Inconclusive Rate with a Positive Operator Valued Measure

Howard E. Brandt

Abstract. Analysis is performed of explict optical implementations of both a positive operator valued measure (POVM) and of randomly choosing between two ordinary von Neumann projective measures. The POVM is demonstrated to have the lower inconclusive rate. Also, the effect of a general unitary disturbance on the inconclusive rate of the POVM implementation is calculated explicitly.

Contents

1. Introduction

A positive operator valued measure (POVM) [1–7] can be usefully implemented in a quantum key receiver [8–14]. The following set of POVM operators represents the possible measurements performed by the receiver:

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

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

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

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 θ.

2000 *Mathematics Subject Classification.* Primary 81P68, 94-02, 94A60.
Key words and phrases. Quantum cryptography, quantum key distribution, quantum communication, quantum information.

The photon is a spin-one representation of the Lorentz group, and it follows that the Dirac bracket between the two states is [11]

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

where

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

(The use of the angle α instead of θ is convenient in the following.) The states $|u\rangle$ and $|v\rangle$ may encode bit values 0 and 1, respectively. The POVM operators, Eqs. (1)–(3), are nonnegative 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.

The advantage of a POVM over an ordinary von Neumann projective measurement is that, for the POVM, the probability of getting an inconclusive result can be lower [8,14,15]. To see this, first consider, for comparison of a projective valued (PV) receiver with the POVM receiver, the simple all-optical PV receiver depicted in Figure 1. Effectively, the device randomly chooses between two ordinary von Neumann projective measures. (The all-optical POVM receiver is already exposited elsewhere [9–13].) The PV receiver consists of an incoming carrier photon in polarization state

$$|\psi\rangle = \bar{\alpha}\,|u\rangle + \bar{\beta}\,|v\rangle \tag{6}$$

for complex numbers $\bar{\alpha}$ and $\bar{\beta}$, a 50-50 beam splitter BS, two Wollaston prisms W_u and W_v, and four photodetectors D_u, $\mathrm{D}_{u_\perp}$, $\mathrm{D}_{v_\perp}$, and D_v. The Wollaston prism W_u is aligned so that a photon in state $|u\rangle$ would take the path labeled by the state $|\psi_3\rangle$ and polarization vector $\hat{e}_u$, and not the path labeled by the state $|\psi_4\rangle$ and polarization vector $\hat{e}_{u_\perp}$. Here, $\hat{e}_u$ denotes a unit polarization vector corresponding to the polarization state $|u\rangle$ and is perpendicular to the polarization vector $\hat{e}_{u_\perp}$ corresponding to the polarization state $|u_\perp\rangle$ orthogonal to $|u\rangle$. Analogously, the Wollaston prism W_v is aligned so that a photon in state $|v\rangle$ would take the path labeled by the state $|\psi_6\rangle$ and polarization vector $\hat{e}_v$, and not the path labeled by the state $|\psi_5\rangle$ and polarization vector $\hat{e}_{v_\perp}$ (perpendicular to $\hat{e}_v$). The beamsplitter BS serves to choose at random between two projective valued measurements, the first having projections $\{|u\rangle\langle u|, |u_\perp\rangle\langle u_\perp|\}$ and the second having projections $\{|v\rangle\langle v|, |v_\perp\rangle\langle v_\perp|\}$. It is immediately evident from Figure 1 that

$$|\psi_1\rangle = 2^{-1/2} i\left(\bar{\alpha}\,|u\rangle + \bar{\beta}\,|v\rangle\right), \tag{7}$$

$$|\psi_2\rangle = 2^{-1/2}\left(\bar{\alpha}\,|u\rangle + \bar{\beta}\,|v\rangle\right), \tag{8}$$

$$|\psi_3\rangle = 2^{-1/2} i\left(\bar{\alpha} + \bar{\beta}\sin 2\alpha\right)\left|\hat{e}_u\right\rangle, \tag{9}$$

