# Quantum-cryptographic entangling probe

Howard E. Brandt*
*U. S. Army Research Laboratory, Adelphi, Maryland 20783, USA*
(Received 20 September 2004; published 6 April 2005)

For a general entangling probe attacking the Bennett-Brassard 1984 protocol in quantum key distribution, I calculate three classes of optimized unitary transformations, all yielding the same maximum information to the probe. The simplest one corresponds to a probe having a two-dimensional Hilbert space of states, and is uniquely determined by the error rate induced by the probe in the legitimate receiver. The second class corresponds to a probe having a four-dimensional Hilbert space of states, and is determined by the error rate and two continuous angle parameters which are mutually constrained by the error rate. The third class corresponds to a probe having a four-dimensional Hilbert space, and is determined by the error rate and two continuous angle parameters, one of which is constrained by the error rate. Furthermore, I show that the simplest quantum circuit representing the optimal entangling probe consists of a single controlled-NOT gate in which the control qubit consists of two polarization-basis states of the signal, the target qubit consists of two probe-basis states, and the initial state of the probe is set by the error rate. A method is determined for measuring the appropriate correlated state of the probe. Finally, a possible implementation of the entangling probe is described.

DOI: 10.1103/PhysRevA.71.042312 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta, 03.65.Ud

## I. INTRODUCTION

For the standard four-state Bennett-Brassard 1984 (BB84) protocol [1] of key distribution in quantum cryptography, Slutsky *et al.* [2] performed an eavesdropping probe optimization, which on average yields the most information to the eavesdropper for a given error rate caused by the probe. The most general possible probe consistent with unitarity was considered [2–7], in which each individual transmitted bit is made to interact with the probe so that the carrier and the probe are left in an entangled state, and measurement of the probe then 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 set error rate induced by the probe in the legitimate receiver. [Recall that the Renyi information [2,4] on an $l$-bit string $X$, having probability $P_X(X)$, is $l+\log_2\Sigma_X P_X^2(X)$.] The results of the optimization were obtained for the standard protocol with an angle of 45° between the signal bases.

In more recent work [3,5,6], a larger set of optimum probe parameters was found than was known previously. It consists of three distinct optimum sets, and although they all yield the same maximum Renyi information gain by the probe, alternative options are made available for optimum probe design. In Sec. II of the present work, the corresponding optimized unitary transformations, representing the action of the probe on the signal, are calculated. I have determined three classes of optimized unitary transformations, all yielding the same maximum information to the probe. The simplest one corresponds to a probe having a two-dimensional Hilbert space of states, and is uniquely determined by the error rate. The second class corresponds to a probe having a four-dimensional Hilbert space of states, and is determined by the error rate and two continuous angle parameters which are mutually constrained by the error rate. The third class corresponds to a probe having a four-dimensional Hilbert space, and is determined by the error rate and two continuous angle parameters, one of which is constrained by the error rate. Furthermore, it is shown in Sec. III that the simplest quantum circuit representing the entangling probe is one corresponding to the simplest optimal unitary transformation, for which the Hilbert space of the probe is only two dimensional. The quantum circuit consists of a single controlled-NOT (CNOT) gate in which the control is a polarization-basis state of the signal, the target is a probe-basis state, and the initial state of the probe is set by the error rate. In Sec. IV, a method is determined for measuring the appropriate correlated states of the probe. In Sec. V, I propose an implementation of the entangling probe. Section VI contains a brief summary.

## II. OPTIMUM ENTANGLING PROBE

The unitary transformation describing the interaction of the entangling probe with the BB84 signal basis states is determined by Eqs. (2)–(4) of Ref. [2], namely,

$$|e_m \otimes w\rangle \rightarrow U|e_m \otimes w\rangle = \sum_n |e_n\rangle \otimes |\Phi_{mn}\rangle. \tag{1}$$

Here $|e_m \otimes w\rangle$ is the tensor product of the initial state $|w\rangle$ of the probe with the orthonormal basis state $|e_m\rangle$ in the two-dimensional Hilbert space of the signal. The signal basis states are given by

$$|e_0\rangle = \cos\frac{\pi}{8}|u\rangle - \sin\frac{\pi}{8}|\overline{u}\rangle, \tag{2}$$

*Electronic address: hbrandt@arl.army.mil

 

$$|e_1\rangle = \cos\frac{\pi}{8}|v\rangle - \sin\frac{\pi}{8}|\overline{v}\rangle, \tag{3}$$

expressed in terms of the BB84 linearly-polarized-photon signal states $\{|u\rangle, |\overline{u}\rangle, |v\rangle, |\overline{v}\rangle\}$, for $\alpha = \pi/8$. Here $\alpha$ is half the complement of the angle between the nonorthogonal signal bases $\{|u\rangle, |\overline{u}\rangle\}$ and $\{|v\rangle, |\overline{v}\rangle\}$ and the state $|\overline{u}\rangle$ is orthogonal to $|u\rangle$, and the state $|\overline{v}\rangle$ is orthogonal to $|v\rangle$. (Here and throughout, only linear polarization states are considered.) It is to be understood here that the states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, and $|\overline{v}\rangle$ correspond to Boolean states $|1\rangle$, $|0\rangle$, $|1\rangle$, and $|0\rangle$, respectively [2]. Also in Eq. (1), $|\Phi_{mn}\rangle$ are the states in the Hilbert space of the probe and are neither normalized nor orthogonal. Using Eqs. (3a), (3b), and (4) of Ref. [2], they can be written as follows in terms of the probe basis states $\{|w_0\rangle, |w_1\rangle, |w_2\rangle, |w_3\rangle\}$ with probe parameters $\{\lambda, \mu, \theta, \phi\}$:

$$|\Phi_{01}\rangle = X_5|w_1\rangle + X_6|w_2\rangle, \tag{4}$$

$$|\Phi_{10}\rangle = X_6|w_1\rangle + X_5|w_2\rangle, \tag{5}$$

$$|\Phi_{00}\rangle = X_0|w_0\rangle + X_1|w_1\rangle + X_2|w_2\rangle + X_3|w_3\rangle, \tag{6}$$

$$|\Phi_{11}\rangle = X_3|w_0\rangle + X_2|w_1\rangle + X_1|w_2\rangle + X_0|w_3\rangle, \tag{7}$$

where

$$X_0 = \sin\lambda\cos\mu, \tag{8}$$

$$X_1 = \cos\lambda\cos\theta\cos\phi, \tag{9}$$

$$X_2 = \cos\lambda\cos\theta\sin\phi, \tag{10}$$

$$X_3 = \sin\lambda\sin\mu, \tag{11}$$

$$X_5 = \cos\lambda\sin\theta\cos\phi, \tag{12}$$

$$X_6 = -\cos\lambda\sin\theta\sin\phi, \tag{13}$$

and

$$0 \leqslant \lambda, \mu, \theta, \phi \leqslant \pi. \tag{14}$$

The unitary transformation representing the optimum entangling probe can be obtained from Eqs. (1)–(13) by substituting the optimum probe parameters as determined in Eqs. (89), (90), and (119) in Ref. [6]. In summary, the three sets of optimum probe parameters for the standard BB84 protocol with $\alpha = \pi/8$ are

$$S^{(1)} \equiv \{\lambda, \mu, \theta, \phi; \cos\lambda = 0, \sin 2\mu = 1 - 4E\}, \tag{15}$$

$$S^{(2)} \equiv \{\lambda, \mu, \theta, \phi; \sin 2\mu \sin^2\lambda = 1 - 4E - \cos^2\lambda \sin 2\phi, \cos 2\theta = 1\}, \tag{16}$$

$$S^{(3)} \equiv \{\lambda, \mu, \theta, \phi; \sin 2\phi = -1, \sin 2\mu \sin^2\lambda = 1 - 4E + \cos^2\lambda\}, \tag{17}$$

where

$$0 \leqslant E < 1/2. \tag{18}$$

All three sets of probe parameters Eqs. (15)–(17) yield the identical maximum Renyi information gain $I^R_{\text{opt}}$ to the probe, namely [2,3,5,6],

$$I^R_{\text{opt}} = \log_2\left[2 - \left(\frac{1-3E}{1-E}\right)^2\right]. \tag{19}$$

We first evaluate the unitary transformation $U^{(1)}$ corresponding to the set $S^{(1)}$ of optimum probe parameters Eq. (15). In Eq. (15) one has

$$\sin 2\mu = 1 - 4E. \tag{20}$$

Using a trigonometric identity, it follows that

$$\cos 2\mu = \pm(1 - \sin^2 2\mu)^{1/2}. \tag{21}$$

Then substituting Eq. (20) in Eq. (21), one obtains

$$\cos 2\mu = \pm[1 - (1 - 4E)^2]^{1/2} \tag{22}$$

or

$$\cos 2\mu = \pm[8E(1 - 2E)]^{1/2}. \tag{23}$$

Also, the following trigonometric identities are true:

$$\cos\frac{x}{2} = \pm\left(\frac{1+\cos x}{2}\right)^{1/2}, \tag{24}$$

$$\sin\frac{x}{2} = \pm\left(\frac{1-\cos x}{2}\right)^{1/2}, \tag{25}$$

in which the sign depends on the quadrant in which $x/2$ lies. Consistent with Refs. [2–6], in the case of $U^{(1)}$, I extend the range in Eq. (14) to $-\pi \leqslant (\lambda, \mu) \leqslant \pi$. Then substituting Eq. (23) in Eqs. (24) and (25), one obtains

$$\cos\mu = \pm\left[\frac{1}{2}\{1 \pm [8E(1-2E)]^{1/2}\}\right]^{1/2}, \tag{26}$$

$$\sin\mu = \pm\left[\frac{1}{2}\{1 \mp [8E(1-2E)]^{1/2}\}\right]^{1/2}. \tag{27}$$

Using Eqs. (26) and (27), Eq. (15) can be rewritten as follows:

$$S^{(1)} = \left\{\lambda, \mu, \theta, \phi; \cos\lambda = 0, \cos\mu = \pm\left(\frac{1}{2}\{1 \pm [8E(1-2E)]^{1/2}\}\right)^{1/2}, \sin\mu = \pm\left(\frac{1}{2}\{1 \mp [8E(1-2E)]^{1/2}\}\right)^{1/2}\right\}. \tag{28}$$

