RAPID COMMUNICATIONS

PHYSICAL REVIEW A VOLUME 48, NUMBER 1 JULY 1993

Information-theoretic limits to quantum cryptography

Stephen M. Barnett
Department of Physics and Applied Physics, John Anderson Building, University of Strathclyde, Glasgow G4 0NG, United Kingdom

Simon J. D. Phoenix
BT Laboratories, Martlesham Heath, Ipswich IP5 7RE, United Kingdom

(Received 13 October 1992)

We develop an information-theoretic formalism to describe a quantum-cryptographically protected communication channel. We thereby establish the fundamental limits on the security of the channel. This formalism enables us to propose protocols that allow detection of an eavesdropper by examination of data that would normally be discarded.

PACS number(s): 03.65.Bz, 42.50.Wm, 89.70.+c

Quantum cryptography is the name given to a technique of distributing a sequence of random bits to two or more parties in such a way that can guarantee security against an unauthorized eavesdropping attempt. The legitimate users of the channel then possess a shared, and *secret,* random sequence of bits. This shared, secret information can then be used as a key for cryptographic purposes. The aim of an eavesdropper is to obtain as much of the secret key as possible without being detected. Quantum cryptography frustrates both of these ambitions. Three ingenious schemes that fulfill this function have so far been proposed. The first, by Bennett *et al.* [1], relies on the uncertainty principle of quantum mechanics to provide key security. This particular scheme has been demonstrated experimentally [2]. A further elegant technique has been proposed by Ekert [3], which relies on the violation of the Bell inequalities to provide the key security. An experimental realization of this scheme has also been proposed [4]. The security of this latter scheme has been shown to be equivalent to that of the first [5], although the Ekert scheme gives the additional feature of secure key *storage.* The third technique, devised by Bennett [6], is based on the transmission of nonorthogonal quantum states. Communication using quantum states allows many novel and fundamental techniques to be exploited [7]. These techniques cannot be envisaged within the framework of classical physics. It is clear that quantum cryptography represents a radical new departure both in physics and cryptology.

Broadly speaking, quantum-cryptographic key-distribution techniques can be classified in the following way: they are the exploitation of a physical phenomenon through a data-handling protocol to provide security against eavesdroppers. Thus there are two crucial elements: the physical effect (for example, the uncertainty principle or the violation of the Bell theorem) and the protocol designed to exploit this effect to yield a guaranteed security. The Bennett-Brassard protocol (BB, for short) is fundamentally different from the Ekert protocol in that the BB protocol discards approximately $\frac{1}{2}$ of the collected data before any test for the eavesdropper is made. The BB protocol sacrifices some of the potentially useful key data to detect the presence of the eavesdropper. The Ekert protocol splits the data into two groups and performs the eavesdropper detection test on one group and then, if eavesdropper-free, uses the other group of data as the key. One of the purposes of this paper is to describe a method whereby the BB cryptographic scheme can be adapted so that none of the potentially useful data is lost; the eavesdropper detection test is performed only on "rejected" data, data that would not be used as key data and would, under the original BB protocol, be discarded or rejected.

One of the problems with the proposed quantum-cryptography schemes is that it is not easy to see where the limits of the techniques lie. We present in this paper an information-theoretic formulation of the quantum communication channel that allows a natural description of the fundamental limits to quantum cryptography. It is interesting to note that this formalism has to be developed still further if it is to be applied to a quantum-correlated channel [8]. In such cases the information only "comes into being" after the users of the channel make an *a posteriori* agreement on their measurements [3]. The information is *stored* in a nonlocal fashion in such channels; that is, it has no aspect of local reality, even though the information flow between the users of the channel does not violate causality [8]. We shall present, in this paper, the application of information theory to channels designed to exploit the BB protocol. We find that an eavesdropper can both destroy *and create* information on the quantum channel. It is this creation of information by the eavesdropper that allows the development of a rejected-data protocol.

Let us consider two legitimate users of a quantum channel and a third, unauthorized, user with access to that quantum channel. We follow the established convention and call the legitimate users "Alice" and "Bob" and the eavesdropper we shall call "Eve." The various possible communication pathways between these users of the channel are depicted schematically in Fig. 1. Alice will send a sequence of quantum states $|\{\alpha_j\}\rangle$, which form the symbols of an alphabet. These states will be assumed to be the eigenstates of a Hermitian operator $\hat{A}$. Bob will attempt to measure the symbols $|\{\beta_k\}\rangle$ of some alphabet consisting of the operator $\hat{B}$, which is not neces-

