09 New secrets threaten past secrets

- Vulnerability assessment of quantum secret sharing-

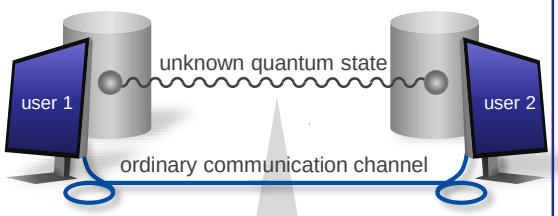
Abstract

We investigate a counter-intuitive phenomenon of quantum state discrimination that the success probability of identifying all the unknown quantum states increases even when the number of unknown states increases. The phenomenon is known for vulnerability of quantum secret sharing (QSS), which enables one to distribute a secret amongst untrusted participants securely, however, the necessary and sufficient condition for the phenomenon was unknown. We show the condition for a specific discrimination task and construct a practical method to realize the phenomenon. These results advance the analysis of the phenomenon and reveal the vulnerability of QSS. Since quantum state discrimination lies at the heart of many quantum information processing tasks, our research widely contributes to the future information society based on quantum technologies, where people would obtain the benefits from genuine quantum information processing.

Quantum state discrimination

1. Distribute a randomly chosen quantum state to two users

2. The users try to identify the state by using an ordinary communication channel



Suppose the quantum state is randomly chosen from four Bell states (standard and useful quantum states)

Bell 1
Bell 2
Bell 3
Bell 4

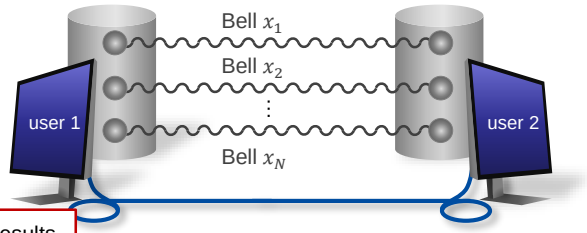
Bell x

Success probability of the identification< 1

Discrimination of independent Bell states

1. Distribute randomly chosen Bell states to two users

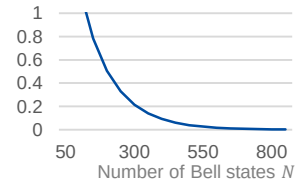
2. The users try to identify all the states $x_1, x_2, \cdots, x_N$ by using an ordinary communication channel



Main Results

(i) Entropy of the randomness> 1

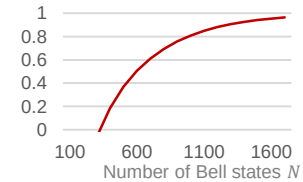
Upper bound of the success probability



Fail the identification no matter how well one identify

(ii) Entropy of the randomness < 1

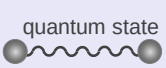
Lower bound of the success probability



Succeed the identification with a practical method

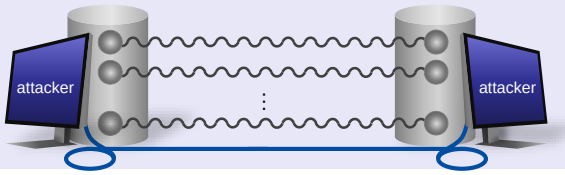
Vulnerability assessment of QSS

1. Distribute quantum states each of which encodes secret x to two users



Bell 1 if $x = 1$
Bell 2 if $x = 2$
Bell 3 if $x = 3$
Bell 4 if $x = 4$

2. Attacking users try to read secret $x_1, x_2, \cdots, x_N$ by identifying the distributed quantum states



Main results → The more secrets one distribute to attacking users, the more vulnerable the secrets become

References

[1] S. Akibue, G. Kato, "Bipartite discrimination of independently prepared quantum states as a counterexample to a parallel repetition conjecture," *Physical Review A*, Vol. 97, No. 10, 042309, 2018.

Contact

Seiseki Akiube Email: cs-liaison-ml at hco.ntt.co.jp Computing Theory Research Group, Media Information Laboratory

Innovative R&D by NTT

Open House 2019