Inconclusive rate in quantum key distribution

Howard E. Brandt
U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, Maryland 20783
(Received 1 June 2001; published 18 September 2001)

After summarizing a recent calculation of the maximum Renyi information loss (for fixed error and inconclusive rates) from a positive operator valued measure (POVM) quantum cryptographic receiver to a general unitary probe, I calculate the worst inconclusive rate for the legitimate receiver. Disturbed inconclusive rates are considered which are less, as well as greater, than the unperturbed inconclusive rate. I also demonstrate that for an optimized individual attack there is a minimum induced error rate which is fixed by the induced inconclusive rate.

DOI: 10.1103/PhysRevA.64.042316 PACS number(s): 03.67.Dd, 03.67.-a, 03.67.Hk, 03.65.Ta

I. INTRODUCTION

Recently the maximum Renyi information gain by a general unitary disturbing eavesdropping probe was calculated analytically for fixed positive operator valued measure (POVM)-receiver error and inconclusive rates in the two-state protocol of quantum key distribution in the presence of an individual attack [1,2]. It was demonstrated that the maximum allowable information gain by the probe for fixed error rate (on sifted bits) and fixed inconclusive rate is generally less than that for fixed error rate only, and decreases with a suitably increasing inconclusive rate. Here, information gain by the probe corresponds to information loss from the POVM receiver [3,4].

The maximum Renyi information gain by the eavesdropper, at fixed error and inconclusive rates, is given by [1,2]

$$I^R_{\rm opt}=\log_2(2-Q^2), \tag{1}$$

where Q, the minimum overlap of the correlated probe states, is given by

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

Here the parameter ϵ is expressed in terms of the error rate E by

$$\epsilon=1-2E \tag{3}$$

and the following functions, depending on the error rate and the inconclusive rate, are defined as

$$f(\epsilon)=\frac{\alpha(\epsilon)}{\beta(\epsilon)}, \tag{4}$$

$$g(\epsilon)=\frac{\delta(\epsilon)}{\alpha(\epsilon)}, \tag{5}$$

$$\alpha(\epsilon)=\rho^3\cos^4 2\alpha-\rho(1-\rho)(\cos^2 2\alpha)\epsilon-(1-\rho\sin^2 2\alpha)\epsilon^2, \tag{6}$$

$$\beta(\epsilon)=\rho^2\cos^2 2\alpha-\epsilon^2, \tag{7}$$

$$\begin{aligned}\delta(\epsilon)=\cos^2 2\alpha\{&\rho^2(1-\rho)^2\csc^2 2\alpha\cos^4 2\alpha+[2\rho(1-\rho)\\&\times(1-\rho-\rho\sin^2 2\alpha)\cot^2 2\alpha-2\rho^3\cos^2 2\alpha]\epsilon\\&+[(1-\rho-\rho\sin^2 2\alpha)^2\csc^2 2\alpha-\rho^2]\epsilon^2\\&+2\rho(\sec^2 2\alpha)\epsilon^3+(\sec^4 2\alpha)\epsilon^4\},\end{aligned} \tag{8}$$

where α [not to be confused with the function $\alpha(\epsilon)$] is half the complement of the angle θ between the two nonorthogonal linear-polarization states of the signal,

$$\alpha=\frac{1}{2}\left(\frac{\pi}{2}-\theta\right), \tag{9}$$

and the inconclusive rate $R_?$ enters only through the parameter ρ,

$$\rho=\frac{1}{(1+\sin 2\alpha)(1-R_?)}. \tag{10}$$

The optimization resulting in Eqs. (1)–(10) was obtained by comparing all possible relative extrema of the corresponding Lagrange function, on the basis of parametric analysis for inconclusive rates equal to, or exceeding, the unperturbed value, $\sin 2\alpha$ [1]. In the present work, in the process of determining the so-called worst inconclusive rate, inconclusive rates less than the unperturbed value are also addressed, and the same optimization, Eqs. (1)–(10), is shown to apply.

