

Quantum Cryptography with 3-State Systems

Helle Bechmann-Pasquinucci¹ and Asher Peres²

¹*Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland*

²*Department of Physics, Technion-Israel Institute of Technology, 32000 Haifa, Israel*

(Received 24 January 2000)

We consider quantum cryptographic schemes where the carriers of information are 3-state particles. One protocol uses four mutually unbiased bases and appears to provide better security than obtainable with 2-state carriers. Another possible method allows quantum states to belong to more than one basis. Security is not better, but many curious features arise.

PACS numbers: 03.67.Dd, 03.65.Bz

When Samuel Morse invented the telegraph, he devised for it an alphabet consisting of three symbols: dash, dot, and space. More modern communication methods use binary signals, conventionally called 0 and 1. Information theory, whose initial goal was to improve communication efficiency, naturally introduced binary digits (bits) as its accounting units. However, the theory can easily be reformulated in terms of ternary digits (trits) 0, 1, 2, or larger sets of symbols [1]. For example, instead of bytes (sets of 8 bits) representing 256 ordinary characters, we would have “trytes” (5 trits) for 243 characters. An ordinary text would thus be encoded into a string of trits. If we wish to encrypt the latter, this can be done by adding to it (modulo 3) a *random* string, called *key*, known only to legitimate users. Decrypting is then performed by subtracting that key (modulo 3).

The aim of quantum cryptography [2] is to generate a secret key by using quantum carriers for the initial communication between distant parties (conventionally called Alice and Bob). The simplest methods use 2-state systems, such as polarized photons. Orthogonal states represent bit values 0 and 1. One may use either two [2] or three [3,4] orthogonal bases, chosen in such a way that any basis vectors $|e_j\rangle$ and $|e_\mu\rangle$ belonging to different bases satisfy $|\langle e_j, e_\mu \rangle|^2 = 1/2$. Such bases are called *mutually unbiased* [5,6]. As a consequence, if an eavesdropper (Eve) uses the wrong basis, she gets no information at all and causes maximal disturbance (error rate 1/2) to the transmission, thereby revealing her presence.

In this Letter, we consider 3-state systems as the quantum carriers for cryptographic key distribution. For example, one may use “biphotons” [7], namely, photon pairs in symmetric Fock states $|0, 2\rangle$, $|2, 0\rangle$, and $|1, 1\rangle$. Biphotons can easily be produced with present technology, and detecting arbitrary linear combinations of them will probably be possible soon. (Another possibility would be to use four states of a pair of photons [8], but here we consider only 3-state systems.)

Following the method of Refs. [3,4], we introduce four mutually unbiased bases. Let $|\alpha\rangle$, $|\beta\rangle$, and $|\gamma\rangle$ be the unit vectors of one of the bases. Another basis is obtained by a discrete Fourier transform,

$$\begin{aligned} |\alpha'\rangle &= (|\alpha\rangle + |\beta\rangle + |\gamma\rangle)/\sqrt{3}, \\ |\beta'\rangle &= (|\alpha\rangle + e^{2\pi i/3}|\beta\rangle + e^{-2\pi i/3}|\gamma\rangle)/\sqrt{3}, \\ |\gamma'\rangle &= (|\alpha\rangle + e^{-2\pi i/3}|\beta\rangle + e^{2\pi i/3}|\gamma\rangle)/\sqrt{3}. \end{aligned} \quad (1)$$

The two other bases can be taken as

$$(e^{2\pi i/3}|\alpha\rangle + |\beta\rangle + |\gamma\rangle)/\sqrt{3} \text{ and cyclic perm}, \quad (2)$$

and

$$(e^{-2\pi i/3}|\alpha\rangle + |\beta\rangle + |\gamma\rangle)/\sqrt{3} \text{ and cyclic perm}. \quad (3)$$

Any basis vectors $|e_j\rangle$ and $|e_\mu\rangle$ belonging to different bases now satisfy $|\langle e_j, e_\mu \rangle|^2 = 1/3$.

The protocol for establishing a secret key is the usual one. Alice randomly chooses one of the 12 vectors and sends to Bob a signal whose quantum state is represented by that vector. Bob randomly chooses one of the four bases and “measures” the signal (that is, Bob tests whether the signal is one of the basis vectors). Having done that, Bob publicly reveals which basis he chose, but not the result he obtained. Alice then reveals whether her vector belongs to that basis. If it does, Alice and Bob share the knowledge of one trit. If it does not, that transmission was useless. This procedure is repeated until Alice and Bob have obtained a long enough key. They will then have to sacrifice some of the trits for error correction and privacy amplification [9] (we shall not discuss these points, which are the same as in all cryptographic protocols, except that we have to use trits instead of bits, and therefore parity checks become triality checks, that is, sums modulo 3).

