Quantum cryptography without conjugate coding

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

(Received 16 July 1992)

We extend the quantum key distribution method of Bennett and Brassard [IBM Tech. Discl. Bull. **28**, 3153 (1985)] by exploiting a nonconjugate coding scheme. Using this scheme we are able to show that the original method of Bennett and Brassard gives optimal security.

PACS number(s): 03.65.Bz, 42.79.−e, 89.70.+c

I. INTRODUCTION

One of the most intriguing and exciting recent developments in quantum mechanics has been the prediction and demonstration of a cryptographic key distribution scheme, the security of which is guaranteed by the laws of physics, or, rather, the laws of quantum mechanics [1–3]. The security of these schemes is dependent on the uncertainty principle at a single-particle level. In an ingenious extension to these ideas, Ekert has shown how a quantum-correlated communication channel can be exploited to provide both secure key distribution and secure key storage [4]. The degree of security for the key distribution has been shown to be equivalent for both the Bennett-Brassard and Ekert schemes [5]. What has not, to my knowledge, been demonstrated is that the use of the conjugate coding technique of Wiesner [6] affords *optimal* security for the distribution of the key. One of the aims of the present work is to show that this is indeed the case.

We shall begin by defining the basic notions of quantum alphabets and channels. We shall introduce a measure of conjugacy for alphabets based on the information rate of a quantum channel [7] and relate this to the ability to distribute the key in a secure fashion. By considering an appropriate generalization of the Bennett-Brassard scheme [1,3] to nonconjugate coding we shall show that conjugate coding does indeed provide optimal security. We shall consider only those schemes for which the alphabet symbols are orthogonal although the alphabets are not mutually conjugate. A cryptography scheme can be developed [8] for which the alphabet symbols are not orthogonal, but the alphabets themselves are conjugate. This latter scheme is related to the recent work of Bennett [9]. We shall also discuss briefly ways in which the effectiveness of the Breidbart basis for eavesdropping [1] can be reduced.

II. QUANTUM ALPHABETS

A quantum communication channel is one for which the channel transition probabilities are, in the absence of noise, solely governed by the rules of quantum mechanics. The channel is represented by a set of Hermitian operators which describe the physical properties of the channel. Simple examples of quantum channels are the free-space transmission of single particles such as electrons or photons. What makes these channels truly quantum mechanical is the possibility that the transmission and reception may occur using different alphabets and that the transition probabilities for these alphabets are *entirely determined by the laws of quantum mechanics.* It is the features that quantum mechanics introduces which make such channels particularly interesting. We can think of the Hermitian operators which describe the channel as being the generators of a set of eigenstates which can be used as the symbols of an alphabet. The alphabets need not necessarily contain *all* the eigenstates of a particular operator as its symbols, nor, indeed, do they need to contain symbols generated by only one operator. However, as we shall see, the effectiveness of the alphabet is reduced unless *all* the symbols associated with a *unique* operator are employed.

In order to make some of these notions more precise, we shall concentrate on a communication channel between two legitimate users who we shall call "Alice" and "Bob." Alice will transmit messages to Bob using a particular alphabet and Bob will attempt to read the message in his own alphabet. The mutual dependence of the transmitted and received alphabets determines the information transmission rate of the channel. Initially we shall suppose that both Alice and Bob are using alphabets generated from a complete set of eigenstates of the Hermitian operators $\hat{A}$ and $\hat{B}$, respectively. The eigenvalue relations for these operators are

$$\hat{A}|\alpha_j\rangle=\alpha_j|\alpha_j\rangle \ , \quad \hat{B}|\beta_k\rangle=\beta_k|\beta_k\rangle \tag{2.1}$$

so that we adopt the terminology that Alice uses the alphabet $\{|\alpha\rangle\}$ sourced by the operator $\hat{A}$ with a similar terminology employed for Bob. We shall make the simplifying, but not restrictive, assumption that the alphabets used by Alice and Bob each have N symbols. This situation is shown schematically in Fig. 1. In general, $\hat{A}$ and $\hat{B}$ are different operators so that Alice and Bob transmit and receive in different alphabets. The channel transition probabilities, in the absence of noise, are determined by the expansion coefficients of the symbols of one alphabet in terms of the other. Thus for the channel that we have just described we find that the probability that Bob receives the symbol $|\beta_k\rangle$ *given* that Alice transmitted the symbol $|\alpha_j\rangle$ is just

