acta physica slovaca vol. 49 No. 4, 533 – 539 **August 1999**

SECRET SHARING VIA QUANTUM ENTANGLEMENT *

M. Hillery[a], **V. Bužek**[b,c]
[a] *Department of Physics & Astronomy, Hunter College, CUNY, 695 Park Avenue, New York, NY 10021, USA*
[b] *Institute of Physics, Slovak Academy of Sciences, Dúbravská cesta 9, 842 28 Bratislava, Slovakia*
[c] *Faculty of Informatics, Masaryk University, Botanická 68a 602 00 Brno, Czech Republic*

Received 25 April 1999, accepted 10 May 1999

Secret sharing is a procedure for splitting a message into several parts so that no single part is sufficient to read the message, but the entire set is. This procedure can be implemented using either GHZ states or two-particle entangled states. In the quantum case the presence of an eavesdropper will introduce errors so that her presence can be detected. We also discuss how quantum information can be split into parts so that the message can be reconstructed from a sufficiently large subset of the parts.

PACS: 03.65.Bz, 03.67.-a

1 Introduction

Suppose Alice, who is in Bratislava, wants to have an action taken on her behalf in Brno. There she has two agents, Bob and Charlie, who can carry it out for her, but she knows that one of them, and only one, is dishonest, and she does not know which is the honest one. She cannot simply send a message to both, because the dishonest one will try to sabotage the action, but she knows that if the two of them carry out it together, the honest one will keep the dishonest one from doing any damage. What can she do?

Classical cryptography provides an answer which is known as secret sharing [1]. It can be used, for example, to guarantee that no single person can open a vault, has access to an industrial secret, or can launch a missile with a nuclear warhead, but two together can. This means that for security to be breached, two people must act in concert, thereby making it more difficult for any single person who wants to gain illegal access to the secret information; he must convince the other party to go along, and he risks discovery in the process.

How can Alice implement this procedure? From her original message, she creates two coded messages one of which is sent to Bob and the other to Charlie. Each of the encrypted

* Presented at the 6th Central-European Workshop on Quantum Optics, Château Chudobín, Czech Republic, April 30 - May 3, 1999.

messages contains no information about her original message, but together they contain the complete message. Therefore, neither Bob nor Charlie alone can find out what Alice wants to do, but the two of them acting together can. This can be accomplished by taking the original message, which we can think of as a binary bit string, and adding to it a random bit string of the same length. The addition is done modulo 2 and bitwise. Alice then takes this string and a copy of the random string and sends one to Bob and the other to Charlie. At this point neither is in a position to learn Alice's message. However, if they get together and add their two strings together, bitwise and modulo 2, Alice's message emerges. There are also classical protocols which allow Alice to split her message into more than two parts.

It is also possible to implement more complicated secret-sharing protocols. Alice may want to divide her secret into n parts so that any k of them can be used to reconstruct the secret, but fewer than k cannot. This is known as an (k, n) secret sharing scheme.

So far we have not mentioned the problem of eavesdropping, but this is something Alice must consider. If either a fourth party or the dishonest member of the Bob-Charlie pair gains access to both of Alice's transmissions, then they can learn the contents of her message. Eavesdroppers can, however, be defeated by using quantum cryptographic protocols. Quantum cryptography provides for the secure transmission of information by enabling one to determine whether an eavesdropper has attempted to gain information about the key which is being used to encode the message [2–4]. If not, the key can be used and the information sent by using it will be secure, and if an eavesdropper has been detected, then one has to establish a new key.

We would like to show that it is possible to combine quantum cryptography with secret sharing in a way that will allow one to determine whether an eavesdropper has been active during the secret sharing protocol. In the protocols examined here, quantum mechanics is used to do both the information splitting and the eavesdropper protection simultaneously.

We shall discuss two methods of implementing a quantum secret-sharing scheme in which a key is spit into two parts. The first method uses maximally entangled three-particle states, or GHZ states [5] and the second uses maximally entangled two-particle states [6]. In addition, it is possible to split quantum information, e. g. the information contained in a qubit, into several parts. One method of doing this is discussed in [5], and a thorough study of the problem has been performed by Cleve, Gottesman and Lo who have shown how to construct (k, n) schemes for quantum information [7]. We briefly discuss an example of a $(2, 3)$ scheme presented in their paper.

