Renyi information gain on quantum key

Howard E. Brandt
U.S. Army Research Laboratory, Adelphi, MD
E-mail: hbrandt@arl.army.mil

Abstract. The concept of maximum Renyi information gain from quantum key is important in eavesdropping and security analyses of quantum key distribution. It is particularly useful in the design optimization of eavesdropping probes. The present work reviews the quantitative measure of Renyi information gain, its optimization, and application to the design of eavesdropping probes in which single-photon probe states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver.

Keywords: quantum cryptography, quantum key distribution, quantum communication, entanglement.

1. Introduction
In cryptography, the key is a random binary sequence used for encryption. An encrypted message can be produced by adding the key to the message (also written in binary), and decrypted by subtracting the key from the encryption. The key must be secure from eavesdropping. In the Bennett-Brassard 1984 (BB84) protocol [1] of quantum key distribution (QKD) [2], the ones and zeros of a potential key can be encoded in four different single-photon linear polarization states. Those four states \( |u\rangle \), \( |\tilde{u}\rangle \), \( |v\rangle \), and \( |\tilde{v}\rangle \) all lie in a real two-dimensional Hilbert space such that \( \langle u|\tilde{u}\rangle = 0 \), \( \langle v|\tilde{v}\rangle = 0 \), and \( \langle u|v\rangle = 2^{-1/2} \). The states \( |u\rangle \) and \( |v\rangle \) can be chosen to encode binary number 1, and the states \( |\tilde{u}\rangle \) and \( |\tilde{v}\rangle \) encode the number 0. The states \{\( |u\rangle , |\tilde{u}\rangle \} \) form one basis, the states \{\( |v\rangle , |\tilde{v}\rangle \} \) form the other basis, and the states \( |u\rangle \) and \( |v\rangle \) are nonorthogonal with angle \( \pi/4 \) between them. For analytical purposes it is convenient to choose two orthonormal basis states \( |e_0\rangle \) and \( |e_1\rangle \) oriented symmetrically with respect to the four signal states, the state \( |e_0\rangle \) making an angle of magnitude \( \pi/8 \) with the states \( |u\rangle \) and \( |\tilde{u}\rangle \), and the state \( |e_1\rangle \) making an angle of magnitude \( \pi/8 \) with the states \( |v\rangle \) and \( |\tilde{v}\rangle \) [3]. In the BB84 protocol, the transmitter (also known as Alice) randomly chooses a basis \{\( |u\rangle , |\tilde{u}\rangle \} \) or \{\( |v\rangle , |\tilde{v}\rangle \} \) and then randomly picks one of the two states in the chosen basis and then sends it to the receiver (also known as Bob). The receiver randomly chooses one of the two measurement bases \{\( |u\rangle , |\tilde{u}\rangle \} \) or \{\( |v\rangle , |\tilde{v}\rangle \} \), and during reconciliation publicly announces which measurement basis is chosen. This procedure is repeated for each photon in a train of single photons transmitted from the transmitter to the receiver. In those cases in which the basis choices by the transmitter and the receiver are the same, those bits are kept and contribute to the potential key. Bits resulting from differing basis selections by the transmitter and receiver, as well as any erroneous bits identified by block checksums and bisective search, are discarded and do not contribute to the key. Also during reconciliation the relative order of selected and discarded bits along with the respective basis choices are in principle publicly available to an eavesdropper. Numerous analyses of various eavesdropping protocols have appeared in the literature [2], making quantitative comparisons...
between various protocols, including the protocol addressed here [3–5]. Eavesdropping probe optimizations have been performed [3, 4, 6, 7], which on average yield the most information to the eavesdropper for a given error rate caused by the probe. The most general possible probes consistent with unitarity were considered [3–8] in which each individual transmitted bit is made to interact with the probe so that the carrier and the probe are left in an optimum entangled state, and measurement of the probe then yields information about the carrier state. The probe optimizations are based on maximizing the order-two Renyi information gain by the probe on corrected data for a set error rate induced by the probe in the legitimate receiver.

The purpose of the present work is to (1) review the quantitative measure of Renyi information gain from the key by an eavesdropping probe entangled with the QKD signal, (2) sketch the procedure for calculating the maximum Renyi information gain by the probe in terms of the induced error rate, and (3) briefly describe recent designs for entangling probes that can extract maximum Renyi information from the quantum key.

