Tatra Mt. Math. Publ. **33** (2006), 71–74

TATRA MOUNTAINS
Mathematical Publications

NON-THRESHOLD QUANTUM INFORMATION SPLITTING SCHEME

Andrzej Grudka — Antoni Wójcik

ABSTRACT. We propose a protocol for the quantum state splitting among n parties. Our protocol enables to recover this state provided that all n parties cooperate. On the other hand if only m of n parties cooperate, the state cannot be recovered perfectly. Fidelity of the recovered state is shown to be a monotonically increasing function of m/n.

Secret sharing is a cryptographic protocol enabling splitting a message among n parties in such a way that the cooperation of parties is the necessary and sufficient condition to recover it. The existence of the threshold m guarantees that less than m parties cannot gain any information about the message. Recently, some groups proposed quantum versions of secret sharing [1-7]. Both classical information and quantum information (quantum state) proposed in the scheme can be split among many parties. Some of these schemes have been already realized experimentally [8, 9].

In this note we propose a novel scheme of quantum information splitting. Its novelty relies on the fact that accessibility of information does not depend on the number of cooperators in a threshold way but in a smooth way. Let us suppose that one party has quantum information in the form of single qubit in the state $|\psi\rangle = a|0\rangle + b|1\rangle$. In addition it has $n-1$ auxiliary qubits, all in the state. Thus the state of the whole system is given by $|\Psi\rangle = (a|0\rangle + b|1\rangle)|00\ldots0\rangle$. The information splitting starts with transforming the state $|\Psi\rangle$ by the unitary operation U according to

$$U|\Psi\rangle = a|00\ldots0\rangle + \frac{b}{\sqrt{n}}\big(|10\ldots0\rangle + |01\ldots0\rangle + \cdots + |00\ldots1\rangle\big)\,. \tag{1}$$

In the second step all qubits are sent to n parties (one qubit to one party). The information which can be accessed by a single party is described by the density matrix

$$\rho_1 = \begin{pmatrix} 1 - \frac{1}{n}|b|^2 & \frac{1}{\sqrt{n}}ab^* \\ \frac{1}{\sqrt{n}}a^*b & \frac{1}{n}|b|^2 \end{pmatrix}. \tag{2}$$

2000 Mathematics Subject Classification: 81P68.
Keywords: quantum cryptography.

The above expression should be compared with the density matrix for a qubit in the state $|\psi\rangle$, i.e.,

$$\rho = \begin{pmatrix} 1-|b|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix} . \tag{3}$$

One sees that the elements of the density matrix ρ_1 are suppressed to a degree dependent on n. In the limit of large n we have

$$\rho_1 \to \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} , \tag{4}$$

where all the information present in the amplitudes a and b is erased. It is quite easy to recover the desired state $|\psi\rangle$ provided that all n parties gather together, and perform the unitary operation U^{-1} on the state $|\Psi_n\rangle$. Obviously $U^{-1}|\Psi_n\rangle = |\Psi\rangle$. On the other hand if only m of n parties cooperate, the best they can do is to transfer all the available information into one arbitrary chosen qubit. This can be done if there exists unitary operator which transforms the remaining $m-1$ qubits into some standard state (e.g., $|00\ldots0\rangle$). One can check that the unitary operator U_m defined as

$$U_m|\Psi_n\rangle = |\Psi_n^m\rangle = \left(a|0\rangle + \sqrt{\tfrac{m}{n}}\, b|1\rangle\right)|00\ldots0\rangle|00\ldots0\rangle + \sqrt{\tfrac{m-n}{n}}\, b|0\rangle|00\ldots0\rangle|\Phi\rangle , \tag{5}$$

where $|\Phi\rangle$ is some state of $n-m$ qubits orthogonal to $|00\ldots0\rangle$, fulfils the above condition. The reduced density matrix of the first qubit is

$$\rho_m = \begin{pmatrix} 1-\frac{m}{n}|b|^2 & \sqrt{\frac{m}{n}}ab^* \\ \sqrt{\frac{m}{n}}a^*b & \frac{m}{n}|b|^2 \end{pmatrix} . \tag{6}$$

In order to compare the state ρ_m to the original one we calculate the fidelity F defined as $\langle\psi|\rho_m|\psi\rangle$. It should be noted that the fidelity equal to $1/2$ corresponds to randomly chosen state, and the fidelity equal to 1 corresponds to perfectly recovered state. After simple algebra one obtains

$$F = 1 - \left(1 - 2\sqrt{\frac{m}{n}} + \frac{m}{n}\right)|b|^2 + 2\left(\frac{m}{n} - \sqrt{\frac{m}{n}}\right) . \tag{7}$$