Next, substituting Eq. (28) in Eqs. (8)–(13), one obtains

$$X_0 = \left[\frac{1}{2}\{1 \pm [8E(1-2E)]^{1/2}\}\right]^{1/2}, \tag{29}$$

$$X_1 = 0, \tag{30}$$

$$X_2 = 0, \tag{31}$$

$$X_3 = \left[\frac{1}{2}\{1 \mp [8E(1-2E)]^{1/2}\}\right]^{1/2}, \tag{32}$$

$$X_5 = 0, \tag{33}$$

$$X_6 = 0. \tag{34}$$

Note that in Eqs. (29) and (32), the overall signs must be positive in order to yield Eq. (19). Then substituting Eqs. (29)–(34) in Eqs. (4)–(7), one obtains

$$|\Phi_{01}\rangle = 0, \tag{35}$$

$$|\Phi_{10}\rangle = 0, \tag{36}$$

$$|\Phi_{00}\rangle = |A_1\rangle, \tag{37}$$

$$|\Phi_{11}\rangle = |A_2\rangle, \tag{38}$$

where

$$|A_1\rangle \equiv \left(\frac{1}{2}\{1 \pm [8E(1-2E)]^{1/2}\}\right)^{1/2} |w_0\rangle + \left(\frac{1}{2}\{1 \mp [8E(1-2E)]^{1/2}\}\right)^{1/2} |w_3\rangle, \tag{39}$$

and

$$|A_2\rangle \equiv \left(\frac{1}{2}\{1 \mp [8E(1-2E)]^{1/2}\}\right)^{1/2} |w_0\rangle + \left(\frac{1}{2}\{1 \pm [8E(1-2E)]^{1/2}\}\right)^{1/2} |w_3\rangle. \tag{40}$$

The signal states, expressed in terms of the basis states Eqs. (2) and (3), are given by Eq. (1) of Ref. [2], namely,

$$|u\rangle \equiv \cos\frac{\pi}{8}|e_0\rangle + \sin\frac{\pi}{8}|e_1\rangle, \tag{41}$$

$$|\overline{u}\rangle \equiv -\sin\frac{\pi}{8}|e_0\rangle + \cos\frac{\pi}{8}|e_1\rangle, \tag{42}$$

$$|v\rangle \equiv \sin\frac{\pi}{8}|e_0\rangle + \cos\frac{\pi}{8}|e_1\rangle, \tag{43}$$

$$|\overline{v}\rangle \equiv \cos\frac{\pi}{8}|e_0\rangle - \sin\frac{\pi}{8}|e_1\rangle. \tag{44}$$

To see how the initial state $|u \otimes w\rangle$ transforms, we use Eq. (41) to write

$$|u \otimes w\rangle = \left(\cos\frac{\pi}{8}|e_0\rangle + \sin\frac{\pi}{8}|e_1\rangle\right) \otimes |w\rangle, \tag{45}$$

or

$$|u \otimes w\rangle = \cos\frac{\pi}{8}|e_0 \otimes w\rangle + \sin\frac{\pi}{8}|e_1 \otimes w\rangle, \tag{46}$$

so that using Eq. (1) in Eq. (46), the transformed state is described by

$$|u \otimes w\rangle \to \cos\frac{\pi}{8}\sum_n |e_n\rangle \otimes |\Phi_{0n}\rangle + \sin\frac{\pi}{8}\sum_n |e_n\rangle \otimes |\Phi_{1n}\rangle, \tag{47}$$

or performing the summations, then

$$|u \otimes w\rangle \to \cos\frac{\pi}{8}(|e_0\rangle \otimes |\Phi_{00}\rangle + |e_1\rangle \otimes |\Phi_{01}\rangle) + \sin\frac{\pi}{8}(|e_0\rangle \otimes |\Phi_{10}\rangle + |e_1\rangle \otimes |\Phi_{11}\rangle). \tag{48}$$

Next, substituting Eqs. (2) and (3) in Eq. (48), one gets

$$\begin{aligned}|u \otimes w\rangle \to \cos\frac{\pi}{8}\Bigg[&\left(\cos\frac{\pi}{8}|u\rangle - \sin\frac{\pi}{8}|\overline{u}\rangle\right) \otimes |\Phi_{00}\rangle \\ &+ \left(\cos\frac{\pi}{8}|v\rangle - \sin\frac{\pi}{8}|\overline{v}\rangle\right) \otimes |\Phi_{01}\rangle\Bigg] \\ + \sin\frac{\pi}{8}\Bigg[&\left(\cos\frac{\pi}{8}|u\rangle - \sin\frac{\pi}{8}|\overline{u}\rangle\right) \otimes |\Phi_{10}\rangle \\ &+ \left(\cos\frac{\pi}{8}|v\rangle - \sin\frac{\pi}{8}|\overline{v}\rangle\right) \otimes |\Phi_{11}\rangle\Bigg],\end{aligned} \tag{49}$$

or

$$\begin{aligned}|u \otimes w\rangle \to |u\rangle \otimes &\left(\cos^2\frac{\pi}{8}|\Phi_{00}\rangle + \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{10}\rangle\right) \\ &+ |\overline{u}\rangle \otimes \left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{00}\rangle - \sin^2\frac{\pi}{8}|\Phi_{10}\rangle\right) \\ &+ |v\rangle \otimes \left(\cos^2\frac{\pi}{8}|\Phi_{01}\rangle + \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{11}\rangle\right) \\ &+ |\overline{v}\rangle \otimes \left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{01}\rangle - \sin^2\frac{\pi}{8}|\Phi_{11}\rangle\right).\end{aligned} \tag{50}$$

Next substituting Eqs. (35)–(38) in Eq. (50), one obtains

$$\begin{aligned}|u \otimes w\rangle \to \cos^2\frac{\pi}{8}|u\rangle \otimes |A_1\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\overline{u}\rangle \otimes |A_1\rangle \\ + \sin\frac{\pi}{8}\cos\frac{\pi}{8}|v\rangle \otimes |A_2\rangle - \sin^2\frac{\pi}{8}|\overline{v}\rangle \otimes |A_2\rangle,\end{aligned} \tag{51}$$

or equivalently,

$$\begin{aligned}|u \otimes w\rangle \to \frac{1}{4}[&(2+2^{1/2})|u\rangle \otimes |A_1\rangle - 2^{1/2}|\overline{u}\rangle \otimes |A_1\rangle \\ &+ 2^{1/2}|v\rangle \otimes |A_2\rangle - (2-2^{1/2})|\overline{v}\rangle \otimes |A_2\rangle].\end{aligned} \tag{52}$$

It is evident from Eqs. (52), (39), and (40) that the effect of the transformation is to entangle the probe states $|w_0\rangle$ and $|w_3\rangle$ with the signal states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, and $|\overline{v}\rangle$.

Next consider the transformation of the state $|\overline{u}\otimes w\rangle$ also for the optimum parameter set $S^{(1)}$. According to Eq. (42), one has

$$|\overline{u}\otimes w\rangle = \left(-\sin\frac{\pi}{8}|e_0\rangle + \cos\frac{\pi}{8}|e_1\rangle\right)\otimes|w\rangle, \tag{53}$$

or

$$|\overline{u}\otimes w\rangle = -\sin\frac{\pi}{8}|e_0\otimes w\rangle + \cos\frac{\pi}{8}|e_1\otimes w\rangle, \tag{54}$$

so that using Eq. (1) in Eq. (54), the transformed state is described by

$$|\overline{u}\otimes w\rangle \rightarrow -\sin\frac{\pi}{8}\sum_n |e_n\rangle\otimes|\Phi_{0n}\rangle + \cos\frac{\pi}{8}\sum_n |e_n\rangle\otimes|\Phi_{1n}\rangle, \tag{55}$$

or performing the summations, and substituting Eqs. (2) and (3), one obtains

$$\begin{aligned}|\overline{u}\otimes w\rangle \rightarrow{}& |u\rangle\otimes\left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{00}\rangle + \cos^2\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |\overline{u}\rangle\otimes\left(\sin^2\frac{\pi}{8}|\Phi_{00}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |v\rangle\otimes\left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{01}\rangle + \cos^2\frac{\pi}{8}|\Phi_{11}\rangle\right)\\ &+ |\overline{v}\rangle\otimes\left(\sin^2\frac{\pi}{8}|\Phi_{01}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{11}\rangle\right).\end{aligned} \tag{56}$$

Next substituting Eqs. (35)–(38) in Eq. (56), one obtains

$$\begin{aligned}|\overline{u}\otimes w\rangle \rightarrow \frac{1}{4}[&-2^{1/2}|u\rangle\otimes|A_1\rangle + (2-2^{1/2})|\overline{u}\rangle\otimes|A_1\rangle\\ &+ (2+2^{1/2})|v\rangle\otimes|A_2\rangle - 2^{1/2}|\overline{v}\rangle\otimes|A_2\rangle].\end{aligned} \tag{57}$$

Again, the probe states are entangled with the signal states.

Next consider the transformation of the state $|v\otimes w\rangle$ also for the optimum parameter set $S^{(1)}$. Using Eq. (43), one has

$$|v\otimes w\rangle = \left(\sin\frac{\pi}{8}|e_0\rangle + \cos\frac{\pi}{8}|e_1\rangle\right)\otimes|w\rangle, \tag{58}$$

or

$$|v\otimes w\rangle = \left(\sin\frac{\pi}{8}|e_0\otimes w\rangle + \cos\frac{\pi}{8}|e_1\otimes w\rangle\right), \tag{59}$$

so that using Eq. (1) in Eq. (59), the transformed state is described by

$$|v\otimes w\rangle \rightarrow \sin\frac{\pi}{8}\sum_n |e_n\rangle\otimes|\Phi_{0n}\rangle + \cos\frac{\pi}{8}\sum_n |e_n\rangle\otimes|\Phi_{1n}\rangle, \tag{60}$$

or performing the summations, and substituting Eqs. (2) and (3), one obtains

$$\begin{aligned}|v\otimes w\rangle \rightarrow{}& |u\rangle\otimes\left(\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{00}\rangle + \cos^2\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |\overline{u}\rangle\otimes\left(-\sin^2\frac{\pi}{8}|\Phi_{00}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |v\rangle\otimes\left(\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{01}\rangle + \cos^2\frac{\pi}{8}|\Phi_{11}\rangle\right)\\ &+ |\overline{v}\rangle\otimes\left(-\sin^2\frac{\pi}{8}|\Phi_{01}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{11}\rangle\right).\end{aligned} \tag{61}$$

Then substituting Eqs. (35)–(38) in Eq. (61), one gets

$$\begin{aligned}|v\otimes w\rangle \rightarrow \frac{1}{4}[&2^{1/2}|u\rangle\otimes|A_1\rangle - (2-2^{1/2})|\overline{u}\rangle\otimes|A_1\rangle\\ &+ (2+2^{1/2})|v\rangle\otimes|A_2\rangle - 2^{1/2}|\overline{v}\rangle\otimes|A_2\rangle].\end{aligned} \tag{62}$$

Again, the probe states are entangled with the signal states.