In Sec. II the worst inconclusive rate (from the point of view of the legitimate receiver) is defined and determined numerically. In Sec. III the optimization given by Eqs. (1)–(10) is shown to apply for inconclusive rates less than, as well as greater than, the unperturbed value. A minimum induced error rate, which is fixed by the induced inconclusive rate, is also determined. In Sec. IV an analytical expression is obtained for the worst inconclusive rate. Section V contains a summary.

II. WORST INCONCLUSIVE RATE

In Sec. IV of [1], parametric analysis was presented of the dependence of the maximum information gain by the eavesdropper, at fixed error and inconclusive rates, as a function of the inconclusive rate and for various values of the error rate.

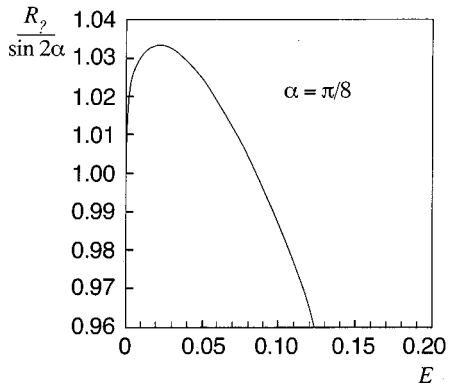

FIG. 1. Worst inconclusive rate $R_?$ as a function of the error rate E for $\alpha=\pi/8$, and corresponding to the solution of Eq. (11).

It was pointed out that, as the inconclusive rate increases while the error rate is held constant, the Renyi information gain possible for an eavesdropper may first increase and then decrease, in which case there is an inconclusive rate at which the eavesdropper gains maximum Renyi information for a fixed error rate. Taking the point of view of the legitimate receiver, I call this the ''worst inconclusive rate'' for a given error rate. Thus in Fig. 14 of [1], $I^R_{\rm opt}$, plotted as a function of $R_?$ for fixed E, peaks at a particular inconclusive rate, that is, for $R_?$ such that

$$\frac{\partial I^R_{\rm opt}}{\partial R_{?|E}}=0, \tag{11}$$

where $I^R_{\rm opt}$ is given by Eqs. (1)–(10). The solution to Eq. (11) determines for a fixed error rate E the inconclusive rate $R_?$ for which $I^R_{\rm opt}$ is maximal. If one directly substitutes Eqs. (1)–(10) in Eq. (11), one obtains a rather formidable appearing equation to solve for the extremum. I have solved Eq. (11) numerically, by picking off the peaks while varying E, and the result is shown in Fig. 1, giving the worst inconclusive rate $R_?$ as a function of error rate E for $\alpha=\pi/8$.

In Sec. IV an algebraic expression is obtained which also yields the identical curve in Fig. 1, and is an analytical solution to Eq. (11). However, to support the arguments leading to the analytical solution, it is necessary to first reconsider the optimization given in [1] for inconclusive rates less than the unperturbed value, $\sin 2\alpha$, since explicit parametric analysis in [1] was limited to inconclusive rates equaling or exceeding the unperturbed value. (Note that inconclusive rates less than the unperturbed value are included in Fig. 1.) Generally, the eavesdropping probe can induce inconclusive rates in the POVM receiver, less than, as well as exceeding, the unperturbed value.

III. INCONCLUSIVE RATES LESS THAN THE UNPERTURBED VALUE

Possible extrema for the optimization at fixed error and inconclusive rates are given by Eqs. (42), (76), (104), (117) with (118), (126), and (136) of [1]. For inconclusive rates equaling or exceeding the unperturbed value, it was argued in [1] that for $R_?\geqslant\sin 2\alpha$, Eq. (137) or, equivalently, Eq. (76) with the minus sign choice [or Eq. (2) above], along with Eq. (83) of [1] [or Eq. (1) above] give the minimum overlap Q of correlated probe states and the maximum Renyi information gain by the eavesdropper, respectively. It can be shown that if one plots the general expression for the nonoptimized overlap [Eqs. (B1), (B2), and (B4)–(B6) of Appendix B in [1]] versus the error rate for $R_?\geqslant\sin 2\alpha$, $\alpha=\pi/8$, and for a representative range of values of the nonoptimized probe parameters, the nonoptimized values of Q all lie above the corresponding solid curves in Fig. 8 of [1], as must be the case. (This was shown explicitly in Fig. 6 of [1] for $R_?=\sin 2\alpha$.) Furthermore, Eq. (76) of [1] with the plus sign choice yields values of Q exceeding those for the minus sign choice. Equations (42) and (104), for $R_?\geqslant\sin 2\alpha$, also fail to yield the minimum overlap and maximum information because they each yield $Q\geqslant 1$, which is nonphysical for $Q>1$ since, physically, one requires $|Q|\leqslant 1$, and $Q=1$ corresponds to perfect information in Eq. (1). (Here $|Q|$ denotes the absolute value of Q.)