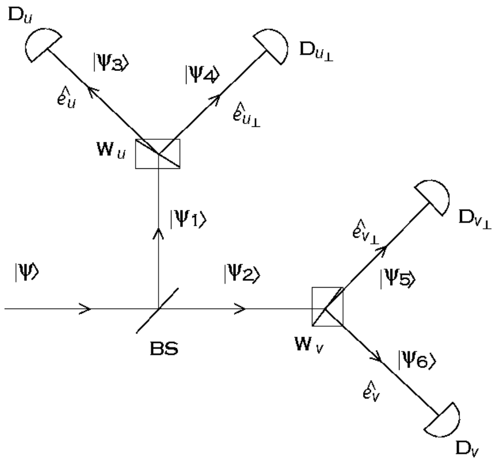

Figure 1. PV receiver.

$$|\psi_4\rangle = 2^{-1/2} i\bar{\beta}\cos 2\alpha \left|\hat{e}_{u_\perp}\right\rangle, \tag{10}$$

$$|\psi_5\rangle = 2^{-1/2} \bar{\alpha}\cos 2\alpha \left|\hat{e}_{v_\perp}\right\rangle, \tag{11}$$

$$|\psi_6\rangle = 2^{-1/2} \left(\bar{\alpha}\sin 2\alpha + \bar{\beta}\right) \left|\hat{e}_{v}\right\rangle, \tag{12}$$

where $\left|\hat{e}_u\right\rangle$, $\left|\hat{e}_{u_\perp}\right\rangle$, $\left|\hat{e}_v\right\rangle$, and $\left|\hat{e}_{v_\perp}\right\rangle$ represent unit kets corresponding to polarization vectors $\hat{e}_u$, $\hat{e}_{u_\perp}$, $\hat{e}_v$, and $\hat{e}_{v_\perp}$, respectively. It then follows that the probability $P_{\psi u}$ that the photon in state $|\psi\rangle$ is detected by ideal detector D_u is given by

$$P_{\psi u} = |\psi_3|^2 = \frac{1}{2}\left|\bar{\alpha} + \bar{\beta}\sin 2\alpha\right|^2. \tag{13}$$

Analogously, for detectors $\mathrm{D}_{u_\perp}$, $\mathrm{D}_{v_\perp}$, and D_v, one has

$$P_{\psi u_\perp} = |\psi_4|^2 = \frac{1}{2}\left|\bar{\beta}\right|^2 \cos^2 2\alpha, \tag{14}$$

$$P_{\psi v_\perp} = |\psi_5|^2 = \frac{1}{2}\left|\bar{\alpha}\right|^2 \cos^2 2\alpha, \tag{15}$$

$$P_{\psi v} = |\psi_6|^2 = \frac{1}{2}\left|\bar{\alpha}\sin 2\alpha + \bar{\beta}\right|^2. \tag{16}$$

From Eqs. (13)–(16), it follows that

$$P_{\psi u} + P_{\psi u_\perp} + P_{\psi v} + P_{\psi v_\perp} = |\bar{\alpha}|^2 + \bar{\alpha}^*\bar{\beta}\sin 2\alpha + \bar{\alpha}\bar{\beta}^*\sin 2\alpha + \left|\bar{\beta}\right|^2 = 1, \tag{17}$$

as must be the case, provided that the state $|\psi\rangle$, Eq. (6), is normalized to unity, and probability is conserved.