Next consider the transformation of the state $|\overline{v}\otimes w\rangle$ also for the optimum parameter set $S^{(1)}$. According to Eq. (44), one has

$$|\overline{v}\otimes w\rangle = \left(\cos\frac{\pi}{8}|e_0\rangle - \sin\frac{\pi}{8}|e_1\rangle\right)\otimes|w\rangle, \tag{63}$$

and substituting Eqs. (1)–(3) in Eq. (63), the transformed state is described by

$$\begin{aligned}|\overline{v}\otimes w\rangle \rightarrow{}& |u\rangle\otimes\left(\cos^2\frac{\pi}{8}|\Phi_{00}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |\overline{u}\rangle\otimes\left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{00}\rangle + \sin^2\frac{\pi}{8}|\Phi_{10}\rangle\right)\\ &+ |v\rangle\otimes\left(\cos^2\frac{\pi}{8}|\Phi_{01}\rangle - \sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{11}\rangle\right)\\ &+ |\overline{v}\rangle\otimes\left(-\sin\frac{\pi}{8}\cos\frac{\pi}{8}|\Phi_{01}\rangle + \sin^2\frac{\pi}{8}|\Phi_{11}\rangle\right).\end{aligned} \tag{64}$$

Next substituting Eqs. (35)–(38) in Eq. (64), one obtains

$$\begin{aligned}|\overline{v}\otimes w\rangle \rightarrow \frac{1}{4}[&(2+2^{1/2})|u\rangle\otimes|A_1\rangle - 2^{1/2}|\overline{u}\rangle\otimes|A_1\rangle\\ &- 2^{1/2}|v\rangle\otimes|A_2\rangle + (2-2^{1/2})|\overline{v}\rangle\otimes|A_2\rangle].\end{aligned} \tag{65}$$

Again, the probe states are entangled with the signal states.

Assembling together Eqs. (52), (57), (62), and (65), one may simply represent them in matrix form as follows:

$$\begin{pmatrix} |u\otimes w\rangle \\ |\overline{u}\otimes w\rangle \\ |v\otimes w\rangle \\ |\overline{v}\otimes w\rangle \end{pmatrix} \rightarrow \frac{1}{4}\begin{pmatrix} (2+\sqrt{2})|A_1\rangle & -\sqrt{2}|A_1\rangle & \sqrt{2}|A_2\rangle & -(2-\sqrt{2})|A_2\rangle \\ -\sqrt{2}|A_1\rangle & (2-\sqrt{2})|A_1\rangle & (2+\sqrt{2})|A_2\rangle & -\sqrt{2}|A_2\rangle \\ \sqrt{2}|A_1\rangle & -(2-\sqrt{2})|A_1\rangle & (2+\sqrt{2})|A_2\rangle & -\sqrt{2}|A_2\rangle \\ (2+\sqrt{2})|A_1\rangle & -\sqrt{2}|A_1\rangle & -\sqrt{2}|A_2\rangle & (2-\sqrt{2})|A_2\rangle \end{pmatrix}\begin{pmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{pmatrix}. \tag{66}$$

In Eq. (66), if one multiplies rows by the column vector, the entanglement of the probe states with the signal states is manifest, the probe states $|A_1\rangle$ and $|A_2\rangle$ being given by Eqs. (39) and (40), respectively. Since $|A_1\rangle$ and $|A_2\rangle$ depend only on the two probe basis states $|w_0\rangle$ and $|w_3\rangle$, the probe states, for the case of the optimum parameter set $S^{(1)}$, Eqs. (15) or (28), lie in a two-dimensional Hilbert space.

From the geometry of the two-dimensional Hilbert space of the signal states in the BB84 protocol, it follows that [2]

$$|v\rangle = 2^{-1/2}|u\rangle + 2^{-1/2}|\overline{u}\rangle, \tag{67}$$

$$|\overline{v}\rangle = 2^{-1/2}|u\rangle - 2^{-1/2}|\overline{u}\rangle, \tag{68}$$

$$|u\rangle = 2^{-1/2}|v\rangle + 2^{-1/2}|\overline{v}\rangle, \tag{69}$$

$$|\overline{u}\rangle = 2^{-1/2}|v\rangle - 2^{-1/2}|\overline{v}\rangle. \tag{70}$$

Using Eqs. (67)–(70), it is useful to rewrite Eq. (66) in block-diagonal form:

$$\begin{bmatrix} |u\rangle|w\rangle \\ |\overline{u}\rangle|w\rangle \\ |v\rangle|w\rangle \\ |\overline{v}\rangle|w\rangle \end{bmatrix} \rightarrow \frac{1}{4}\begin{bmatrix} |\alpha_+\rangle & |\alpha\rangle & 0 & 0 \\ |\alpha\rangle & |\alpha_-\rangle & 0 & 0 \\ 0 & 0 & |\alpha_-\rangle & -|\alpha\rangle \\ 0 & 0 & -|\alpha\rangle & |\alpha_+\rangle \end{bmatrix}\begin{bmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{bmatrix}, \tag{71}$$

where

$$|\alpha_+\rangle = [(2^{1/2}+1)(1\pm\eta)^{1/2} + (2^{1/2}-1)(1\mp\eta)^{1/2}]|w_0\rangle + [(2^{1/2}+1)(1\mp\eta)^{1/2} + (2^{1/2}-1)(1\pm\eta)^{1/2}]|w_3\rangle, \tag{72}$$

$$|\alpha_-\rangle = [(2^{1/2}-1)(1\pm\eta)^{1/2} + (2^{1/2}+1)(1\mp\eta)^{1/2}]|w_0\rangle + [(2^{1/2}-1)(1\mp\eta)^{1/2} + (2^{1/2}+1)(1\pm\eta)^{1/2}]|w_3\rangle, \tag{73}$$

$$|\alpha\rangle = [-(1\pm\eta)^{1/2} + (1\mp\eta)^{1/2}]|w_0\rangle + [-(1\mp\eta)^{1/2} + (1\pm\eta)^{1/2}]|w_3\rangle, \tag{74}$$

$$\eta \equiv [8E(1-2E)]^{1/2}. \tag{75}$$

It is to be noted in Eq. (71) that the projected probe state $|\psi_{uu}\rangle$ correlated with the correct received signal state (in the notation of Refs. [2,6]), in which the state $|u\rangle$ is sent by the transmitter, and is also received by the legitimate receiver, is $|\alpha_+\rangle$. Analogously, the correlated probe state $|\psi_{\overline{uu}}\rangle$ is $|\alpha_-\rangle$. The two states $|\alpha_+\rangle$ and $|\alpha_-\rangle$ are to be distinguished by the measurement of the probe. Also in Eq. (71), the same two probe states $|\alpha_+\rangle$ and $|\alpha_-\rangle$ are the appropriate correlated states $|\psi_{v\overline{v}}\rangle$ and $|\psi_{vv}\rangle$, respectively. This is consistent with the assumption in Sec. II of Ref. [2] that only two probe states must be distinguished by the probe. Also, using Eqs. (74) and (75), it can be shown that, for small induced error rates, the disturbance of the signal states scales as $2(2E)^{1/2}$.

We next evaluate the unitary transformation $U^{(2)}$, corresponding to the set $S^{(2)}$ of optimum probe parameters, Eq. (16). In Eq. (16), one has

$$\sin 2\mu \sin^2\lambda = 1 - 4E - \cos^2\lambda \sin 2\phi, \tag{76}$$

or equivalently,

$$\sin 2\mu(1-\cos^2\lambda) = 1 - 4E - \cos^2\lambda \sin 2\phi, \tag{77}$$

and therefore

$$\cos^2\lambda = \frac{\sin 2\mu - 1 + 4E}{\sin 2\mu - \sin 2\phi}. \tag{78}$$

Since, according to Eq. (14), $\lambda$ lies in quadrant I or II, it then follows from Eq. (78) that one must require $\sin 2\phi < \sin 2\mu \geqslant 1-4E$, or $\sin 2\phi > \sin 2\mu \leqslant 1-4E$, and then

$$\cos\lambda = e_\lambda\left(\frac{\sin 2\mu - 1 + 4E}{\sin 2\mu - \sin 2\phi}\right)^{1/2}, \tag{79}$$

where

$$e_\lambda \equiv \pm 1. \tag{80}$$

Summarizing Eqs. (79) and (80), one has (letting $\cup$ denote "or")

$$\cos\lambda = e_\lambda r, \quad \sin 2\phi < \sin 2\mu \geqslant 1-4E \quad \cup \quad \sin 2\phi > \sin 2\mu \leqslant 1-4E, \tag{81}$$

and

$$\sin\lambda = (1-r^2)^{1/2}, \quad \sin 2\phi < \sin 2\mu \geqslant 1-4E \quad \cup \quad \sin 2\phi > \sin 2\mu \leqslant 1-4E, \tag{82}$$

where

$$r \equiv \left(\frac{\sin 2\mu - 1 + 4E}{\sin 2\mu - \sin 2\phi}\right)^{1/2}. \tag{83}$$

Also, according to Eq. (16), one has

$$\cos 2\theta = 1, \tag{84}$$

and therefore

$$\cos\theta = e_\theta, \tag{85}$$

where

$$e_\theta \equiv \pm 1. \tag{86}$$

Next, using Eqs. (81), (82), (85), and (86), Eq. (16) can be rewritten as follows:

$$S^{(2)} = \{\lambda, \mu, \theta, \phi; \cos\theta = e_\theta, \sin\theta = 0,$$

$$\cos\lambda = e_\lambda r, \sin\lambda = (1-r^2)^{1/2},$$

$$\sin 2\phi < \sin 2\mu \geqslant 1 - 4E \ \cup \ \sin 2\phi > \sin 2\mu \leqslant 1 - 4E\}. \tag{87}$$

We proceed by substituting Eq. (87) in Eqs. (8)–(13), and obtain

$$X_0 = \cos\mu(1-r^2)^{1/2}, \tag{88}$$

$$X_1 = e_\lambda e_\theta r\cos\phi, \tag{89}$$

$$X_2 = e_\lambda e_\theta r\sin\phi, \tag{90}$$

$$X_3 = \sin\mu(1-r^2)^{1/2}, \tag{91}$$

$$X_5 = 0, \tag{92}$$

$$X_6 = 0. \tag{93}$$

Then substituting Eqs. (88)–(93) in Eqs. (4)–(7) one obtains

$$|\Phi_{01}\rangle = 0, \tag{94}$$

$$|\Phi_{10}\rangle = 0, \tag{95}$$

$$|\Phi_{00}\rangle = |B_1\rangle, \tag{96}$$

$$|\Phi_{11}\rangle = |B_2\rangle, \tag{97}$$

in which

$$|B_1\rangle = (1-r^2)^{1/2}\cos\mu|w_0\rangle + e_\lambda e_\theta r\cos\phi|w_1\rangle + e_\lambda e_\theta r\sin\phi|w_2\rangle + (1-r^2)^{1/2}\sin\mu|w_3\rangle \tag{98}$$

and

$$|B_2\rangle = (1-r^2)^{1/2}\sin\mu|w_0\rangle + e_\lambda e_\theta r\sin\phi|w_1\rangle + e_\lambda e_\theta r\cos\phi|w_2\rangle + (1-r^2)^{1/2}\cos\mu|w_3\rangle. \tag{99}$$

