Security of quantum cryptography against individual attacks

Boris A. Slutsky,* Ramesh Rao, Pang-Chen Sun, and Y. Fainman
Department of Electrical and Computer Engineering, University of California, San Diego, Mail Code 0407, 9500 Gilman Drive, La Jolla, California 92093-0407

(Received 16 July 1997)

An attempt to eavesdrop on a quantum cryptographic channel reveals itself through errors it inevitably introduces into the transmission. We investigate the relationship between the induced error rate and the maximum amount of information the eavesdropper can extract, in both the two-state B92 [B92 refers to the work of C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992)] and the four-state BB84 [BB84 refers to the work of C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179] quantum cryptographic protocols. In each case, the optimal eavesdropping method that on average yields the most information for a given error rate is explicitly constructed. Analysis is limited to eavesdropping strategies where each bit of the quantum transmission is attacked individually and independently from other bits. Subject to this restriction, however, we believe that all attacks not forbidden by physical laws are covered. Unlike previous work, the eavesdropper's advantage is measured in terms of Renyi (rather than Shannon) information, and with respect only to bits received error-free by Bob (rather than all bits). This alters both the maximum extractable information and the optimal eavesdropping attack. The result can be used directly at the privacy amplification stage of the protocol to accomplish secure communication over a noisy channel. [S1050-2947(98)06304-5]

PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography is a technique which permits two parties, who share no secret information initially, to communicate over an open channel and establish between themselves a shared secret sequence of bits. Each bit of data is encoded using an alphabet of nonorthogonal states of a quantum particle, and therefore cannot be duplicated or measured in transit without inducing a disturbance that would ultimately be revealed through transmission errors. It is believed that no eavesdropping attack consistent with the laws of quantum mechanics can compromise the secret data unknowingly to the legitimate users of the channel. Principles and procedures of quantum cryptography have been described in the literature [1–5].

In practice, however, a communication is not completely free of errors even when no eavesdropping is present. To implement an unconditionally secure key exchange despite channel defects, the legitimate users, referred to as Alice and Bob, adopt the worst-case assumption that *all* of their errors are eavesdrop induced, and attempt to upper bound the information that may in such a case have fallen into the hands of their adversary, the eavesdropper Eve. If this upper bound is correctly estimated, a method known as (so-called ''*classical*'') *privacy amplification* permits Alice and Bob to distill from their transmission a shorter key that is unconditionally secure [4,6,7]. To establish a secret key in a noisy environment, therefore, the basic fact that no distinguishing information can be extracted from a pair of nonorthogonal states without perturbing them is no longer sufficient. Rather, it becomes necessary to relate the nonzero *extent* of the inflicted perturbation to the nonzero *amount* of the information that may be obtained.

Finding this relationship in the general case is a difficult quantum-theoretical problem, which takes somewhat varying forms depending on the particular perturbation and information measures that may be adopted [8]. In the context of quantum cryptography, early work was limited to specific classes of eavesdropping strategies, which broadened over time as the theory matured [4,9–14]. Until recently, only so-called *individual* attacks were considered, wherein each data-carrying particle is treated by the eavesdropper independently from other particles. In the most general such attack, the eavesdropper involves the carrier particle in an interaction with her own quantum system, referred to as *probe*, so that the particle and the probe are left in an entangled state, and a subsequent measurement of the probe yields information about the particle. Some investigators are now turning their attention to *collective* attacks, where the eavesdropper entangles a separate probe with each particle but measures all probes as a single quantum system, and to even more general *joint* attacks, where a single probe is entangled with the entire set of particles [15–17]. Such attacks are especially difficult to analyze, because they can take advantage of the various parity-type relationships between data bits, disclosed by Alice and Bob subsequently in the protocol. Eavesdropping can therefore no longer be considered separately from error correction and privacy amplification. Although collective and joint attacks have stimulated a great deal of interest, at present they seem impractical due to their complexity [12,14], and their theory is still at an early stage of development. No specific joint attacks have yet been suggested [16].

The most general treatments yet of individual attacks, which appear to include all strategies not forbidden by the laws of physics, are due to Fuchs and Peres [13] (hereafter

*Electronic address: bslutsky@ucsd.edu

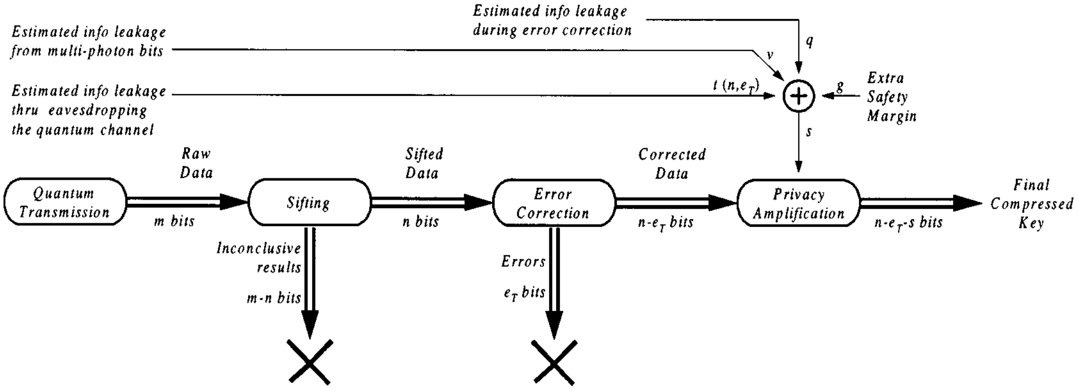

FIG. 1. Distillation of secret key from a quantum transmission. Alice and Bob arrive at privacy amplification compression level s by summing estimates of possible information leakage at various stages of the protocol, together with an arbitrary safety margin.

''FP96''), and Fuchs, Gisin, Griffiths, Niu, and Peres [14] (hereafter ''FGGNP97''). Both works investigate the tradeoff between the information learned from a quantum test, and the disturbance induced by the test. FGGNP97 formally find the maximum obtainable information for a given disturbance under conditions closely mirroring the so-called four-state, or BB84, quantum cryptographic protocol [1]; for the so-called two-state, or B92, protocol [5], FP96 construct a suspected maximum and confirm it by numerical simulation.

The problems posed in FP96 and FGGNP97, however, as their authors point out, were not designed to precisely replicate those arising in a quantum cryptographic communication. The latter can be illustrated with reference to Fig. 1, which sketches a procedure Alice and Bob might use to defend their secret key against individual eavesdropping attacks [4,7,18]. Starting from *raw data* obtained in the course of quantum transmission, Alice and Bob first discard so-called *inconclusive* bits.[1] They then exchange a series of block checksums, and where the checksums do not match, use bisective search within the block to identify and discard the error. The resulting *corrected data* are input into the privacy amplification algorithm [6], which produces a shorter but more secure key. This last step requires, however, an upper bound estimate of Eve's *Renyi information* on the corrected data [6]. Eve's information may come from block checksums disclosed during error correction, from the rare but unavoidable instances when Alice's device emits multiple photons in a single bit cell [4,18,19], and, most importantly for the purposes of the present work, from individual attacks on the carrier particles in the quantum channel.

Alice and Bob are thus in need of a theorem that relates carrier particle disturbance, as expressed in terms of available parameters such as the error rate of a particular communication system, to Renyi information accrued to Eve with respect to corrected data only. It can be shown that such a result permits Alice and Bob to construct the so-called *defense frontier*, and ultimately to secure their data, at least against individual attacks, in the sense that Eve is exponentially unlikely to end up with more than token knowledge of the final key [7]. Both FP96 and FGGNP97, on the other hand, assert bounds on Eve's *Shannon* information averaged over *all* bits of the transmission, including those eventually discarded because they are not received or received incorrectly by Bob. More precisely, with reference to Fig. 1, FP96 relates *raw data* error rate e_T/m to Eve's *Shannon* information on *raw data*, and FGGNP97 relates *sifted data* error rate e_T/n to Eve's *Shannon* information on *sifted data*. Although the FP96 and FGGNP97 results are of fundamental importance, from the perspective of quantum cryptography it is necessary to consider Eve's *Renyi* information on *corrected data*. Focusing only on the corrected data, i.e., only on the bits that are error-free to Bob, alters, as we shall see, both the upper bound of Eve's information, and her optimal strategy.

The results reported in this manuscript apply to the same general class of individual eavesdropping attacks as FP96 and FGGNP97. However, we adopt as the measure of information gain the conditional average appropriate for quantum cryptographical application. Starting with the FP96 eavesdropping interaction model, we formally solve for Eve's maximum Renyi information gain $I^R_{\max}$ on bits not in error, as a function of the error rate E observed by Alice and Bob, in both B92 and BB84 contexts. The optimal attack that leads to $I^R_{\max}$ is also explicitly constructed, and is shown to be superior (in the sense of Eve's Renyi information on bits not in error) to some of the most powerful attacks previously known, including those from FP96 and FGGNP97 works.

This paper is organized as follows. Section II reviews the FP96 eavesdropping model, with the generalization necessary to cover BB84, and to use Renyi information instead of Shannon. The model defines the eavesdropper's probe in terms of four independent parameters λ, μ, θ, ϕ. Sections III and IV, dealing, respectively, with B92 and BB84, relate λ, μ, θ, ϕ to the error rate E and to information gain I^R on bits not in error, and use the method of Lagrange multipliers to tune λ, μ, θ, ϕ for the maximum of I^R at any given E. Our main result is the relationship between the error rate and the maximum information gain, which can serve as input for the construction of the so-called *defense frontier*, used by Alice and Bob to secure their communication against individual attacks [7]. Finally, Sec. V discusses application and some-

[1] Inconclusive bits are those whose value is not revealed with certainty by Bob's measurement, for example, those measured in the wrong BB84 basis by Bob. Inconclusive bits are an integral feature of quantum cryptographic protocols even in the absence of channel and detector imperfections.

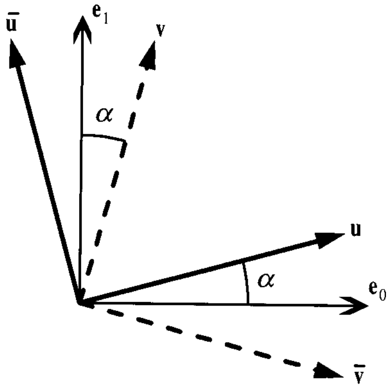

FIG. 2. Quantum states used in BB84 and B92.

limitations of our theorem. The bulk of the algebraic manipulation is removed into Appendixes A–E.

II. THE EAVESDROPPING MODEL

Quantum cryptographic protocols BB84 [4] and B92 [5] each involve a quantum particle in a pure state, prepared by the sender Alice and transmitted towards the recipient Bob. B92 employs two pure states $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$, while BB84 additionally uses two states $|\overline{\mathbf{u}}\rangle,|\overline{\mathbf{v}}\rangle$ in the same Hilbert plane, and respectively orthogonal to the first pair (Fig. 2). In B92, Alice sends towards Bob the state $|\mathbf{u}\rangle$ to communicate bit value 1, and the state $|\mathbf{v}\rangle$ to communicate 0. In BB84, she sends either $|\mathbf{u}\rangle$ for 1, $|\overline{\mathbf{u}}\rangle$ for 0, or $|\mathbf{v}\rangle$ for 1, $|\overline{\mathbf{v}}\rangle$ for 0, and it is subsequently disclosed which of the two alphabets was used to encode each particular bit. The states for a BB84 transmission are normally chosen so that $|\langle\mathbf{u}|\mathbf{v}\rangle|=|\langle\overline{\mathbf{u}}|\mathbf{v}\rangle|=|\langle\mathbf{u}|\overline{\mathbf{v}}\rangle|=|\langle\overline{\mathbf{u}}|\overline{\mathbf{v}}\rangle|=1/\sqrt{2}$.

We shall select basis vectors $|\mathbf{e}_0\rangle,|\mathbf{e}_1\rangle$ in the plane of $|\mathbf{u}\rangle,|\mathbf{v}\rangle$, in such a way that

$$|\mathbf{u}\rangle=|\mathbf{e}_0\rangle\cos\alpha+|\mathbf{e}_1\rangle\sin\alpha,\qquad |\overline{\mathbf{u}}\rangle=-|\mathbf{e}_0\rangle\sin\alpha+|\mathbf{e}_1\rangle\cos\alpha,$$
$$|\mathbf{v}\rangle=|\mathbf{e}_0\rangle\sin\alpha+|\mathbf{e}_1\rangle\cos\alpha,\qquad |\overline{\mathbf{v}}\rangle=|\mathbf{e}_0\rangle\cos\alpha-|\mathbf{e}_1\rangle\sin\alpha \tag{1}$$

for some $0<\alpha<\pi/4$. An orthonormal basis $|\mathbf{e}_0\rangle,|\mathbf{e}_1\rangle$ in which the two equations in the left column of Eq. (1) hold, can be found for any pair of unit vectors $|\mathbf{u}\rangle,|\mathbf{v}\rangle$ with real inner product $\langle\mathbf{u}|\mathbf{v}\rangle=\sin 2\alpha$; and where the inner product is complex, it can be made real by adjusting the otherwise arbitrary phases of $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$. A similar adjustment in $|\overline{\mathbf{u}}\rangle,|\overline{\mathbf{v}}\rangle$ is sufficient to ensure the validity of the remaining two equations in Eq. (1), because any companion vectors respectively orthogonal to $|\mathbf{u}\rangle,|\mathbf{v}\rangle$ in the same Hilbert plane can only differ by a phase factor from the $|\overline{\mathbf{u}}\rangle,|\overline{\mathbf{v}}\rangle$ given by Eq. (1).

