Inconclusive rate as a disturbance measure in quantum cryptography

Howard E. Brandt
U.S. Army Research Laboratory, AMSRL-SE-DP, 2800 Powder Mill Road, Adelphi, Maryland 20783
(Received 4 February 2000; published 14 September 2000)

The inconclusive rate is considered as a disturbance measure in key distribution in quantum cryptography. Bennett's two-state protocol is addressed for the case in which a positive operator-valued measure is implemented by the legitimate receiver in the presence of an individual attack by a general unitary disturbing eavesdropping probe. The maximum Renyi information gain by the disturbing probe is calculated for given receiver error and inconclusive rates. It is demonstrated explicitly that less information is available to an eavesdropper at a fixed inconclusive rate and error rate than is available at a fixed error rate only.

PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Bz

I. INTRODUCTION

An essential ingredient of quantum cryptography is the trade-off between the maximum information that an eavesdropper can obtain by intercepting the key-distribution transmission and the resulting disturbance induced in the transmission. The error rate alone is commonly chosen as the disturbance measure [1,2]; however, it has been conjectured [1] that the monitoring of other disturbance measures, along with the error rate, may allow less information gain by the eavesdropper and necessitate that fewer bits be sacrificed by the legitimate users during key distillation. In the present work, I consider the inconclusive rate (the rate of inconclusive measurement outcomes) as an additional disturbance measure. I demonstrate that, in fact, less information is available to an eavesdropper at a fixed inconclusive rate and error rate than is available at a fixed error rate only. It then follows that fewer bits need to be sacrificed during key distillation if the inconclusive rate is appropriately monitored along with the error rate.

In particular, I consider the two-state protocol [3] subjected to an individual eavesdropping attack [1] in which the legitimate receiver implements a positive operator-valued measure (POVM) [4–8]. The following set of POVM operators represents the possible measurements performed by the 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, the kets $|u\rangle$ and $|v\rangle$ represent the two possible nonorthogonal normalized polarization states of a carrier photon, with linear polarizations designated by u and v, respectively. The angle between the corresponding polarization vectors is $\overline{\theta}$. Since the photon is a spin-one representation of the Lorentz group, it follows that the Dirac bracket between the two states is [6]

$$\langle u|v\rangle=\sin 2\alpha, \tag{4}$$

where

$$\alpha=\frac{1}{2}\left(\frac{\pi}{2}-\overline{\theta}\right). \tag{5}$$

(Parametrization in terms of the angle α, instead of $\overline{\theta}$, is chosen for convenience.) The states $|u\rangle$ and $|v\rangle$ encode bit values 0 and 1, respectively. The POVM operators, Eqs. (1)–(3), are positive and their sum is unity. The operators A_u and A_v measure the probability of outcomes u and v, respectively. The operator $A_?$ measures the probability of an inconclusive measurement outcome.

One advantage of a POVM over a standard projective-valued (PV) measurement is that, for the POVM, the probability of obtaining an inconclusive result can be lower [9–12]. For the POVM receiver [13] considered in the present work, the undisturbed inconclusive rate $R_?^{\mathrm{POVM}}$ is given by [4,6,8,12]

$$R_?^{\mathrm{POVM}}=\sin 2\alpha. \tag{6}$$

(Note that $R_?^{\mathrm{POVM}}=P_?^{\mathrm{POVM}}$ in the notation of [12], since $P_?^{\mathrm{POVM}}$ is a probability per incident photon, which I designate here as a rate.) For an ordinary PV receiver consisting of a beam splitter with Wollaston prisms located at each of its two exit ports to distinguish the polarization state $|u\rangle$ from the perpendicular polarization state $|u_\perp\rangle$, or the polarization state $|v\rangle$ from the perpendicular polarization state $|v_\perp\rangle$, respectively, the inconclusive rate is given by [11,12]

$$R_?^{\mathrm{PV}}=\tfrac{1}{2}\,(1+\sin^2 2\alpha). \tag{7}$$

(Note that $R_?^{\mathrm{PV}}=P_?^{\mathrm{PV}}$ in the notation of [12].) It follows from Eqs. (6) and (7) that the inconclusive rate of the ideal POVM receiver is less than that for the PV receiver, since [12]

$$\frac{R_?^{\mathrm{POVM}}}{R_?^{\mathrm{PV}}}=\frac{2\sin 2\alpha}{1+\sin^2 2\alpha}<1. \tag{8}$$

The Fuchs-Peres model of eavesdropping on the two-state key distribution protocol represents the most general possible unitary disturbance of each encoded photon incident on the receiver [1,2] and caused by the eavesdropper's probe. Based on this model, it has been shown that the eavesdropping optimization of Slutsky *et al.* [1] for the two-state protocol holds for a POVM receiver, as well as for a PV receiver [5].

For both types of receiver, identical algebraic expressions were shown to result for both the Renyi information gain by the eavesdropper, and for the error rate induced by the eavesdropper, expressed in terms of the parameters characterizing the key distribution system and the eavesdropper's probe. The resulting disturbed inconclusive rate $R_?$ of the POVM receiver is given by Eq. (A29) of Appendix A [12]. Equivalently, one has

$$R_? = \frac{\sin 2\alpha(1 + c + a \sin 2\alpha)}{1 + \sin 2\alpha}, \tag{9}$$

where (in the notation of [1])

$$a = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \cos 2\theta \sin 2\phi, \tag{10}$$

$$c = \cos^2 \lambda \sin 2\theta \cos 2\phi, \tag{11}$$

expressed in terms of the probe parameters λ, μ, θ, and ϕ in the Fuchs-Peres model [1,2].

The security analysis for the two-state protocol against individual attacks is based on maximal Renyi information gained by the eavesdropper on corrected data for a fixed error rate [1,5]. The error rate is treated as the disturbance measure by the eavesdropper. The inconclusive rate of the legitimate receiver is the additional disturbance measure considered in the present work. In the following, an analysis is presented of the maximal Renyi information gain for fixed error and inconclusive rates. In Sec. II possible conditional extrema of the corresponding Lagrange function are calculated. In Sec. III a parametric analysis is presented to determine the extremum representing the absolute minimum overlap of the correlated probe states. In Sec. IV the maximum Renyi information gain for fixed error and inconclusive rates is specified and shown to be less than that for the fixed error rate alone. The advantage of monitoring the inconclusive rate is demonstrated by further parametric analysis. Section V presents a summary of results and conclusions. In Appendix A a derivation is given of the disturbed inconclusive rate, Eqs. (9)–(11). In Appendix B analytic expressions are obtained for the nonoptimized overlap and the error rate in terms of the probe parameters. In Appendix C a parametric expression is obtained for the minimum overlap of the correlated probe states as a function of error rate (with no constraint on the inconclusive rate).

II. INFORMATION-GAIN EXTREMA

In [1] the quantity E', simply related to the error rate E, was introduced in the problem of conditional minimization of the overlap Q between the two pertinent correlated probe states for a fixed error rate, namely,

$$E' = \frac{\cos^2 2\alpha}{1 - 2E}. \tag{12}$$

Also

$$E' = \frac{1}{d}(1 - a \sin^2 2\alpha - c \sin 2\alpha), \tag{13}$$

where

$$d = \sin^2 \lambda + \cos^2 \lambda \cos 2\theta, \tag{14}$$

and a and c are given by Eqs. (10) and (11). It follows from Eq. (13) that

$$a \sin^2 2\alpha + c \sin 2\alpha = 1 - dE'. \tag{15}$$

Therefore, substituting Eq. (15) in Eq. (9), one obtains

$$R_? = (1 + \sin 2\alpha)^{-1}(\sin 2\alpha + 1 - dE'). \tag{16}$$

From Eq. (16), it therefore follows that

$$d = \frac{(1 + \sin 2\alpha)(1 - R_?)}{E'}. \tag{17}$$

Since constant error rate E corresponds to constant E' [see Eq. (12), noting α is constant], it follows from Eq. (17) that d is constant for the constant error rate E and the constant inconclusive rate $R_?$. In all of the following, the inconclusive rate $R_?$ will appear only through the expression for d, Eq. (17), and can be treated simply as a fixed prescribed parameter.

