Aspects of entangled translucent eavesdropping in quantum cryptography

Howard E. Brandt
U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, Maryland 20783

John M. Myers
Gordon McKay Laboratory, Harvard University, Cambridge, Massachusetts 02138

Samuel J. Lomonaco, Jr.
Department of Computer Science, University of Maryland, Baltimore County, Maryland 21228
(Received 10 February 1997; revised manuscript received 30 June 1997)

We present a mathematical physics analysis of entangled translucent eavesdropping in quantum cryptography, based on the recent work of Ekert, Huttner, Palma, and Peres [Phys. Rev. A **50**, 1047 (1994)]. The key generation procedure involves the transmission, interception, and reception of two nonorthogonal photon polarization states. At the receiving end, a positive operator valued measure (POVM) is employed in the measurement process. The eavesdropping involves an information-maximizing von Neumann–type projective measurement. We propose a design for a receiver that is an all-optical realization of the POVM, using a Wollaston prism, a mirror, two beam splitters, a polarization rotator, and three photodetectors. We present a quantitative analysis of the receiver. We obtain closed-form algebraic expressions for the error rates and mutual information, expressed in terms of the POVM-receiver error rate and the angle between the carrier polarization states. We also prove a significant result, namely, that in the entangled translucent eavesdropping approach, the unsafe error rate based on standard mutual information comparisons is equivalent to the maximum allowable error rate based on perfect mutual information for the eavesdropper. In this case, the above unsafe error rate is in fact not overly conservative. [S1050-2947(97)01212-2]

PACS number(s): 03.65.Bz, 89.70.+c, 42.50.−p, 42.79.Sz

I. INTRODUCTION

For the purpose of secure key generation in quantum cryptography, one can employ a train of single photons having two possible equally likely nonorthogonal polarization states $|u\rangle$ and $|v\rangle$, which encode 0 and 1, respectively, to securely communicate a random bit sequence between a sender (Alice) and a receiver (Bob) in the presence of an eavesdropper (Eve). Recently, Ekert *et al.* [1] presented an analysis of an entangled translucent eavesdropping scenario of key generation in quantum cryptography. In the present work we carry their analysis further for an approach that uses two nonorthogonal photon polarization states. The eavesdropping is translucent in the sense that the eavesdropper Eve perturbs the polarization of the carrier on its way to Bob. The eavesdropper uses a probe that causes the carrier states to become entangled with the probe states. For detection, Eve makes an information-maximizing von Neumann–type projective measurement and Bob uses a positive operator valued measure (POVM). Bennett's two-state protocol [2] is employed, in which a positive response of Bob's POVM receiver, indicating the reception of a photon in a u-polarization or a v-polarization state, is publicly communicated to Eve without revealing which polarization was detected and the corresponding bits then constitute the preliminary key secretly shared by Alice and Bob. Bits corresponding to photons that do not excite the u- or v-polarization state detectors are excluded from the key. Because of the noncommutativity of nonorthogonal photon polarization-measurement operators representing nonorthogonal photon polarization states and also because arbitrary quantum states cannot be cloned [3,4], any attempt by Eve to eavesdrop can in principle be detected by Bob and Alice.

Entangled translucent eavesdropping is, of course, only one possible eavesdropping scenario. Ekert *et al.* [1] also examine so-called opaque eavesdropping and also translucent eavesdropping without entanglement. Lutkenhaus [5] recently provided a very extensive analysis (based on Shannon information and collision probability) of security against eavesdropping for a wide class of eavesdropping strategies in the case of the Bennett-Brassard two-basis protocol. For the two-state protocol, Fuchs and Peres [6] recently performed extensive quantum-information theoretic analyses for a general eavesdropping strategy in which Eve employs a POVM in order to extract as much information as possible. Clearly, a POVM receiver can be used by Eve as well as by Bob. Still other recent analyses of various eavesdropping scenarios are those of Gisin and co-workers [7,8] and Fuchs *et al.* [9]. The present work primarily limits itself to a few aspects of the entangled translucent eavesdropping scenario of Ref. [1].

We first present in Sec. II a design for the POVM receiver to be used by Bob. The design is totally optical. Because it is also interferometric, it demands precise phase alignment; however, it faithfully represents the perturbed statistics resulting from entangled translucent eavesdropping. Additional analysis pertaining to the device appears in Ref. [10]. Huttner *et al.* [11] recently presented a design and experimental proof of principle for an optical setup implementing a so-called loss-induced generalized quantum measurement. The device is also an interferometric implementation of a POVM. However, our design has fewer components and our theoret-

 © 1997 The American Physical Society

ical analysis of the statistics and cryptographic applications of our device is more extensive.

In Sec. III we obtain closed-form algebraic expressions for the error rate and mutual information in each communication channel as a function of the POVM receiver error rate Q and the angle θ between the carrier polarization states. All explicit dependence on unknown entanglement parameters of the eavesdropper's probe is removed.

In Sec. IV we obtain a significant result. We prove that for the entangled translucent eavesdropping scenario, the unsafe error rate based on standard mutual information comparisons is equivalent to the maximum allowable error rate based on perfect information for the eavesdropper and both are given by the square of the sine of half the complement of the angle between the two nonorthogonal photon polarization states of the carrier. The implication of this result is that the unsafe error rate is not in fact overly conservative for entangled translucent eavesdropping, as has been suggested by earlier work [1,12].

In Sec. V we summarize our results and conclusions. Included in Appendixes A–D are essential mathematical developments that logically support the results in the main text.

II. POVM RECEIVER

The positive operator valued measure [13–20], also known as the *probability* operator valued measure [14], is finding increasing use in quantum cryptography [13]. In the work of Ekert *et al.* [1] on entangled translucent eavesdropping, the following set of POVM operators represents the possible measurements performed by Bob's receiver:

$$A_u=(1+\langle u|v\rangle)^{-1}(1-|v\rangle\langle v|), \tag{1}$$

$$A_v=(1+\langle u|v\rangle)^{-1}(1-|u\rangle\langle u|), \tag{2}$$

$$A_?=1-A_u-A_v\,. \tag{3}$$

Here kets $|u\rangle$ and $|v\rangle$ represent the two possible nonorthogonal normalized polarization states of the carrier, with polarizations designated by u and v, respectively. The angle between the corresponding polarization vectors is θ, from which it follows (from the spin-1 behavior of the photon under the rotation group) that the overlap between the two states is

$$\langle u|v\rangle=\cos\theta. \tag{4}$$

The state $|u\rangle$ encodes bit value 0 and the state $|v\rangle$ encodes bit value 1. The POVM operators (1)–(3) are positive and their sum is unity. They are appropriate for realizing Bennett's two-state protocol because

$$\langle v|A_u|v\rangle=0 \tag{5}$$

and

$$\langle u|A_v|u\rangle=0. \tag{6}$$

Therefore, when an ideal detector representing the operator A_u responds positively, it follows that a photon with a v-polarization state cannot have been received. Likewise, when an ideal detector representing the operator A_v responds, a photon with a u-polarization state cannot have been received. The operator $A_?$ represents inconclusive responses of Bob's receiver. A u-polarized photon can result in a nonzero expectation value (and the associated response) only for the detectors representing A_u or $A_?$ operators. A v-polarized photon excites only the A_v or $A_?$ detectors. The advantage of the POVM over the von Neumann–type of projective measurement [2] is that for the POVM, the probability of getting an inconclusive result is lower [1].

