Probe optimization in four-state protocol of quantum cryptography

Howard E. Brandt
U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, Maryland 20783
and Institute of Theoretical Physics, University of California, Santa Barbara, California 93106
(Received 21 December 2001; published 10 September 2002)

Following a review of the probe optimization of Slutsky, Rao, Sun, and Fainman [Phys. Rev. A **57**, 2383 (1998)] for the standard four-state protocol of quantum key distribution, I generalize the optimization to a variable angle between the signal bases. I calculate the corresponding maximum Renyi information gain by the probe, and determine the optimum probe parameters. A larger set of optimum probe parameters is found for the standard protocol than was known previously.

DOI: 10.1103/PhysRevA.66.032303 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta

I. INTRODUCTION

Since the pioneering discoveries of Wiesner [1] and Bennett and Brassard [2,3], research efforts by many investigators have significantly advanced the field of quantum cryptography [4]. The primary emphasis of the research has been placed on quantum key distribution, the generation by means of quantum mechanics of a secure random binary sequence which can be used together with the Vernam cipher (one-time pad) [5] for secure encryption and decryption. Various protocols have been devised for quantum key distribution, including the single-particle four-state Bennett-Brassard 1984 protocol (BB84) [2], the single-particle two-state Bennett 1992 protocol (B92) [6], and the two-particle entangled-state Einstein-Podolsky-Rosen [7] protocol. However, the original BB84 protocol is presently the most practical and robust protocol.

One effective implementation of the BB84 protocol [2] uses single photons linearly polarized along one of the four basis vectors of two sets of coplanar orthogonal bases oriented at an angle of 45° (equivalently, $\pi/4$) relative to each other. The polarization measurement operators in one basis do not commute with those in the other, since they correspond to nonorthogonal polarization states. At a fundamental level, the potential security of the key rests on the fact that nonorthogonal photon polarization measurement operators do not commute, and this results in quantum uncertainty in the measurement of those states by an eavesdropping probe [8]. Before transmission of each photon, the transmitter and the receiver each independently and randomly select one of the two bases. The transmitter sends a single photon with polarization chosen at random along one of the orthogonal basis vectors in the chosen basis. The receiver makes a polarization measurement in its chosen basis. Next, the transmitter and the receiver, using a public communication channel, openly compare their choices of basis, without disclosing the polarization states transmitted or received. Events in which the transmitter and the receiver choose different bases are ignored, while the remaining events ideally have completely correlated polarization states. The two orthogonal states in each of the two bases encode binary numbers 0 and 1, and thus a sequence of photons transmitted in this manner can establish a random binary sequence shared by both the transmitter and the receiver and can then serve as the secret key, following error correction and privacy amplification [9,10]. Using the Vernam cipher, the key can then be used to encode a message which can be securely transmitted over an open communication line and then decoded, using the shared secret key at the receiver. (The encrypted message can be created at the transmitter by adding the key to the message and can be decrypted at the receiver by subtracting the shared secret key.)

Numerous analyses of various eavesdropping strategies have appeared in the literature. A recent review is given in Ref. [4]. The present work is limited to an individual attack in which each transmitted photon is measured by an independent probe after the photon polarization basis is revealed. In addition to the individual attack, other approaches include: coherent collective attacks in which the eavesdropper entangles a separate probe with each transmitted photon and measures all probes together as one system; and also coherent joint attacks in which a single probe is entangled with the entire set of carrier photons. However, these approaches require maintenance of coherent superpositions of large numbers of states, and this is not currently feasible.

For the standard four-state (BB84) protocol [2] of key distribution in quantum cryptography, Slutsky, Rao, Sun, and Fainman [11] performed an eavesdropping probe optimization, which on average yields the most information to the eavesdropper for a given error rate caused by the probe. A Fuchs-Peres probe [11,12] is considered, which is the most general possible probe consistent with unitarity. Each individual transmitted photon is made to interact with the probe so that the carrier and the probe are left in an entangled state, and projective measurement by the probe, made subsequent to projective measurement by the legitimate receiver, yields information about the carrier state. The probe optimization is based on maximizing the Renyi information gain by the probe on corrected data for a given error rate induced by the probe in the legitimate receiver. Corrected data include data remaining after discarding inconclusive results and also erroneous data as determined by block checksums and bisective search. A minimum overlap of the probe states which are correlated with the signal states (because of the entanglement) determines the maximum Renyi information gain by the probe. This is related to the idea that the more nearly orthogonal the correlated probe states are, the easier they are to distinguish. The optimization is needed to establish the

security of the key against individual attack. The upper bound on Renyi information gain by the probe is needed in determining the number of bits which must be sacrificed during privacy amplification in order that it be exponentially unlikely that more than token leakage of the final key be available to the eavesdropper following key distillation [9–11]. The results of the probe optimization in Ref. [11] were obtained for the standard protocol with an angle of 45° between the signal bases. The present work generalizes the probe optimization for an arbitrary angle between the signal bases and determines the maximum information gain by the probe and the optimum values for the probe parameters. The standard BB84 protocol with an angle of 45° between the signal bases is shown to yield the least information to the probe. However, sensitivity to practical tuning variations in this angle can be useful in quantifying tolerances. Also, a larger set of optimum probe parameters is found for the standard BB84 protocol than was known previously.

In Sec. II, a detailed review is given of the optimization of the standard BB84 protocol by Slutsky *et al.* [11]. Section III along with Appendix A establishes the necessary conditions for the existence of possible extrema of the overlap of correlated probe states for an arbitrary angle between the signal bases. Section IV along with Appendix B identifies the possible extrema and associated probe parameters. Section V determines an analytical algebraic expression for the maximum Renyi information gain by the probe for fixed error rate and angle between the signal bases. A useful symmetry, involving interchange of the signal states, is exploited to accommodate angles lesser or greater than 45°. Also, two sets of optimum probe parameters are determined, which both correspond to the same optimization. Section VI contains a summary.

II. PROBE OPTIMIZATION FOR STANDARD BB84 PROTOCOL

In this section, the probe optimization of Ref. [11] is addressed for the standard BB84 protocol in which the angle between the signal bases is restricted precisely to $\pi/4$ (equivalently, $\alpha=\pi/8$ in Fig. 2 of Ref. [11]). From Sec. IV and Table II of Ref. [11], one has for the induced error rate E in the receiver by the eavesdropping probe,

$$E=\frac{P_{u\bar{u}}+P_{\bar{u}u}}{P_{u\bar{u}}+P_{\bar{u}u}+P_{uu}+P_{\bar{u}\bar{u}}}, \tag{1}$$

where P_{ij} is the probability that if a photon in polarization state $|i\rangle$ is transmitted in the presence of the disturbing probe, the polarization state $|j\rangle$ is detected by the legitimate receiver, where $\{i,j\}=\{u,\bar{u},v,\bar{v}\}$ corresponds to nonorthogonal polarization states $|u\rangle$ and $|v\rangle$, and the state $|\bar{u}\rangle$ orthogonal to $|u\rangle$, and $|\bar{v}\rangle$ orthogonal to $|v\rangle$. The states $|u\rangle$ and $|v\rangle$ both correspond to Boolean state $|1\rangle$, and $|\bar{u}\rangle$ and $|\bar{v}\rangle$ correspond to Boolean state $|0\rangle$.

One has

$$P_{ij}=\langle\psi_{ij}|\psi_{ij}\rangle=|\psi_{ij}|^2, \tag{2}$$

where $|\psi_{ij}\rangle$ is the projected state of the probe when polarization state $|i\rangle$ is transmitted, and polarization state $|j\rangle$ is detected by the receiver in the presence of the probe [11].

From Eqs. (1) and (8) of Ref. [11], it follows that

$$|\psi_{u\bar{u}}\rangle=\langle\bar{u}|U|u\otimes w\rangle, \tag{3}$$

where U is the general unitary operator producing the entanglement of the probe states with the signal states, or

$$|\psi_{u\bar{u}}\rangle=(-\langle e_0|\sin\alpha+\langle e_1|\cos\alpha)\times U(|e_0\rangle\cos\alpha+|e_1\rangle\sin\alpha)\otimes|w\rangle. \tag{4}$$