2. Inconclusive rates comparison

If the incoming photon state is $|\psi\rangle = |u\rangle$, one has $\{\bar{\alpha}, \bar{\beta}\} = \{1, 0\}$ and Eqs. (13)–(16) yield $P_{uu} = \frac{1}{2}$, $P_{uu_\perp} = 0$, $P_{uv_\perp} = \frac{1}{2}\cos^2 2\alpha$, $P_{uv} = \frac{1}{2}\sin^2 2\alpha$. Analogously, in the case where the incoming photon state is $|\psi\rangle = |v\rangle$, one has $\{\bar{\alpha}, \bar{\beta}\} = \{0, 1\}$ and $P_{vu} = \frac{1}{2}\sin^2 2\alpha$, $P_{vu_\perp} = \frac{1}{2}\cos^2 2\alpha$, $P_{vv_\perp} = 0$, $P_{vv} = \frac{1}{2}$. If states $|u\rangle$ and $|v\rangle$ are equiprobably incident on the receiver, then since detector D_u or D_v can be triggered by both states $|u\rangle$ and $|v\rangle$, it follows that the probability $P_?^{\mathrm{PV}}$ of an inconclusive measurement is given by

$$P_?^{\mathrm{PV}} = P_{uu} + P_{uv} = \frac{1}{2}\left(1 + \sin^2 2\alpha\right), \tag{18}$$

or equivalently,

$$P_?^{\mathrm{PV}} = P_{vv} + P_{vu} = \frac{1}{2}\left(1 + \sin^2 2\alpha\right). \tag{19}$$

One can conclude that for the two-state quantum key distribution protocol, in which a photon is incident equiprobably in state $|u\rangle$ or $|v\rangle$, the inconclusive rate $P_?^{\mathrm{PV}}$ for the projective receiver is

$$P_?^{\mathrm{PV}} = \frac{1}{2}\left(1 + \sin^2 2\alpha\right). \tag{20}$$

One can also obtain Eq. (20) by reasoning that the inconclusive rate for the PV measure is given by

$$P_?^{\mathrm{PV}} = 1 - P_{con}^{\mathrm{PV}}, \tag{21}$$

where P_{con}^{PV} is the probability of obtaining a conclusive result. From Fig. 1, it is evident that

$$\begin{aligned} P_{con}^{\mathrm{PV}} = P_{uv_\perp} &= \frac{1}{2}\langle u|\left(|v_\perp\rangle\langle v_\perp|\right)|u\rangle = \frac{1}{2}\left|\langle u|v_\perp\rangle\right|^2 \\ &= \frac{1}{2}\sin^2\theta = \frac{1}{2}\left(1 - \sin^2 2\alpha\right). \end{aligned} \tag{22}$$

Equation (22) follows, since the ideal detector $\mathrm{D}_{v_\perp}$ cannot have been excited by the state $|v\rangle$, and therefore can only have been excited by the state $|u\rangle$, and the measurement operator for the state $|v_\perp\rangle$ is $|v_\perp\rangle\langle v_\perp|$ [11]. (The overall factor of $\frac{1}{2}$ appears in Eq. (22), because the probability is $\frac{1}{2}$ that the photon takes the path from the beamsplitter leading to the Wollaston prism W_v. Also note that Eq. (22) is consistent with Eq. (15) for $\bar{\alpha} = 1$.) If one substitutes Eq. (22) in Eq. (21), then Eq. (20) again follows. Of course, Eq. (22) also follows analogously from

$$\begin{aligned} P_{con}^{\mathrm{PV}} = P_{vu_\perp} &= \frac{1}{2}\langle v|\left(|u_\perp\rangle\langle u_\perp|\right)|v\rangle = \frac{1}{2}\left|\langle v|u_\perp\rangle\right|^2 \\ &= \frac{1}{2}\sin^2\theta = \frac{1}{2}\left(1 - \sin^2 2\alpha\right). \end{aligned} \tag{23}$$

It has been demonstrated in previous work that the inconclusive rate $P_{\psi?}^{\mathrm{POVM}}$ of the POVM receiver for the arbitrary incoming state, Eq. (6), is given by [9,11–13]

$$P_{\psi?}^{\mathrm{POVM}} = \langle\psi|A_?|\psi\rangle = \left|\bar{\alpha} + \bar{\beta}\right|^2 \sin 2\alpha. \tag{24}$$

(The second equality in Eq. (24) is also consistent with the first, as can be seen by substituting Eqs. (3) and (6) in the first.)

