Physicists show that it is impossible to mask quantum information in correlations

June 21 2018, by Lisa Zyga

Credit: Photo by Rafael Guajardo, Pexels.com

Information is typically stored in physical systems, such as memory devices. But in a new study, physicists have investigated an alternative way to store and hide information, which is by storing it only in the quantum correlations among two or more systems, rather than in the systems themselves. This idea, which is called "masking," is a way of making the information inaccessible to everyone, without destroying it (as destroying quantum information is impossible).

Although previous research has shown that it's possible to mask classical information, in the new study the physicists show that masking quantum information for two systems is impossible in general, with certain exceptions. The results highlight an important difference between classical and quantum information, and—due to the exceptions—may lead to potential applications for secretly sharing quantum information.

The physicists, Kavan Modi at Monash University in Australia, along with Arun Kumar Pati, Aditi Sen(De) and Ujjwal Sen at the Harish-Chandra Research Institute in India, have published a paper on the impossibility of masking quantum information in a recent issue of *Physical Review Letters*.

No masking

"Quantum information differs from classical information in many ways," Pati told *Phys.org*. "Researchers have pondered over this question since the early days of quantum information and have come up with several important no-go results, such as the no-cloning, the no-deleting, and the no-hiding theorems." (In 2007, Pati and coauthor Samuel Braunstein proved the no-hiding theorem.)

As their names suggest, these no-go theorems prohibit the cloning, deleting, and hiding of quantum information—all operations which are allowable for classical information. The difference occurs because the no-go theorems arise directly from the fundamental laws of quantum mechanics and so have no classical counterparts, which suggests that quantum information is in a sense more robust than classical information.

The new study adds another no-go theorem to the list: the no-masking theorem. The physicists proved that it is impossible to map quantum information (in the form of quantum states) from one physical system, A, to the quantum correlations between A and a second physical system, B, in such a way that neither A nor B contain that information. That is, it is not possible to completely store quantum information in the correlations, in a sense "spreading it out" between the two systems.

"In the masking process, we ask the question: If quantum information is not there either in the subsystem A or in the subsystem B, can that information remain only in the quantum correlations, which Einstein called the 'spooky' correlations?" Modi said. "Masking has more to do with complete shielding of information in both the subsystems such that it is not possible to read out by either A or B. Then, we prove that if quantum information is blind to both the subsystems A and B, and we want to keep the information concealed only in the spooky correlations, then that is not allowed by quantum mechanics."

Notable exceptions

Although the no-masking theorem holds for arbitrary quantum states, the physicists also show that a surprisingly large number of special quantum states are maskable. Similar exceptions exist for the no-cloning and no-deleting theorems, where likewise cloning and deleting is possible for certain quantum states, such as orthogonal states. Together, these findings show just how blurry the boundary is between quantum and classical information.

A further caveat of the no-masking theorem is that it holds only for two systems. When a third system is included, the physicists show that masking may be possible for any arbitrary quantum state. However, the scientists note that there are ways to get around this masking, at least partially.

"Collusion between any two of the parties can reveal part of the masked quantum information by using a strategy called error correction codes, which deals with encoding quantum information in multipartite states," Sen said.

Impossibility implications

One implication of the new results is that they show that it's impossible to design a "qubit commitment protocol," which generalizes the famous results for "no bit commitment." This line of research addresses the question of whether it's possible for one party to commit to choosing the state of a bit (0 or 1) or—in the new result—a qubit (0, 1, or a superposition of both). Previous studies have shown that commitment is impossible for bits, and the new study now adds that it's impossible for qubits as well. This means that someone can always cheat by pretending to choose a qubit state, but then switching. As the physicists explain, the no-bit/qubit commitment results have important implications for designing secure quantum communication protocols.

"One of the most important implications of the no-masking theorem is that this leads to a new impossibility result, namely, the no-qubit commitment," Pati said. "Since it is not possible to conceal information only in the correlations, it is impossible to make Alice and Bob blind to the quantum information. In other words, two parties cannot be blind at the same time, if quantum information is encoded in joint bipartite states. One can be blind, but not both. In either case, information cannot be kept secret only in the correlations. This is stronger than the no-bit commitment protocol."

In the future, the physicists plan to further investigate the no-masking theorem and its exceptions—the maskable sets and the partial maskers.

"This may prove useful for designing quantum information protocols that require hiding and secretly sharing quantum information," Sen(De) said.

More information: Kavan Modi et al. "Masking Quantum Information is Impossible." Physical Review Letters. DOI: 10.1103/PhysRevLett.120.230501

© 2018 Phys.org

Citation: Physicists show that it is impossible to mask quantum information in correlations (2018, June 21) retrieved 23 April 2024 from https://phys.org/news/2018-06-physicists-impossible-mask-quantum.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.