Eavesdropping optimization for quantum cryptography using a positive operator-valued measure

Howard E. Brandt
U.S. Army Research Laboratory, 2800 Powder Mill Road, Adelphi, Maryland 20783
(Received 15 September 1998; revised manuscript received 16 December 1998)

It is demonstrated that the eavesdropping optimization obtained recently by Slutsky *et al.* [Phys. Rev. A **57**, 2383 (1998)] for Bennett's two-state protocol of key distribution in quantum cryptography holds, not only for the case in which an ordinary von Neumann projective measure is implemented by the legitimate receiver, but also for the case in which a positive operator-valued measure is implemented, as in Brandt *et al.* [Phys. Rev. A **56**, 4456 (1997)]. In both cases, identical expressions hold for both the Renyi information gained by the eavesdropper and for the error rate induced by the eavesdropper in terms of the parameters characterizing the key distribution system and the eavesdropper's probe. [S1050-2947(99)03004-8]

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

I. INTRODUCTION

For Bennett's two-state protocol ($B92$) of key distribution in quantum cryptography [1], Slutsky *et al.* recently constructed the optimal eavesdropping method, which on average yields the most information to the eavesdropper for a given error rate caused by a unitary probe of the eavesdropper [2]. The most general possible *individual* attack consistent with quantum mechanics was constructed in which each transmitted bit is attacked individually and independently from other bits. The eavesdropper causes the carrier to interact with her probe so that the carrier and the probe are left in an entangled state, and subsequent measurement of the probe by the eavesdropper yields information about the carrier state.

The optimal eavesdropping method is based on maximization of the Renyi information gained by the eavesdropper on corrected data for a given error rate. Corrected data include data remaining after discarding inconclusive results and also erroneous data as determined by block checksums and bisective search. The optimization is needed to establish the security of the key against individual attack, by guaranteeing it to be exponentially unlikely that more than token knowledge of the final key is available to the eavesdropper following key distillation [3–5]. Slutsky *et al.* based their optimization on the very general eavesdropping interaction model of Fuchs and Peres [6]. The Fuchs-Peres model analytically characterizes the most general possible unitary probe consistent with quantum mechanics.

Slutsky *et al.* assumed that the legitimate receiver of the key implements a simple pair of ordinary von Neumann projective measurements. However, it is well known that the number of inconclusive results can be reduced by using a key receiver based on a positive operator-valued measure (POVM) [7,8]. In the present paper I extend the analysis of Slutsky *et al.* to include the case in which a particular all-optical POVM receiver [8,9] is used in the $B92$ protocol, employing two nonorthogonal photon polarization states. In particular, I demonstrate here that the identical optimization obtained by Slutsky *et al.* [2] applies for the POVM receiver of Brandt, Myers, and Lomonaco [8], as well as for the ordinary von Neumann projective receiver.

Because of the noncommutativity of nonorthogonal photon polarization measurement operators, a simple von Neumann projective measurement cannot conclusively distinguish the state of a photon having two possible nonorthogonal polarization states as in the $B92$ protocol. To distinguish conclusively between two nonorthogonal states $|u\rangle$ and $|v\rangle$, one can implement the following POVM representing the possible measurements performed by the key receiver [7–11]:

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

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

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

The POVM operators, Eqs. (1)–(3), are positive and sum to the identity. When an ideal detector representing the operator A_u responds positively, it follows that a photon with a v polarization state cannot have been received. Likewise, when an ideal detector representing the A_v operator responds positively, a photon with a u polarization state cannot have been received. The operator $A_?$ is represented by a detector that registers inconclusive events. All-optical implementations of the POVM, Eqs. (1)–(3), in quantum cryptography have recently been proposed [8,11–13].

Before proceeding, it is well to mention other related work. Numerous analyses of various eavesdropping strategies for several protocols have appeared in the recent literature [14–40]. These works include analyses of (1) independent attacks, (2) *collective* attacks, in which the eavesdropper entangles a separate probe with each transmitted particle and measures all probes together as one system, and (3) *coherent* or *joint* attacks, in which a single probe is entangled with the entire set of carrier particles. The collective and coherent attacks are, however, impractical at present with current quantum technology. They require the maintenance of coherent superpositions of large numbers of quantum states. State storage and decoherence present major issues.

In Sec. II, I calculate the disturbed states for the $B92$ protocol by using the eavesdropping model of Slutsky *et al.* [2] and assuming the POVM receiver of Brandt, Myers, and Lomonaco [8] is implemented. In Sec. III, I calculate the

associated information gained by the eavesdropper and demonstrate it to be identical to that for the case in which an ordinary von Neumann projective receiver is used. Then in Sec. IV, I calculate the error rate and show that it, too, is identical for either a POVM receiver or a projective receiver. Section V presents a summary of results and conclusions.