For incoming state $|\psi\rangle = |u\rangle$, one then has $\{\bar{\alpha},\bar{\beta}\} = \{1,0\}$, and Eq. (24) becomes

$$P_{u?}^{\mathrm{POVM}} = \sin 2\alpha. \tag{25}$$

For incoming state $|\psi\rangle = |v\rangle$, one has $\{\bar{\alpha},\bar{\beta}\} = \{0,1\}$, and

$$P_{v?}^{\mathrm{POVM}} = P_{u?}^{\mathrm{POVM}} = \sin 2\alpha. \tag{26}$$

It follows that the inconclusive rate $P_?^{\mathrm{POVM}}$ of the ideal POVM receiver for the equiprobable two-state protocol is given by

$$P_?^{\mathrm{POVM}} = \sin 2\alpha. \tag{27}$$

Using Eqs. (20) and (27), one then obtains

$$\frac{P_?^{\mathrm{POVM}}}{P_?^{\mathrm{PV}}} = \frac{2\sin 2\alpha}{1+\sin^2 2\alpha} < 1, \tag{28}$$

as depicted in Figure 2. Thus, in fact, the inconclusive rate for the POVM receiver is less than that of the PV receiver, and the rate ratio is determined by the angle between the two polarization states (see Eq. (5)).

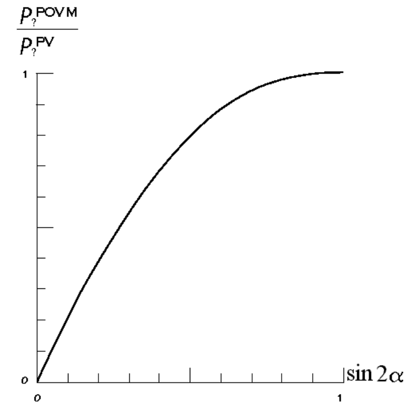

Figure 2. Inconclusive rate comparison for POVM and PV receivers.

3. Disturbed inconclusive rate

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 [16]. 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 [10,16,17]:

$$\begin{aligned} U\,|u\otimes w\rangle = \frac{1}{2}\big[&(1+\sec 2\alpha)\,|\Phi_{00}\rangle + \tan 2\alpha\,|\Phi_{10}\rangle - \tan 2\alpha\,|\Phi_{01}\rangle \\ &+\ (1-\sec 2\alpha)\,|\Phi_{11}\rangle\,\big]\otimes|u\rangle - \ \frac{1}{2}\big[\tan 2\alpha\,|\Phi_{00}\rangle - (1-\sec 2\alpha)\,|\Phi_{10}\rangle \\ &-\ (1+\sec 2\alpha)\,|\Phi_{01}\rangle - \tan 2\alpha\,|\Phi_{11}\rangle\,\big]\otimes|v\rangle\,. \end{aligned} \tag{29}$$

Here $|\Phi_{mn}\rangle$ are states in the Hilbert space of the disturbing probe, and are neither normalized nor orthogonal. Equation (29) follows from Eqs. (1) and (2) of Slutsky et al [17]. Similarly, for an incoming state $|v\rangle$, one has

$$
\begin{aligned}
U\,|v\otimes w\rangle = \frac{1}{2}\big[&\tan 2\alpha\,|\Phi_{00}\rangle + (1+\sec 2\alpha)\,|\Phi_{10}\rangle + (1-\sec 2\alpha)\,|\Phi_{01}\rangle \\
&-\ \tan 2\alpha\,|\Phi_{11}\rangle\big]\otimes|u\rangle +\ \frac{1}{2}\big[(1-\sec 2\alpha)\,|\Phi_{00}\rangle - \tan 2\alpha\,|\Phi_{10}\rangle \\
&+\ \tan 2\alpha\,|\Phi_{01}\rangle + (1+\sec 2\alpha)\,|\Phi_{11}\rangle\big]\otimes|v\rangle\,.
\end{aligned}
\tag{30}
$$