The appropriate Lagrange function for determining possible conditional extrema is then given by [1]

$$F = Q' + \xi E', \tag{18}$$

where ξ is a Lagrange multiplier, and

$$Q' = [1 + (\sec^2 2\alpha)E']Q + (\sec^2 2\alpha)E', \tag{19}$$

where Q is the overlap between the correlated states of the probe. One also has [1]

$$Q' = \frac{a + b + 1}{d}, \tag{20}$$

where a and d are given by Eqs. (10) and (17), respectively, and

$$b = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \sin 2\phi. \tag{21}$$

Since d is constant, it follows from Eq. (14) that λ and θ are constrained by

$$\cos^2 \lambda = \frac{1 - d}{1 - \cos 2\theta}. \tag{22}$$

Therefore λ will be treated as a dependent variable. Also,

$$\sin^2 \lambda = 1 - \cos^2 \lambda, \tag{23}$$

and substituting Eq. (22) in Eq. (23), one obtains

$$\sin^2 \lambda = \frac{d - \cos 2\theta}{1 - \cos 2\theta}. \tag{24}$$

Substituting Eqs. (13) and (20) in Eq. (18), one obtains

$$F=\frac{F'+1+\xi}{d}, \tag{25}$$

where

$$F'=a+b-\xi\overline{E}, \tag{26}$$

and

$$\overline{E}=a\sin^2 2\alpha+c\sin 2\alpha. \tag{27}$$

Since ξ and d are constant in Eq. (25), extremization of F' must also result in extremization of F, and, because of this, F' may be taken as the effective Lagrange function. I therefore extremize the Lagrange function, Eq. (26). Substituting Eqs. (10), (11), (21)–(23), and (27) in Eq. (26), we obtain

$$\begin{aligned}F'=&(2-\xi\sin^2 2\alpha)\sin 2\mu\left(1-\frac{1-d}{1-\cos 2\theta}\right)\\&+[(1-\xi\sin^2 2\alpha)\cos 2\theta\sin 2\phi+\sin 2\phi\\&-\xi\sin 2\alpha\sin 2\theta\cos 2\phi]\frac{1-d}{1-\cos 2\theta}.\end{aligned} \tag{28}$$

Note that in the expression for the effective Lagrange function F', the constants $R_?$ and E appear implicitly in the constant d through Eqs. (17) and (12).

For the extremum, one requires [1,14]

$$\frac{\partial F'}{\partial\mu}=0, \tag{29}$$

$$\frac{\partial F'}{\partial\theta}=0, \tag{30}$$

$$\frac{\partial F'}{\partial\phi}=0, \tag{31}$$

or

$$\frac{\partial\overline{E}}{\partial\mu}=0, \tag{32}$$

$$\frac{\partial\overline{E}}{\partial\theta}=0, \tag{33}$$

$$\frac{\partial\overline{E}}{\partial\phi}=0. \tag{34}$$

[Equations (32)–(34) may alternatively be considered as special cases of Eqs. (29)–(31) in the limit of an infinite Lagrange multiplier ξ in Eq. (26).] First, substituting Eq. (28) in Eq. (29), we obtain

$$(2-\xi\sin^2 2\alpha)(d-\cos 2\theta)\cos 2\mu=0. \tag{35}$$

Equation (35) can be satisfied in three possible ways:

$$\text{(i)}\quad \xi=\frac{2}{\sin^2 2\alpha}, \tag{36}$$

$$\text{(ii)}\quad \cos 2\theta=d, \tag{37}$$

$$\text{(iii)}\quad \cos 2\mu=0. \tag{38}$$

In the following, we refer to Eqs. (36), (37), and (38) as possible extrema (i), (ii), and (iii), respectively.

First consider possible extremum (i), corresponding to Eq. (36). If we substitute Eq. (28) in Eq. (30), and use Eq. (36), we obtain

$$\sin 2\phi=\pm 1. \tag{39}$$

But substituting Eq. (28) in Eq. (31), and using Eq. (36), we also obtain

$$\tan 2\phi=\frac{\sin 2\alpha(\cos 2\theta-1)}{2\sin 2\theta}. \tag{40}$$

According to Eqs. (39) and (40), we require that

$$\cos 2\theta=-1. \tag{41}$$

Combining Eqs. (10)–(13), (17), (19)–(22), (39), and (41), one obtains

$$Q=\frac{(1-R_?)^{-1}(1+\sin 2\alpha)^{-1}[2+(1\pm 1)\sin^2 2\alpha]-[1\pm(1-2E)]\tan^2 2\alpha-2}{2(1-E)\tan^2 2\alpha}. \tag{42}$$

Note that Eq. (42) yields an unphysical value $Q\geqslant 1$ if the inconclusive rate assumes or exceeds its unperturbed value,

$$R_?=\sin 2\alpha. \tag{43}$$

Next, the alternative possible extremum (ii) satisfies Eq. (37). Also, substituting Eq. (28) in Eq. (30), one requires

$$\begin{aligned}0=\frac{\partial F'}{\partial\theta}=2(1-d)(1-\cos 2\theta)^{-2}\{&(2-\xi\sin^2 2\alpha)\sin 2\mu\sin 2\theta\\&-[(1-\xi\sin^2 2\alpha)\cos 2\theta\sin 2\phi+\sin 2\phi-\xi\sin 2\alpha\sin 2\theta\cos 2\phi]\sin 2\theta\\&-[(1-\xi\sin^2 2\alpha)\sin 2\phi\sin 2\theta+\xi\sin 2\alpha\cos 2\phi\cos 2\theta](1-\cos 2\theta)\}.\end{aligned} \tag{44}$$

From a trigonometric identity and Eq. (37), it follows that

$$\sin 2\theta = \pm(1-\cos^2 2\theta)^{1/2} = e_\theta(1-d^2)^{1/2}, \tag{45}$$

where

$$e_\theta = \pm 1. \tag{46}$$

Next, substituting Eqs. (37) and (45) in Eq. (44), one obtains

$$\sin 2\mu = \frac{(2-\xi\sin^2 2\alpha)\sin 2\phi - \xi e_\theta(1-d)(1-d^2)^{-1/2}\sin 2\alpha\cos 2\phi}{2-\xi\sin^2 2\alpha}. \tag{47}$$

Furthermore, substituting Eq. (28) in Eq. (31), one obtains

$$0 = \frac{\partial F'}{\partial \phi} = 2\frac{1-d}{1-\cos 2\theta}\{[1+(1-\xi\sin^2 2\alpha)\cos 2\theta]\cos 2\phi + \xi\sin 2\alpha\sin 2\theta\sin 2\phi\}. \tag{48}$$

Next, substituting Eqs. (37) and (45) in Eq. (48), one obtains

$$\tan 2\phi = e_\theta\left[\frac{d\sin^2 2\alpha - (1+d)\xi^{-1}}{(1-d^2)^{1/2}\sin 2\alpha}\right]. \tag{49}$$

Solving Eq. (49) for ξ, one therefore requires

$$\xi = \frac{1+d}{d\sin^2 2\alpha - e_\theta(1-d^2)^{1/2}\sin 2\alpha\tan 2\phi}. \tag{50}$$

Next, substituting Eq. (37) in Eq. (22), one requires for possible extremum (ii),

$$\cos^2\lambda = 1, \tag{51}$$

and therefore, one also requires

$$\sin\lambda = 0. \tag{52}$$

Next, using Eqs. (20), (21), and (10), it follows that

$$Q' = \frac{1}{d}[2\sin^2\lambda\sin 2\mu + \cos^2\lambda\sin 2\phi(\cos 2\theta+1)+1]. \tag{53}$$

Also using Eqs. (13), (10), and (11), one gets

$$E' = \frac{1}{d}[1-\sin^2 2\alpha(\sin^2\lambda\sin 2\mu + \cos^2\lambda\cos 2\theta\sin 2\phi) - \sin 2\alpha\cos^2\lambda\sin 2\theta\cos 2\phi]. \tag{54}$$

Substituting Eqs. (51), (52), and (37) in Eq. (53) (which holds generally), one gets

$$Q' = \frac{1}{d}[1+(1+d)\sin 2\phi], \tag{55}$$

or equivalently,

$$\sin 2\phi = \frac{dQ'-1}{1+d}. \tag{56}$$

Then one also has

$$\cos 2\phi = e_\phi\left[1-\left(\frac{dQ'-1}{1+d}\right)^2\right]^{1/2}, \tag{57}$$

where

$$e_\phi = \pm 1. \tag{58}$$

Next, substituting Eqs. (51), (52), (37), and (45) in Eq. (54) (which holds generally), one obtains

$$E' = \frac{1}{d}[1-d\sin^2 2\alpha\sin 2\phi - e_\theta(1-d^2)^{1/2}\sin 2\alpha\cos 2\phi]. \tag{59}$$

If we next substitute Eqs. (56) and (57) in Eq. (59), and solve for Q', it follows from the quadratic formula that

$$Q' = \frac{-B\pm(B^2-4AC)^{1/2}}{2A} = -\frac{1}{2}\left(\frac{B}{A}\right)\left\{1\mp\left[1-4\left(\frac{A}{B}\right)^2\left(\frac{C}{A}\right)\right]^{1/2}\right\}, \tag{60}$$

where

$$A = \frac{d^2}{(1+d)^2}\sin^2 2\alpha(1-d^2\cos^2 2\alpha), \tag{61}$$

$$B = \frac{2d}{(1+d)^2}\sin^2 2\alpha[d^2(1+d)E' - 1 - d - d^2\sin^2 2\alpha], \tag{62}$$

$$C = \left(dE' - 1 - \frac{d\sin^2 2\alpha}{1+d}\right)^2 - \frac{d(1-d)(2+d)}{(1+d)}\sin^2 2\alpha. \tag{63}$$