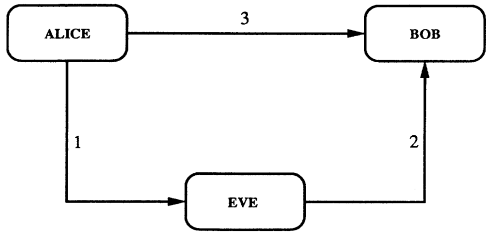


FIG. 1. Schematic representation of the communication pathways between Alice, Bob, and Eve.

sarily the same as the operator used by Alice. Eve will attempt to eavesdrop in yet another basis $|\{\epsilon_m\}\rangle$, which is the eigenbasis of an operator $\hat{E}$, which is not necessarily the same as that used by Alice or Bob. She will then faithfully retransmit the eigenstate she has measured on to Bob. We shall make the simplifying, but not restrictive, assumption that each of the alphabets used consists of N symbols. For a classical channel with finite alphabets of dimension N the channel capacity of $\ln N$ is reached when an equal *a priori* choice of input symbols is made. We shall also adopt this input coding for the quantum channel.

Suppose now that Alice and Bob attempt to communicate along pathway 3 of Fig. 1; that is, in the absence of the eavesdropper. The channel transition probability, that is, the probability that Bob receives the symbol $|\beta_k\rangle$ given that $|\alpha_j\rangle$ was sent is just the square modulus of the overlap integral $|\langle\alpha_j|\beta_k\rangle|^2$. The system mutual information, which measures the correlation between the input and output symbols and therefore defines the information flow rate between Alice and Bob, is given by

$$J_3(\hat{A},\hat{B})=\ln N+\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}|\langle\alpha_j|\beta_k\rangle|^2\ln|\langle\alpha_j|\beta_k\rangle|^2 . \tag{1}$$

This quantity varies between 0 and $\ln N$. The channel capacity is achieved when Alice and Bob use the same alphabets. When Alice and Bob use conjugate alphabets so that $|\langle\alpha_j|\beta_k\rangle|^2=1/N$ and each input symbol is equally likely to cause any output symbol, we have $J_3(\hat{A},\hat{B})=0$. Suppose now, however, that Alice and Bob attempt to communicate along pathways 1 and 2 (in Fig. 1) via Eve. The presence of Eve unavoidably affects the channel, and the channel transition probability, which we label as Γ_{jk}, is given by

$$\Gamma_{jk}=\sum_{m=1}^{N}|\langle\alpha_j|\epsilon_m\rangle|^2|\langle\epsilon_m|\beta_k\rangle|^2 . \tag{2}$$

The system mutual information in the presence of Eve is now given by

$$J_{12}(\hat{A},\hat{B})=\ln N+\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N}\Gamma_{jk}\ln\Gamma_{jk} . \tag{3}$$

We introduce a parameter ξ defined by

$$\xi=\frac{J_{12}(\hat{A},\hat{B})-J_3(\hat{A},\hat{B})}{J_3^{\max}(\hat{A},\hat{B})} , \tag{4}$$

where $J_3^{\max}$ defines the maximum possible information flow between Alice and Bob given their initial choice of input symbols and alphabets, and in the above case is just the channel capacity $\ln N$. This new parameter measures the degree of disturbance introduced by the eavesdropper on the channel, and we find that $-1\leq\xi\leq 1$. A negative value implies that the eavesdropper has caused a reduction in the flow of information between Alice and Bob. In the BB protocol it is this reduction of information flow that is responsible for the ability to detect the presence of Eve; the BB protocol operates in the regime of negative ξ. A positive value of ξ implies that the presence of Eve causes an *increase* in the flow of information. As we shall demonstrate below this is a new operating regime for this quantum cryptography scheme and the increased information flow will betray the presence of an eavesdropper. Only if $\xi=0$ for all possible choices of alphabet by Alice and Bob can Eve escape detection [9]. This is possible if Eve always uses the same alphabet as Alice and/or Bob, and this can be made extremely difficult if Alice and Bob choose randomly between their alphabets. This random choice of transmission and reception alphabets is crucial to the success of the quantum cryptography scheme. Eve can also ensure that $\xi=0$ when Alice and Bob use conjugate alphabets and Eve chooses an alphabet conjugate to *both* of these. However, she remains vulnerable to detection with this strategy whenever Alice and Bob choose the *same* alphabet. Furthermore, by measuring in an alphabet conjugate to both Alice and Bob's in this fashion, Eve will gain *precisely zero information* about the key that is eventually established between Alice and Bob.

