QUANTUM ENTANGLEMENT AND SECRECY*

Artur Ekert, Daniel K.L. Oi, Carolina Moura Alves

Centre for Quantum Computation, Clarendon Laboratory, Oxford University
Parks Road, Oxford, OX1 3PU, U.K.

L.C. Kwek

Department of Natural Sciences, National Institute of Education
Nanyang Technological University
1 Nanyang Walk, Singapore 637616, Republic of Singapore

and Dagomir Kaszlikowski

Department of Physics, Faculty of Science, National University of Singapore
Lower Kent Ridge, Singapore 119260, Republic of Singapore

(Received June 10, 2002)

We describe how quantum entanglement can be used in secure communication.

PACS numbers: 03.67.Dd, 03.67.Hk

1. Is there a perfect cipher?

Despite a long and colourful history, cryptography became part of mathematics and information theory only last century, in the late 1940s, mainly as the result of the work of Claude Shannon of Bell Laboratories in New Jersey. Shannon showed that truly unbreakable ciphers do exist and, in fact, they had been known for over 30 years [1]. The one time pad, devised around 1918 by an American Telephone and Telegraph engineer Gilbert Vernam, is one of the simplest and most secure encryption schemes. The message, also known as the plaintext, is converted into a sequence of numbers using a publicly known digital alphabet (*e.g.* ASCII code) and then combined with another sequence of random numbers called *a key* to produce a cryptogram. Both sender and receiver must have two exact copies of the key beforehand;

* Presented at the Photons, Atoms and All That, PAAT 2002 Conference, Cracow Poland, May 31–June 1, 2002.

the sender needs the key to encrypt the plaintext, the receiver needs the exact copy of the key to recover the plaintext from the cryptogram. For example, if we choose a simple digital alphabet in which we use only capital letters and some punctuation marks such as

A	B	C	D	E	...	...	X	Y	Z		?	,	.
00	01	02	03	04	...	...	23	24	25	26	27	28	29

then we can illustrate the one-time-pad by the following simple example (we refer to the dietary requirements of 007):

S	H	A	K	E	N		N	O	T		S	T	I	R	R	E	D
18	07	00	10	04	13	26	13	14	19	26	18	19	08	17	17	04	03
15	04	28	13	14	06	21	11	23	18	09	11	14	01	19	05	22	07
03	11	28	23	18	19	17	24	07	07	05	29	03	09	06	22	26	10

In order to obtain the cryptogram C (sequence of digits in the bottom row), we add the plaintext numbers P (the top row of digits) to the key numbers K (the middle row of digits), which are randomly selected from between 0 and 29, and take the remainder after division of the sum by 30, that is, we perform addition modulo 30. For example, the first letter of the message "S" becomes a number "18" in the plaintext, then we add $18 + 15 = 33$; $33 = 1 \times 30 + 3$, therefore we get 03 in the cryptogram. The encryption and decryption can be written as $P + K \pmod{30} = C$ and $C - K \pmod{30} = P$, respectively. The randomness of the key wipes out various frequency patterns in the cryptogam that are used by code-breakers to crack ciphers. Without the key the cryptogram looks like a random sequence of numbers.

The modern version "one-time pad" is based on binary representation of messages and keys. That is, the message is usually converted into a sequence of 0's and 1's and the key is another sequence of 0's and 1's of the same length. Each bit of the message is then combined with the respective bit of the key by addition in base 2 (logical XOR). As long as the key is truly random, has the same length as the message, and is never reused, then the one-time pad is perfectly secure. So, if we have a truly unbreakable system, what is wrong with classical cryptography?

There is a snag, however. All one-time pads suffer from a serious practical drawback, known as the key distribution problem. Potential users have to agree secretly, and in advance, on the key — a long, random sequence of 0's and 1's. Once they have done this, they can use the key for enciphering and deciphering and the resulting cryptograms can be transmitted publicly such as by radio or in newspaper without compromising the security of messages. But the key itself must be established between the sender and the receiver by means of a very secure channel — for example, a very secure telephone line, a private meeting or hand-delivery by a trusted courier. Such a secure channel

is usually available only at certain times and under certain circumstances. So users far apart, in order to guarantee perfect security of subsequent cryptocommunication, have to carry around with them an enormous amount of secret and meaningless as such information (cryptographic keys), equal in volume to all the messages they might later wish to send.