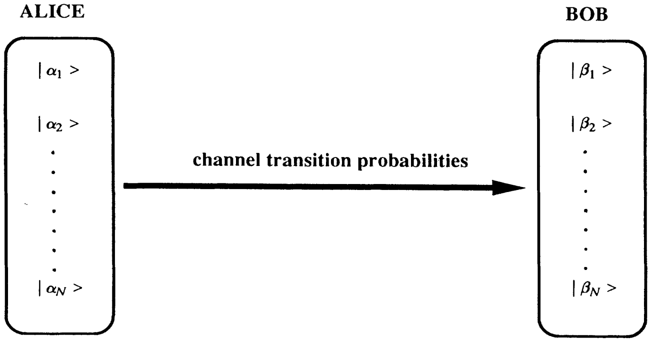

FIG. 1. Schematic illustration of a quantum communication channel in which Alice transmits data using a quantum alphabet $|\{\alpha\}\rangle$ and Bob receives using the quantum alphabet $|\{\beta\}\rangle$. Alice and Bob's alphabets need not necessarily be the same.

$$P(\beta_k|\alpha_j)=|\langle\alpha_j|\beta_k\rangle|^2 , \tag{2.2}$$

where we have employed an obvious, albeit not strictly rigorous, notation. If we now assume that Alice chooses the symbols of her alphabet with equal *a priori* probabilities so that

$$P(\alpha_j)=\frac{1}{N} , \tag{2.3}$$

then the system mutual information, denoted by $J(\hat{A},\hat{B})$, is just given by [7]

$$J(\hat{A},\hat{B})=\ln N+\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N}|\langle\alpha_j|\beta_k\rangle|^2\ln|\langle\alpha_j|\beta_k\rangle|^2 . \tag{2.4}$$

This quantity is just the mutual information per transmitted and received symbol averaged over both the input and output alphabets. Maximizing $J(\hat{A},\hat{B})$ over the input alphabet gives the channel capacity, which in this case is just $\ln N$. It should be noted that this is also the channel capacity for a perfect classical channel with finite input and output alphabets of equal size.

We now introduce an information-theoretic definition of operator conjugacy. Two operators $\hat{A}$ and $\hat{B}$ are said to be conjugate if their system mutual information is precisely zero. From (2.4) this implies that each input symbol is equally likely to cause any output symbol and we have

$$|\langle\alpha_j|\beta_k\rangle|^2=\frac{1}{N} . \tag{2.5}$$

We have arrived at Wiesner's definition of conjugate variables [6] from the perspective of information theory. This tells us that Alice and Bob can exchange no information on their channel if the alphabets they use are sourced by conjugate operators. In such cases we shall simply describe the alphabets as being conjugate to one another. The difference between the mutual information when both Alice and Bob use the same alphabets and the mutual information when different alphabets are used is the amount of information *lost* when different transmission and reception alphabets are employed. For the simple example we have discussed above, this average lost information is given by

$$\ln N-J(\hat{A},\hat{B})=-\frac{1}{N}\sum_{j=1}^{N}\sum_{k=1}^{N}|\langle\alpha_j|\beta_k\rangle|^2\ln|\langle\alpha_j|\beta_k\rangle|^2 . \tag{2.6}$$

Thus N bits of information (in suitable units) are lost if the communication channel is sourced at input and output by conjugate operators. We can define a dimensionless quantity Q which gives the fraction of information lost by measurement of different alphabets at the input and output of the channel by writing

$$Q=1-\frac{J(\hat{A},\hat{B})}{J(\hat{A},\hat{A})}=1-\frac{J(\hat{A},\hat{B})}{J(\hat{B},\hat{B})} . \tag{2.7}$$

Q varies between 0 and 1 and is zero only when the same alphabets are measured at the input and output, that is, no information is lost. If the input and output alphabets are conjugate, then $Q=1$ and *all* of the information is lost. We can express this in another way. Let us suppose that Alice transmits the symbol $|\alpha_j\rangle$ and that Bob measures the conjugate operator $\hat{B}$. After the measurement, Bob *cannot* reconstruct the information about $\hat{A}$ contained in the original state. It is this irreversible loss of information about the conjugate variable upon measurement which enables the quantum key distribution scheme to work.

Suppose now that Alice and Bob are to try and use their conjugate alphabets to distribute a key for use in a cryptographic application. The protocol can be summarized as follows. Alice and Bob decide to use alphabets sourced by the operators $\hat{A}$ and $\hat{B}$. Alice and Bob are free to choose which of these alphabets to use. They map each of the conjugate alphabets onto a new alphabet of N symbols $1,2,\ldots,N$ so that if Alice transmits $|\alpha_j\rangle$ and Bob measures $\hat{A}$ then Bob reads the symbol "j"; if Alice transmits $|\beta_j\rangle$, which is also equivalent to the symbol j, then Bob has to measure $\hat{B}$ in order to be certain of reading the symbol j from Alice's transmission. Alice and Bob transmit and receive, respectively, by randomly choosing between the two alphabets. Alice and Bob will now have a string of symbols such as $1,3,16,N-4,25,7,N-12,\ldots,$ which will almost certainly disagree. Alice chooses a small subset of these data and asks Bob to discard all of those symbols for which a different choice of alphabet was made. Alice and Bob should now have a set of symbols which are in perfect agreement (in the absence of noise). Any attempt at eavesdropping will disturb this perfect agreement. This comes about because an eavesdropper, Eve, also needs to make a choice between the alphabets. There will be some symbols for which Alice and Eve have used conjugate alphabets, but for which Alice and Bob have used the same alphabet. Eve's intervention will randomize the information encoded in the correct alphabet and so lead to the possibility that Alice and Bob will obtain a different result even though they have used the same alphabet. Alice and Bob will be able to determine whether or not an attempt at interception has been made.

