Quantum Information and Computation, Vol. 12, No. 3&4 (2012) 0253–0261

PROBABILISTIC SECRET SHARING THROUGH NOISY QUANTUM CHANNEL

SATYABRATA ADHIKARI[a] INDRANIL CHAKRABARTY[b] PANKAJ AGRAWAL[c]
Institute of Physics, Sainik School Post
Bhubaneswar-751005, Orissa, India

Received April 22, 2011
Revised December 7, 2011

In a realistic situation, the secret sharing of classical or quantum information will involve the transmission of this information through noisy channels. We consider a three qubit pure state. This state becomes a mixed-state when the qubits are distributed over noisy channels. We focus on a specific noisy channel, the phase-damping channel. We propose a protocol for secret sharing of classical information with this and related noisy channels. This protocol can also be thought of as cooperative superdense coding. We also discuss other noisy channels to examine the possibility of secret sharing of classical information.

Keywords: Secret Sharing, Phase damping channel, POVM, GHZ states
Communicated by: S Braunstein & H Zbinden

1 Introduction

Quantum entanglement [1] plays a pivotal role in understanding the deepest nature of reality. In classical world there is no counter part of quantum entanglement. Entanglement is a very useful resource in the sense that using entanglement a lot of things can be done that cannot be done otherwise. Entanglement is also essential for the communication tasks like quantum teleportation [2], quantum cryptography [3] and quantum secret sharing [4].

In a secret sharing protocol, one distributes a secret message among a group of people. This is done by allocating a share of the secret to each of these participants. The beauty of the entire secret sharing process lies in the fact that, if there is a dishonest member in the group of participants, he will not be able to find the secret without the collaboration of other members. In other words, the secret can be reconstructed only when a sufficient number of shares are combined together; individual shares are of no use.

The secret sharing protocol in a quantum scenario was first introduced in Ref [4]. After its introduction, Karlsson et.al.[5] studied the similar quantum secret sharing protocol using bipartite pure entangled state. Many authors studied the concept of quantum secret sharing using tripartite pure entangled states and also for multi partite states like graph states [6, 7, 8, 9, 10, 11]. Recently Q. Li et.al. proposed semi-quantum secret sharing protocols using maximally entangled GHZ state which was shown to be secure against eavesdropping [12].

[a]E-mail: tapisatya@gmail.com
[b]E-mail: indranil@iopb.res.in
[c]E-mail: agrawal@iopb.res.in

Recently in [13], it was shown that Quantum secret sharing is possible with bipartite two qubit mixed states (formed due to noisy environment). Quantum secret sharing can also be realized in experiment [14, 15, 16, 17].

The purpose of this paper is to introduce a protocol which can be used to secretly share classical information in the presence of noisy quantum communication channels. We first show that this secret sharing scheme is deterministically possible for a shared pure three qubit GHZ state. Then, we consider a realistic situation where a source creates a pure GHZ state and then the qubits are distributed to different parties through noisy channels. These noisy channels convert the initial pure state into a mixed state. We carry out the analysis and find the number of classical bits that can be secretly shared for a specific noisy channel, the phase-damping channel. One of the important feature of this channel is that it describes the loss of quantum information without loss of energy. We also talk about several other noisy channels and comment on the possibility of secret sharing using those channels.

The organization of the paper is as follows. In Section II, we describe our protocol for pure three qubit GHZ state. In Section III, we deviate from the ideal scenario and consider the realistic situation where qubits are transferred through phase-damping channels and reinvestigate our secret sharing scheme. In the last section, we discuss other noisy channels and present our conclusions.

2 Secret sharing scheme with shared pure GHZ state

In this section, we introduce a protocol for quantum secret sharing with shared pure GHZ state. In this protocol, three parties start with a shared pure GHZ state. Then one of the members encodes secret by doing some local unitary operation on her qubit. Thereafter, she sends her qubit to one of the other two members. Interestingly neither of these two members would be able to know about the local unitaries performed by the encoder individually. However, we show that if they agree to collaborate, then one of the parties can decode the two bit secrets. Our protocol goes like this.