Cryptologists and mathematicians tried very hard to eliminate the problem. The 1970s, for example, brought a clever mathematical discovery in the shape of "public key" systems. The two main public key cryptography techniques in use today are the Diffie–Hellman key exchange protocol [2] and the RSA encryption system (named after the three inventors, Ron Rivest, Adi Shamir, and Leonard Adleman) [3]. They were discovered in the academic community in 1976 and 1978, respectively. However, it was widely rumoured that these techniques were known to the British government agencies prior to these dates, although this was not officially confirmed until recently. In fact, the techniques were first discovered at the British Government Communication Headquarters in the early 1970s by James Ellis, who called them "Non-Secret Encryption". In 1973, building on Ellis' idea, C. Cocks designed what we now call RSA, and in 1974 M. Williamson proposed what is essentially known today as the Diffie–Hellman key exchange protocol.

In the public-key systems users do not need to agree on a secret key before they send the message. They work on the principle of a safe with two keys, one public key to lock it, and another private one to open it. Everyone has a key to lock the safe but only one person has a key that will open it again, so anyone can put a message in the safe but only one person can take it out. The systems avoid the key distribution problem but unfortunately their security depends on unproven mathematical assumptions. For example, RSA — probably the most popular public key cryptosystem — derives its security from the difficulty of factoring large numbers. This means that if and when mathematicians or computer scientists come up with fast and clever procedures for factoring, the whole privacy and discretion of public-key cryptosystems could vanish overnight.

Indeed, more recent work in quantum computation shows that quantum computers can, at least in principle, factor much faster than classical computers [4]! Thus, in one sense, public key cryptosystems are already insecure: any RSA-encrypted message that is recorded today will become readable moments after the first quantum computer is switched on, and therefore RSA cannot be used for securely transmitting any information that will still need to be secret on that happy day. Admittedly, that day is probably decades away, but can anyone prove, or give any reliable assurance, that it is? Confidence in the slowness of technological progress is all that the security of the RSA system now rests on.

Mathematics apart, one can approach the problem from a different angle. Physicists view the key distribution as a physical process associated with sending information from one place to another and eavesdropping as measurements performed on carriers of information. Until now, such eavesdropping has depended on the eavesdropper having the best possible technology. Suppose an eavesdropper is tapping a telephone line. Any measurement on the signal in the line may disturb it and so leave traces. Legitimate users can try to guard against this by making their own measurements on the line to detect the effect of tapping. However, the tappers will escape detection provided the disturbances they cause are smaller than the disturbances that the users can detect. So given the right equipment, eavesdropping can go undetected. Even if legitimate users do detect an eavesdropper, what do they conclude if one day they find no traces of interception? Has the eavesdropping stopped? Or has the eavesdropper acquired better technology? The way round this problem may lie in quantum physics, which brings us to an entirely new way of solving the key distribution problem.

2. Quantum key distribution

Quantum entanglement was singled out by Erwin Schrödinger as the most remarkable feature of quantum theory [5]. At the time in 1935, it was not clear whether entanglement would be of any practical use but it already played a key role in philosophical debates about the meaning of quantum mechanics. Over fifty year later quantum entanglement was recognized as a useful physical resource which can be used, among many other things, to solve the key distribution problem.

The quantum key distribution which we are going to discuss here is based on distribution of entangled particles [6]. It had been discovered independently from the key distribution based on partial indistinguishibility of non-orthogonal state vectors, pioneered by Stephen Wiesner [8], and subsequently developed into a full fledged key distribution scheme by Charles Bennett and Gilles Brassard [9]. In fact, it was discovered almost by chance, as a by-product of late night readings about the EPR programme by one of the authors.