Introducing the notation,

$$\rho = \frac{1}{(1+\sin 2\alpha)(1-R_?)}, \tag{64}$$

we can write Eq. (17) as

$$d=\frac{1}{\rho E'}. \tag{65}$$

In Eq. (64) and the following, the parameter ρ is a measure of the inconclusive rate $R_?$ and the angle α specifying the nonorthogonal polarization states of the signal. Using Eqs. (61)–(63) and (65), one can show that

$$\left(\frac{B}{A}\right)=-2(\rho^2E'^2-\cos^2 2\alpha)^{-1}[\rho^3E'^3-\rho(1-\rho)\times E'^2-(1-\rho\sin^2 2\alpha)E'], \tag{66}$$

and

$$\left(\frac{C}{A}\right)=(\rho^2E'^2-\cos^2 2\alpha)^{-1}\{[\rho^2(1-\rho)^2\csc^2 2\alpha]E'^4+[2\rho(1-\rho)(1-\rho-\rho\sin^2 2\alpha)\csc^2 2\alpha-2\rho^3]E'^3+[(1-\rho-\rho\sin^2 2\alpha)^2\csc^2 2\alpha-\rho^2]E'^2+2\rho E'+1\}. \tag{67}$$

Substituting Eqs. (66) and (67) in Eq. (60), one obtains

$$Q'=\frac{\gamma(E')}{\sigma(E')}\left\{1\mp\left[1-\frac{\sigma(E')\kappa(E')}{\gamma(E')^2}\right]^{1/2}\right\}, \tag{68}$$

where the functions $\gamma(E')$, $\sigma(E')$, and $\kappa(E')$ are defined by

$$\gamma(E')=-(1-\rho\sin^2 2\alpha)E'-\rho(1-\rho)E'^2+\rho^3E'^3, \tag{69}$$

$$\sigma(E')=-\cos^2 2\alpha+\rho^2E'^2, \tag{70}$$

and

$$\kappa(E')=1+2\rho E'+[(1-\rho-\rho\sin^2 2\alpha)^2\csc^2 2\alpha-\rho^2]E'^2+[2\rho(1-\rho)(1-\rho-\rho\sin^2 2\alpha)\csc^2 2\alpha-2\rho^3]E'^3+[\rho^2(1-\rho)^2\csc^2 2\alpha]E'^4, \tag{71}$$

respectively.

Next substituting Eq. (12) in Eqs. (66) and (67), one obtains

$$\left(\frac{B}{A}\right)=-2(1-2E)^{-1}[\rho^2\cos^2 2\alpha-(1-2E)^2]^{-1}\times\{\rho^3\cos^4 2\alpha-\rho(1-\rho)(\cos^2 2\alpha)(1-2E)-(1-\rho\sin^2 2\alpha)(1-2E)^2\}, \tag{72}$$

$$\left(\frac{C}{A}\right)=(1-2E)^{-2}[\rho^2\cos^2 2\alpha-(1-2E)^2]^{-1}\times\{\rho^2(1-\rho)^2\csc^2 2\alpha\cos^6 2\alpha+[2\rho(1-\rho)\times(1-\rho-\rho\sin^2 2\alpha)\csc^2 2\alpha-2\rho^3](\cos^4 2\alpha)(1-2E)+[(1-\rho-\rho\sin^2 2\alpha)^2\csc^2 2\alpha-\rho^2]\cos^2 2\alpha\times(1-2E)^2+2\rho(1-2E)^3+(\sec^2 2\alpha)(1-2E)^4\}. \tag{73}$$

Equation (19) (which holds generally) can be written as follows:

$$Q=\frac{Q'-(\sec^2 2\alpha)E'}{1+(\sec^2 2\alpha)E'}. \tag{74}$$

Substituting Eq. (12) in Eq. (74), one then obtains

$$Q=\frac{1}{2(1-E)}[(1-2E)Q'-1]. \tag{75}$$

Then if we substitute Eqs. (60), (72), and (73) in Eq. (75), the overlap Q, expressed in terms of the error rate E and inconclusive rate $R_?$ [through ρ in Eq. (64)] becomes

$$Q=\frac{1}{\epsilon+1}\left\{f(\epsilon)\left[1\mp\left(1-\frac{g(\epsilon)}{f(\epsilon)}\right)^{1/2}\right]-1\right\}, \tag{76}$$

where

$$\epsilon=1-2E, \tag{77}$$

and the following functions are defined:

$$f(\epsilon)=\frac{\alpha(\epsilon)}{\beta(\epsilon)}, \tag{78}$$

$$g(\epsilon)=\frac{\delta(\epsilon)}{\alpha(\epsilon)}, \tag{79}$$

$$\alpha(\epsilon)=\rho^3\cos^4 2\alpha-\rho(1-\rho)(\cos^2 2\alpha)\epsilon-(1-\rho\sin^2 2\alpha)\epsilon^2, \tag{80}$$

$$\beta(\epsilon)=\rho^2\cos^2 2\alpha-\epsilon^2, \tag{81}$$

$$\delta(\epsilon)=\cos^2 2\alpha\{\rho^2(1-\rho)^2\csc^2 2\alpha\cos^4 2\alpha+[2\rho(1-\rho)(1-\rho-\rho\sin^2 2\alpha)\cot^2 2\alpha-2\rho^3\cos^2 2\alpha]\epsilon+[(1-\rho-\rho\sin^2 2\alpha)^2\csc^2 2\alpha-\rho^2]\times\epsilon^2+2\rho(\sec^2 2\alpha)\epsilon^3+(\sec^4 2\alpha)\epsilon^4\}, \tag{82}$$

where ρ is given by Eq. (64). The corresponding possible extremum in the Renyi information gain by the eavesdropper is given by [1,5]

$$I^R_{\rm opt}=\log_2(2-Q^2) \tag{83}$$

and Eq. (76).

Another alternative possible extremum (iii) satisfies Eq. (38), from which it also follows that

$$\sin 2\mu=e_\mu, \tag{84}$$

where

$$e_\mu = \pm 1. \tag{85}$$

Substituting Eq. (28) in Eq. (30), one obtains [as in Eq. (44)]

$$0 = \frac{\partial F'}{\partial \theta} = \frac{2(1-d)}{(1-\cos 2\theta)^2}\{(2-\xi \sin^2 2\alpha)\sin 2\mu \sin 2\theta - [(1-\xi \sin^2 2\alpha)\cos 2\theta \sin 2\phi + \sin 2\phi - \xi \sin 2\alpha \sin 2\theta \cos 2\phi]\sin 2\theta - [(1-\xi \sin^2 2\alpha)\sin 2\theta \sin 2\phi + \xi \sin 2\alpha \cos 2\theta \cos 2\phi](1-\cos 2\theta)\}. \tag{86}$$

Next, substituting Eq. (84) in Eq. (86), and solving for ξ, we see that possible extremum (iii) requires

$$\xi = \frac{2 \sin 2\theta (e_\mu - \sin 2\phi)}{\sin 2\alpha [\sin 2\alpha \sin 2\theta (e_\mu - \sin 2\phi) - \sin^2 2\theta \cos 2\phi + \cos 2\theta (1-\cos 2\theta)\cos 2\phi]}. \tag{87}$$

Furthermore, from Eqs. (28) and (31) one again obtains Eq. (48), from which one gets

$$\tan 2\phi = \frac{-\xi^{-1}(1+\cos 2\theta) + \sin^2 2\alpha \cos 2\theta}{\sin 2\alpha \sin 2\theta}. \tag{88}$$

If we then substitute Eq. (87) in Eq. (88), we obtain

$$\sin 2\theta \{(e_\mu - \sin 2\phi)[2 \tan 2\phi \sin 2\theta + \sin 2\alpha (1-\cos 2\theta)] - \sin 2\theta \cos 2\phi\} = 0. \tag{89}$$

One notes that if

$$\sin 2\theta = 0 \tag{90}$$

is taken as a possible solution to Eq. (89), then one also has

$$\cos 2\theta = e_\theta = \pm 1, \tag{91}$$

and then according to Eq. (14), one has

$$d = \sin^2 \lambda + e_\theta \cos^2 \lambda, \tag{92}$$

or

$$d = \sin^2 \lambda (1 - e_\theta) + e_\theta. \tag{93}$$

Comparing Eq. (93) with Eq. (17), we conclude that, since E', $R_?$, and α are fixed, $e_\theta = -1$, and then, according to Eq. (91),

$$\cos 2\theta = -1. \tag{94}$$

[Also, F' in Eq. (28) is singular for $\cos 2\theta = 1$, and the derivation of Eq. (35) implicitly assumes $\cos 2\theta \neq 1$.) It then follows from Eq. (93) that

$$\sin^2 \lambda = \frac{d+1}{2}, \tag{95}$$

and then also

$$\cos^2 \lambda = \frac{1-d}{2}. \tag{96}$$

Next substituting Eqs. (90) and (94) in Eq. (88), we obtain

$$\tan 2\phi = -\infty, \tag{97}$$

$$\sin 2\phi = \pm 1, \tag{98}$$

and

$$\cos 2\phi = 0. \tag{99}$$

Therefore, substituting Eqs. (84), (95), (96), (98), and (94) in Eq. (53), one obtains

$$Q' = \left(1 + \frac{1}{d}\right) e_\mu + \frac{1}{d}. \tag{100}$$

Next substituting Eq. (65) in Eq. (100), we get

$$Q' = e_\mu + (1 + e_\mu)\rho E'. \tag{101}$$

Then if one substitutes Eqs. (101) and (12) in Eq. (19), and solves for Q, one obtains

$$Q = \frac{1}{2(1-E)}[(1+e_\mu)\rho \cos^2 2\alpha + e_\mu (1-2E) - 1], \tag{102}$$

where ρ is given by Eq. (64). But the error rate must be positive, and for $e_\mu = -1$ in Eq. (102), one gets $Q = -1$, which is nonphysical. Therefore

$$e_\mu = 1 \tag{103}$$

must be chosen, and Eq. (102) becomes

$$Q = \frac{1}{(1-E)}(\rho \cos^2 2\alpha - E). \tag{104}$$

The corresponding possible extremum in the Renyi information gain by the eavesdropper is given by Eqs. (83) and (104).