Next substituting Eqs. (94)–(97) in Eqs. (50), (56), (61), and (64), one obtains

$$\begin{pmatrix} |u\otimes w\rangle \\ |\overline{u}\otimes w\rangle \\ |v\otimes w\rangle \\ |\overline{v}\otimes w\rangle \end{pmatrix} \rightarrow \frac{1}{4}\begin{pmatrix} (2+\sqrt{2})|B_1\rangle & -\sqrt{2}|B_1\rangle & \sqrt{2}|B_2\rangle & -(2-\sqrt{2})|B_2\rangle \\ -\sqrt{2}|B_1\rangle & (2-\sqrt{2})|B_1\rangle & (2+\sqrt{2})|B_2\rangle & -\sqrt{2}|B_2\rangle \\ \sqrt{2}|B_1\rangle & -(2-\sqrt{2})|B_1\rangle & (2+\sqrt{2})|B_2\rangle & -\sqrt{2}|B_2\rangle \\ (2+\sqrt{2})|B_1\rangle & -\sqrt{2}|B_1\rangle & -\sqrt{2}|B_2\rangle & (2-\sqrt{2})|B_2\rangle \end{pmatrix}\begin{pmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{pmatrix}. \tag{100}$$

In Eq. (100), if one multiplies rows by the column, the entanglement of the probe states with the signal states is manifest, the probe states $|B_1\rangle$ and $|B_2\rangle$ being given by Eqs. (98) and (99). Since $|B_1\rangle$ and $|B_2\rangle$ depend on the four probe basis states $|w_0\rangle$, $|w_1\rangle$, $|w_2\rangle$, and $|w_3\rangle$, the probe states, for the case of the optimal parameter set $S^{(2)}$, lie in a four-dimensional Hilbert space.

Using Eqs. (67)–(70), one can rewrite Eq. (100) in the following block-diagonal form:

$$\begin{bmatrix} |u\rangle|w\rangle \\ |\overline{u}\rangle|w\rangle \\ |v\rangle|w\rangle \\ |\overline{v}\rangle|w\rangle \end{bmatrix} \rightarrow \frac{1}{4}\begin{bmatrix} |\beta_+\rangle & |\beta\rangle & 0 & 0 \\ |\beta\rangle & |\beta_-\rangle & 0 & 0 \\ 0 & 0 & |\beta_-\rangle & -|\beta\rangle \\ 0 & 0 & -|\beta\rangle & |\beta_+\rangle \end{bmatrix}\begin{bmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{bmatrix}, \tag{101}$$

where

$$|\beta_\pm\rangle = (1-r^2)^{1/2}[(2\mp 2^{1/2})\sin\mu + (2\pm 2^{1/2})\cos\mu]|w_0\rangle + (1-r^2)^{1/2}[(2\pm 2^{1/2})\sin\mu + (2\mp 2^{1/2})\cos\mu]|w_3\rangle + e_\lambda e_\theta r[(2\mp 2^{1/2})\sin\phi + (2\pm 2^{1/2})\cos\phi]|w_1\rangle + e_\lambda e_\theta r[(2\pm 2^{1/2})\sin\phi + (2\mp 2^{1/2})\cos\phi]|w_2\rangle, \tag{102}$$

$$|\beta\rangle = 2^{1/2}(1-r^2)^{1/2}(\sin\mu - \cos\mu)(|w_0\rangle - |w_3\rangle) + 2^{1/2}e_\lambda e_\theta r(\sin\phi - \cos\phi)(|w_1\rangle - |w_2\rangle), \tag{103}$$

in which $r$ is given by Eq. (83), and $\mu$ and $\phi$ are restricted by Eq. (87). It is to be noted in Eq. (101) that the projected probe state $|\psi_{uu}\rangle$ correlated with the correct received signal state (in the notation of Refs. [2,6]), in which the state $|u\rangle$ is sent by the transmitter, and is also received by the legitimate receiver, is $|\beta_+\rangle$. Analogously, the correlated probe state $|\psi_{\overline{uu}}\rangle$ is $|\beta_-\rangle$. The two states $|\beta_+\rangle$ and $|\beta_-\rangle$ are to be distinguished by the measurement of the probe. Also in Eq. (101), the same two probe states $|\beta_+\rangle$ and $|\beta_-\rangle$ are the appropriate correlated

states $|\psi_{\overline{vv}}\rangle$ and $|\psi_{vv}\rangle$, respectively. This is consistent with the assumption in Sec. II of Ref. [2] that only two probe states must be distinguished by the probe.

We next evaluate the unitary transformation $U^{(3)}$, corresponding to the set $S^{(3)}$ of optimum probe parameters Eq. (17). In Eq. (17), one has

$$\sin 2\mu \sin^2 \lambda = 1 - 4E + \cos^2 \lambda. \tag{104}$$

Using the trigonometric identity,

$$\cos^2 \lambda = 1 - \sin^2 \lambda \tag{105}$$

in Eq. (104), one gets

$$\sin 2\mu \sin^2 \lambda = 2 - 4E - \sin^2 \lambda, \tag{106}$$

and therefore

$$\sin^2 \lambda = \frac{2(1-2E)}{1+\sin 2\mu}. \tag{107}$$

But one has the inequality

$$0 \leqslant \sin^2 \lambda \leqslant 1, \tag{108}$$

and then substituting Eq. (107) in Eq. (108), one requires

$$0 \leqslant 2 - 4E \leqslant 1 + \sin 2\mu, \tag{109}$$

or equivalently,

$$\sin 2\mu \geqslant 1 - 4E, \tag{110}$$

since $E < 1/2$. Also, one requires

$$\sin 2\mu \leqslant 1, \tag{111}$$

and combining Eqs. (110) and (111), one requires

$$1 \geqslant \sin 2\mu \geqslant 1 - 4E. \tag{112}$$

Next, from Eqs. (107), (14), and (105), one obtains

$$\sin \lambda = p, \tag{113}$$

and

$$\cos \lambda = \pm (1-p^2)^{1/2}, \tag{114}$$

where

$$p \equiv \left[\frac{2(1-2E)}{1+\sin 2\mu}\right]^{1/2}. \tag{115}$$

Also, according to Eq. (17), one has

$$\sin 2\phi = -1. \tag{116}$$

It then follows that

$$\sin \phi = 2^{-1/2} \tag{117}$$

and

$$\cos \phi = -2^{-1/2}. \tag{118}$$

Next, using Eqs. (112)–(115), (117), and (118), Eq. (17) can be rewritten as follows:

$$S^{(3)} = \{\lambda, \mu, \theta, \phi; \sin \phi = 2^{-1/2},\ \cos \phi = -2^{-1/2},\ \sin \lambda = p,$$
$$\cos \lambda = \pm (1-p^2)^{1/2},\ 1 \geqslant \sin 2\mu \geqslant 1 - 4E\}. \tag{119}$$

We proceed by substituting Eq. (119) in Eqs. (8)–(13), and obtain

$$X_0 = p \cos \mu, \tag{120}$$

$$X_1 = \mp 2^{-1/2}(1-p^2)^{1/2}\cos \theta, \tag{121}$$

$$X_2 = \pm 2^{-1/2}(1-p^2)^{1/2}\cos \theta, \tag{122}$$

$$X_3 = p \sin \mu, \tag{123}$$

$$X_5 = \mp 2^{-1/2}(1-p^2)^{1/2}\sin \theta, \tag{124}$$

$$X_6 = \mp 2^{-1/2}(1-p^2)^{1/2}\sin \theta. \tag{125}$$

Then substituting Eqs. (120)–(125) in Eqs. (4)–(7), one obtains

$$|\Phi_{01}\rangle = |S_0\rangle, \tag{126}$$

$$|\Phi_{10}\rangle = |S_0\rangle, \tag{127}$$

$$|\Phi_{00}\rangle \equiv |S_1\rangle, \tag{128}$$

$$|\Phi_{11}\rangle \equiv |S_2\rangle, \tag{129}$$

in which

$$|S_0\rangle \equiv \mp 2^{-1/2}(1-p^2)^{1/2}\sin \theta(|w_1\rangle + |w_2\rangle), \tag{130}$$

$$|S_1\rangle \equiv p \cos \mu |w_0\rangle \mp 2^{-1/2}(1-p^2)^{1/2}\cos \theta |w_1\rangle$$
$$\pm 2^{-1/2}(1-p^2)^{1/2}\cos \theta |w_2\rangle + p \sin \mu |w_3\rangle, \tag{131}$$

$$|S_2\rangle \equiv p \sin \mu |w_0\rangle \pm 2^{-1/2}(1-p^2)^{1/2}\cos \theta |w_1\rangle$$
$$\mp 2^{-1/2}(1-p^2)^{1/2}\cos \theta |w_2\rangle + p \cos \mu |w_3\rangle. \tag{132}$$

Next substituting Eqs. (126)–(129) in Eq. (50), one obtains

$$|u \otimes w\rangle \rightarrow \frac{1}{4}[(2+2^{1/2})|u\rangle \otimes |S_1\rangle + 2^{1/2}|u\rangle \otimes |S_0\rangle$$
$$- 2^{1/2}|\overline{u}\rangle \otimes |S_1\rangle - (2-2^{1/2})|\overline{u}\rangle \otimes |S_0\rangle$$
$$+ (2+2^{1/2})|v\rangle \otimes |S_0\rangle + 2^{1/2}|v\rangle \otimes |S_2\rangle$$
$$- 2^{1/2}|\overline{v}\rangle \otimes |S_0\rangle - (2-2^{1/2})|\overline{v}\rangle \otimes |S_2\rangle], \tag{133}$$

or equivalently,

$$|u \otimes w\rangle \rightarrow \frac{1}{4}[(2+2^{1/2})|u\rangle \otimes |S_{11}\rangle - 2^{1/2}|\overline{u}\rangle \otimes |S_{11}\rangle$$
$$+ 2^{1/2}|v\rangle \otimes |S_{12}\rangle - (2-2^{1/2})|\overline{v}\rangle \otimes |S_{12}\rangle], \tag{134}$$

in which we define

$$|S_{11}\rangle \equiv |S_1\rangle + (2^{1/2}-1)|S_0\rangle, \tag{135}$$

$$|S_{12}\rangle \equiv |S_2\rangle + (2^{1/2}+1)|S_0\rangle. \tag{136}$$

Substituting Eqs. (130)–(132) in Eqs. (135) and (136), one obtains

$$\begin{aligned}|S_{11}\rangle = {} & p\cos\mu|w_0\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}-1)\sin\theta] \\ & \times|w_1\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}-1)\sin\theta]|w_2\rangle \\ & + p\sin\mu|w_3\rangle\end{aligned} \tag{137}$$

and

$$\begin{aligned}|S_{12}\rangle = {} & p\sin\mu|w_0\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}+1)\sin\theta] \\ & \times|w_1\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}+1)\sin\theta]|w_2\rangle \\ & + p\cos\mu|w_3\rangle.\end{aligned} \tag{138}$$