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 [16,17]

$$|\Phi_{00}| = |\Phi_{11}|\,, \tag{31}$$

$$|\Phi_{01}| = |\Phi_{10}|\,, \tag{32}$$

$$\langle\Phi_{00}|\Phi_{01}\rangle = \langle\Phi_{11}|\Phi_{10}\rangle\,, \tag{33}$$

$$\langle\Phi_{00}|\Phi_{10}\rangle = \langle\Phi_{11}|\Phi_{01}\rangle\,, \tag{34}$$

$$\langle\Phi_{01}|\Phi_{10}\rangle = \langle\Phi_{10}|\Phi_{01}\rangle\,, \tag{35}$$

$$\langle\Phi_{01}|\Phi_{00}\rangle = \langle\Phi_{10}|\Phi_{11}\rangle\,, \tag{36}$$

$$\langle\Phi_{01}|\Phi_{11}\rangle = \langle\Phi_{10}|\Phi_{00}\rangle\,, \tag{37}$$

$$\langle\Phi_{11}|\Phi_{00}\rangle = \langle\Phi_{00}|\Phi_{11}\rangle\,. \tag{38}$$

According to Eq. (24), the inconclusive rate $R_?$ induced by the disturbing probe in the POVM receiver is given by

$$R_? = P_{u?} = \langle u\otimes w|\,U^\dagger A_? U\,|u\otimes w\rangle\,, \tag{39}$$

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. Alternatively, one also has

$$R_? = P_{v?} = \langle v\otimes w|\,U^\dagger A_? U\,|v\otimes w\rangle\,, \tag{40}$$

because of the symmetry of the two-state protocol. Equivalently, using Eq. (3) in Eq. (39), one also has for the induced inconclusive rate:

$$R_? = 1 - P_{uu} - P_{uv}, \tag{41}$$

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

$$P_{uu} = \langle u\otimes w|\,U^\dagger A_u U\,|u\otimes w\rangle\,, \tag{42}$$

$$P_{uv} = \langle u\otimes w|\,U^\dagger A_v U\,|u\otimes w\rangle\,. \tag{43}$$

Substituting Eqs. (2), (29) and (31)–(38) in Eq. (43), one obtains

$$P_{uv} = (1+\sin 2\alpha)^{-1}\Big[\left(1-\sin^4\alpha-\cos^4\alpha\right)|\Phi_{00}|^2+\left(1-\frac{1}{2}\sin^2 2\alpha\right)|\Phi_{01}|^2 .$$
$$+\ \frac{1}{2}\sin 2\alpha\,\langle\Phi_{01}|\Phi_{11}\rangle+\frac{1}{2}\sin 2\alpha\,\langle\Phi_{00}|\Phi_{10}\rangle-\frac{1}{2}\sin 2\alpha\,\langle\Phi_{00}|\Phi_{01}\rangle$$
$$-\ \frac{1}{2}\sin^2 2\alpha\,\langle\Phi_{00}|\Phi_{11}\rangle-\frac{1}{2}\sin 2\alpha\,\langle\Phi_{01}|\Phi_{00}\rangle-\frac{1}{2}\sin^2 2\alpha\,\langle\Phi_{01}|\Phi_{10}\rangle\Big]. \tag{44}$$