2 Quantum Secret Sharing of Classical Information

Let us suppose that Alice, Bob, and Charlie each have one particle from a GHZ triplet which is in the state [8]

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{1}$$

They each choose at random whether to measure their particle in the x or y direction. They then announce publicly in which direction they have made a measurement, but not the results of their measurements. Half the time, Bob and Charlie, by combining the results of their measurements, can determine what the result of Alice's measurement was. This allows Alice to establish a joint key with Bob and Charlie, which she can then use to send her message.

Let us see how this works in more detail. Define the x and y eigenstates

$$
\begin{aligned}
|+x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle); \qquad & |+y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle); \\
|-x\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle); \qquad & |-y\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle).
\end{aligned} \tag{2}
$$

We can see the effects of measurements by Alice and Bob on the state of Charlie's particle, if we express the GHZ state in different ways. Noting that

$$
|0\rangle = \frac{1}{\sqrt{2}}(|+x\rangle + |-x\rangle); \; |1\rangle = \frac{1}{\sqrt{2}}(|+x\rangle - |-x\rangle) \tag{3}
$$

we can write

$$
\begin{aligned}
|\psi\rangle \;=\; & \frac{1}{2\sqrt{2}}\left[(|+x\rangle_a|+x\rangle_b + |-x\rangle_a|-x\rangle_b)(|0\rangle_c + |1\rangle_c)\right. \\
& + \left.(|+x\rangle_a|-x\rangle_b + |-x\rangle_a|+x\rangle_b)(|0\rangle_c - |1\rangle_c)\right].
\end{aligned} \tag{4}
$$

This decomposition of $|\psi\rangle$ tells us what happens if both Alice and Bob make measurements in the x direction. If they both get the same result, then Charlie will have the state $(|0\rangle_c+|1\rangle_c)/\sqrt{2}$, and if they get different results he will have the state $(|0\rangle_c - |1\rangle_c)/\sqrt{2}$. He can determine which of these states he has by performing a measurement along the x direction. The following table summarizes the effects of Alice's and Bob's measurements on Charlie's state:

Bob \ Alice	$+x$	$-x$	$+y$	$-y$
$+x$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle - i\|1\rangle$	$\|0\rangle + i\|1\rangle$
$-x$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle + i\|1\rangle$	$\|0\rangle - i\|1\rangle$
$+y$	$\|0\rangle - i\|1\rangle$	$\|0\rangle + i\|1\rangle$	$\|0\rangle - \|1\rangle$	$\|0\rangle + \|1\rangle$
$-y$	$\|0\rangle + i\|1\rangle$	$\|0\rangle - i\|1\rangle$	$\|0\rangle + \|1\rangle$	$\|0\rangle - \|1\rangle$

Alice's measurements are given in the columns and Bob's are given in the rows. Charlie's state, up to normalization, appears in the boxes. From the table it is clear that if Charlie knows what measurements Alice and Bob made (that is, x or y), he can determine whether their results are the same or opposite, and also that he will gain no knowledge of what their results actually are. Similarly, Bob will not be able to determine what Alices's result is without Charlie's assistance, because he does not know if his result is the same as Alice's, or the opposite of hers.

With each party choosing to make x or y measurements at random, only half of the GHZ triplets will give useful results. For example, if Alice and Bob both measure their particles in the x direction, Charlie must also measure his in the x direction in order to determine whether the results of Alice's and Bob's measurements are correlated or anticorrelated; if he measures in the y direction he gains no information. Because Charlie is choosing his measurement direction at random, he will only choose correctly half the time. This is why all three parties must announce the directions of their measurements, so that they can decide whether to keep or to discard the results from a given triplet. This announcement should be done in the following way: Bob and Charlie both send to Alice the direction of their measurements who then sends all three measurement directions to Bob and Charlie.