II. DISTURBED STATES

In the Fuchs-Peres model of eavesdropping on the B92 protocol, an incoming carrier state $|u\rangle$ and the eavesdropper's probe state $|w\rangle$ undergo joint unitary evolution represented by a unitary operator U, resulting in the entangled state [2,6]:

$$U|u\otimes w\rangle=\tfrac{1}{2}[(1+\sec 2\alpha)|\Phi_{00}\rangle+\tan 2\alpha|\Phi_{10}\rangle-\tan 2\alpha|\Phi_{01}\rangle+(1-\sec 2\alpha)|\Phi_{11}\rangle]\otimes|u\rangle$$
$$-\tfrac{1}{2}[\tan 2\alpha|\Phi_{00}\rangle-(1-\sec 2\alpha)|\Phi_{10}\rangle-(1+\sec 2\alpha)|\Phi_{01}\rangle-\tan 2\alpha|\Phi_{11}\rangle]\otimes|v\rangle. \tag{4}$$

Here the angle α is given by

$$\alpha=\tfrac{1}{2}\sin^{-1}\langle u|v\rangle, \tag{5}$$

in terms of the Dirac bracket of the nonorthogonal states $|u\rangle$ and $|v\rangle$, and $|\Phi_{mn}\rangle$ are the states in the Hilbert space of the probe and are neither normalized nor orthogonal. Equation (4) follows from Eqs. (1) and (2) of Slutsky *et al.* [2]. Similarly, for an incoming state $|v\rangle$, one has

$$U|v\otimes w\rangle=\tfrac{1}{2}[\tan 2\alpha|\Phi_{00}\rangle+(1+\sec 2\alpha)|\Phi_{10}\rangle+(1-\sec 2\alpha)|\Phi_{01}\rangle-\tan 2\alpha|\Phi_{11}\rangle]\otimes|u\rangle$$
$$+\tfrac{1}{2}[(1-\sec 2\alpha)|\Phi_{00}\rangle-\tan 2\alpha|\Phi_{10}\rangle+\tan 2\alpha|\Phi_{01}\rangle+(1+\sec 2\alpha)|\Phi_{11}\rangle]\otimes|v\rangle. \tag{6}$$

The probe states $|\Phi_{mn}\rangle$ have the following symmetry properties [2,6]:

$$|\Phi_{00}|=|\Phi_{11}|, \tag{7}$$
$$|\Phi_{01}|=|\Phi_{10}|, \tag{8}$$
$$\langle\Phi_{00}|\Phi_{01}\rangle=\langle\Phi_{11}|\Phi_{10}\rangle, \tag{9}$$
$$\langle\Phi_{00}|\Phi_{10}\rangle=\langle\Phi_{11}|\Phi_{01}\rangle, \tag{10}$$
$$\langle\Phi_{01}|\Phi_{10}\rangle=\langle\Phi_{10}|\Phi_{01}\rangle, \tag{11}$$
$$\langle\Phi_{01}|\Phi_{00}\rangle=\langle\Phi_{10}|\Phi_{11}\rangle, \tag{12}$$
$$\langle\Phi_{01}|\Phi_{11}\rangle=\langle\Phi_{10}|\Phi_{00}\rangle, \tag{13}$$
$$\langle\Phi_{11}|\Phi_{00}\rangle=\langle\Phi_{00}|\Phi_{11}\rangle. \tag{14}$$

These symmetries arise from the random equiprobable selection of carrier states $|u\rangle$ and $|v\rangle$ by the key transmitter and the resulting symmetry of the probe under interchange of $|u\rangle$ and $|v\rangle$.

For the all-optical POVM receiver, the state $|\psi_6\rangle$, entering the u detector for an input state

$$|\psi\rangle=\overline{\alpha}|u\rangle+\overline{\beta}|v\rangle \tag{15}$$

is given by

$$|\psi_6\rangle=-\overline{\alpha}(1-\sin 2\alpha)^{1/2}|e\rangle, \tag{16}$$

where $|e\rangle$ is a unit ket [8,11]. Also, the state $|\psi_7\rangle$ entering the v detector is