For an arbitrary polarization state $|\psi\rangle$ of a photon, given by

$$|\psi\rangle=\alpha|u\rangle+\beta|v\rangle, \tag{7}$$

where α and β are arbitrary real constants, the expectation values of the POVM operators become

$$\langle\psi|A_u|\psi\rangle=\alpha^2(1-\cos\theta), \tag{8}$$

$$\langle\psi|A_v|\psi\rangle=\beta^2(1-\cos\theta), \tag{9}$$

$$\langle\psi|A_?|\psi\rangle=(\alpha+\beta)^2\,\cos\theta. \tag{10}$$

For the case of a transmitted state $|u\rangle$ in the two-state protocol, in the absence of perturbations, one has $(\alpha,\beta)=(1,0)$ in Eq. (7) and Eqs. (8)–(10) become

$$\langle u|A_u|u\rangle=(1-\cos\theta), \tag{11}$$

$$\langle u|A_v|u\rangle=0, \tag{12}$$

$$\langle u|A_?|u\rangle=\cos\theta, \tag{13}$$

consistent with Eq. (6). Alternatively, if $(\alpha,\beta)=(0,1)$, then

$$\langle v|A_u|v\rangle=0, \tag{14}$$

$$\langle v|A_v|v\rangle=(1-\cos\theta), \tag{15}$$

$$\langle v|A_?|v\rangle=\cos\theta, \tag{16}$$

consistent with Eq. (5). Either alternative is equally likely in the unperturbed two-state protocol. Although the POVM scheme in quantum cryptography is described mathematically in Ref. [1], no concrete physical model is provided. In the present work, we provide a possible physical realization for the POVM receiver (also, see Ref. [11]).

The circuit design for the POVM receiver that we propose here is shown in Fig. 1 [21–23]. It is an all-optical system. The straight lines with arrows represent possible optical pathways for a photon to move through the device. The path labeled $|\psi\rangle$ is the incoming path for a photon represented by the arbitrary polarization state given by Eq. (7). Also in Fig. 1, D_u, D_v, and $D_?$ designate photodetectors representing the measurement operators A_u, A_v, and $A_?$, respectively. Shown also is a Wollaston prism W, which is aligned so that an incident photon with polarization vector $\hat{\mathbf{e}}_{u+v}$ would take the path labeled by the state $|\psi_1\rangle$ and $\hat{\mathbf{e}}_{u+v}$ and not the path labeled by polarization vector $\hat{\mathbf{e}}_{u-v}$ and $|\psi_2\rangle$. Here $\hat{\mathbf{e}}_{u+v}$ denotes a unit polarization vector corresponding to polarization state $|u+v\rangle=|u\rangle+|v\rangle$ and is perpendicular to the unit

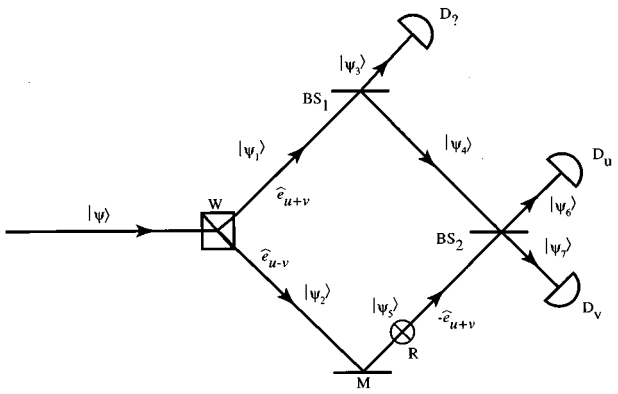

FIG. 1. POVM receiver.

polarization vector $\hat{\mathbf{e}}_{u-v}$ corresponding to the polarization state $|u-v\rangle=|u\rangle-|v\rangle$. The states $|u+v\rangle$ and $|u-v\rangle$ are orthogonal and one has

$$\langle u+v|u-v\rangle=0, \quad \hat{\mathbf{e}}_{u+v}\cdot\hat{\mathbf{e}}_{u-v}=0. \tag{17}$$

The device also has two beam splitters designated by BS_1 and BS_2 in Fig. 1. Beam splitter BS_2 is taken to be a 50-50 beam splitter for a photon entering either of its entrance ports. Both paths from the Wollaston prism to the beam splitter BS_2 have equal optical path lengths. The device is clearly interferometric. Also shown in Fig. 1 is a 90° polarization rotator designated by R, which transforms a photon with polarization vector $\hat{\mathbf{e}}_{u-v}$ into one with polarization vector $-\hat{\mathbf{e}}_{u+v}$. Also shown in Fig. 1 is a single mirror M.

In Appendix A we obtain expressions for the photon states $|\psi_i\rangle$ corresponding to each of the paths designated by $|\psi_i\rangle$, $i=1,2,...,7$ in Fig. 1. The states are

$$|\psi_1\rangle=2^{-1/2}(\alpha+\beta)(1+\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle, \tag{18}$$

$$|\psi_2\rangle=2^{-1/2}(\alpha-\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u-v}\rangle, \tag{19}$$

$$|\psi_3\rangle=(\alpha+\beta)(\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle, \tag{20}$$

$$|\psi_4\rangle=i2^{-1/2}(\alpha+\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle, \tag{21}$$

$$|\psi_5\rangle=-2^{-1/2}(\alpha-\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle, \tag{22}$$

$$|\psi_6\rangle=-\alpha(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle, \tag{23}$$

$$|\psi_7\rangle=i\beta(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle. \tag{24}$$

Here $|\hat{\mathbf{e}}_{u\pm v}\rangle$ represent unit kets corresponding to photon polarization vectors $\hat{\mathbf{e}}_{u\pm v}$. From Eq. (23) it follows that

$$\langle\psi_6|\psi_6\rangle=\alpha^2(1-\cos\theta), \tag{25}$$

and comparing Eq. (25) with Eq. (8), one sees that

$$\langle\psi_6|\psi_6\rangle=\langle\psi|A_u|\psi\rangle, \tag{26}$$

consistent with Fig. 1 and the requirements for the POVM. Also from Eq. (24) it follows that

$$\langle\psi_7|\psi_7\rangle=\beta^2(1-\cos\theta), \tag{27}$$

and comparing Eq. (27) with Eq. (9), one sees that

$$\langle\psi_7|\psi_7\rangle=\langle\psi|A_v|\psi\rangle, \tag{28}$$

again consistent with Fig. 1. Also, from Eq. (20) it follows that

$$\langle\psi_3|\psi_3\rangle=(\alpha+\beta)^2\cos\theta, \tag{29}$$

and comparing Eq. (29) with Eq. (10), it follows that

$$\langle\psi_3|\psi_3\rangle=\langle\psi|A_?|\psi\rangle, \tag{30}$$

again consistent with Fig. 1. Furthermore, using Eqs. (29), (25), (27), (4), and (7), one concludes that

$$\langle\psi_3|\psi_3\rangle+\langle\psi_6|\psi_6\rangle+\langle\psi_7|\psi_7\rangle=\langle\psi|\psi\rangle \tag{31}$$

or, equivalently,

$$|\psi_3|^2+|\psi_6|^2+|\psi_7|^2=|\psi|^2, \tag{32}$$

as required to conserve probability. Equations (26), (28), (30), and (32) are just the probabilistic properties one would expect of a POVM acting as a *probability* operator valued measure.