Step I: Pure GHZ State shared by three parties

Let us consider three parties say, Alice (A), Bob (B) and Charlie (C) share a pure GHZ state

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle]. \tag{1}$$

Step II: Unitary operations performed by Alice

In this step, Alice encodes two bits of secret information by performing one of the $\{I, \sigma_x, i\sigma_y, \sigma_z\}$ unitary operations on her qubit. After performing one of the unitary operations the state (1) transforms correspondingly to one of the following states

$$(I \otimes I \otimes I)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}[|000\rangle + |111\rangle],$$
$$(\sigma_x \otimes I \otimes I)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}[|100\rangle + |011\rangle],$$
$$(i\sigma_y \otimes I \otimes I)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}[|100\rangle - |011\rangle],$$

$$(\sigma_z \otimes I \otimes I)|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}[|000\rangle - |111\rangle]. \tag{2}$$

Alice then sends her qubit to Bob.

Step III: Charlie performs single-qubit measurement

The above set of equations (2) can be rewritten as

$$\begin{aligned}
|\Psi\rangle^{I}_{BBC} &= \frac{1}{2}[|\Phi^+\rangle \otimes (|0\rangle + |1\rangle) + |\Phi^-\rangle \otimes (|0\rangle - |1\rangle)],\\
|\Psi\rangle^{X}_{BBC} &= \frac{1}{2}[|\Psi^+\rangle \otimes (|0\rangle + |1\rangle) - |\Psi^-\rangle \otimes (|0\rangle - |1\rangle)],\\
|\Psi\rangle^{Y}_{BBC} &= \frac{1}{2}[|\Psi^+\rangle \otimes (|0\rangle - |1\rangle) - |\Psi^-\rangle \otimes (|0\rangle + |1\rangle)],\\
|\Psi\rangle^{Z}_{BBC} &= \frac{1}{2}[|\Phi^+\rangle \otimes (|0\rangle - |1\rangle) + |\Phi^-\rangle \otimes (|0\rangle + |1\rangle)],
\end{aligned} \tag{3}$$

where $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|00\rangle \pm |11\rangle], |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}[|01\rangle \pm |10\rangle]$.

At this stage, it is not possible either for Bob or for Charlie to decipher the secret encoded by Alice. However, Bob can unmask the secret if Charlie agrees to cooperate with him. Since Charlie now has a single particle at his disposal, he performs a single-qubit measurement in the Hadamard basis $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$. Then he can help Bob to decode the message by conveying to him the outcomes of his measurement.

Step IV: Bob performs Bell-state measurement

According to the measurement outcomes announced by Charlie, Bob performs a Bell-state measurement on his two qubits. According to his Bell-state measurement outcome, he can find the secret encoded by Alice. The two bits secret decoded by Bob as a result of the declaration of the measurement outcome by Charlie is given in the following table.

TABLE I:

Qubits at Bob's side	Charlie's Measurement Outcome	Secrets deciphered by Bob
$\|\Phi^+\rangle_{BB}$	$\frac{1}{\sqrt{2}}[\|0\rangle_C + \|1\rangle_C]$	I
	$\frac{1}{\sqrt{2}}[\|0\rangle_C - \|1\rangle_C]$	σ_z
$\|\Phi^-\rangle_{BB}$	$\frac{1}{\sqrt{2}}[\|0\rangle_C + \|1\rangle_C]$	σ_z
	$\frac{1}{\sqrt{2}}[\|0\rangle_C - \|1\rangle_C]$	I
$\|\Psi^+\rangle_{BB}$	$\frac{1}{\sqrt{2}}[\|0\rangle_C + \|1\rangle_C]$	σ_x
	$\frac{1}{\sqrt{2}}[\|0\rangle_C - \|1\rangle_C]$	$i\sigma_y$
$\|\Psi^-\rangle_{BB}$	$\frac{1}{\sqrt{2}}[\|0\rangle_C + \|1\rangle_C]$	$i\sigma_y$
	$\frac{1}{\sqrt{2}}[\|0\rangle_C - \|1\rangle_C]$	σ_x

3 Secret sharing with mixed state

In this section, we consider a more realistic situation in which a party, say, Charlie generates a three qubit pure GHZ state in his laboratory. Then he keeps one qubit with him and sends the other two qubits through two identical noisy channels to two of his friends Alice (A) and