2. Renyi information gain
It is first well to recall the definition of Renyi entropy as it is used in QKD privacy amplification. Privacy amplification is the required process of distilling the key in order to make it secure. The Renyi entropy of order two, which is commonly referred to for short as Renyi entropy, is defined as the negative base-two logarithm of the collision probability of a random variable, as in Eqs. (2) or (3) below [9, 10]. The collision probability of the random variable is the sum of the squares of the probabilities for each value of the random variable. The importance of the Renyi entropy in QKD lies in its role 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 an eavesdropper following key distillation [3, 5, 11–13]. In this connection it is well to recall the privacy amplification theorem [11]. Here, a useful quantity is the Renyi information gain on a random variable, and is defined as the decrease in Renyi entropy. The privacy amplification theorem states that if an eavesdropper’s Renyi information gain \( I^R(l) \) on an \( l \) bit data string is less than some quantity \( r \), then the eavesdropper’s Shannon information \( I^H(l - s) \) on the reduced \( (l - s) \) bit string, for a privacy amplification compression level \( s \), averaged over the choice of privacy amplification hash function, is bounded above, namely, \( \langle I^H(l - s) \rangle \leq 2^{r-s}/\ln 2 \), in which the bracket denotes the average. Here, the privacy amplification compression level \( s \) is the reduction in the number of bits from the pre-privacy amplified key which is required in order to make the key secure. By choosing the compression level \( s \) sufficiently large, the exponent appearing in the above upper bound becomes sufficiently negative that the average Shannon information can be made arbitrarily small. Of course the price to pay is reduction in the amount of secure key which is produced. The secrecy of the final key is recovered (but reduced in size) if an upper bound \( r \) can be determined on the Renyi information gain by the eavesdropper on the pre-privacy amplified key. It then follows that the greater the Renyi information gain by an eavesdropping probe, the greater the amount of key which must be sacrificed during privacy amplification, and the more taxing is the eavesdropping attack.

The expectation value of the Renyi information gain by the eavesdropping probe for each single-photon transmission in the BB84 QKD protocol is given by the expected value of the decrease in Renyi entropy of the probe, namely [3],

\[
I^R = \sum_{\mu} P_{\mu} (R_0 - R_{\mu}),
\]

where \( P_{\mu} \) is the a priori probability of probe measurement outcome \( \mu \), \( R_0 \) is the initial Renyi entropy, and \( R_{\mu} \) is the a posteriori Renyi entropy concerning the probe state for outcome \( \mu \). It is to be understood here that the entanglement produced by the probe puts the probe in some...
correlated state \(i\) which when measured yields some measurement outcome \(\mu\). The initial Renyi entropy \(R_0\) is given by [10, 11]

\[
R_0 = -\log_2 \sum_i p_i^2,
\]

(2)

where \(p_i\) is the a priori probability that the probe is in state \(i\), and the a posteriori entropy \(R_\mu\) is given by

\[
R_\mu = -\log_2 \sum_i q_{i\mu}^2,
\]

(3)

where \(q_{i\mu}\) is the a posteriori probability that the probe is in state \(i\) for a measurement outcome \(\mu\). In the present work, for two probe states, one has \(i = 1\) or \(2\); and for two measurement outcomes, one has \(\mu = 1\) or \(2\). The a priori probability \(P_\mu\) of probe measurement outcome \(\mu\) is given by

\[
P_\mu = \Tr \left( E_\mu \sum_i p_i \rho^{(i)} \right).
\]

(4)

The operators \(E_\mu\) and \(\rho^{(i)}\) are defined in the following. Here \(\rho^{(i)}\) is the density operator for the projected state \(|\psi_i\rangle\) of the probe, correlated with the correct measurement outcome of the legitimate receiver, namely,

\[
\rho^{(i)} = |\psi_i\rangle \langle \psi_i|.
\]

(5)