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 Slutsky et al [17], namely,

$$|\Phi_{00}\rangle = X_0\,|w_0\rangle+X_1\,|w_1\rangle+X_2\,|w_2\rangle+X_3\,|w_3\rangle\,, \tag{45}$$

$$|\Phi_{11}\rangle = X_3\,|w_0\rangle+X_2\,|w_1\rangle+X_1\,|w_2\rangle+X_0\,|w_3\rangle\,, \tag{46}$$

$$|\Phi_{01}\rangle = X_5\,|w_1\rangle+X_6\,|w_2\rangle\,, \tag{47}$$

$$|\Phi_{10}\rangle = X_6\,|w_1\rangle+X_5\,|w_2\rangle\,. \tag{48}$$

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 [16,17]

$$X_0 = \sin\lambda\cos\mu, \tag{49}$$

$$X_1 = \cos\lambda\cos\theta\cos\phi, \tag{50}$$

$$X_2 = \cos\lambda\cos\theta\sin\phi, \tag{51}$$

$$X_3 = \sin\lambda\sin\mu, \tag{52}$$

$$X_5 = \cos\lambda\sin\theta\cos\phi, \tag{53}$$

$$X_6 = -\cos\lambda\sin\theta\sin\phi, \tag{54}$$

consistent with the assumed unitarity of the disturbing probe.

Next, substituting Eqs. (45)–(48) in Eq. (44), one gets

$$P_{uv} = (1+\sin 2\alpha)^{-1}\Big[\left(1-\sin^4\alpha-\cos^4\alpha\right)\left(X_0^2+X_1^2+X_2^2+X_3^2\right)$$
$$+\ \left(1-\frac{1}{2}\sin^2 2\alpha\right)\left(X_5^2+X_6^2\right)+\sin 2\alpha\,(X_1X_6+X_2X_5)$$
$$-\ \sin 2\alpha\,(X_1X_5+X_2X_6)$$
$$-\ \sin^2 2\alpha\,(X_0X_3+X_1X_2+X_5X_6)\Big]. \tag{55}$$

Then if one substitutes Eqs. (49)–(54) in Eq. (55), the latter becomes

$$P_{uv} = \frac{1}{4}(1+\sin 2\alpha)^{-1}\Big[1-\cos 4\alpha+2(1+\cos 4\alpha)\cos^2\lambda\sin^2\theta$$
$$-\ 2\sin 2\alpha\cos^2\lambda\sin 2\theta\cos 2\phi-2\sin^2 2\alpha\sin^2\lambda\sin 2\mu$$
$$-\ 2\sin^2 2\alpha\cos^2\lambda\cos 2\theta\sin 2\phi\Big]. \tag{56}$$

Analogously, it can be shown that Eq. (42) becomes

$$
\begin{aligned}
P_{uu} = \frac{1}{2}(1-\sin 2\alpha)\Big[& 2\sin^2\lambda + 2\cos^2\lambda\cos^2\theta + \tan^2 2\alpha \\
& - \tan 2\alpha \sec 2\alpha \cos^2\lambda \sin 2\theta \cos 2\phi \\
& - \tan^2 2\alpha \left(\sin^2\lambda \sin 2\mu + \cos^2\lambda \cos 2\theta \sin 2\phi\right)\Big].
\end{aligned} \tag{57}
$$

Next, substituting Eqs. (56) and (57) in Eq. (41), one obtains, after extensive algebraic reduction, the following expression for the inconclusive rate induced by the disturbing probe:

$$
R_? = \frac{\sin 2\alpha\,(1+c+a\sin 2\alpha)}{1+\sin 2\alpha}, \tag{58}
$$

where (in the notation of Slutsky et al [17]),

$$
a = \sin^2\lambda\sin 2\mu + \cos^2\lambda\cos 2\theta\sin 2\phi, \tag{59}
$$

$$
c = \cos^2\lambda\sin 2\theta\cos 2\phi, \tag{60}
$$

expressed in terms of the probe parameters λ, μ, θ, and ϕ.