Bob (B). As a result of the interaction of the qubit with the environment, the three parties share a three-qubit mixed state after the distribution of the qubits. We would consider the case of phase-damping channel as the noisy channel. The action of a phase-damping channel are given by the set of three Kraus operators $E_0 = \sqrt{1-p}I, E_1 = \sqrt{p}|0\rangle\langle 0|, E_2 = \sqrt{p}|1\rangle\langle 1|$, where p $(0 < p < 1)$ is the channel parameter [18]. In this case, our protocol for secret sharing may be described in the following steps:

Step I: Transferring qubits through phase-damping channels

Let us assume that Charlie prepares a three-qubit pure GHZ state. Thereafter, he keeps one qubit with him and sends the other two qubits through two phase-damping channels to two of his friends Alice and Bob. As a result of the action of the channels, described by the above Kraus operators, on their respective qubits, the resultant state shared by the three parties becomes a mixed state

$$\rho^{ABC} = \frac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] + \frac{(1-p)^2}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|]. \tag{4}$$

Step II: Local Unitary operation by Alice

After receiving the qubits from Charlie, one of the party say Alice encodes two bits of information by carrying out the local unitary transforms $\{I(00), \sigma_x(01), i\sigma_y(10), \sigma_z(11)\}$ on her qubit. After performing one of the unitary operations the state transforms to one of the following states

$$\begin{aligned}
I : \rho_I^{ABC} &= \frac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] + \frac{(1-p)^2}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|],\\
\sigma_x : \rho_X^{ABC} &= \frac{1}{2}[|100\rangle\langle 100| + |011\rangle\langle 011|] + \frac{(1-p)^2}{2}[|100\rangle\langle 011| + |011\rangle\langle 100|],\\
i\sigma_y : \rho_Y^{ABC} &= \frac{1}{2}[|100\rangle\langle 100| + |011\rangle\langle 011|] - \frac{(1-p)^2}{2}[|100\rangle\langle 011| + |011\rangle\langle 100|],\\
\sigma_z : \rho_Z^{ABC} &= \frac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] - \frac{(1-p)^2}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|].
\end{aligned} \tag{5}$$

Then Alice sends her qubit to Bob through the same phase-damping channel, described by the channel parameter p. Bob now has two qubits with him while the third qubit is with Charlie. As a result, the three-qubit density operators representing the above states reduce to the states

$$\begin{aligned}
\rho_1^{BBC} &= \frac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] + \frac{(1-p)^3}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|],\\
\rho_2^{BBC} &= \frac{1}{2}[|100\rangle\langle 100| + |011\rangle\langle 011|] + \frac{(1-p)^3}{2}[|100\rangle\langle 011| + |011\rangle\langle 100|],\\
\rho_3^{BBC} &= \frac{1}{2}[|100\rangle\langle 100| + |011\rangle\langle 011|] - \frac{(1-p)^3}{2}[|100\rangle\langle 011| + |011\rangle\langle 100|],\\
\rho_4^{BBC} &= \frac{1}{2}[|000\rangle\langle 000| + |111\rangle\langle 111|] - \frac{(1-p)^3}{2}[|000\rangle\langle 111| + |111\rangle\langle 000|].
\end{aligned} \tag{6}$$

Step III: Charlie performs single qubit measurement

After receiving the particle from Alice, Bob has two particles at his disposal. But, it is not possible either for Bob or for Charlie independently to decode the information encoded by Alice. However, Bob can decode the secret if Charlie is willing to help him. Charlie co-operates by conveying his measurement outcomes. Charlie performs a measurement on his qubits in the basis $\{|+\rangle = \alpha|0\rangle + \beta|1\rangle, |-\rangle = \beta|0\rangle - \alpha|1\rangle\}$, (where $\alpha^2 + \beta^2 = 1$). As a result of this measurement, the state that collapses on Bob's side are given by the following table.