The projected probe states \(|\psi_i\rangle\) are in general nonorthogonal. The intervening probe disturbs the signal states, when any one of the four BB84 signal states is transmitted to the legitimate receiver, and the probe transforms the combined signal state and initial state of the probe into an entangled state which is a superposition of the combined correct state of the signal with the correlated probe state and a combined signal error state with its correlated probe state. For example, if in the \(|u\rangle, |\tilde{u}\rangle\) basis a state \(|u\rangle\) is transmitted and also correctly received by the legitimate receiver, then the projected probe state \(|\psi_1\rangle\) is correlated with the event; or if instead \(|\tilde{u}\rangle\) is sent and correctly received, then the projected probe state \(|\psi_2\rangle\) is correlated with the event. Also in Eq.(4), \(E_\mu\) is the probe measurement operator,

\[
E_\mu = |\tilde{w}_\mu\rangle \langle \tilde{w}_\mu|,
\]

(6)

where \(|\tilde{w}_\mu\rangle\) are the orthonormal measurement basis vectors of the probe. According to Bayes’ rule, the a posteriori probability \(q_{i\mu}\) that the probe is in state \(i\) for probe measurement outcome \(\mu\) is given by

\[
q_{i\mu} = \frac{1}{P_\mu} \Tr \left( E_\mu \rho^{(i)} \right) p_i.
\]

(7)

From Eqs.(4) and (7), it follows that

\[
\sum_i q_{i\mu} = 1.
\]

(8)

For the case in which only two probe states must be distinguished (which for both bases is the case in the present work), it follows from the symmetry of the BB84 protocol that one has equal a priori probabilities for the probe to be in state 1 or 2, namely,
For the case of two probe states, $|\psi_1\rangle$ and $|\psi_2\rangle$, correlated with the correct measurements made by the legitimate receiver, it is known that the information gain is maximized when a simple two-dimensional von Neumann projective measurement is made in which the orthonormal measurement vectors $|\tilde{w}_1\rangle$ and $|\tilde{w}_2\rangle$ are located symmetrically with respect to the two correlated state vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ of the probe in the real two-dimensional Hilbert space of the probe [3, 14, 15]. This symmetric von Neumann test maximizes both the Renyi and Shannon information gain [3]. From the geometry of the Hilbert space of the probe (see Section 1), it follows, for example, that the angle $\xi$ between $|\psi_1\rangle$ and $|\tilde{w}_1\rangle$ is half the complement of the angle between $|\psi_1\rangle$ and $|\psi_2\rangle$. Thus one has

$$\langle \psi_1 | \tilde{w}_1 \rangle = \langle \psi_2 | \tilde{w}_2 \rangle \equiv \cos \xi = \cos \left( \frac{1}{2} \left[ \frac{\pi}{2} - \cos^{-1} Q \right] \right),$$

(10)

and

$$\langle \psi_1 | \tilde{w}_2 \rangle = \langle \psi_2 | \tilde{w}_1 \rangle \equiv \sin \xi = \sin \left( \frac{1}{2} \left[ \frac{\pi}{2} - \cos^{-1} Q \right] \right),$$

(11)

in which one defines the overlap of the states $|\psi_1\rangle$ and $|\psi_2\rangle$, correlated with the measurements of the signal, by [3]

$$Q \equiv \frac{\langle \psi_1 | \psi_2 \rangle}{|\psi_1||\psi_2|}.$$  

(12)

Next substituting Eqs.(6), (9), and (5) in Eq.(4), one has

$$P_\mu = \sum_i \frac{1}{2} \text{Tr} \left( |\tilde{w}_\mu\rangle \langle \tilde{w}_\mu| |\psi_i\rangle \langle \psi_i| \right),$$

(13)

or equivalently,

$$P_\mu = \frac{1}{2} \left[ |\langle \psi_1 | \tilde{w}_\mu \rangle|^2 + |\langle \psi_2 | \tilde{w}_\mu \rangle|^2 \right].$$

(14)

Substituting Eqs.(10) and (11) in Eq.(14), one obtains

$$P_1 = \frac{1}{2} \left[ \cos^2 \xi + \sin^2 \xi \right] = \frac{1}{2},$$

(15)

$$P_2 = \frac{1}{2} \left[ \sin^2 \xi + \cos^2 \xi \right] = \frac{1}{2}.$$  

(16)