Consider the simplest eavesdropping strategy: Eve intercepts a particle, measures it, and resends to Bob the state that she found. In 3/4 of the cases, she uses a wrong basis, gets no information, and causes maximal disturbance to the transmission: Bob’s error rate (that is, the probability of a wrong identification of the trit value) is 2/3. On the average, over all transmissions, Eve gets $I_E = 1/4$ of a trit and Bob’s error rate is $E_B = 1/2$. (It is natural to measure Eve’s information in trits, since Bob gets one trit for each successful transmission.) These results may be compared

to those obtained by using 2-state systems. With only two bases as in Ref. [2] and with the same simple eavesdropping strategy, Eve learns on the average $1/2$ of a bit for each transmitted bit, and Bob's error rate is $1/4$. If we use three bases as in [3,4], these numbers become $1/3$. Thus, with the present method, Eve learns a smaller fraction of the information and causes a larger disturbance. It is likely that this is also true in the presence of more sophisticated eavesdropping strategies, such as using an ancilla to gently probe the transmission without completely disrupting it. When people seek Eve's "optimal" eavesdropping strategy [10], their criterion usually is the maximal value of I_E/E_B .

Do the above results mean that using 3-state systems improves cryptographic security? This is a very difficult problem and we shall not attempt its complete analysis here. In the simplest scenario, if Alice and Bob only wish to be warned that an eavesdropper is active, then obviously the highest possible ratio E_B/I_E is desirable. (This assumes that they know which eavesdropping methods are available to Eve, so that they can estimate I_E . Here, we shall consider only intercept-and-resend attacks on individual particles, and most statements below are valid only for that case.) Anyway, even if Alice and Bob detect no error, they can never be sure that no information at all was leaked to Eve and some kind of privacy amplification [9] is needed to achieve security. It is known [11,12] that, in the asymptotic limit, secure key distribution can in principle be achieved against single particle attacks if Bob's mutual information with Alice, I_B , is larger than Eve's I_E . This requires only one-way communication between Alice and Bob. With two-way communication, a more advanced method called *advantage distillation* [13] can sometimes produce a secure key even if Eve's information is initially larger. However, a rigorous proof exists only for binary quantum channels, and there are indications that the method may fail for ternary channels [14]. In this Letter, we shall only require $I_B > I_E$.

Note that even if Bob and Eve have the same error rate, as in one of the above examples, $I_E > I_B$. The reason is that Eve knows whether Alice and Bob used the same basis, and therefore which ones of her data are correct and which ones are worthless. On the other hand, Bob can only compare with Alice a subset of data, so as to measure his mean error rate E_B , and from the latter deduce the Shannon entropy of his string. For 2-state systems, assuming all bit values equally probable, he obtains

$$I_B = 1 + (1 - E_B) \log_2(1 - E_B) + E_B \log_2 E_B, \quad (4)$$

and likewise for 3-state systems,

$$I_B = 1 + (1 - E_B) \log_3(1 - E_B) + E_B \log_3(E_B/2). \quad (5)$$

Numerical results, in bits and trits, respectively, will be given in Table II at the end of this Letter, together with

TABLE I. Components of 21 unnormalized vectors. The symbols $\bar{1}$ and $\bar{2}$ stand for -1 and -2 , respectively. Orthogonal vectors have different colors.

Green	001	101	$0\bar{1}1$	$1\bar{1}1$	$1\bar{1}2$	112	$2\bar{1}1$
Red	100	110	$10\bar{1}$	$11\bar{1}$	$21\bar{1}$	211	$12\bar{1}$
Blue	010	011	$\bar{1}10$	$\bar{1}11$	$\bar{1}21$	121	$\bar{1}\bar{1}2$

those for two other cryptographic protocols, discussed below.

New types of cryptographic protocols may indeed be devised if the Hilbert space has more than two dimensions. The reason is that a basis vector may now belong to several bases. In that case, it is natural to assume that each vector represents a definite trit (0, 1, or 2), which is the same in all the bases to which that vector belongs [15]. An example is given in the above table, where vectors are labeled green, red, and blue, for later convenience.

Although this new algorithm is not likely to improve transmission security (as shown below), it has many fascinating aspects and leads to new insights into quantum information theory. The 12 vectors in the first four columns of Table I are shown in Fig. 1, as dots on the faces of a cube, in a way similar to the graphical representation of a Kochen-Specker uncolorable set [16]. In the present case, the tricolor analog of the Kochen-Specker theorem requires only 13 rays for its proof, because ray (111) is orthogonal to all the rays in the third column, which have three different colors. These 12 vectors form 13 bases, but only four bases are complete. The nine other bases have only two vectors each and have to be completed by nine new vectors, listed in the last three columns of the table. To display these nine vectors on Fig. 1, their integer components should be divided by 2. The corresponding dots are then located at the centers of various squares on the faces of the cube.