It was also argued in [1] that for $R_?=\sin 2\alpha$, Eqs. (117) with (118) fail to give a minimum for $e_\mu=-1$ and $e_\theta=\pm 1$, since they yield $|Q|\geqslant 1$; and they also fail for $e_\mu=1$ and $e_\theta=\pm 1$, since they yield $E=0$. It can also be shown that for $(R_?/\sin 2\alpha)=1.08$, 1.10, Eq. (117) with Eq. (118) fail to give a minimum for $e_\mu=-1$ and $e_\theta=\pm 1$, since they again yield $|Q|\geqslant 1$.

Before considering Eqs. (117) and (118) of [1] for $R_?>\sin 2\alpha$ and $e_\mu=1$ and $e_\theta=\pm 1$, it is useful to observe that according to Eq. (24) of [1], one requires

$$\cos 2\theta\leqslant d\leqslant 1, \tag{12}$$

because, trigonometrically, $0\leqslant\sin^2\lambda\leqslant 1$. But according to Eqs. (17) and (12) of [1], one has

$$d=\frac{(1-R_?)(1-2E)}{1-\sin 2\alpha}. \tag{13}$$

Then substituting Eq. (13) in Eq. (12), one obtains

$$\frac{\sin 2\alpha-R_?}{2(1-R_?)}\leqslant E\leqslant\frac{1}{2}\left(1-\frac{1-\sin 2\alpha}{1-R_?}\cos 2\theta\right). \tag{14}$$

[The upper limit in Eq. (14) is equivalent to Eq. (B4) of [1].] Equation (14) is a general constraint on the error rate, which must be satisfied.

For $(R_?/\sin 2\alpha)=1.08$, 1.10, Eq. (117) with Eq. (118) of [1] also fail to give a minimum for $e_\mu=1$ and $e_\theta=\pm 1$, since the upper limit in Eq. (14) [along with Eqs. (108) and (109) of [1]] must be satisfied, and it can then be shown that Q exceeds that given by Eq. (2). Equations (126) and (136) of [1] also fail to yield the minimum overlap for $(R_?/\sin 2\alpha)=1.00$, 1.08, 1.10, since for them E is constant, and the corresponding single value of Q is nonphysical or exceeds the value of Q given by Eq. (137) of [1] [or Eq. (2) above].

It should be noted here that in [1], negative values of Q were improperly described as nonphysical. Clearly, the overlap (Dirac bracket) Q can be negative provided $|Q|\leqslant 1$, and

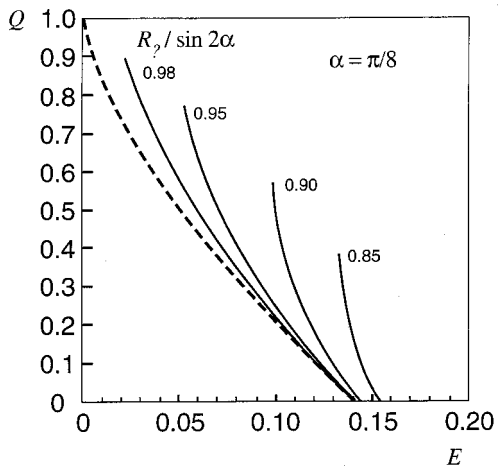

FIG. 2. Solid curves are the minimum overlap Q, Eq. (2), as a function of the error rate E for various values of the inconclusive rate $R_?$ less than the unperturbed value $\sin 2\alpha$ and for $\alpha=\pi/8$. The dashed curve is the minimum overlap for the fixed error rate only (as in Fig. 8 of [1]).

the maximum Renyi information according to Eq. (1) effectively depends on $|Q|$; however, negative Q can generally be effectively ignored if the minimum Q is positive for low error rates and decreases with the error rate E, since vanishing Q corresponds to perfect information, according to Eq. (1).