One concludes that the POVM receiver of Fig. 1 satisfies the appropriate statistics. Also, both beam-splitter transmission coefficients (A11) and (A18) have the desirable feature that they do not depend on the coefficients α and β associated with an arbitrary incoming polarization state and therefore the device can also faithfully represent the perturbed statistics arising from entangled translucent eavesdropping. The statistics corresponding to the entangled translucent eavesdropping scenario are examined in considerable detail in the following section.

III. ERROR RATES AND MUTUAL INFORMATION

In the entangled translucent eavesdropping scenario of Ref. [1], the two excited states $|e_u\rangle$ and $|e_v\rangle$ of the eavesdropper's probe are entangled with the carrier polarization states $|u\rangle$ and $|v\rangle$. Letting $|\phi_1\rangle$ and $|\phi_2\rangle$ denote the two possible initial tensor-product states of the carrier with the ground state $|e\rangle$ of the probe, one has

$$|\phi_1\rangle=|u\rangle\otimes|e\rangle \tag{33}$$

and

$$|\phi_2\rangle=|v\rangle\otimes|e\rangle. \tag{34}$$

The effect of the entangled translucent eavesdropping is to convert $|\phi_1\rangle$ or $|\phi_2\rangle$ to $|\phi_1'\rangle$ or $|\phi_2'\rangle$, respectively, where

$$|\phi_1'\rangle=a|u\rangle\otimes|e_u\rangle+b|v\rangle\otimes|e_v\rangle \tag{35}$$

and

$$|\phi_2'\rangle=b|u\rangle\otimes|e_u\rangle+a|v\rangle\otimes|e_v\rangle, \tag{36}$$

where a and b are real constants [1].

Without loss of generality, orthogonal basis states $|x\rangle$ and $|y\rangle$, defined by

$$|x\rangle=\begin{bmatrix}0\\1\end{bmatrix}, \quad |y\rangle=\begin{bmatrix}1\\0\end{bmatrix}, \quad \langle x|y\rangle=0, \tag{37}$$

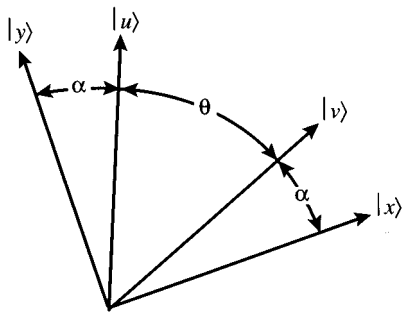

FIG. 2. Two-dimensional Hilbert space of carrier states.

are chosen to be arranged symmetrically about the two carrier states $|u\rangle$ and $|v\rangle$ in the plane of the two-dimensional Hilbert space defined by the carrier states, as shown in Fig. 2. For convenience here and in the following, our notation does not explicitly distinguish between a ket and its representative [24]. The angle between $|u\rangle$ and $|y\rangle$ is equal to the angle between $|v\rangle$ and $|x\rangle$; both angles are denoted by α, half the complement of the angle θ between the two polarization states $|u\rangle$ and $|v\rangle$. One has therefore

$$|u\rangle=\begin{bmatrix}\cos\alpha\\ \sin\alpha\end{bmatrix}, \tag{38}$$

$$|v\rangle=\begin{bmatrix}\sin\alpha\\ \cos\alpha\end{bmatrix}. \tag{39}$$

One notes that Eqs. (38) and (39) are consistent with Eq. (4), which can also be written in terms of the angle α:

$$\langle u|v\rangle=\sin(2\alpha). \tag{40}$$

The probe states $|e_u\rangle$ and $|e_v\rangle$ are chosen to be oriented symmetrically relative to the photon polarization states and the orthogonal basis [1]. The angle between the state $|e_u\rangle$ and the basis state $|y\rangle$ is equal to the angle between $|e_v\rangle$ and $|x\rangle$; these angles are denoted by γ, as depicted in Fig. 3. Hence one has

$$|e_u\rangle=\begin{bmatrix}\cos\gamma\\ \sin\gamma\end{bmatrix}, \tag{41}$$

$$|e_v\rangle=\begin{bmatrix}\sin\gamma\\ \cos\gamma\end{bmatrix}. \tag{42}$$

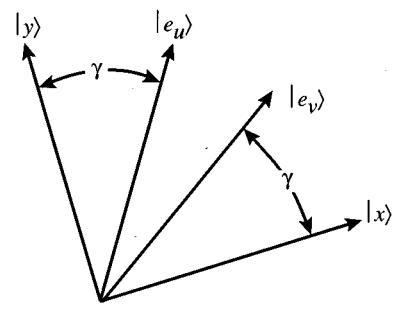

FIG. 3. Two-dimensional Hilbert space of probe states.

The following normalizations are assumed:

$$\langle\phi_1|\phi_1\rangle=\langle\phi_2|\phi_2\rangle=\langle\phi_1'|\phi_1'\rangle=\langle\phi_2'|\phi_2'\rangle=1 \tag{43}$$

and

$$\langle u|u\rangle=\langle v|v\rangle=\langle e_u|e_u\rangle=\langle e_v|e_v\rangle=1. \tag{44}$$

Since the effect of the eavesdropper's ideal probe can be represented by a unitary transformation (if environmental interactions are ignored), unitarity requires that

$$(\langle\phi_1|+\langle\phi_2|)(|\phi_1\rangle+|\phi_2\rangle)=(\langle\phi_1'|+\langle\phi_2'|)(|\phi_1'\rangle+|\phi_2'\rangle). \tag{45}$$

Using Eq. (43), we transform Eq. (45) to

$$\mathrm{Re}\langle\phi_1|\phi_2\rangle=\mathrm{Re}\langle\phi_1'|\phi_2'\rangle. \tag{46}$$

Therefore, substituting Eqs. (33)–(36) and (44) into Eq. (46) and using Eqs. (40)–(42), one concludes that

$$\sin(2\alpha)=2ab+(a^2+b^2)\sin(2\alpha)\sin(2\gamma). \tag{47}$$

Also, substituting Eq. (35) into the third equality of Eq. (43) and using Eqs. (38)–(42) and (44), one obtains

$$1=a^2+b^2+2ab\ \sin(2\alpha)\sin(2\gamma). \tag{48}$$

Thus unitarity places the constraints given by Eqs. (47) and (48) on the values of the entanglement parameters a, b, and γ of the eavesdropper's probe, for the carrier states specified by the angle α. We refer in the following to Eqs. (47) and (48) as the unitarity relations involving the eavesdropping parameters.