As a particular example we shall choose a communication channel based on an alphabet size $N=2$ (that is, equivalent to a spin system or the polarization basis of the BB protocol). Alice and Bob use alphabets generated by the spin-z and spin-x operators labeled as $\hat{\sigma}_z$ and $\hat{\sigma}_x$. The spin-up states $|+\rangle_z$ and $|+\rangle_x$ will represent the logical symbol 1 and the spin-down states $|-\rangle_z$ and $|-\rangle_x$ will represent the logical symbol 0. We shall assume that Eve tries to measure some intermediate spin operator, say $\hat{\sigma}_\theta$, and faithfully retransmits the results in this basis on to Bob. The advantages of using some intermediate basis in the standard BB protocol have been explained elsewhere [1,2,10]. The transmission and reception probabilities are shown in the table of Fig. 2. Let us follow through a particular sequence by way of example. Alice sends the state $|+\rangle_z$ and the expansion of this state in Eve's basis is

$$|+\rangle_z=\cos(\theta/2)|+\rangle_\theta-\sin(\theta/2)|-\rangle_\theta . \tag{5}$$

Therefore, Eve will read the symbol 1 with probability $\cos^2\theta/2$ and the symbol 0 with probability $\sin^2\theta/2$. We shall suppose that Eve, in fact, reads the symbol 1 and therefore transmits the state $|+\rangle_\theta$ on to Bob, whom we assume to measure $\hat{\sigma}_x$. The expansion of this state in Bob's basis is

$$\begin{aligned}|+\rangle_\theta=&\frac{1}{\sqrt{2}}(\cos\theta/2+\sin\theta/2)|+\rangle_x\\&+\frac{1}{\sqrt{2}}(\sin\theta/2-\cos\theta/2)|-\rangle_x ,\end{aligned} \tag{6}$$

so that Bob reads the symbol 1 with probability $\frac{1}{2}|\cos\theta/2+\sin\theta/2|^2$ and the symbol 0 with probability $\frac{1}{2}|\cos\theta/2-\sin\theta/2|^2$. From the table of Fig. 2 we see that the probability that Alice and Bob disagree, *if they choose different alphabets,* is given by

$$q=\tfrac{1}{2}-\tfrac{1}{4}\sin 2\theta \ . \tag{7}$$

Thus if Alice and Bob compare M bits of data for which they have measured different alphabets they find that the number of disagreements is substantially changed when an eavesdropper is present. We denote the probability of k disagreements by $P(k)$ and use the subscript exp to denote the *expected* distribution in the absence of the eavesdropper. The probability of k disagreements between Alice and Bob is given by the kth term in the binomial expansion

$$P(k)=\frac{M!}{k!(M-k)!}q^k(1-q)^{M-k} \ . \tag{8}$$

The expected distribution can be obtained from (8) by setting $\theta=0$ so that $q=\frac{1}{2}$.

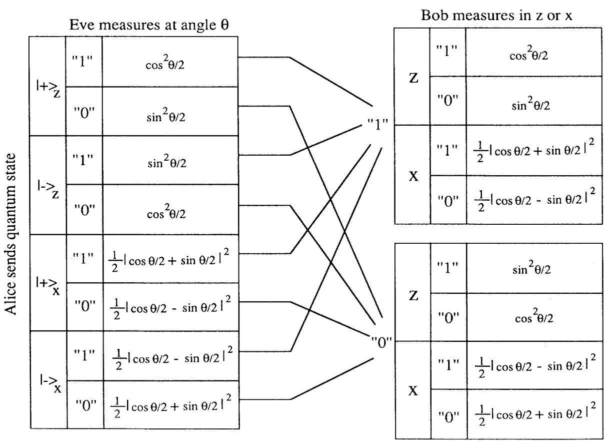
For large M this distribution can be approximated by a Gaussian function, so that we find

$$\begin{aligned} P(k)&\approx\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left[-\frac{1}{2\sigma^2}\left[k-\frac{M}{4}[2-\sin 2\theta]\right]^2\right] ,\\ P_{\exp}(k)&\approx\sqrt{2/M\pi}\exp\left[-\frac{2}{M}(k-M/2)^2\right] , \end{aligned} \tag{9}$$

where we have written the width of the Gaussian function σ as

$$\sigma^2=\frac{M}{4}(1-\tfrac{1}{4}\sin^2 2\theta) \ . \tag{10}$$

Alice and Bob now set some threshold $k_{\text{th}}<\bar{k}_{\exp}$, the average expected number of disagreements. The threshold is set below this mean value because Eve's intervention always causes the number of disagreements to fall.