Let us formalize the above discussion. Suppose that Alice transmits the symbol j as the state $|\alpha_j\rangle$. In the absence of any interception, Alice and Bob will only agree to use this information *if and only if* both Alice and Bob use the same alphabets. In this case, for example, Bob will have chosen to orient his detection apparatus to measure the operator $\hat{A}$ and will, with unit probability, have measured the symbol j. The situation is different in the presence of an eavesdropper. Suppose that the eavesdropper, Eve, chooses to measure $\hat{A}$. In this case Eve will read the symbol j with unit probability. Shen then transmits the state $|\alpha_j\rangle$ to Bob who can decide to measure either of the conjugate alphabets. It is important to keep in mind the fact that Alice and Bob will simply discard those results for which different choices of input and output alphabets were used. If Eve chooses to measure $\hat{B}$ then she will read the symbol j with probability $1/N$. Eve has no sensible option other than to retransmit faithfully to Bob the state she thinks she has observed. This is because Eve has no way of knowing whether her choice of measurement was, in fact, correct. Eve then, after measurement of $\hat{B}$, will retransmit some state $|\beta_k\rangle$. Upon reception of this state, Bob, choosing to make a measurement of $\hat{A}$, will read the symbol j with probability $1/N$. Alice and Bob upon subsequent communication will find, with probability $(N-1)/N$, that they do not agree about this result. Clearly, for a perfect channel in the absence of eavesdropping Alice and Bob *must* agree about every result for which they make the same choice of alphabets. Overall then, per transmission, the probability that Eve will escape detection is given by

$$P_{\mathrm{esc}}=\frac{1}{2}\left[1+\frac{1}{N}\right] . \tag{2.8}$$

If Alice and Bob compare M results then the probability that Eve will escape detection is just $(P_{\mathrm{esc}})^M$. If N, the alphabet size, is quite large then Eve's chances of escaping detection are approximately 2^{-M}, which rapidly becomes negligible as M is increased. Current experimental and theoretical key distribution schemes use an alphabet size of $N=2$ [1,4,10]. In the next sections we shall restrict ourselves to this dimensionality, noting, however, that the dimensionality of the alphabet space can be increased.

III. KEY DISTRIBUTION WITHOUT CONJUGATE CODING

The essential ingredient of a conjugate coding scheme is that measurement of the incorrect variable will give precisely no information about its conjugate. However, one can envisage situations in which a measurement of the incorrect variable will give *partial* information about the other, correct, variable. We show in this section that a secure key distribution scheme can still be implemented in this case although a longer subset of data is needed to achieve a given degree of security. We shall consider an alphabet size of 2 and shall consider the standard spin variables as the operators which generate our alphabets. We shall consider a spin variable aligned along the z direction and a spin variable aligned at angles θ and ϕ to this. This is shown schematically in Fig. 2. We label the spin operators in these directions by $\hat{\sigma}_z$ and $\hat{\sigma}(\theta,\phi)$. The non-Hermitian spin-flip operators associated with the z direction of spin are labeled by $\hat{\sigma}_{\pm}$. The eigenstates of the spin-z operator can be expanded in terms of the eigenstates of $\hat{\sigma}(\theta,\phi)$ and vice versa so that we have the expansions

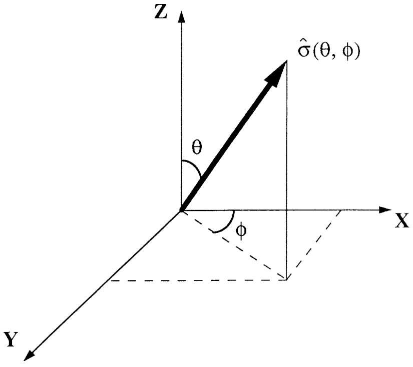

FIG. 2. Geometric representation of the spin variables which are characterized by the angles θ and ϕ.