Here $|e_0\rangle$ and $|e_1\rangle$ are orthonormal basis vectors in the plane of the polarization states of the signal, $|w\rangle$ is the initial state of the probe, and $\alpha=\frac{1}{2}(\pi/2-\bar{\theta})$ is half the complement of the angle $\bar{\theta}=\cos^{-1}(\langle u|v\rangle/|u||v|)$ between the two nonorthogonal linear-polarization states $|u\rangle$ and $|v\rangle$ of the signal (see Fig. 2 of Ref. [11]; I also refer to $\bar{\theta}$ as the angle between the two orthogonal bases $\{|u\rangle,|\bar{u}\rangle\}$ and $\{|v\rangle,|\bar{v}\rangle\}$). Using Eq. (2) of Ref. [11] in Eq. (4) above, one obtains

$$|\psi_{u\bar{u}}\rangle=(-\langle e_0|\sin\alpha+\langle e_1|\cos\alpha)\times\left(\cos\alpha\sum_n|e_n\rangle\otimes|\Phi_{0n}\rangle+\sin\alpha\sum_n|e_n\rangle\otimes|\Phi_{1n}\rangle\right), \tag{5}$$

where $|\Phi_{mn}\rangle$ are the unnormalized nonorthogonal states of the probe. Equation (5) becomes

$$|\psi_{u\bar{u}}\rangle=|\Phi_{01}\rangle\cos^2\alpha-|\Phi_{10}\rangle\sin^2\alpha+(|\Phi_{11}\rangle-|\Phi_{00}\rangle)\sin\alpha\cos\alpha, \tag{6}$$

and substituting Eq. (6) in Eq. (2), and using the symmetry properties of the probe states [11–13], and Eqs. (3a), (3b), and (12) of Ref. [11], one obtains

$$P_{u\bar{u}}=\tfrac{1}{2}(1-d)+\tfrac{1}{2}(d-a)\sin^2 2\alpha-\tfrac{1}{2}c\sin 2\alpha, \tag{7}$$

where a, b, c, and d, expressed in terms of the eavesdropping probe parameters λ, μ, θ, and ϕ, are given by [11,12]

$$a=\sin^2\lambda\sin 2\mu+\cos^2\lambda\cos 2\theta\sin 2\phi, \tag{8}$$

$$b=\sin^2\lambda\sin 2\mu+\cos^2\lambda\sin 2\phi, \tag{9}$$

$$c=\cos^2\lambda\sin 2\theta\cos 2\phi, \tag{10}$$

$$d=\sin^2\lambda+\cos^2\lambda\cos 2\theta. \tag{11}$$

Summarizing Eq. (7), along with other results in Appendix C of Ref. [11], one has

$$P_{uu}=\tfrac{1}{2}(1+d)-\tfrac{1}{2}(d-a)\sin^2 2\alpha+\tfrac{1}{2}c\sin 2\alpha, \tag{12}$$

$$P_{u\bar{u}}=\tfrac{1}{2}(1-d)+\tfrac{1}{2}(d-a)\sin^2 2\alpha-\tfrac{1}{2}c\sin 2\alpha, \tag{13}$$

$$P_{\bar{u}u}=\tfrac{1}{2}(1-d)+\tfrac{1}{2}(d-a)\sin^2 2\alpha+\tfrac{1}{2}c\sin 2\alpha, \tag{14}$$

$$P_{\overline{uu}} = \tfrac{1}{2}(1+d) - \tfrac{1}{2}(d-a)\sin^2 2\alpha - \tfrac{1}{2}c\sin 2\alpha. \quad (15)$$

Substituting Eqs. (12)–(15) in Eq. (1), one obtains

$$E = \tfrac{1}{2}[1-d+(d-a)\sin^2 2\alpha]. \quad (16)$$

Also from Sec. IV of Ref. [11], one has for the overlap Q of the probe states correlated with the signal states received by the legitimate receiver,

$$Q = \frac{\langle \psi_{uu} | \psi_{\overline{uu}} \rangle}{|\psi_{uu}||\psi_{\overline{uu}}|}, \quad (17)$$

or equivalently, using Eq. (2) in Eq. (17), one obtains

$$Q = \frac{\langle \psi_{uu} | \psi_{\overline{uu}} \rangle}{(P_{uu} P_{\overline{uu}})^{1/2}}. \quad (18)$$

From Appendix C of Ref. [11], one also has

$$|\psi_{uu}\rangle = |\Phi_{00}\rangle\cos^2\alpha + |\phi_{11}\rangle\sin^2\alpha + (|\Phi_{10}\rangle + |\Phi_{01}\rangle)\sin\alpha\cos\alpha \quad (19)$$

and

$$|\psi_{\overline{uu}}\rangle = |\Phi_{11}\rangle\cos^2\alpha + |\Phi_{00}\rangle\sin^2\alpha - (|\Phi_{10}\rangle + |\Phi_{01}\rangle)\sin\alpha\cos\alpha. \quad (20)$$

Using Eqs. (19), (20), the symmetry properties [11–13] of the probe states $|\Phi_{ij}\rangle$, and Eqs. (12), (3a), (3b) of Ref. [11], one obtains

$$\langle \psi_{uu} | \psi_{\overline{uu}} \rangle = \tfrac{1}{2}(a+b) + \tfrac{1}{2}(d-a)\sin^2 2\alpha. \quad (21)$$

Next, substituting Eqs. (21), (12), and (15) in Eq. (18), one obtains

$$Q = [\tfrac{1}{2}(a+b) + (d-a)\tfrac{1}{2}\sin^2 2\alpha][\tfrac{1}{2}(1+d) + (-d+a)\tfrac{1}{2}\sin^2 2\alpha + c\tfrac{1}{2}\sin 2\alpha]^{-1/2} \times [\tfrac{1}{2}(1+d) + (-d+a)\tfrac{1}{2}\sin^2 2\alpha - c\tfrac{1}{2}\sin 2\alpha]^{-1/2}, \quad (22)$$

in agreement with Eq. (15) of Ref. [11]. The optimum information gain $I^R_{\rm opt}$ by the probe is given in terms of the overlap Q of correlated probe states by

$$I^R_{\rm opt} = \log_2(2-Q^2) \quad (23)$$

(for the BB84 protocol, as well as the B92 protocol) [11,13–15]. It follows from Eq. (23) that $I^R_{\rm opt}$ is maximized when Q is minimized.

It is of interest to first limit the analysis to the standard BB84 protocol in which $\alpha = \pi/8$, corresponding to a 45° angle ($\overline{\theta} = \pi/2 - 2\alpha = \pi/4$) between the signal bases and also between the two nonorthogonal polarization states $|u\rangle$ and $|v\rangle$ of the signal, namely, $\langle u|v\rangle = \cos\overline{\theta} = \cos(\pi/2 - 2\alpha) = \sin 2\alpha = \cos(\pi/4) = 2^{-1/2}$. The conditional optimization in Ref. [11], which is performed for fixed error rate E, is limited to this case. In that case, Eqs. (16) and (22) become

$$E_0 \equiv E_{|\alpha=\pi/8} = \tfrac{1}{2}[1 - \tfrac{1}{2}(d+a)] \quad (24)$$

and

$$Q_0 \equiv Q_{|\alpha=\pi/8} = \frac{\frac{1}{2}(d+a)+b}{\{[1+\frac{1}{2}(d+a)]^2 - \frac{1}{2}c^2\}^{1/2}}, \quad (25)$$

respectively, in agreement with Eqs. (15) of Ref. [11]. Substituting Eq. (24) in Eq. (25), the latter becomes

$$Q_0 = \frac{1-2E_0+b}{[(2-2E_0)^2 - \frac{1}{2}c^2]^{1/2}}, \quad (26)$$

also in agreement with Eq. (15) of Ref. [11].

For any value of E_0, the numerator of Eq. (26) has a conditional (fixed error rate E_0) minimum at some point where the denominator has a conditional maximum, namely, $c = 0$. (This is further substantiated in the following.) Clearly, the numerator of Eq. (26) for fixed E_0 is minimum when b is minimum. Before minimizing b, substituting Eqs. (8) and (11) in Eq. (24), one obtains

$$E_0 = \tfrac{1}{2} - \tfrac{1}{4}[\sin^2\lambda(1+\sin 2\mu) + \cos^2\lambda\cos 2\theta(1+\sin 2\phi)] \quad (27)$$

or

$$\sin 2\phi = \frac{2 - 4E_0 - \sin^2\lambda(1+\sin 2\mu)}{\cos^2\lambda\cos 2\theta} - 1. \quad (28)$$

Next substituting Eq. (28) in Eq. (9), in order to eliminate the variable ϕ, one gets

$$b = \sin^2\lambda\sin 2\mu + \frac{2 - 4E_0 - \sin^2\lambda(1+\sin 2\mu)}{\cos 2\theta} - \cos^2\lambda. \quad (29)$$

In order that b be minimum, so that Q_0 can be minimum in Eq. (26), one requires that b in Eq. (29) satisfy

$$\frac{\partial b}{\partial \mu} = 0, \quad (30)$$

$$\frac{\partial b}{\partial \lambda}=0, \tag{31}$$

and

$$\frac{\partial b}{\partial \theta}=0. \tag{32}$$

Substituting Eq. (29) in Eqs. (30), (31), and (32), one requires

$$\sin^2\lambda\cos 2\mu\left(1-\frac{1}{\cos 2\theta}\right)=0, \tag{33}$$

$$\sin 2\lambda(\sin 2\mu+1)\left(1-\frac{1}{\cos 2\theta}\right)=0, \tag{34}$$

$$\frac{\sin 2\theta}{\cos^2 2\theta}[2-4E_0-\sin^2\lambda(1+\sin 2\mu)]=0. \tag{35}$$

Equations (33)–(35) are necessary conditions for minimum b and Q_0.

Equation (33) requires

$$\sin\lambda=0, \tag{36}$$

$$\cos 2\mu=0, \tag{37}$$

or

$$\cos 2\theta=1. \tag{38}$$

Equation (34) requires

$$\sin 2\lambda=0, \tag{39}$$

$$\sin 2\mu=-1, \tag{40}$$

or

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

Equation (35) requires

$$\sin 2\theta=0 \tag{42}$$

or

$$\sin^2\lambda(1+\sin 2\mu)=2-4E_0. \tag{43}$$

A solution to Eqs. (33)–(35), which leads to the optimization given in Ref. [11], is given by

$$\sin\lambda=0, \quad \sin 2\theta=0, \quad \cos 2\theta=e_\theta\equiv\pm 1. \tag{44}$$

Equations (44) satisfy Eqs. (36), (39), and (42), and therefore also Eqs. (33)–(35). Next, substituting Eqs. (44) in Eq. (10), one gets

$$c=0, \tag{45}$$

consistent with the conditional maximum of the denominator in Eq. (26), as declared above.