Consider now a generic eavesdropping attack, as described by FP96. The information-carrying particle prepared by Alice in one of the states $|\mathbf{u}\rangle,|\mathbf{v}\rangle,|\overline{\mathbf{u}}\rangle,|\overline{\mathbf{v}}\rangle$ collides en route to Bob with Eve's probe (Fig. 3). There is no loss of generality in assuming the probe to be initially in a pure state $|\mathbf{w}\rangle$, for a mixed state can be thought of as a partial trace over the extra degrees of freedom of a larger probe. The particle and the probe undergo joint unitary evolution represented by an operator $\mathbf{U}$, defined in relevant part by relations

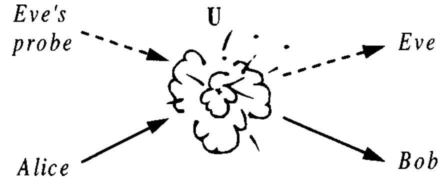

FIG. 3. Eavesdropping attack.

$$|\mathbf{e}_m\otimes\mathbf{w}\rangle\rightarrow\mathbf{U}|\mathbf{e}_m\otimes\mathbf{w}\rangle=\sum_n|\mathbf{e}_n\rangle\otimes|\Phi_{mn}\rangle,$$
$$|\Phi_{mn}\rangle\triangleq\langle\mathbf{e}_n|\mathbf{U}|\mathbf{e}_m\otimes\mathbf{w}\rangle,\qquad m,n=0,1 \tag{2}$$

where vectors $|\Phi_{mn}\rangle$ in the Hilbert space of the probe are in general neither normalized nor orthogonal. Following the evolution, the probe and the particle become correlated in a manner determined by the operator $\mathbf{U}$, known to Eve. Subsequent measurement of the probe can therefore reveal to Eve partial (or even complete) information about the particle.

Both B92 and BB84 protocols provide for random and equiprobable selection between the states $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$. (Variations that favor one state over the other will not be considered.) The eavesdropper thus finds herself in an environment manifestly symmetric with respect to the reflection $\mathbf{R}$ that interchanges $\mathbf{e}_0\leftrightarrow\mathbf{e}_1$, $\{\mathbf{u},\overline{\mathbf{u}}\}\leftrightarrow\{\mathbf{v};\overline{\mathbf{v}}\}$. For reasons set forth in greater detail in Appendix A, the eavesdropping device may be assumed without loss of generality to be endowed with the same symmetry: more precisely, reflection $\mathbf{R}$ may be assumed extendable into the space of the probe in such a way that both the evolution operator $\mathbf{U}$ and the initial probe state $|\mathbf{w}\rangle$ are invariant under $\mathbf{R}$. It then follows that $\mathbf{R}$ interchanges $|\Phi_{00}\rangle$ with $|\Phi_{11}\rangle$, and $|\Phi_{01}\rangle$ with $|\Phi_{10}\rangle$, and inner products of these vectors therefore obey symmetries $\langle\Phi_{00}|\Phi_{01}\rangle=\langle\Phi_{11}|\Phi_{10}\rangle$, $\langle\Phi_{00}|\Phi_{10}\rangle=\langle\Phi_{11}|\Phi_{01}\rangle$, as well as $\|\Phi_{00}\|=\|\Phi_{11}\|$, $\|\Phi_{01}\|=\|\Phi_{10}\|$. Similarly, again with reference to Appendix A, since $|\mathbf{u}\rangle,|\overline{\mathbf{u}}\rangle,|\mathbf{v}\rangle,|\overline{\mathbf{v}}\rangle$ all have real projections onto basis $\{\mathbf{e}_0,\mathbf{e}_1\}$, $\mathbf{U}$ and $\mathbf{w}$ may also be assumed to have real elements (and $|\Phi_{mn}\rangle$ to have real projections) in some orthonormal basis $\mathcal{W}$ that includes $\{\mathbf{e}_0,\mathbf{e}_1\}$.

Let us now pick in the space of the probe the particular orthonormal basis $\{\mathbf{w}_\beta\}$ to be used throughout the remainder of this paper. Taking the real-valued representation of $|\Phi_{mn}\rangle$ in basis $\mathcal{W}$ as a starting point, the following steps can be carried out without introducing any complex numbers. (One can think of the entire procedure as being implemented in the corresponding Euclidian space.) First, select orthonormal basis vectors $|\mathbf{w}_1\rangle,|\mathbf{w}_2\rangle$ in the plane of $|\Phi_{01}\rangle,|\Phi_{10}\rangle$ in such a way that[2]

$$|\Phi_{01}\rangle=X_5|\mathbf{w}_1\rangle+X_6|\mathbf{w}_2\rangle,\qquad |\Phi_{10}\rangle=X_6|\mathbf{w}_1\rangle+X_5|\mathbf{w}_2\rangle. \tag{3a}$$

(The notation X_k is chosen here for consistency with FP96.) Note that $|\mathbf{w}_1\rangle,|\mathbf{w}_2\rangle$ are themselves interchanged by the reflection $\mathbf{R}$, so that the projections $X_1\triangleq\langle\Phi_{00}|\mathbf{w}_1\rangle=\langle\Phi_{11}|\mathbf{w}_2\rangle$, and similarly $X_2\triangleq\langle\Phi_{00}|\mathbf{w}_2\rangle=\langle\Phi_{11}|\mathbf{w}_1\rangle$. Two

[2] If $|\Phi_{01}\rangle=\pm|\Phi_{10}\rangle$, basis $\{\mathbf{w}_1,\mathbf{w}_2\}$ is chosen in the plane containing $|\Phi_{01}\rangle$ and orthogonal to the mirror plane of the reflection $\mathbf{R}$.

more basis vectors, $|\mathbf{w}_0\rangle$ and $|\mathbf{w}_3\rangle$, are selected in the plane defined by the components $|\tilde{\Phi}_{00}\rangle, |\tilde{\Phi}_{11}\rangle$ of $|\Phi_{00}\rangle$ and $|\Phi_{11}\rangle$ orthogonal to both $|\mathbf{w}_1\rangle, |\mathbf{w}_2\rangle$. By applying the reflection $\mathbf{R}$ it is found that $\|\tilde{\Phi}_{00}\| = \|\tilde{\Phi}_{11}\|$, and $|\mathbf{w}_0\rangle$ and $|\mathbf{w}_3\rangle$ can be picked symmetrically, to obtain

$$\begin{aligned} |\Phi_{00}\rangle &= X_0|\mathbf{w}_0\rangle + X_1|\mathbf{w}_1\rangle + X_2|\mathbf{w}_2\rangle + X_3|\mathbf{w}_3\rangle, \\ |\Phi_{11}\rangle &= X_3|\mathbf{w}_0\rangle + X_2|\mathbf{w}_1\rangle + X_1|\mathbf{w}_2\rangle + X_0|\mathbf{w}_3\rangle. \end{aligned} \tag{3b}$$

Any other degrees of freedom of the probe are immaterial, because all four vectors of interest $|\Phi_{mn}\rangle$ are already contained within the four-dimensional space spanned by $\{\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3\}$. As stated earlier, all the coefficients X_k appearing in Eqs. (3a) and (3b) are real valued.

For the evolution in Eq. (2) to be unitary [or, more precisely, for a unitary operator $\mathbf{U}$ to exist that is consistent with Eq. (2)], it is necessary and sufficient that orthonormal vectors $|\mathbf{e}_m \otimes \mathbf{w}\rangle$, $m=0,1$, transform into orthonormal vectors:

$$\langle \mathbf{e}_{m'} \otimes \mathbf{w}|\mathbf{U}^{\dagger}\mathbf{U}|\mathbf{e}_m \otimes \mathbf{w}\rangle = \sum_{n=0,1} \langle \Phi_{m'n}|\Phi_{mn}\rangle = \delta_{m'm}, \qquad m', m = 0,1$$

which expands into constraints

$$\begin{aligned} &\|\Phi_{00}\|^2 + \|\Phi_{01}\|^2 = \|\Phi_{10}\|^2 + \|\Phi_{11}\|^2 \\ &\quad = X_5^2 + X_6^2 + X_0^2 + X_3^2 + X_1^2 + X_2^2 = 1, \\ &\langle \Phi_{10}|\Phi_{00}\rangle + \langle \Phi_{11}|\Phi_{01}\rangle = 2(X_1X_6 + X_2X_5) = 0. \end{aligned}$$

These constraints can be satisfied by means of the following parametrization with four independent variables $\lambda, \mu, \theta, \phi$:

$$\begin{aligned} X_0 &= \sin\lambda\, \cos\mu, & X_1 &= \cos\lambda\, \cos\theta\, \cos\phi, \\ X_2 &= \cos\lambda\, \cos\theta\, \sin\phi, & X_3 &= \sin\lambda\, \sin\mu, \\ X_5 &= \cos\lambda\, \sin\theta\, \cos\phi, & X_6 &= -\cos\lambda\, \sin\theta\, \sin\phi. \end{aligned} \tag{4}$$

Relations (4) also appear in the FP96 work.

The joint evolution described by Eq. (2) leaves the particle and the probe in an entangled quantum state, causing a correlation between Eve's and Bob's measurements. Mathematically, every outcome i observed by Bob is associated with its own "projected state" $\rho^{(i)}$ of the probe. Eve thus faces a task that can be described in the following way: The probe, now known to be in one of a set of quantum states $\{\rho^{(i)}\}$ with corresponding *a priori* probabilities p_i, must be analyzed to determine, insofar as possible, its particular state $\rho^{(i)}$.

Let us assume that Eve employs a so-called positive operator valued measure (POVM) [20], believed to be the most general test to which a quantum system may be subjected [21]. A POVM is constructed around a set of non-negative operators $\mathbf{E}_{\mu}$, which add up to the unit matrix. The POVM has as many possible outcomes as there are operators in the set $\{\mathbf{E}_{\mu}\}$, and, when applied to an input state represented by density matrix ρ, produces each outcome μ with probability

$$\mathrm{Prob}[\mu|\rho] = \mathrm{Tr}(\mathbf{E}_{\mu}\rho).$$

Having obtained a particular outcome μ, Eve uses Bayes's rule to compute *a posteriori* probabilities

$$\begin{aligned} q_{i\mu} \mathrel{\hat{=}} \mathrm{Prob}[\rho^{(i)}|\mu] &= \frac{\mathrm{Prob}[\mu|\rho^{(i)}]\mathrm{Prob}[\rho^{(i)}]}{\mathrm{Prob}[\mu]} \\ &= \frac{\mathrm{Tr}(\mathbf{E}_{\mu}\rho^{(i)})p_i}{P_{\mu}}, \end{aligned}$$

where $P_{\mu} \mathrel{\hat{=}} \mathrm{Prob}[\mu] = \mathrm{Tr}(\mathbf{E}_{\mu}\Sigma p_i \rho^{(i)})$ is the *a priori* probability of outcome μ. Eve's information gain from the POVM is reflected in the reduction of her Shannon entropy regarding the probe state, from its initial level $H_0 = -\Sigma p_i \log_2 p_i$ to the *a posteriori* value $H_{\mu} = -\Sigma q_{i\mu} \log_2 q_{i\mu}$ following the outcome μ. The expected value of the gain is expressed as

$$\begin{aligned} I^H &= \sum_{\mu} P_{\mu}(H_0 - H_{\mu}) \\ &= \sum_{\mu} P_{\mu}\left(-\sum_i p_i \log_2 p_i + \sum_i q_{i\mu} \log_2 q_{i\mu} \right). \end{aligned} \tag{5}$$

An alternative metric of Eve's success is the reduction of Renyi entropy from its initial level $R_0 = -\log_2 \Sigma p_i^2$. The expected gain in terms of Renyi information is

$$\begin{aligned} I^R &= \sum_{\mu} P_{\mu}(R_0 - R_{\mu}) \\ &= \sum_{\mu} P_{\mu}\left(-\log_2 \sum_i p_i^2 + \log_2 \sum_i q_{i\mu}^2 \right). \end{aligned} \tag{6}$$

Finding the measurement with the greatest expected information gain is a difficult problem, which, except for the simplest special cases, remains unsolved. Fortunately, the only situation encountered in Secs. III and IV is one where the set $\{\rho^{(i)}\}$ consists of only two pure states $\rho^{(1)} = |\psi_1\rangle\langle\psi_1|$, $\rho^{(2)} = |\psi_2\rangle\langle\psi_2|$, with equal *a priori* probabilities $p_1 = p_2 = \frac{1}{2}$. The Shannon information I^H from Eq. (5) is in this case maximized by a simple two-dimensional von Neumann test symmetrically arranged around the vectors $|\psi_1\rangle, |\psi_2\rangle$ in the Hilbert plane spanned by $|\psi_1\rangle, |\psi_2\rangle$ [22]. This optimal test results in *a posteriori* probabilities

$$q_{11} = q_{22} = \cos^2\zeta, \quad q_{12} = q_{21} = \sin^2\zeta$$

and in Shannon and Renyi information gain

$$\begin{aligned} I^H_{\mathrm{opt}} &= 1 + \sin^2\zeta \log_2 \sin^2\zeta + \cos^2\zeta \log_2 \cos^2\zeta \\ &= \tfrac{1}{2}(1 - \cos 2\zeta)\log_2(1 - \cos 2\zeta) + \tfrac{1}{2}(1 + \cos 2\zeta) \\ &\quad \times \log_2(1 + \cos 2\zeta), \\ I^R_{\mathrm{opt}} &= 1 + \log_2(\sin^4\zeta + \cos^4\zeta) = \log_2(1 + \cos^2 2\zeta), \end{aligned} \tag{7a}$$

where the angle ζ is defined by

$$Q \mathrel{\hat{=}} \sin 2\zeta \mathrel{\hat{=}} |\langle\psi_1|\psi_2\rangle|. \tag{7b}$$

TABLE I. Interpretation of events in a B92 transmission.

Alice transmits	$\mathbf{u}$				$\mathbf{v}$			
Bob measures	$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$		$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$	
Bob detects	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$
Interpretation	inconclusive	error	inconclusive	1	inconclusive	0	inconclusive	error

It is proven in Appendix B that the symmetrical von Neumann test just described maximizes Eve's Renyi information as well as her Shannon information. We will henceforth assume that Eve employs this symmetrical test.

The results of this section will now be applied in the context of B92 and BB84 protocols. In each case, parameters λ,μ,θ,ϕ from Eq. (4) will be related to Bob's error rate E, and to the overlap Q of the two-state vectors which, as will be shown, Eve needs to distinguish. Equation (7) confirms the intuitive understanding that Eve's advantage is increased as the two states move closer to orthogonality. When the parameters λ,μ,θ,ϕ are tuned to minimize the overlap Q for a fixed E, an eavesdropping apparatus results that yields Eve the most Renyi (and Shannon) information consistent with a given error rate between Alice and Bob.