$$|\psi_7\rangle=i\overline{\beta}(1-\sin 2\alpha)^{1/2}|e\rangle. \tag{17}$$

Equations (16) and (17) are Eqs. A21 and A22 of Brandt, Myers, and Lomonaco [8] expressed in a more convenient notation. They follow from the detailed structure of the all-optical POVM receiver [8,11,12]. Comparing Eqs. (4) and (16), it follows that if the sender Alice sends a u state, the eavesdropper Eve with her probe relays the state Eq. (4) to the receiver Bob, and Bob's POVM receiver detects a u state, then the probe is left in the correlated state,

$$|\psi_{uu}\rangle=-\tfrac{1}{2}(1-\sin 2\alpha)^{1/2}[(1+\sec 2\alpha)|\Phi_{00}\rangle+\tan 2\alpha|\Phi_{10}\rangle$$
$$-\tan 2\alpha|\Phi_{01}\rangle+(1-\sec 2\alpha)|\Phi_{11}\rangle]. \tag{18}$$

Also, from Eqs. (4) and (17), one can conclude that if the v detector responds, then the probe is left in the state

$$|\psi_{uv}\rangle=\frac{i}{2}(1-\sin 2\alpha)^{1/2}[-\tan 2\alpha|\Phi_{00}\rangle+(1-\sec 2\alpha)|\Phi_{10}\rangle+(1+\sec 2\alpha)|\Phi_{01}\rangle+\tan 2\alpha)|\Phi_{11}\rangle]. \tag{19}$$

Analogously, one obtains

$$|\psi_{vv}\rangle=\frac{i}{2}(1-\sin 2\alpha)^{1/2}[(1-\sec 2\alpha)|\Phi_{00}\rangle-\tan 2\alpha|\Phi_{10}\rangle+\tan 2\alpha|\Phi_{01}\rangle+(1+\sec 2\alpha)|\Phi_{11}\rangle], \tag{20}$$

and

$$|\psi_{vu}\rangle = -\tfrac{1}{2}(1-\sin 2\alpha)^{1/2}[\tan 2\alpha|\Phi_{00}\rangle + (1+\sec 2\alpha)|\Phi_{10}\rangle + (1-\sec 2\alpha)|\Phi_{01}\rangle - \tan 2\alpha|\Phi_{11}\rangle]. \quad (21)$$

We proceed to calculate the information gain available to the eavesdropper.

III. EAVESDROPPER'S INFORMATION GAIN

Eve must distinguish between the two equiprobable states $|\psi_{uu}\rangle$ and $|\psi_{vv}\rangle$, since all other events appear as errors or inconclusive results to Alice and Bob, and are announced and discarded in the *B*92 protocol. Both the Shannon and Renyi information are in this case maximized by a simple two-dimensional von Neumann test, symmetric about the state vectors $|\psi_{uu}\rangle$ and $|\psi_{vv}\rangle$ [41,42]. The resulting Renyi information gain is

$$I_{opt}^{R} = \log_2(2-Q^2), \quad (22)$$

expressed in terms of the overlap

$$Q = \frac{|\langle\psi_{uu}|\psi_{vv}\rangle|}{|\psi_{uu}||\psi_{vv}|} \quad (23)$$

between the projected correlated probe states $|\psi_{uu}\rangle$ and $|\psi_{vv}\rangle$ [Eq. (22) follows from Eqs. (7a) and (7b) of Slutsky *et al.* [2]]. In the optimized individual attack when Bob uses the POVM receiver, Eve must minimize the overlap Q, Eq. (23), between the projected correlated probe states, given by Eqs. (18) and (20).

Next, by using Eqs. (18) and (20) and simple trigonometric identities, the states $|\psi_{uu}\rangle$ and $|\psi_{vv}\rangle$ appearing in Eq. (23), can be rewritten as follows:

$$|\psi_{uu}\rangle = -(1-\sin 2\alpha)^{1/2}\sec 2\alpha[|\Phi_{00}\rangle\cos^2\alpha - |\Phi_{11}\rangle\sin^2\alpha + (|\Phi_{10}\rangle - |\Phi_{01}\rangle)\sin\alpha\cos\alpha], \quad (24)$$

$$|\psi_{vv}\rangle = i(1-\sin 2\alpha)^{1/2}\sec 2\alpha[|\Phi_{11}\rangle\cos^2\alpha - |\Phi_{00}\rangle\sin^2\alpha - (|\Phi_{10}\rangle - |\Phi_{01}\rangle)\sin\alpha\cos\alpha]. \quad (25)$$