Next substituting Eqs.(15), (6), (5), and (9) in Eq.(7), one has

$$q_{11} = 2 \text{Tr} \left( \frac{1}{2} |\tilde{w}_1\rangle \langle \tilde{w}_1| |\psi_1\rangle \langle \psi_1| \right) = |\langle \psi_1 | \tilde{w}_1 \rangle|^2,$$

(17)

and substituting Eq.(10) in Eq.(17), one has

$$q_{11} = \cos^2 \left( \frac{1}{2} \left[ \frac{\pi}{2} - \cos^{-1} Q \right] \right),$$

(18)

or equivalently, using a trigonometric identity, one has

$$q_{11} = \frac{1}{2} + \frac{1}{2} \cos \left( \frac{\pi}{2} - \cos^{-1} Q \right) = \frac{1}{2} \left( 1 + \sin \cos^{-1} Q \right),$$

(19)
or
\[ q_{11} = \frac{1}{2} \left[ 1 + (1 - Q^2)^{1/2} \right]. \]  
(20)

Analogously, one obtains
\[ q_{12} = \frac{1}{2} \left[ 1 - (1 - Q^2)^{1/2} \right], \]  
(21)
\[ q_{21} = \frac{1}{2} \left[ 1 - (1 - Q^2)^{1/2} \right], \]  
(22)
\[ q_{22} = \frac{1}{2} \left[ 1 + (1 - Q^2)^{1/2} \right]. \]  
(23)

Next substituting Eq.(9) in Eq.(2), one has
\[ R_0 = - \log_2 \left[ \left( \frac{1}{2} \right)^2 + \left( \frac{1}{2} \right)^2 \right] = 1. \]  
(24)

Also, according to Eq.(3), one has
\[ R_1 = - \log_2 \left[ q_{21}^2 + q_{22}^2 \right], \]  
(25)
and substituting Eqs.(20) and (22) in Eq.(25), one obtains
\[ R_1 = - \log_2 \left( 1 - \frac{1}{2} Q^2 \right). \]  
(26)

Analogously,
\[ R_2 = - \log_2 \left[ q_{12}^2 + q_{22}^2 \right], \]  
(27)
or
\[ R_2 = - \log_2 \left( 1 - \frac{1}{2} Q^2 \right). \]  
(28)

Next substituting Eqs.(15), (16), (24), (26), and (28) in Eq.(1), one obtains
\[ I^R = \frac{1}{2} \left[ 1 + \log_2 \left( 1 - \frac{1}{2} Q^2 \right) \right] + \frac{1}{2} \left[ 1 + \log_2 \left( 1 - \frac{1}{2} Q^2 \right) \right], \]  
(29)
or
\[ I^R = 1 + \log_2 \left( 1 - \frac{1}{2} Q^2 \right) = \log_2 \left[ 2 \left( 1 - \frac{1}{2} Q^2 \right) \right], \]  
(30)
or equivalently [3],
\[ I^R = \log_2 \left( 2 - Q^2 \right). \]  
(31)

It is evident from Eq.(31) that to maximize the Renyi information gain $I^R$, one can equivalently minimize $Q$, the overlap of correlated probe states. This is consistent with Eq.(12) and the fact that the more nearly orthogonal two states are, the easier they are to distinguish.
3. Maximum Renyi information gain

Because the signal states $|u\rangle$, $|\tilde{u}\rangle$, $|v\rangle$, and $|\tilde{v}\rangle$ in the two-dimensional real Hilbert space of the signal can be expanded in terms of the signal basis states, namely,

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

$$|\tilde{u}\rangle = -\sin \frac{\pi}{8} |e_0\rangle + \cos \frac{\pi}{8} |e_1\rangle,$$