III. INFORMATION LEAKAGE AND ERROR RATE IN B92

A. Eavesdropping in B92

Nonorthogonal states $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$, which make up the alphabet of a B92 transmission, cannot be reliably separated on every occasion. Rather, the protocol calls for a detector that can identify the particle state with certainty some of the time, and at other times indicate an ''inconclusive'' outcome, later to be discarded. The simplest implementation of such a device, and the first one proposed, is based on a pair of von Neumann measurements [5]. Although the number of inconclusive results can be somewhat reduced with a POVM design [23], it will be assumed here that Bob has chosen the less efficient von Neumann method. This assumption not only makes the optimization problem in Sec. III B below more tractable, but also recognizes that Bob, unlike the hypothetical Eve, is constrained by technological reality, and therefore might well be interested in the simplest, rather than the most efficient, type of receiver.

Operation of B92 in its von Neumann variant is illustrated in Table I. The carrier particle, transmitted by Alice in one of the two states $|\mathbf{u}\rangle,|\mathbf{v}\rangle$, is measured by Bob in one of the two orthonormal bases $\{\mathbf{u},\bar{\mathbf{u}}\}$, $\{\mathbf{v},\bar{\mathbf{v}}\}$ (see Fig. 2), chosen at random. Bob's detection of $|\bar{\mathbf{v}}\rangle$ rules out the input state $|\mathbf{v}\rangle$, and therefore indicates with certainty state $|\mathbf{u}\rangle$, and hence bit value 1; and vice versa, $|\bar{\mathbf{u}}\rangle$ indicates $|\mathbf{v}\rangle$ and hence bit value 0. Measurement outcomes $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$, which are each consistent with both inputs $|\mathbf{u}\rangle$ and $|\mathbf{v}\rangle$, are discarded as inconclusive.

Let us denote as $(i;j)$ the event in which Alice transmits state $|i\rangle$, and, following the joint evolution $\mathbf{U}$ of $|i\rangle$ with the eavesdropping probe, Bob detects outcome $|j\rangle$, $i,j \in\{\mathbf{u},\bar{\mathbf{u}},\mathbf{v},\bar{\mathbf{v}}\}$. Given Alice's choice of i and Bob's choice of basis $\{j,\bar{j}\}$, quantum mechanics dictates that the event $(i;j)$ occurs with probability

$$P_{i,j} \hat{=} \mathrm{Prob}[j|i;\{j,\bar{j}\}] = \|\psi_{i,j}\|^2, \quad \text{where } |\psi_{i,j}\rangle \hat{=} \langle j|\mathbf{U}|i\otimes\mathbf{w}\rangle \tag{8}$$

and leaves the probe in the corresponding projected state $|\psi_{i,j}\rangle$ (or, more precisely, the normalized version thereof) given by Eq. (8). The error rate between Alice and Bob is the frequency of events identified as errors in Table I, relative to error and correct reception events combined. (Inconclusive outcome events are not included in the count.) Since both Alice's and Bob's choices are random and symmetric, the error rate is expressed as

$$E = \frac{P_{\mathbf{u},\bar{\mathbf{u}}} + P_{\mathbf{v},\bar{\mathbf{v}}}}{P_{\mathbf{u},\bar{\mathbf{v}}} + P_{\mathbf{u},\bar{\mathbf{u}}} + P_{\mathbf{v},\bar{\mathbf{u}}} + P_{\mathbf{v},\bar{\mathbf{v}}}} = \frac{P_{\mathbf{u},\bar{\mathbf{u}}}}{P_{\mathbf{u},\bar{\mathbf{v}}} + P_{\mathbf{u},\bar{\mathbf{u}}}}$$

$$= \frac{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2}{\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2 + \|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2}, \tag{9}$$

where simplification follows from the symmetry properties of $P_{i,j}$.[3]

Next consider the eavesdropper Eve, who seeks to distinguish states $|\psi_{i,j}\rangle$ from one another in order to infer Alice's and Bob's data. It can be observed from Table I that Eve need in fact only distinguish between *two* pure states, $|\psi_{\mathbf{u},\bar{\mathbf{v}}}\rangle$ and $|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle$, for all other events appear as errors or inconclusive results to Alice and Bob, and as such are announced and removed subsequently in the protocol. The problem of optimally distinguishing between two pure states has already been discussed in Sec. II, where it was concluded that Eve must minimize the overlap

$$Q = \frac{|\langle\psi_{\mathbf{u},\bar{\mathbf{v}}}|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle|}{\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|\,\|\psi_{\mathbf{v},\bar{\mathbf{u}}}\|} = \frac{|\langle\psi_{\mathbf{u},\bar{\mathbf{v}}}|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle|}{\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2}. \tag{10}$$

This she does by manipulating the four independent parameters λ,μ,θ,ϕ, which control the matrix elements X_k in Eq. (4), and through them $|\Phi_{mn}\rangle$ in Eq. (3), the projection vectors $|\psi_{i,j}\rangle$, and ultimately the error rate E, Eq. (9), and the overlap Q, Eq. (10). The conditional minimum $Q_{\min}(E)$ of Q subject to $E=\text{const}$ leads via Eq. (7) to the expression for the maximum Renyi information on error-free bits $I^R_{\max}(E)$ Eve can obtain for a given error rate.

In what follows, we shall drop the modulus sign in Eq. (10). This simplification is possible because the conditional minimum of Q (without the modulus) will turn out to be positive for low error rates E, and decrease with E. Analysis

[3] The ''disturbance'' D adopted as the measure of eavesdropping intrusiveness in Ref. [13], in our notation becomes simply $P_{\mathbf{u},\bar{\mathbf{u}}}$. This is equivalent to the inclusion of inconclusive outcomes in the denominator of E.

may safely end when $Q_{\min}(E)$ reaches zero, for at that error rate the eavesdropper already has complete information about the transmission, $I^R=1$. Consideration will also be limited to error rates $E<\frac{1}{2}$, because only a perverse eavesdropper would use a strategy with an error rate higher than chance.

B. Optimization of eavesdropping in B92

In searching for the conditional minimum $Q_{\min}(E)$, the first step is to obtain explicit expressions for E and Q. This is accomplished through direct substitution of carrier states from Eq. (1), and the unitary evolution from Eq. (2), into Eq. (8), to obtain the required projection vectors $|\psi_{i,j}\rangle$ for use in Eqs. (9) and (10). Simple algebraic manipulations reproduced in Appendix C lead to

$$E=\frac{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2}{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2+\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2}=\frac{1}{2}\left(1-\frac{\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2-\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2}{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2+\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2}\right)$$

$$=\frac{1}{2}\left(1-\frac{d\ \cos^2 2\alpha}{1-a\ \sin^2 2\alpha-c\ \sin 2\alpha}\right),$$

$$Q=\frac{\langle\psi_{\mathbf{u},\bar{\mathbf{v}}}|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle}{\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2}=\frac{(a+b)-(1+b)\sin^2 2\alpha+c\ \sin 2\alpha}{(1+d)+(-d-a)\sin^2 2\alpha-c\ \sin 2\alpha}, \tag{11}$$

where

$$a\hat{=}\Phi_{00}\Phi_{11}+\Phi_{01}\Phi_{10}=2X_0X_3+2X_1X_2+2X_5X_6$$
$$=\sin^2\lambda\ \sin 2\mu+\cos^2\lambda\ \cos 2\theta\ \sin 2\phi,$$

$$b\hat{=}\Phi_{00}\Phi_{11}-\Phi_{01}\Phi_{10}=2X_0X_3+2X_1X_2-2X_5X_6$$
$$=\sin^2\lambda\ \sin 2\mu+\cos^2\lambda\ \sin 2\phi,$$

$$c\hat{=}2\Phi_{00}(\Phi_{01}\pm\Phi_{10})=2\Phi_{11}(\Phi_{10}\pm\Phi_{01})$$
$$=2(X_1\pm X_2)(X_5\pm X_6)=\cos^2\lambda\ \sin 2\theta\ \cos 2\phi,$$

$$d\hat{=}\Phi_{00}^2-\Phi_{01}^2=X_0^2+X_1^2+X_2^2+X_3^2-X_5^2-X_6^2$$
$$=\sin^2\lambda+\cos^2\lambda\ \cos 2\theta. \tag{12}$$

The conditional minimum $Q_{\min}(E)$ is then found using the method of Lagrange multipliers, as described in Appendix D. The desired solution for $\{\lambda,\mu,\theta,\phi\}$ is defined parametrically on an auxiliary variable γ by relations

$$\lambda=\mu=0,\quad \sin 2\phi=\frac{\sin\gamma}{\sin\delta},\quad \cos 2\theta=\frac{\cos\delta}{\cos\gamma},$$
$$-\delta\leqslant\gamma\leqslant\delta, \tag{13}$$

where $\sin\delta\hat{=}\sin 2\alpha/\sqrt{1+\sin^2 2\alpha}$, $\cos\delta\hat{=}1/\sqrt{1+\sin^2 2\alpha}$, $0<\delta<\pi/4$, and where angles ϕ and θ are chosen so that $\cos 2\phi\geqslant 0$ and $\sin 2\theta\geqslant 0$. The quantities E and $Q_{\min}(E)$, and the unitary evolution $\mathbf{U}$, are computed from Eq. (13) by means, respectively, of Eq. (11), and of Eqs. (4), (3), (2).

The relationship $Q_{\min}(E)$ implied by Eqs. (11) and (13) for a particular $\alpha=\pi/5$ is plotted in Fig. 4(a), together with points $\{E;Q\}$ resulting from other, suboptimal combinations of λ,μ,θ,ϕ. For reasons already explained, the plot is truncated to $Q\geqslant 0$. Validity of the optimization algebra carried out in Appendix D is indirectly confirmed by the fact that the various realizable points $\{E;Q\}$ all lie above and to the right of the curve $Q_{\min}(E)$. Figure 4(b), obtained by solving numerically for E in $Q_{\min}(E)=0$, shows, as a function of angle α, the smallest error rate that permits the eavesdropper complete knowledge of the transmission.

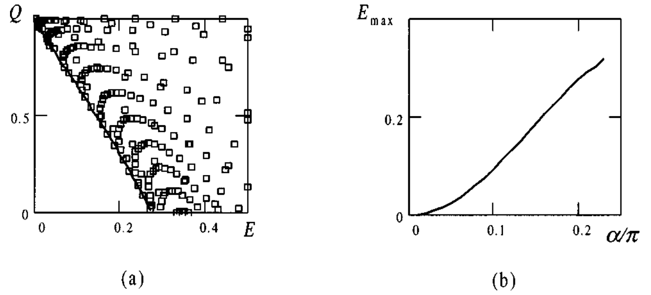

FIG. 4. (a) Realizations of E and Q for various suboptimal combinations of parameters λ,μ,θ,ϕ (boxes), and the conditional minimum implied by Eq. (13) (solid line), for the case when carrier states $\mathbf{u}$, $\mathbf{v}$ make angle $\alpha=\pi/5$ with basis $\mathbf{e}_0$, $\mathbf{e}_1$. (b) The error rate $E_{\max}$ at which the eavesdropper can obtain complete knowledge of the transmission, $Q_{\min}(E_{\max})=0$, as a function of angle α.

The eavesdropper's Renyi information on error-free bits $I^R_{\max}(E)$, computed from $Q_{\min}(E)$ via Eq. (7), is depicted by solid line in Fig. 5. For error rate $E=0$, we have $Q_{\min}=1$ and $I^R_{\max}=0$, confirming that no information can be extracted without inducing a disturbance. Higher error rates, reflecting progressively more intrusive eavesdropping activities, are accompanied by greater information gain to Eve, until the point $E=E_{\max}$ is reached where Eve has complete information.

The dotted line in Fig. 5 illustrates the same information gain vs error rate tradeoff for a family of eavesdropping strategies described by Ekert *et al.* [10] as ''*translucent eavesdropping with entanglement*,'' which in our present notation take the form

$$|\mathbf{u}\otimes\mathbf{w}\rangle\rightarrow\mathbf{U}|\mathbf{u}\otimes\mathbf{w}\rangle=x|\mathbf{u}\otimes\mathbf{w}_\mathbf{u}\rangle+y|\mathbf{v}\otimes\mathbf{w}_\mathbf{v}\rangle,$$

$$|\mathbf{v}\otimes\mathbf{w}\rangle\rightarrow\mathbf{U}|\mathbf{v}\otimes\mathbf{w}\rangle=y|\mathbf{u}\otimes\mathbf{w}_\mathbf{u}\rangle+x|\mathbf{v}\otimes\mathbf{w}_\mathbf{v}\rangle,$$

where

$$|\mathbf{w}_\mathbf{u}\rangle\hat{=}\cos\gamma|\mathbf{w}_1\rangle+\sin\gamma|\mathbf{w}_2\rangle,$$

$$|\mathbf{w}_\mathbf{v}\rangle\hat{=}\sin\gamma|\mathbf{w}_1\rangle+\cos\gamma|\mathbf{w}_2\rangle, \tag{14}$$

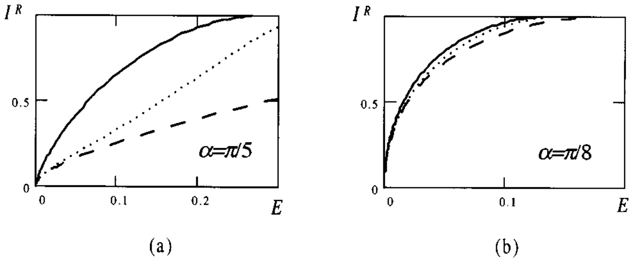

FIG. 5. Eavesdropper's information I^R on error-free bits versus the error rate E in B92: the attack based on Eq. (13) (solid); ''translucent eavesdropping with entanglement'' [10] (dotted); the FP96 attack [13] (dashed).

TABLE II. Interpretation of events in a BB84 transmission.