To measure the carrier states entangled with her probe states, Eve performs an information-maximizing von Neumann–type measurement represented by projection operators $|y\rangle\langle y|$ and $|x\rangle\langle x|$, which test for eigenvectors $|y\rangle$ and $|x\rangle$, respectively [1,14,25]. In the following, it is convenient to reuse the symbols α and β as index variables for Alice's transmission and Bob's reception (the context distinguishes the usage). With an additional index ε for Eve, we write $|\varepsilon\alpha\rangle$ as the perturbed state that Eve relays to Bob after measuring ε, when Alice transmits α. The ranges of these indices are

$$\alpha,\varepsilon\in\{0,1\};\quad \beta\in\{0,1,?\}. \tag{49}$$

In Appendix B we obtain expressions for the probability amplitude $|\varepsilon\alpha\rangle$ that Eve measures an ε when Alice sends an α, namely,

$$|00\rangle=a\ \cos\gamma|u\rangle+b\ \sin\gamma|v\rangle, \tag{50}$$

$$|10\rangle=a\ \sin\gamma|u\rangle+b\ \cos\gamma|v\rangle, \tag{51}$$

$$|01\rangle=b\ \cos\gamma|u\rangle+a\ \sin\gamma|v\rangle, \tag{52}$$

$$|11\rangle=b\ \sin\gamma|u\rangle+a\ \cos\gamma|v\rangle. \tag{53}$$

They are all of the general form given by Eq. (7), with coefficients expressed for each case in terms of the eavesdropping parameters a, b, and γ.

The probability that Eve detects an ε and Bob detects a β when Alice sends an α can be transcribed into the convenient notation [26]

$$p(\alpha,\varepsilon,\beta)\equiv\begin{pmatrix} B & E & | & A \\ \beta & \varepsilon & | & \alpha \end{pmatrix}. \tag{54}$$

By the rules of conditional probability, one has

$$\begin{pmatrix} B & E & | & A \\ \beta & \varepsilon & | & \alpha \end{pmatrix}=\begin{pmatrix} E & | & A \\ \varepsilon & | & \alpha \end{pmatrix}\begin{pmatrix} B & | & E & A \\ \beta & | & \varepsilon & \alpha \end{pmatrix}, \tag{55}$$

where $\left(\begin{smallmatrix} E & | & A \\ \varepsilon & | & \alpha \end{smallmatrix}\right)$ denotes the probability that Eve detects an ε when Alice sends an α and $\left(\begin{smallmatrix} B & | & E & A \\ \beta & | & \varepsilon & \alpha \end{smallmatrix}\right)$ denotes the conditional probability that Bob detects a β, given that Eve detects an ε when Alice sends an α. For the positive operator valued measure (or *probability* operator valued measure) it is true that

$$\begin{pmatrix} B & | & E & A \\ \beta & | & \varepsilon & \alpha \end{pmatrix}=\frac{\langle\varepsilon\alpha|A_\beta|\varepsilon\alpha\rangle}{\langle\varepsilon\alpha|\varepsilon\alpha\rangle}, \tag{56}$$

where

$$\{A_\beta\}\equiv\{A_0,A_1,A_?\}\equiv\{A_u,A_v,A_?\}. \tag{57}$$

Also it is clear that

$$\begin{pmatrix} E & | & A \\ \varepsilon & | & \alpha \end{pmatrix}=\langle\varepsilon\alpha|\varepsilon\alpha\rangle, \tag{58}$$

expressed in terms of the relayed states (50)–(53), relayed by Eve to Bob. Substituting Eqs. (56) and (58) into Eq. (55) and using Eq. (54), one obtains

$$p(\alpha,\varepsilon,\beta)=\begin{pmatrix} B & E & | & A \\ \beta & \varepsilon & | & \alpha \end{pmatrix}=\langle\varepsilon\alpha|A_\beta|\varepsilon\alpha\rangle. \tag{59}$$

Thus, for example, the probability $p(0,0,0)$ that Eve detects a 0 and Bob detects a 0 when Alice sends a 0 is given by

$$p(0,0,0)=\langle 00|A_0|00\rangle. \tag{60}$$

Then substituting Eqs. (50), (57), and (1) into Eq. (60) and using Eqs. (38)–(40), we obtain

$$p(0,0,0)=a^2[1-\sin(2\alpha)]\cos^2\alpha. \tag{61}$$

Analogously, using Eq. (59), we obtain

$$p(0,0,1)=b^2[1-\sin(2\alpha)]\sin^2\gamma, \tag{62}$$

$$p(0,0,?)=\sin(2\alpha)(a\ \cos\gamma+b\ \sin\gamma)^2, \tag{63}$$

$$p(0,1,0)=a^2[1-\sin(2\alpha)]\sin^2\gamma, \tag{64}$$

$$p(0,1,1)=b^2[1-\sin(2\alpha)]\cos^2\gamma, \tag{65}$$

$$p(0,1,?)=\sin(2\alpha)(a\ \sin\gamma+b\ \cos\gamma)^2, \tag{66}$$

$$p(1,0,0)=b^2[1-\sin(2\alpha)]\cos^2\gamma, \tag{67}$$

$$p(1,0,1)=a^2[1-\sin(2\alpha)]\sin^2\gamma, \tag{68}$$

$$p(1,0,?)=\sin(2\alpha)(b\ \cos\gamma+a\ \sin\gamma)^2, \tag{69}$$

$$p(1,1,0)=b^2[1-\sin(2\alpha)]\sin^2\gamma, \tag{70}$$

$$p(1,1,1)=a^2[1-\sin(2\alpha)]\cos^2\gamma, \tag{71}$$

$$p(1,1,?)=\sin(2\alpha)(b\ \sin\gamma+a\ \cos\gamma)^2. \tag{72}$$

The arguments used here in obtaining Eqs. (61)–(72) differ from those of Ref. [1]; however, the results are in complete agreement.

In Appendix C we obtain explicit expressions for the error rates Q_{AE} and Q_{BE} in the Alice-Eve and Bob-Eve channels, respectively, expressed in terms of the error rate in the Alice-Bob channel and the eavesdropping parameter γ. These expressions are in agreement with Ref. [1]; however, two errors in supporting equations in Ref. [1] are corrected in Appendix C.