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

$$|\tilde{v}\rangle = \cos \frac{\pi}{8} |e_0\rangle - \sin \frac{\pi}{8} |e_1\rangle,$$

then by the linearity of quantum mechanics, the action of the probe on the signal states is fully described by the general unitary transformation $U$, representing the probe, acting on the signal basis states $|e_0\rangle$ and $|e_1\rangle$, which is given by [3, 8]

$$|e_m \otimes w\rangle \rightarrow U |e_m \otimes w\rangle = |e_0\rangle |\Phi_{0m}\rangle + |e_1\rangle |\Phi_{1m}\rangle,$$

where $|w\rangle$ is the initial state of the probe, and the $|\Phi_{nm}\rangle$ are the transformed states of the probe (unnormalized and not orthogonal) and are functions of parameters $\{\lambda, \mu, \theta, \phi\}$,

$$|\Phi_{nm}\rangle = |\Phi_{nm}(\lambda, \mu, \theta, \phi)\rangle.$$

In general, $0 \leq (\lambda, \mu, \theta, \phi) \leq 2\pi$. Unitarity and symmetry arguments determine the probe states $|\Phi_{nm}\rangle$ to be given by [3, 8]

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

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

$$|\Phi_{10}\rangle = X_0 |w_1\rangle + X_2 |w_2\rangle,$$

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

where

$$X_0 = \sin \lambda \cos \mu,$$

$$X_1 = \cos \lambda \cos \theta \cos \phi,$$

$$X_2 = \cos \lambda \cos \theta \sin \phi,$$

$$X_3 = \sin \lambda \sin \mu,$$

$$X_5 = \cos \lambda \sin \theta \cos \phi,$$

$$X_6 = -\cos \lambda \sin \theta \sin \phi.$$

The two states $|\psi_1\rangle$ and $|\psi_2\rangle$ which must be distinguished by the probe, for the basis $\{|u\rangle, |\tilde{u}\rangle\}$, are

$$|\psi_1\rangle = |\psi_{uu}\rangle,$$

$$|\psi_2\rangle = |\psi_{\tilde{u}\tilde{u}}\rangle,$$

where $|\psi_{uu}\rangle$ is the projected state of the probe when state $|u\rangle$ is transmitted by the transmitter and also received by the legitimate receiver, namely,

$$|\psi_{uu}\rangle = \langle u | U | u \otimes w\rangle.$$
and analogously,
\[ |\psi_{\tilde{u}\tilde{a}}\rangle = \langle \tilde{u}|U|\tilde{u} \otimes w \rangle. \]  
(51)

Substituting Eqs.(48)-(51) in Eq.(12), then
\[ Q = \frac{\langle \psi_{uu}|\psi_{\tilde{u}\tilde{a}}\rangle}{|\psi_{uu}|^2|\psi_{\tilde{u}\tilde{a}}|^2}. \]  
(52)

By the symmetry of the BB84 protocol, the value of \( Q \) given by Eq.(52) also holds in the \{\ket{v}, \ket{\tilde{v}}\} basis. Expanding the signal states in terms of the signal basis states, and using Eqs.(50)-(52), (36), (38)-(47), it can be shown that \[ Q = \frac{1}{2} \left( d + a \right) + b \left\{ \left[ 1 + \frac{1}{2} (d + a) \right]^2 - \frac{1}{2} c^2 \right\}^{1/2}, \]  
(53)
where
\[ a = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \cos 2\phi \sin 2\phi, \]  
(54)
\[ b = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \sin 2\phi, \]  
(55)
\[ c = \cos^2 \lambda \sin 2\theta \cos 2\phi, \]  
(56)
\[ d = \sin^2 \lambda + \cos^2 \lambda \cos 2\theta. \]  
(57)