Alice transmits	$\mathbf{u}$				$\bar{\mathbf{u}}$				$\mathbf{v}$				$\bar{\mathbf{v}}$			
Bob measures	$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$		$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$		$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$		$\{\mathbf{u},\bar{\mathbf{u}}\}$		$\{\mathbf{v},\bar{\mathbf{v}}\}$	
Bob detects	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$	$\mathbf{u}$	$\bar{\mathbf{u}}$	$\mathbf{v}$	$\bar{\mathbf{v}}$
Interpretation	1	error	inconclusive	inconclusive	error	0	inconclusive	inconclusive	inconclusive	inconclusive	1	error	inconclusive	inconclusive	error	0

and where $x=\cos(\alpha+\omega)/\cos 2\omega$, $y=\sin(\alpha-\omega)/\cos 2\omega$, $\sin 2\omega=\sin 2\alpha\ \sin 2\gamma$. The single independent parameter γ, $0<\gamma<\pi/4$, controls the intrusiveness of the strategy: lower values of γ produce higher error rates, but also higher information yields to Eve. It follows immediately from Eq. (14) that

$$|\psi_{\mathbf{u},\bar{\mathbf{v}}}\rangle=\langle\bar{\mathbf{v}}|\mathbf{U}|\mathbf{u}\otimes\mathbf{w}\rangle=x\ \cos 2\alpha|\mathbf{w}_{\mathbf{u}}\rangle,$$

$$|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle=\langle\bar{\mathbf{u}}|\mathbf{U}|\mathbf{v}\otimes\mathbf{w}\rangle=x\ \cos 2\alpha|\mathbf{w}_{\mathbf{v}}\rangle,$$

$$|\psi_{\mathbf{u},\bar{\mathbf{u}}}\rangle=\langle\bar{\mathbf{u}}|\mathbf{U}|\mathbf{u}\otimes\mathbf{w}\rangle=y\ \cos 2\alpha|\mathbf{w}_{\mathbf{v}}\rangle,$$

and with the aid of Eqs. (9) and (10), $E=y^2/(y^2+x^2)$, $Q=\langle\mathbf{w}_{\mathbf{u}}|\mathbf{w}_{\mathbf{v}}\rangle=\sin 2\gamma$, which is the result plotted in Fig. 5.

Finally, Fig. 5 also shows information gain from the eavesdropping strategy of FP96 [see Eq. (52) in FP96] (dashed line). As noted in the Introduction, this strategy is believed to be the strongest in the sense of Eve's knowledge averaged over *all* transmitted bits. However, it is Eve's knowledge of bits received *error-free*, rather than of all bits on average, that is material to Alice and Bob if they want to secure their transmission by privacy amplification [7]. When the figure of merit for eavesdropping attacks is changed accordingly, one can observe from Fig. 5 that the FP96 strategy from the strongest becomes the weakest of those plotted, while the attack represented by Eq. (13) is seen to be the most powerful.

IV. INFORMATION LEAKAGE AND ERROR RATE IN BB84

A. Eavesdropping in BB84

Our analysis of BB84 follows the same general path as that of the B92 protocol in Sec. III. In BB84, Alice transmits one of the two states $|i\rangle,|\bar{i}\rangle$, which Bob subjects to one of the two von Neumann measurements $\{j,\bar{j}\}$, $i,j\in\{\mathbf{u},\mathbf{v}\}$. The parties subsequently announce which alphabet ($\mathbf{u}$ or $\mathbf{v}$) was used for each bit, and bits where the transmitting alphabet did not match the receiving one are discarded as inconclusive. The operation of BB84 is illustrated in Table II.

It shall be assumed that Eve is capable of preserving the projection state $|\psi_{i,j}\rangle$ of her probe until the alphabets are disclosed. Thereafter, as Table II makes clear, Eve must only distinguish between *two* pure states associated with error-free transmission between Alice and Bob. With the notation of Eq. (8), the pair of states to be distinguished is either $|\psi_{\mathbf{u},\mathbf{u}}\rangle,|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\rangle$, or $|\psi_{\mathbf{v},\mathbf{v}}\rangle,|\psi_{\bar{\mathbf{v}},\bar{\mathbf{v}}}\rangle$, depending on which alphabet had been used for the bit. In the same manner as for B92, and similarly taking advantage of the anticipated symmetry between $\mathbf{u}$ and $\mathbf{v}$, we find the BB84 analogs of Eqs. (9) and (10):

$$E=\frac{P_{\mathbf{u},\bar{\mathbf{u}}}+P_{\bar{\mathbf{u}},\mathbf{u}}+P_{\mathbf{v},\bar{\mathbf{v}}}+P_{\bar{\mathbf{v}},\mathbf{v}}}{P_{\mathbf{u},\bar{\mathbf{u}}}+P_{\bar{\mathbf{u}},\mathbf{u}}+P_{\mathbf{v},\bar{\mathbf{v}}}+P_{\bar{\mathbf{v}},\mathbf{v}}+P_{\mathbf{u},\mathbf{u}}+P_{\bar{\mathbf{u}},\bar{\mathbf{u}}}+P_{\mathbf{v},\mathbf{v}}+P_{\bar{\mathbf{v}},\bar{\mathbf{v}}}}$$

$$=\frac{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2+\|\psi_{\bar{\mathbf{u}},\mathbf{u}}\|^2}{\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2+\|\psi_{\bar{\mathbf{u}},\mathbf{u}}\|^2+\|\psi_{\mathbf{u},\mathbf{u}}\|^2+\|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\|^2},$$

$$Q=\frac{\langle\psi_{\mathbf{u},\mathbf{u}}|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\rangle}{\|\psi_{\mathbf{u},\mathbf{u}}\|\|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\|}=\frac{\langle\psi_{\mathbf{v},\mathbf{v}}|\psi_{\bar{\mathbf{v}},\bar{\mathbf{v}}}\rangle}{\|\psi_{\mathbf{v},\mathbf{v}}\|\|\psi_{\bar{\mathbf{v}},\bar{\mathbf{v}}}\|}.$$

B. Optimization of eavesdropping in BB84

As in Sec. III, Q needs to be minimized over all combinations $\{\lambda,\mu,\theta,\phi\}$, subject to constraint $E=\text{const}$. Algebraic manipulation given in Appendix C, with the same notation a,b,c,d as before, see Eq. (12), yields explicit expressions

$$E=\frac{(1-d)+(d-a)\sin^2 2\alpha}{(1-d)+(d-a)\sin^2 2\alpha+(1+d)+(-d+a)\sin^2 2\alpha}$$

$$=\frac{1-\frac{1}{2}(d+a)}{2},$$

$$Q=\frac{\frac{1}{2}(a+b)+(d-a)\frac{1}{2}\ \sin^2 2\alpha}{\sqrt{\frac{1}{2}(1+d)+(-d+a)\frac{1}{2}\ \sin^2 2\alpha+c\frac{1}{2}\ \sin 2\alpha}\sqrt{\frac{1}{2}(1+d)+(-d+a)\frac{1}{2}\ \sin^2 2\alpha-c\frac{1}{2}\ \sin 2\alpha}}=\frac{\frac{1}{2}(d+a)+b}{\sqrt{[1+\frac{1}{2}(d+a)]^2-\frac{1}{2}c^2}}$$

$$=\frac{1-2E+b}{\sqrt{[2-2E]^2-\frac{1}{2}c^2}}, \tag{15}$$

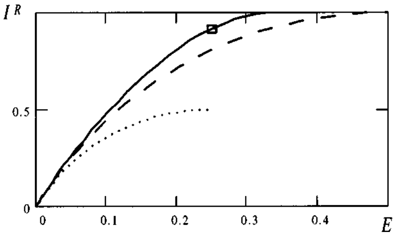

FIG. 6. Eavesdropper's information I^R on error-free bits versus the error rate E in BB84: the attack based on Eq. (16) (solid); Breidbart basis attack [9] (box); ''measurement of intensity γ'' [12] (dotted); the FGGNP97 attack [14] (dashed).

where, as is normally the case in the context of BB84, we let $\alpha = \pi/8$. The conditional minimum of Q subject to $E = \text{const}$ results when

$$\lambda = \mu = 0, \quad \cos 2\theta = 1, \quad -1 < \sin 2\phi \leqslant 1,$$

$$a = b = \sin 2\phi, \quad c = 0, \quad d = 1,$$

$$E = \tfrac{1}{4}(1 - \sin 2\phi), \quad Q_{\min} = \frac{1 - 2E + \sin 2\phi}{2 - 2E} = 3 - \frac{2}{1 - E} \tag{16}$$

(see Appendix E). As in the case of B92, $\lambda, \mu, \theta, \phi$ from Eq. (16) can be substituted into Eqs. (4), (3), (2) to find explicitly the evolution $\mathbf{U}$ associated with the optimal eavesdropping strategy.[4]

The solid line in Fig. 6 shows Renyi information on error-free bits $I^R_{\max}(E)$, computed from $Q_{\min}(E)$ by means of Eq. (7). It can be seen that Eve can learn nothing without inducing a disturbance, and has complete knowledge of (the error-free part of) the transmission at error rate $E = \frac{1}{3}$.

The result from Eq. (16) can be compared to the eavesdropping strategy described by Huttner and Ekert [9]. These authors consider a situation where the eavesdropper intercepts, measures, and retransmits particles in some basis intermediate between Alice's $\mathcal{B}_1 \hat{=} \{\mathbf{u}, \overline{\mathbf{u}}\}$ and $\mathcal{B}_2 \hat{=} \{\mathbf{v}, \overline{\mathbf{v}}\}$. It is shown that all such strategies induce the same error rate $E = \frac{1}{4}$, and that the so-called Breidbart basis ''half way in between'' $\mathcal{B}_1$ and $\mathcal{B}_2$ yields the eavesdropper the most information. It can now be seen that this Breidbart basis attack, marked by a box in Fig. 6, dominates all eavesdropping strategies with 25% error rates, and not just those considered in [9]. On the other hand, if the eavesdropper wishes to reduce the error rate from $E = \frac{1}{4}$ to, say, $E = \frac{1}{8}$, she could do better than simply apply the Breidbart measurement to half the bits and let the other half proceed undisturbed to Bob. The latter method would place her on a straight line connecting the box in Fig. 6 with the origin, which lies below the curve $I^R_{\max}(E)$.

For another comparison, the dotted line in Fig. 6 illustrates the so-called ''measurement of intensity γ'' attack [12], based on the unitary transformation

$$|\mathbf{u} \otimes \mathbf{w}\rangle \rightarrow |\mathbf{u}\rangle \otimes \left[|\mathbf{w}_1\rangle \cos\left(\frac{\pi}{4} - \frac{\gamma}{2}\right) + |\mathbf{w}_2\rangle \sin\left(\frac{\pi}{4} - \frac{\gamma}{2}\right) \right],$$

$$|\overline{\mathbf{u}} \otimes \mathbf{w}\rangle \rightarrow |\overline{\mathbf{u}}\rangle \otimes \left[|\mathbf{w}_1\rangle \cos\left(\frac{\pi}{4} + \frac{\gamma}{2}\right) + |\mathbf{w}_2\rangle \sin\left(\frac{\pi}{4} + \frac{\gamma}{2}\right) \right],$$

$$0 \leqslant \gamma \leqslant \frac{\pi}{2}.$$

When Alice transmits in the basis $\{\mathbf{u}, \overline{\mathbf{u}}\}$, Eve inflicts no disturbance and learns the bit to the extent that she can distinguish the two vectors in square brackets, whose overlap $Q = \cos \gamma$. Conversely, if Alice has chosen $\{\mathbf{v}, \overline{\mathbf{v}}\}$, Eve learns nothing and introduces an error with probability $(1 - \cos \gamma)/2$.

Finally, we turn to the FGGNP97 eavesdropping attack, illustrated by the dashed line in Fig. 6, which was proven to be the strongest from the point of view of Eve's Shannon information averaged over *all* intercepted bits [14]. As in Sec. III, however, focusing only on bits received error-free by Bob materially alters the situation, making the attack represented by Eqs. (16), rather than the FGGNP97 attack, the greatest threat to Alice and Bob, especially at high error rates.

V. CONCLUSIONS AND DISCUSSION

When Alice and Bob implement a quantum cryptographic key exchange over a noisy channel, they must allow the possibility that channel errors are eavesdrop induced and that Eve has obtained a nonzero amount of information about the key. Security can be recovered (with a performance loss) by ''classical'' privacy amplification, if Alice and Bob can use available parameters such as error rate to upper-bound Eve's advantage. The appropriate measure of advantage has been shown to be Renyi information on bits transmitted error-free from Alice to Bob. Previous optimization work, however, not being specifically tailored to the quantum cryptographic context, considered only *Shannon* information averaged over *all* transmitted bits.

In this paper, we find the requisite upper bound on Eve's Renyi information on error-free bits. This bound can be computed from Eq. (13) for B92 and Eq. (16) for BB84, and is plotted against the error rate, respectively, in Figs. 5 and 6 (solid lines). The switch from Shannon to Renyi information changes the value of the bound, but, thanks to the link between the two measures established in Appendix B, does not affect the choice of eavesdropping strategy. Focusing exclusively on bits received error-free by Bob, on the other hand, alters both the bound and the optimal strategy. As seen in Figs. 5 and 6, eavesdropping attacks that are or might be optimal in the sense of Eve's knowledge of all bits are no longer so when the figure of merit reflects her knowledge of the error-free part of the transmission. This is particularly noticeable at higher error rates, where the set of error-free bits significantly differs from the set of all bits. To correctly determine the degree of compression required at the privacy

[4] It is interesting to note that the solution given by Eq. (16) can also be obtained by slightly altering the FGGNP97 derivation. Specifically, it is obtained if the information gain under the error-free condition [the first of Eqs. (72) in the FGGNP97 work] is maximized instead of the overall information gain [Eq. (73)]. Together with the link between Shannon and Renyi information established in our Appendix B, this offers an alternative proof of the results of this section.

amplification stage, Alice and Bob must concentrate their attention on the former set.