The key distribution is performed via a quantum channel which consists of a source that emits pairs of spin $\frac{1}{2}$ particles in the singlet state

$$\frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right). \tag{1}$$

The particles fly apart along the y-axis towards the two legitimate users of the channel, Alice and Bob, who, after the particles have separated, perform measurements and register spin components along one of three directions,

given by unit vectors $\vec{a}_i$ and $\vec{b}_j$ $(i,j=1,2,3)$, respectively, for Alice and Bob. For simplicity, both $\vec{a}_i$ and $\vec{b}_j$ vectors lie in the x–z plane, perpendicular to the trajectory of the particles, and are characterized by azimuthal angles: $\phi_1^a = 0, \phi_2^a = \frac{1}{4}\pi, \phi_3^a = \frac{1}{2}\pi$ and $\phi_1^b = \frac{1}{4}\pi, \phi_2^b = \frac{1}{2}\pi, \phi_3^b = \frac{3}{4}\pi$. Superscripts "a" and "b" refer to Alice's and Bob's analysers, respectively, and the angle is measured from the vertical z-axis. The users choose the orientation of the analysers randomly and independently for each pair of the incoming particles. Each measurement, in $\frac{1}{2}\hbar$ units, can yield two results, $+1$ (spin up or bit value 0) and -1 (spin down or bit value 1), and can potentially reveal one bit of information. Alice and Bob keep separate records which list, for each pair of incoming particles, the orientation of the local analyser and the registered bit value.

The quantity

$$E(\vec{a}_i,\vec{b}_j) = P_{++}(\vec{a}_i,\vec{b}_j) + P_{--}(\vec{a}_i,\vec{b}_j) - P_{+-}(\vec{a}_i,\vec{b}_j) - P_{-+}(\vec{a}_i,\vec{b}_j) \qquad (2)$$

is the correlation coefficient of the measurements performed by Alice along $\vec{a}_i$ and by Bob along $\vec{b}_j$. Here, $P_{\pm\pm}(\vec{a}_i,\vec{b}_j)$ denotes the probability that result ± 1 has been obtained along $\vec{a}_i$ and ± 1 along $\vec{b}_j$. According to the quantum rules

$$E(\vec{a}_i,\vec{b}_j) = \langle \vec{a}_i\cdot\vec{\sigma}\otimes b_j\cdot\vec{\sigma}\rangle = -\vec{a}_i\cdot\vec{b}_j, \qquad (3)$$

where $\vec{\sigma}$ represents the three Pauli matrices $\sigma_x,\ \sigma_y,\ \sigma_z$, and the averaging is performed for the singlet state. For the two pairs of analysers of the same orientation ($\vec{a}_2$, $\vec{b}_1$ and $\vec{a}_3,\vec{b}_2$), quantum mechanics predicts total anticorrelation of the results obtained by Alice and Bob: $E(\vec{a}_2,\vec{b}_1) = E(\vec{a}_3,\vec{b}_2) = -1$.

For the purpose of what follows, it is instructive to derive Eq. (3) by writing the singlet state as the density operator in the $\sigma_a\otimes\sigma_b$ basis $(a,b = x,y,z)$,

$$|\,\Psi_-\rangle\,\langle\Psi_-\,| = \frac{1}{4}(\mathbb{1} - \sigma_x\otimes\sigma_x - \sigma_y\otimes\sigma_y - \sigma_z\otimes\sigma_z) \qquad (4)$$

and then evaluate

$$\mathrm{Tr}\ [(\vec{a}_i\cdot\vec{\sigma}\otimes b_j\cdot\vec{\sigma})\,|\,\Psi_-\rangle\,\langle\Psi_-\,|] \qquad (5)$$

using, for example, the identity

$$(\vec{a}\cdot\vec{\sigma})(\vec{b}\cdot\vec{\sigma}) = \vec{a}\cdot\vec{b}\ \mathbb{1} + i\ (\vec{a}\times\vec{b})\cdot\vec{\sigma}, \qquad (6)$$

together with $\sigma_{x,y,z}^2 = 1$, and $\mathrm{Tr}\ \sigma_{x,y,z} = 0$.