Before presenting a more general discussion of eavesdropping, we shall consider a specific situation in order to show that it can be detected. Suppose that Bob is dishonest and that he has managed to get a hold of Charlie's particle as well as his own. He then measures the two particles and sends one of them on to Charlie. His objective is to discover what Alice's bit is, without any assistance from Charlie, and to do so in a way that cannot be detected. Alice has measured her particle in either the x or y direction, but Bob does not know which. He would like to measure the quantum state of his two-particle system, but because he does not know what measurement Alice made, he does not know whether to make his in the $(|00\rangle \pm |11\rangle)/\sqrt{2}$ basis or in the $|00\rangle \pm i|11\rangle)/\sqrt{2}$ basis. Choosing at random he has a probability of $1/2$ of making a mistake. If he chooses correctly, he will know, for valid combinations of measurement axes, what the result of Charlie's measurement is from the result of his own, and this means he will then know what Alice's bit is. For example, if Alice measured in the x direction and found $|{+x}\rangle$, then the state Bob receives is $|00\rangle + |11\rangle)/\sqrt{2}$. If Bob now measures in the $|00\rangle \pm |11\rangle)/\sqrt{2}$ basis, he knows what the two- particle state is, and because

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|+x\rangle|+x\rangle + |-x\rangle|-x\rangle). \tag{5}$$

Bob knows that Charlie's measurement will produce a result identical to his.

What happens if he is wrong? Suppose that Alice has measured her particle in the y direction and that Bob measures his particles in the $(|00\rangle \pm |11\rangle)/\sqrt{2}$ basis. He has a probability of $1/2$ of getting either basis vector. He now sends one of his particles to Charlie, and both Bob and Charlie measure their particles. Because Alice measured y, in order for this round of measurements to produce a valid key bit, Bob and Charlie must make different measurements, i. e. one must measure x and the other y. We note that in the $(|00\rangle \pm |11\rangle)/\sqrt{2}$ basis there is no correlation between x and y measurements, for example

$$\begin{aligned}\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad &= \quad \frac{1}{2}\Big[e^{-i\pi/4}(|+x\rangle|+y\rangle + |-x\rangle|-y\rangle) \\ &+ \quad e^{i\pi/4}(|+x\rangle|-y\rangle + |-x\rangle|+y\rangle)\Big]\,. \end{aligned}\tag{6}$$

Therefore, in half the situations the results of the measurements will be wrong. If, for example, Alice found $|+y\rangle$ and Bob found $|+x\rangle$, then Charlie should measure $|-y\rangle$ if he measures his particle in the y direction, but because of Bob's measurement, he has a probability of $1/2$ of finding $|+y\rangle$. The overall probability of an error in this cheating scheme is $1/4$, one half of picking the wrong basis and then one half of getting the wrong result.

There are two additional points to notice here. First, if Bob were able to learn the direction of Alice's and Charlie's measurements before having to reveal his, he could cheat more successfully. In the cases in which he made the wrong measurement, Bob could simply tell Alice a measurement direction which would cause the results from that triplet to be thrown out. Alice and Charlie would, however, notice a higher than usual failure rate, 75 % as opposed to 50 %, which would tell them that something unusual was happening. Insisting that Bob send a measurement direction to Alice before learning what kind of measurement Alice and Charlie makes this kind of cheating more difficult. Second, there is also the possibility that Bob could lie at certain points in the procedure; he could lie about his measurement direction or about the result of his measurement. In the cheating scheme considered above he gains, however, nothing by doing so.

Now let us look at a more general situation. We assume that there is an eavesdropper, Eve (who could also be either Bob or Charlie). Her problem, as in the example which we just discussed, is that she does not know what bases have been or will be used to measure the particles. If she measures them herself, and chooses the wrong bases, she will introduce errors which Alice, Bob and Charlie will be able to detect by publicly comparing a subset of their measurements.