Furthermore, substituting Eqs. (44) in Eq. (28), one obtains

$$\sin 2\phi=\frac{2}{e_\theta}(1-2E_0)-1. \tag{46}$$

Since only $E_0<1/2$ is considered [11], and clearly $E_0\geqslant 0$, then one requires

$$0\leqslant E_0<1/2. \tag{47}$$

Then substituting Eq. (46) in Eq. (47), one requires

$$0<e_\theta(\sin 2\phi+1)\leqslant 2. \tag{48}$$

Clearly one requires $e_\theta=+1$ because if $e_\theta=-1$, then Eq. (48) implies $\sin 2\varphi<-1$, which is impossible. Therefore, one has in Eq. (44),

$$\cos 2\theta=e_\theta=1, \tag{49}$$

and Eq. (48) becomes

$$-1<\sin 2\phi\leqslant 1. \tag{50}$$

Next, substituting Eqs. (44) and (49) in Eqs. (8)–(11), one requires

$$a=\sin 2\phi, \tag{51}$$

$$b=\sin 2\phi, \tag{52}$$

$$c=0, \tag{53}$$

and

$$d=1. \tag{54}$$

[Equation (53) restates Eq. (45).] Next, substituting Eqs. (51) and (54) in Eq. (24), one obtains

$$E_0=\tfrac{1}{4}(1-\sin 2\phi), \tag{55}$$

and therefore

$$\sin 2\varphi=1-4E_0. \tag{56}$$

Also, substituting Eqs. (52), (53), and (56) in Eq. (26), one obtains

$$Q_0=3-\frac{2}{1-E_0}. \tag{57}$$

Equations (57), (44), (49), and (50)–(55) agree with Eqs. (16) of Ref. [11]. The choice of $\mu=0$ in Ref. [11] is allowed because μ only enters through a and b in Eqs. (8) and (9), and according to Eq. (44), $\sin\lambda=0$. In general, however, any μ $(0\leqslant\mu\leqslant\pi)$ produces the same optimization. Also, $\lambda=\pi$ satisfies Eq. (44) as well as $\lambda=0$. Other combinations of Eqs. (36)–(43) may also yield solutions, and this issue is addressed in Sec. IV.

It is also well to further clarify the arguments of Appendix E of Ref. [11]. Note that according to Eq. (9), b is indepen-

dent of θ, and E_0 in Eq. (27) is clearly least when $\cos 2\theta = 1$, since in the last term of Eq. (27), $\cos^2\lambda \geqslant 0$, and according to Eq. (50), $0 < (1+\sin 2\phi) \leqslant 2$. But then substituting Eq. (49) in Eq. (27), the latter becomes

$$E_0 = \tfrac{1}{2} - \tfrac{1}{4}[1 + \sin^2\lambda \sin 2\mu + \cos^2\lambda \sin 2\phi]. \quad (58)$$

Substituting Eq. (9) in Eq. (58), then

$$E_0 = \tfrac{1}{4}[1-b], \quad (59)$$

which agrees with Eqs. (52) and (55). According to Eq. (59), E_0 is a monotonically decreasing function of b, and the problem of minimizing b, subject to constant E, can be inverted so that E is minimized, subject to constant b. One also sees by substituting Eqs. (59) and (53) in Eq. (26) that Eq. (57) is again obtained, and since Eq. (57) results from minimizing b with E_0 constant, this is equivalent to minimizing E_0 with b constant, and is consistent with Appendix E of Ref. [11]. In the following section, the analysis is continued for an arbitrary angle between the signal bases.

III. CONDITIONS FOR POSSIBLE EXTREMA

In this section, conditions for possible relative extrema are calculated of the overlap of correlated probe states of the Fuchs-Peres probe [11,12] for an arbitrary angle between the signal bases. First, Eq. (22) can be rewritten as

$$Q = \frac{\frac{1}{2}(a+b) + (d-a)\frac{1}{2}\sin^2 2\alpha}{\{\frac{1}{4}[1+d+(a-d)\sin^2 2\alpha]^2 - \frac{1}{4}c^2 \sin^2 2\alpha\}^{1/2}}. \quad (60)$$

Also, from Eq. (16), it follows that

$$(d-a)\sin^2 2\alpha = 2E - 1 + d, \quad (61)$$

and substituting Eq. (61) in Eq. (60), one obtains

$$Q = \frac{\frac{1}{2}(a+b+d-1)+E}{\{(1-E)^2 - \frac{1}{4}c^2 \sin^2 2\alpha\}^{1/2}}. \quad (62)$$

From Eq. (61), it follows that

$$d = -\frac{2E - 1 + a\sin^2 2\alpha}{\cos^2 2\alpha}. \quad (63)$$

Next, using Eqs. (8), (9), and (63), one can show that

$$q \equiv a+b+d = (2-\tan^2 2\alpha)\sin^2\lambda \sin 2\mu + \cos^2\lambda \times \sin 2\phi[1+(1-\tan^2 2\alpha)\cos 2\theta] - \frac{2E-1}{\cos^2 2\alpha}. \quad (64)$$

Next, substituting Eqs. (8) and (11) in Eq. (16), one has

$$E = \tfrac{1}{2}[1 - \sin^2\lambda - \cos^2\lambda \cos 2\theta + \sin^2 2\alpha(\sin^2\lambda + \cos^2\lambda \cos 2\theta - \sin^2\lambda \sin 2\mu - \cos^2\lambda \cos 2\theta \sin 2\phi)]. \quad (65)$$

It then follows from Eq. (65) that

$$\sin 2\mu = \frac{\cos^2\lambda(1-\cos 2\theta) + \sin^2 2\alpha(\sin^2\lambda + \cos^2\lambda \cos 2\theta - \cos^2\lambda \cos 2\theta \sin 2\phi) - 2E}{\sin^2 2\alpha \sin^2\lambda}. \quad (66)$$

Next, substituting Eq. (66) in Eq. (64) to eliminate dependence on μ, it follows that

$$q \equiv a+b+d = \cos^2\lambda\{(2-\tan^2 2\alpha)[\cot^2 2\alpha - \cos 2\theta(\sin 2\phi + \cot^2 2\alpha)] + \sin 2\phi[1+(1-\tan^2 2\alpha)\cos 2\theta]\} - 4\csc^2 2\alpha E + 3. \quad (67)$$

Also, substituting the definition of q, Eq. (64) in Eq. (62), one obtains

$$Q = \frac{\frac{1}{2}(q-1)+E}{[(1-E)^2 - \frac{1}{4}c^2 \sin^2 2\alpha]^{1/2}}, \quad (68)$$

where q is given by Eq. (67), c is given by Eq. (10), and E is constant. Since E is constant, and q and c depend only on the variables λ, θ, and ϕ, then Q depends only on the variables λ, θ, and ϕ. It then follows that possible extrema of the overlap Q for fixed E must satisfy

$$\frac{\partial Q}{\partial \lambda} = 0, \quad (69)$$

$$\frac{\partial Q}{\partial \theta} = 0, \quad (70)$$

$$\frac{\partial Q}{\partial \phi} = 0. \quad (71)$$

In general, Eqs. (69)–(71) may determine absolute or relative maximum, minimum, or saddle points in the space of probe parameters. The minimum Q is sought here. Possible solutions to Eqs. (69)–(71), giving the values of the probe parameters at the possible extrema, are derived in Appendix A, and each possible solution corresponds to one of the following combinations in which the functions F_1, F_2, and F_3 are defined by Eqs. (A5), (A10), and (A15), respectively,

$$\sin\lambda=0,\quad \sin 2\theta=0,\quad \cos 2\phi=0, \tag{72}$$

$$\sin\lambda=0,\quad \sin 2\theta=0,\quad F_3=0, \tag{73}$$

$$\sin\lambda=0,\quad \cos 2\phi=0,\quad F_2=0, \tag{74}$$

$$\sin\lambda=0,\quad F_2=0,\quad F_3=0, \tag{75}$$

$$\cos\lambda=0, \tag{76}$$

$$\sin 2\theta=0,\quad \cos 2\phi=0,\quad F_1=0, \tag{77}$$

$$\cos\lambda=0,\quad \sin 2\theta=0,\quad F_1=0, \tag{78}$$

$$\sin 2\theta=0,\quad F_1=0,\quad F_3=0, \tag{79}$$

$$\cos\lambda=0,\quad F_1=0, \tag{80}$$

$$\cos 2\phi=0,\quad F_1=0,\quad F_2=0, \tag{81}$$

$$\cos\lambda=0,\quad F_1=0,\quad F_2=0, \tag{82}$$

$$F_1=0,\quad F_2=0,\quad F_3=0. \tag{83}$$

In the following section, together with Appendix B, the possible extrema and associated probe parameters are determined from possibilities (72)–(83).