Also, substituting Eqs. (126)–(129) in Eq. (56), one obtains

$$\begin{aligned}|\overline{u}\otimes w\rangle \to \frac{1}{4}[ & -2^{1/2}|u\rangle\otimes|S_1\rangle + (2+2^{1/2})|u\rangle\otimes|S_0\rangle \\ & + (2-2^{1/2})|\overline{u}\rangle\otimes|S_1\rangle - 2^{1/2}|\overline{u}\rangle\otimes|S_0\rangle \\ & - 2^{1/2}|v\rangle\otimes|S_0\rangle + (2+2^{1/2})|v\rangle\otimes|S_2\rangle \\ & + (2-2^{1/2})|\overline{v}\rangle\otimes|S_0\rangle - 2^{1/2}|\overline{v}\rangle\otimes|S_2\rangle],\end{aligned} \tag{139}$$

or equivalently,

$$\begin{aligned}|\overline{u}\otimes w\rangle \to \frac{1}{4}[ & -2^{1/2}|u\rangle\otimes|S_{21}\rangle + (2-2^{1/2})|\overline{u}\rangle\otimes|S_{21}\rangle \\ & + (2+2^{1/2})|v\rangle\otimes|S_{22}\rangle - 2^{1/2}|\overline{v}\rangle\otimes|S_{22}\rangle],\end{aligned} \tag{140}$$

in which we define

$$|S_{21}\rangle \equiv |S_1\rangle - (2^{1/2}+1)|S_0\rangle, \tag{141}$$

$$|S_{22}\rangle \equiv |S_2\rangle - (2^{1/2}-1)|S_0\rangle. \tag{142}$$

Substituting Eqs. (130)–(132) in Eqs. (141) and (142), one obtains

$$\begin{aligned}|S_{21}\rangle = {} & p\cos\mu|w_0\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}+1)\sin\theta] \\ & \times|w_1\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}+1)\sin\theta]|w_2\rangle \\ & + p\sin\mu|w_3\rangle\end{aligned} \tag{143}$$

and

$$\begin{aligned}|S_{22}\rangle = {} & p\sin\mu|w_0\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}-1)\sin\theta] \\ & \times|w_1\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}-1)\sin\theta]|w_2\rangle \\ & + p\cos\mu|w_3\rangle.\end{aligned} \tag{144}$$

Also, substituting Eqs. (126)–(129) in Eq. (61), one gets

$$\begin{aligned}|v\otimes w\rangle \to \frac{1}{4}[ & 2^{1/2}|u\rangle\otimes|S_1\rangle + (2+2^{1/2})|u\rangle\otimes|S_0\rangle - (2-2^{1/2}) \\ & \times|\overline{u}\rangle\otimes|S_1\rangle - 2^{1/2}|\overline{u}\rangle\otimes|S_0\rangle + 2^{1/2}|v\rangle\otimes|S_0\rangle \\ & + (2+2^{1/2})|v\rangle\otimes|S_2\rangle - (2-2^{1/2})|\overline{v}\rangle\otimes|S_0\rangle \\ & - 2^{1/2}|\overline{v}\rangle\otimes|S_2\rangle],\end{aligned} \tag{145}$$

or equivalently,

$$\begin{aligned}|v\otimes w\rangle \to \frac{1}{4}[ & 2^{1/2}|u\rangle\otimes|S_{31}\rangle - (2-2^{1/2})|\overline{u}\rangle\otimes|S_{31}\rangle + (2+2^{1/2}) \\ & \times|v\rangle\otimes|S_{32}\rangle - 2^{1/2}|\overline{v}\rangle\otimes|S_{32}\rangle],\end{aligned} \tag{146}$$

in which we define

$$|S_{31}\rangle \equiv |S_1\rangle + (2^{1/2}+1)|S_0\rangle, \tag{147}$$

$$|S_{32}\rangle \equiv |S_2\rangle + (2^{1/2}-1)|S_0\rangle. \tag{148}$$

Substituting Eqs. (130)–(132) in Eqs. (147) and (148), one obtains

$$\begin{aligned}|S_{31}\rangle = {} & p\cos\mu|w_0\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}+1)\sin\theta] \\ & \times|w_1\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}+1)\sin\theta]|w_2\rangle \\ & + p\sin\mu|w_3\rangle\end{aligned} \tag{149}$$

and

$$\begin{aligned}|S_{32}\rangle = {} & p\sin\mu|w_0\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta - (2^{1/2}-1)\sin\theta] \\ & \times|w_1\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta + (2^{1/2}-1)\sin\theta]|w_2\rangle \\ & + p\cos\mu|w_3\rangle.\end{aligned} \tag{150}$$

Substituting Eqs. (126)–(129) in Eq. (64), one gets

$$\begin{aligned}|\overline{v}\otimes w\rangle \to \frac{1}{4}[ & (2+2^{1/2})|u\rangle\otimes|S_1\rangle - 2^{1/2}|u\rangle\otimes|S_0\rangle - 2^{1/2}|\overline{u}\rangle \\ & \otimes|S_1\rangle + (2-2^{1/2})|\overline{u}\rangle\otimes|S_0\rangle + (2+2^{1/2})|v\rangle\otimes|S_0\rangle \\ & - 2^{1/2}|v\rangle\otimes|S_2\rangle - 2^{1/2}|\overline{v}\rangle\otimes|S_0\rangle + (2-2^{1/2})|\overline{v}\rangle \\ & \otimes|S_2\rangle],\end{aligned} \tag{151}$$

or equivalently,

$$\begin{aligned}|\overline{v}\otimes w\rangle \to \frac{1}{4}[ & (2+2^{1/2})|u\rangle\otimes|S_{41}\rangle - 2^{1/2}|\overline{u}\rangle\otimes|S_{41}\rangle - 2^{1/2}|v\rangle \\ & \otimes|S_{42}\rangle + (2-2^{1/2})|\overline{v}\rangle\otimes|S_{42}\rangle],\end{aligned} \tag{152}$$

in which we define

$$|S_{41}\rangle \equiv |S_1\rangle + (1-2^{1/2})|S_0\rangle, \tag{153}$$

$$|S_{42}\rangle \equiv |S_2\rangle - (1+2^{1/2})|S_0\rangle. \tag{154}$$

Substituting Eqs. (130)–(132) in Eqs. (153) and (154),

one obtains

$$|S_{41}\rangle = p\cos\mu|w_0\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta-(2^{1/2}-1)\sin\theta] \times|w_1\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta+(2^{1/2}-1)\sin\theta]|w_2\rangle + p\sin\mu|w_3\rangle \quad (155)$$

and

$$|S_{42}\rangle = p\sin\mu|w_0\rangle \pm 2^{-1/2}(1-p^2)^{1/2}[\cos\theta+(2^{1/2}+1)\sin\theta] \times|w_1\rangle \mp 2^{-1/2}(1-p^2)^{1/2}[\cos\theta-(2^{1/2}+1)\sin\theta]|w_2\rangle + p\cos\mu|w_3\rangle. \quad (156)$$

Therefore, summarizing Eqs. (134), (140), (146), and (152), one has

$$\begin{pmatrix} |u\otimes w\rangle \\ |\overline{u}\otimes w\rangle \\ |v\otimes w\rangle \\ |\overline{v}\otimes w\rangle \end{pmatrix} \rightarrow \frac{1}{4}\begin{pmatrix} (2+\sqrt{2})|S_{11}\rangle & -\sqrt{2}|S_{11}\rangle & \sqrt{2}|S_{12}\rangle & -(2-\sqrt{2})|S_{12}\rangle \\ -\sqrt{2}|S_{21}\rangle & (2-\sqrt{2})|S_{21}\rangle & (2+\sqrt{2})|S_{22}\rangle & -\sqrt{2}|S_{22}\rangle \\ \sqrt{2}|S_{31}\rangle & -(2-\sqrt{2})|S_{31}\rangle & (2+\sqrt{2})|S_{32}\rangle & -\sqrt{2}|S_{32}\rangle \\ (2+\sqrt{2})|S_{41}\rangle & -\sqrt{2}|S_{41}\rangle & -\sqrt{2}|S_{42}\rangle & (2-\sqrt{2})|S_{42}\rangle \end{pmatrix}\begin{pmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{pmatrix}. \quad (157)$$

In Eq. (157), if one multiplies rows by the column, the entanglement of the probe states with the signal states is manifest, the probe states $|S_{ij}\rangle$ being given by Eqs. (137), (138), (143), (144), (149), (150), (155), (156), (115), (112), and (14). Since the probe states $|S_{ij}\rangle$ depend on the four probe basis states $|w_0\rangle$, $|w_1\rangle$, $|w_2\rangle$, and $|w_3\rangle$, the probe states for the case of the optimal parameter set $S^{(3)}$ lie in a four-dimensional Hilbert space.

Using Eqs. (67)–(70), it is useful to rewrite Eq. (157) in block-diagonal form:

$$\begin{bmatrix} |u\rangle|w\rangle \\ |\overline{u}\rangle|w\rangle \\ |v\rangle|w\rangle \\ |\overline{v}\rangle|w\rangle \end{bmatrix} \rightarrow \frac{1}{4}\begin{bmatrix} |\sigma_+\rangle & |\sigma\rangle & 0 & 0 \\ |\sigma\rangle & |\sigma_-\rangle & 0 & 0 \\ 0 & 0 & |\delta_+\rangle & |\delta\rangle \\ 0 & 0 & |\delta\rangle & |\delta_-\rangle \end{bmatrix}\begin{bmatrix} |u\rangle \\ |\overline{u}\rangle \\ |v\rangle \\ |\overline{v}\rangle \end{bmatrix}, \quad (158)$$

where

$$|\sigma_+\rangle = p[(2-2^{1/2})\sin\mu+(2+2^{1/2})\cos\mu]|w_0\rangle \mp 2(1-p^2)^{1/2}(\sin\theta+\cos\theta)|w_1\rangle \mp 2(1-p^2)^{1/2} \times(\sin\theta-\cos\theta)|w_2\rangle + p[(2+2^{1/2})\sin\mu + (2-2^{1/2})\cos\mu]|w_3\rangle, \quad (159)$$

$$|\sigma_-\rangle = p[(2+2^{1/2})\sin\mu+(2-2^{1/2})\cos\mu]|w_0\rangle \pm 2(1-p^2)^{1/2}(\sin\theta+\cos\theta)|w_1\rangle \pm 2(1-p^2)^{1/2} \times(\sin\theta-\cos\theta)|w_2\rangle + p[(2-2^{1/2})\sin\mu + (2+2^{1/2})\cos\mu]|w_3\rangle, \quad (160)$$