Next, if one compares Eqs. (23)–(25) with Eq. (10) of Slutsky *et al.* [2], and with the expressions given there for the states $|\psi_{u,\bar{v}}\rangle$ and $|\psi_{v,\bar{u}}\rangle$ (see Appendix C of [2]), it becomes immediately evident that both expressions for the overlap Q are identical. In particular, $|\psi_{uu}\rangle$ here differs from $|\psi_{u,\bar{v}}\rangle$ there by only an overall factor of $-(1-\sin 2\alpha)^{1/2}\sec 2\alpha$ and $|\psi_{vv}\rangle$ here differs from $|\psi_{v,\bar{u}}\rangle$ there by only an overall factor of $i(1-\sin 2\alpha)^{1/2}\sec 2\alpha$. One can therefore conclude that the overlap Q, in the case of the POVM receiver of Brandt, Myers, and Lomonaco [8], is identical to the overlap obtained in Slutsky *et al.* [2] for a von Neumann projective receiver. The corresponding Renyi information gained by the eavesdropper, Eq. (22), is then also equivalent for both receivers. We proceed to calculate the error rate induced by the eavesdropper in the POVM receiver of the legitimate users, Alice and Bob.

IV. ERROR RATE INDUCED BY EVE

Because states $|u\rangle$ and $|v\rangle$ are equiprobable, and due to the resulting symmetry in $|u\rangle$ and $|v\rangle$, the error rate between Alice and Bob is the frequency of erroneous events in which $|u\rangle$ is transmitted and $|v\rangle$ is received relative to the sum of (1) the frequency of valid events in which $|u\rangle$ is transmitted and received, and (2) the frequency that $|u\rangle$ is transmitted and $|v\rangle$ is received. The error rate in Bob's POVM receiver due to the disturbance caused by the eavesdropper is thus given by

$$E = \frac{P_{uv}}{P_{uv}+P_{uu}}, \quad (26)$$

where P_{ij} is the probability that Bob detects a j polarization state when Alice sends an i polarization state. For the POVM receiver, one has, in terms of the POVM operator A_v, Eq. (2),

$$P_{uv} = \langle u\otimes w|U^{\dagger}A_v U|u\otimes w\rangle. \quad (27)$$

However, without directly evaluating Eq. (27), which can be shown by lengthy algebraic reduction leads to the same conclusion, one can see from Eqs. (17) and (4) that for the POVM receiver considered here,

$$P_{uv} = |\psi_7|^2 = \langle\psi_7|\psi_7\rangle, \quad (28)$$

where

$$|\psi_7\rangle = -\frac{i}{2}(1-\sin 2\alpha)^{1/2}[\tan 2\alpha|\Phi_{00}\rangle - (1-\sec 2\alpha)|\Phi_{10}\rangle - (1+\sec 2\alpha)|\Phi_{01}\rangle - \tan 2\alpha|\Phi_{11}\rangle]. \quad (29)$$

Next, using simple trigonometric identities in Eq. (29), one easily obtains

$$|\psi_7\rangle = i(1-\sin 2\alpha)^{1/2}\sec 2\alpha[|\Phi_{01}\rangle\cos^2\alpha - |\Phi_{10}\rangle\sin^2\alpha + (|\Phi_{11}\rangle - |\Phi_{00}\rangle)\sin\alpha\cos\alpha]. \quad (30)$$

Also, one has

$$P_{uu} = |\psi_{uu}|^2. \quad (31)$$

Then, if one compares Eqs. (26), (28), (30), (31), and (24) with Eq. (9) of Slutsky *et al.* [2], and with the expressions given there for the states $|\psi_{u,\bar{u}}\rangle$ and $|\psi_{u,\bar{v}}\rangle$ (see Appendix C of [2]), it immediately becomes evident that both expressions for the error rate E are identical. In particular, $|\psi_7\rangle$ here differs from $|\psi_{u,\bar{u}}\rangle$ there by only an overall factor of $i(1-\sin 2\alpha)^{1/2}\sec 2\alpha$, and, as noted previously, $|\psi_{uu}\rangle$ here differs from $|\psi_{u,\bar{v}}\rangle$ there by only an overall factor of $-(1-\sin 2\alpha)^{1/2}\sec 2\alpha$. One can conclude that the error rate E is identical to the error rate that was obtained by Slutsky *et al.* [2] for a receiver based on a von Neumann projective measurement, just as is the overlap, and the Renyi information gain. Since both the error rate and the Renyi information available to the eavesdropper are the same for the POVM receiver considered here as for the ordinary projective receiver, it follows that the same optimization of Slutsky *et al.* [2] must apply whether Bob uses a von Neumann projective receiver or the POVM receiver considered here. For other possible POVM implementations, any such equivalence may or may not apply.