IV. EXTREMUM AND PROBE PARAMETERS

In Appendix B, possibilities (72)–(83) are addressed. Possibilities (72), (74), (75), and (81) are excluded because they cannot yield an optimization. Possibilities (73), (76)–(80), (82), and (83) all give the same result, Eq. (B10), namely,

$$Q=\frac{1+(1-2\csc^2 2\alpha)E}{1-E}, \tag{84}$$

which for $\alpha=\pi/8$ corresponds to the standard BB84 optimization, Eq. (57). However, the possibilities differ in the values of the optimized probe parameters.

First consider possibility (73). According to Eqs. (B1), (B4), and (B5), one has for the probe parameters λ, μ, θ, and ϕ,

$$\sin\lambda=0, \tag{85}$$

$$\cos 2\theta=1, \tag{86}$$

$$\sin 2\phi=1-2E\csc^2 2\alpha. \tag{87}$$

Evidently, according to Eqs. (85) and (66), the probe parameter μ is arbitrary ($0\leqslant\mu\leqslant\pi$). In summary, then for possibility (73), the optimized probe parameters are

$$\{\lambda,\mu,\theta,\phi;\sin\lambda=0,\ \cos 2\theta=1,\ \sin 2\phi=1-2E\csc^2 2\alpha\}. \tag{88}$$

Next, consider possibility (76). According to Eqs. (B81) and (B82), one has

$$\cos\lambda=0, \tag{89}$$

$$\sin 2\mu=1-2E\csc^2 2\alpha. \tag{90}$$

Evidently θ and ϕ are arbitrary ($0\leqslant\theta\leqslant\pi, 0\leqslant\phi\leqslant\pi$). Thus for possibility (76), the optimized probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha\}. \tag{91}$$

For possibility (77), according to Eqs. (B88), (B93), (B90), (B94), and (B16), the optimized probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \sin 2\mu\sin^2\lambda=1-2E\csc^2 2\alpha\mp\cos^2\lambda,\ \cos 2\theta=1,\ \sin 2\phi=\pm 1\}. \tag{92}$$

For possibility (78), according to Eqs. (B95), (B97), (B99), and (B101) or (B102), the optimized probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha,\ \cos 2\theta=1\} \tag{93}$$

or

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha,\ \sin 2\phi=1-2\cot^2 2\alpha,\ \cos 2\theta=e_\theta\}. \tag{94}$$

Equations (93) and (94) are apparently included in Eq. (91).

For possibility (79), according to Eqs. (B107) and (B109), one has

$$\{\lambda,\mu,\theta,\phi;\ \sin 2\mu\sin^2\lambda=1-2E\csc^2 2\alpha-\cos^2\lambda\sin 2\phi,\cos 2\theta=1\}. \tag{95}$$

Evidently Eqs. (88) and (92) are included in Eq. (95).

For possibility (80), according to Eqs. (B110), (B112), and (B114) or (B115), one has

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha,\ \cos 2\theta=1\}, \tag{96}$$

or, alternatively

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha,\ \sin 2\phi=1-2\cot^2 2\alpha\}. \tag{97}$$

Equations (96) and (97) are evidently included in Eq. (91).

For possibility (82), according to Eqs. (B121), (B124), and (B125), the optimum probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha,\ \sin 2\phi=1-2\cot^2 2\alpha\}. \tag{98}$$

Comparing Eq. (98) with Eq. (91), it is evident that Eq. (98) is included in Eq. (91)

Finally, for possibility (83), according to Eqs. (B132)–(B134), the optimum probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \sin 2\mu\sin^2\lambda=1-2E\csc^2 2\alpha-\cos^2\lambda\sin 2\phi,\ \cos 2\theta=1,\ \cos^2\lambda=2(1-E)^2(1-2\cot^2 2\alpha-\sin 2\phi)$$
$$\times\{\sin^2 2\alpha\cos^2 2\phi[1+(1-2\csc^2 2\alpha)E]\}^{-1}\}. \tag{99}$$

Comparing Eq. (99) with Eq. (95), one sees that Eq. (99) is included in Eq. (95).

Equations (91) and (95) are different possible sets of optimized probe parameters, both of which correspond to the same optimization, Eq. (84). In summary, the optimized sets of probe parameters are

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha\}, \tag{100}$$

$$\{\lambda,\mu,\theta,\phi;\ \sin 2\mu\sin^2\lambda=1-2E\csc^2 2\alpha-\cos^2\lambda\sin 2\phi,\cos 2\theta=1\}. \tag{101}$$

For $\alpha=\pi/8$, these reduce to

$$\{\lambda,\mu,\theta,\phi;\ \cos\lambda=0,\ \sin 2\mu=1-4E\}, \tag{102}$$

$$\{\lambda,\mu,\theta,\phi;\ \sin 2\mu\sin^2\lambda=1-4E-\cos^2\lambda\sin 2\phi,\ \cos 2\theta=1\}. \tag{103}$$

Equation (103), for $\sin\lambda=0$, corresponds to the standard optimization in Ref. [11] and in Sec. II above, but, other than that, the two sets of optimized probe parameters given by Eqs. (102) and (103) were not found by the simplified arguments appearing there. Both Eqs. (102) and (103) [together with Eqs. (8)–(11), (24), and (26)] yield Eq. (57). It can also be shown that all sets of optimum probe parameters following from Eqs. (36)–(43) are subsets of Eq. (101), and also yield Eq. (57).

V. MAXIMUM INFORMATION GAIN

In Sec. IV, it was determined that the only remaining possible extremum of the overlap Q of correlated probe states for fixed error rate E is given by Eq. (84). I have found that if one plots points using the general expression for the nonoptimized overlap given by the parametric Eqs. (60) and (16) along with Eqs. (8)–(11) for a representative range of values of the error rate E and the probe parameters λ, μ, θ, and ϕ, and for a range of $\alpha\leqslant\pi/8$, the nonoptimized values of Q all lie above the corresponding curves given by Eq. (84). Also, by explicitly calculating the difference between the optimized overlap, Eq. (84), and the nonoptimized overlap, Eqs. (60) and (16), for representative ranges of the error rate and the probe parameters in the neighborhood surrounding each of the optimized sets, Eqs. (100) and (101), I have found that for $\alpha=\pi/8$ or $\pi/9$, the nonoptimized overlap is not decreasing, and therefore Eq. (84) does in fact represent a minimum. Also, it is evident from Eq. (84) that the minimum overlap Q, for constant E, decreases as α decreases below $\pi/8$. Apparently, the optimization holds for $\alpha\leqslant\pi/8$. However, for $\alpha>\pi/8$, this is not the case [points resulting from Eqs. (60) and (16) fall above and below the curves given by Eq. (84)], and therefore the extremization does not correspond to a minimum for $\alpha>\pi/8$. [For example, if $\alpha=\pi/8+10^{-6}$, $E=0.2$, $\mu/\pi=0.156\,816$, $\lambda/\pi=0.3$, $\theta/\pi=0.1$, and $\phi/\pi=0.75$, one obtains, using Eqs. (16), (60), and (8)–(11), the value $Q=0.500\,003$ for the nonoptimized overlap; but Eq. (84) yields a larger value, $Q=0.500\,004$. Also, if $\alpha=\pi/5$, $E=0.3$, $\mu/\pi=0.071\,127\,5$, $\lambda/\pi=0.7$, $\theta/\pi=0.7$, and $\phi/\pi=0.7$, one obtains $Q=0.348\,28$ for the nonoptimized overlap, but Eq. (84) yields $Q=0.909\,509$.]

However, it is at this point essential to note the invariance of the error rate E, Eq. (1), and the overlap Q, Eq. (17), under an interchange of the states $|u\rangle$ and $|\overline{u}\rangle$; thus

$$\{E,Q\}\xrightarrow[|u\rangle\leftrightarrow|\overline{u}\rangle]{}\{E,Q\}. \tag{104}$$

Also, from Fig. 2 of Ref. [11], it is evident that under the interchange of $|u\rangle$ and $|\overline{u}\rangle$, the angle $\overline{\theta}$ between the nonorthogonal polarization states becomes 2α; thus

$$\overline{\theta}\xrightarrow[|u\rangle\leftrightarrow|\overline{u}\rangle]{}2\alpha, \tag{105}$$

or equivalently, since $\overline{\theta}=\pi/2-2\alpha$,

$$\alpha\xrightarrow[|u\rangle\leftrightarrow|\overline{u}\rangle]{}\frac{\pi}{4}-\alpha. \tag{106}$$

Also, using Eq. (106), one has

$$\{\alpha\leqslant\pi/8\}\xrightarrow[|u\rangle\leftrightarrow|\overline{u}\rangle]{}\{\alpha\geqslant\pi/8\}. \tag{107}$$