Let us now define the quantity S composed of the correlation coefficients for which Alice and Bob used analysers of different orientation

$$S = E(\vec{a}_1,\vec{b}_1) - E(\vec{a}_1,\vec{b}_3) + E(\vec{a}_3,\vec{b}_1) + E(\vec{a}_3,\vec{b}_3). \qquad (7)$$

This is the same S as in the generalised Bell theorem proposed by Clauser, Horne, Shimony, and Holt [7] (CHSH). For the singlet state, quantum mechanics requires

$$S = -2\sqrt{2}\,, \tag{8}$$

and all local theories which attribute elements of reality to measured properties satisfy the CHSH inequality

$$|S| \leq 2\,. \tag{9}$$

Let us try to use this inequality as a criterion for secure key distribution. After the transmission has taken place, Alice and Bob can announce in public the orientations of the analysers they have chosen for each particular measurement (N.B. results of the measurements remain seceret) and divide the measurements into two separate groups: a first group for which they used different orientations of the analysers, and a second group for which they used the same orientation of the analysers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently, Alice and Bob can reveal publicly the results they obtained but within the first group of measurements only. This allows them to establish the value of S, which if the particles were not directly or indirectly "disturbed" should reproduce the result of Eq. (8). This assures the legitimate users that the results they obtained within the second second group of measurements are anticorrelated and can be converted into a secret string of bits the key.

An eavesdropper, Eve, cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there! The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. Eve may try to substitute her own prepared data for Alice and Bob to misguide them, but as she does not know which orientation of the analysers will be chosen for a given pair of particles there is no good strategy to escape being detected. In this case her intervention will be equivalent to introducing elements of *physical reality* to the spin components and will lower S below its 'quantum' value. Indeed, suppose that Eve prepares each particle in each pair separately so that each individual particle in the pair has a well defined spin in some direction. These directions may vary from pair to pair so we can say that she prepares with probability $p(\vec{n}_a, \vec{n}_b)$ Alice's particle in state $|\,\vec{n}_a\rangle$ and Bob's particle in state $|\,\vec{n}_b\rangle$, where $\vec{n}_a$ and $\vec{n}_b$ are two unit vectors describing the spin orientations. The density operator for each pair is

$$\rho = \int p(\vec{n}_a, \vec{n}_b)\,|\,\vec{n}_a\rangle\,\langle\vec{n}_a\,|\otimes|\,\vec{n}_b\rangle\,\langle\vec{n}_b\,|\;d\vec{n}_a d\vec{n}_b. \tag{10}$$

Eq. (7) with appropriately modified correlation coefficients reads

$$S = \int p(\vec{n}_a, \vec{n}_b) d\vec{n}_a d\vec{n}_b [(\vec{a}_1 \cdot \vec{n}_a)(\vec{b}_1 \cdot \vec{n}_b) - (\vec{a}_1 \cdot \vec{n}_a)(\vec{b}_3 \cdot \vec{n}_b) + (\vec{a}_3 \cdot \vec{n}_a)(\vec{b}_1 \cdot \vec{n}_b) + (\vec{a}_3 \cdot \vec{n}_a)(\vec{b}_3 \cdot \vec{n}_b)], \tag{11}$$

and leads to

$$S = \int p(\vec{n}_a, \vec{n}_b) d\vec{n}_a d\vec{n}_b [\sqrt{2} \vec{n}_a \cdot \vec{n}_b] \tag{12}$$

which implies

$$-\sqrt{2} \leq S \leq \sqrt{2}, \tag{13}$$

for any state preparation described by the probability distribution $p(\vec{n}_a, \vec{n}_b)$.

This is the case where Eve, who has total control over the state of individual particles, will always have the edge and Alice and Bob should abandon establishing the key; they will learn about it by estimating $|S|$ which in this case will always be smaller than $\sqrt{2}$. However, this is a negative statement - it does not tell us for which values of S Alice and Bob can establish a secret key. Let us investigate if there is any cryptographic meaning to the CHSH threshold, $|S| = 2$.