It is desirable to express all channel error rates explicitly in terms of (i) the error rate Q in the Alice-Bob channel and (ii) the angle θ between the two nonorthogonal photon polarization states, or in terms of the angle α, which is half the complement of θ (see Fig. 2). Clearly,

$$\alpha=\frac{1}{2}\left(\frac{\pi}{2}-\theta\right). \tag{73}$$

In Appendix D we obtain the following explicit expressions for the error rate $Q_{AE}(Q,\theta)$ in the Alice-Eve channel and the error rate $Q_{BE}(Q,\theta)$ in the Bob-Eve channel, respectively [21,27,28]:

$$Q_{AE}(Q,\theta)=\tfrac{1}{2}-(\tfrac{1}{2}-Q)[1-F(Q,\theta)^2]^{1/2} \tag{74}$$

and

$$Q_{BE}(Q,\theta)=\tfrac{1}{2}-\tfrac{1}{2}[1-F(Q,\theta)^2]^{1/2}, \tag{75}$$

where

$$F(Q,\theta)=\frac{2[Q(1-Q)]^{1/2}\sec\theta-1}{2[Q(1-Q)]^{1/2}\cos\theta-1}. \tag{76}$$

Equations (74)–(76) parametrize the error rates in the Alice-Eve and Bob-Eve channels, respectively, in terms of the angle θ between the two nonorthogonal photon polarization states of the carrier and the error rate Q in the Alice-Bob channel.

Because the inconclusive results are removed, the Alice-Bob channel, although operationally a binary erasure channel, becomes effectively a binary symmetric channel; thus the maximal mutual information (channel capacity) I_{AB} in the Alice-Bob channel is given by the well-known expression for a binary symmetric channel, namely [1,29,30],

$$I_{AB}(Q)=1+Q\ \log_2 Q+(1-Q)\log_2(1-Q), \tag{77}$$

expressed in terms of the error rate Q in the Alice-Bob channel. Since the Bob-Eve and Alice-Eve channels are also effectively binary symmetric, one also has for the mutual information in the Bob-Eve channel

$$I_{BE}(Q_{BE}) = 1 + Q_{BE}\log_2 Q_{BE} + (1 - Q_{BE})\log_2(1 - Q_{BE}) \tag{78}$$

and for the mutual information in the Alice-Eve channel

$$I_{AE}(Q_{AE}) = 1 + Q_{AE}\log_2 Q_{AE} + (1 - Q_{AE})\log_2(1 - Q_{AE}), \tag{79}$$

where Q_{BE} and Q_{AE} are given by Eqs. (75) and (74), respectively [21,27,28]. Thus the mutual information in each channel is also expressed explicitly in terms of the angle θ between the two nonorthogonal photon polarization states and the error rate in the Alice-Bob channel, with no explicit dependence on the generally unknown eavesdropping parameters.

IV. UNSAFE ERROR RATE

The error rate in the Alice-Bob channel, resulting from eavesdropping, is considered to be unsafe if the mutual information in the Alice-Bob channel does not exceed the minimum of the mutual information in the Alice-Eve channel and of that in the Bob-Eve channel [1]. Equivalently, this unsafe transmission criterion may be expressed as

$$I_{AB} \leqslant \min(I_{AE}, I_{BE}). \tag{80}$$

It is suggested in Ref. [1] that this condition may be overly cautious; however, we proceed to show that this is not the case for the entangled translucent eavesdropping scenario.

We define the unsafe error rate Q_u to be the smallest error rate Q in the Alice-Bob channel such that the equality in Eq. (80) is satisfied, namely,

$$Q_u = \text{smallest } Q \text{ such that}$$

$$I_{AB}(Q) = \min[I_{AE}(Q_{AE}(Q,\theta)), I_{BE}(Q_{BE}(Q,\theta))]. \tag{81}$$

First note that by substituting $Q = \sin^2\alpha$ into Eq. (74) and using Eqs. (76) and (73), one obtains

$$Q_{AE}(\sin^2\alpha, \theta) = \sin^2\alpha. \tag{82}$$

Next, substituting Eq. (82) into Eq. (79), one obtains

$$I_{AE}(Q_{AE}(\sin^2\alpha,\theta)) = 1 + \sin^2\alpha\ \log_2(\sin^2\alpha) + \cos^2\alpha\ \log_2(\cos^2\alpha). \tag{83}$$

However, from Eq. (77) it follows immediately that

$$I_{AB}(\sin^2\alpha) = 1 + \sin^2\alpha\ \log_2(\sin^2\alpha) + \cos^2\alpha\ \log_2(\cos^2\alpha). \tag{84}$$

Comparing Eq. (83) with Eq. (84), one can conclude that

$$I_{AE}(Q_{AE}(\sin^2\alpha,\theta)) = I_{AB}(\sin^2\alpha). \tag{85}$$

We next note, using Eqs. (75), (76), and (73), that

$$Q_{BE}(\sin^2\alpha, \theta) = 0 \tag{86}$$

and therefore, substituting Eq. (86) into Eq. (78), we obtain

$$I_{BE}(Q_{BE}(\sin^2\alpha,\theta)) = 1. \tag{87}$$

Using Eq. (87), we next observe that since $I_{AE} \leqslant 1$, one has

$$\min[I_{AE}(Q_{AE}(\sin^2\alpha,\theta)), I_{BE}(Q_{BE}(\sin^2\alpha,\theta))] = I_{AE}(Q_{AE}(\sin^2\alpha,\theta)). \tag{88}$$

Next, substituting Eq. (85) into Eq. (88), one has

$$\min[I_{AE}(Q_{AE}(\sin^2\alpha,\theta)), I_{BE}(Q_{BE}(\sin^2\alpha,\theta))] = I_{AB}(\sin^2\alpha). \tag{89}$$

Therefore, comparing Eq. (89) with Eq. (81), one can conclude that [21,27,28]

$$Q_u = \sin^2\alpha. \tag{90}$$

The maximum allowable error rate $Q_{\max}$ is the value of the error rate in the Alice-Bob channel, for which the mutual information in the Bob-Eve channel is unity, namely [1],

$$Q_{\max} = Q \text{ such that } I_{BE}(Q_{BE}(Q,\theta)) = 1. \tag{91}$$

This corresponds to perfect mutual information for the eavesdropper. Comparing Eq. (91) with Eq. (87), one observes that

$$Q_{\max} = \sin^2\alpha, \tag{92}$$

in accord with Ref. [1].

Finally, comparing Eq. (90) with Eq. (92), we obtain the result

$$Q_u = Q_{\max}. \tag{93}$$

Thus, for entangled translucent eavesdropping, the unsafe error rate is in fact equal to the maximum allowable error rate.

Using Eq. (73), one can also express Eqs. (90), (92), and (93) in terms of the angle θ between the two nonorthogonal photon polarization states, namely [21,27,28],

$$Q_u = Q_{\max} = \tfrac{1}{2}(1 - \sin\theta). \tag{94}$$

In this case, the unsafe error rate is not in fact overly conservative.