It then follows from Eqs. (84), (106), and (107) that the optimum overlap,

$$Q=\frac{1+(1-2\csc^2 2\alpha)E}{1-E}, \quad \alpha\leqslant\pi/8, \tag{108}$$

becomes

$$Q=\frac{1+\left[1-2\csc^2 2\left(\frac{\pi}{4}-\alpha\right)\right]E}{1-E}, \quad \alpha\geqslant\pi/8, \tag{109}$$

or equivalently,

$$Q=\frac{1+(1-2\sec^2 2\alpha)E}{1-E}, \quad \alpha\geqslant\pi/8. \tag{110}$$

Also, the optimized sets of probe parameters, Eqs. (100) and (101), namely,

$$\{\lambda,\mu,\theta,\phi;\cos\lambda=0,\ \sin 2\mu=1-2E\csc^2 2\alpha\}, \quad \alpha\leqslant\pi/8, \tag{111}$$

$$\{\lambda,\mu,\theta,\phi;\sin 2\mu\sin^2\lambda=1-2E\csc^2 2\alpha-\cos^2\lambda\sin 2\phi,\ \cos 2\theta=1\}, \quad \alpha\leqslant\pi/8 \tag{112}$$

become, for $\alpha\rightarrow\pi/4-\alpha$,

$$\{\lambda,\mu,\theta,\phi;\cos\lambda=0,\ \sin 2\mu=1-2E\sec^2 2\alpha\}, \quad \alpha\geqslant\pi/8, \tag{113}$$

$$\{\lambda,\mu,\theta,\phi;\sin 2\mu\sin^2\lambda=1-2E\sec^2 2\alpha-\cos^2\lambda\sin 2\phi,\ \cos 2\theta=1\}, \quad \alpha\geqslant\pi/8. \tag{114}$$

I have found that if one plots points using the general expression for the nonoptimized overlap, given by the parametric Eqs. (60) and (16) along with Eqs. (8)–(11), for a representative range of values of the error rate E and the probe parameters λ, μ, θ, and ϕ, for a range of $\alpha\geqslant\pi/8$, the nonoptimized values of Q all lie above the corresponding curves given by Eq. (110). Apparently, for $\alpha\geqslant\pi/8$, the optimization, Eq. (110), holds.

With the restrictions on α, the maximum Renyi information gain by the probe is given by Eq. (23), namely, Refs. [11,13–15],

$$I^R_{\rm opt}=\log_2(2-Q^2), \tag{115}$$

where Q is given by Eq. (108) for $\alpha\leqslant\pi/8$, and Eq. (110) for $\alpha\geqslant\pi/8$, or

$$Q=\begin{cases}\dfrac{1+(1-2\csc^2 2\alpha)E}{1-E}, & \alpha\leqslant\pi/8\\[2ex] \dfrac{1+(1-2\sec^2 2\alpha)E}{1-E}, & \alpha\geqslant\pi/8.\end{cases} \tag{116}$$

Thus for the BB84 protocol, one has

$$I^R_{\rm opt}=\begin{cases}\log_2\left(2-\left[\dfrac{1+(1-2\csc^2 2\alpha)E}{1-E}\right]^2\right), & \alpha\leqslant\pi/8\\[2ex] \log_2\left(2-\left[\dfrac{1+(1-2\sec^2 2\alpha)E}{1-E}\right]^2\right), & \alpha\geqslant\pi/8.\end{cases} \tag{117}$$

For $\alpha=\pi/8$, Eq. (117) produces Fig. 6 of Ref. [11], as it must. Also, $I^R_{\rm opt}$ in Eq. (117) increases as α decreases below $\pi/8$, or increases above $\pi/8$. The standard BB84 protocol with $\alpha=\pi/8$ yields the least information. Equation (117) can be used in the calculation of the secrecy capacity of the BB84 protocol [16,17].

VI. SUMMARY

The maximum Renyi information gain, Eq. (117), by a Fuchs-Peres probe [11,12] is calculated for a varying angle between the signal bases in the four-state protocol [2] of quantum key distribution. The invariance of the error rate and overlap under signal-state interchange, Eq. (104), was exploited to accommodate any angle between the signal bases in the optimization. Two sets of optimized probe parameters, Eqs. (111) and (112) for $\alpha\leqslant\pi/8$, and Eqs. (113) and (114) for $\alpha\geqslant\pi/8$, are found to yield the optimization. Only a subset of one of these sets was found previously [11], for $\alpha=\pi/8$ [Eq. (112) with $\sin\lambda=0$ and $\alpha=\pi/8$, or equivalently Eq. (103) with $\sin\lambda=0$]. When the angle between the signal bases is the standard 45° ($\alpha=\pi/8$), the result, Eq. (57), of Slutsky, Rao, Sun, and Fainman [11] is recovered. It was shown by explicit calculations that Eq. (117) gives the maximum information gain by the probe for a representative range of values of α. Also, the maximum Renyi information, Eq. (117), for constant error rate, increases as α decreases below $\pi/8$, or increases above $\pi/8$. However, sensitivity to practical tuning variations in the angle can be useful in quantifying tolerances.

ACKNOWLEDGMENTS

This work was supported in part by the U.S. Army Research Laboratory, the Defense Advanced Research Projects

Agency, and the National Science Foundation under Grant No. PHY99-07949. The hospitality of the Institute of Theoretical Physics at the University of California at Santa Barbara, where part of this work was performed, is gratefully acknowledged. The author wishes to thank David Gross for inviting him to participate in the program, *Quantum Information*, at the Institute of Theoretical Physics. Also, the author thanks John Myers for alerting him to the useful symmetry involving the signal states. He also thanks S. J. Lomonaco, J. D. Franson, M. Foster, and J. D. Murley for stimulating communications.

APPENDIX A: EXTREMA CONDITIONS

In this appendix, the sets of conditions given by Eqs. (72)–(83) for the existence of possible extrema of the overlap of correlated probe states are determined by using Eqs. (69)–(71). First, substituting Eq. (68) in Eq. (69), one obtains

$$\frac{\partial q}{\partial \lambda}+\frac{q-1+2E}{[4(1-E)^2-c^2\sin^2 2\alpha]}\sin^2 2\alpha c\frac{\partial c}{\partial \lambda}=0. \quad \text{(A1)}$$

Using Eqs. (67) and (10), it follows that

$$\frac{\partial q}{\partial \lambda}=-2(\cos\lambda\sin\lambda)\{(2-\tan^2 2\alpha)\times[\cot^2 2\alpha-\cos 2\theta(\sin 2\phi+\cot^2 2\alpha)]+\sin 2\phi[1+(1-\tan^2 2\alpha)\cos 2\theta]\}, \quad \text{(A2)}$$

$$c\frac{\partial c}{\partial \lambda}=-2\cos^3\lambda\sin\lambda\sin^2 2\theta\cos^2 2\phi. \quad \text{(A3)}$$

Then substituting Eqs. (A2) and (A3) in Eq. (A1), one requires

$$\sin\lambda\cos\lambda F_1(\lambda,\theta,\phi)=0, \quad \text{(A4)}$$

where

$$F_1(\lambda,\theta,\phi)=2\{(2-\tan^2 2\alpha)[\cot^2 2\alpha-\cos 2\theta(\sin 2\phi+\cot^2 2\alpha)]+\sin 2\phi[1+(1-\tan^2 2\alpha)\cos 2\theta]\}+\frac{2(q-1+2E)}{4(1-E)^2-c^2\sin^2 2\alpha}\sin^2 2\alpha\cos^2\lambda\sin^2 2\theta\cos^2 2\phi. \quad \text{(A5)}$$

Next, substituting Eq. (68) in Eq. (70), one obtains

$$\frac{\partial q}{\partial \theta}+\frac{q-1+2E}{[4(1-E)^2-c^2\sin^2 2\alpha]}\sin^2 2\alpha c\frac{\partial c}{\partial \theta}=0. \quad \text{(A6)}$$

Using Eqs. (67) and (10), it follows that

$$\frac{\partial q}{\partial \theta}=2\sin 2\theta\cos^2\lambda(\sin 2\phi+2\cot^2 2\alpha-1), \quad \text{(A7)}$$

$$c\frac{\partial c}{\partial \theta}=2\sin 2\theta\cos^4\lambda\cos 2\theta\cos^2 2\phi. \quad \text{(A8)}$$

Then substituting Eqs. (A7) and (A8) in Eq. (A6), one requires

$$\sin 2\theta\cos^2\lambda F_2(\lambda,\theta,\phi)=0, \quad \text{(A9)}$$

where

$$F_2(\lambda,\theta,\phi)=2(\sin 2\phi+2\cot^2 2\alpha-1)+\frac{2(q-1+2E)}{[4(1-E)^2-c^2\sin^2 2\alpha]}\times\sin^2 2\alpha\cos^2\lambda\cos 2\theta\cos^2 2\phi. \quad \text{(A10)}$$

Next, substituting Eq. (68) in Eq. (71), one obtains

$$\frac{\partial q}{\partial \phi}+\frac{q-1+2E}{[4(1-E)^2-c^2\sin^2 2\alpha]}\sin^2 2\alpha c\frac{\partial c}{\partial \phi}=0. \quad \text{(A11)}$$

Using Eqs. (67) and (10), one gets

$$\frac{\partial q}{\partial \phi}=2\cos^2\lambda\cos 2\phi(1-\cos 2\theta), \quad \text{(A12)}$$

$$c\frac{\partial c}{\partial \phi}=-2\cos^4\lambda\sin^2 2\theta\sin 2\phi\cos 2\phi. \quad \text{(A13)}$$

Then substituting Eqs. (A12) and (A13) in Eq. (A11), one requires

$$\cos^2\lambda\cos 2\phi F_3(\lambda,\theta,\phi)=0, \quad \text{(A14)}$$

where

$$F_3(\lambda,\theta,\phi)=2(1-\cos 2\theta)-\frac{2(q-1+2E)}{[4(1-E)^2-c^2\sin^2 2\alpha]}\times\sin^2 2\alpha\cos^2\lambda\sin^2 2\theta\sin 2\phi. \quad \text{(A15)}$$