TABLE II:

Secret Encoded	State shared by Bob and Charlie	Charlie's Measurement Outcomes	Qubits at Bob's side
$I(00)$	ρ_1^{BBC}	$\|+\rangle$ $\|-\rangle$	ρ_1^{BB+} ρ_1^{BB-}
$\sigma_x(01)$	ρ_2^{BBC}	$\|+\rangle$ $\|-\rangle$	ρ_2^{BB+} ρ_2^{BB-}
$i\sigma_y(10)$	ρ_3^{BBC}	$\|+\rangle$ $\|-\rangle$	ρ_3^{BB+} ρ_3^{BB-}
$\sigma_z(11)$	ρ_4^{BBC}	$\|+\rangle$ $\|-\rangle$	ρ_4^{BB+} ρ_4^{BB-}

where

$$\begin{aligned}
\rho_1^{BB+} &= \alpha^2|00\rangle\langle 00| + \beta^2|11\rangle\langle 11| + \alpha\beta(1-p)^3(|11\rangle\langle 00| + |00\rangle\langle 11|),\\
\rho_1^{BB-} &= \beta^2|00\rangle\langle 00| + \alpha^2|11\rangle\langle 11| - \alpha\beta(1-p)^3(|11\rangle\langle 00| + |00\rangle\langle 11|),\\
\rho_2^{BB+} &= \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| + \alpha\beta(1-p)^3(|01\rangle\langle 10| + |10\rangle\langle 01|),\\
\rho_2^{BB-} &= \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| - \alpha\beta(1-p)^3(|01\rangle\langle 10| + |10\rangle\langle 01|),\\
\rho_3^{BB+} &= \alpha^2|10\rangle\langle 10| + \beta^2|01\rangle\langle 01| - \alpha\beta(1-p)^3(|01\rangle\langle 10| + |10\rangle\langle 01|),\\
\rho_3^{BB-} &= \beta^2|10\rangle\langle 10| + \alpha^2|01\rangle\langle 01| + \alpha\beta(1-p)^3(|01\rangle\langle 10| + |10\rangle\langle 01|),\\
\rho_4^{BB+} &= \alpha^2|00\rangle\langle 00| + \beta^2|11\rangle\langle 11| - \alpha\beta(1-p)^3(|11\rangle\langle 00| + |00\rangle\langle 11|),\\
\rho_4^{BB-} &= \beta^2|00\rangle\langle 00| + \alpha^2|11\rangle\langle 11| + \alpha\beta(1-p)^3(|11\rangle\langle 00| + |00\rangle\langle 11|). \qquad (7)
\end{aligned}$$

Charlie sends his results to Bob through a classical channel by spending one classical bit. This is done by encoding 0 for $|+\rangle$ and 1 for $|-\rangle$ respectively.

Step IV: Bob performs two qubit projective measurement and POVM

As we see in the above table when Charlie's measurement result is $|+\rangle$ then Bob can have one of the four possible states $\rho_1^{BB+}, \rho_2^{BB+}, \rho_3^{BB+}, \rho_4^{BB+}$. Similarly when Charlie's qubit collapses into the state $|-\rangle$, Bob can have any one of the state four possible states $\rho_1^{BB-}, \rho_2^{BB-}, \rho_3^{BB-}, \rho_4^{BB-}$ at his disposal.

If Charlie sends 0, then Bob guesses that the two qubit states in his possession would be either ρ_1^{BB+} or ρ_2^{BB+} or ρ_3^{BB+} or ρ_4^{BB+}. He then performs projective measurements $P_1 = |00\rangle\langle 00| + |11\rangle\langle 11|$ and $P_2 = |01\rangle\langle 01| + |10\rangle\langle 10|$ to get close to identify the secret. The projectors P_1 and P_2 classify the above four states into two classes as $C_1 = \{\rho_1^{BB+}, \rho_4^{BB+}\}$ and $C_2 = \{\rho_2^{BB+}, \rho_3^{BB+}\}$ respectively. The states within the two classes are now lying in a two dimensional subspace spanned by $\{|00\rangle, |11\rangle\}$ and $\{|01\rangle, |10\rangle\}$ respectively.