Alice sends quantum state	Eve measures at angle θ	
$\|+>_z$	"1"	$\cos^2\theta/2$
	"0"	$\sin^2\theta/2$
$\|->_z$	"1"	$\sin^2\theta/2$
	"0"	$\cos^2\theta/2$
$\|+>_x$	"1"	$\frac{1}{2}\|\cos\theta/2+\sin\theta/2\|^2$
	"0"	$\frac{1}{2}\|\cos\theta/2-\sin\theta/2\|^2$
$\|->_x$	"1"	$\frac{1}{2}\|\cos\theta/2-\sin\theta/2\|^2$
	"0"	$\frac{1}{2}\|\cos\theta/2+\sin\theta/2\|^2$

Bob measures in z or x		
z	"1"	$\cos^2\theta/2$
	"0"	$\sin^2\theta/2$
x	"1"	$\frac{1}{2}\|\cos\theta/2+\sin\theta/2\|^2$
	"0"	$\frac{1}{2}\|\cos\theta/2-\sin\theta/2\|^2$
z	"1"	$\sin^2\theta/2$
	"0"	$\cos^2\theta/2$
x	"1"	$\frac{1}{2}\|\cos\theta/2-\sin\theta/2\|^2$
	"0"	$\frac{1}{2}\|\cos\theta/2+\sin\theta/2\|^2$

FIG. 2. Probability table for Alice and Bob's possible transmissions and receptions if they use the spin-z and spin-x alphabets and Eve measures and retransmits in some intermediate alphabet at an angle θ.

The probability that Eve causes fewer than k_{th} errors to occur between Alice and Bob is simply given by

$$\begin{aligned} P(\text{Eve}<k_{\text{th}})&=\int_0^{k_{\text{th}}}P(k)dk\\ &\approx\frac{1}{2}\left[1+\text{erf}\left[\frac{4k_{\text{th}}-M}{\sqrt{6M}}\right]\right] , \end{aligned} \tag{11}$$

and the probability that the expected distribution gives rise to fewer than this number is

$$\begin{aligned} P(\exp<k_{\text{th}})&=1-\int_0^{M-k_{\text{th}}}P_{\exp}(k)dk\\ &\approx\tfrac{1}{2}\,\text{erfc}\left[\frac{M-2k_{\text{th}}}{\sqrt{2M}}\right] , \end{aligned} \tag{12}$$

where the error function and complementary error function are defined in the usual way [11]. These probabilities are plotted in Figs. 3–5, where the thresholds have been set at $k_{\text{th}}=3M/8$, $k_{\text{th}}=5M/16$, and $k_{\text{th}}=7M/16$, respectively, and Eve is assumed to have made an attack in the Breidbart basis [1,10] at $\theta=\pi/4$. Curve (*a*) in each of these figures is the probability that Eve triggers the alarm, and curve (*b*) is the probability of a false alarm from the expected distribution. The threshold in Fig. 3 has been set midway between the mean values of the expected and actual distributions. At $M=24$, Eve is 92% likely to trigger the alarm if the midpoint threshold is used, 76% likely if the lower threshold is used, and 98% likely if the upper threshold is used. Conversely, the alarm is 11% likely to have been triggered by the expected distribution for the midpoint threshold, 3% likely for the lower threshold, and 27% likely for the upper threshold. These statistics improve considerably as M increases, so that for the midpoint threshold and the number of compared bits M set at 75 we have that Eve is 99.4% likely to trigger the alarm and a false alarm is only 1.5% likely. The users of the channel must set their required confidence level by an adjustment of M and k_{th}.

Clearly the sensible course of action is for Alice and Bob to first examine their normally rejected data to determine whether an eavesdropping attempt has been made in an intermediate basis. The standard BB check can then be used to test for an attack in the spin-z or spin-x

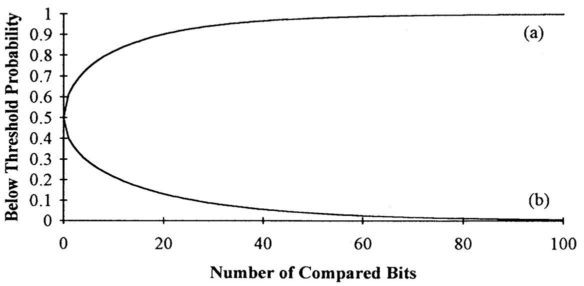


FIG. 3. Plots of (*a*) the probability that Eve, eavesdropping in the Breidbart basis at $\theta=\pi/4$, causes fewer than k_{th} errors to occur between Alice and Bob, and (*b*) the probability that fewer than k_{th} errors arise from the expected distribution. Both curves are plotted against the number of compared bits M, and the threshold is set at the midpoint $k_{\text{th}}=3M/8$.