Summarizing Eqs. (A4), (A9), and (A14), possible extrema of the overlap of correlated probe states are determined by

$$\sin\lambda\cos\lambda F_1(\lambda,\theta,\phi)=0, \tag{A16}$$

$$\sin 2\theta\cos^2\lambda F_2(\lambda,\theta,\phi)=0, \tag{A17}$$

$$\cos^2\lambda\cos 2\phi F_3(\lambda,\theta,\phi)=0. \tag{A18}$$

Three possible ways of satisfying Eq. (A16) are

$$\sin\lambda=0, \tag{A19}$$

$$\cos\lambda=0, \tag{A20}$$

$$F_1=0. \tag{A21}$$

Two possible ways of satisfying Eqs. (A19) and (A17) are

$$\sin\lambda=0,\quad \sin 2\theta=0, \tag{A22}$$

$$\sin\lambda=0,\quad F_2=0. \tag{A23}$$

Two possible ways of satisfying Eqs. (A22) and (A18), and therefore also Eqs. (A16) and (A17), are

$$\sin\lambda=0,\quad \sin 2\theta=0,\quad \cos 2\phi=0, \tag{A24}$$

$$\sin\lambda=0,\quad \sin 2\theta=0,\quad F_3=0. \tag{A25}$$

Two possible ways of satisfying Eqs. (A23) and (A18), and therefore also Eqs. (A16) and (A17), are

$$\sin\lambda=0,\quad \cos 2\phi=0,\quad F_2=0, \tag{A26}$$

$$\sin\lambda=0,\quad F_2=0,\quad F_3=0. \tag{A27}$$

Equation (A20) satisfies Eqs. (A17) and (A18). Therefore, another way of satisfying Eqs. (A16)–(A18) is

$$\cos\lambda=0. \tag{A28}$$

Three possible ways of satisfying Eqs. (A21) and (A17) are

$$F_1=0,\quad \sin 2\theta=0, \tag{A29}$$

$$F_1=0,\quad \cos\lambda=0, \tag{A30}$$

$$F_1=0,\quad F_2=0. \tag{A31}$$

Three possible ways of satisfying Eqs. (A29) and (A18), and therefore also Eqs. (A16) and (A17), are

$$F_1=0,\quad \sin 2\theta=0,\quad \cos 2\phi=0, \tag{A32}$$

$$F_1=0,\quad \sin 2\theta=0,\quad \cos\lambda=0, \tag{A33}$$

$$F_1=0,\quad \sin 2\theta=0,\quad F_3=0. \tag{A34}$$

Equation (A30) satisfies Eq. (A18), and therefore, another way of satisfying Eqs. (A16)–(A18) is

$$F_1=0,\quad \cos\lambda=0. \tag{A35}$$

Three possible ways of satisfying Eqs. (A31) and (A18), and therefore also Eqs. (A16) and (A17), are

$$F_1=0,\quad F_2=0,\quad \cos 2\phi=0, \tag{A36}$$

$$F_1=0,\quad F_2=0,\quad \cos\lambda=0, \tag{A37}$$

$$F_1=0,\quad F_2=0,\quad F_3=0. \tag{A38}$$

Summarizing Eqs. (A24)–(A28) and (A32)–(A38), possible solutions to Eqs. (A16)–(A18) are determined by Eqs. (72)–(83).

APPENDIX B: POSSIBLE EXTREMA OF OVERLAP OF CORRELATED PROBE STATES

In this appendix, possible extrema of the overlap of correlated probe states, and also the associated probe parameters, are calculated. First consider possible extrema determined by possibility (73):

$$\sin\lambda=0, \tag{B1}$$

$$\sin 2\theta=0, \tag{B2}$$

$$F_3=0. \tag{B3}$$

From Eqs. (A15), (B2), and (B3), it follows that

$$\cos 2\theta=1. \tag{B4}$$

Substituting Eqs. (B1) and (B4) in Eq. (66), it follows that

$$\sin 2\phi=1-2E\csc^2 2\alpha. \tag{B5}$$

Next, substituting Eqs. (B1), (B2), and (B4) in Eqs. (8)–(11), one obtains

$$a=\sin 2\phi, \tag{B6}$$

$$b=\sin 2\phi, \tag{B7}$$

$$c=0, \tag{B8}$$

$$d=1. \tag{B9}$$

Then substituting Eqs. (B5)–(B9) in Eq. (62), one obtains

$$Q=\frac{1+(1-2\csc^2 2\alpha)E}{1-E}. \tag{B10}$$

For $\alpha=\pi/8$, Eq. (B10) becomes Eq. (57), corresponding to the standard BB84 optimization [11].

Next, consider possibility (72),

$$\sin\lambda=0, \tag{B11}$$

$$\sin 2\theta=0, \tag{B12}$$

$$\cos 2\phi=0. \tag{B13}$$

From Eqs. (B12) and (B13), it follows that

$$\cos 2\theta = e_\theta \tag{B14}$$

and

$$\sin 2\phi = e_\phi, \tag{B15}$$

where

$$e_\theta = \pm 1, \quad e_\phi = \pm 1. \tag{B16}$$

Substituting Eqs. (B11), (B14), and (B15) in Eq. (65), then one requires

$$E = \tfrac{1}{2}[1 - e_\theta + e_\theta(1 - e_\phi)\sin^2 2\alpha]. \tag{B17}$$

Next, substituting Eqs. (B11)–(B16) in Eqs. (8)–(11), one obtains

$$a = e_\theta e_\phi, \tag{B18}$$

$$b = e_\phi, \tag{B19}$$

$$c = 0, \tag{B20}$$

$$d = e_\theta. \tag{B21}$$

Then substituting Eqs. (B17)–(B21) in Eq. (62), one obtains

$$Q = \frac{e_\phi(1 + e_\theta) + e_\theta(1 - e_\phi)\sin^2 2\alpha}{(1 + e_\theta) - e_\theta(1 - e_\phi)\sin^2 2\alpha}. \tag{B22}$$

For $e_\theta = \pm 1$ and $e_\phi = +1$, Eq. (B22) yields

$$Q = 1. \tag{B23}$$

For $e_\theta = \pm 1$ and $e_\phi = -1$, Eq. (B22) yields

$$Q = -1. \tag{B24}$$

One concludes that possibility (72) does not yield the minimum overlap.

Next, consider possibility (74),

$$\sin\lambda = 0, \tag{B25}$$

$$\cos 2\phi = 0, \tag{B26}$$

$$F_2 = 0. \tag{B27}$$

Next, substituting Eqs. (A10) and (B26) in Eq. (B27), one obtains

$$\sin 2\phi = 1 - 2\cot^2 2\alpha. \tag{B28}$$

Then combining Eqs. (B26) and (B28), one requires

$$\cot^2 2\alpha = \tfrac{1}{2}(1 - e_\phi), \tag{B29}$$

and therefore using Eq. (B16), one requires $e_\phi = -1$, and

$$\alpha = \pi/8. \tag{B30}$$

Furthermore, using Eqs. (B25), (B26), and (B30) in Eq. (66), one requires

$$E = \tfrac{1}{2}. \tag{B31}$$

Therefore possibility (74) does not yield a solution.

Next consider possibility (75),

$$\sin\lambda = 0, \tag{B32}$$

$$F_2 = 0, \tag{B33}$$

$$F_3 = 0. \tag{B34}$$

Using Eqs. (B32) and (10), one has

$$c = \sin 2\theta \cos 2\phi. \tag{B35}$$

Also, using Eqs. (B32), (B33), and (A10), one requires

$$\left[\frac{q - 1 + 2E}{4(1-E)^2 - c^2\sin^2 2\alpha}\right] = \frac{(1 - 2\cot^2 2\alpha - \sin 2\phi)}{\sin^2 2\alpha \cos 2\theta \cos^2 2\phi}. \tag{B36}$$

Also, Eqs. (B32), (B34), and (A15) require

$$\left[\frac{q - 1 + 2E}{4(1-E)^2 - c^2\sin^2 2\alpha}\right] = \frac{1 - \cos 2\theta}{\sin^2 2\alpha \sin^2 2\theta \sin 2\phi}. \tag{B37}$$

Furthermore, using Eq. (B32), Eq. (67) becomes

$$q = (2 - \tan^2 2\alpha)[\cot^2 2\alpha - \cos 2\theta(\sin 2\phi + \cot^2 2\alpha)] + \sin 2\phi[1 + (1 - \tan^2 2\alpha)\cos 2\theta] - 4E\csc^2 2\alpha + 3. \tag{B38}$$

Next equating Eqs. (B36) and (B37) requires

$$(1 - 2\cot^2 2\alpha - \sin 2\phi)\sin^2 2\theta \sin 2\phi = (1 - \cos 2\theta)\cos 2\theta \cos^2 2\phi. \tag{B39}$$