After classifying the states, Bob performs optimal POVM to identify the state in which secret is encoded. First of all he considers the class $C_1 = \{\rho_1^{BB+}, \rho_4^{BB+}\}$ and constructs the optimal POVM operators Π_1, Π_2 for discriminating the density matrices present in the class. The optimal POVM measurement is the one that minimizes the error rate

$$E_R = \frac{1}{2}[Tr[\Pi_1 \rho_4^{BB+}] + Tr[\Pi_2 \rho_1^{BB+}]. \tag{8}$$

subject to the constraints that they forms a complete set of projectors (i.e $\Pi_1 + \Pi_2 = I$) [19].

The optimal POVM elements are

$$\Pi_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \Pi_2 = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}. \tag{9}$$

and the error rate in discriminating the states ρ_1^{BB+} and ρ_4^{BB+} is [19]

$$E_R = \frac{1}{2}(1 - 2\alpha\beta(1-p)^3). \tag{10}$$

Similarly, Bob can distinguish the mixed states belonging to the other class $C_2 = \{\rho_2^{BB+}, \rho_3^{BB+}\}$ by using the same set of POVM operators Π_1 and Π_2. The error rate E_R in this case will also be the same. Therefore the total probability of success in distinguishing these states is

$$P_S = 2\alpha\beta(1-p)^3. \tag{11}$$

In such a situation, the total number of classical bits that Bob can extract are

$$B = 1 + 2\alpha\beta(1-p)^3. \tag{12}$$

Clearly, the amount of classical information that can be extracted by Bob will depend upon the channel noise (p) and also on the basis that Charlie uses for the measurement. We note that when $p = 1$, the channel is totally noisy, and Bob can extract at most one classical bit. This can also be seen from Figure 1. B is independent of α and is always equal to 1 when $p = 1$. The limit $p = 0$ corresponds to the case when there is no noise. In this case, B is maximum when measurement has been done in the Hadamard basis (i.e $\alpha = \beta = \frac{1}{\sqrt{2}}$). This is also clear from the Figure 1. In general, B have the largest value when Charlie makes his measurement in Hadamard basis. In such a scenario

$$B = 1 + (1-p)^3. \tag{13}$$

In Figure 2, we have plotted B as a function of the channel parameter (p). It takes maximum value 2 when $p = 0$ and the minimum value 1 when $p = 1$.

Thus we see that deterministic secret sharing is not possible with a phase-damping channel. We also find that the amount of classical information decoded by Bob is dependent on the noise parameter (p) and also on the choice of basis. In a practical situation when we carry out quantum information processing task we face the decoherence problem and we always have mixed state at our disposal. As a consequence of which the tasks which can be done deterministically in case of pure states, can not be done so for the mixed states.

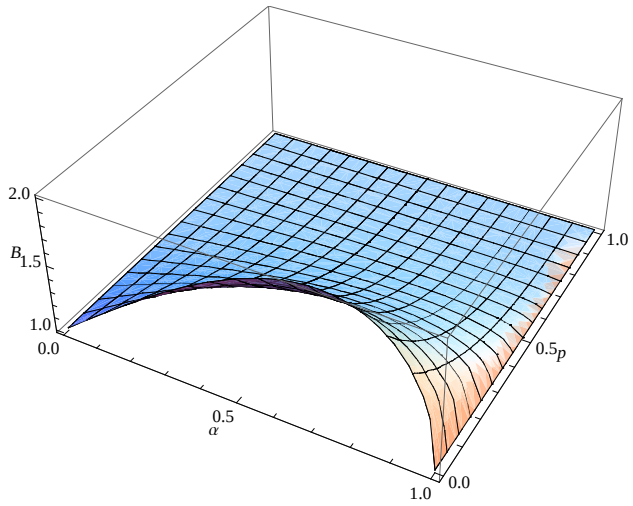

Fig. 1. B (the classical bits decoded by Bob) is plotted against the parameters α and p.

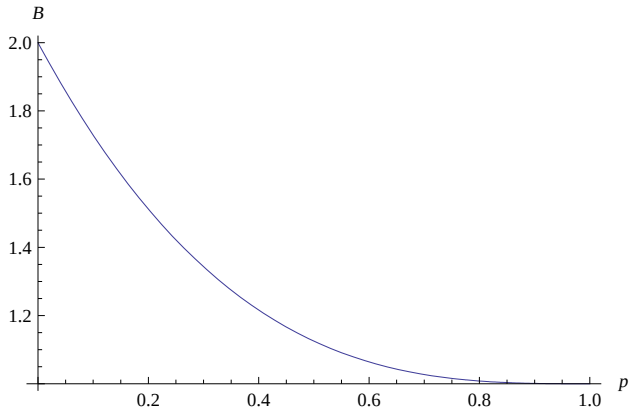

Fig. 2. B (the classical bits decoded by Bob) is plotted against the channel parameter p when the measurement is done in the Hadamard basis.