The treatment we have presented appears to cover all individual eavesdropping attacks not forbidden by physical laws. Subject to the limitations discussed below, no permissible device can provide Eve with greater knowledge for a given error rate than indicated by the uppermost curves in Figs. 5 and 6, at least so long as Alice and Bob use the versions of B92 and BB84 protocols described in the beginning of Secs. III A and IV A. (In particular, Bob must be using von Neumann detection in B92.) Armed with Eqs. (13) and (16), Alice and Bob can be confident that after privacy amplification their key is secure, in the sense that Eve is exponentially unlikely to have more than token knowledge of it.

It is important, however, to point out known limitations of our result. First, it has been assumed throughout that Eve subjects each of Alice's bits to identical and independent individual attacks. In the alternative, Eve could direct each of Alice's particles into a separate probe, and subsequently make a single quantum measurement of all probes at once. Even more generally, Eve could entangle all particles with a single probe. Mathematical analyses of such attacks, which have been respectively termed *collective* and *joint*, only recently started appearing in the literature. Although collective and joint attacks at present seem impractical, they are a subject of intensive investigation. However, such attacks are beyond the scope of this paper.

Secondly, it has of course been assumed that carrier states $|\mathbf{u}\rangle,|\mathbf{v}\rangle,|\overline{\mathbf{u}}\rangle,|\overline{\mathbf{v}}\rangle$ all lie in the same Hilbert plane, and that Bob makes von Neumann measurements in that plane. Let us note that a quantum cryptographic implementation may sometimes violate these assumptions in ways not immediately apparent to Alice and Bob. For example, a single photon polarized vertically, $|1_{\uparrow}\rangle$, and one polarized diagonally, $|1_{\nearrow}\rangle$, are nonorthogonal states that satisfy the requirements of quantum cryptographic protocols as $\mathbf{u}$ and $\mathbf{v}$. However, a slight optical misalignment in space, or a slight difference in spectral profile, could reduce the overlap $\sin 2\alpha$ between the two states, or even render them orthogonal, and leave the system vulnerable to eavesdropping. Similarly, the overlap between n-photon states $|n_{\uparrow}\rangle$, $|n_{\nearrow}\rangle$ is smaller than between likewise polarized single photons (and tends to zero for large n), so that multiphoton states, if occasionally emitted by Alice's source, require special handling. (By the same argument, the transmission becomes vulnerable if Alice and Bob use a carrier particle that, unbeknown to them, possesses an internal structure Eve can probe.) One possible attack on multiphoton states is described in detail in Ref. [19]; one possible defense available to Alice and Bob is to adopt the worst-case assumption that all multiphoton bits have been intercepted, and use extra compression at the privacy amplification stage [18].

For an example of another kind, consider a B92 eavesdropping strategy wherein Eve intercepts each passing particle and measures it in the same manner as Bob would. Whenever Eve obtains a conclusive result, she learns the data bit for certain and retransmits the particle error-free; and when Eve's result is inconclusive, she blocks the particle so Bob receives nothing. Ultimately, the entire transmission is error-free, and Eve has complete knowledge of it—a result a complacent Alice and Bob might have thought impossible. In this example, security theorems fail because Eve is transmitting to Bob a particle state (namely, the vacuum state) that does not lie in the same Hilbert plane with the states he expects, and Bob does not register this condition as an error. Counting each nondetection as an error would resolve the difficulty, but is generally impractical because of ''natural'' losses in the channel. An alternative approach is to design the system so that no particle state can be transmitted by Eve without the risk of causing an error; one such design, involving a combination of a strong and a weak pulse, appears in Ref. [5]. Safety of this and similar countermeasures, however, does not follow from the analysis we have presented, and must be proven separately.

Finally, let us mention a possible enhancement to known quantum cryptographic protocols that is suggested by the present work. At the core of quantum cryptography is the relationship between the maximum information the eavesdropper can extract, and the disturbance she necessarily introduces into the transmission [8]. The error rate need not be the sole measure of this disturbance. Any other quantity available to Alice and Bob, for example, the rate of inconclusive outcomes, can serve the same purpose, so long as firm connection is demonstrated between deviation of this quantity from its interference-free level, and the eavesdropper's information gain. Indeed, several alternative metrics of disturbance have already been investigated [8], but their eavesdrop-detecting power in the context of quantum cryptography is yet to be explored. It seems likely that the use of additional indicators, along with the error rate, would make the eavesdropper's task more difficult, and hence improve system throughput by allowing Alice and Bob to secure the transmission at the cost of sacrificing less data. Expected values for many such indicators can be constructed with reference to Table I in the same manner as the error rate in Eq. (9), and used along with Eq. (9) as an additional constraint in optimizing information gain on the eavesdropper's behalf. Effectiveness of the various disturbance metrics and their combinations as estimators of information gain must remain a subject for future investigation.

ACKNOWLEDGMENTS

This research is supported in part by the Focused Research Initiative program of BMDO, the U.S. Air Force Office of Scientific Research, and the National Science Foundation.

APPENDIX A: SYMMETRIES OF THE EAVESDROPPING APPARATUS

In this appendix we prove that the eavesdropping probe may be assumed, without loss of generality, to have some of the same symmetries as Alice's transmitter and Bob's receiver.

The first symmetry to be considered is a reflection $\mathbf{R_e}$ in the carrier particle space that interchanges $\mathbf{e}_0 \leftrightarrow \mathbf{e}_1$. An eavesdropping probe will be called $\mathbf{R}$-*symmetric* if there exists an extension $\mathbf{R}=\mathbf{R_e}\otimes\mathbf{R_w}$ of $\mathbf{R_e}$ into the space of the probe, under which both the evolution operator $\mathbf{U}$ and the initial probe state $|\mathbf{w}\rangle$ are invariant. Although Eve is under no obligation to employ an **R**-symmetric device, we shall argue that, for any probe lacking such symmetry, there exists an **R**-symmetric variant at least as effective for eavesdropping purposes.

Recall that our model views the transmission as a series of independent events, in which Alice emits a particle in state $\mathbf{x}\in\{\mathbf{u},\mathbf{v},\overline{\mathbf{u}},\overline{\mathbf{v}}\}$, Bob detects it as $\mathbf{y}\in\{\mathbf{u},\mathbf{v},\overline{\mathbf{u}},\overline{\mathbf{v}},\mathbf{i}\}$ (where **i** stands for an inconclusive result), and Eve obtains an outcome **z** from the measurement of her probe. The joint probability distribution $P_{XYZ}(\mathbf{x},\mathbf{y},\mathbf{z})$, known to Eve, implies statistical dependence between **z** and $\{\mathbf{x},\mathbf{y}\}$, from which Eve derives her knowledge of the key. It also implies statistical dependence between **x** and **y**, which Alice and Bob estimate through public discussion and scrutinize for evidence of possible eavesdropping.

Since the state pairs $\{\mathbf{u},\overline{\mathbf{u}}\},\{\mathbf{v},\overline{\mathbf{v}}\}$ play symmetrical roles in the protocol, a statistical connection between **z** and an event involving **u** has the same worth to Eve as a similar connection involving **v**. In mathematical terms, if two physical systems give rise, respectively, to event probability distributions P_{XYZ} and P'_{XYZ} such that they can be obtained from one another by interchanging **u** and **v** [i.e., $P_{XYZ}(\mathbf{u},\overline{\mathbf{v}},\mathbf{z})=P'_{XYZ}(\mathbf{v},\overline{\mathbf{u}},\mathbf{z})$, etc.], then Eve can expect to learn the same amount of information from these two physical systems. (This amount is explicitly computed in Secs. III and IV.) Alice and Bob's analysis of P_{XYZ} and P'_{XYZ} for evidence of eavesdropping would also yield identical conclusions, so long as Alice and Bob employ symmetrical indicators such as the error rate, which are themselves invariant under the interchange of **u** and **v**. Consequently, the two physical systems corresponding to P_{XYZ} and P'_{XYZ} are substantially equivalent to all parties.

Let **U** and $|\mathbf{w}\rangle$ be the evolution operator and the initial state of an asymmetric probe, and let the associated event distribution be P_{XYZ}. The physical system associated with the companion distribution P'_{XYZ} can be obtained by everywhere interchanging **u** and **v**. However, since both the transmitter and the receiver are invariant with respect to this interchange (in that they generate statistically the same events before and after it), it is sufficient to interchange **u** and **v** only in the eavesdropping probe, by replacing **U** with its image $\mathbf{U}'$ under $\mathbf{R_e}$: $\mathbf{U}'=(\mathbf{R_e}\otimes\mathbb{1})\mathbf{U}(\mathbf{R_e}^{-1}\otimes\mathbb{1})$. For the reasons just stated, **U** and $\mathbf{U}'$ yield substantially equivalent eavesdropping systems. Now define

$$\tilde{\mathbf{U}}\hat{=}\mathbf{U}\otimes\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\mathbf{U}'\otimes\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},$$

$$\tilde{\mathbf{R}}\hat{=}\mathbf{R_e}\otimes\mathbb{1}\otimes\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad |\tilde{\mathbf{w}}\rangle\hat{=}|\mathbf{w}\rangle\otimes\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}.$$

It is immediately evident that $\tilde{\mathbf{U}}$ is unitary; that $\tilde{\mathbf{R}}$ is a reflection (it is accomplished by an interchange of basis vectors); and that the probe represented by $\{\tilde{\mathbf{U}};|\tilde{\mathbf{w}}\rangle\}$ is **R**-symmetric, since both $\tilde{\mathbf{R}}\tilde{\mathbf{U}}\tilde{\mathbf{R}}^{-1}=\tilde{\mathbf{U}}$ and $\tilde{\mathbf{R}}|\tilde{\mathbf{w}}\rangle=|\tilde{\mathbf{w}}\rangle$ hold. The rightmost factor in the tensor product can be interpreted as the Hilbert space of an auxiliary spin-$\frac{1}{2}$ particle. If Eve subsequently measures the auxiliary particle in the basis $\{(0,1);(1,0)\}$, the evolution $\tilde{\mathbf{U}}$ reduces to a coin toss, followed by equiprobable application of either **U** or $\mathbf{U}'$. Thus $\tilde{\mathbf{U}}$ can lead to an eavesdropping device at least as effective as one based on **U** or $\mathbf{U}'$. This completes the proof.

Consider next another symmetry, represented by the transformation $\mathcal{Z}_{\mathcal{W}}$ in the Hilbert space that consists of replacing all vector projections and operator matrix elements in some orthonormal basis $\mathcal{W}$ with their complex conjugates, and call an eavesdropping device *$\mathcal{Z}$-symmetric* if there exists a basis $\mathcal{W}$ such that both the evolution operator **U** and the initial probe state $|\mathbf{w}\rangle$ are invariant under $\mathcal{Z}_{\mathcal{W}}$. As before, we shall construct an equally effective $\mathcal{Z}$-symmetric alternative for any probe lacking $\mathcal{Z}$-symmetry.

Since probabilities of events in quantum mechanics are given by moduli squared of vector inner products, two physical systems related to one another via $\mathcal{Z}_{\mathcal{W}}$ yield the same event probability distribution $P_{XYZ}(\mathbf{x},\mathbf{y},\mathbf{z})$, and are therefore substantially equivalent to all parties. Let us now select $\mathcal{W}$ to include vectors $|\mathbf{e}_0\rangle,|\mathbf{e}_1\rangle$, and $|\mathbf{w}\rangle$, and let $\mathbf{U}'$ be the image of **U** under $\mathcal{Z}_{\mathcal{W}}$. Since carrier states $|\mathbf{u}\rangle,|\overline{\mathbf{u}}\rangle,|\mathbf{v}\rangle,|\overline{\mathbf{v}}\rangle$ have real projections and are hence invariant under $\mathcal{Z}_{\mathcal{W}}$, transformation $\mathcal{Z}_{\mathcal{W}}$ of the entire Hilbert space is reduced to replacing **U** with $\mathbf{U}'$. It follows that **U** and $\mathbf{U}'$ represent substantially equivalent eavesdropping apparata. Defining

$$\tilde{\mathbf{U}}\hat{=}\mathbf{U}\otimes\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\mathbf{U}'\otimes\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix},\quad |\tilde{\mathbf{w}}\rangle\hat{=}|\mathbf{w}\rangle\otimes\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix},$$

$$\tilde{\mathcal{W}}=\mathcal{W}\otimes\left\{\begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix};i\begin{pmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{pmatrix}\right\}$$

it is found, as before, that $\tilde{\mathbf{U}}$ is unitary; that the probe $\{\tilde{\mathbf{U}};|\tilde{\mathbf{w}}\rangle\}$ is $\mathcal{Z}$-symmetric because both $\tilde{\mathbf{U}}$ and $|\tilde{\mathbf{w}}\rangle$ are invariant under $\mathcal{Z}_{\tilde{\mathcal{W}}}$; and that, with the proper measurement of the auxiliary particle, $\tilde{\mathbf{U}}$ reduces to a coin toss and equiprobable application of either **U** or $\mathbf{U}'$. The invariance of $\tilde{\mathbf{U}}$ and $|\tilde{\mathbf{w}}\rangle$ under $\mathcal{Z}_{\tilde{\mathcal{W}}}$ means, of course, that in basis $\tilde{\mathcal{W}}$ all matrix elements of $\tilde{\mathbf{U}}$ and all projections of $|\tilde{\mathbf{w}}\rangle$ are real numbers.

APPENDIX B: RENYI AND SHANNON INFORMATION

Here we prove the following statement: If a POVM test is used to distinguish between two *a priori* equiprobable states, then the test that yields on average the most Shannon information, also yields on average the most Renyi information.