$$\begin{aligned}|+\rangle_{\theta,\phi}&=\cos(\theta/2)\exp(-i\phi/2)|+\rangle_z\\&\quad+\sin(\theta/2)\exp(i\phi/2)|-\rangle_z ,\\|-\rangle_{\theta,\phi}&=-\sin(\theta/2)(-i\phi/2)|+\rangle_z\\&\quad+\cos(\theta/2)\exp(i\phi/2)|-\rangle_z ,\end{aligned} \tag{3.1}$$

and the complementary expansions

$$\begin{aligned}|+\rangle_z&=\exp(i\phi/2)[\cos(\theta/2)|+\rangle_{\theta,\phi}\\&\quad-\sin(\theta/2)|-\rangle_{\theta,\phi}] ,\\|-\rangle_z&=\exp(-i\phi/2)[\sin(\theta/2)|+\rangle_{\theta,\phi}\\&\quad+\cos(\theta/2)|-\rangle_{\theta,\phi}] .\end{aligned} \tag{3.2}$$

Although it is not necessary to do so at this stage we have retained the phase factors in these expressions as these are important when we consider an attack using the Breidbart basis [1].

Let us suppose that Alice and Bob wish to set up a secure key distribution scheme using the two alphabets generated by these spin operators. The alphabets consist of the z states $\{|\pm\rangle_z\}$ and the θ-states $\{|\pm\rangle_{\theta,\phi}\}$. Alice sends to Bob a random sequence of the symbols "1" and "0" by randomly choosing between the states of these alphabets. Alice and Bob will have previously agreed to read a spin-up result as a logical 1 and a spin-down result as a logical 0. In the *absence* of interception, the probability that Bob will read the symbol that Alice actually sent is just

$$P(\text{Bob correct: no interception})=1-\tfrac{1}{2}\sin^2(\theta/2) . \tag{3.3}$$

After Alice and Bob have discarded those bits for which they used different alphabets this probability rises to unity. Physically there can be no difference between an eavesdropper and the legitimate receiver. Consequently the above probability (3.3) is also the probability that Eve will read the correct symbol. However, *after* interception Eve and Bob are no longer indistinguishable as far as the channel is concerned. This is because Eve has disturbed the information encoded in some of the spins sent by Alice. Eve must retransmit the spin in order to try and fool Alice and Bob and, in this case, the probability per bit that Bob and Alice agree, after discarding the appropriate bits, is no longer unity but is given by

$$P(\text{Bob correct: after Eve's retransmission}) = 1-\tfrac{1}{4}\sin^2\theta \ . \qquad (3.4)$$

This is also clearly equal to the probability, per bit, that Eve escapes detection after an attempt at interception of the key. The key distribution schemes currently in the literature [1,3,4] all employ conjugate coding which for the spin operators discussed above are equivalent to the choice $\theta=\pi/2$. In this case we have that the probability that Eve escapes detection per bit is $\frac{3}{4}$. Suppose now that Alice and Bob need to compare K bits of data for a *conjugate* coding scheme in order to achieve a given degree of certainty that an interception has not taken place. Let M be the number of bits that Alice and Bob have to compare in a *nonconjugate* coding scheme, such as that discussed above, in order to achieve the same degree of certainty as for the conjugate scheme. The ratio of the number of bits M/K is then given by

$$\frac{M}{K}=\frac{\ln(\frac{3}{4})}{\ln[1-\frac{1}{4}\sin^2\theta]} \ . \qquad (3.5)$$

This ratio is plotted in Fig. 3. It should be noted that the penalty for using a nonconjugate scheme does not become prohibitively severe until the angle between the spin operators is about $\pi/3$. The graph demonstrates that secure key distribution is possible for a nonconjugate coding scheme, however the number of bits of data which Alice and Bob need to compare to achieve a given degree of security increases as the degree of conjugacy decreases. The ratio M/K is also equal to the ratio of the information gains per received bit about the eavesdropping attempt for the conjugate and nonconjugate coding schemes.

It is clear from the figure that conjugate alphabets ($\theta=\pi/2$) give the greatest degree of protection against interception for this particular key distribution and this particular eavesdropping attempt. However, there are alternative distribution schemes and different methods of interception. Alice could, for example, use biased statistics in her choice of alphabets, as could Bob. Equally, Eve could use the Breidbart basis which increases her chances of reading the correct bit without compromising her chances of escaping detection [3]. In the following sections we examine these various options open to both the legitimate and illegitimate users of the channel.