$$|\sigma\rangle = 2^{1/2}p(\sin\mu-\cos\mu)(|w_0\rangle-|w_3\rangle) \mp 2(1-p^2)^{1/2} \times(\sin\theta-\cos\theta)|w_1\rangle \mp 2(1-p^2)^{1/2} \times(\sin\theta+\cos\theta)|w_2\rangle, \quad (161)$$

$$|\delta_+\rangle = p[(2+2^{1/2})\sin\mu+(2-2^{1/2})\cos\mu]|w_0\rangle \mp 2(1-p^2)^{1/2}(\sin\theta-\cos\theta)|w_1\rangle \mp 2(1-p^2)^{1/2}(\sin\theta+\cos\theta)|w_2\rangle + p[(2-2^{1/2})\sin\mu + (2+2^{1/2})\cos\mu]|w_3\rangle, \quad (162)$$

$$|\delta_-\rangle = p[(2-2^{1/2})\sin\mu+(2+2^{1/2})\cos\mu]|w_0\rangle \pm 2(1-p^2)^{1/2}(\sin\theta-\cos\theta)|w_1\rangle \pm 2(1-p^2)^{1/2} \times(\sin\theta+\cos\theta)|w_2\rangle + p[(2+2^{1/2})\sin\mu + (2-2^{1/2})\cos\mu]|w_3\rangle, \quad (163)$$

$$|\delta\rangle = 2^{1/2}p(-\sin\mu+\cos\mu)(|w_0\rangle-|w_3\rangle) \mp 2(1-p^2)^{1/2}(\sin\theta+\cos\theta)|w_1\rangle \mp 2(1-p^2)^{1/2}(\sin\theta-\cos\theta)|w_2\rangle, \quad (164)$$

in which $p$ is given by Eq. (115), and $\mu$ is restricted by Eq. (112). It is however significant to note in Eq. (158) that the projected probe state $|\psi_{uu}\rangle$ correlated with the correct received signal state (in the notation of Refs. [2,6]), in which the state $|u\rangle$ is sent by the transmitter, and is also received by the legitimate receiver, is $|\sigma_+\rangle$. Analogously, the correlated probe state $|\psi_{\overline{uu}}\rangle$ is $|\sigma_-\rangle$. The two states $|\sigma_+\rangle$ and $|\sigma_-\rangle$ are to be distinguished by the measurement of the probe. But one also notes in Eq. (158) that probe states $|\delta_+\rangle$ and $|\delta_-\rangle$, distinct from $|\sigma_+\rangle$ and $|\sigma_-\rangle$, are the correlated states $|\psi_{vv}\rangle$ and $|\psi_{\overline{vv}}\rangle$, respectively. However, the sets $\{|\sigma_+\rangle,|\sigma_-\rangle\}$ and $\{|\delta_+\rangle,|\delta_-\rangle\}$ have the same overlap $Q$ and they (and $|\sigma\rangle$ and $|\delta\rangle$) go into each other under the reflection symmetry of Ref. [2] in which the basis vectors $|w_0\rangle$ and $|w_3\rangle$, and also $|w_1\rangle$ and $|w_2\rangle$, are interchanged. Also $U^{(3)}$ does in fact yield the same maximum information as $U^{(1)}$ and $U^{(2)}$.

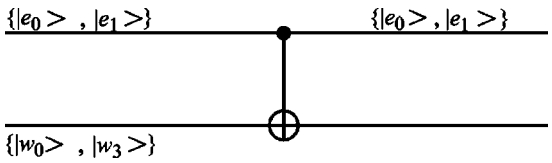


FIG. 1. Quantum CNOT gate: Signal basis states $\{|e_0\rangle,|e_1\rangle\}$; probe basis states $\{|w_0\rangle,|w_3\rangle\}$.

## III. QUANTUM CIRCUIT

Although all three optimum unitary transformations $U^{(1)}$, $U^{(2)}$, and $U^{(3)}$ produce the identical maximum information gain by the entangling probe, Eq. (19), the transformation $U^{(1)}$, given by Eq. (66) or Eq. (71) is clearly the simplest, and should therefore be the easiest to implement. In this section, I exploit the quantum-circuit model of quantum computation to determine the quantum circuit corresponding to the optimum unitary transformation $U^{(1)}$. From Eq. (1), it follows that for a signal basis state $|e_0\rangle$ or $|e_1\rangle$ entering the probe in initial state $|w\rangle$, the probe produces the following states, respectively:

$$|e_0 \otimes w\rangle \rightarrow |e_0\rangle \otimes |\phi_{00}\rangle + |e_1\rangle \otimes |\phi_{01}\rangle \tag{165}$$

and

$$|e_1 \otimes w\rangle \rightarrow |e_0\rangle \otimes |\phi_{10}\rangle + |e_1\rangle \otimes |\phi_{11}\rangle. \tag{166}$$

Then substituting Eqs. (35)–(38) in Eqs. (165) and (166), one obtains

$$|e_0 \otimes w\rangle \rightarrow |e_0\rangle \otimes |A_1\rangle \tag{167}$$

and

$$|e_1 \otimes w\rangle \rightarrow |e_1\rangle \otimes |A_2\rangle, \tag{168}$$

expressed in terms of the probe states $|A_1\rangle$ and $|A_2\rangle$, given by Eqs. (39) and (40). Equivalently, using Eqs. (39) and (40), one has

$$|e_0 \otimes w\rangle \rightarrow |e_0\rangle \otimes |A_1\rangle = |e_0\rangle \otimes (a_1|w_0\rangle + a_2|w_3\rangle) \tag{169}$$

and

$$|e_1 \otimes w\rangle \rightarrow |e_1\rangle \otimes |A_2\rangle = |e_1\rangle \otimes (a_2|w_0\rangle + a_1|w_3\rangle), \tag{170}$$

where

$$a_1 = 2^{-1/2}(1 \pm \eta)^{1/2}, \tag{171}$$

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $\|e_0>$ | $\|w_0>$ | $\|e_0>$ | $\|w_3>$ |
| $\|e_0>$ | $\|w_3>$ | $\|e_0>$ | $\|w_0>$ |
| $\|e_1>$ | $\|w_0>$ | $\|e_1>$ | $\|w_0>$ |
| $\|e_1>$ | $\|w_3>$ | $\|e_1>$ | $\|w_3>$ |

FIG. 2. Truth table for CNOT gate.

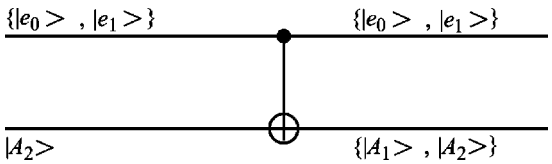


FIG. 3. Quantum circuit for entangling probe; initial probe state $|A_2\rangle$.

$$a_2 = 2^{-1/2}(1 \mp \eta)^{1/2}, \tag{172}$$

and

$$\eta = [8E(1-2E)]^{1/2}. \tag{173}$$

Next, consider the quantum controlled-NOT gate in Fig. 1, in which the control qubit consists of the two signal basis states $\{|e_0\rangle,|e_1\rangle\}$, and the target qubit consists of the probe basis states $\{|w_0\rangle,|w_3\rangle\}$. The associated truth table is shown in Fig. 2. It then follows that a simple quantum circuit effecting the transformations (169) and (170), and thereby faithfully representing the entangling probe, is that shown in Fig. 3, in which, according to Eqs. (169) and (170),

$$|A_1\rangle = a_1|w_0\rangle + a_2|w_3\rangle, \tag{174}$$

$$|A_2\rangle = a_2|w_0\rangle + a_1|w_3\rangle. \tag{175}$$

The associated truth table is shown in Fig. 4.

Next, according to Eqs. (41)–(44), the legitimate signal states $\{|u\rangle,|\overline{u}\rangle,|v\rangle,|\overline{v}\rangle\}$, with which the probe states become entangled, can be written in terms of the signal basis states as follows:

$$|u\rangle = c|e_0\rangle + s|e_1\rangle, \tag{176}$$

$$|\overline{u}\rangle = -s|e_0\rangle + c|e_1\rangle, \tag{177}$$

$$|v\rangle = s|e_0\rangle + c|e_1\rangle, \tag{178}$$

$$|\overline{v}\rangle = c|e_0\rangle - s|e_1\rangle, \tag{179}$$

in which, for notational convenience in Figs. 5–8 I define

$$s \equiv \sin\frac{\pi}{8} = \frac{1}{2}(2-2^{1/2})^{1/2}, \tag{180}$$

$$c \equiv \cos\frac{\pi}{8} = \frac{1}{2}(2+2^{1/2})^{1/2}. \tag{181}$$

In Fig. 5, for initial probe state $|A_2\rangle$, the effect of the quantum circuit on signal state $|u\rangle$, Eq. (176), is shown. It then follows from Fig. 5 that the quantum circuit effects the following transformation:

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $\|e_0>$ | $\|A_2>$ | $\|e_0>$ | $\|A_1>$ |
| $\|e_1>$ | $\|A_2>$ | $\|e_1>$ | $\|A_2>$ |

FIG. 4. Truth table for entangling probe.

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $c\|e_0\rangle$ | $\|A_2\rangle$ | $c\|e_0\rangle$ | $\|A_1\rangle$ |
| $s\|e_1\rangle$ | $\|A_2\rangle$ | $s\|e_1\rangle$ | $\|A_2\rangle$ |

FIG. 5. Action of quantum circuit on signal state $|u\rangle$.

$$|u\rangle \otimes |A_2\rangle \rightarrow c|e_0\rangle \otimes |A_1\rangle + s|e_1\rangle \otimes |A_2\rangle, \tag{182}$$

or substituting Eqs. (2) and (3) in Eq. (182), one has equivalently

$$|u\rangle \otimes |A_2\rangle \rightarrow c(c|u\rangle - s|\overline{u}\rangle) \otimes |A_1\rangle + s(c|v\rangle - s|\overline{v}\rangle) \otimes |A_2\rangle, \tag{183}$$

or, using Eqs. (180) and (181),

$$|u\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}[(2+2^{1/2})|A_1\rangle \otimes |u\rangle - 2^{1/2}|A_1\rangle \otimes |\overline{u}\rangle + 2^{1/2}|A_2\rangle \otimes |v\rangle - (2-2^{1/2})|A_2\rangle \otimes |\overline{v}\rangle], \tag{184}$$

which agrees with Eq. (66).

