu}, Q_{2,\mu}, \dots, \lambda) = & - \sum_i Q_{i,\mu} \log_2(Q_{i,\mu}) \\ & + \lambda \left(\sum_i Q_{i,\mu} - 1 \right). \end{aligned} \quad (\text{A3})$$

The optimization problem can be solved by imposing that the gradient of the Lagrange function is

$$\nabla_{Q_{1,\mu}, \dots, Q_{2,\mu}, \lambda} \mathcal{L}(Q_{1,\mu}, Q_{2,\mu}, \dots, \lambda) = 0. \quad (\text{A4})$$

The partial derivatives are

$$\frac{\partial}{\partial Q_{i,\mu}} \mathcal{L}(Q_{1,\mu}, Q_{2,\mu}, \dots, \lambda) = - \log_2 Q_{i,\mu} - \frac{1}{\ln 2} + \lambda, \quad (\text{A5})$$

$$\frac{\partial}{\partial \lambda} \mathcal{L}(Q_{1,\mu}, Q_{2,\mu}, \dots, \lambda) = \sum_i Q_{i,\mu} - 1. \quad (\text{A6})$$

By imposing the condition in (A4), the following system of equations is obtained:

$$\begin{aligned} - \log_2 Q_{i,\mu} - \frac{1}{\ln 2} + \lambda = 0 \quad \forall i = 1, \dots, N, \\ \sum_i Q_{i,\mu} - 1 = 0, \end{aligned} \quad (\text{A7})$$

which has the solution

$$Q_{i,\mu} = \frac{1}{N} \quad \forall i = 1, \dots, N. \quad (\text{A8})$$

This critical point leads to an entropy of

$$H_\mu = - \log_2 \frac{1}{N}, \quad (\text{A9})$$

and it is possible to demonstrate that it is a point of absolute maximum. Since the entropy is a continuous function, the points of absolute minimum are at the border, which is when

$$\begin{aligned} Q_{j,\mu} = 1 \quad j \in 1, 2, \dots, N, \\ Q_{i,\mu} = 0 \quad \forall i \neq j, i \in 1, 2, \dots, N. \end{aligned} \quad (\text{A10})$$

[1] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, *Appl. Phys. Lett.* **87**, 194108 (2005).

[2] K. Inoue, *IEEE J. Sel. Top. Quantum Electron.* **21**, 109 (2014).

- [3] A. Peres, *Quantum Theory: Concepts and Methods* (Springer, NY, USA, 1997).
- [4] J. Von Neumann, *Mathematical Foundations of Quantum Mechanics*, new ed. (Princeton University Press, Princeton, NJ, 2018).
- [5] A. Peres and W. K. Wootters, *Phys. Rev. Lett.* **66**, 1119 (1991).
- [6] W. K. Wootters, *Int. J. Quantum. Inf.* **4**, 219 (2006).
- [7] Y. C. Eldar and G. D. Forney, *IEEE Trans. Inf. Theory* **47**, 858 (2001).
- [8] Y. C. Eldar, *IEEE Trans. Inf. Theory* **49**, 446 (2003).
- [9] C. Eckart and G. Young, *Psychometrika* **1**, 211 (1936).
- [10] G. Grimmett and D. Welsh, *Probability: An Introduction* (Oxford University Press, Oxford, 2014).
- [11] R. Bhatia, *Matrix Analysis* (Springer, NY, USA, 1997).
- [12] L. Mirsky, *Q. J. Math.* **11**, 50 (1960).
- [13] R. M. Johnson, *Psychometrika* **31**, 61 (1966).
- [14] J. R. Norris, *Markov Chains* (Cambridge University Press, Cambridge, 1999).
- [15] M. Marcus and M. Newman, *Proc. Am. Math. Soc.* **16**, 826 (1965).
- [16] R. Sinkhorn and P. Knopp, *Pacific J. Math.* **21**, 343 (1967).
- [17] R. Stone and J. A. C. Brown, *A Computable Model of Economic Growth, A Programme for Growth 1*, London, Chapman and Hall (1962).
- [18] M. Bacharach, *Int. Econ. Rev.* **6**, 294 (1965).
- [19] P. Hausladen and W. K. Wootters, *J. Mod. Opt.* **41**, 2385 (1994).
- [20] I. D. Ivanovic, *Phys. Lett. A* **123**, 257 (1987).
- [21] D. Dieks, *Phys. Lett. A* **126**, 303 (1988).
- [22] A. Peres, *Phys. Lett. A* **128**, 19 (1988).
- [23] A. Peres and D. R. Terno, *J. Phys. A* **31**, 7105 (1998).
- [24] A. Chefles, *Phys. Lett. A* **239**, 339 (1998).
- [25] N. Karimi, *Chin. J. Phys.* **72**, 681 (2021).
- [26] R. Penrose, *Math. Proc. Cambridge Philos. Soc.* **51**, 406 (1955).
- [27] B. Huttner and A. Peres, *J. Mod. Opt.* **41**, 2397 (1994).
- [28] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, *Phys. Rev. A* **50**, 1047 (1994).
- [29] C. H. Bennett, T. Mor, and J. A. Smolin, *Phys. Rev. A* **54**, 2675 (1996).
- [30] C. A. Fuchs and A. Peres, *Phys. Rev. A* **53**, 2038 (1996).
- [31] R. Jozsa, *J. Mod. Opt.* **41**, 2315 (1994).
- [32] J. Preskill (unpublished), <http://theory.caltech.edu/~preskill/>.
- [33] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2016).