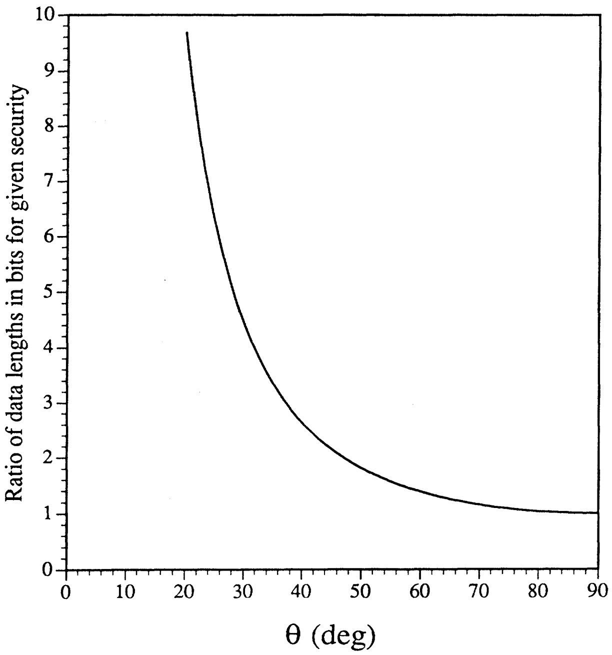

FIG. 3. The ratio of the lengths, in bits, of the data sets for conjugate and nonconjugate coding needed to achieve the same degree of channel security as a function of θ.

IV. THE BREIDBART BASIS AND RANDOM STATISTICS

Eve is clearly not restricted from choosing any particular direction in which to orient her measuring apparatus. It has been shown [3] for the case of unbiased transmission statistics and conjugate alphabets that Eve's optimum strategy is to align her apparatus to measure spin at $\pi/4$ and to retransmit in this basis. Her chances of escaping detection remain at 75% per bit but her chances of reading the bit correctly increase to nearly 85% [3]. This basis is known as the Breidbart basis. We shall continue to use this terminology for the basis which "bisects" the alphabets, even though this may not prove to be the optimum strategy for Eve. What should Eve do to optimize her chances if nonconjugate coding is employed and one of the alphabets is, for example, only chosen 40% of the time, on average? Let us first examine Eve's measurement basis or alphabet. We shall assume that Eve aligns her apparatus at the angles θ' and ϕ' with respect to the z direction of spin (refer to Fig. 2). We shall write $\psi=\phi-\phi'$ to denote the phase difference between Eve's alphabet and the θ alphabet used by Alice and Bob. We should note that Eve merely orients her apparatus to measure the Breidbart alphabet and does not have to make a choice between alphabets. This is slightly different to her strategy if she uses the legitimate alphabets. The expansion equivalent to (3.1) and (3.2) are achieved for Eve's basis by the simple expedient of replacing unprimed quantities with the respective primed versions. The expansions of the θ alphabet in terms of Eve's alphabet, and vice versa, are easy to obtain by a simple substitution procedure and we find, for example, that the spin-up state in the θ alphabet has an expansion in terms of Eve's alphabet given by

$$|+\rangle_{\theta,\phi}=[\cos(\theta/2)\cos(\theta'/2)\exp(-i\psi/2)+\sin(\theta/2)\sin(\theta'/2)\exp(i\psi/2)]|+\rangle_E$$
$$+[\sin(\theta/2)\cos(\theta'/2)\exp(i\psi/2)-\cos(\theta/2)\sin(\theta'/2)\exp(-i\psi/2)]|-\rangle_E\ , \qquad (4.1)$$

with similar expressions for the other expansions. We have used the subscript E to denote the eigenstates which form Eve's alphabet.

We shall assume, for the moment, that Alice makes a completely random choice between her available alphabets so that each alphabet is chosen with a probability of $\frac{1}{2}$. Let us further assume that Alice transmits the state $|+\rangle_{\theta,\phi}$. Eve reads the symbol 1 with a probability given by

$$|\cos(\theta/2)\cos(\theta'/2)\exp(-i\psi/2)$$
$$+\sin(\theta/2)\sin(\theta'/2)\exp(i\psi/2)|^2$$

and retransmits the state $|+\rangle_E$ to Bob. If Bob aligns his apparatus to measure in the θ direction then he reads 1 with this probability also. There are two important probabilities to determine. The first is the probability that Eve reads the correct bit and the second is the probability that Eve escapes detection. The probability that Eve reads the correct bit is determined from the expansion coefficients such as those in (4.1) and, after some trigonometric manipulation, we find that

$$P(\text{Eve correct})=\tfrac{1}{2}+\tfrac{1}{4}(1+\cos\theta)\cos\theta'$$
$$+\tfrac{1}{4}\sin\theta\sin\theta'\cos\psi\ . \qquad (4.2)$$

It is an easy task now to determine which angle Eve should measure to maximize her chances of reading the correct bit. we find that Eve should choose the angle given by

$$\theta'=\tan^{-1}\left[\frac{\sin\theta}{1+\cos\theta}\right]=\theta/2\ . \qquad (4.3)$$