Next, multiplying Eq. (66) by $\sin^2\lambda$ and substituting Eq. (B32), one gets

$$\cos 2\theta = \frac{1 - 2E}{1 - \sin^2 2\alpha(1 - \sin 2\phi)}. \tag{B40}$$

Then substituting Eq. (B40) in Eq. (B39), one obtains

$$(1 - 2\cot^2 2\alpha - \sin 2\phi)\sin 2\phi\{[1 - \sin^2 2\alpha(1 - \sin 2\phi)]^2 - (1 - 2E)^2\} = (1 - 2E)\cos^2 2\phi[1 - \sin^2 2\alpha(1 - \sin 2\phi) - (1 - 2E)], \tag{B41}$$

or equivalently,

$$[1-\sin^2 2\alpha(1-\sin 2\phi)-(1-2E)]\{(1-2E)\cos^2 2\phi-(1-2\cot^2 2\alpha-\sin 2\phi)$$
$$\times\sin 2\phi[1-\sin^2 2\alpha(1-\sin 2\phi)+(1-2E)]\}=0. \tag{B42}$$

Therefore, either

$$[1-\sin^2 2\alpha(1-\sin 2\phi)-(1-2E)]=0 \tag{B43}$$

or else

$$(1-2E)\cos^2 2\phi-(1-2\cot^2 2\alpha-\sin 2\phi)\sin 2\phi[1-\sin^2 2\alpha(1-\sin 2\phi)+(1-2E)]=0. \tag{B44}$$

Equation (B43) gives

$$\sin 2\phi=1-2E\csc^2 2\alpha, \tag{B45}$$

which when substituted in Eq. (B40) gives

$$\cos 2\theta=1, \tag{B46}$$

and substituting Eqs. (B32), (B45), (B46), and (8)–(11) in Eq. (62), one again obtains the same solution resulting from possibility (73), Eqs. (B5)–(B10). However, Eq. (B45) must also be compatible with the remaining requirements if possibility (75) is to represent a solution.

Alternatively, one has Eq. (B44), which becomes the cubic

$$a_1\sin^3 2\phi+a_2\sin^2 2\phi+a_3\sin 2\phi+a_4=0, \tag{B47}$$

where

$$a_1=\sin^2 2\alpha, \tag{B48}$$

$$a_2=3-4\sin^2 2\alpha, \tag{B49}$$

$$a_3=(2E-\cos^2 2\alpha-1)(1-2\cot^2 2\alpha), \tag{B50}$$

$$a_4=(1-2E). \tag{B51}$$

The possible solutions to the cubic Eq. (B47) are given by

$$\sin 2\phi=x-\frac{p}{3}, \tag{B52}$$

$$\sin 2\phi=x_+-\frac{p}{3}, \tag{B53}$$

$$\sin 2\phi=x_--\frac{p}{3}, \tag{B54}$$

where

$$x=c_++c_-, \tag{B55}$$

$$x_\pm=-\frac{1}{2}(c_++c_-)\pm\frac{3^{1/2}}{2}i(c_+-c_-), \tag{B56}$$

$$c_\pm=\left[-\frac{B}{2}\pm\left(\frac{B^2}{4}+\frac{A^3}{27}\right)^{1/2}\right]^{1/3}, \tag{B57}$$

$$A=\frac{1}{3}(3q-p^2), \tag{B58}$$

$$B=\frac{1}{27}(2p^3-9pq+27r), \tag{B59}$$

$$p=\frac{a_2}{a_1}, \tag{B60}$$

$$q=\frac{a_3}{a_1}, \tag{B61}$$

$$r=\frac{a_4}{a_1}. \tag{B62}$$

Next, substituting Eqs. (B35) and (B40) in Eq. (B37), one obtains

$$[2E-\sin^2 2\alpha(1-\sin 2\phi)]\left[4(1-E)^2-\frac{[2(1-E)-\sin^2 2\alpha(1-\sin 2\phi)]}{[1-\sin^2 2\alpha(1-\sin 2\phi)]^2}\{[2E-\sin^2 2\alpha(1-\sin 2\phi)]\sin^2 2\alpha\cos^2 2\phi\right.$$
$$\left.+[1-\sin^2 2\alpha(1-\sin 2\phi)](q-1+2E)\sin^2 2\alpha\sin 2\phi\}\right]=0. \tag{B63}$$

Therefore, either

$$[2E-\sin^2 2\alpha(1-\sin 2\phi)]=0 \tag{B64}$$

or else

$$4(1-E)^2=\frac{[2(1-E)-\sin^2 2\alpha(1-\sin 2\phi)]}{[1-\sin^2 2\alpha(1-\sin 2\phi)]^2}\{[2E-\sin^2 2\alpha(1-\sin 2\phi)]\sin^2 2\alpha\cos^2 2\phi+[1-\sin^2 2\alpha(1-\sin 2\phi)]$$
$$\times(q-1+2E)\sin^2 2\alpha\sin 2\phi\}. \tag{B65}$$

Equation (B64) gives

$$\sin 2\phi=1-2E\csc^2 2\alpha, \tag{B66}$$

which together with Eqs. (B40), (B32), (8)–(11), and (62) again yields the same result as possibility (73), Eqs. (B5)–(B10). However, Eqs. (B45) and (B66) must also be compatible with the remaining restrictions, if possibility (75) is to represent a solution.

Alternatively, one has Eq. (B65). The quantity q appearing in Eq. (B65) and given by Eq. (B38) reduces using Eq. (B40) to

$$q=\sin 2\phi+\frac{(1+\sin 2\phi)(1-2E)}{\cos^2 2\alpha+\sin^2 2\alpha\sin 2\phi}. \tag{B67}$$

Then substituting Eq. (B67) in Eq. (B65), one obtains the cubic

$$b_1\Lambda^3+b_2\Lambda^2+b_3\Lambda+b_4=0, \tag{B68}$$

where

$$\Lambda=\cos^2 2\alpha+\sin^2 2\alpha\sin 2\phi, \tag{B69}$$

$$b_1=(1-2E)(1-2\csc^2 2\alpha), \tag{B70}$$

$$b_2=4(1-E)^2-\sin^2 2\alpha+(1-2E)^2(1-2\csc^2 2\alpha)-(1-2E)(1+\cos^2 2\alpha-4\cot^2 2\alpha), \tag{B71}$$

$$b_3=-(1-2E)^2(1+\cos^2 2\alpha-4\cot^2 2\alpha)+(1-2E)\cos^2 2\alpha(1-2\cot^2 2\alpha), \tag{B72}$$

$$b_4=(1-2E)^2(1-2\cos^2 2\alpha\cot^2 2\alpha). \tag{B73}$$

[In obtaining Eq. (B68), an overall factor of Λ was removed and ignored, since $\Lambda=0$ can only be satisfied if $E=1/2$.]

Next, substituting Eqs. (B35), (B40), and (B67) in Eq. (B36), leads to the quintic

$$c_1\sin^5 2\phi+c_2\sin^4 2\phi+c_3\sin^3 2\phi+c_4\sin^2 2\phi+c_5\sin 2\phi+c_6=0, \tag{B74}$$

where

$$c_1=\sin^6 2\alpha, \tag{B75}$$

$$c_2=\sin^4 2\alpha(5\cos^2 2\alpha+2E-2), \tag{B76}$$

$$c_3=\sin^4 2\alpha(5-12E+8E^2)-\sin^2 2\alpha\cos^2 2\alpha(1-2E)-2\sin^2 2\alpha(1-2E)^2-2\sin^4 2\alpha\cos^2 2\alpha+5\sin^2 2\alpha\cos^4 2\alpha$$
$$-\sin^6 2\alpha, \tag{B77}$$

$$c_4=(1-2\cot^2 2\alpha)[\sin^2 2\alpha(1-2E)^2-4\sin^4 2\alpha(1-E)^2+\sin^6 2\alpha-\sin^2 2\alpha\cos^4 2\alpha]-2\sin^4 2\alpha\cos^2 2\alpha$$
$$+2\sin^4 2\alpha E(1-2E)+8\sin^2 2\alpha\cos^2 2\alpha(1-E)^2, \tag{B78}$$

$$c_5=(1-2\cot^2 2\alpha)[-8\sin^2 2\alpha\cos^2 2\alpha(1-E)^2+2\sin^4 2\alpha\cos^2 2\alpha]+4\cos^4 2\alpha(1-E)^2+\sin^2 2\alpha(2-\sin^2 2\alpha)(1-2E)^2$$
$$+\sin^2 2\alpha\cos^2 2\alpha(1-2E)-\sin^2 2\alpha\cos^4 2\alpha, \tag{B79}$$

$$c_6=(1-2\cot^2 2\alpha)[\sin^2 2\alpha\cos^4 2\alpha-4\cos^4 2\alpha(1-E)^2-\sin^2 2\alpha(1-2E)^2]+\sin^4 2\alpha(1-2E)^2. \tag{B80}$$

In summary, the possibility (75) requires that one of the following three sets of equations be satisfied: (i) Eqs. (B47), (B68), and (B74); (ii) Eqs. (B45), (B68), and (B74); (iii) Eqs. (B45) and (B74). But none of these alternatives, (i), (ii), or (iii) can be satisfied. It can be shown numerically that Eqs. (B47), (B68), and (B74) cannot be simultaneously satisfied. Evidently, it can also be shown numerically that Eqs. (B45) and (B74) cannot be simultaneously satisfied. (This has been verified explicitly for $\alpha=\pi/9$, $\pi/8$, and $\pi/5$.) Thus, possibility (75) apparently does not produce a solution.