The parametric analysis in [1] did not explicitly address inconclusive rates less than the unperturbed value. In Fig. 2 I plot Q given by Eq. (2) as a function of E for $R_?<\sin 2\alpha$ and $\alpha=\pi/8$, and represented by the solid curves for $(R_?/\sin 2\alpha)=0.98, 0.95, 0.90, 0.85$. Also plotted in Fig. 2 is the dashed curve corresponding to Q for fixed error rate only, as given by Eqs. (C1)–(C4) of [1] (also the dashed curve in Fig. 8 of [1]). As in Fig. 8 of [1], the curves in Fig. 2 have a least possible value E_0 of the error rate. This is the case, since according to Eq. (2), for $E<E_0$, Q becomes complex. This occurs for E such that

$$g(\epsilon)>f(\epsilon), \tag{15}$$

and the value E_0 is given by solving for E_0 such that

$$g(\epsilon)_{|E_0}=f(\epsilon)_{|E_0}, \tag{16}$$

in which the functions $f(\epsilon)$ and $g(\epsilon)$ are both evaluated at $E=E_0$. But it can be shown numerically that for inconclusive rates less than the unperturbed value, the lower bound in Eq. (14) solves Eq. (16). Therefore one has

$$E_0=\frac{\sin 2\alpha-R_?}{2(1-R_?)} \tag{17}$$

for

$$R_?<\sin 2\alpha. \tag{18}$$

Thus for inconclusive rates less than the unperturbed value, one has

$$E\geqslant E_0, \tag{19}$$

where E_0 is given by Eq. (17). One can conclude that in the optimized individual attack there is a minimum induced error rate E_0 which is fixed by the inconclusive rate. According to Eq. (17), when the inconclusive rate assumes its unperturbed value, $\sin 2\alpha$, the minimum error rate E_0 is vanishing (as is to be expected), but the minimum error rate increases with decreasing inconclusive rate less than the unperturbed value. Also, from Fig. 8 of [1], it can be seen that the minimum error rate increases with an increasing inconclusive rate greater than the unperturbed value.

Next, by parametric analysis, one can demonstrate that for $R_?<\sin 2\alpha$, Eq. (76) with the plus sign choice yields values of Q exceeding those given by Eq. (2). Also, for error rates E satisfying the constraint Eq. (19), all values of Q in Eqs. (42) and (104) of [1] for $(R_?/\sin 2\alpha)=0.98, 0.95, 0.90, 0.85$, and $\alpha=\pi/8$, exceed Q given by Eq. (2) above. Also the values of Q in Eq. (117) with Eq. (118) of [1] for $\alpha=\pi/8$, $(R_?/\sin 2\alpha)=0.98, 0.95, 0.90, 0.85$, $e_\mu=\pm 1$, and $e_\theta=\pm 1$, and satisfying the constraint Eq. (19), exceed Q given by Eq. (2), or $|Q|\geqslant 1$. Also, Eqs. (126) and (136) of [1], for $R_?<\sin 2\alpha$, again fail to yield the minimum overlap, for the same reasons stated above for $R_?\geqslant\sin 2\alpha$. Furthermore, it can be shown that if one plots the general expression for the nonoptimized overlap [Eqs. (B1), (B2), and (B4)–(B6) of Appendix B in [1]) versus the error rate for inconclusive rate less than the unperturbed value, and for a representative range of values of the nonoptimized probe parameters, with $\alpha=\pi/8$, and enforces the necessary constraint Eq. (19), the nonoptimized values of Q all lie above the corresponding curves given by Eq. (2), as must be the case. One concludes that also for inconclusive rates less than the unperturbed value, Eq. (18), it is true that Eq. (2) (plotted in Fig. 2) gives the absolute minimum overlap of correlated probe states for fixed error and inconclusive rates. The corresponding maximum Renyi information gain by the eavesdropper is given by Eq. (1).