In order to demonstrate this for a large class of measurements, let us assume that Eve has been able to entangle an ancilla with the three particle state which Alice, Bob, and Charlie are using. At some later time she can measure the ancilla to gain information about the measurement results of Alice, Bob and Charlie. The state describing the state of the three particles and the ancilla is

$$|\Psi\rangle = \sum_{j,k,n=0}^{1} |jkn\rangle_3 |R_{jkn}\rangle_\xi, \tag{7}$$

where $|jkn\rangle_3$ is a state of the three particles, and $|R_{jkn}\rangle_\xi$ is an unnormalized ancilla state. It can be shown is that if this entanglement introduces no errors into the secret sharing procedure, then $|\Psi\rangle$ must be a product of a GHZ triplet and the ancilla [5]. This implies that Eve will gain no information about measurements on the triplet from observing the ancilla, or, conversely, if Eve is to gain information about Alice's bit, she must invariably introduce errors.

A different secret-sharing scheme was introduced by Karlsson, Koashi, and Imoto [6]. Alice now uses two sets of two-particle states, $\{|\psi^+\rangle, |\phi^-\rangle\}$ and $\{|\Psi^+\rangle, |\Phi^-\rangle\}$, where

$$\begin{aligned}
|\psi^+\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle|+x\rangle - |-x\rangle|-x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) \\
|\phi^-\rangle &= \frac{1}{\sqrt{2}}(|+x\rangle|-x\rangle + |-x\rangle|+x\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|+x\rangle + |1\rangle|-x\rangle) = \frac{1}{\sqrt{2}}(|+x\rangle|0\rangle + |-x\rangle|1\rangle) \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle|-x\rangle - |1\rangle|+x\rangle) = \frac{1}{\sqrt{2}}(|+x\rangle|1\rangle - |-x\rangle|0\rangle).
\end{aligned} \tag{8}$$

In turning states into key bits, 0 corresponds to either $|\psi^+\rangle$ or $|\Psi^+\rangle$, and 1 corresponds to either $|\phi^-\rangle$ or $|\Phi^-\rangle$. Note that while states within the two sets are orthogonal, $\langle\psi^+|\phi^-\rangle = \langle\Psi+|\Phi^-\rangle = 0$, those in different sets are not, $|\langle\psi^+|\Psi^+\rangle|^2 = |\langle\psi^+|\Phi^-\rangle|^2 = 1/2$ and $|\langle\phi^-|\Psi^+\rangle|^2 = |\langle\phi^-|\Phi^-\rangle|^2 = 1/2$. This means that states within a single set are perfectly distinguishable, but those in different sets are not.

In order to send Bob and Charlie a key bit, Alice chooses one of the two sets and sends the state to them, one particle to each, corresponding to the key bit she wishes to send. Bob and Charlie choose at random whether to measure their particles in the z $(|0\rangle, |1\rangle)$ or the x basis. Bob and Charlie then state in which bases they made their measurements, and Alice declares from which of the two sets the state she sent was from. In half the cases useful results will be obtained: if Alice sent either $|\psi^+\rangle$ or $|\phi^-\rangle$ and Bob and Charlie chose the same basis, or if Alice sent either $|\Psi^+\rangle$ or $|\Phi^-\rangle$ and Bob and Charlie chose different bases. In these cases, by comparing the results of their measurements, they can determine which state Alice sent and, therefore, the value of the bit, 0 or 1, which she sent. Each party separately, however, cannot figure out Alice's bit. For example, let us suppose that Alice sent a state from the set $\{|\psi^+\rangle, |\phi^-\rangle\}$, and that Bob and Charlie both measured their particles in the x direction. If on comparing their results, Bob and Charlie find they are the same, they can conclude that Alice sent $|\psi^+\rangle$, and if the are different, then Alice must have sent $|\phi^-\rangle$.

Because the two sets which Alice is using are not orthogonal, an eavesdropper has a problem. She does not know which set is being used, and, because states in different sets are not orthogonal, she cannot distinguish between the two sets by making a measurement. She is thus reduced to guessing, and if she guesses incorrectly, she will disturb the state and introduce errors. The problem of cheating by Bob or Charlie is a bit more subtle, but it can be overcome, and a method for doing so is clearly discussed in [6].

3 Sharing Quantum Information

So far, we have only discussed how quantum mechanics can be used to split classical information in a way which provides protection against eavesdropping and cheating. Suppose instead that we want to split the information in a qubit into two pieces so that neither piece alone can be used to reconstruct the qubit, but both together can. One method of doing this, which is based on teleportation using GHZ states [9, 10], is presented in [5]. Here we would like to present a scheme which appeared in a recent paper by Cleve, Gottesman, and Lo [7].