This shows that, when Alice uses unbiased statistics to choose between the alphabets, the Breidbart basis is the basis which gives the maximum chance for the eavesdropper to determine the correct bit. However, this potential advantage is of no use to an eavesdropper if the use of such a basis increases the chances for the legitimate users of the channel to detect her presence. Guided by previous work [1] which examines the situation $\theta=\pi/2$, we should expect that the use of this basis does not confer any disadvantage on the eavesdropper as far as her chances of escaping detection. The probability that Eve escapes detection is the same as the probability that Alice and Bob agree after having rejected those results which were taken for different alphabets. This can also be determined from the eigenstate expansions such as (4.1) and we find that, for unbiased choice of alphabets, the probability that Eve escapes detection is

$$P(\text{Eve escapes detection})=\tfrac{1}{2}(1-\tfrac{1}{2}\sin^2\theta')(2-\tfrac{1}{2}\sin^2\theta)+\tfrac{1}{8}[2\cos^2\psi+1]\sin^2\theta\sin^2\theta'+\tfrac{1}{2}\cos\theta\cos\theta'\sin\theta\sin\theta'\cos\psi\ . \qquad (4.4)$$

This, of course, reduces to the expected value of $\frac{3}{4}$ when $\theta=\theta'=\pi/2$, but, more significantly, it reduces to the value $1-\frac{1}{4}\sin^2\theta$ when $\theta=\theta'$, which is our previous result. The question to be answered is whether Eve benefits from use of the Breidbart basis as far as her chances of escaping detection are concerned. For the Breidbart basis we have Eve's choice $\theta'=\theta/2$ and (4.4) reduces to

$$P(\text{Eve escapes detection: Breidbart})=1-\tfrac{1}{2}\sin^2(\theta/2)\ . \qquad (4.5)$$

These results are plotted in Figs. 4(a) and 4(b) in which we plot the graphs of the relevant probabilities for Eve in the cases when she does and does not use the Breidbart basis. It is clear from these graphs that Eve's chances of escaping detection *increase* if she uses the Breidbart basis when Alice and Bob employ a nonconjugate coding scheme. In fact, differentiation of (4.4) with respect to θ' shows that this quantity is *maximized* at $\theta'=\theta/2$. The Breidbart basis is clearly optimal for Eve. For the special case of conjugate coding, $\theta=\pi/2$, Eve's chances of escaping detection remain unchanged.

So far in this section we have considered only an equal random choice between the alphabets. Let us suppose now that Alice chooses to send the z alphabet with a probability P_z^A and the θ alphabet with probability P_θ^A such that $P_z^A+P_\theta^A=1$. Let us also suppose that Eve is *not* using the Breidbart basis, for the moment. Eve is also free to choose between alphabets and we use the superscript "E" to denote the relative probabilities with which Eve chooses these alphabets. Let us suppose that Alice sends the state $|+\rangle_z$ the probability that Eve reads the correct bit 1 given that Alice transmitted this state is given by

$$P(\text{Eve correct}|\text{ Alice sends}|+\rangle_z)$$
$$=P_z^E+P_\theta^E\cos^2(\theta/2)\ . \qquad (4.6)$$

Working out these probabilities for all possible transmitted states and combining them gives the probability that Eve reads the correct bit for *any* transmitted state as

$$P(\text{Eve correct})$$
$$=1-[P_\theta^A+P_\theta^E-2P_\theta^AP_\theta^E]\sin^2(\theta/2)\ . \qquad (4.7)$$

A similar exercise in probability calculus gives the probability that Eve escapes detection as

$$P(\text{Eve escapes detection}) = 1-\tfrac{1}{2}[P_\theta^A+P_\theta^E-2P_\theta^A P_\theta^E]\sin^2\theta \ . \quad (4.8)$$

Both of these expressions reduce to $\frac{3}{4}$ for conjugate alphabets and equal *a priori* choice of alphabets. It should be noted that the term in square brackets is common to both expressions and clearly Eve must minimize this quantity to optimize her chances of successful interception using these alphabets. However, the only parameter which is under the direct control of Eve is the relative probability P_θ^E with which she chooses to measure the alphabets. From (4.7) and (4.8) we see that if Alice, in fact, makes an equal *a priori* choice of alphabets so that $P_\theta^A=\frac{1}{2}$, then Eve's choice of alphabet is irrelevant and she could align her apparatus along a single direction. If, on the other hand, Alice chooses $P_\theta^A>\frac{1}{2}$, then Eve minimizes the quantity in square brackets by choosing $P_\theta^E=1$. Conversely, if Alice chooses to transmit more frequently in the z alphabet, then Eve must orient her apparatus to measure along this direction to optimize her chances. Eve's strategy is based on an all or nothing choice, rather than a precise reflection of Alice's transmission statistics as we might have expected at the outset. Alice's best strategy is to remove any control Eve may have over the channel and the only way she can do this is by resorting to an equal *a priori* choice of alphabets so that $P_\theta^A=\frac{1}{2}$.