Next, consider possibility (76),

$$\cos\lambda=0. \tag{B81}$$

Substituting Eq. (B81) in Eq. (66), one has

$$\sin 2\mu=1-2E\csc^2 2\alpha. \tag{B82}$$

Next, substituting Eqs. (B81) and (B82) in Eqs. (8)–(11), one obtains

$$a=1-2E\csc^2 2\alpha, \tag{B83}$$

$$b=1-2E\csc^2 2\alpha, \tag{B84}$$

$$c=0, \tag{B85}$$

$$d=1. \tag{B86}$$

Then substituting Eqs. (B83)–(B86) in Eq. (62), one again obtains Eq. (B10). Therefore, possibility (76), gives the same result as possibility (73). Note, however, that the probe parameter μ is restricted by Eq. (B82), and the probe parameter ϕ is unrestricted, while for possibility (73), ϕ is restricted by Eq. (B5), and μ is unrestricted. This is addressed in Sec. IV.

Next, consider possibility (77),

$$\sin 2\theta=0, \tag{B87}$$

$$\cos 2\theta=e_\theta, \tag{B88}$$

$$\cos 2\phi=0, \tag{B89}$$

$$\sin 2\phi=e_\phi, \tag{B90}$$

$$F_1=0. \tag{B91}$$

Substituting Eqs. (A5), and (B87)–(B90) in Eq. (B91), one requires

$$(1-e_\theta)[e_\phi\cot^2 2\alpha(2-\tan^2 2\alpha)+1]=0, \tag{B92}$$

and therefore

$$e_\theta=1. \tag{B93}$$

Next, substituting Eqs. (B88), (B93), and (B90) in Eq. (66), one gets

$$\sin 2\mu=\frac{\sin^2 2\alpha(1-e_\phi\cos^2\lambda)-2E}{\sin^2 2\alpha\sin^2\lambda}. \tag{B94}$$

Then substituting Eqs. (B87)–(B90), (B93), and (B94) in Eqs. (8)–(11), one again obtains Eqs. (B83)–(B86), and (B10). Thus possibility (77) also gives the same result as possibility (73). Note, however, that the probe parameters μ and λ are restricted by Eq. (B94). This is addressed in Sec. IV.

Next, consider possibility (78),

$$\cos\lambda=0, \tag{B95}$$

$$\sin 2\theta=0, \tag{B96}$$

$$\cos 2\theta=e_\theta, \tag{B97}$$

$$F_1=0. \tag{B98}$$

Substituting Eq. (B95) in Eq. (66), one gets

$$\sin 2\mu=1-2E\csc^2 2\alpha. \tag{B99}$$

Substituting Eqs. (A5) and (B95)–(B97) in Eq. (B98), one obtains

$$(1-e_\theta)[\sin 2\phi+\cot^2 2\alpha(2-\tan^2 2\alpha)]=0. \tag{B100}$$

Therefore, one requires

$$e_\theta=1, \tag{B101}$$

or alternatively,

$$\sin 2\phi=1-2\cot^2 2\alpha. \tag{B102}$$

Substituting Eqs. (B95), (B96), and (B99) in Eqs. (8)–(11), one again obtains Eqs. (B83)–(B86) and (B10). The differing values of the probe parameters are addressed in Sec. IV.

Next consider possibility (79),

$$\sin 2\theta=0, \tag{B103}$$

$$\cos 2\theta=e_\theta, \tag{B104}$$

$$F_1=0, \tag{B105}$$

$$F_3=0. \tag{B106}$$

Substituting Eqs. (A15) and (B103) in Eq. (B106), one gets

$$\cos 2\theta=1, \tag{B107}$$

and therefore

$$e_\theta=1 \tag{B108}$$

in Eq. (B104). Next, using Eqs. (A5) and (B107), one sees that Eq. (B105) is satisfied. Also, substituting Eq. (B107) in Eq. (66), one obtains

$$\sin 2\mu=\frac{\sin^2 2\alpha(1-\cos^2\lambda\sin 2\phi)-2E}{\sin^2 2\alpha\sin^2\lambda}. \tag{B109}$$

Then substituting Eqs. (B103), (B107), and (B109) in Eqs. (8)–(11), one again obtains Eqs. (B83)–(B86) and (B10). The differing values of the probe parameters are addressed in Sec. IV.

Next consider possibility (80),

$$\cos\lambda = 0, \tag{B110}$$

$$F_1 = 0. \tag{B111}$$

Substituting Eq. (B110) in Eq. (66), one gets

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha. \tag{B112}$$

Next, substituting Eqs. (A5) and (B110) in Eq. (B111), one obtains

$$(1 - \cos 2\theta)[\sin 2\phi + 2\cot^2 2\alpha - 1] = 0. \tag{B113}$$

Therefore one requires

$$\cos 2\theta = 1 \tag{B114}$$

or else

$$\sin 2\phi = 1 - 2\cot^2 2\alpha. \tag{B115}$$

Using Eqs. (B110), (B112), and (B114) or (B115) in Eqs. (8)–(11), one again obtains Eqs. (B83)–(B86) and (B10). The differing values of the probe parameters are addressed in Sec. IV.

Next, consider possibility (81),

$$\cos 2\phi = 0, \tag{B116}$$

$$\sin 2\phi = e_\phi, \tag{B117}$$

$$F_1 = 0, \tag{B118}$$

$$F_2 = 0. \tag{B119}$$

Then substituting Eqs. (A10) and (B117) in Eq. (B119), one gets

$$\cot^2 2\alpha = \frac{1}{2}(1 - e_\phi), \tag{B120}$$

which cannot be satisfied for arbitrary α. Therefore possibility (81) cannot represent a solution.

Next, consider possibility (82),

$$\cos\lambda = 0, \tag{B121}$$

$$F_1 = 0, \tag{B122}$$

$$F_2 = 0. \tag{B123}$$

Substituting Eqs. (A10) and (B121) in Eq. (B123), one obtains

$$\sin 2\phi = 1 - 2\cot^2 2\alpha. \tag{B124}$$

Next, substituting Eqs. (A5), (B121), and (B124) in Eq. (B122), one gets a trivial identity for any $\cos 2\theta$. Then substituting Eq. (B121) in Eq. (66), one obtains

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha, \tag{B125}$$

and, using Eqs. (B121), (B125), (8)–(11), and (62), then Eqs. (B83)–(B86) and (B10) again follow. The differing values of the probe parameters are addressed in Sec. IV.

Next consider possibility (83),

$$F_1 = 0, \tag{B126}$$

$$F_2 = 0, \tag{B127}$$

$$F_3 = 0. \tag{B128}$$

From Eqs. (A5) and (B126), it follows that

$$\sin^2 2\alpha \cos^2\lambda \left[\frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha}\right] = -\frac{-2\{(2-\tan^2 2\alpha)[\cot^2 2\alpha - \cos 2\theta(\sin 2\phi + \cot^2 2\alpha)] + \sin 2\phi[1 + (1-\tan^2 2\alpha)\cos 2\theta]\}}{\sin^2 2\theta \cos^2 2\phi}. \tag{B129}$$

From Eqs. (A10) and (B127), one gets

$$\sin^2 2\alpha \cos^2\lambda \left[\frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha}\right] = \frac{-2(\sin 2\phi + 2\cot^2 2\alpha - 1)}{\cos 2\theta \cos^2 2\phi}. \tag{B130}$$

From Eqs. (A15) and (B128), one gets

$$\sin^2 2\alpha \cos^2\lambda \left[\frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha}\right] = \frac{2(1-\cos 2\theta)}{\sin^2 2\theta \sin 2\phi}. \tag{B131}$$

Next, equating Eqs. (B129) and (B131) leads to

$$\cos 2\theta = 1, \tag{B132}$$

and Eqs. (B129) and (B131) are both identically satisfied. But then substituting Eq. (B132), (67), and (10) in Eq. (B130), one obtains

$$\cos^2\lambda = \frac{2(1-E)^2(1-2\cot^2 2\alpha - \sin 2\phi)}{\sin^2 2\alpha \cos^2 2\phi[1+(1-2\csc^2 2\alpha)E]}. \tag{B133}$$

Also, substituting Eqs. (B132) in Eq. (66) gives

$$\sin 2\mu \sin^2\lambda = 1-2E\csc^2 2\alpha - \cos^2\lambda \sin 2\phi. \tag{B134}$$

Furthermore, substituting Eqs. (B132) and (B134) in Eqs. (8)–(11) yields

$$a = 1-2E\csc^2 2\alpha, \tag{B135}$$

$$b = 1-2E\csc^2 2\alpha, \tag{B136}$$

$$c = 0, \tag{B137}$$

$$d = 1. \tag{B138}$$

Then substituting Eqs. (B135)–(B138) in Eq. (62), one again obtains Eq. (B10). The differing values of the probe parameters are addressed in Sec. IV.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[3] C. H. Bennett and G. Brassard, IBM Tech. Discl. Bull. **28**, 3153 (1985).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[5] G. Vernam, J. Am. Inst. Electr. Eng. **45**, 295 (1926).
[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[7] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[8] H. E. Brandt, Am. J. Phys. **67**, 434 (1999).
[9] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[11] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[12] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[13] H. E. Brandt, Phys. Rev. A **59**, 2665 (1999).
[14] H. E. Brandt, Phys. Rev. A **62**, 042310 (2000).
[15] H. E. Brandt, Phys. Rev. A **64**, 042316 (2001).
[16] B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and S. Fainman, Appl. Opt. **37**, 2869 (1998).
[17] H. E. Brandt, J. Math. Phys. **43**, 4526 (2002).