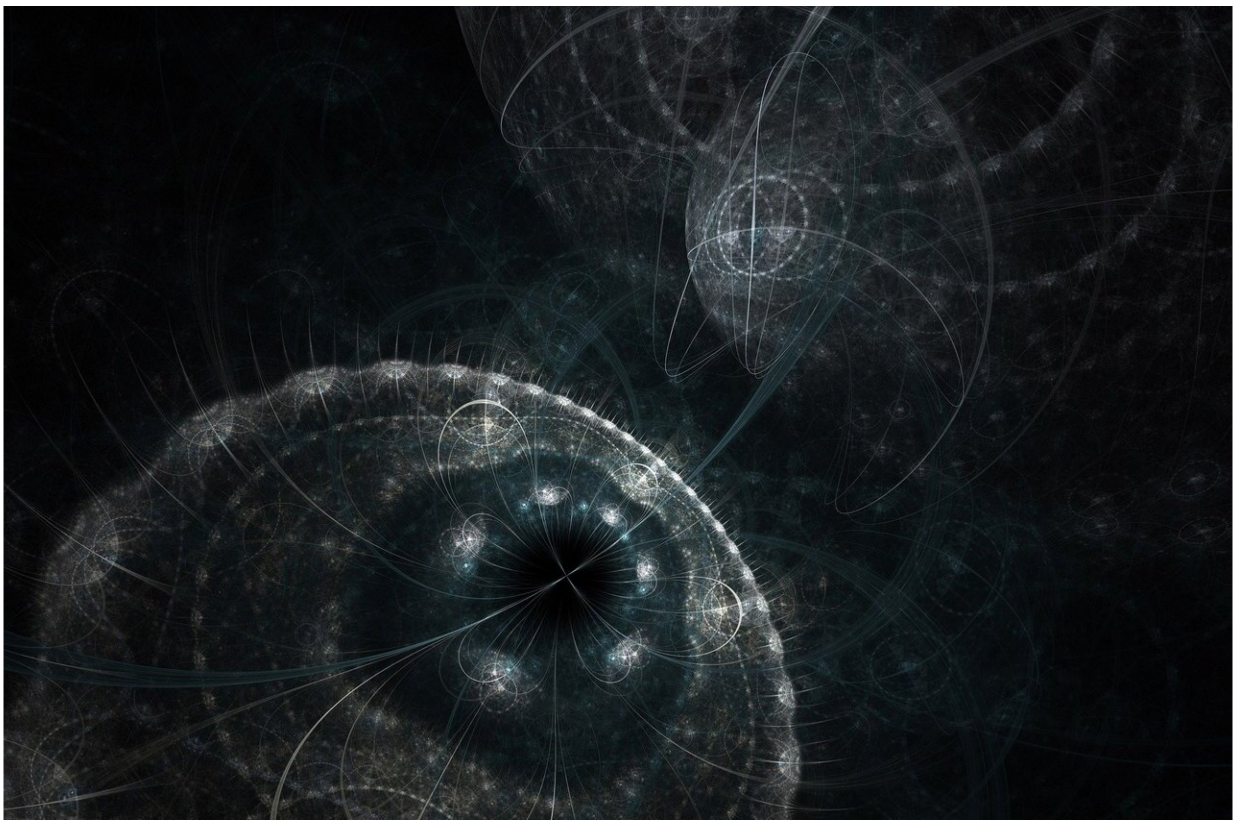
Quantifying how much quantum information can be eavesdropped

January 28 2019



Credit: CC0 Public Domain

Summary The most basic type of quantum information processing is quantum entanglement. In a new study published in *EPJ B*, Zhaonan Zhang from Shaanxi Normal University, Xi'an, China, and colleagues

have provided a much finer characterisation of the distributions of entanglement in multi-qubit systems than previously available. These findings can be used in quantum cryptography to estimate the quantity of information an eavesdropper can capture regarding the secret encryption key.

Encrypted communication is achieved by sending quantum information in basic units called quantum bits, or qubits. The most basic type of quantum information processing is quantum entanglement. However, this process remains poorly understood. Better controlling quantum entanglement could help to improve quantum teleportation, the development of quantum computers, and quantum cryptography. Now, a team of Chinese physicists have focused on finding ways to enhance the reliability of quantum secret sharing. In a new study published in EPJ B, Zhaonan Zhang from Shaanxi Normal University, Xi'an, China, and colleagues provide a much finer characterisation of the distributions of entanglement in multi-qubit systems than previously available. In the context of quantum cryptography, these findings can be used to estimate the quantity of information an eavesdropper can capture regarding the secret encryption key.

Physicists working on new ways of securing quantum encrypted messages are exploiting the fact that, at the quantum scale, a given qubit can only be entangled with one other qubit; this unique trait is referred to as monogamy of entanglement. In practical terms, the quantum rules for entanglement are explained by considering three qubits, called A, B and C, belonging to Alice, Bob and Charlie, respectively. If Alice and Bob share quantum information via a two-qubit system, called AB, they cannot share any entangled states with Charlie's qubit C.

However, there is also another kind of entanglement, called polygamy, in which qubits display partial entanglement with several qubits at the same time.

In this study, the authors develop a series of equations explaining the conditions for monogamy and polygamy, which are much better characterised than previous work. Specifically, they first investigate three-qubit systems under certain restrictions and then derive a general result for multi-qubit systems.

More information: Zhaonan Zhang et al, Tighter monogamy and polygamy relations in multiqubit systems, *The European Physical Journal D* (2019). DOI: 10.1140/epjd/e2018-90563-2

Provided by Springer