As a final illustration of the kind of complexities that can occur, let us now suppose that Alice uses biased transmission statistics and that Eve chooses to measure in a single alphabet characterized, as before, by the angles θ' and ϕ'. We shall, for the moment, set the relative phase $\psi=0$. The probability that Eve reads the correct bit is now given by

$$P(\text{Eve correct})=\tfrac{1}{2}(1+\cos\theta') + \frac{P_\theta^A}{2}(\sin\theta\sin\theta'+\cos\theta'[\cos\theta-1]) \ . \quad (4.9)$$

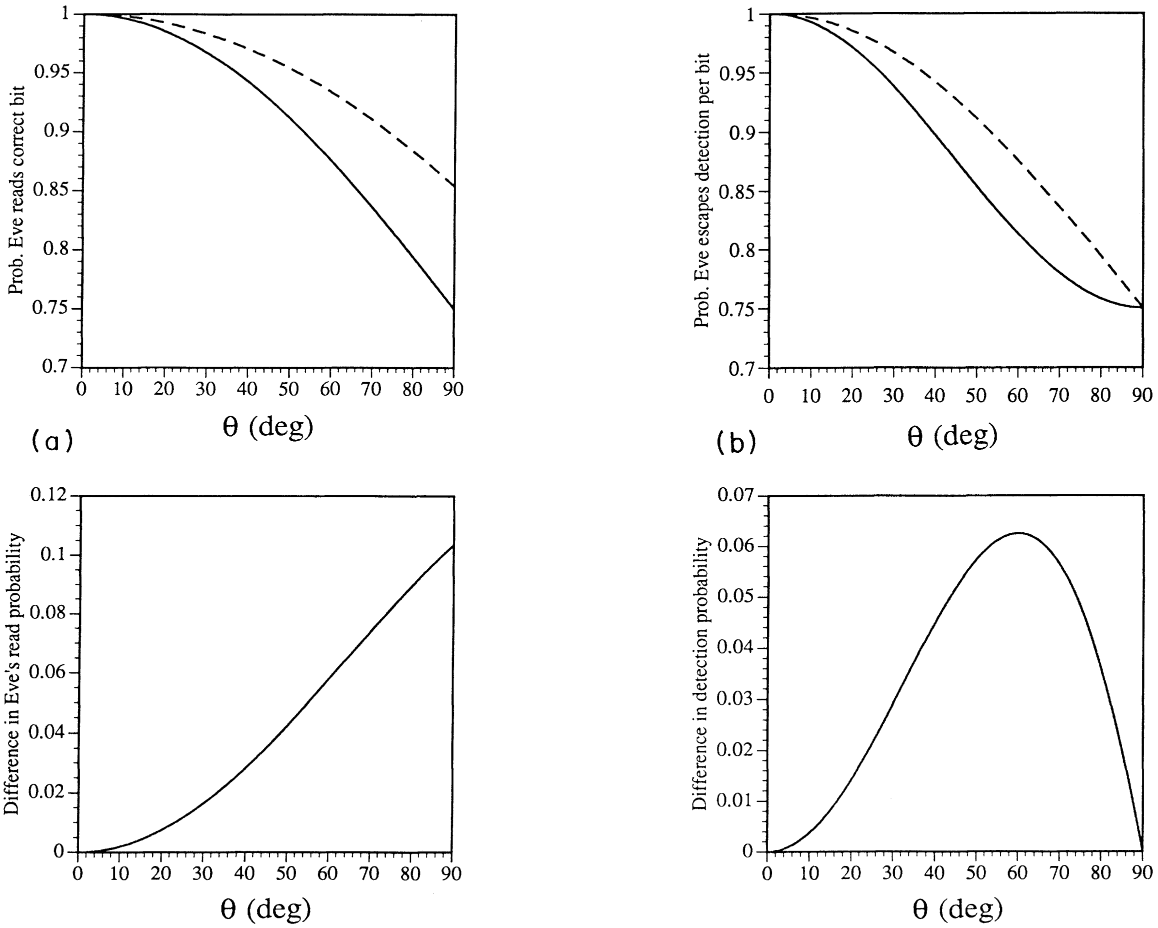

FIG. 4. (a) The probability that Eve reads the correct bit upon interception is plotted as a function of θ. The solid line is for an interception scheme based on the legitimate alphabets, and the dashed line is for an interception using the Breidbart basis. The lower graph gives the difference between these curves as a function of θ. (b) The probability that Eve escapes detection, per bit, as a function of θ. The solid line is for an interception scheme based on the legitimate alphabets, and the dashed line is for an interception using the Breidbart basis. The lower graph gives the difference between these curves as a function of θ.