3. Eavesdropping revisited

The eavesdropping analysis presented above is merely a sketch. Clearly Eve can prepare more complicated states. The question is — what kind of states Eve should prepare and what kind of procedures she should implement in order to maximise her chances of guessing the key bits correctly and to minimise the disturbance. Of course, Eve is bound to introduce some disturbance if she eavesdrops. Her only chance of avoiding detection is to hide behind what, to Alice and Bob, may look like environmental noise in the channel. Let us assume that the noise is symmetrical in the x–z plane, *i.e.* we require that

$$E(\vec{a}, \vec{b}) = \langle \vec{a} \cdot \vec{\sigma} \otimes b \cdot \vec{\sigma} \rangle = -\eta \, \vec{a} \cdot \vec{b}, \tag{14}$$

for any two unit vectors $\vec{a}$ and $\vec{b}$ in the x–z plane and for some fixed $0 \leq \eta \leq 1$. The noise might show asymmetry if the y components of $\vec{a}$ and $\vec{b}$ were taken into account, however, Alice and Bob have to follow a prescribed protocol, and this one excludes measurements with non-zero y components of $\vec{a}$ and $\vec{b}$. Of course, Alice and Bob may consider including such measurements but this would be a new protocol with a new eavesdropping method.

Eq. (14) demands that the reduced density operator of the two particles A and B is of the form

$$\rho = A|\,\Psi_-\rangle\,\langle\Psi_-\,| + B|\,\Phi_+\rangle\,\langle\Phi_+\,| + C\frac{1}{4}\mathbb{1}\,, \tag{15}$$

where $A + B + C = 1$ (N.B. this is not a convex sum, negative values of A, B, and C are allowed). This form follows from the fact that both $\mathbb{1}$ and the two states

$$|\,\Psi_-\rangle\,\langle\Psi_-\,| \;=\; \frac{1}{4}(\mathbb{1} - \sigma_x\otimes\sigma_x - \sigma_y\otimes\sigma_y - \sigma_z\otimes\sigma_z)\,, \tag{16}$$

$$|\,\Phi_+\rangle\,\langle\Phi_+\,| \;=\; \frac{1}{4}(\mathbb{1} + \sigma_x\otimes\sigma_x - \sigma_y\otimes\sigma_y + \sigma_z\otimes\sigma_z) \tag{17}$$

are invariant under rotations in the x–z plane. For state ρ we obtain

$$\langle\vec{a}\cdot\vec{\sigma}\otimes\vec{b}\cdot\vec{\sigma}\rangle = \mathrm{Tr}\;\rho\,(\vec{a}\cdot\vec{\sigma}\otimes b\cdot\vec{\sigma}) = -\,(A-B)\,\vec{a}\cdot\vec{b}\,. \tag{18}$$

Eve can prepare the state ρ by preparing the two particles, and an ancilla E in an entangled state

$$\sqrt{F}\,\frac{1}{\sqrt{2}}\,(|\,01\rangle|\,E_{01}\rangle + |\,10\rangle|\,E_{10}\rangle) + \sqrt{D}\,\frac{1}{\sqrt{2}}\,(|\,00\rangle|\,E_{00}\rangle + |\,11\rangle|\,E_{11}\rangle)\;, \tag{19}$$

where we switched to more convenient notation: $|\,0\rangle$ for spin up $|\,\uparrow\rangle$ and $|\,1\rangle$ for spin down $|\,\downarrow\rangle$ along *any* direction in the x–z plane. Indeed, tracing over the ancilla we obtain ρ as in Eq. (15) provided that $F = 1/2(1 + A - B)$, $D = 1/2(1 - A + B)$, and that normalised, but not necessarily mutually orthogonal, states of the ancilla $|\,E_{ij}\rangle$ satisfy

$$\langle\,E_{01}\,|\,E_{10}\,\rangle = \frac{A}{F} = \cos\alpha\,, \quad \langle\,E_{00}\,|\,E_{11}\,\rangle = \frac{B}{D} = \cos\beta, \tag{20}$$

for some α and β (this convenient parametrisation is taken from [10]). All the remaining inner products are zero, *i.e.* states $\{|\,E_{01}\rangle, |\,E_{10}\rangle\}$ and $\{|\,E_{00}\rangle, |\,E_{11}\rangle\}$ belong to orthogonal subspaces.

The vectors $|\,E_{ij}\rangle$ change when we move from one basis to another in the x–z plane but their inner products $\langle\,E_{ij}\,|\,E_{nm}\,\rangle$ remain invariant under all rotations in that plane.