Analogously, in Figs. 6–8, the effects of the quantum circuit on signal states $|\overline{u}\rangle$, $|v\rangle$, and $|\overline{v}\rangle$ are shown. It then follows that the quantum circuit effects the following transformations:

$$|\overline{u}\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}[-2^{1/2}|A_1\rangle \otimes |u\rangle + (2-2^{1/2})|A_1\rangle \otimes |\overline{u}\rangle + (2+2^{1/2})|A_2\rangle \otimes |v\rangle - 2^{1/2}|A_2\rangle \otimes |\overline{v}\rangle], \tag{185}$$

$$|v\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}[2^{1/2}|A_1\rangle \otimes |u\rangle - (2-2^{1/2})|A_1\rangle \otimes |\overline{u}\rangle + (2+2^{1/2})|A_2\rangle \otimes |v\rangle - 2^{1/2}|A_2\rangle \otimes |\overline{v}\rangle\ , \tag{186}$$

$$|\overline{v}\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}[(2+2^{1/2})|A_1\rangle \otimes |u\rangle - 2^{1/2}|A_1\rangle \otimes |\overline{u}\rangle - 2^{1/2}|A_2\rangle \otimes |v\rangle + (2-2^{1/2})|A_2\rangle \otimes |\overline{v}\rangle\ , \tag{187}$$

all of which also agree with Eq. (66).

One concludes that the quantum circuit of Fig. 3 does faithfully represent the action of the unitary transformation $U^{(1)}$ in optimally entangling the signal states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, and $|\overline{v}\rangle$ with the probe states $|A_1\rangle$ and $|A_2\rangle$. It is to be emphasized that the initial state of the probe must be $|A_2\rangle$, given by Eq. (40). [A sign choice in Eq. (40) is made below in Sec. IV, consistent with the measurement procedure defined there.]

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $-s\|e_0\rangle$ | $\|A_2\rangle$ | $-s\|e_0\rangle$ | $\|A_1\rangle$ |
| $c\|e_1\rangle$ | $\|A_2\rangle$ | $c\|e_1\rangle$ | $\|A_2\rangle$ |

FIG. 6. Action of quantum circuit on signal state $|\overline{u}\rangle$.

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $s\|e_0\rangle$ | $\|A_2\rangle$ | $s\|e_0\rangle$ | $\|A_1\rangle$ |
| $c\|e_1\rangle$ | $\|A_2\rangle$ | $c\|e_1\rangle$ | $\|A_2\rangle$ |

FIG. 7. Action of quantum circuit on signal state $|v\rangle$.

## IV. PROBE MEASUREMENT CORRELATIONS

According to the block-diagonal form of the transformation $U^{(1)}$, Eq. (71), and the analysis of Sec. III, the probe produces the following entanglements for initial probe state $|w\rangle = |A_2\rangle$ and incoming signal states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, or $|\overline{v}\rangle$, respectively:

$$|u\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}(|\alpha_+\rangle \otimes |u\rangle + |\alpha\rangle \otimes |\overline{u}\rangle), \tag{188}$$

$$|\overline{u}\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}(|\alpha\rangle \otimes |u\rangle + |\alpha_-\rangle \otimes |\overline{u}\rangle), \tag{189}$$

$$|v\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}(|\alpha_-\rangle \otimes |v\rangle - |\alpha\rangle \otimes |\overline{v}\rangle), \tag{190}$$

$$|\overline{v}\rangle \otimes |A_2\rangle \rightarrow \frac{1}{4}(-|\alpha\rangle \otimes |v\rangle + |\alpha_+\rangle \otimes |\overline{v}\rangle). \tag{191}$$

Then, according to Eqs. (188) and (189), if, following the public reconciliation phase of the BB84 protocol, the signal basis mutually selected by the legitimate transmitter and receiver is publicly revealed to be $\{|u\rangle, |\overline{u}\rangle\}$, then the probe measurement must distinguish the projected probe state $|\alpha_+\rangle$, when the signal state $|u\rangle$ is both sent and received, from the projected probe state $|\alpha_-\rangle$, when the signal state $|\overline{u}\rangle$ is both sent and received. In this case one has the correlations

$$|u\rangle \Leftrightarrow |\alpha_+\rangle, \tag{192}$$

$$|\overline{u}\rangle \Leftrightarrow |\alpha_-\rangle. \tag{193}$$

The same two states $|\alpha_+\rangle$ and $|\alpha_-\rangle$ must be distinguished, no matter which basis is chosen during reconciliation. This is indeed the case since, according to Eqs. (190) and (191), if, following the public reconciliation phase of the BB84 proto-

Truth Table

| in | | out | |
|---|---|---|---|
| control | target | control | target |
| $c\|e_0\rangle$ | $\|A_2\rangle$ | $c\|e_0\rangle$ | $\|A_1\rangle$ |
| $-s\|e_1\rangle$ | $\|A_2\rangle$ | $-s\|e_1\rangle$ | $\|A_2\rangle$ |

FIG. 8. Action of quantum circuit on signal state $|\overline{v}\rangle$.

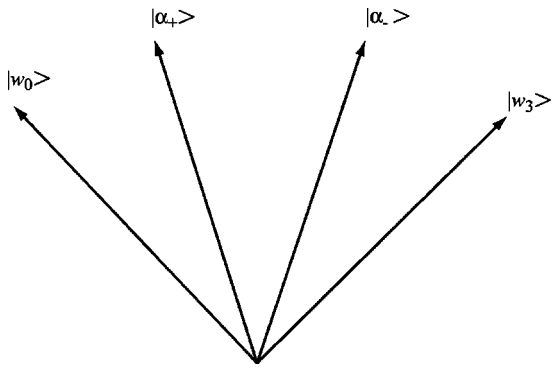


FIG. 9. Geometry of states in the two-dimensional Hilbert space of the probe; correlated probe states $\{|\alpha_+\rangle, |\alpha_-\rangle\}$; probe basis states $\{|w_0\rangle, |w_3\rangle\}$.

col, the signal basis mutually selected by the legitimate transmitter and receiver is publicly revealed to be $\{|v\rangle, |\overline{v}\rangle\}$, then the probe measurement must distinguish the projected probe state $|\alpha_-\rangle$, when the signal state $|v\rangle$ is both sent and received, from the projected probe state $|\alpha_+\rangle$, when the signal state $|\overline{v}\rangle$ is both sent and received. In this case one has the correlations

$$|v\rangle \Leftrightarrow |\alpha_-\rangle, \tag{194}$$

$$|\overline{v}\rangle \Leftrightarrow |\alpha_+\rangle. \tag{195}$$

Next, one notes that the correlations of the projected probe states $|\alpha_+\rangle$ and $|\alpha_-\rangle$ with the probe's two orthogonal basis states $|w_0\rangle$ and $|w_3\rangle$ are indicated, according to Eqs. (72) and (73), by the following probabilities:

$$\frac{|\langle w_0|\alpha_+\rangle|^2}{|\alpha_+|^2} = \frac{|\langle w_3|\alpha_-\rangle|^2}{|\alpha_-|^2} = \frac{1}{2} \pm \frac{[E(1-2E)]^{1/2}}{(1-E)}, \tag{196}$$

$$\frac{|\langle w_0|\alpha_-\rangle|^2}{|\alpha_-|^2} = \frac{|\langle w_3|\alpha_+\rangle|^2}{|\alpha_+|^2} = \frac{1}{2} \mp \frac{[E(1-2E)]^{1/2}}{(1-E)}. \tag{197}$$

At this point I make a choice of the positive sign in Eq. (196), and correspondingly the negative sign in Eq. (197). This choice serves to define the Hilbert-space orientation of the probe basis states, in order that the probe basis state $|w_0\rangle$ be dominantly correlated with the signal states $|u\rangle$ and $|\overline{v}\rangle$, and that the probe basis state $|w_3\rangle$ be dominantly correlated with the signal states $|\overline{u}\rangle$ and $|v\rangle$. With this sign choice, and enforcing monotonicity in $E$, Eqs. (196) and (197) become

$$\frac{|\langle w_0|\alpha_+\rangle|^2}{|\alpha_+|^2} = \frac{|\langle w_3|\alpha_-\rangle|^2}{|\alpha_-|^2} = \frac{1}{2} + \frac{[E(1-2E)]^{1/2}}{(1-E)}, \tag{198}$$

$$\frac{|\langle w_0|\alpha_-\rangle|^2}{|\alpha_-|^2} = \frac{|\langle w_3|\alpha_+\rangle|^2}{|\alpha_+|^2} = \frac{1}{2} - \frac{[E(1-2E)]^{1/2}}{(1-E)}, \tag{199}$$

and one then has the following state correlations:

$$|\alpha_+\rangle \Leftrightarrow |w_0\rangle, \tag{200}$$

$$|\alpha_-\rangle \Leftrightarrow |w_3\rangle. \tag{201}$$

Next combining the correlations (192)–(195), (200), and (201), one then establishes the following correlations:

$$\{|u\rangle, |\overline{v}\rangle\} \Leftrightarrow |\alpha_+\rangle \Leftrightarrow |w_0\rangle, \tag{202}$$

$$\{|\overline{u}\rangle, |v\rangle\} \Leftrightarrow |\alpha_-\rangle \Leftrightarrow |w_3\rangle, \tag{203}$$

to be implemented by the probe measurement method. This can be simply accomplished by a von Neumann–type projective measurement of the orthogonal probe basis states $|w_0\rangle$ and $|w_3\rangle$, implementing the probe projective measurement operators $\{|w_0\rangle\langle w_0|, |w_3\rangle\langle w_3|\}$. The chosen geometry in the two-dimensional Hilbert space of the probe is displayed in Fig. 9, in which the sign choice is enforced in Eqs. (72) and (73), namely,

$$|\alpha_+\rangle = [(2^{1/2}+1)(1+\eta)^{1/2} + (2^{1/2}-1)(1-\eta)^{1/2}]|w_0\rangle + [(2^{1/2}+1)(1-\eta)^{1/2} + (2^{1/2}-1)(1+\eta)^{1/2}]|w_3\rangle, \tag{204}$$

$$|\alpha_-\rangle = [(2^{1/2}+1)(1-\eta)^{1/2} + (2^{1/2}-1)(1+\eta)^{1/2}]|w_0\rangle + [(2^{1/2}+1)(1+\eta)^{1/2} + (2^{1/2}-1)(1-\eta)^{1/2}]|w_3\rangle, \tag{205}$$

where

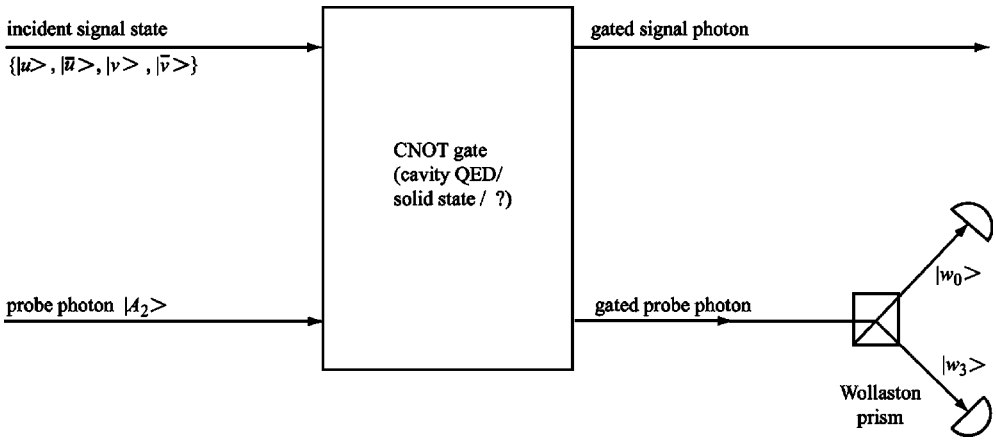


FIG. 10. Entangling probe schematic.