V. CONCLUSION

In this work, we have presented a design for a receiver that is an all-optical realization of a POVM for use in quantum cryptography. The device, depicted in Fig. 1, interferometrically implements the statistics of all three POVM operators. Also, we have obtained closed-form algebraic expressions for the error rate and mutual information in each channel, expressed in terms of the error rate in the Alice-Bob channel and the angle between the two nonorthogonal photon polarization states of the carrier. The expressions are given by Eqs. (74)–(76), (78), and (79). We also demonstrated that, in the presence of entangled translucent eavesdropping, the unsafe error rate based on standard mutual information comparisons is equivalent to the maximum allowable error rate based on perfect information for the eavesdropper.

ACKNOWLEDGMENT

This work was supported by the U.S. Army Research Laboratory.

APPENDIX A: POVM RECEIVER STATES

It follows from the geometry of Fig. 1 and the projective property of polarized photon states [Eq. (4)] that the state of a photon taking the path designated by the state $|\psi_1\rangle$ is given by

$$|\psi_1\rangle=(\alpha\langle u|+\beta\langle v|)\left(\frac{|u\rangle+|v\rangle}{||u+v\rangle|}\right)|\hat{\mathbf{e}}_{u+v}\rangle, \tag{A1}$$

where $|\hat{\mathbf{e}}_{u+v}\rangle$ represents a unit ket corresponding to polarization vector $\hat{\mathbf{e}}_{u+v}$. Also in Eq. (A1), the Dirac bracket, appearing as an overall factor of the unit ket, is the probability amplitude that a photon takes the path under consideration. Analogously, one has

$$|\psi_2\rangle=(\alpha\langle u|+\beta\langle v|)\left(\frac{|u\rangle-|v\rangle}{||u-v\rangle|}\right)|\hat{\mathbf{e}}_{u-v}\rangle, \tag{A2}$$

where $|\hat{\mathbf{e}}_{u-v}\rangle$ represents a unit ket corresponding to polarization vector $\hat{\mathbf{e}}_{u-v}$. Expanding Eqs. (A1) and (A2), using Eq. (4), we obtain

$$|\psi_1\rangle=2^{-1/2}(\alpha+\beta)(1+\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle \tag{A3}$$

and

$$|\psi_2\rangle=2^{-1/2}(\alpha-\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u-v}\rangle. \tag{A4}$$

The detectors D_u, D_v, and $D_?$ are treated here as ideal. We require

$$\langle\psi_6|\psi_6\rangle=\langle\psi|A_u|\psi\rangle, \tag{A5}$$

in order that the expectation value of A_u, measured by the detector D_u in Fig. 1, equal the probability $\langle\psi_6|\psi_6\rangle$ that a photon is incident on it. This makes the POVM effectively a *probability* operator valued measure. Analogously, we require

$$\langle\psi_7|\psi_7\rangle=\langle\psi|A_v|\psi\rangle \tag{A6}$$

for the detector D_v and

$$\langle\psi_3|\psi_3\rangle=\langle\psi|A_?|\psi\rangle \tag{A7}$$

for the detector $D_?$. Substituting Eq. (10) into Eq. (A7), we obtain

$$\langle\psi_3|\psi_3\rangle=(\alpha+\beta)^2\cos\theta \tag{A8}$$

and therefore

$$|\psi_3\rangle=(\alpha+\beta)(\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle. \tag{A9}$$

It can be shown, using the methods of Ref. [10], that one can effectively ignore the unused vacuum port of beam splitter BS_1, in complete agreement with physical intuition. From Fig. 1 one sees that in order for the state $|\psi_3\rangle$ of a photon to result from a photon in state $|\psi_1\rangle$ hitting the beam splitter BS_1, the transmission coefficient T_1 of beam splitter BS_1 must be given by

$$T_1=\frac{\langle\psi_3|\psi_3\rangle}{\langle\psi_1|\psi_1\rangle}, \tag{A10}$$

and therefore substituting Eqs. (A8) and (A3) in Eq. (A10), one obtains

$$T_1=1-\tan^2(\theta/2), \tag{A11}$$

independent of α and β. The corresponding reflection coefficient becomes

$$R_1=\tan^2(\theta/2), \tag{A12}$$

and from Fig. 1 one sees that

$$\langle\psi_4|\psi_4\rangle=R_1\langle\psi_1|\psi_1\rangle. \tag{A13}$$

Substituting Eqs. (A12) and (A3) in Eq. (A13), one obtains

$$\langle\psi_4|\psi_4\rangle=\tfrac{1}{2}(\alpha+\beta)^2(1-\cos\theta). \tag{A14}$$

Next, taking account of the reflection at BS_1 that introduces a factor of i, it therefore follows that

$$|\psi_4\rangle=i2^{-1/2}(\alpha+\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle. \tag{A15}$$

Also one sees from the geometry of Fig. 1, together with Eq. (A4), that, because of the polarization rotator R, which effectively converts polarization in the direction $\hat{\mathbf{e}}_{u-v}$ into that in the direction $-\hat{\mathbf{e}}_{u+v}$, one has

$$|\psi_5\rangle=-2^{-1/2}(\alpha-\beta)(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle. \tag{A16}$$

Next, from Fig. 1, one sees that because of beam splitter BS_2, states $|\psi_4\rangle$ and $|\psi_5\rangle$ combine and interfere to produce states $|\psi_6\rangle$ and $|\psi_7\rangle$. In particular, because a 50-50 beam splitter is assumed here for BS_2 with reflection coefficient

$$R_2=\tfrac{1}{2} \tag{A17}$$

and transmission coefficient

$$T_2=\tfrac{1}{2} \tag{A18}$$

for both entrance paths, one has

$$|\psi_6\rangle=2^{-1/2}|\psi_5\rangle+i2^{-1/2}|\psi_4\rangle \tag{A19}$$

and

$$|\psi_7\rangle=2^{-1/2}|\psi_4\rangle+i2^{-1/2}|\psi_5\rangle. \tag{A20}$$

The implementation of the interferometric equations (A19) and (A20) demands precise phase alignment in the interferometric circuit of Fig. 1. Next, substituting Eqs. (A15) and (A16) into Eqs. (A19) and (A20), one obtains

$$|\psi_6\rangle=-\alpha(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle \tag{A21}$$

and

$$|\psi_7\rangle=i\beta(1-\cos\theta)^{1/2}|\hat{\mathbf{e}}_{u+v}\rangle. \tag{A22}$$

APPENDIX B: RELAYED STATES OF THE CARRIER

The effect of Eve's measurement process on the initial carrier and probe states can be represented by the tensor-product projection operators

$$P_0 = I \otimes (|y\rangle\langle y|) = I \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} [1 \quad 0] = I \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad \text{(B1)}$$

and

$$P_1 = I \otimes (|x\rangle\langle x|) = I \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} [0 \quad 1] = I \otimes \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}. \quad \text{(B2)}$$

Here we have used Eq. (37) and I is the unit operator in the carrier space.