Maximizing this quantity with respect to θ' shows that the angle Eve must choose is given by

$$\theta'=\tan^{-1}\left[\frac{P_\theta^A\sin\theta}{1-P_\theta^A+P_\theta^A\cos\theta}\right]. \tag{4.10}$$

Only if Alice makes an equal *a priori* choice of alphabet does this angle exactly bisect the alphabets. The effect of Alice's biased transmission statistics is to shift Eve's optimal angle away from the Breidbart angle which bisects the two alphabets. However, the angle given in (4.10) merely maximizes Eve's chances of reading the correct bit if Eve uses some intermediate basis. We also need to determine the probability that Eve remains undetected. This can again be worked out quite simply by following through all the relevant probabilities and for $\psi=0$ we find that the angle Eve must choose to minimize the chance that she will be detected is given by

$$\theta'=\tfrac{1}{2}\tan^{-1}\left[\frac{P_\theta^A\sin2\theta}{1-P_\theta^A+P_\theta^A\cos2\theta}\right], \tag{4.11}$$

which is clearly not equal to the angle (4.10) which optimizes Eve's chances of reading the correct bit. These angles coincide, of course, when Alice chooses each alphabet with equal likelihood.

V. DISCUSSION AND CONCLUSIONS

It is easy to see from an information-theoretic viewpoint exactly why a conjugate coding scheme has to be optimal. It is not so easy to see whether a nonconjugate coding scheme can work when the loss of information on measuring the incorrect basis is only partial. We have demonstrated in this article that a nonconjugate coding scheme can, in fact, give a secure key distribution. In doing so we have established the limits of the technique and have explicitly shown that conjugate coding [1] is indeed the optimal strategy for the legitimate users of the channel. Our analysis has been based on the protocol that Alice and Bob will reject any measurement for which they used different alphabets. This is, in fact, unnecessarily restrictive and Alice and Bob can gain statistical information about the eavesdropper if they are prepared to consider some of their rejected data [11]. This reduces the length of data that Alice and Bob will need to collect in order to perform a reasonable statistical test on their results to check for eavesdropping. The lower bound is given by a conjugate coding scheme and the upper bound is given by the protocol described in this paper.

We have examined the use of the Breidbart basis for the eavesdropper and have shown that it is *more* effective if used when a nonconjugate coding scheme is being employed. Thus not only are the legitimate users handicapped by having to collect more data they are also more vulnerable to attack by an eavesdropper employing the Breidbart basis. There is a way, however, to reduce the effectiveness of the Breidbart basis which will reduce Eve's chances of reading the correct bit at the expense of having to collect more data. The essential thing to notice is that there are three mutually conjugate alphabets for a two-dimensional Hilbert space [6]. Alice and Bob can reduce the effectiveness of the Breidbart basis if Alice uses all three alphabets to transmit data. Eve is at a disadvantage in adopting the Breidbart basis as we can see from (4.2) and (4.4). The important thing to note is that the read and detection probabilities for Eve are influenced by the relative phase ψ. Eve cannot but help in disturbing the measurement statistics when using the Breidbart basis when $\psi=\pi/2$. Unfortunately the use of a third alphabet which is essentially performing no useful function other than to give statistical information about an eavesdropper requires the collection of more data by Alice and Bob and the use of a slightly different protocol [12]. The benefit accrued is small compared to the extra complexity. It should also be noted that even though the use of the Breidbart basis for a conjugate coding scheme can give about 85% chance per bit for an eavesdropper to determine the correct key this statistical information can be reduced by a privacy amplification technique [13]. Furthermore, with a 75% per bit of remaining undetected Eve's chances of escaping detection for a reasonable data set are effectively negligible.

ACKNOWLEDGMENTS

I would like to thank G. McLaren of the Secure Systems section at BT Labs for many helpful discussions and ideas throughout this work. I would also like to thank S. M. Barnett and K. J. Blow for their suggestions.

[1] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, *Advances in Cryptology: Proceedings of Crypto '82* (Plenum, New York, 1983).

[2] C. H. Bennett and G. Brassard, IBM Tech. Discl. Bull. **28**, 3153 (1985).

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

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

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

[6] S. Wiesner, SIGACT News **15**, 78 (1983).

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

[8] S. J. D. Phoenix (unpublished).

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

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

[11] S. M. Barnett and S. J. D. Phoenix, this issue, Phys. Rev. A (to be published); K. J. Blow and S. J. D. Phoenix, J. Mod. Opt. **40**, 33 (1993).

[12] This protocol and another more sophisticated protocol involving four conjugate alphabets, will be discussed elsewhere.

[13] C. H. Bennett, G. Brassard, and J-M. Robert, SIAM J. Comput. **17**, 210 (1988).