Now the eavesdropping proceeds as follows. Eve prepares the state (19), sends the particles A and B to Alice and Bob, respectively, and keeps E. She then waits for public communication between Alice and Bob. When the orientations of the analysers are revealed Eve follows the algorithm:

- If the orientations are different ignore the ancilla.
- If the orientations are the same identify the state of the ancilla.

The second point is not trivial, however, Eve knows the orientation of the two analysers and therefore she knows that her ancilla is in one of the four states $|E_{00}\rangle$, $|E_{01}\rangle$, $|E_{10}\rangle$, or $|E_{11}\rangle$. She also knows (*e.g.* from [11]) the optimal measurement that can distinguish between two given non-orthogonal states $|E_{ij}\rangle$ and $|E_{mn}\rangle$ with the minimal probability of error, which is

$$\frac{1}{2}\left(1-\sqrt{1-|\langle E_{ij}\,|\,E_{mn}\rangle|^2}\right). \tag{21}$$

Eve can first check whether the state of the ancilla is in the subspace spanned by $\{|E_{01}\rangle, |E_{10}\rangle\}$ (probability F) or in the orthogonal subspace spanned by $\{|E_{00}\rangle, |E_{11}\rangle\}$ (probability D). This can be done without any errors. Then she can apply the optimal measurement to distinguish either between $|E_{01}\rangle, |E_{10}\rangle$ or between $|E_{00}\rangle, |E_{11}\rangle$. This procedure gives her the bit values registered by Alice and Bob with the error rate

$$Q_E = F\,\frac{1}{2}\,(1-\sin\alpha) + D\,\frac{1}{2}\,(1-\sin\beta)\,. \tag{22}$$

Fixing the disturbance of the correlations

$$\eta = A - B = F\cos\alpha - D\cos\beta \tag{23}$$

Eve can minimise her error rate Q_E by choosing $\cos\alpha = -\cos\beta$, which gives,

$$Q_E = \frac{1}{2}(1-\sin\alpha)\,, \quad \eta = \cos\alpha\,. \tag{24}$$

The error rate in the generated key is

$$Q_{AB} = \frac{1}{2}(1-\cos\alpha)\,, \tag{25}$$

and it matches Eve's error $Q_E = Q_{AB}$, for $\cos\alpha = \sin\alpha = 1/\sqrt{2}$, *i.e.* in terms of the CHSH inequality exactly for

$$|S| = 2\,. \tag{26}$$

Thus the CHSH threshold corresponds to the crossing point of the two error rates. This point is of some significance in cryptanalysis. It is, roughly speaking, the maximal error rate at which Alice and Bob can establish a secure key using some prescribed error correcting codes and without any further communication in public (see, for example, [12]). Thus the positive statement is: Alice and Bob can establish a secret key whenever $|S| > 2$.

4. Quantum Privacy Amplification

In fact Alice and Bob can establish a secret key even for some values of S which are smaller than 2. For this, Alice and Bob may use *Quantum Privacy Amplification* (QPA) [13]. The essential element of the QPA procedure is 'entanglement purification' [14]. Without going into technical details one can describe the QPA as an iterative quantum algorithm which, if performed with perfect accuracy, starting with a collection of EPR-pairs in mixed states, would discard some of them and leave the remaining ones in states converging to the pure singlet state. This means that $|S|$ for the remaining pairs will converge to $2\sqrt{2}$. Since the remaining pairs are maximally entangled with each other, they cannot be entangled with anything else, especially states in Eve's possession. The QPA procedure can be performed by Alice and Bob at distant locations by a sequence of local unitary operations and measurements which are agreed upon by communication over a public channel.