V. CONCLUSIONS

It has been demonstrated that the eavesdropping optimization obtained recently by Slutsky *et al.* for Bennett's two-state protocol of key generation in quantum cryptography holds for the case in which the POVM implementation of Brandt, Myers, and Lomonaco [8] is employed by the legitimate receiver, as well as for the case in which an ordinary von Neumann projective measurement is implemented. For the POVM receiver considered here, the eavesdropper's gain in Renyi information on corrected data was formulated in terms of the overlap of the appropriate correlated probe states. Also, the POVM receiver error rate due to eavesdropping was formulated. For both types of receiver, identical expressions were shown to result for both the Renyi information gained by the eavesdropper and for the error rate induced by the eavesdropper in terms of the parameters characterizing the key distribution system and the eavesdropper's probe.

ACKNOWLEDGMENTS

This work was supported by the U.S. Army Research Laboratory. Useful communications with J. M. Myers, J. D. Franson, B. A. Slutsky, D. Mayers, W. K. Wootters, S. J. Lomonaco, J. D. Murley, and M. Kruger are gratefully acknowledged.

[1] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[2] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, Phys. Rev. A **57**, 2383 (1998).
[3] B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and S. Fainman, Appl. Opt. **37**, 2869 (1998).
[4] B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, J. Mod. Opt. **44**, 953 (1997).
[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[6] C. A. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[7] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
[8] H. E. Brandt, J. M. Myers, and S. J. Lomonaco, Jr., Phys. Rev. A **56**, 4456 (1997); **58**, 2617 (1998).
[9] J. M. Myers and H. E. Brandt, Meas. Sci. Technol. **8**, 1222 (1997).
[10] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1993).
[11] H. E. Brandt, Am. J. Phys. (to be published).
[12] H. E. Brandt and J. M. Myers, Invention disclosure: POVM Receiver for Quantum Cryptography (U.S. Army Research Laboratory, Adelphi, MD, 1996).
[13] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[14] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[15] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[16] D. Mayers, in *Advances in Cryptology*, Proceedings of CRYPTO 95: 15th Annual International Cryptology Conference, Santa Barbara, California, 1995, edited by D. Coppersmith (Springer, Berlin, 1995), pp. 124–135.
[17] A. C. Yao, in *Proceedings of the 27th Annual ACM Symposium on Theory of Computing: Las Vegas, Nevada, 1995*, (ACM, New York, 1995).
[18] N. Lütkenhaus, Phys. Rev. A **54**, 97 (1996).
[19] D. Mayers, in *Advances in Cryptology*, Proceedings of CRYPTO 96: 16th Annual International Cryptology Conference, Santa Barbara, California, 1996, edited by N. Roblitz (Springer, Berlin, 1996), pp. 343–357.
[20] H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).
[21] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[22] C. H. Bennett, T. Mor, and J. A. Smolin, Phys. Rev. A **54**, 2675 (1996).
[23] B. Slutsky, P. C. Sun, Y. Mazurenko, R. Rao, and Y. Fainman, Proc. SPIE **2690**, 63 (1996).
[24] N. Gisin and B. Huttner, Phys. Lett. A **228**, 13 (1997); **232**, 463 (1997).
[25] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[26] C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[27] R. B. Griffiths and C. S. Niu, Phys. Rev. A **56**, 1173 (1997).
[28] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).

[29] E. Biham and T. Mor, Phys. Rev. Lett. **79**, 4034 (1997).
[30] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[31] M. Hillery and V. Buzek, Phys. Rev. A **56**, 1212 (1997).
[32] C. A. Fuchs and J. van de Graaf, e-print quant-ph/9712042 (unpublished).
[33] N. Lütkenhaus and S. M. Barnett, in *Quantum Communication, Computing and Measurement*, edited by O. Hirota *et al.* (Plenum, New York, 1997), pp. 89–98.
[34] V. Buzek, M. Hillery, and P. L. Knight, Fortschr. Phys. **46**, 521 (1998).
[35] D. Brusz, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[36] D. Mayers and A. Yao, e-print quant-ph/9802025 (unpublished).
[37] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, e-print quant-ph/9801022 (unpublished).
[38] C. A. Fuchs, Fortschr. Phys. **46**, 535 (1998).
[39] N. Lütkenhaus, e-print quant-ph/9806008 (unpublished).
[40] H. K. Lo and H. F. Chau, e-print quant-ph/9803006 (unpublished).
[41] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[42] L. B. Levitin, in *Quantum Communications and Measurement*, edited by V. P. Belovkin, O. Hirota, and R. L. Hudson (Plenum, New York, 1995), pp. 439–448.