Review of: "Standard (3, 5)-threshold quantum secret sharing by maximally entangled 6-qubit states"

Ebrahim Ghasemian

Potential competing interests: The author(s) declared that no potential competing interests exist.

The authors presented a theoretical scheme for standard quantum secret sharing wherein three of five participants can resume cooperatively the classical secret from the dealer, but one or two shares contain absolutely no information about the secret.

They evaluated the scheme's security by considering different approaches such as the intercept-and-resend attack and entangle-and-measure attack.

The paper contains some original ideas and interesting results, but I have some questions and criticisms.

%

1- My first criticism regarding this paper is the issues corresponding to the clarity of explanation.

The authors are suggested to provide more explanations and not assume that the readers can read their minds.

In particular, the paper contains a detailed review of the previous works, but some of the results have been presented without any explanation.

For instance on pages 3 and 4, the authors did some Schmidt decomposition without any explanation about the obtained results.

Also, Ψ_{6qb} was not defined (6-qubit entangled state!). Also, it is not clear why they chose these particular Schmidt decompositions.

The authors should provide at least a reference for the BPB state.

2- The authors stated that "It is worth pointing out, to fulfil the task, only specific two users(e.g., Bob2 and Bob4 in the example above), instead of any two users, can be chosen to unite to make measurement with Bell basis."

Isn't this issue a drawback for the presented scheme to be restricted to only specific two users?

Hence, it is expected the authors justify their model according to practical implementations.

Also, as can be found, the paper contains some misprints and grammar mistakes.

For instance, see the above expression and the following cases.

- to fulfil the task

Moreover, "only specific two users" or "only two specific users" which one do the authors prefer?

3- The scheme has been established based on photon decoy, so it is an ideal model. The main issue regarding such schemes is photon loss.

What is the effect of dissipation effect on the secret sharing process?

Is it possible to overcome or mitigate this issue?

4- I failed to find any realistic connection with experiments. Even though simple, minimalist models could be in principle a useful tool to

capture some gross features of experiments or more realistic models, there is no attempt

in the manuscript to make any comparison between the formulas obtained therein and

experimental or numerical data.

Is there any experimental proof that such a scheme can be implemented in practice?

5- So far, several protocols based on decoy states have been implemented for quantum key distribution (QKD). Practical QKD systems use multi-photon sources, in contrast to the standard BB84 protocol, making them susceptible to photon number splitting attacks. This would significantly limit the secure transmission rate or the maximum channel length in practical QKD systems. In decoy state technique, this fundamental weakness of practical QKD systems is addressed by using multiple intensity levels at the transmitter's source.

So a key point that should be addressed is that why the authors used the decoy photon technique. What are the advantages/drawbacks of the techniques used for quantum secret sharing?

6- The authors presented a brief comparison of the various existing standard TQSS schemes. It would be of interest to discuss their advantages/drawbacks.

Which one is more efficient in practice?