The probability amplitude $|00\rangle$ that Eve measures a 0 with her information-maximizing measurement when Alice sends a 0 may be determined from the projection

$$P_0 |\phi_1'\rangle = |00\rangle \otimes |y\rangle. \quad \text{(B3)}$$

Proceeding to evaluate the left-hand side of Eq. (B3), using Eqs. (B1), (35), (41), and (42), one obtains

$$P_0 |\phi_1'\rangle = I \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \left(a|u\rangle \otimes \begin{bmatrix} \cos\gamma \\ \sin\gamma \end{bmatrix} + b|v\rangle \otimes \begin{bmatrix} \sin\gamma \\ \cos\gamma \end{bmatrix} \right). \quad \text{(B4)}$$

Equation (B4) reduces to

$$P_0 |\phi_1'\rangle = (a \cos\gamma |u\rangle + b \sin\gamma |v\rangle) \otimes |y\rangle \quad \text{(B5)}$$

and therefore, comparing Eq. (B5) with Eq. (B3), one obtains

$$|00\rangle = a \cos\gamma |u\rangle + b \sin\gamma |v\rangle. \quad \text{(B6)}$$

Similarly, the probability amplitude $|10\rangle$ that Eve measures a 1 when Alice sends a 0 is determined by

$$P_1 |\phi_1'\rangle = |10\rangle \otimes |x\rangle, \quad \text{(B7)}$$

from which it follows that

$$|10\rangle = a \sin\gamma |u\rangle + b \cos\gamma |v\rangle. \quad \text{(B8)}$$

Also, the probability amplitude $|01\rangle$ that Eve measures a 0 when Alice sends a 1 is determined by

$$P_0 |\phi_2'\rangle = |01\rangle \otimes |y\rangle, \quad \text{(B9)}$$

which yields

$$|01\rangle = b \cos\gamma |u\rangle + a \sin\gamma |v\rangle. \quad \text{(B10)}$$

Finally, the probability amplitude $|11\rangle$ that Eve measures a 1 when Alice sends a 1 is determined by

$$P_1 |\phi_2'\rangle = |11\rangle \otimes |x\rangle \quad \text{(B11)}$$

and therefore

$$|11\rangle = b \sin\gamma |u\rangle + a \cos\gamma |v\rangle. \quad \text{(B12)}$$

Equations (B6), (B8), (B10), and (B12) are the four possible perturbed states resulting from the perturbation by Eve of states on their way from Alice to Bob.

APPENDIX C: ERROR RATES

If we denote by r, w, and i, respectively, the number of generic measurement results that are right, wrong, and inconclusive, then the error rate q before inconclusive results are discarded is clearly given by

$$q = \frac{w}{w + r + i}. \quad \text{(C1)}$$

Also, the error rate Q after inconclusive results are discarded is

$$Q = \frac{w}{w + r} \quad \text{(C2)}$$

and the rate R of inconclusive results is

$$R = \frac{i}{w + r + i}. \quad \text{(C3)}$$

Using Eqs. (C1)–(C3), we find that

$$Q = \frac{q}{1 - R}, \quad \text{(C4)}$$

as in Ref. [1].

Bob's error rate q, before inconclusive results are discarded, is

$$q = \sum_{\varepsilon=0,1} p(0,\varepsilon,1) = \sum_{\varepsilon=0,1} p(1,\varepsilon,0). \quad \text{(C5)}$$

Substituting Eqs. (62) and (65) into Eq. (C5), one obtains

$$q = b^2 [1 - \sin(2\alpha)]. \quad \text{(C6)}$$

Bob's rate R of inconclusive results is

$$R = \sum_{\varepsilon=0,1} p(0,\varepsilon,?) = \sum_{\varepsilon=0,1} p(1,\varepsilon,?), \quad \text{(C7)}$$

which with Eqs. (63) and (66) becomes

$$R = [a^2 + b^2 + 2ab \sin(2\gamma)] \sin(2\alpha). \quad \text{(C8)}$$

Therefore, substituting Eqs. (C6) and (C8) into Eq. (C4) and using the unitarity relation (48), one obtains the error rate Q in the Alice-Bob channel

$$Q = \frac{b^2}{a^2 + b^2}. \quad \text{(C9)}$$

Equations (C6), (C8), and (C9) all agree with Ref. [1].

The error rate Q_{AE} in the Alice-Eve channel, after inconclusive results are discarded, is given by

$$Q_{AE}=\frac{\sum_{\beta=0,1} p(0,1,\beta)}{\sum_{\beta=0,1}[p(0,1,\beta)+p(0,0,\beta)]}. \quad \text{(C10)}$$

Equivalently, Eq. (C10) can be written as

$$Q_{AE}=\frac{\sum_{\beta=0,1} p(0,1,\beta)}{1-\sum_{\varepsilon=0,1} p(0,\varepsilon,?)}. \quad \text{(C11)}$$

We give the numerator in Eq. (C11) the name q_{AE}:

$$q_{AE}=\sum_{\beta=0,1} p(0,1,\beta). \quad \text{(C12)}$$

Then substituting Eqs. (C12) and (C7) into Eq. (C11), one has

$$Q_{AE}=\frac{q_{AE}}{1-R}. \quad \text{(C13)}$$

Next, substituting Eqs. (64) and (65) into Eq. (C12), one obtains

$$q_{AE}=(a^2\sin^2\gamma+b^2\cos^2\gamma)[1-\sin(2\alpha)]. \quad \text{(C14)}$$

Equations (C12) and (C14) correct Eq. (35) of Ref. [1], which is erroneous. Next, substituting Eqs. (C14) and (C8) into Eq. (C13) and using the unitarity relation (48), one obtains

$$Q_{AE}=Q\cos^2\gamma+(1-Q)\sin^2\gamma, \quad \text{(C15)}$$

in agreement with Ref. [1].

The error rate q_{BE} in the Bob-Eve channel, before inconclusive results are discarded, is

$$q_{BE}=\sum_{\alpha=0,1} p(\alpha,0,1), \quad \text{(C16)}$$

or substituting Eqs. (62) and (68), we obtain

$$q_{BE}=(a^2+b^2)[1-\sin(2\alpha)]\sin^2\gamma. \quad \text{(C17)}$$

Also, one has for the error rate in the Bob-Eve channel, after inconclusive results are discarded,

$$Q_{BE}=\frac{q_{BE}}{1-R}, \quad \text{(C18)}$$

or substituting Eq. (C17) and (C8) and using the unitarity relation (48), we obtain

$$Q_{BE}=\sin^2\gamma. \quad \text{(C19)}$$

Equations (C17) and (C19) also agree with Ref. [1].