One sees that the fidelity depends on the state to be split (via the amplitude b) and the fraction of cooperating parties. It will be useful to average the fidelity $\langle F\rangle$ over possible states. Density of states can be expressed in a simple form $\frac{1}{4\pi}\sin\theta$, provided that the state will be written in the form $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\phi}|1\rangle$, where θ varies from 0 to π, and ϕ varies from 0 to 2π. For the average fidelity defined as $\langle F\rangle = \frac{1}{4\pi}\int_0^\pi\int_0^{2\pi} F\sin\theta\, d\theta\, d\phi$ one obtains

$$\langle F\rangle = 1 - \frac{1}{2}\left(1 - \sqrt{\frac{m}{n}}\right)^2 + \frac{2}{3}\sqrt{\frac{m}{n}}\left(\sqrt{\frac{m}{n}} - 1\right) . \tag{8}$$

In Fig. 1 we present the average fidelity $\langle F \rangle$ versus the fraction of cooperating parties. One sees that the greater number of cooperating parties the better the state recovery.

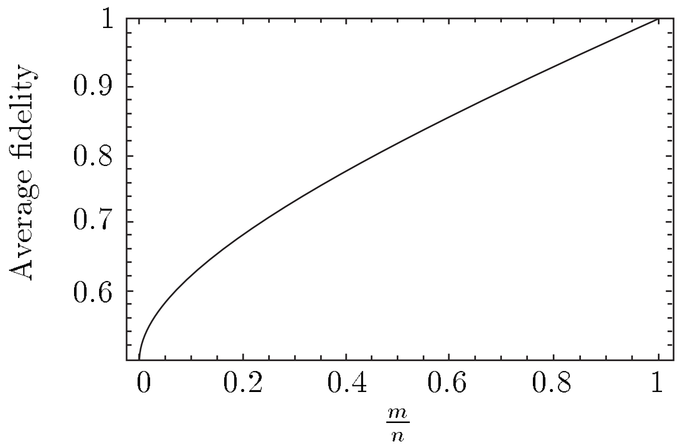

FIGURE 1. Average fidelity $\langle F \rangle$ versus the fraction of cooperating parties.

We would like to thank the *State Committee for Scientific Research* for financial support under grant no. 0 T00A 003 23. We would also like to thank Jerzy Jaworski for motivation.

REFERENCES

[1] CLEVE, R.—GOTTESMAN, G.—LO, H. K.: *How to share a quantum secret*, Phys. Rev. Lett. **83** (1999), 648–651.

[2] KARLSSON, A.—KOASHI, M.—IMOTO, N.: *Quantum entanglement for secret sharing and secret splitting*, Phys. Rev. **A 59** (1999), 162–168.

[3] HILLERY, M.—BUŽEK, V.—BERTHIAUME, A.: *Quantum secret sharing*, Phys. Rev. **A 59** (1999), 1829–1834.

[4] BANDYOPADHYAY, S.: *Teleportation and secret sharing with pure entangled states*, Phys. Rev. **A 62** (2000), 012308–7.

[5] BAGHERINEZHAD, S.—KARIMIPOUR, V.: *Quantum secret sharing based on reusable Greenberger-Horne-Zeilinger states as secure carriers*, Phys. Rev. **A 67** (2003), 044302–4.

[6] HSU, L. Y.: *Quantum secret-sharing protocol based on Grover's algorithm*, Phys. Rev. **A 68** (2003), 022306–4.

[7] XIAO, L.—LONG, G. L.—DENG, F. G.—PAN, J. W.: *Efficient multiparty quantum--secret-sharing schemes*, Phys. Rev. **A 69** (2004), 052307–5.

[8] TITTEL, W.—ZBINDEN, H.—GISIN, N.: *Experimental demonstration of quantum secret sharing states*, Phys. Rev. **A 64** (2001), 042301–6.

[9] LANCE, A. M.—SYMUL, T.—BOWEN, W. P.—SANDERS, B. C.—LAM, P. K.: *Tripartite quantum state sharing*, Phys. Rev. Lett. **92** (2004), 177903.

Received November 15, 2004

Quantum Electronic Laboratory
Faculty of Physics
Adam Mickiewicz University
Umultowska 85
PL–61-614 Poznań
POLAND

E-mail: andrzej.grudka@amu.edu.pl
antwoj@amu.edu.pl