In Fig. 2 it can be seen that the solid curves, corresponding to the optimization for fixed error and inconclusive rates, all lie above the dashed curve, corresponding to the optimization for the fixed error rate only (as in Fig. 8 of [1]). Thus the Renyi information gain by the eavesdropper for the fixed error and inconclusive rates is less than that for the fixed error rate only, for inconclusive rates less, as well as greater, than the unperturbed value. It is important for the following to also observe that the solid curves in Fig. 2, corresponding to the fixed error rate and inconclusive rate, approach the dashed curve, corresponding to the fixed error rate only, but never fall below it.

IV. ANALYTICAL EXPRESSION FOR THE WORST INCONCLUSIVE RATE

In Eqs. (1)–(10), and correspondingly in Fig. 2 and Fig. 8 of [1], if the fixed inconclusive rate $R_?$ is chosen to be that given by Eqs. (9)–(11) of [1], evaluated at the optimum probe parameters λ, μ, θ, ϕ corresponding to the optimization for fixed error rate only [5,6], then the optimum at the

fixed error rate and inconclusive rate becomes equivalent to that at the fixed error rate only. This is corroborated by the fact that in Fig. 2 here, and in Fig. 8 of [1], the solid curves approach the dashed curve. It is also important to note that the solid curves never fall below the dashed curve. These facts enable one to find an exact fit to the curve in Fig. 1 and consequently an analytical solution to Eq. (11). To proceed then, we recall that 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 the POVM receiver, is given parametrically in terms of a parameter γ by Eqs. (11)–(13) of [5],

$$Q=\frac{(a+b)-(1+b)\sin^2 2\alpha+c\sin 2\alpha}{(1+d)+(-d-a)\sin^2 2\alpha-c\sin 2\alpha}, \tag{20}$$

$$E=\frac{1}{2}\left(1-\frac{d\cos^2 2\alpha}{1-a\sin^2 2\alpha-c\sin 2\alpha}\right), \tag{21}$$

where a, b, c, and d are given in terms of the eavesdropping probe parameters, λ, μ, θ, and ϕ by

$$a=\sin^2\lambda\sin 2\mu+\cos^2\lambda\cos 2\theta\sin 2\phi, \tag{22}$$

$$b=\sin^2\lambda\sin 2\mu+\cos^2\lambda\sin 2\phi, \tag{23}$$

$$c=\cos^2\lambda\sin 2\theta\cos 2\phi, \tag{24}$$

$$d=\sin^2\lambda+\cos^2\lambda\cos 2\theta, \tag{25}$$

and for the optimization, the probe parameters are given by

$$\lambda=0, \tag{26}$$

$$\mu=0, \tag{27}$$

$$\sin 2\phi=\frac{\sin\gamma}{\sin\delta}, \tag{28}$$

$$\cos 2\theta=\frac{\cos\delta}{\cos\gamma}, \tag{29}$$

where the parameters γ and δ are defined by

$$-\delta\leqslant\gamma\leqslant\delta, \tag{30}$$

$$\sin\delta=\frac{\sin 2\alpha}{(1+\sin^2 2\alpha)^{1/2}}, \tag{31}$$

$$\cos\delta=(1+\sin^2 2\alpha)^{-1/2}. \tag{32}$$

Here,

$$0<\delta<\pi/4, \tag{33}$$

$$\cos 2\phi\geqslant 0, \tag{34}$$

and

$$\sin 2\theta\geqslant 0. \tag{35}$$

Substituting Eqs. (26)–(32) in Eq. (22), one gets

$$a=\frac{\tan\gamma}{\sin 2\alpha}. \tag{36}$$

Also, substituting Eqs. (26)–(28), and (31) in Eq. (23), one gets

$$b=\frac{\sin\gamma}{\sin 2\alpha}(1+\sin^2 2\alpha)^{1/2}. \tag{37}$$

Then substituting Eqs. (26) and (28)–(35) in Eq. (24), one gets

$$c=\left[1-\frac{1}{(1+\sin^2 2\alpha)\cos^2\gamma}-\frac{\sin^2\gamma}{\sin^2 2\alpha}(1+\sin^2 2\alpha)+\frac{\tan^2\gamma}{\sin^2 2\alpha}\right]^{1/2}. \tag{38}$$