4. Consistency

It is well to check the consistency of Eq. (58) with the analogue of the second equality of Eq. (24) in which $\bar{\alpha}$ and $\bar{\beta}$ correspond to the correlated probe states of Eq. (29). Specifically, if

$$
|\psi\rangle = |C_u\rangle \otimes |u\rangle + |C_v\rangle \otimes |v\rangle \tag{61}
$$

for generic correlated states $|C_u\rangle$ and $|C_v\rangle$, then it can be shown, by using the first equality of Eq. (24) together with Eq. (3), that

$$
P^{\mathrm{POVM}}_{\psi ?} = (\langle C_u| + \langle C_v|)(|C_u\rangle + |C_v\rangle)\sin 2\alpha. \tag{62}
$$

Comparing Eqs. (61) and (29), and using Eq. (62), one then also has

$$
R_? = P_{u?} = \langle \Phi_u|\Phi_u\rangle \sin 2\alpha, \tag{63}
$$

where

$$
\begin{aligned}
|\Phi_u\rangle = \frac{1}{2}\Big[& (1+\sec 2\alpha)|\Phi_{00}\rangle + \tan 2\alpha|\Phi_{10}\rangle - \tan 2\alpha|\Phi_{01}\rangle \\
& + (1-\sec 2\alpha)|\Phi_{11}\rangle - \tan 2\alpha|\Phi_{00}\rangle + (1-\sec 2\alpha)|\Phi_{10}\rangle \\
& + (1+\sec 2\alpha)|\Phi_{01}\rangle + \tan 2\alpha|\Phi_{11}\rangle\Big].
\end{aligned} \tag{64}
$$

Using Eqs. (45)–(48) in Eq. (63), the latter becomes

$$
\begin{aligned}
R_? = \sin 2\alpha\,(\sec 2\alpha - \tan 2\alpha)\big[& \sec 2\alpha\left(X_0^2 + X_1^2 + X_2^2 + X_3^2\right) \\
& + 2\tan 2\alpha\,(X_1X_6 + X_2X_5) + 2\sec 2\alpha\,(X_1X_5 + X_2X_6) \\
& + 2\tan 2\alpha\,(X_0X_3 + X_1X_2) + \sec 2\alpha\left(X_6^2 + X_5^2\right) \\
& + 2\tan 2\alpha X_5X_6\big].
\end{aligned} \tag{65}
$$

Next, substituting Eqs. (49)–(54) in Eq. (65), and using trigonometric identities, one obtains

$$R_? = \sin 2\alpha \, (1 + \sin 2\alpha)^{-1} \left[1 + \cos^2 \lambda \sin 2\theta \cos 2\phi \right.$$
$$\left. + \; \left(\sin^2 \lambda \sin 2\mu + \cos^2 \lambda \cos 2\theta \sin 2\phi\right) \sin 2\alpha\right], \tag{66}$$

which agrees with Eqs. (58)–(60).

Equivalently, one also has, using Eqs. (62) and (30),

$$R_? = P_{v?} = \langle \Phi_v | \Phi_v \rangle \sin 2\alpha, \tag{67}$$

where

$$|\Phi_v\rangle = \frac{1}{2}\Big[\tan 2\alpha \, |\Phi_{00}\rangle + (1 + \sec 2\alpha) \, |\Phi_{10}\rangle + (1 - \sec 2\alpha) \, |\Phi_{01}\rangle$$
$$- \; \tan 2\alpha \, |\Phi_{11}\rangle + \; (1 - \sec 2\alpha) \, |\Phi_{00}\rangle - \; \tan 2\alpha \, |\Phi_{10}\rangle$$
$$+ \; \tan 2\alpha \, |\Phi_{01}\rangle + (1 + \sec 2\alpha) \, |\Phi_{11}\rangle\Big], \tag{68}$$

and if one substitutes Eqs. (45)–(54) in Eq. (67), it can be shown that Eq. (67) also reduces to Eqs. (58)–(60).

Equation (58) can be used in optimizing the disturbing probe parameters for maximum Renyi information gain by the probe with both a fixed induced inconclusive rate and a fixed induced error rate on corrected bits [18,19]. This is a challenging nonlinear optimization problem.