Theirs is a $(2, 3)$ scheme which splits the information in a qutrit, a 3-level quantum system, into three parts any two of which can be used to reconstruct the state of the qutrit. The state of the original qutrit is split among three qutrits as

$$\begin{aligned} \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \to |\Psi\rangle &= \alpha(|000\rangle + |111\rangle + |222\rangle) \\ &+ \beta(|012\rangle + |120\rangle + |201\rangle) \\ &+ \gamma(|021\rangle + |102\rangle + |210\rangle). \end{aligned} \tag{9}$$

Any two of the three particles can be used reconstruct the qutrit, and we shall show explicitly how this can be done with particles 1 and 2.

If we have particles 1 and 2 we can apply the unitary operator U to them, where U acts on the basis vectors, $|p, q, r\rangle$, where p, q, and r range over the values 0, 1, and 2, as

$$U|p, q, r\rangle = |2p + q, p + q, r\rangle, \tag{10}$$

and all operations on the right-hand side are performed modulo 3. Note that this transformation does not affect particle 3. If we now apply this transformation to the state $|\Psi\rangle$ in Eq. (9), we find

$$U|\Psi\rangle = (\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle)(|00\rangle + |12\rangle + |21\rangle), \tag{11}$$

and the original qutrit is recovered. If one has a different pair of particles, a similar transformation can be applied to obtain the encoded qutrit.

In their paper, Cleve, Gottesman, and Lo develop a complete theory of quantum (k,n) schemes. One result which follows immediately from the no-cloning theorem is that for a (k,n) scheme to exist, we must have $n < 2k$ [11]. They then showed that if this condition is satisfied, a quantum (k,n) scheme can be constructed.

4 Conclusion

Quantum mechanics can be used either to split classical information in such a way that it is protected against eavesdroppers, or to split quantum information. There is a second method of splitting quantum information, approximate quantum cloning, in which one takes a single qubit and produces two approximate copies of it [12]. The information splitting produced in this process is different from that which results from a secret splitting procedure, in that the original qubit cannot be reconstructed from the two copies; some of the information remains in the cloning machine itself. We therefore, have at least two ways of breaking quantum information into parts, and we strongly suspect that these do not exhaust the possibilities.

Acknowledgments We thank André Berthiaume for collaboration and Richard Cleve for helpful discussions and correspondence. This research was supported by the Royal Society, the Slovak Academy of Sciences, and by the GACR (project 201/98/0369).

References

[1] B. Schneier: *Applied Cryptography* (Wiley, New York, 1996) p. 70; see also J. Gruska: *Foundations of Computing* (Thomson Computer Press, London, 1997) p. 504

[2] C. Bennett, G. Brassard: in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (Bangalore, India 1984) p. 175

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

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

[5] M. Hillery, V. Bužek, A. Berthiaume: *Phys. Rev. A* **59** (1999) 1829

[6] A. Karlsson, M. Koashi, N. Imoto: *Phys. Rev. A* **59** (1999) 162

[7] R. Cleve, D. Gottesman, H.K. Lo: *quant-ph/9901025*

[8] D. Greenberger, M. Horne, A. Zeilinger: in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kaftos (Kluwer Academic, Dordrecht, 1989)

[9] C.H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W.K. Wootters: *Phys. Rev. Lett.* **70** (1993) 1895. For experimental realization of quantum teleportation see D. Boumeester, J.W. Pan, K. Mattle, M. Eisl, H. Weinfurter, A. Zeilinger: *Nature* **360** (1997) No. 6660, 575, as well as D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu: *Phys. Rev. Lett.* **80** (1998) 1121

[10] Richard Cleve: *private communication*. The idea of using teleportation to split quantum information is due to Louis Salvail.

[11] W. Wootters, W. Zurek: *Nature* **299** (1982) 802; D. Dieks: *Phys. Lett. A* **92** (1982) 271

[12] V. Bužek, M. Hillery: *Phys. Rev. A* **54** (1996) 1844; *Phys. Rev. Lett.* **81** (1998) 5003