The cryptographic protocol is the same as before, but now Alice has 21 vectors to choose from, and Bob has a choice of 13 bases. The essential difference is that these

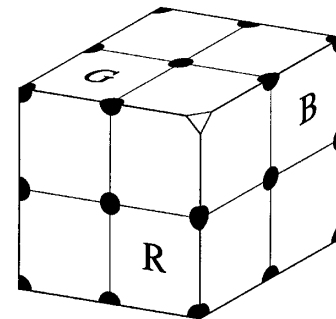


FIG. 1. Twelve vectors are obtained by connecting the center of the cube to the various dots on its faces (diametrically opposite dots represent the same vector). The four dots at the vertices of the squares labeled G, R, and B, are green, red, and blue, respectively. The truncated vertex corresponds to the uncolorable ray (111).

TABLE II. Result of IRE on various cryptographic protocols: Eve's information, Bob's information and error rate for a single IRE event, and the fraction of eavesdropped transmissions needed to make both informations equal to each other.

Units	Bases	Vectors	I_E	I_B	E_B	x
Bits	2	4	0.500 000	0.188 722	0.250 000	0.682 14
Bits	3	6	0.333 333	0.081 710	0.333 333	0.681 28
Trits	4	12	0.250 000	0.053 605	0.500 000	0.717 70
Trits	13	12	0.575 142	0.143 418	0.391 738	0.510 07
Trits	13	21	0.442 765	0.150 431	0.385 022	0.689 94

bases are not mutually unbiased, so that if Eve chooses a different basis (which happens 12/13 of the time), she still gets *at least* probabilistic information on Alice's vector. It may also happen that Eve's basis is different from Bob's, but both bases contain the vector found by Eve. In that case, when Bob announces his basis and Alice confirms it, Eve can infer that she got the correct state and caused no error.

Let us analyze what happens for each successful transmission, that is, when Alice's vector $|e_j\rangle$ is one of those in the basis announced by Bob. Suppose that in her eavesdropping attempt, Eve obtains a state $|e_\mu\rangle$. This happens with probability $P_{\mu j} = |\langle e_j, e_\mu \rangle|^2$. This is also the probability that Bob gets the correct $|e_j\rangle$ when Eve resends to him $|e_\mu\rangle$. On the average over all of Alice's $|e_j\rangle$ and all of Eve's choices of a basis, the probability that Bob gets a correct result is

$$C = \sum_{j=1}^{21} \sum_{\mu=1}^{21} M_\mu (P_{\mu j})^2 / (21 \times 13), \quad (6)$$

where M_μ is the number of bases to which $|e_\mu\rangle$ belongs (namely, $M_\mu = 2$ for the vectors in the first and third columns of Table I, $M_\mu = 3$ for those of the second and fourth columns, and $M_\mu = 1$ for the rest). Bob's mean error probability is $E_B = 1 - C = 0.385 022$.

To evaluate Eve's gain of information I_E , we note that when Alice confirms the basis chosen by Bob, Eve is left with a choice of three vectors having equal prior probabilities, $p_j = 1/3$. The initial Shannon entropy is $H_i = 1$ trit, and the prior probability for Eve's result μ is

$$q_\mu = \sum_{j=0}^2 P_{\mu j} p_j = 1/3. \quad (7)$$

It then follows from Bayes's theorem that the likelihood (posterior probability) of signal j is (see Ref. [16], p. 282)

$$Q_{j\mu} = P_{\mu j} p_j / q_\mu = P_{\mu j}. \quad (8)$$

The new Shannon entropy, following result μ , is

$$H_f = - \sum_{j=0}^2 Q_{j\mu} \log_3 Q_{j\mu}. \quad (9)$$

Eve's information gain is obtained by averaging H_f over all results μ , all Eve's bases, and all Bob's bases. The final result is

$$I_E = H_i - \langle H_f \rangle, \quad (10)$$

$$= 1 + \sum_{j=1}^{21} \sum_{\mu=1}^{21} M_j M_\mu P_{\mu j} \log_3 P_{\mu j} / (3 \times 13^2). \quad (11)$$

Table II lists the relevant data for intercept-and-resend eavesdropping (IRE) on all the above cryptographic protocols.