Alternatively, Eq. (89) is also clearly satisfied if

$$(e_\mu-\sin 2\phi)[2\tan 2\phi\sin 2\theta+\sin 2\alpha(1-\cos 2\theta)]$$
$$=\sin 2\theta\cos 2\phi. \tag{105}$$

From Eq. (105), it follows that

$$[(A^2+1)\sin 2\theta+2A]\sin 2\theta=0, \tag{106}$$

where

$$A=\frac{1}{\sin 2\alpha}\left[\frac{2(e_\mu-\sin 2\phi)\tan 2\phi-\cos 2\phi}{e_\mu-\sin 2\phi}\right]. \tag{107}$$

One possible solution to Eq. (106) is again given by Eq. (90), and again results in Eq. (104). The other possible solution to Eq. (106) is

$$\sin 2\theta=\frac{2\sin 2\alpha(e_\mu-\sin 2\phi)[\cos 2\phi-2(e_\mu-\sin 2\phi)\tan 2\phi]}{\sin^2 2\alpha(e_\mu-\sin 2\phi)^2+[\cos 2\phi-2(e_\mu-\sin 2\phi)\tan 2\phi]^2} \tag{108}$$

and

$$\cos 2\theta=e_\theta(1-\sin^2 2\theta)^{1/2}. \tag{109}$$

Also, one has, according to Eqs. (22) and (24) (which hold generally)

$$\cos^2\lambda=\frac{1-d}{1-\cos 2\theta} \tag{110}$$

and

$$\sin^2\lambda=\frac{d-\cos 2\theta}{1-\cos 2\theta}. \tag{111}$$

Substituting Eqs. (84), (110), and (111) in Eqs. (53) and (54), one obtains

$$Q'=\frac{1+2de_\mu+(1-d)\sin 2\phi-[1+2e_\mu-(1-d)\sin 2\phi]\cos 2\theta}{d(1-\cos 2\theta)} \tag{112}$$

and

$$E'=[d(1-\cos 2\theta)]^{-1}\{1-de_\mu\sin^2 2\alpha$$
$$-[1-e_\mu\sin^2 2\alpha+(1-d)\sin^2 2\alpha\sin 2\phi]$$
$$\times\cos 2\theta-(1-d)\sin 2\alpha\cos 2\phi\sin 2\theta\}. \tag{113}$$

Next, substituting Eq. (65) in Eq. (113) and solving for E', one obtains

$$E'=\frac{1}{\rho(1+R)}, \tag{114}$$

where

$$R=\frac{[\rho^{-1}-(1-e_\mu\sin^2 2\alpha)](1-\cos 2\theta)}{\sin 2\alpha[\sin 2\alpha(\sin 2\phi\cos 2\theta-e_\mu)+\cos 2\phi\sin 2\theta]}. \tag{115}$$

Then substituting Eqs. (65) and (114) in Eq. (112), one gets

$$Q'=\frac{1}{1+R}\left[1+2e_\mu-\sin 2\phi-\frac{2(e_\mu-\sin 2\phi)}{1-\cos 2\theta}\right]$$
$$+\sin 2\phi+\frac{2(e_\mu-\sin 2\phi)}{1-\cos 2\theta}. \tag{116}$$

Equations (114)–(116), together with Eqs. (108) and (109), determine Q' as a function of E', parametrically in terms of the parameter ϕ.

Next, substituting Eqs. (116) and (12) in Eq. (19), and solving for Q, we obtain

$$Q=\frac{1-2E}{2(1-E)}\left\{\sin 2\phi+\frac{2(e_\mu-\sin 2\phi)}{1-\cos 2\theta}-\frac{1}{1-2E}+\frac{1}{1+R}\right.$$
$$\left.\times\left[1-\sin 2\phi-\frac{2(e_\mu\cos 2\theta-\sin 2\phi)}{1-\cos 2\theta}\right]\right\}. \tag{117}$$

Also, from Eqs. (12) and (114), it follows that

$$E=\tfrac{1}{2}[1-\rho(\cos^2 2\alpha)(1+R)]. \tag{118}$$

Equations (117), (118), (115), (108), and (109) determine the function $Q(E)$ in terms of E, parametrically in terms of the parameter ϕ. The corresponding possible extrema in the Re-

nyi information gain by the eavesdropper from the receiver are then given by Eq. (83) and $Q(E)$.

Proceeding to solve Eqs. (32)–(34), we first substitute Eqs. (10), (11), (22), and (24) in Eq. (27) to obtain

$$\overline{E}=\sin^2 2\alpha \sin 2\mu\left(1-\frac{1-d}{1-\cos 2\theta}\right)+[\sin^2 2\alpha \cos 2\theta \sin 2\phi + \sin 2\alpha \sin 2\theta \cos 2\phi]\frac{1-d}{1-\cos 2\theta}. \tag{119}$$

Then substituting Eq. (119) in Eq. (32), one obtains

$$(d-\cos 2\theta)\cos 2\mu=0. \tag{120}$$

Equation (120) can be satisfied in two possible ways:

$$\text{(iv)}\quad \cos 2\theta=d, \tag{121}$$

$$\text{(v)}\quad \cos 2\mu=0. \tag{122}$$

In the following, we refer to Eqs. (121) and (122) as possible extrema (iv) and (v), respectively.

The possible extremum (iv) satisfies Eq. (121). Also, substituting Eq. (119) in Eq. (33), and using Eqs. (45) and (121), one requires

$$\sin 2\mu=\sin 2\phi+\frac{e_\theta(1-d)^{1/2}\cos 2\phi}{(1+d)^{1/2}\sin 2\alpha}. \tag{123}$$

Next, substituting Eq. (119) in Eq. (34), and using Eqs. (121) and (45), one requires

$$\tan 2\phi=\frac{e_\theta d \sin 2\alpha}{(1-d^2)^{1/2}}. \tag{124}$$

Then substituting Eq. (124) in Eq. (55), and using Eq. (65), one gets

$$Q'=\rho E'\left[1+\frac{e_\phi(1+\rho E')\sin 2\alpha}{\rho E'(\rho^2 E'^2-\cos^2 2\alpha)^{1/2}}\right]. \tag{125}$$

Then substituting Eqs. (125) and (12) in Eq. (75), we obtain

$$Q=\frac{1}{2(1-E)}\left\{\rho\cos^2 2\alpha-1+\frac{e_\phi(\tan 2\alpha)(1-2E)(1-2E+\rho\cos^2 2\alpha)}{[\rho^2\cos^2 2\alpha-(1-2E)^2]^{1/2}}\right\}. \tag{126}$$

Another possible extremum (v) satisfies Eq. (122), from which Eqs. (84) and (85) again follow. Also, substituting Eq. (119) in Eq. (33), and using Eq. (84), one obtains

$$\tan 2\theta=\frac{2e_\theta\cos 2\phi \sin 2\alpha(e_\mu-\sin 2\phi)}{\cos^2 2\phi-\sin^2 2\alpha(e_\mu-\sin 2\phi)^2}. \tag{127}$$

[Alternatively, Eq. (90) is also possible here, but this again leads to Eq. (104).] Furthermore, Eqs. (119) and (34) also require

$$\tan 2\phi=\sin 2\alpha\cot 2\theta. \tag{128}$$

Then substituting Eq. (127) in Eq. (128), the latter becomes

$$\sin 2\phi=e_\mu-\frac{2(1-e_\theta)e_\mu}{2-e_\theta(1+\sin^2 2\alpha)}. \tag{129}$$

If $e_\theta=+1$ in Eqs. (46) and (129), then one has

$$\sin 2\phi=e_\mu, \tag{130}$$

and then substituting Eq. (130) in Eq. (127), one also has

$$\tan 2\theta=0, \tag{131}$$

from which Eqs. (90)–(104) again follow. If $e_\theta=-1$ in Eqs. (46), (129), and (127), then

$$\sin 2\phi=-\frac{\cos^2 2\alpha e_\mu}{3+\sin^2 2\alpha} \tag{132}$$

and

$$\tan 2\theta=-8^{1/2}e_\mu e_\phi \sec 2\alpha \tan 2\alpha(1+\sin^2 2\alpha)^{1/2}. \tag{133}$$