What is needed is the maximum Renyi information (or minimum \( Q \) in Eq.(31)) for any error rate \( E \) chosen by the eavesdropper and induced in the legitimate receiver. Evidently the error rate induced by the probe is \[ E = \frac{P_{u\tilde{u}} + P_{\tilde{u}u}}{P_{u\tilde{a}} + P_{\tilde{u}u} + P_{uu} + P_{\tilde{u}\tilde{a}}}, \]  
(58)
where \( P_{ij} \) is the probability that if a photon in polarization state \( \ket{i} \) is transmitted by the transmitter in the presence of the disturbing probe, the polarization state \( \ket{j} \) is detected by the legitimate receiver. Again by the symmetry of the protocol, the value of \( E \) given by Eq.(58) also holds in the \{\ket{v}, \ket{\tilde{v}}\} basis. One has
\[ P_{ij} = |\psi_{ij}|^2, \]  
(59)
where \( |\psi_{ij}\rangle \) is the projected state of the probe when polarization state \( \ket{i} \) is transmitted, and polarization state \( \ket{j} \) is detected by the legitimate receiver in the presence of the probe. The states \( |\psi_{uu}\rangle \) and \( |\psi_{\tilde{u}\tilde{a}}\rangle \) are given by Eqs.(50) and (51). Analogously one has
\[ |\psi_{uu}\rangle = \langle u|U|u \otimes w \rangle, \]  
(60)
and
\[ |\psi_{\tilde{u}\tilde{a}}\rangle = \langle \tilde{u}|U|\tilde{u} \otimes w \rangle. \]  
(61)
Using Eqs.(59)-(61), (32)-(35), (38)-(47), (54) and (57) in Eq.(58), it can be shown that the induced error rate is given by \[ E = \frac{1}{2} \left[ 1 - \frac{1}{2} (d + a) \right]. \]  
(62)
Next substituting Eq.(62) in Eq.(53), one obtains
\[ Q = \frac{1 - 2E + b}{\left(2 - 2E\right)^2 - \frac{1}{2}c^2}^{1/2}. \]  

(63)

The optimization then becomes that of finding the probe parameters \( \{\lambda, \mu, \theta, \phi\} \) such that \( Q \) in Eq.(63) is minimum for fixed \( E \). (An appropriate error rate \( E \) is chosen by the eavesdropper.) The complete optimization was performed in [4, 6, 7]. To accomplish this, the critical points of \( Q \) were found by analytically determining the values of \( \lambda, \mu, \theta, \phi \) such that for fixed \( E \),
\[ \frac{\partial Q}{\partial \lambda}|_E = \frac{\partial Q}{\partial \mu}|_E = \frac{\partial Q}{\partial \theta}|_E = \frac{\partial Q}{\partial \phi}|_E = 0, \]
and then distinguishing maxima, saddle points, and minima by numerically calculating \( Q \) in the neighborhood of the critical points. Three sets of optimum probe parameters were found, each yielding the identical minimum \( Q \) and maximum Renyi information gain for set error rate \( E \).

The three sets of optimum probe parameters are [4, 6, 7]

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

(65)

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

(66)

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

(67)

The minimum \( Q \) for each of the three sets, Eqs.(65)-(67), is the same, namely, [3, 4]
\[ Q_{\min} = \frac{1 - 3E}{1 - E}, \]  

(68)

and finally substituting Eq.(68) in Eq.(31), the maximum Renyi information gain by the probe is
\[ I_{opt}^{R} = \log_2 \left[2 - \left(\frac{1 - 3E}{1 - E}\right)^2\right]. \]

(69)

Here \( 0 \leq E \leq 1/3 \), since according to Eq.(69), \( E = 1/3 \) corresponds to perfect information. The maximum Renyi gain by the probe is of course sensitive to any variations from the ideal BB84 QKD protocol. For example, sensitivity to deviations from \( \pi/4 \) of the angle between the nonorthogonal signal states was calculated in [4–7].

4. Implementations

Corresponding to each set of optimum probe parameters, \( S^{(1)}, S^{(2)}, \) and \( S^{(3)} \) in Eqs.(65)-(67) is an optimum unitary transformation \( U^{(1)}, U^{(2)}, \) and \( U^{(3)} \), respectively, obtained by evaluating the transformations, Eq.(36), for the optimum values of the probe parameters, Eqs.(65)-(67), respectively [16–20]. Corresponding to the set \( S^{(1)}, \) Eq.(65), is the unitary transformation \( U^{(1)} \) that produces the following optimal entanglements [17, 18]:
\[ |u\rangle \otimes |w\rangle \rightarrow \frac{1}{4} (|u\rangle \otimes |\alpha_+\rangle + |\bar{u}\rangle \otimes |\alpha\rangle), \]

(70)

\[ |\bar{u}\rangle \otimes |w\rangle \rightarrow \frac{1}{4} (|u\rangle \otimes |\alpha\rangle + |\bar{u}\rangle \otimes |\alpha_-\rangle), \]

(71)

\[ |v\rangle \otimes |w\rangle \rightarrow \frac{1}{4} (|v\rangle \otimes |\alpha_-\rangle - |\bar{v}\rangle \otimes |\alpha\rangle), \]