Also, substituting Eqs. (26), (29), and (32) in Eq. (25), one gets

$$d=\frac{1}{\cos\gamma(1+\sin^2 2\alpha)^{1/2}}. \tag{39}$$

Next substituting Eqs. (36)–(39) in Eq. (20), it follows that the minimum overlap of correlated probe states, at the fixed error rate only, is given by

$$Q=[\cos^2 2\alpha+f_1(\gamma)-f_2(\gamma)]^{-1}\{(1+\sin^2 2\alpha)^{1/2}\times(\sin\gamma\csc 2\alpha-\cos\gamma\sin^2 2\alpha)+(1+\sin^2 2\alpha)\times\sin\gamma\cos\gamma\cos 2\alpha\cot 2\alpha+f_2(\gamma)\}, \tag{40}$$

expressed in terms of the parameter γ, and the functions $f_1(\gamma)$ and $f_2(\gamma)$ are given by

$$f_1(\gamma)=(1+\sin^2 2\alpha)^{1/2}(\cos\gamma-\sin\gamma\sin 2\alpha), \tag{41}$$

and

$$f_2(\gamma)=\sin 2\alpha[\cos^4\gamma\sin^2 2\alpha+\sin^4\gamma\csc^2 2\alpha-2\sin^2\gamma\cos^2\gamma]^{1/2}, \tag{42}$$

respectively. The parameter γ, appearing in the parametric Eqs. (40)–(42), is defined by Eqs. (30)–(33). Next substituting Eqs. (36), (38), and (39) in Eq. (21), one can show that the corresponding error rate is given by

$$E=\tfrac{1}{2}\{1-\cos^2 2\alpha[f_1(\gamma)-f_2(\gamma)]^{-1}\}, \tag{43}$$

also expressed in terms of the parameter γ. Equations (40)–(43) determine the minimum overlap Q (for fixed error rate only) as a function of error rate E, expressed parametrically in terms of the parameter γ.

Next, substituting Eq. (39) in Eq. (13), and solving for the corresponding disturbed inconclusive rate $R_?$, one obtains

$$R_? = 1 - \frac{\cos^2 2\alpha}{(1-2E)\cos\gamma(1+\sin 2\alpha)(1+\sin^2 2\alpha)^{1/2}}. \tag{44}$$

Furthermore, substituting Eq. (43) in Eq. (44), one obtains the following expression for the disturbed inconclusive rate for the optimization at the fixed error rate:

$$R_? = 1 - \frac{f_1(\gamma) - f_2(\gamma)}{\cos\gamma(1+\sin 2\alpha)(1+\sin^2 2\alpha)^{1/2}}, \tag{45}$$

also expressed in terms of the parameter γ. Equations (45) and (43) determine the disturbed inconclusive rate $R_?$ as a function of the error rate E, expressed parametrically in terms of the parameter γ for the case of maximum information gain by the eavesdropper for the fixed error rate only. This function is plotted in Fig. 1 and the corresponding curve is indistinguishable from that corresponding to the numerical solution of Eq. (11), as discussed in Sec. II. This is remarkable, since directly attempting to analytically solve Eq. (11) apparently requires that a very complicated equation be solved for $R_?$ in terms of E.