We also investigated the possibility that Alice uses only the 12 vectors in the first four columns of Table I (those represented by the dots in Fig. 1). The IRE results are also listed in Table II. However, it is interesting that in this

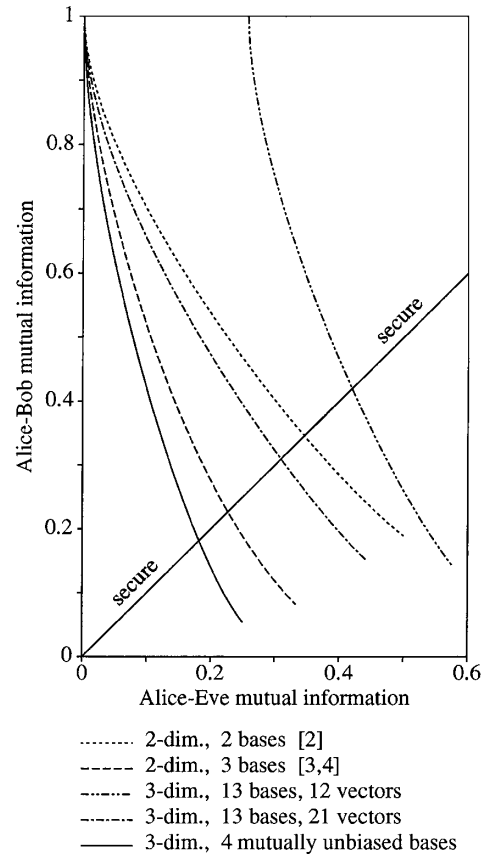


FIG. 2. Mutual informations for the various protocols listed in Table II, when the fraction of intercepted particles is $0 < x < 1$. For the case of 13 bases and 12 vectors, it is assumed that in the remaining fraction $(1 - x)$, Eve performs passive eavesdropping on incomplete bases. The data are given in bits for 2-dimensional systems, and trits for 3-dimensional ones.

case, Eve can get some information without performing any active eavesdropping and without causing any error, just by passively listening and waiting for Alice to confirm Bob's choice of an incomplete basis. Eve then learns that one of the three trit values is eliminated. On the average, she gets information

$$I_E = (9/13)(1 + \log_3 2) = 0.255\,510 \text{ trit}. \quad (12)$$

Finally, let us investigate what happens if Eve eavesdrops only on a fraction x of the particles sent by Alice. In that case, both I_E and E_B are multiplied by x , and I_B is still given by Eqs. (4) and (5), with E_B replaced by xE_B on the right-hand side. The results are displayed in Fig. 2, which also shows the security domain $I_B \geq I_E$, assuming standard error correction and privacy amplification [9]. The values of x for which $I_B = I_E$ are listed in the last column of Table II. We see that the use of four mutually unbiased bases for 3-state particles requires the highest value of x to breach the security. Moreover, for any given value of I_B , this protocol is the one that gives the lowest value of I_E . It thus appears that this method is the one giving the best results against IRE attacks. We believe that it will also be the best for more sophisticated eavesdropping strategies, including joint attacks on several particles. However this problem, and, in particular, a formal proof of security, lie beyond the scope of the present Letter.

We thank Nicolas Gisin for helpful comments on cryptographic security, and Daniel Terno for bringing Ref. [1] to our attention. H.B.-P. was supported by the Danish National Science Research Council (Grant No. 9601645) and also acknowledges support from the European IST Project EQUIP. A.P. was supported by the Gerard Swope Fund and the Fund for Encouragement of Research.

- [1] A computer with ternary logic was built at Moscow State University. This is reported in the Russian translation of D. Knuth, *The Art of Computer Programming* (Nauka, Moscow, 1976), Vol. 1, p. 156 (comment of the translator).
- [2] C.H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
- [3] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
- [4] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
- [5] I.D. Ivanović, J. Phys. A **14**, 3241 (1981).
- [6] W.K. Wootters, Found. Phys. **16**, 391 (1986).
- [7] A.V. Burlakov, M.V. Chekhova, O.A. Karabutova, D.N. Klyshko, and S.P. Kulik, Phys. Rev. A **60**, R4209 (1999).
- [8] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
- [9] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptol. **5**, 3 (1992).
- [10] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
- [11] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
- [12] A.K. Ekert, B. Huttner, G.M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1994).
- [13] C. Cachin and U.M. Maurer, J. Cryptol. **10**, 97 (1997).
- [14] N. Gisin and S. Wolf, quant-ph/0005042, and references therein.
- [15] We also considered the possibility that a vector has different values in different bases. This brings no improvement, since Eve will learn which basis was actually used by Bob.
- [16] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer, Dordrecht, 1995), p. 198.