From Eq. (133), one obtains

$$\cos 2\theta=\frac{\overline{e_\theta}}{[1+8\sec^2 2\alpha\tan^2 2\alpha(1+\sin^2 2\alpha)]^{1/2}}, \tag{134}$$

where

$$\overline{e_\theta}=\pm 1. \tag{135}$$

Next, using Eqs. (112), (12), (65), (132), and (134), Eq. (75) becomes

$$Q=\frac{1}{2(1-E)}\left\{(1+2e_\mu)\rho\cos^2 2\alpha-1+e_\mu\frac{(7+\sin^2 2\alpha)(1-2E-\rho\cos^2 2\alpha)}{(3+\sin^2 2\alpha)} - \frac{8e_\mu(1-2E-\rho\cos^2 2\alpha)}{(3+\sin^2 2\alpha)\{1-\overline{e_\theta}[1+8\sec^2 2\alpha\tan^2 2\alpha(1+\sin^2 2\alpha)]^{1/2}\}}\right\}. \tag{136}$$

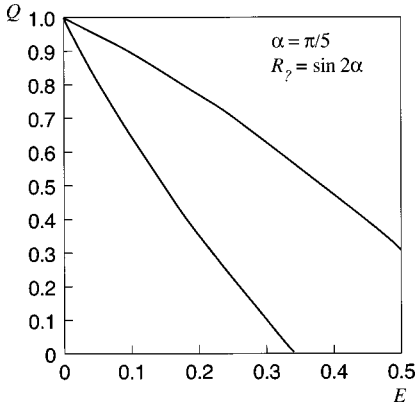

FIG. 1. Overlap extrema Q, Eq. (76), as a function of error rate E for the inconclusive rate $R_?=\sin 2\alpha$ and $\alpha=\pi/5$. The upper curve corresponds to the positive sign choice in Eq. (76). The lower curve corresponds to the negative sign choice and is the absolute minimum overlap, Eq. (137).

Parametric analysis is next to be completed of the possible extrema determined here [Eqs. (42), (76), (104), (117), (118), (126), and (136)] to determine the global minimum overlap Q for fixed error and inconclusive rates, and the corresponding maximum Renyi information gain by the eavesdropper from the POVM receiver.

III. MINIMUM OVERLAP OF CORRELATED PROBE STATES

We seek the minimum overlap Q in order to get the maximum Renyi information gain I [see Eq. (83)]. First consider the possible extremum given by Eq. (104). Note that if the parameter $R_?$ is chosen to equal or exceed the unperturbed inconclusive rate, Eq. (6), then $R_?\geqslant\sin 2\alpha$, and, according to Eq. (64), one has $\rho\geqslant 1/\cos^2 2\alpha$. It then follows from Eq. (104) that $Q\geqslant 1$, which cannot correspond to a minimum, since $0\leqslant Q\leqslant 1$. Therefore Eq. (104) cannot represent a possible minimum of Q. Also recall that Eq. (42) is unphysical for $R_?\geqslant\sin 2\alpha$.

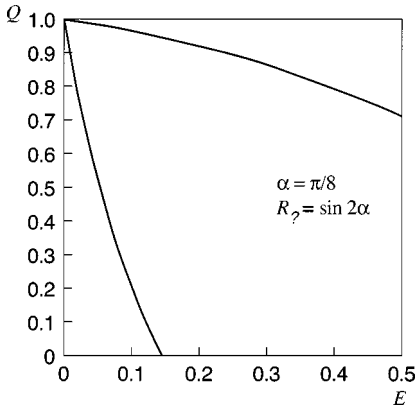

FIG. 2. Overlap extrema Q, Eq. (76), as a function of error rate E for the inconclusive rate $R_?=\sin 2\alpha$ and $\alpha=\pi/8$. The upper curve corresponds to the positive sign choice in Eq. (76). The lower curve corresponds to the negative sign choice and is the absolute minimum overlap, Eq. (137).

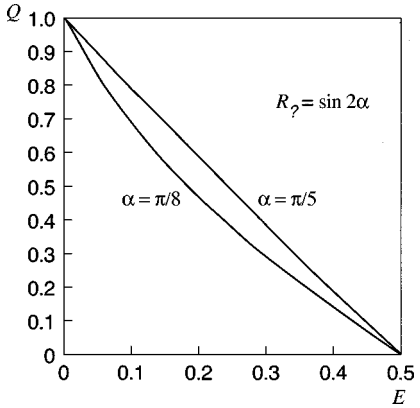

FIG. 3. Overlap extrema Q, Eq. (126), as a function of E, for $R_?=\sin 2\alpha$, $e_\phi=+1$, and $\alpha=\pi/5$ and $\pi/8$.

Next consider the possible extremum given by Eq. (76). In Figs. 1 and 2, I plot Q as a function of E for $R_?=\sin 2\alpha$ and for $\alpha=\pi/5$ and $\pi/8$, respectively. The lower curve in both figures corresponds to the negative sign choice in Eq. (76). Thus, the lower value of Q is represented by the negative sign choice in Eq. (76), namely,

$$Q=\frac{1}{\epsilon+1}\left\{f(\epsilon)\left[1-\left(1-\frac{g(\epsilon)}{f(\epsilon)}\right)^{1/2}\right]-1\right\}, \qquad (137)$$

and Eq. (137) represents a possible minimum.

We next calculate Q for the possible extrema given parametrically in terms of ϕ by Eqs. (117), (118), (108), (109), and (115), also for $R_?=\sin 2\alpha$, for $\alpha=\pi/5$ or $\pi/8$, and for $0\leqslant\phi\leqslant\pi$. It turns out that Q is negative for $e_\mu=-1$ and $e_\theta=-1$, that is, $Q(\phi)_{|e_\mu=-1,e_\theta=-1}<0$. Also $-1\geqslant Q(\phi)_{|e_\mu=-1,e_\theta=+1}\geqslant 1$; and $E(\phi)_{|e_\mu=+1,e_\theta=\pm 1}=0$. Thus Eqs. (117) and (118) cannot, in this case, represent a possible minimum of Q. (Note that for $R_?\geqslant\sin 2\alpha$, Eq. (B4) must be enforced.)

Next consider possible extrema given by Eq. (126). In Fig. 3 Q is plotted as a function of E for $R_?=\sin 2\alpha$, $e_\phi=+1$, and $\alpha=\pi/5$ and $\pi/8$. For $e_\phi=-1$, one gets $Q(E)<0$ for $E<\frac{1}{2}$, which is nonphysical. (As in [1], it is assumed in the present work that $E<\frac{1}{2}$.) Actually, Eqs. (54), (65). (12). (22), (24), (121), (123). and (124) imply that E is in each case constant (independent of Q).

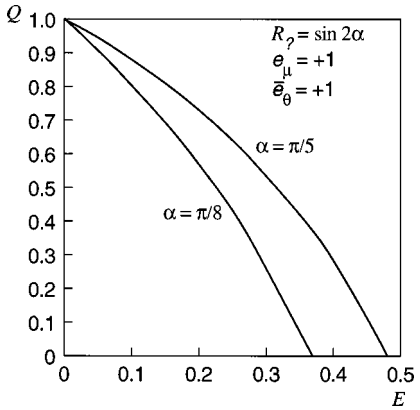

FIG. 4. Overlap extrema Q, Eq. (136), as a function of E for $R_?=\sin 2\alpha$, $e_\mu=+1$, $\overline{e_\theta}=+1$, and $\alpha=\pi/5$ and $\pi/8$.

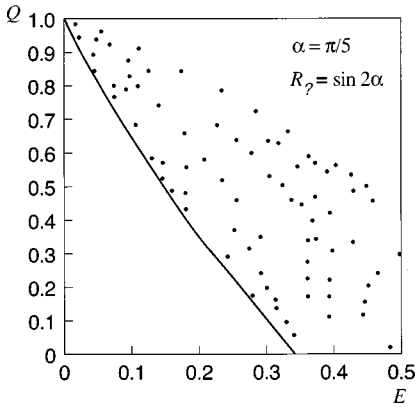

FIG. 5. Points correspond to the unoptimized overlap Q (Appendix B) versus the error rate E for $R_?=\sin 2\alpha$ and $\alpha=\pi/5$ for a range of values of nonoptimal probe parameters. The solid curve is the corresponding minimum overlap, Eq. (137).

Next consider possible extrema given by Eq. (136). In Fig. 4 Q is plotted as a function of E for $R_?=\sin 2\alpha$, $e_\mu=+1$, $\overline{e_\theta}=+1$, and $\alpha=\pi/5$ and $\pi/8$. For $e_\mu=+1$ and $\overline{e_\theta}=-1$, $Q(E)$ exceeds the upper curve in Fig. 4 for $\alpha=\pi/5$ and $\pi/8$, and can be ignored. For $e_\mu=-1$ and $\overline{e_\theta}=+1$, one gets $Q(E)<0$ for $E<0.37$, which is nonphysical. For $e_\mu=-1$ and $\overline{e_\theta}=-1$, one also gets $Q(E)<0$, which is nonphysical. Actually, Eqs. (113), (65), (12), (132)–(134), and (128) imply that E is in each case constant (independent of Q).

Comparing Figs. 1, 2, 3, and 4, one can conclude that for $\alpha=\pi/5$ and $\pi/8$, the minimum overlap Q is given by Eq. (137), corresponding to the lower curve in both Figs. 1 and 2. This is corroborated by Figs. 5 and 6, in which I plot, using Eqs. (B1), (B2), and (B4)–(B6) of Appendix B, the general expression for the overlap versus error rate for $R_?=\sin 2\alpha$, for a representative range of values for the nonoptimal probe parameters, and for $\alpha=\pi/5$ and $\pi/8$, respectively. The solid curve in both figures corresponds to the absolute minimum, Eq. (137). In all cases the nonoptimal values lie above the absolute minimum, as must be the case.