One can check that the parametric Eqs. (43) and (45) do in fact satisfy Eq. (11) for all pertinent γ (as they must). To see this, one first notes that according to Eqs. (1), (2), and (10), the left-hand side of Eq. (11) is given by

$$\frac{\partial I^R_{\rm opt}}{\partial R_{?|E}} = \frac{dI^R_{\rm opt}}{dQ}\frac{\partial Q}{\partial \rho_{|E}}\frac{\partial \rho}{\partial R_?}. \tag{46}$$

From Eq. (1), it follows that

$$\frac{dI^R_{\rm opt}}{dQ} = -2(\log_2 e)\frac{Q}{2-Q^2}. \tag{47}$$

Also, according to Eq. (10), one has

$$\frac{\partial \rho}{\partial R_?} = \frac{1}{(1+\sin 2\alpha)(1-R_?)^2}. \tag{48}$$

Furthermore, using Eqs. (2) and (3), one can show that

$$\frac{\partial Q}{\partial \rho_{|E}} = \frac{1}{1+\epsilon}\left(1-\frac{g}{f}\right)^{-1/2}\left\{\left[\left(1-\frac{g}{f}\right)^{1/2} + \frac{g}{2f} - 1\right]\frac{\partial f}{\partial \rho_{|\epsilon}} + \frac{1}{2}\frac{\partial g}{\partial \rho_{|\epsilon}}\right\}. \tag{49}$$

According to Eq. (4), one has

$$\frac{\partial f}{\partial \rho_{|\epsilon}} = \frac{1}{\beta}\frac{\partial \alpha}{\partial \rho_{|\epsilon}} - \frac{\alpha}{\beta^2}\frac{\partial \beta}{\partial \rho_{|\epsilon}}. \tag{50}$$

Also, Eq. (5) yields

$$\frac{\partial g}{\partial \rho_{|\epsilon}} = \frac{1}{\alpha}\frac{\partial \delta}{\partial \rho_{|\epsilon}} - \frac{\delta}{\alpha^2}\frac{\partial \alpha}{\partial \rho_{|\epsilon}}. \tag{51}$$

Using Eq. (6), one obtains

$$\frac{\partial \alpha}{\partial \rho_{|\epsilon}} = 3\rho^2\cos^4 2\alpha + [(2\rho-1)\cos^2 2\alpha]\epsilon + (\sin^2 2\alpha)\epsilon^2. \tag{52}$$

Also, Eq. (7) yields

$$\frac{\partial \beta}{\partial \rho_{|\epsilon}} = 2\rho\cos^2 2\alpha. \tag{53}$$

Furthermore, using Eq. (8), one can show that

$$\frac{\partial \delta}{\partial \rho_{|\epsilon}} = \cos^2 2\alpha\{2\rho(1-\rho)(1-2\rho)\cos^2 2\alpha\cot^2 2\alpha + 2[(1-\rho)(1-3\rho)\cot^2 2\alpha - 2\rho\cos^2 2\alpha]\epsilon - 2[(1-\rho)\times(\csc^2 2\alpha + 1) - \rho\sin^2 2\alpha]\epsilon^2 + 2(\sec^2 2\alpha)\epsilon^3\}. \tag{54}$$

Substituting Eqs. (47)–(54), (43), and (45) in Eq. (46), and evaluating the latter numerically for a range of pertinent values of γ, one can show that Eq. (11) is in fact satisfied.

V. CONCLUSION

The worst inconclusive rate $R_?$ has been calculated analytically as a function of the error rate E, and corresponding to the maximum Renyi information loss by the POVM receiver at fixed error and inconclusive rates. The result is given by the parametric Eqs. (45) and (43) expressed in terms of the parameter γ. It was argued that the optimization given by Eqs. (1)–(10) holds for inconclusive rates less, as well as greater, than the unperturbed value. Also, it was shown that for the optimized individual attack there is a minimum induced error rate which is fixed by the induced inconclusive rate.

ACKNOWLEDGMENTS

This work was supported by the U.S. Army Research Laboratory and the Defense Advanced Research Projects Agency.

[1] H. E. Brandt, Phys. Rev. A **62**, 042310 (2000).
[2] H. E. Brandt, University of Cambridge, Isaac Newton Institute for Mathematical Sciences Report No. NI99015-CCP, 1999 [Contemp. Math. (to be published)].
[3] H. E. Brandt, Am. J. Phys. **67**, 434 (1999).
[4] H. E. Brandt, Prog. Quantum Electron. **22**, 257 (1998).
[5] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[6] H. E. Brandt, Phys. Rev. A **59**, 2665 (1999).