In the case of two *a priori* equiprobable states, Eqs. (5) and (6) reduce to

$$I^H=\sum_\mu P_\mu[1+q_{1\mu}\log_2 q_{1\mu}+q_{2\mu}\log_2 q_{2\mu}]$$

$$=\sum_\mu P_\mu\tfrac{1}{2}[(1+r_\mu)\log_2(1+r_\mu)+(1-r_\mu)\log_2(1-r_\mu)],$$

$$I^R=\sum_\mu P_\mu[1+\log_2(q_{1\mu}^2+q_{2\mu}^2)]=\sum_\mu P_\mu\log_2(1+r_\mu^2), \tag{B1}$$

where $r_\mu\hat{=}q_{1\mu}-q_{2\mu}$, so that $q_{1\mu}=\frac{1}{2}(1+r_\mu)$, $q_{2\mu}=\frac{1}{2}(1-r_\mu)$. Define on the interval $0<x<1$ functions

$$f(x)\hat{=}(1+\sqrt{x})\ln(1+\sqrt{x})+(1-\sqrt{x})\ln(1-\sqrt{x}),$$

$$g(x)\hat{=}\ln(1+x)$$

and evaluate their derivatives

$$
\begin{aligned}
g'(x)&=(1+x)^{-1}>0,\\
g''(x)&=-(1+x)^{-2}<0,\\
f'(x)&=[\ln(1+x^{1/2})-\ln(1-x^{1/2})]\tfrac{1}{2}x^{-1/2}>0,\\
f''(x)&=\left[\frac{1}{1+x^{1/2}}+\frac{1}{1-x^{1/2}}\right]\tfrac{1}{2}x^{-1/2}\tfrac{1}{2}x^{-1/2}\\
&\quad+[\ln(1+x^{1/2})-\ln(1-x^{1/2})]\tfrac{1}{2}(-\tfrac{1}{2}x^{-3/2})\\
&=\frac{1}{4x^{3/2}(1-x)}\left[2x^{1/2}-(1-x)\ln\frac{1+x^{1/2}}{1-x^{1/2}}\right]>0.
\end{aligned}
\tag{B2}
$$

To prove the last of the four inequalities (B2), consider

$$h(z)\triangleq 2z-(1-z^2)\ln\frac{1+z}{1-z},$$

which is positive on $0<z<1$ because $h(0)=0$ and

$$
\begin{aligned}
h'(z)&=2+2z\ \ln\frac{1+z}{1-z}-(1-z^2)\left(\frac{1}{1+z}+\frac{1}{1-z}\right)\\
&=2z\ \ln\frac{1+z}{1-z}>0 \quad (0<z<1).
\end{aligned}
$$

Since $f''(x)>0$ on the interval of interest, it follows that $f(x)$ is a *convex* function, with the property $\Sigma\lambda_i f(\delta_i)\geqslant f(\Sigma\lambda_i\delta_i)$ for any set $\{\lambda_i\}$ that sums up to 1. Applying this in Eq. (B1), we have for an arbitrary POVM test

$$2\ \ln(2)I^H=\sum_\mu P_\mu f(r_\mu^2)\geqslant f\left(\sum_\mu P_\mu r_\mu^2\right).$$

On the other hand, the quantity $I_{\rm opt}^H$ given by Eq. (7a) is known to be the greatest Shannon information gain possible, and therefore

$$2\ \ln(2)I_{\rm opt}^H=f(\cos^2 2\zeta)\geqslant 2\ \ln(2)I^H.$$

Noting from Eq. (B2) that $f'(x)>0$, it can now be concluded that for any POVM test

$$\cos^2 2\zeta\geqslant\sum_\mu P_\mu r_\mu^2.$$

Consider next the function $g(x)$, which according to Eq. (B2) is positively sloped, $g'(x)>0$, and *concave*, $g''(x)<0$. With the aid of the inequality immediately above, concavity of $g(x)$ leads to

$$
\begin{aligned}
\ln(2)I^R&=\sum_\mu P_\mu g(r_\mu^2)\leqslant g\left(\sum_\mu P_\mu r_\mu^2\right)\leqslant g(\cos^2 2\zeta)\\
&=\ln(2)I_{\rm opt}^R,
\end{aligned}
$$

where $I_{\rm opt}^R$ is the quantity given in Eq. (7a). This completes the proof.

APPENDIX C: EXPLICIT EXPRESSIONS FOR PROJECTION VECTORS $\psi_{i,j}$

Expressions for $|\psi_{i,j}\rangle$, $i,j\in\{\mathbf{u},\overline{\mathbf{u}},\mathbf{v},\overline{\mathbf{v}}\}$, are obtained by direct substitution of carrier states from Eq. (1), and the unitary evolution from Eq. (2), into Eq. (8):

$$
\begin{aligned}
|\psi_{\mathbf{u},\mathbf{v}}\rangle&=\langle\mathbf{v}|\mathbf{U}|\mathbf{u}\otimes\mathbf{w}\rangle=(\cos\ \alpha\langle\mathbf{e}_1|+\sin\ \alpha\langle\mathbf{e}_0|)\mathbf{U}\\
&\quad\times(\cos\ \alpha|\mathbf{e}_0\otimes\mathbf{w}\rangle+\sin\ \alpha|\mathbf{e}_1\otimes\mathbf{w}\rangle)\\
&=|\Phi_{01}\rangle\cos^2\ \alpha+|\Phi_{10}\rangle\sin^2\ \alpha+(|\Phi_{11}\rangle\\
&\quad+|\Phi_{00}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\mathbf{u},\mathbf{u}}\rangle&=|\Phi_{00}\rangle\cos^2\ \alpha+|\Phi_{11}\rangle\sin^2\alpha\\
&\quad+(|\Phi_{10}\rangle+|\Phi_{01}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\mathbf{u},\overline{\mathbf{v}}}\rangle&=|\Phi_{00}\rangle\cos^2\ \alpha-|\Phi_{11}\rangle\sin^2\ \alpha\\
&\quad+(|\Phi_{10}\rangle-|\Phi_{01}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\mathbf{u},\overline{\mathbf{u}}}\rangle&=|\Phi_{01}\rangle\cos^2\ \alpha-|\Phi_{10}\rangle\sin^2\ \alpha\\
&\quad+(|\Phi_{11}\rangle-|\Phi_{00}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\mathbf{v},\overline{\mathbf{u}}}\rangle&=|\Phi_{11}\rangle\cos^2\ \alpha-|\Phi_{00}\rangle\sin^2\ \alpha\\
&\quad-(|\Phi_{10}\rangle-|\Phi_{01}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\overline{\mathbf{u}},\mathbf{u}}\rangle&=|\Phi_{10}\rangle\cos^2\ \alpha-|\Phi_{01}\rangle\sin^2\ \alpha\\
&\quad+(|\Phi_{11}\rangle-|\Phi_{00}\rangle)\sin\ \alpha\ \cos\ \alpha,
\end{aligned}
$$

$$
\begin{aligned}
|\psi_{\overline{\mathbf{u}},\overline{\mathbf{u}}}\rangle&=|\Phi_{11}\rangle\cos^2\ \alpha+|\Phi_{00}\rangle\sin^2\ \alpha\\
&\quad-(|\Phi_{10}\rangle+|\Phi_{01}\rangle)\sin\ \alpha\ \cos\ \alpha.
\end{aligned}
$$

Taking advantage of symmetries $\|\Phi_{00}\|^2=\|\Phi_{11}\|^2$, $\|\Phi_{10}\|^2=\|\Phi_{01}\|^2$, $\langle\Phi_{11}|\Phi_{10}\rangle=\langle\Phi_{00}|\Phi_{01}\rangle$, $\langle\Phi_{11}|\Phi_{01}\rangle=\langle\Phi_{00}|\Phi_{10}\rangle$ (recall also that both these inner products are real), $\|\Phi_{00}\|^2+\|\Phi_{01}\|^2=\|\Phi_{11}\|^2+\|\Phi_{10}\|^2=1$, and the identity $\cos^4\alpha+\sin^4\alpha=1-\frac{1}{2}\sin^2 2\alpha$,

$$
\begin{aligned}
\|\psi_{\mathbf{u},\mathbf{v}}\|^2&=\|\Phi_{01}\|^2\ \cos^4\ \alpha+\|\Phi_{10}\|^2\ \sin^4\ \alpha\\
&\quad+(\|\Phi_{11}\|^2+\|\Phi_{00}\|^2+2\langle\Phi_{11}|\Phi_{00}\rangle)\sin^2\ \alpha\ \cos^2\ \alpha\\
&\quad+2\langle\Phi_{01}|\Phi_{10}\rangle\sin^2\ \alpha\ \cos^2\ \alpha\\
&\quad+2(\langle\Phi_{01}|\cos^2\ \alpha+\langle\Phi_{10}|\sin^2\ \alpha)(|\Phi_{11}\rangle\\
&\quad+|\Phi_{00}\rangle)\sin\ \alpha\ \cos\ \alpha\\
&=\|\Phi_{01}\|^2(1-\tfrac{1}{2}\ \sin^2\ 2\alpha)\\
&\quad+(\|\Phi_{00}\|^2+\langle\Phi_{11}|\Phi_{00}\rangle+\langle\Phi_{01}|\Phi_{10}\rangle)\tfrac{1}{2}\ \sin^2\ 2\alpha\\
&\quad+(\langle\Phi_{01}|\Phi_{11}\rangle+\langle\Phi_{10}|\Phi_{11}\rangle)\sin\ 2\alpha\\
&=\tfrac{1}{2}(1-d)+(d+a)\tfrac{1}{2}\ \sin^2\ 2\alpha+c\tfrac{1}{2}\ \sin\ 2\alpha,
\end{aligned}
$$

$$\|\psi_{\mathbf{u},\mathbf{u}}\|^2=\tfrac{1}{2}(1+d)+(-d+a)\tfrac{1}{2}\ \sin^2 2\alpha+c\tfrac{1}{2}\ \sin 2\alpha,$$

$$\|\psi_{\mathbf{u},\bar{\mathbf{v}}}\|^2=\tfrac{1}{2}(1+d)+(-d-a)\tfrac{1}{2}\sin^2 2\alpha-c\tfrac{1}{2}\ \sin 2\alpha,$$

$$\|\psi_{\mathbf{u},\bar{\mathbf{u}}}\|^2=\tfrac{1}{2}(1-d)+(d-a)\tfrac{1}{2}\ \sin^2 2\alpha-c\tfrac{1}{2}\ \sin 2\alpha,$$

$$\|\psi_{\bar{\mathbf{u}},\mathbf{u}}\|^2=\tfrac{1}{2}(1-d)+(d-a)\tfrac{1}{2}\ \sin^2 2\alpha+c\tfrac{1}{2}\ \sin 2\alpha,$$

$$\|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\|^2=\tfrac{1}{2}(1+d)+(-d+a)\tfrac{1}{2}\ \sin^2 2\alpha-c\tfrac{1}{2}\ \sin 2\alpha,$$

with the notation a,b,c,d of Eq. (12). (The result for $|\psi_{\bar{\mathbf{u}}\bar{\mathbf{u}}}\rangle$ can be obtained from $|\psi_{\mathbf{u},\mathbf{u}}\rangle$ by replacing $\alpha\rightarrow\alpha+\frac{1}{2}\pi$, and $|\psi_{\bar{\mathbf{u}}\mathbf{u}}\rangle$ can be obtained from interchanging indices $\Phi_{mn}\rightarrow\Phi_{nm}$.) Finally, evaluate the inner products

$$\begin{aligned}\langle\psi_{\mathbf{u},\bar{\mathbf{v}}}|\psi_{\mathbf{v},\bar{\mathbf{u}}}\rangle=&\langle\Phi_{00}|\Phi_{11}\rangle(\cos^4\alpha+\sin^4\alpha)\\&+[-\|\Phi_{00}\|^2-\|\Phi_{11}\|^2-(\|\Phi_{10}\|^2+\|\Phi_{01}\|^2\\&-2\langle\Phi_{10}|\Phi_{01}\rangle)]\sin^2\alpha\ \cos^2\alpha\\&+(-\langle\Phi_{00}|\cos^2\alpha+\langle\Phi_{11}|\sin^2\alpha+\langle\Phi_{11}|\cos^2\alpha\\&-\langle\Phi_{00}|\sin^2\alpha)(|\Phi_{10}\rangle-|\Phi_{01}\rangle)\sin\alpha\ \cos\alpha\\=&\langle\Phi_{00}|\Phi_{11}\rangle(1-\tfrac{1}{2}\ \sin^2 2\alpha)\\&+(-1+\langle\Phi_{10}|\Phi_{01}\rangle)\tfrac{1}{2}\ \sin^2 2\alpha+((\langle\Phi_{11}|\\&-\langle\Phi_{00}|)(|\Phi_{10}\rangle-|\Phi_{01}\rangle)\tfrac{1}{2}\ \sin 2\alpha\\=&\tfrac{1}{2}(a+b)-(1+b)\tfrac{1}{2}\ \sin^2 2\alpha+c\tfrac{1}{2}\ \sin 2\alpha,\end{aligned}$$

$$\begin{aligned}\langle\psi_{\mathbf{u},\mathbf{u}}|\psi_{\bar{\mathbf{u}},\bar{\mathbf{u}}}\rangle=&\langle\Phi_{00}|\Phi_{11}\rangle(\cos^4\alpha+\sin^4\alpha)\\&+[\|\Phi_{00}\|^2+\|\Phi_{11}\|^2-(\|\Phi_{10}\|^2+\|\Phi_{01}\|^2\\&+2\langle\Phi_{10}|\Phi_{01}\rangle)]\sin^2\alpha\ \cos^2\alpha\\&+(-\langle\Phi_{00}|\cos^2\alpha-\langle\Phi_{11}|\sin^2\alpha+\langle\Phi_{11}|\cos^2\alpha\\&+\langle\Phi_{00}|\sin^2\alpha)(|\Phi_{10}\rangle+|\Phi_{01}\rangle)\sin\alpha\ \cos\alpha\\=&\langle\Phi_{00}|\Phi_{11}\rangle(1-\tfrac{1}{2}\ \sin^2 2\alpha)\\&+(\|\Phi_{00}\|^2-\|\Phi_{01}\|^2-\langle\Phi_{10}|\Phi_{01}\rangle)\tfrac{1}{2}\ \sin^2 2\alpha\\&+((\langle\Phi_{11}|-\langle\Phi_{00}|)\cos 2\alpha(|\Phi_{10}\rangle\\&+|\Phi_{01}\rangle)\tfrac{1}{2}\ \sin 2\alpha\\=&\tfrac{1}{2}(a+b)+(d-a)\tfrac{1}{2}\ \sin^2 2\alpha.\end{aligned}$$

APPENDIX D: CONDITIONAL MINIMIZATION FOR B92

The task of this appendix is to find conditional minimum $Q_{\min}(E)$ of the quantity Q subject to $E=\text{const}$, over all combinations $\{\lambda,\mu,\theta,\phi\}$, where Q and E are given by Eqs. (11) and (12). Cases of interest are those where both $E<\frac{1}{2}$ and $Q_{\min}(E)\geqslant 0$. Note that the denominator in the first of equations (11) is strictly positive, so $E<\frac{1}{2}$ implies $d>0$. It is convenient to introduce new variables

$$E'\hat{=}\frac{\cos^2 2\alpha}{1-2E}=\frac{1-a\ \sin^2 2\alpha-c\ \sin 2\alpha}{d},\quad Q'\hat{=}\frac{a+b+1}{d}.\tag{D1}$$

Minimization of Q subject to $E=\text{const}$ is equivalent to minimization of Q' subject to $E'=\text{const}$, because E' is one-to-one related to E, and Q grows with Q' for any fixed E':

$$\begin{aligned}Q&=\frac{(a+b)\cos^2 2\alpha+(1-dE')-\sin^2 2\alpha}{d\ \cos^2 2\alpha+dE'}\\&=\frac{1}{\cos^2 2\alpha+E'}\left(\cos^2 2\alpha\left\{\frac{a+b+1}{d}\right\}-E'\right).\end{aligned}$$

(Recall that α is a fixed system parameter outside the scope of the minimization problem.) The interval of interest $0\leqslant E<\frac{1}{2}$ maps $\cos^2 2\alpha\leqslant E'<+\infty$.