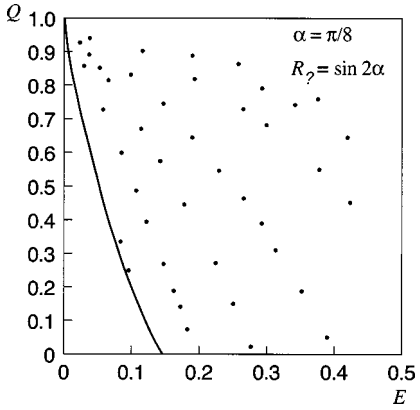

FIG. 6. Points correspond to the unoptimized overlap Q (Appendix B) versus the error rate E for $R_?=\sin 2\alpha$ and $\alpha=\pi/8$ for a range of values of nonoptimal probe parameters. The solid curve is the corresponding minimum overlap, Eq. (137).

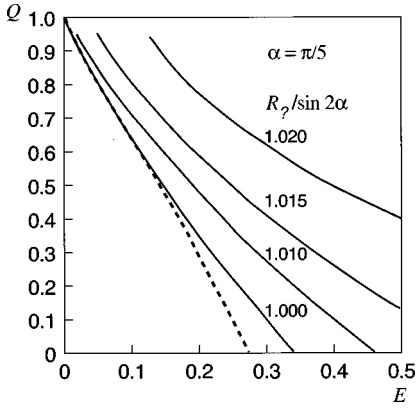

FIG. 7. Solid curves are the minimum overlap Q, Eq. (137), as a function of the error rate E for various values of the inconclusive rate $R_?$ for $\alpha=\pi/5$. The dashed curve is the minimum overlap for the fixed error rate only (Appendix C).

IV. ADVANTAGE OF MONITORING THE INCONCLUSIVE RATE

The minimum overlap Q of the correlated probe states as a function of error rate E and inconclusive rate $R_?$ for a range of system parameters is given by Eq. (137), together with Eqs. (77)–(82) and (64); and the corresponding maximum Renyi information gain by the probe is given by $I^B_{\rm opt}$, Eq. (83), together with Eq. (137). For the fixed error rate E only, with no restriction on the inconclusive rate, the minimum overlap is given parametrically in terms of γ by Eqs. (C1)–(C4) of Appendix C, and the corresponding maximum Renyi information gain is given by Eq. (83), together with Eqs. (C1)–(C4). In Figs. 7–10, I plot Eq. (137) and the corresponding Eq. (83) as a function of error rate for various values of the inconclusive rate $R_?$, and for $\alpha=\pi/5$ and $\pi/8$, respectively. Also plotted in Figs. 7–10 are Eqs. (C1)–(C4) of Appendix C, and the corresponding Eq. (83) as a function of the error rate (the dashed lowest curve for the overlap, and the dashed highest curve for the information gain). The maximum allowable information gain by the probe for the fixed error rate and fixed inconclusive rate is less than that at

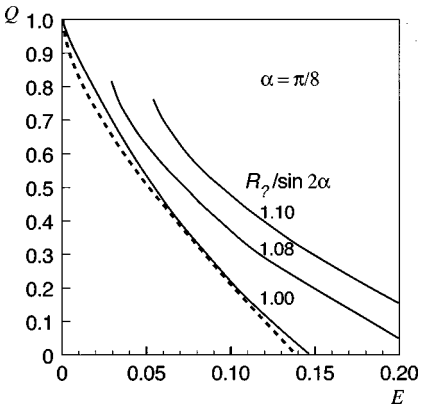

FIG. 8. Solid curves are the minimum overlap Q, Eq. (137), as a function of the error rate E for various values of the inconclusive rate $R_?$ for $\alpha=\pi/8$. The dashed curve is the minimum overlap for the fixed error rate only (Appendix C).

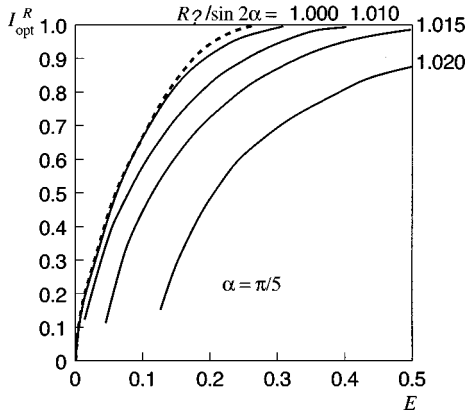

FIG. 9. Solid curves are the maximum Renyi information gain by the probe $I_{\rm opt}^R$, Eqs. (83) and (137), as a function of the error rate E for various values of the inconclusive rate $R_?$ for $\alpha=\pi/5$. The dashed curve is the maximum Renyi information gain by the probe for the fixed error rate only [Eqs. (83) and (C1)–(C4)].

the fixed error rate only, and decreases with an increasing inconclusive rate. One can conclude that by monitoring the inconclusive rate of the POVM receiver as well as the error rate, the achievable information gain by the probe can be reduced below that achievable when only the error rate is monitored. It then follows that fewer bits need be sacrificed in the process of key distillation if the inconclusive rate is also monitored. Also, by increasing the inconclusive-rate monitoring threshold, the achievable information gain can be further decreased.

In Figs. 11–14, I plot Eqs. (137) and (83) as a function of the inconclusive rate for various values of the error rate, and for $\alpha=\pi/5$ and $\pi/8$, respectively. In Fig. 13 for $\alpha=\pi/5$, the information gain is seen to monotonically decrease with an increasing value of the inconclusive-rate monitoring threshold. However, as in Fig. 14 for $\alpha=\pi/8$, the information gain may first increase before decreasing with an increasing inconclusive rate, in which case there is a least desirable inconclusive rate threshold exceeding $\sin 2\alpha$.

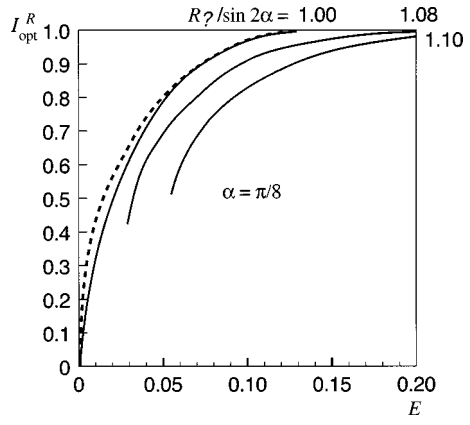

FIG. 10. Solid curves are the maximum Renyi information gain by the probe $I_{\rm opt}^R$, Eqs. (83) and (137), as a function of the error rate E for various values of the inconclusive rate $R_?$ for $\alpha=\pi/8$. The dashed curve is the maximum Renyi information gain by the probe for the fixed error rate only [Eqs. (83) and (C1)–(C4)].

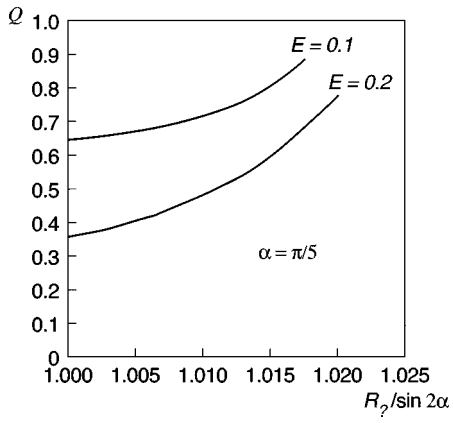

FIG. 11. Minimum overlap Q, Eq. (137), as a function of the inconclusive rate $R_?$ for various values of the error rate E and $\alpha=\pi/5$.

In the upper curve in Fig. 15, I plot as a function of α, for $R_?=\sin 2\alpha$, the fixed error rate $E_{\rm max}$ for which the information gain by the probe is unity (complete information). The dashed lower curve corresponds to the case in which the inconclusive rate is not fixed. One sees that the probe gains complete information at the price of inducing a larger error rate if the inconclusive rate is also monitored.

V. CONCLUSIONS

The inconclusive rate can be a useful disturbance measure in quantum cryptography. Here the maximum Renyi information gain by a disturbing eavesdropping probe is calculated analytically for fixed POVM-receiver error and inconclusive rates in the two-state protocol in the presence of an individual attack. The maximum Renyi information gain is given by Eq. (83), together with Eqs. (137), (77)–(82), and (64). It has been demonstrated that the maximum allowable information gain by the probe for the fixed error rate and fixed inconclusive rate is less than that for the fixed error rate only, and decreases with a suitably increasing inconclusive rate. It follows that by monitoring the inconclusive rate of the POVM receiver, as well as the error rate, the achievable

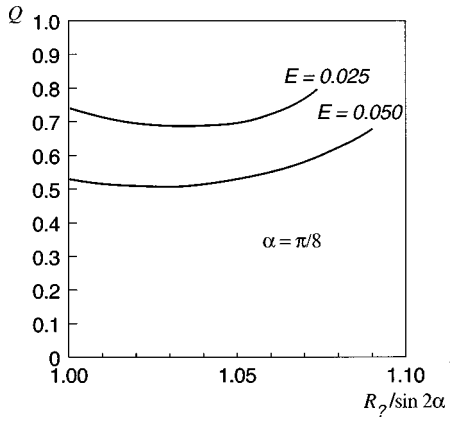

FIG. 12. Minimum overlap Q, Eq. (137), as a function of the inconclusive rate $R_?$ for various values of the error rate E and $\alpha=\pi/8$.