(72)
have been obtained for two different optimal entangling probes for attacking the BB84 QKD expressed in terms of orthonormal probe basis vectors
in which the probe states
in which the probe states
the same optimal entanglement Eqs.(70)-(78) [20]. The set

\begin{align}
|\alpha_+\rangle &= \left(2^{1/2} + 1\right) (1 + \eta)^{1/2} + \text{sgn}(1 - 4E) \left(2^{1/2} - 1\right) (1 - \eta)^{1/2} |w_0\rangle \\
&+ \left[ \text{sgn}(1 - 4E) \left(2^{1/2} + 1\right) (1 - \eta)^{1/2} + \left(2^{1/2} - 1\right) (1 + \eta)^{1/2} \right] |w_3\rangle,
\end{align}

respectively, expressed in terms of probe orthonormal basis states $|w_0\rangle$ and $|w_3\rangle$, and also the set error rate $E$ induced by the probe, where for $0 \leq E \leq 1/3$,

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

Also in Eqs.(74)-(76),

$$
\text{sgn}(x) \equiv \begin{cases} 
1, & x > 0 \\
0, & x = 0 \\
-1, & x < 0 
\end{cases} .
$$

The set $S^{(2)}$, Eq.(66), for $\sin 2\mu = 0$, $\sin 2\phi = 1 - 4E$, and $e^x e^y = 1$ yields $U^{(2)} = U^{(1)}$, and again the same optimal entanglement Eqs.(70)-(78) [20].

The set $S^{(3)}$, Eq.(67), for $\sin \mu = \cos \mu = 2^{1/2}$ and $\cos \theta = 1$, produces the following optimal entanglements [19]

\begin{align}
|u\rangle \otimes |w\rangle &\longrightarrow \frac{1}{4} \left(|u\rangle \otimes |\sigma_+\rangle + |\tilde{u}\rangle \otimes |\sigma_-\rangle\right), \\
|\tilde{u}\rangle \otimes |w\rangle &\longrightarrow \frac{1}{4} \left(|u\rangle \otimes |\sigma\rangle + |\tilde{u}\rangle \otimes |\sigma_-\rangle\right), \\
|v\rangle \otimes |w\rangle &\longrightarrow \frac{1}{4} \left(|v\rangle \otimes |\sigma_-\rangle - |\tilde{v}\rangle \otimes |\sigma\rangle\right), \\
|\tilde{v}\rangle \otimes |w\rangle &\longrightarrow \frac{1}{4} \left(-|v\rangle \otimes |\sigma\rangle + |\tilde{v}\rangle \otimes |\sigma_+\rangle\right),
\end{align}

in which the probe states $|\sigma_+\rangle$, $|\sigma_-\rangle$, and $|\sigma\rangle$, for $0 \leq E \leq 1/3$, are given by

\begin{align}
|\sigma_+\rangle &= 4\left((1 - 2E)^{1/2} |w_a\rangle - E^{1/2} |w_b\rangle\right), \\
|\sigma_-\rangle &= 4\left((1 - 2E)^{1/2} |w_a\rangle + E^{1/2} |w_b\rangle\right), \\
|\sigma\rangle &= -|\bar{\delta}\rangle = 4E^{1/2} |w_b\rangle,
\end{align}

equipped in terms of orthonormal probe basis vectors $|w_a\rangle$ and $|w_b\rangle$.

Based on the transformations, Eqs.(70)-(73) and (79)-(82), quantum circuits and designs have been obtained for two different optimal entangling probes for attacking the BB84 QKD.
protocol and yielding maximum Renyi information to the probe. Probe photon polarization states become optimally entangled with the signal states on their way between the legitimate transmitter and receiver. The quantum circuit for both probes consists of a single CNOT gate in which the control qubit is a photon polarization basis state of the signal, and the target qubit is a photon polarization basis state of the probe. The target state of the probe is set by the error rate. In the design implementation for $U^{(1)}$ and $U^{(2)}$, the target state is given by [18]