Since the independent variable λ appears in Eq. (12) only through $\cos^2\lambda$, it is sufficient to consider $0\leqslant\lambda\leqslant\pi/2$. Most of the following discussion deals with the special case $\lambda=0$. It will be shown later in this appendix that the solution associated with $\lambda=0$ is also the desired global conditional minimum over all values of λ.

In the case $\lambda=0$, Eqs. (D1) and (12) reduce to

$$\begin{aligned}Q'&=\frac{(\cos 2\theta+1)\sin 2\phi+1}{\cos 2\theta},\\E'&=\frac{1-\cos 2\theta\ \sin 2\phi\ \sin^2 2\alpha-\sin 2\theta\ \cos 2\phi\ \sin 2\alpha}{\cos 2\theta},\end{aligned}\tag{D2}$$

with only two surviving independent variables, θ and ϕ. The Lagrange multipliers theorem states that at any point $\{\theta,\phi\}$ where Q' may be reaching extremum subject to $E'=\text{const}$, at least one of the following two conditions must hold: either (i) all partial derivatives of E' on the independent variables θ, ϕ simultaneously vanish; or (ii) there exists a value ζ such that all partial derivatives on the independent variables θ, ϕ of the Lagrange function

$$F\hat{=}Q'+\zeta E'=\frac{[\cos 2\theta(1-\zeta\ \sin^2 2\alpha)+1]\sin 2\phi-\zeta\ \sin 2\theta\ \sin 2\alpha\ \cos 2\phi+(1+\zeta)}{\cos 2\theta}\tag{D3}$$

Note that Eq. (D2) implies

$$\frac{1}{\cos 2\theta}=\frac{E'+\sin 2\phi\ \sin^2 2\alpha}{1-\sin 2\theta\ \cos 2\phi \sin 2\alpha}<\frac{E'+1}{1-\sin 2\alpha}$$

and therefore each constraint contour $E'=\text{const}$ is contained within the interior of some closed region $\{-1\leqslant\sin 2\phi\leqslant 1, 0<\epsilon\leqslant\cos 2\theta\leqslant 1\}$ where both Q' and E' are differentiable. This guarantees that Q' would indeed reach its conditional extrema at some of its Lagrange points.

The condition constraining partial derivatives of E' will be addressed first. Observe that as a function of ϕ, E' in Eq. (D2) has the form

$$E'=A_{E\phi}\sin 2\phi+B_{E\phi}\cos 2\phi+C_{E\phi},$$

where the coefficients $A_{E\phi}\hat{=}-\sin^2 2\alpha$, $B_{E\phi}\hat{=}-\tan 2\theta\sin 2\alpha$, $C_{E\phi}\hat{=}(\cos 2\theta)^{-1}$ do not depend on ϕ. The roots ϕ_{E0} of the partial derivative $\partial E'/\partial\phi$ therefore satisfy

$$\sin 2\phi_{E0}=\pm\frac{A_{E\phi}}{\sqrt{A_{E\phi}^2+B_{E\phi}^2}},\quad \cos 2\phi_{E0}=\pm\frac{B_{E\phi}}{\sqrt{A_{E\phi}^2+B_{E\phi}^2}}. \tag{D4}$$

The other partial derivative $\partial E'/\partial\theta$ vanishes simultaneously with $\partial E'/\partial\phi$ when

$$\left.\frac{\partial E'(\theta,\phi)}{\partial\theta}\right|_{\phi=\phi_{E0}(\theta)}=0 \Leftrightarrow \frac{\partial E'}{d\theta}\frac{(\theta,\phi_{E0}(\theta))}{\partial\theta}$$

$$=\frac{\partial}{\partial\theta}\{\pm\sqrt{A_{E\phi}^2+B_{E\phi}^2}+C_{E\phi}\}=0.$$

With change of variables $z\hat{=}(\cos 2\theta)^{-1}$, the above condition transforms into

$$\frac{\partial}{\partial z}\{\pm\sin 2\alpha\sqrt{\sin^2 2\alpha+(z^2-1)}+z\}$$

$$\propto\pm z\ \sin 2\alpha+\sqrt{\sin^2 2\alpha+(z^2-1)}=0 \Rightarrow z^2=1 \tag{D5}$$

to which must be added any roots of $dz/d\theta$. The latter yields only one relevant root $\cos 2\theta_{E0}=1$, as does Eq. (D5) [recall that $d=\cos 2\theta$ is restricted to positive values to ensure $E<\frac{1}{2}$ in Eq. (11)]. The first alternative of the Lagrange theorem is thus only satisfied with $\cos 2\theta=1$ and [via Eq. (D4)] $\sin 2\phi=\pm 1$.

Turn now to the second possibility, that all partial derivatives of the Lagrange function vanish. The Lagrange function F can be analyzed in the same general manner as E', although the required algebraic manipulation is more extensive. In particular, Eq. (D3) has the familiar form $F=A_\phi\sin 2\phi+B_\phi\cos 2\phi+C_\phi$, with roots ϕ_0 of the partial derivative $\partial F/\partial\phi$ given by

$$\sin 2\phi_0=\pm\frac{A_\phi}{\sqrt{A_\phi^2+B_\phi^2}},\quad \cos 2\phi_0=\pm\frac{B_\phi}{\sqrt{A_\phi^2+B_\phi^2}}, \tag{D6}$$

which reduce the simultaneous condition on $\partial F/\partial\theta$ to

$$\frac{\partial}{\partial z}\{\pm\sqrt{A_\phi^2+B_\phi^2}+C_\phi\}=\frac{\partial}{\partial z}\{\pm\sqrt{(1-\zeta\ \sin^2 2\alpha+z)^2+\zeta^2(z^2-1)\sin^2 2\alpha}+(1+\zeta)z\}=0,$$

where $z\hat{=}(\cos 2\theta)^{-1}$ as before. Next rewrite the above relation as

$$\frac{\partial}{\partial z}\{\pm\sqrt{(1+\zeta^2\ \sin^2 2\alpha)z^2+2(1-\zeta\ \sin^2 2\alpha)z+[(1-\zeta\ \sin^2 2\alpha)^2-\zeta^2\ \sin^2 2\alpha]}+(1+\zeta)z\}$$

$$=\frac{\partial}{\partial z}\{A_\theta z\pm\sqrt{B_\theta z^2+2C_\theta z+D_\theta}\}\propto A_\theta\sqrt{B_\theta z^2+2C_\theta z+D_\theta}\pm(B_\theta z+C_\theta)=0 \tag{D7}$$

and solve the resulting quadratic,

$$\begin{gathered}A_\theta^2(B_\theta z^2+2C_\theta z+D_\theta)=B_\theta^2 z^2+2B_\theta C_\theta z+C_\theta^2 \Leftrightarrow (A_\theta^2-B_\theta)B_\theta z^2+2(A_\theta^2-B_\theta)C_\theta z+(A_\theta^2 D_\theta-C_\theta^2)=0\\ z_\pm=-\frac{C_\theta}{B_\theta}\pm\left(\frac{C_\theta^2}{B_\theta^2}-\frac{A_\theta^2 D_\theta-C_\theta^2}{B_\theta(A_\theta^2-B_\theta)}\right)^{1/2}=-\frac{C_\theta}{B_\theta}\pm\frac{A_\theta}{B_\theta}\left(\frac{C_\theta^2-B_\theta D_\theta}{A_\theta^2-B_\theta}\right)^{1/2},\end{gathered} \tag{D8}$$

where

$$\left(\frac{C_\theta^2-B_\theta D_\theta}{A_\theta^2-B_\theta}\right)^{1/2}=\left(\frac{(1-\zeta\ \sin^2 2\alpha)^2-(1+\zeta^2\ \sin^2 2\alpha)[(1-\zeta\ \sin^2 2\alpha)^2-\zeta^2\ \sin^2 2\alpha]}{(1+\zeta)^2-(1+\zeta^2\ \sin^2 2\alpha)}\right)^{1/2}$$

$$=\left(\frac{(1-\zeta\ \sin^2 2\alpha)^2(-\zeta^2\ \sin^2 2\alpha)+(1+\zeta^2\ \sin^2 2\alpha)\zeta^2\ \sin^2 2\alpha}{2\zeta+\zeta^2-\zeta^2\ \sin^2 2\alpha}\right)^{1/2}=|\zeta|\sin^2 2\alpha$$

so that finally

$$z_{\pm}=-\frac{C_\theta}{B_\theta}\pm\frac{A_\theta}{B_\theta}|\zeta|\sin^2 2\alpha=\frac{-1+\zeta\sin^2 2\alpha\pm(1+\zeta)|\zeta|\sin^2 2\alpha}{1+\zeta^2\sin^2 2\alpha}. \tag{D9}$$

Note that only the choice of positive sign in Eq. (D9), together with $\zeta\geqslant 0$, can produce a root $z\geqslant 1$, as required for the existence of a valid value for θ and to satisfy $d>0$, $E<\frac{1}{2}$. Substitution of Eq. (D8) back into Eq. (D7) demonstrates that z_+ solves for the negative sign in Eqs. (D6) and (D7) and also yields the identity

$$\sqrt{B_\theta z_+^2+2C_\theta z_++D_\theta}=\frac{B_\theta z_++C_\theta}{A_\theta}=\left(\frac{C_\theta^2-B_\theta D_\theta}{A_\theta^2-B_\theta}\right)^{1/2}=|\zeta|\sin^2 2\alpha,$$

which, together with Eqs. (D9) and (D6), leads to explicit expressions for the first set of suspected extremum points $\{\theta_{0a},\phi_{0a}\}$,

$$(\cos 2\theta_{0a})^{-1}=z_+=\frac{(\zeta^2\sin^2 2\alpha-1)+2\zeta\sin^2 2\alpha}{1+\zeta^2\sin^2 2\alpha},$$

$$\sin 2\phi_{0a}=\frac{-A_\phi}{\sqrt{A_\phi^2+B_\phi^2}}=\frac{-A_\phi}{\sqrt{B_\theta z_+^2+2C_\theta z_++D_\theta}}=\frac{\zeta\sin^2 2\alpha-1-z_+}{\zeta\sin^2 2\alpha}=\frac{(\zeta^2\sin^2 2\alpha-1)-2\zeta}{1+\zeta^2\sin^2 2\alpha}. \tag{D10}$$

The above result is simplified by a change of variables: specifically, the identity

$$\begin{aligned}(\cos 2\theta_{0a})^{-2}+\sin^2 2\phi_{0a}\sin^2 2\alpha&=(1+\zeta^2\sin^2 2\alpha)^{-2}[(\zeta^2\sin^2 2\alpha-1)^2+4\zeta^2\sin^4 2\alpha+4\zeta\sin^2 2\alpha(\zeta^2\sin^2 2\alpha-1)]\\&\quad+(1+\zeta^2\sin^2 2\alpha)^{-2}[(\zeta^2\sin^2 2\alpha-1)^2+4\zeta^2-4\zeta(\zeta^2\sin^2 2\alpha-1)]\sin^2 2\alpha\\&=(1+\zeta^2\sin^2 2\alpha)^{-2}(1+\sin^2 2\alpha)[(\zeta^2\sin^2 2\alpha-1)^2+4\zeta^2\sin^2 2\alpha]=1+\sin^2 2\alpha\end{aligned}$$

permits us to introduce a new parameter γ, defined by

$$\sin\gamma=\sin 2\phi_{0a}\sin\delta,\quad \cos\gamma=(\cos 2\theta_{0a})^{-1}\cos\delta,$$
$$-\delta\leqslant\gamma\leqslant\delta, \tag{D11a}$$

where $\sin\delta\hat{=}\sin 2\alpha/\sqrt{1+\sin^2 2\alpha}$, $\cos\delta\hat{=}1/\sqrt{1+\sin^2 2\alpha}$, $0<\delta<\pi/4$. Equation (D11a) covers the entire range $-1\leqslant\sin 2\phi<1$ generated (with $\sin^{-2}2\alpha\leqslant\zeta<+\infty$) by Eq. (D10). Equation (D11a) covers as well the remaining point $\sin 2\phi=1$, which is also an extremum candidate by virtue of the first Lagrange condition, see Eq. (D5). To each value of $\sin 2\phi_0$ corresponds exactly one positive value of $\cos 2\theta_0$. Note that the negative sign in Eq. (D6) gives $\cos 2\phi_0$ the same sign as $\sin 2\theta_0$. It can be freely assumed that both are positive, since only the product $\sin 2\theta\cos 2\phi$ appears in the problem [see Eq. (D2)].