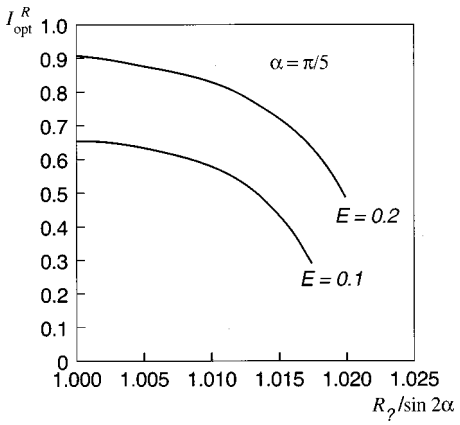

FIG. 13. Maximum Renyi information gain by the probe $I_{\rm opt}^R$, Eqs. (83) and (137), as a function of the inconclusive rate $R_?$ for various values of the error rate E and $\alpha = \pi/5$.

information gain by the probe can be reduced below that achievable when only the error rate is monitored. Also, by suitably increasing the inconclusive rate monitoring threshold, the achievable information gain can be further decreased.

ACKNOWLEDGMENTS

This work was supported by the U.S. Army Research Laboratory through Dr. John W. Lyons and his *Director's Research Initiative*. The author gratefully acknowledges the hospitality of the Isaac Newton Institute for Mathematical Sciences at the University of Cambridge, where part of this work was completed. The author wishes to especially thank Professor Peter Knight, FRS, for inviting him to participate in the program, *Complexity, Computation, and the Physics of Information* at the Newton Institute. Useful communications with J. D. Franson, J. D. Murley, and M. Kruger are gratefully acknowledged.

APPENDIX A: DISTURBED INCONCLUSIVE RATE

The Fuchs-Peres model of eavesdropping on the two-state key-distribution protocol represents the most general pos-

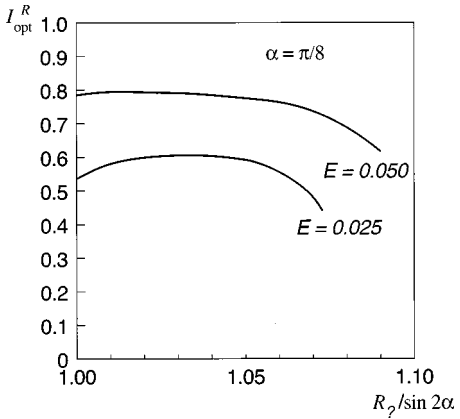

FIG. 14. Maximum Renyi information gain by the probe $I_{\rm opt}^R$, Eqs. (83) and (137), as a function of the inconclusive rate $R_?$ for various values of the error rate E and $\alpha = \pi/8$.

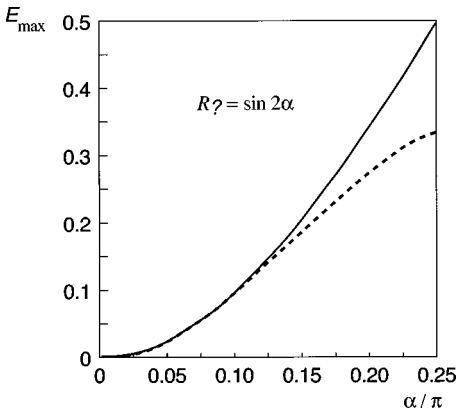

FIG. 15. The solid curve is the fixed error rate $E_{\rm max}$ which gives complete information, as a function of α, for the inconclusive rate $R_? = \sin 2\alpha$. The dashed curve corresponds to the case in which the inconclusive rate is not fixed (Appendix C).

sible unitary disturbance of each encoded photon incident on the receiver [2]. In this model, an incoming carrier state $|u\rangle$ and the state $|w\rangle$ of a disturbing probe undergo joint unitary evolution represented by a unitary operator U, resulting in the entangled state [1,2,5]:

$$\begin{aligned} U|u\otimes w\rangle = \tfrac{1}{2}\,[&(1+\sec 2\alpha)|\Phi_{00}\rangle + \tan 2\alpha|\Phi_{10}\rangle \\ &- \tan 2\alpha|\Phi_{01}\rangle + (1-\sec 2\alpha)|\Phi_{11}\rangle]\otimes|u\rangle \\ &- \tfrac{1}{2}\,[\tan 2\alpha|\Phi_{00}\rangle - (1-\sec 2\alpha)|\Phi_{10}\rangle \\ &- (1+\sec 2\alpha)|\Phi_{01}\rangle - \tan 2\alpha|\Phi_{11}\rangle]\otimes|v\rangle. \end{aligned} \tag{A1}$$

Here $|\Phi_{mn}\rangle$ are states in the Hilbert space of the disturbing probe, and are neither normalized nor orthogonal. Equation (A1) follows from Eqs. (1) and (2) of [1]. Similarly, for an incoming state $|v\rangle$, one has

$$\begin{aligned} U|v\otimes w\rangle = \tfrac{1}{2}\,[&\tan 2\alpha|\Phi_{00}\rangle + (1+\sec 2\alpha)|\Phi_{10}\rangle \\ &+ (1-\sec 2\alpha)|\Phi_{01}\rangle - \tan 2\alpha|\Phi_{11}\rangle]\otimes|u\rangle \\ &+ \tfrac{1}{2}\,[(1-\sec 2\alpha)|\Phi_{00}\rangle - \tan 2\alpha|\Phi_{10}\rangle \\ &+ \tan 2\alpha|\Phi_{01}\rangle + (1+\sec 2\alpha)|\Phi_{11}\rangle]\otimes|v\rangle. \end{aligned} \tag{A2}$$

The probe states $|\Phi_{mn}\rangle$ have certain symmetry properties that arise from the random equiprobable selection of carrier states $|u\rangle$ and $|v\rangle$ by the key transmitter, and the resulting symmetry of the probe under interchange of $|u\rangle$ and $|v\rangle$. Specifically, one has [1,2]

$$|\Phi_{00}| = |\Phi_{11}|, \tag{A3}$$

$$|\Phi_{01}| = |\Phi_{10}|, \tag{A4}$$

$$\langle\Phi_{00}|\Phi_{01}\rangle = \langle\Phi_{11}|\Phi_{10}\rangle, \tag{A5}$$

$$\langle\Phi_{00}|\Phi_{10}\rangle = \langle\Phi_{11}|\Phi_{01}\rangle, \tag{A6}$$

$$\langle\Phi_{01}|\Phi_{10}\rangle=\langle\Phi_{10}|\Phi_{01}\rangle, \tag{A7}$$

$$\langle\Phi_{01}|\Phi_{00}\rangle=\langle\Phi_{10}|\Phi_{11}\rangle, \tag{A8}$$

$$\langle\Phi_{01}|\Phi_{11}\rangle=\langle\Phi_{10}|\Phi_{00}\rangle, \tag{A9}$$

$$\langle\Phi_{11}|\Phi_{00}\rangle=\langle\Phi_{00}|\Phi_{11}\rangle. \tag{A10}$$

It has been shown in previous work [4,6–8] that the inconclusive rate $P_?$ of the POVM receiver, for an incoming state $|\psi\rangle$, is given by

$$P_?=\langle\psi|A_?|\psi\rangle. \tag{A11}$$

According to Eq. (A11), the inconclusive rate $R_?$ induced by the disturbing probe in the POVM receiver is given by

$$R_?=P_{u?}=\langle u\otimes w|U^\dagger A_? U|u\otimes w\rangle, \tag{A12}$$

where $P_{u?}$ is the probability that if a photon in polarization state $|u\rangle$ is transmitted, then the measurement by the POVM receiver is inconclusive. Equivalently, using Eq. (3) in Eq. (A12), one also has for the induced inconclusive rate

$$R_?=1-P_{uu}-P_{uv}, \tag{A13}$$

where P_{uu} and P_{uv} are the probabilities that if the carrier is a $|u\rangle$ state, then the detectors of u and v polarization states, respectively, respond. Here, one has

$$P_{uu}=\langle u\otimes w|U^\dagger A_u U|u\otimes w\rangle, \tag{A14}$$

$$P_{uv}=\langle u\otimes w|U^\dagger A_v U|u\otimes w\rangle. \tag{A15}$$

Substituting Eqs. (2), (A1), and (A3)–(A10) in Eq. (A15), one obtains

$$\begin{aligned}P_{uv}=(1+\sin 2\alpha)^{-1}[&(1-\sin^4\alpha-\cos^4\alpha)|\Phi_{00}|^2\\&+(1-\tfrac{1}{2}\sin^2 2\alpha)|\Phi_{01}|^2+\tfrac{1}{2}\sin 2\alpha\langle\Phi_{01}|\Phi_{11}\rangle\\&+\tfrac{1}{2}\sin 2\alpha\langle\Phi_{00}|\Phi_{10}\rangle-\tfrac{1}{2}\sin 2\alpha\langle\Phi_{00}|\Phi_{01}\rangle\\&-\tfrac{1}{2}\sin^2 2\alpha\langle\Phi_{00}|\Phi_{11}\rangle-\tfrac{1}{2}\sin 2\alpha\langle\Phi_{01}|\Phi_{00}\rangle\\&-\tfrac{1}{2}\sin^2 2\alpha\langle\Phi_{01}|\Phi_{10}\rangle].\end{aligned} \tag{A16}$$