4 Discussion and Conclusions

In this paper, we have introduced a protocol for secret sharing which is different from the existing secret sharing schemes. We have considered a realistic scenario where there are noisy quantum channels. In such a scenario, the deterministic secret sharing is not possible. We consider POVM measurements to implement our protocol and find out the number of classical bits that Alice can share with Bob with the help of Charlie. The answer is $1+(1-p)^3$ classical bits with p characterizing the noisy channel. The earlier scheme of secret sharing with pure GHZ state was more like cooperative teleportation while our scheme of secret sharing is like cooperative dense coding. The three-qubit mixed state considered here is generated by passing the qubits through noisy channels. In particular, we have shown how the phase-damping noisy channel generated three-qubit mixed state can be used in our secret sharing protocol.

Now it would be important to ask that whether our secret sharing scheme succeeds only when the noisy channel is a phase-damping channel. Indeed the answer is 'no'. We find that if phase-flip channel is the noisy channel, then our secret sharing scheme would succeed. However, one needs to explore further if the secret sharing scheme can succeed with noisy channels like amplitude-damping channel, depolarizing channel, bit-flip channel, bit-phase flip channel or two Pauli channels. In the case of phase-damping and phase-flip channels, the Kraus operators are diagonal and it is not difficult to construct appropriate POVM operators. We also note that these channels are related by unitary transformations. Therefore, it appears that our proposed protocol would succeed if the noisy channel is related to phase-damping channel by a unitary transformation. The reason behind the success of our protocol may be the diagonal form of the Kraus operators that represent the noisy channels. The cases of other noisy channels that are described by the Kraus operators with off-diagonal elements may involve loss of energy and need further exploration. In these cases, probabilistic secret sharing may be possible with more complicated POVM measurements.

Acknowledgements

We would like to thank Dr. S. Bandopadhyay and Dr. R. Srikanth for their useful comments.

References

1. A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).
2. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993); D. Bouwmeester, J-W Pan, K. Mattle, M. Eibl, H. Weinfurter and A. Zeilinger, Nature **390**, 575 (1997).
3. N. Gisin, G. Ribordy, W. Tittel, and H.Zbinden, Rev. Mod. Phys. **74**, 145 (2002)
4. M. Hillery, V. Buek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999);R. Cleve, D. Gottesman, and H-K. Lo, Phys. Rev. Lett. **83**, 648 (1999).
5. A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999).
6. S. Bandyopadhyay, Phys. Rev. A **62**, 012308 (2000);
7. S. Bagherinezhad, and V. Karimipour, Phys. Rev. A **67**, 044302 (2003).
8. A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, Phys. Rev. Lett. **92**, 177903 (2004).
9. G. Gordon, and G. Rigolin, Phys. Rev. A
10. S. B. Zheng, Phys. Rev. A **74**, 054303 (2006).
11. A. Keet, B. Fortescue, D. Markham, B. C. Sanders, Phys. Rev. A **82**, 062315 (2010)

12. Q. Li, W. H. Chan, and D-Y Long, Phys. Rev. A **82**, 022303 (2010).
13. S. Adhikari, Quantum secret sharing with two qubit bipartite mixed states, arXiv:1011.2868.
14. W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **63**, 042301 (2001).
15. C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
16. C. Schmid, P. Trojek, S. Gaertner, M. Bourennane, C. Kurtsiefer, M. Zukowski, and H. Weinfurter, Fortschritte der Physik **54**, 831 (2006).
17. J. Bogdanski, N. Rafiei, and M. Bourennane, Phys. Rev. A **78**, 062307 (2008).
18. L. Xian-Ting, Commun. Theor. Phys. (Beijing, China) **39** 537 (2003).
19. M.Jezek. Phys. Lett. A **299** 441 (2002).