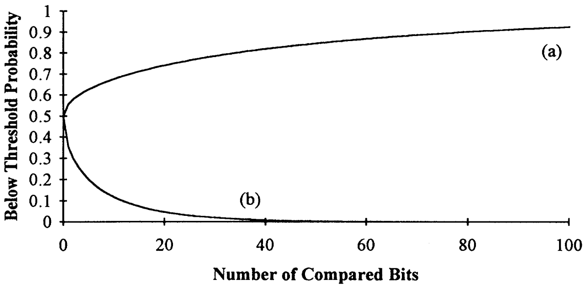


FIG. 4. Same as Fig. 3 but with a lower threshold set at $k_{\text{th}}=5M/16$.

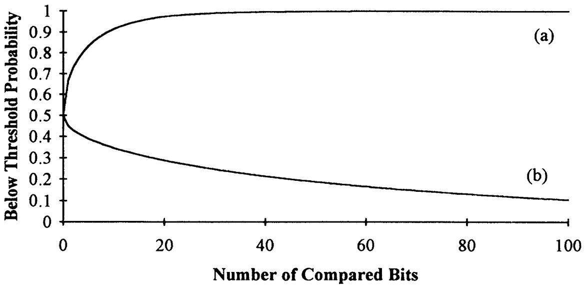


FIG. 5. Same as Fig. 3 but with a raised threshold set at $k_{\text{th}}=7M/16$.

alphabets. However, Alice and Bob can apply a different method to avoid sacrificing any of their key data. Alice now chooses *three* alphabets, the spin-x, spin-z, and spin-$\pi/4$. Bob still measures only in the spin-z and spin-x alphabets. Alice and Bob will use the same alphabets $\frac{1}{3}$ of the time, on average. Alice and Bob now select those data for which Alice used spin-x or spin-z and Bob measured in a *different* alphabet. This allows the statistical test for an interception in an alphabet intermediate to the z or x alphabets. Again approximately $\frac{1}{3}$ of the data is used, on average, for this purpose. If no eavesdropper is detected at this stage a further check is carried out on the data for which Alice used the spin-$\pi/4$ alphabet. This determines whether an eavesdropping attempt has been made in either the spin-z or spin-x alphabets. Approximately $\frac{1}{3}$ of the data is used for this purpose. The remaining $\frac{1}{3}$, on average, can now be used as the key if the statistical tests have shown there to be no eavesdropper. Using this new technique Alice and Bob can establish a key without sacrificing any of their key data, although this is at a cost of having to transmit more data overall. Furthermore, Alice and Bob can make a reasonable guess as to the alphabet Eve was trying to measure. The eavesdropper cannot only be detected but information about her strategy can be obtained.

As a final point we note that Eve is free to choose more complicated strategies than the simple intercept-resend strategy presented here. Eve must be extremely careful that her strategy optimizes both her chances of avoiding detection *and* her information about the key. She could, for example, choose to measure and transmit in a random basis in order to minimize the probability that she will be detected. By adopting such a strategy, however, she radically reduces the information she can gain about the key. She may also choose to measure in an intermediate basis and retransmit in a random basis. This strategy, while undermining a rejected data protocol, increases the likelihood of Eve being detected under the original protocol. These and other possible strategies of Eve are discussed in more detail elsewhere [12,13]. It seems that Eve's strategies to optimize success under a rejected-data protocol compromise her effectiveness under the original protocol and vice versa.

S.M.B. would like to thank the Royal Society of Edinburgh for financial support. We would also like to thank Professor A. J. Leggett and Professor R. Loudon for helpful comments.

[1] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, in *Advances in Cryptology: Proceedings of Crypto '82,* edited by D. Chaum, R. L. Rivest and A. T. Sherman (Plenum, New York, 1983).

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] A. K. Ekert, J. G. Rarity, P. R. Tapster, and G. M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[5] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[7] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[8] S. M. Barnett, D. T. Pegg, and S. J. D. Phoenix (unpublished).

[9] K. J. Blow and S. J. D. Phoenix, J. Mod. Opt. **40**, 33 (1993).

[10] S. J. D. Phoenix, Phys. Rev. A, this issue, **48**, 100 (1993) (to be published).

[11] *Handbook of Mathematical Functions,* edited by M. Abramowitz and I. A. Stegun (Dover, New York, 1972), p. 297.

[12] B. Huttner and A. K. Ekert, J. Mod. Opt. (to be published).

[13] S. M. Barnett, B. Huttner, and S. J. D. Phoenix (unpublished).