It has been shown that any entangled states of two qubits can be purified [15]. Taking the density operator (15) and inserting the optimal coefficients, A, B, and C (which at a given disturbance $\eta = \cos\alpha$ minimize the error rate Q_E) we obtain

$$\rho(\alpha) = \frac{1}{2}\cos\alpha(1+\cos\alpha)|\,\Psi_-\rangle\,\langle\Psi_-\,| - \frac{1}{2}\cos\alpha(1-\cos\alpha)|\,\Phi_+\rangle\,\langle\Phi_+\,| + \sin^2\alpha\mathbb{1}. \tag{27}$$

This gives $|S(\alpha)| = \cos\alpha 2\sqrt{2}$. Now, using the partial transposition test [16, 17] we can check that $\rho(\alpha)$ is entangled when $\cos\alpha > \sqrt{2}-1$. This implies that if Alice and Bob are prepared to use the QPA then they can establish a secret key for values $|S| > 2(2-\sqrt{2})$. (N.B. this does not contradict Eq.(13) where we did not require the rotational symmetry in the x–z plane, such a requirement would give $S = 0$.)

We should add here that, unfortunately, the QPA is rather inefficient - many pairs of particles are discarded in the process. One should also mention here that there are classical techniques, such as "advantage distillation", which can supplement quantum key distributions and guarantee its secrecy for some $|S| < 2$ (see for example [19]), however, these techniques are equally inefficient. Thus the CHSH inequality may remain as a clean criterion for an efficient and secure quantum key distribution, at least for all practical purposes.

5. Concluding remarks

This brief overview has only scratched the surface of the many activities that are presently being pursued under the heading of quantum cryptography. For example, one may now venture into more complicated security

analysis involving methods in which Eve, instead of pair by pair preparations, prepares several pairs of particles in one go, entangles them with more complicated ancilla, and sends them to Alice and Bob. This kind of methods do not lead to significantly different security limits on error rates but are nonetheless interesting from the theoretical point of view. One can also discuss alternative key distribution protocols, or other cryptographic tasks. However, let me stop here hoping that even the simplest outline of quantum key distribution has enough interesting physics to keep you entertained for a while.

A.E. and C.M.A are greatly indebted to Oh Choo Hiap for his hospitality during their visits to Singapore. A.E. and L.C.K. acknowledge financial support provided under the A*STAR Grant No. 012-104-0040. C.M.A. is supported by the Fundação para a Ciência e Tecnologia (Portugal) and D.K.L.O would like to acknowledge the support of CESG (UK) and QAIP (contract no. IST-1999-11234).

REFERENCES

[1] C.E. Shannon, *Bell. Syst. Tech. J.* **28**, 657 (1949).

[2] W.Diffie, M.E. Hellman, *IEEE Trans. Inf. Theory* **IT-22**, 644 (1976).

[3] R. Rivest, A. Shamir, L. Adleman, *On Digital Signatures and Public-Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212, January, 1979.

[4] P.W. Shor, Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20-22 Nov. 1994, *IEEE Comput. Soc. Press*, 124–134 (1994).

[5] E. Schrödinger, Naturwissenschaften, **23**, 807 (1935); Naturwissenschaften, **23**, 823 (1935); Naturwissenschaften, **23**, 844 (1935) and *Proc. Cambridge Phil. Soc.* **31**, 555 (1935).

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

[7] J.F Clauser, M.A. Horne, A. Shimony, R.A. Holt, *Phys. Rev. Lett.* **23**, 880 (1969).

[8] S. Wiesner, *SIGACT News*, **15**, 78 (1983); original manuscript written *circa* 1970.

[9] C.H. Bennett, G. Brassard, *Proc. IEEE Int. Conference on Computers, Systems and Signal Processing, IEEE*, New York 1984.

[10] J.I. Cirac, N.Gisin, Coherent eavesdropping strategies for the 4 state quantum cryptography protocol, `quant-ph/9702002`.

[11] C.W. Hellstrom, *Quantum Detection and Estimation Theory*, Academic Press, 1976.

[12] I. Csiszár, J. Körner, *IEEE Trans. Inf. Theory*, **24**, 339 (1978).

[13] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

[14] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, W.K. Wootters, *Phys. Rev. Lett.* **76**, 722 (1996).

[15] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Rev. Lett.* **78**, 574 (1997).

[16] A. Peres *Phys. Rev. Lett.* **77**, 1413 (1996).

[17] M. Horodecki, P. Horodecki, R. Horodecki, *Phys. Lett.* **A223**, 1 (1996).

[18] C. Macchiavello, `quant-ph/9807074`

[19] U.M. Maurer, *IEEE Trans. Inf. Theory*, **39**, 733 (1993).