5. Conclusion

For an optical implementation of a projective measure and the POVM implementation of other works [9-13], the unperturbed inconclusive rates are calculated, and the POVM is shown explicitly to have the lower inconclusive rate. The ratio of the two rates is given by Eq. (28). Also, the disturbed inconclusive rate of the POVM receiver due to a general unitary disturbance of the carrier by a probe is calculated in three different ways, and is shown to be given by Eqs. (58)–(60).

6. Acknowledgements

This work was supported by the U.S. Army Research Laboratory. The hospitality and stimulation of the Isaac Newton Institute for Mathematical Sciences at the University of Cambridge is gratefully acknowledged. The author wishes to especially thank Prof. Peter Knight, FRS, for inviting him to participate in the programme *Complexity, Computation, and the Physics of Information* at the Newton Institute, where much of this work was completed. Useful communications with J. M. Myers, J. D. Franson, B. A. Slutsky, A. Peres, S. J. Lomonaco, J. D. Murley, and M. Kruger are gratefully acknowledged.

References

[1] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Academic Press, New York (1976).
[2] J. M. Jauch and C. Piron, "Generalized Localizability," Helv. Phys. Acta **40**, 559–570 (1967).
[3] E. B. Davies and J. T. Lewis, "An Operational Approach to Quantum Probability," Commun. Math Phys. **17**, 239–260 (1970).
[4] E. B. Davies, *Quantum Theory of Open Systems,* Academic, New York (1976).
[5] P. A. Benioff, "Operator Valued Measures in Quantum Mechanics: Finite and Infinite Processes," J. Math. Phys. **13**, 231–242 (1972).

[6] P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement*, 2nd Ed., Springer, Berlin (1996).

[7] P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics*, Springer, Berlin (1995).

[8] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, "Eavesdropping on Quantum-Cryptographical Systems," Phys. Rev. A **50**, 1047–1056 (1994).

[9] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., "Aspects of Entangled Translucent Eavesdropping in Quantum Cryptography," Phys. Rev. A **56**, 4456–4465 (1997); **58**, 2617 (1998).

[10] H. E. Brandt, "Eavesdropping Optimization for Quantum Cryptography Using a Positive Operator Valued Measure," Phys. Rev. A **59**, 2665–2669 (1999).

[11] H. E. Brandt, "Positive Operator Valued Measure in Quantum Information Processing," Am. J. Phys. **67**, 434–439 (1999).

[12] J. M. Myers and H. E. Brandt, "Converting a Positive Operator-Valued Measure to a Design for a Measuring Instrument on the Laboratory Bench," Meas. Sci. Technol. **8**, 1222–1227 (1997).

[13] H. E. Brandt, "Qubit Devices and the Issue of Qauntum Decoherence," Progr. Quantum Electronics **22**, 257–370 (1998).

[14] A. Peres, *Quantum Theory: Concepts and Methods,* Kluwer, Dordrecht (1993).

[15] A. Peres, "How to Differentiate Between Non-Orthogonal States," Phys. Lett. A **128**, 19 (1998).

[16] C. A. Fuchs and A. Peres, "Quantum-State Disturbance Versus Information Gain: Uncertainty Relations for Quantum Information," Phys. Rev. A **53**, 2038–2045 (1996).

[17] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, "Security of Quantum Cryptography Against Individual Attacks," Phys. Rev. A **57**, 2383–2398 (1998).

[18] H. E. Brandt, "Inconclusive Rate as a Disturbance Measure in Quantum Cryptography," Phys. Rev. A **62**, 042310-1-14 (2000).

[19] H. E. Brandt, "Inconclusive Rate in Quantum Key Distribution," Phys. Rev. A **64**, 042316-1-5 (2001).

(Howard E. Brandt) U.S. Army Research Laboratory, Adelphi, MD 20783, and, University of Cambridge, Isaac Newton Institute for the Mathematical Sciences, Cambridge, U.K.

E-mail address, Howard E. Brandt: `hbrandt@arl.army.mil`