Additional solutions result from Eq. (D8) in the degenerate case $A_\theta^2=B_\theta$, which is realized if $\zeta=0$ or $\zeta=-2(1-\sin^2 2\alpha)^{-1}$. The first root, $\zeta=0$, identically satisfies Eq. (D7) with negative sign chosen in Eqs. (D6) and (D7), and leads to

$$\sin 2\phi_{0b}=-1,\quad 0<\cos 2\theta_{0b}\leqslant 1, \tag{D11b}$$

while the second root requires positive sign in Eqs. (D6) and (D7) and

$$\sin 2\phi_{0c}=A_{\phi c}/\sqrt{A_{\phi c}^2+B_{\phi c}^2},\quad 0<\cos 2\theta_{0c}\leqslant 1,$$

where

$$A_{\phi c}=\frac{1+\sin^2 2\alpha}{1-\sin^2 2\alpha}+\frac{1}{\cos 2\theta_{0c}},\quad B_{\phi c}=\frac{2\sin 2\alpha}{1-\sin^2 2\alpha}\tan 2\theta_{0c}. \tag{D11c}$$

The points $\{\theta,\phi\}$ given by Eqs. (D11a) through (D11c) meet the preconditions for extremum according to the Lagrange multipliers theorem, in the case $\lambda=0$. To determine which of them realize the desired conditional minimum of Q', evaluate the dependent variables E',Q' at the suspected extremum points. Equation (D2) yields with Eq. (D11a)

$$Q'_{0a}\hat{=}Q'|_{\substack{\theta_{0a},\phi_{0a}\\ \lambda=0}}=\frac{\sin\gamma}{\sin\delta}+\frac{\sin\gamma\cos\gamma}{\sin\delta\cos\delta}+\frac{\cos\gamma}{\cos\delta}=\frac{\sin(\gamma+\delta)+\frac{1}{2}\sin 2\gamma}{\sin\delta\cos\delta},$$

$$\begin{aligned}E'_{0a}\hat{=}E'|_{\substack{\theta_{0a},\phi_{0a}\\ \lambda=0}}&=\frac{\cos\gamma}{\cos\delta}-\frac{\sin\gamma}{\sin\delta}\sin^2 2\alpha-\left(1-\frac{\sin^2\gamma}{\sin^2\delta}\right)\sin^2 2\alpha\\&=\frac{\cos(\gamma+\delta)+\sin^2\gamma}{\cos^2\delta}-\sin^2 2\alpha=\frac{\cos(\gamma+\delta)-\frac{1}{2}\cos 2\gamma}{\cos^2\delta}+\frac{1}{2}\cos^2 2\alpha,\end{aligned} \tag{D12a}$$

and with Eq. (D11b)

$$Q'_{0b} \hat{=} Q'|^{\theta_{0b},\phi_{0b}}_{\lambda=0} = -1,$$

$$E'_{0b} \hat{=} E'|^{\theta_{0b},\phi_{0b}}_{\lambda=0} = \sin^2 2\alpha + (\cos 2\theta_{0b})^{-1}, \qquad \text{(D12b)}$$

where in evaluation of E'_{0a} use was made of identities $\tan \delta = \sin 2\alpha$ and

$$\tan 2\theta_{0a} = \sqrt{(\cos 2\theta_{0a})^{-2} - 1}$$

$$= \sqrt{(1 + \sin^2 2\alpha - \sin^2 2\phi_{0a} \sin^2 2\alpha) - 1}$$

$$= \cos 2\phi_{0a} \sin 2\alpha.$$

It is evident that Eq. (D12b) parametrically defines a single-valued function $Q'_{\min}(E')$ on the interval $1 + \sin^2 2\alpha \leqslant E' < +\infty$. The same is true of Eq. (D12a) and the interval $1 - \sin^2 2\alpha \leqslant E' \leqslant 1 + \sin^2 2\alpha$, with $\gamma = \pm\delta$ generating the end points of the interval; this follows from the signs of first derivatives

$$\frac{dQ'_{0a}}{d\gamma} \propto \cos(\gamma + \delta) + \cos 2\gamma > 0,$$

$$\frac{dE'_{0a}}{d\gamma} \propto -\sin(\gamma + \delta) + \sin 2\gamma < 0, \quad |\gamma| < \delta < \pi/4.$$

Furthermore, at the sole point of overlap $E' = 1 + \sin^2 2\alpha$, both Eq. (D12a) and Eq. (D12b) yield the same value $Q' = -1$, as can be seen by letting $\gamma = -\delta$ in Eq. (D12a). Taken together, Eqs. (D12a) and (D12b) thus define a single-valued function $Q'_{\min}(E')$ on $1 - \sin^2 2\alpha \leqslant E' < +\infty$, which is the entire domain of E', see Eq. (D1). The function $Q'_{\min}(E')$ is illustrated in Fig. 7 by the curve $\mathcal{L}_0$.

The signs of the derivatives $dQ'_{0a}/d\gamma$ and $dE'_{0a}/d\gamma$ also establish that $Q'_{\min}(E')$ is a nonincreasing function of E', so that

$$Q'_{\min}(E') \leqslant Q'_{\min}(1 - \sin^2 2\alpha) = 3.$$

On the other hand, the quantity $Q'_{0c} \hat{=} Q'|^{\theta_{0c},\phi_{0c}}_{\lambda=0}$ that results from substitution of Eq. (D11c) into Eq. (D2), is seen to be everywhere not less than 3. Apart from the special case $\cos 2\theta_{0c} = 1$, which leads identically to $Q'_{0c} = 3$, the ratio

$$\frac{A_{\phi c}}{|B_{\phi c}|} = \frac{1 + \sin^2 2\alpha + (1 - \sin^2 2\alpha)(\cos 2\theta_{0c})^{-1}}{2 \sin 2\alpha |\tan 2\theta_{0c}|},$$

decreases with $\sin 2\alpha$ for any fixed θ_{0c}. Consequently, $\sin 2\phi_{0c}$ in Eq. (D11c) and Q' in Eq. (D2) also reach their lowest values when $\sin 2\alpha$ is close to 1, hence

$$Q'_{0c} \geqslant Q'_{0c}|_{\sin 2\alpha = 1} = \cos 2\theta_{0c} + 1 + \frac{1}{\cos 2\theta_{0c}} \geqslant 3.$$

Since, as already observed, all conditional extrema of Q' occur at its Lagrange points, $Q'_{\min}(E')$ given indirectly by Eqs. (D12a) and (D12b) must be the desired conditional minimum, and Q'_{0c} must be the conditional maximum.

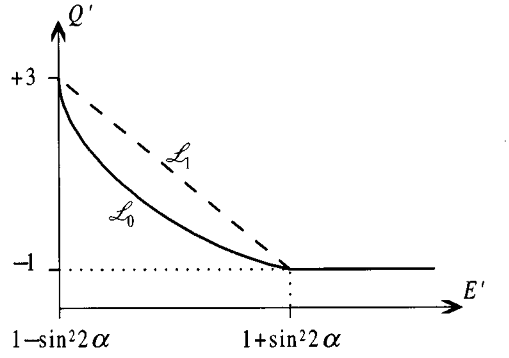

FIG. 7. Sketch illustrating relative position of conditional minimum curves $Q'(E')$ for $\lambda = \pi/2$ ($\mathcal{L}_1$, dashed), and for $\lambda = 0$ ($\mathcal{L}_0$, solid).

It now only remains to show that $Q'_{\min}(E')$, derived for the special case $\lambda = 0$, still yields the lowest possible value of Q' when λ is allowed to vary between 0 and $\pi/2$. First let $\lambda = \pi/2$ in Eq. (D1), which then becomes

$$E' = 1 - \sin 2\mu \sin^2 2\alpha, \quad Q' = 2 \sin 2\mu + 1. \qquad \text{(D13)}$$

With $0 \leqslant \mu < \pi$, relations (D13) parametrically define in the plane $\{E', Q'\}$ a straight line segment $\mathcal{L}_1$ whose end points lie on the curve $\mathcal{L}_0$, see Fig. 7. Apart from the end points, $\mathcal{L}_1$ lies everywhere above and to the right of $\mathcal{L}_0$, because, as confirmed by the sign of the second derivative

$$\frac{d^2 Q'_{0a}}{dE'^2_{0a}} = \frac{d}{d\gamma}\left[\frac{dQ'_{0a}}{dE'_{0a}}\right]\frac{1}{dE'_{0a}/d\gamma} = \frac{d}{d\gamma}\left[\frac{dQ'_{0a}/d\gamma}{dE'_{0a}/d\gamma}\right]\frac{1}{dE'_{0a}/d\gamma}$$

$$\propto \frac{d}{d\gamma}\left[\frac{\cos(\gamma+\delta) + \cos 2\gamma}{-\sin(\gamma+\delta) + \sin 2\gamma}\right]\frac{1}{dE'_{0a}/d\gamma}$$

$$= \frac{-1 - \cos(3\gamma + \delta)}{[-\sin(\gamma+\delta) + \sin 2\gamma]^2}\,\frac{1}{dE'_{0a}/d\gamma} > 0$$

$\mathcal{L}_0$ has positive curvature.

Finally, consider the general case expressions for E', Q', Eq. (D1) with some fixed μ, θ, ϕ, and with varying λ. With substitution from Eq. (12), E' and Q' have the form of bilinear fractions in $\cos^2 \lambda$:

$$E' = \frac{A_\lambda + B_\lambda \cos^2\lambda}{1 - C_\lambda \cos^2\lambda} = A'_\lambda + \frac{B'_\lambda}{1 - C_\lambda \cos^2\lambda},$$

$$Q' = \frac{G_\lambda + H_\lambda \cos^2\lambda}{1 - C_\lambda \cos^2\lambda} = G'_\lambda + \frac{H'_\lambda}{1 - C_\lambda \cos^2\lambda}, \qquad \text{(D14)}$$

where the indexed parameters are all independent of λ. It is evident that, with μ, θ, and ϕ held constant, there is a linear relationship between E' and Q'. Equation (D14) therefore defines a straight line segment $\mathcal{L}_{\mu\theta\phi}$ (in general, a different one for each combination of μ, θ, ϕ) in the plane $\{E', Q'\}$. One end point of the segment, corresponding to $\lambda = \pi/2$, necessarily lies on the line $\mathcal{L}_1$, by construction of $\mathcal{L}_1$. The other end point, corresponding to $\lambda = 0$, lies above and to the right of the curve $\mathcal{L}_0$, or, at most, on $\mathcal{L}_0$, by construction of

$\mathcal{L}_0$ as the conditional minimum curve $Q'_{\min}(E')$ for $\lambda=0$. Since $\mathcal{L}_0$ has been shown to have everywhere positive curvature, the entire line segment $\mathcal{L}_{\mu\theta\phi}$ must lie above and to the left of $\mathcal{L}_0$. The curve $\mathcal{L}_0$, derived from Eqs. (D11a) and (D11b), therefore represents the global conditional minimum $Q'_{\min}(E')$ over all values of λ. This completes the proof.

APPENDIX E: CONDITIONAL MINIMIZATION FOR BB84

Here we show that Eq. (16) represents the conditional minimum of the quantity Q subject to the constraint $E=\text{const}$, with Q and E given by Eq. (15), over all combinations $\{\lambda,\mu,\theta,\phi\}$. Fortunately, it is sufficient to minimize only the numerator of Q, for it will be seen that for any given E the numerator attains its conditional minimum at the same point where the denominator reaches its conditional maximum, i.e., $c=0$. The latter task is equivalent to minimizing b subject to $E=\text{const}$. Further simplification is obtained by inverting the problem, so that E is minimized subject to $b=\text{const}$ instead. The inversion is permissible because, as will be shown, the conditional minimum $E_{\min}(b)$ is a monotonically decreasing function of b in the domain of interest $0\leqslant E<\frac{1}{2}$.

This last problem can be solved by inspection without resorting to Lagrange multipliers. It is clear from

$$E=\tfrac{1}{2}-\tfrac{1}{4}(d+a)=\tfrac{1}{2}-\tfrac{1}{4}[\sin^2\lambda(1+\sin 2\mu)$$
$$+\cos^2\lambda\cos 2\theta(1+\sin 2\varphi)],$$

$$b=\sin^2\lambda\sin 2\mu+\cos^2\lambda\sin 2\phi$$

that one can freely let $\cos 2\theta=1$ to reduce E without affecting the constraint variable b. But $\cos 2\theta=1$ immediately leads to $E=\frac{1}{2}-\frac{1}{4}(1+b)=\frac{1}{4}(1-b)$, resolving the minimization problem. A realization $\{\lambda,\mu,\theta,\phi\}$ exists for every $0\leqslant$E $<\frac{1}{2}$, as Eq. (16) demonstrates.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[4] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[6] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[7] B. Slutsky, R. Rao, L. Tancevski, P. C. Sun, and Y. Fainman, Appl. Opt. (to be published).

[8] C. A. Fuchs, e-print quant-ph/9611010.

[9] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).

[10] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).

[11] Norbert Lütkenhaus, Phys. Rev. A **54**, 97 (1996).

[12] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997); e-print quant-ph/9611041.

[13] Christopher A. Fuchs and Asher Peres, Phys. Rev. A **53**, 2038 (1996).

[14] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu, and Asher Peres, Phys. Rev. A **56**, 1163 (1997); e-print quant-ph/9701039.

[15] Charles H. Bennett, Tal Mor, and John A. Smolin, Phys. Rev. A **54**, 2675 (1996).

[16] Eli Biham and Tal Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[17] Dominic Mayers, *Proceedings of the 16th Annual International Cryptology Conference, Santa Barbara, California, August 1996*, edited by Neal Roblitz (Springer, Berlin, 1996).

[18] B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainaman, J. Mod. Opt. **44**, 953 (1997).

[19] Horace P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).

[20] Asher Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Boston, 1993), p. 283.

[21] P. A. Benioff, J. Math. Phys. **13**, 908 (1972).

[22] L. B. Levitin, in *Quantum Communication and Measurement*, edited by V. P. Belavkin, O. Hirota, and R. Hudson (Plenum, New York, 1995), pp. 439–448.

[23] Asher Peres, Phys. Lett. A **128**, 19 (1988).