$$|A_2\rangle = \text{sgn}(1 - 4E)\left[\frac{1}{2}(1 - \eta)\right]^{1/2}|w_0\rangle + \left[\frac{1}{2}(1 + \eta)\right]^{1/2}|w_3\rangle,$$

in which the probe orthonormal basis states $|w_0\rangle$ and $|w_3\rangle$ also serve as the basis states for the projective measurement of the probe. In the design implementation for $U^{(3)}$, the target state is simply given by

$$|\tilde{A}_2\rangle = (1 - 2E)^{1/2}|w_a\rangle + (2E)^{1/2}|w_b\rangle,$$

and the basis states $|w_+\rangle$ and $|w_-\rangle$ for the projective measurement of the probe are in this case given by

$$|w_{\pm}\rangle = 2^{-1/2}(|w_a\rangle \pm |w_b\rangle).$$

Standard von-Neumann projective measurements of the probe yield maximum information on the pre-privacy amplified key, once basis information becomes available during reconciliation. (It is important to realize that for such correlated states, consistent with the relativity of simultaneity, it is irrelevant whether a measurement is made first by the probe or by the legitimate receiver.)

5. Conclusion
For optimum entangling probes attacking the BB84 protocol of quantum key distribution, the maximum Renyi information gain by the probe has been reviewed and is given by Eq.(69), expressed in terms of the error rate induced by the probe in the legitimate receiver. Optimum entanglements produced by such probes are given by Eqs.(70)-(73), or alternatively by Eqs.(79)-(82). Designs for such probes have been given recently in which the optimum entanglements are in each case produced by a single CNOT gate.

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

References
[1] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum Cryptography,” Rev. Mod. Phys. 74, 145-195 (2002).
[3] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, “Security of quantum cryptography against individual attacks,” Phys. Rev. A 57, 2383-2398 (1998).
[4] H. E. Brandt, “Probe Optimization in four-state protocol of quantum cryptography,” Phys. Rev. A 66, 032303 (16), (2002).
[5] H. E. Brandt, “Secrecy Optimization in the four-state protocol of quantum key distribution,” in J. Math. Phys. 43, 4526-4530 (2002).
[6] H. E. Brandt, “Optimization problem in quantum cryptography,” J. Optics B 5, S557-560 (2003).
[7] H. E. Brandt, "Optimum probe parameters for entangling probe in quantum key distribution," Quantum Information Processing 2, 37-79 (2003).
[8] C. A. Fuchs and A. Peres, "Quantum-state disturbance versus information gain: uncertainty relations for quantum information," Phys. Rev. A 53, 2038–2045 (1996).
[9] I. Csizsar and J. Koerner, Information Theory: Coding Theorems and Discrete Memoryless Systems, Academic Press, New York (1981).
[10] A. Renyi, "On measures of entropy and information," in Proc. 4th Berkeley Symp. on Mathematical Statistics and Probability, Vol. 1, 1961, pp. 547-561.
[11] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inform. Theory 41, 1915-1923 (1995).
[12] C. H. Bennett, F. Besette, G. Brassard, L. Savail, and J. Smolin, "Experimental Quantum Cryptography," J. Cryptology 5, 3 (1992).
[13] B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and S. Fainman, "Defense frontier analysis of quantum cryptographic systems," Appl. Optics 37, 2869-2878 (1998).
[14] C. W. Helstrom, Quantum Detection and Estimation Theory (Academic Press, New York, 1976).
[15] L. B. Levitan in Quantum Communication and Measurement, edited by V. P. Belovkin, O. Hirota, and R. L. Hudson (Plenum, New York, 1995), pp. 439-448.
[16] H. E. Brandt, "Quantum cryptographic entangling probe," Phys. Rev. A 71, 042312 (14), (2005).
[17] H. E. Brandt, "Design for a quantum cryptographic entangling probe," J. Modern Optics 52, 2177-2185 (2005).
[18] H. E. Brandt and J. M. Myers, "Expanded quantum cryptographic entangling probe," quant-ph/0510089, to appear in J. Mod. Optics (2006).
[19] H. E. Brandt, "Alternative design for quantum cryptographic entangling probe," J. Modern Optics 53, 1041 (2006).
[20] H. E. Brandt, "Entangled eavesdropping in quantum key distribution," preprint (2006).