The probe states $|\Phi_{mn}\rangle$, expanded in terms of orthonormal basis vectors $|w_\beta\rangle$, are given by Eqs. (3a), (3b), and (4) of [1], namely,

$$|\Phi_{00}\rangle=X_0|w_0\rangle+X_1|w_1\rangle+X_2|w_2\rangle+X_3|w_3\rangle, \tag{A17}$$

$$|\Phi_{11}\rangle=X_3|w_0\rangle+X_2|w_1\rangle+X_1|w_2\rangle+X_0|w_3\rangle, \tag{A18}$$

$$|\Phi_{01}\rangle=X_5|w_1\rangle+X_6|w_2\rangle, \tag{A19}$$

$$|\Phi_{10}\rangle=X_6|w_1\rangle+X_5|w_2\rangle. \tag{A20}$$

Here the real coefficients $\{X_0,X_1,X_2,X_3,X_5,X_6\}$, expressed in terms of the probe parameters $\{\lambda,\mu,\theta,\phi\}$, are [1,2]

$$X_0=\sin\lambda\cos\mu, \tag{A21}$$

$$X_1=\cos\lambda\cos\theta\cos\phi, \tag{A22}$$

$$X_2=\cos\lambda\cos\theta\sin\phi, \tag{A23}$$

$$X_3=\sin\lambda\sin\mu, \tag{A24}$$

$$X_5=\cos\lambda\sin\theta\cos\phi, \tag{A25}$$

$$X_6=-\cos\lambda\sin\theta\sin\phi, \tag{A26}$$

consistent with the assumed unitarity of the disturbing probe.

Next, substituting Eqs. (A17)–(A26) in Eq. (A16), one gets

$$\begin{aligned}P_{uv}=\tfrac{1}{4}(1+\sin 2\alpha)^{-1}[&1-\cos 4\alpha+2(1+\cos 4\alpha)\\&\times\cos^2\lambda\sin^2\theta-2\sin 2\alpha\cos^2\lambda\sin 2\theta\cos 2\phi\\&-2\sin^2 2\alpha\sin^2\lambda\sin 2\mu\\&-2\sin^2 2\alpha\cos^2\lambda\cos 2\theta\sin 2\phi].\end{aligned} \tag{A27}$$

Analogously, it can be shown that Eq. (A14) becomes

$$\begin{aligned}P_{uu}=\tfrac{1}{2}(1-\sin 2\alpha)[&2\sin^2\lambda+2\cos^2\lambda\cos^2\theta+\tan^2 2\alpha\\&-\tan 2\alpha\sec 2\alpha\cos^2\lambda\sin 2\theta\cos 2\phi\\&-\tan^2 2\alpha(\sin^2\lambda\sin 2\mu+\cos^2\lambda\cos 2\theta\sin 2\phi)].\end{aligned} \tag{A28}$$

Next, substituting Eqs. (A27) and (A28) in Eq. (A13), one obtains, after extensive algebraic reduction, the following expression for the inconclusive rate induced by the disturbing probe:

$$\begin{aligned}R_?=\sin 2\alpha(1+\sin 2\alpha)^{-1}[&1+\cos^2\lambda\sin 2\theta\cos 2\phi\\&+(\sin^2\lambda\sin 2\mu+\cos^2\lambda\cos 2\theta\sin 2\phi)\sin 2\alpha],\end{aligned} \tag{A29}$$

expressed in terms of the angle α, Eq. (5), and the probe parameters λ, μ, θ, and ϕ [12].

APPENDIX B: NONOPTIMIZED OVERLAP

Using Eqs. (22), (24), (65), (12), and (53) in Eq. (75), one can show that

$$\begin{aligned}Q=\frac{1}{2(1-E)}\Bigg\{&\frac{1}{1-\cos 2\theta}[2\sin 2\mu(1-2E\\&-\rho\cos^2 2\alpha\cos 2\theta)+\rho\cos^2 2\alpha[1+\sin 2\phi-\cos 2\theta\\&\times(1-\sin 2\phi)]-\sin 2\phi(1+\cos 2\theta)(1-2E)]-1\Bigg\}.\end{aligned} \tag{B1}$$

Here the parameter ρ is given by Eq. (64). Also, using Eqs. (13), (10), (11), (65), (22), and (24) in Eq. (12), it follows that

$$E=\tfrac{1}{2}\,[\csc 2\alpha \sin 2\theta \cos 2\phi+\cos 2\theta \sin 2\phi-\sin 2\mu]^{-1}$$
$$\times[(\rho-1)\cot^2 2\alpha(1-\cos 2\theta)-(1-\rho\cos^2 2\alpha\cos 2\theta)$$
$$\times\sin 2\mu+(1-\rho\cos^2 2\alpha)(\csc 2\alpha\sin 2\theta\cos 2\phi$$
$$+\cos 2\theta\sin 2\phi)]. \tag{B2}$$

One also requires in Eqs. (B1) and (B2) that

$$d\geqslant\cos 2\theta, \tag{B3}$$

in order that in Eq. (24), $\sin^2\lambda\geqslant 0$, as must clearly be the case. Substituting Eqs. (65) and (12) in Eq. (B3), one therefore requires

$$0\leqslant E\leqslant\tfrac{1}{2}\,(1-\rho\cos^2 2\alpha\cos 2\theta). \tag{B4}$$

The left-hand side of the inequality follows from the physical nature of the error rate. Equations (B1), (B2), (64), and (B4) parametrically determine the dependence of the unoptimized overlap Q on the error rate E, both expressed in terms of the angle α characterizing the nonorthogonal states of the signal, the inconclusive rate $R_?$, and the probe parameters θ, ϕ, and μ. Because of the periodicity in θ, ϕ, and μ in Eqs. (B1), (B2), and (B4), one need only consider

$$0\leqslant\theta\leqslant\pi;\quad 0\leqslant\phi\leqslant\pi;\quad 0\leqslant\mu\leqslant\pi. \tag{B5}$$

Of course, one also has the physical requirement

$$0\leqslant Q\leqslant 1. \tag{B6}$$

APPENDIX C: MINIMUM OVERLAP FOR THE FIXED ERROR RATE ONLY

If only the error rate is fixed (with no constraint on the inconclusive rate), then the minimum overlap Q as a function of error rate E, for both a PV receiver [1] and the POVM receiver [5], is given parametrically in terms of the parameter γ by Eqs. (11–13) of [1]. The latter can be shown to reduce to the following equations, parametric in γ:

$$Q=[\cos^2 2\alpha+f_1(\gamma)-f_2(\gamma)]^{-1}\{(1+\sin^2 2\alpha)^{1/2}$$
$$\times(\sin\gamma\csc 2\alpha-\cos\gamma\sin^2 2\alpha)$$
$$+(1+\sin^2 2\alpha)\sin\gamma\cos\gamma\cos 2\alpha\cot 2\alpha+f_2(\gamma)\} \tag{C1}$$

and

$$E=\tfrac{1}{2}\,\{1-\cos^2 2\alpha[f_1(\gamma)-f_2(\gamma)]^{-1}\} \tag{C2}$$

where

$$f_1(\gamma)=(1+\sin^2 2\alpha)^{1/2}(\cos\gamma-\sin\gamma\sin 2\alpha) \tag{C3}$$

and

$$f_2(\gamma)=\sin 2\alpha[\cos^4\gamma\sin^2 2\alpha+\sin^4\gamma\csc^2 2\alpha$$
$$-2\sin^2\gamma\cos^2\gamma]^{1/2}. \tag{C4}$$

[1] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[2] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., Phys. Rev. A **56**, 4456 (1997); **58**, 2617 (1998).
[5] H. E. Brandt, Phys. Rev. A **59**, 2665 (1999).
[6] H. E. Brandt, Am. J. Phys. **67**, 434 (1999).
[7] J. M. Myers and H. E. Brandt, Meas. Sci. Technol. **8**, 1222 (1997).
[8] H. E. Brandt, Prog. Quantum Electron. **22**, 257 (1998).
[9] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[10] A. Peres, Phys. Lett. A **128**, 19 (1988).
[11] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[12] H. E. Brandt, Newton Institute Report No. NI99015-CCP, University of Cambridge, Isaac Newton Institute for Mathematical Sciences, Cambridge, UK [Contemporary Math. (to be published)].
[13] H. E. Brandt and J. M. Myers, US Patent No. 5,999,285 (7 December 1999).
[14] D. R. Smith, *Variational Methods in Optimization* (Dover, Mineola, NY, 1998).