APPENDIX D: USEFUL PARAMETRIZATION OF ERROR RATES

From the unitarity relations (47) and (48) it follows that

$$\sin(2\gamma)=(1-a^2-b^2)(a^2+b^2+2a^2b^2-a^4-b^4)^{-1} \quad \text{(D1)}$$

and

$$1=a^2+b^2+2ab(a^2+b^2)^{-1}[\sin(2\alpha)-2ab]. \quad \text{(D2)}$$

Also, from Eq. (C9) one obtains

$$b=\pm\left(\frac{Q}{1-Q}\right)^{1/2}a. \quad \text{(D3)}$$

[A physical choice of sign in Eq. (D3) is determined below.] Next, substituting Eq. (D3) into Eq. (D2), one gets

$$|a|=(1-2Q)^{-1}(1-Q)^{1/2}\{1\mp 2[Q(1-Q)]^{1/2}\sin(2\alpha)\}^{1/2}, \quad \text{(D4)}$$

and substituting Eq. (D4) into Eq. (D3), one also has

$$|b|=(1-2Q)^{-1}Q^{1/2}\{1\mp 2[Q(1-Q)]^{1/2}\sin(2\alpha)\}^{1/2}. \quad \text{(D5)}$$

Using Eqs. (D4), (D5), and (D1), one then obtains

$$\sin(2\gamma)=\frac{2Q(1-Q)\mp[Q(1-Q)]^{1/2}\sin(2\alpha)}{[Q(1-Q)]^{1/2}\sin(2\alpha)\{2[Q(1-Q)]^{1/2}\sin(2\alpha)\mp 1\}}. \quad \text{(D6)}$$

In order to make a physical sign choice in Eq. (D6), we first require for the physical angle γ that

$$\sin^2(2\gamma)<1, \quad \text{(D7)}$$

which, together with Eq. (D6), requires

$$|2Q(1-Q)\mp[Q(1-Q)]^{1/2}\sin(2\alpha)| < |[Q(1-Q)]^{1/2}\sin(2\alpha)\{2[Q(1-Q)]^{1/2}\times\sin(2\alpha)\mp 1\}|. \quad \text{(D8)}$$

But for the physical error rate Q one requires

$$0<Q<1 \quad \text{(D9)}$$

and for physical angle α one also requires

$$0\leqslant\alpha\leqslant\pi/4. \quad \text{(D10)}$$

If one chooses the $+$ sign of $\mp$ in Eq. (D8), then because of Eqs. (D9) and (D10), Eq. (D8) becomes

$$2[Q(1-Q)]^{1/2}+\sin(2\alpha)<2[Q(1-Q)]^{1/2}\sin^2(2\alpha)+\sin(2\alpha) \quad \text{(D11)}$$

or, equivalently,

$$\sin^2(2\alpha)>1, \quad \text{(D12)}$$

which is unphysical for physical angle α. Therefore, one must choose the $-$ sign of $\mp$ in Eqs. (D8) and (D6), as well as in Eqs. (D4) and (D5). Thus Eq. (D6) becomes

$$\sin(2\gamma) = \frac{2Q(1-Q)-[Q(1-Q)]^{1/2}\sin(2\alpha)}{[Q(1-Q)]^{1/2}\sin(2\alpha)\{2[Q(1-Q)]^{1/2}\sin(2\alpha)-1\}}. \tag{D13}$$

The angle γ may be taken to be in the range

$$0 \leqslant \gamma \leqslant \pi/4. \tag{D14}$$

One also has the following trigonometric identities expressed in terms of Eq. (D13):

$$\cos^2\gamma = \tfrac{1}{2} + \tfrac{1}{2}[1-\sin^2(2\gamma)]^{1/2} \tag{D15}$$

and

$$\sin^2\gamma = \tfrac{1}{2} - \tfrac{1}{2}[1-\sin^2(2\gamma)]^{1/2}. \tag{D16}$$

Next, substituting Eqs. (D15), (D16), and (D13) into Eqs. (C15) and (C19) and using Eq. (73), it follows that [21,27,28]

$$Q_{AE}(Q,\theta) = \tfrac{1}{2} - (\tfrac{1}{2}-Q)[1-F(Q,\theta)^2]^{1/2} \tag{D17}$$

and

$$Q_{BE}(Q,\theta) = \tfrac{1}{2} - \tfrac{1}{2}[1-F(Q,\theta)^2]^{1/2}, \tag{D18}$$

where

$$F(Q,\theta) = \frac{2[Q(1-Q)]^{1/2}\sec\theta - 1}{2[Q(1-Q)]^{1/2}\cos\theta - 1}. \tag{D19}$$

[1] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[2] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[3] W. K. Wooters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[4] D. Dieks, Phys. Lett. **92A**, 271 (1982).
[5] N. Lutkenhaus, Phys. Rev. A **54**, 97 (1996).
[6] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[7] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997); **232**, 463 (1997).
[8] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[9] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[10] J. M. Myers and H. E. Brandt, Meas. Sci. Technol. **8**, 1222 (1997).
[11] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[12] U. M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[13] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[14] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[15] J. M. Jauch and C. Piron, Helv. Phys. Acta **40**, 559 (1967).
[16] E. B. Davies and J. T. Lewis, Commun. Math. Phys. **17**, 239 (1970).
[17] E. B. Davies, *Quantum Theory of Open Systems* (Academic, New York, 1976).
[18] P. A. Benioff, J. Math. Phys. **13**, 231 (1972).
[19] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement*, 2nd ed. (Springer, Berlin, 1996).
[20] P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics* (Springer, Berlin, 1995).
[21] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., Optical Society of America Annual Meeting, Rochester, NY, 1996 [Program OSA Annual Meeting, 84 (1996)]; H. E. Brandt and J. M. Myers, Invention Disclosure: POVM Receiver for Quantum Cryptography (U.S. Army Research Laboratory, Adelphi, MD, 1996).
[22] H. E. Brandt, in *The Quantum Information and Computing (QUIC) Workshop*, Pasadena, 1996, edited by H. J. Kimble (California Institute of Technology, Pasadena, 1996).
[23] H. E. Brandt, Joint April Meeting of the American Physical Society and the American Association of Physics Teachers, Washington, DC, 1997 [Bull. Am. Phys. Soc. **42**, 967 (1997)].
[24] G. Baym, *Lectures on Quantum Mechanics* (Addison-Wesley, Reading, MA, 1990).
[25] L. B. Levitin, in *Information Complexity and Control in Quantum Physics*, edited by A. Blaquiere, S. Diner, and G. Lochak (Springer, Berlin, 1987), p. 15.
[26] F. H. Madjid and J. M. Myers, Ann. Phys. (N.Y.) **221**, 258 (1993); **226**, 205 (1993).
[27] H. E. Brandt (unpublished).
[28] H. E. Brandt, in *U. S. Army Research Laboratory Proceedings of the 1997 Sensors and Electron Devices Symposium,* edited by S. Harrison (Environmental Research Institute of Michigan, Ann Arbor, MI, 1997), p. 289.
[29] D. Welsh, *Codes and Cryptography* (Clarendon, Oxford, 1995).
[30] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley Interscience, New York, 1991).