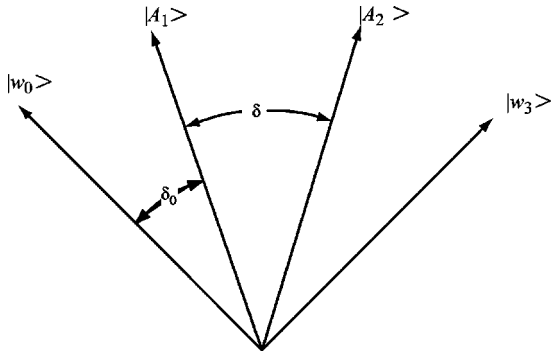


FIG. 11. Geometry of probe states $\{|A_1\rangle, |A_2\rangle\}$; $|A_2\rangle$ is the initial state of the probe.

$$\eta = [8E(1-2E)]^{1/2}, \tag{206}$$

as in Eq. (75). This geometry is consistent with the symmetric von Neumann test, which is an important part of the optimization in Refs. [2–6].

## V. ENTANGLING PROBE IMPLEMENTATION

Based on the results of Secs. III and IV, I invent the entangling probe implementation shown in Fig. 10 [8]. Here, an incident photon coming from the legitimate transmitter is received by the probe in one of the four signal-photon polarization states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, or $|\overline{v}\rangle$. The signal photon enters the control port of the CNOT gate of Figs. 1 and 2. The initial state of the probe is a photon in linear-polarization state $|A_2\rangle$ and entering the target port of the CNOT gate. The probe photon is produced by a single-photon source and is appropriately timed with reception of the signal photon by first sampling a few successive signal pulses to determine the repetition rate of the transmitter. The linear-polarization state $|A_2\rangle$, according to Eq. (40) with the sign choice made in Sec. IV, is given by

$$|A_2\rangle = \left[\frac{1}{2}\{1 - [8E(1-2E)]^{1/2}\}\right]^{1/2}|w_0\rangle + \left[\frac{1}{2}\{1 + [8E(1-2E)]^{1/2}\}\right]^{1/2}|w_3\rangle, \tag{207}$$

and can be simply set for an error rate $E$ by means of a polarization rotator. In this way the device can be tuned to the chosen error rate induced by the probe. The outgoing gated signal photon is relayed on to the legitimate receiver, and the gated probe photon enters a Wollaston prism, oriented to separate orthogonal photon linear-polarization states $|w_0\rangle$ and $|w_3\rangle$, and the photon is then detected by one of two photodetectors. If the basis, revealed during the public basis-reconciliation phase of the BB84 protocol, is $\{|u\rangle, |\overline{u}\rangle\}$, then the photodetector located to receive the polarization state $|w_0\rangle$ or $|w_3\rangle$, respectively, will indicate, in accord with the correlations (202) and (203), that a state $|u\rangle$ or $|\overline{u}\rangle$, respectively, was most likely measured by the legitimate receiver. Alternatively, if the announced basis is $\{\{|v\rangle, |\overline{v}\rangle\}\}$, then the photodetector located to receive the polarization state $|w_3\rangle$ or $|w_0\rangle$, respectively, will indicate, in accord with the correlations (202) and (203), that a state $|v\rangle$ or $|\overline{v}\rangle$, respectively, was most likely measured by the legitimate receiver. By comparing the record of probe-photodetector triggering with the sequence of bases revealed during reconciliation, then the likely sequence of ones and zeros constituting the key, prior to privacy amplification, can be assigned. (Recall that the states $|u\rangle$, $|\overline{u}\rangle$, $|v\rangle$, and $|\overline{v}\rangle$ correspond to Boolean states $|1\rangle$, $|0\rangle$, $|1\rangle$, and $|0\rangle$, respectively [2].) In any case the net effect is to yield, for a set error rate $E$, the maximum information gain to the probe, which is given by Eq. (19), namely,

$$I_{\text{opt}}^{R} = \log_2\left[2 - \left(\frac{1-3E}{1-E}\right)^2\right]. \tag{208}$$

The geometry of the initial and shifted probe polarization states $|A_2\rangle$ and $|A_1\rangle$, respectively, and probe basis states $|w_0\rangle$ and $|w_3\rangle$ in the two-dimensional Hilbert space of the probe is shown in Fig. 11. Here, the angle $\delta_0$ between the probe state $|A_1\rangle$ and the probe basis state $|w_0\rangle$ is given by

$$\delta_0 = \cos^{-1}\left(\frac{\langle w_0|A_1\rangle}{|A_1|}\right), \tag{209}$$

or, substituting $|A_1\rangle$, given by Eq. (39) with the sign choice made in Sec. IV, namely,

$$|A_1\rangle = \left[\frac{1}{2}\{1 + [8E(1-2E)]^{1/2}\}\right]^{1/2}|w_0\rangle + \left[\frac{1}{2}\{1 - [8E(1-2E)]^{1/2}\}\right]^{1/2}|w_3\rangle, \tag{210}$$

in Eq. (209), one obtains

$$\delta_0 = \cos^{-1}\left(\frac{1}{2}\{1 + [8E(1-2E)]^{1/2}\}\right)^{1/2}. \tag{211}$$

This is also the angle between the initial linear-polarization state $|A_2\rangle$ of the probe and the probe basis state $|w_3\rangle$. Also in Fig. 11, the shift $\delta$ in polarization between the initial probe states $|A_2\rangle$ and the state $|A_1\rangle$, in accord with the truth table in Fig. 4, is given by

$$\delta = \cos^{-1}\left(\frac{\langle A_1|A_2\rangle}{|A_1||A_2|}\right), \tag{212}$$

or, substituting Eqs. (207) and (210), one obtains

$$\delta = \cos^{-1}(1-4E). \tag{213}$$

Possible implementations of the CNOT gate are under consideration, including ones based on cavity-QED, solid state, and/or linear optics [8,9]. However, a sufficiently robust high-fidelity CNOT gate, for control and target qubits based on single-photon orthogonal polarization states, is not yet available.

## VI. SUMMARY

Using the sets of optimum probe parameters Eqs. (15)–(17), three corresponding optimized unitary transformations were calculated, representing an entangling probe attacking the BB84 protocol of quantum key distribution. The

corresponding entanglements of the probe states with the signal states are given by Eqs. (66), (100), and (157), or, equivalently, by the corresponding block-diagonal forms Eqs. (71), (101), and (158). All three transformations yield the identical maximum information gain Eq. (19) to the probe, expressed in terms of any set error rate induced by the probe. The simplest of the optimal unitary transformations is represented by Eq. (66), or, equivalently, Eq. (71), in which the Hilbert space of the probe is only two dimensional. Exploiting the quantum-circuit model of quantum computation, the quantum circuit Fig. 3 needed to implement this simplest unitary transformation, was determined and shown to yield the correct entangled states, Eqs. (184)–(187). Thus, the quantum circuit, faithfully representing the optimum entangling probe, consists of a single quantum-controlled-NOT gate in which the control qubit consists of two photon-polarization basis states of the signal, the target qubit consists of the two probe-photon polarization basis states, and the probe photon is prepared in the initial linear-polarization state Eq. (207) set by the induced error rate. The initial polarization state of the probe photon can be produced by a single-photon source together with a linear-polarization rotator. The gated probe photon, optimally entangled with the signal, enters a Wollaston prism which separates the appropriate correlated states of the probe photon to trigger one or the other of two photodetectors. Basis selection, revealed on the public channel during basis reconciliation in the BB84 protocol, is exploited to correlate photodetector clicks with the signal transmitting the key, and to assign the most likely binary number 1 or 0, such that the information gain by the probe of the key, prior to privacy amplification, is maximal. Explicit design parameters for the entangling probe are analytically specified, including (1) the explicit initial polarization state of the probe photon, Eq. (207); (2) the transition state of the probe photon, Eq. (210); (3) the probabilities that one or the other photodetector triggers corresponding to a 0 or 1 of the key, Eqs. (198) and (199); (4) the relative angles between the various linear-polarization states in the Hilbert space of the probe, Eqs. (209), (213), and (5) the information gain by the probe, Eq. (208). The probe is a simple special-purpose quantum-information processor that will improve the odds for an eavesdropper in gaining access to the pre-privacy-amplified key, as well as impose a potentially severe sacrifice of key bits during privacy amplification [4]. The successful implementation of the probe awaits the development of a single robust high-fidelity CNOT gate, and also a practical single-photon source.

## ACKNOWLEDGMENTS

This work was supported by the U. S. Army Research Laboratory, the Defense Advanced Research Projects Agency, and the Advanced Research and Development Activity. The hospitality of the Isaac Newton Institute for Mathematical Sciences at the University of Cambridge, where part of this work was performed, is gratefully acknowledged. The author wishes to thank Noah Linden for inviting him to participate in the Newton Institute program "Quantum Information Theory: Present Status and Future Directions." Also, the author wishes to thank Jeffrey Shapiro, Bryan Jacobs, Charles Bennett, John Preskill, and Jeff Kimble for useful discussions.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[3] H. E. Brandt, Phys. Rev. A **66**, 032303 (2002).
[4] H. E. Brandt, J. Math. Phys. **43**, 4526 (2002).
[5] H. E. Brandt, J. Opt. B: Quantum Semiclassical Opt. **5**, S557 (2003).
[6] H. E. Brandt, Quantum Inf. Process. **2**, 37 (2003).
[7] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[8] H. E. Brandt, U. S. Army Research Laboratory, Adelphi, MD, Invention Disclosure, 2004 (unpublished).
[9] See, e.g., L.-M. Duan and H. J. Kimble, Phys. Rev. Lett. **92**, 127902 (2004); T. B. Pittman, M. J. Fitch, B. C. Jacobs, and J. D. Franson, Phys. Rev. A **68**, 032316 (2003); J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning, Nature (London) **426**, 264 (2003); M. Fiorentino and F. N. C. Wong, Phys. Rev. Lett. **93**, 070502 (2004); S. Gasparoni, J. W. Pan, P. Walther, T. Rudolph, and A. Zeilinger, *ibid.* **93**, 020504 (2004).