Variational quantum cloning machine on a photonic integrated interferometer: trying to answer to some questions

G. Bertelli, D. Di Gregorio, F. Fissore, E. Ricci

Münich PushQuantum Hackathon, 28 nov – 01 dec 2024

1 Quantum Key Distribution (QKD) and Attacks Using Variational Cloning Machines

Quantum Key Distribution (QKD) protocols enable secure communication between two parties, Alice and Bob, by allowing them to exchange cryptographic keys over an insecure channel. The security of QKD relies on quantum principles, especially the *no-cloning theorem*, which asserts that it is impossible to perfectly copy an unknown quantum state. However, certain quantum states can be cloned with high fidelity using *variational cloning machines*, posing a potential threat to QKD.

Variational Cloning Machines are quantum devices designed to replicate quantum states. The *symmetric phase-covariant cloner*, in particular, works on states that lie on the equator of the Bloch sphere, where the states are parameterized by a phase ϕ. These states are of the form:

$$|\psi_\phi\rangle = \cos(\theta)|0\rangle + \sin(\theta)e^{i\phi}|0\rangle$$

The goal of the cloner is to generate two copies of the input state with high fidelity, ensuring that the quantum information is accurately replicated. The machine is designed to be *phase-covariant*, meaning it works for any phase ϕ, producing the same result regardless of the phase difference.

QKD protocols, such as $BB84$ and $B92$, rely on the transmission of quantum states that are inherently fragile: any attempt by an eavesdropper (Eve) to measure or copy these states causes detectable disturbances. However, a *variational phase-covariant cloner* could be used by an adversary to clone the quantum states exchanged between Alice and Bob without introducing detectable errors. If Eve is able to create high-fidelity clones of the quantum states, she can measure them and potentially extract information about the shared secret key without detection.

The phase-covariant cloner is particularly dangerous for QKD because it is optimized to replicate quantum states that differ only by their relative phase.

This capability allows Eve to bypass security mechanisms that depend on the *no-cloning theorem*. If Eve can perform cloning operations across all possible phases ϕ, she could potentially clone quantum states without disturbing them, thus evading detection in protocols where key security relies on the ability to detect eavesdropping.

The case of the $E91$ protocol

The $E91$ protocol may appear to be the most secure, but in reality, it is still vulnerable to quantum cloning attacks. Indeed, a variational cloning machine could attack the E91 protocol by intercepting the entangled photon pairs, cloning them with high fidelity, and then measuring the clones to extract the secret key. The variational cloning machine could be used by Eve to clone the quantum states of the entangled photons she intercepts. The symmetric phase-covariant cloner is particularly dangerous because it is designed to clone quantum states that differ only by phase. Since entangled photons in the E91 protocol often involve polarization states that are parameterized by a phase angle, Eve could use the cloning machine to replicate the quantum states of the photons with high fidelity. The ability of a phase-covariant cloner to replicate quantum states without disturbing them could potentially allow Eve to circumvent the usual security mechanisms of the E91 protocol, which rely on detecting disturbances caused by eavesdropping. This highlights the potential vulnerability of quantum key distribution protocols to advanced cloning techniques, even in the presence of quantum entanglement.

Conclusions

In summary, while QKD protocols are designed to secure communication by ensuring that any interference with the quantum states is detectable, variational cloning machines like the *symmetric phase-covariant cloner* could potentially undermine this security by cloning quantum states with high fidelity, allowing undetected eavesdropping.

2 Quantum Cloning as a resource for Quantum Memory development

Though exact cloning is forbidden, approximate quantum cloning involves transferring quantum information from one state to another (often using a quantum channel). This idea can inspire new approaches to quantum memory. One area of quantum cloning research involves *entanglement swapping*, which is a technique that allows for the transfer of entanglement between quantum systems. This concept can be used in the development of quantum memory systems by transferring quantum states from one memory location to another through entanglement. This would allow for more flexible and robust memory architectures. In quantum memory, entanglement is often used to encode and store information. If quantum cloning techniques can help transfer or "swap" entanglement across different quantum memory nodes, it could lead to more scalable and efficient storage systems, especially for quantum communication networks. Thus, an optimized cloning algorithm would not only improve the quality of quantum memory, but also accelerate memorization and enhance the stability of storage over time. Indeed, quantum cloning protocols might be used to repeat or "amplify" the quantum information stored in a memory system. By creating approximate copies of a state, the memory system could potentially become more robust or error-resistant.

Multiplexing

Another area where quantum cloning can influence quantum memory is through multiplexing. In quantum communications, multiplexing involves dividing information into smaller parts and sending them through different channels or storing them in different locations. In some quantum communication protocols, "cloning" might involve copying or approximating parts of a quantum state into different channels. While not a perfect clone, this can act as a method of encoding quantum states into multiple memory devices. These techniques could contribute to improved storage techniques in quantum memory systems, allowing for more efficient use of resources and better management of quantum information in distributed systems.

Conclusions

Approximate quantum cloning, including entanglement swapping and multiplexing, can enhance quantum memory by transferring quantum states between locations, improving memory scalability, robustness, and error-resistance. Optimized cloning algorithms may accelerate memorization, increase stability, and enable more efficient quantum storage and communication systems.

3 Quantum Cloning and the NCT

The relationship between quantum cloning and the no-cloning theorem is central to understanding the nature of quantum information. While the no-cloning theorem forbids the exact duplication of arbitrary quantum states, quantum cloning protocols explore how closely one can approximate this cloning process. These approximations play a key role in quantum information science, particularly in areas like quantum communication, quantum memory, and quantum computing. The no-cloning theorem ensures that quantum information remains secure and unique, leading to the development of techniques that preserve quantum states without copying them exactly.

Application of approximate cloning

Since exact copying is prohibited, quantum information can be preserved but not duplicated. This limitation drives the development of other quantum information processing techniques, such as quantum error correction, quantum memory, and entanglement swapping, which do not require the creation of exact duplicates of quantum states. Moreover, the development of quantum cloning machines has been primarily aimed at exploring the limits of the no-cloning theorem and understanding how quantum information behaves under various protocols.

Conclusions

The no-cloning theorem prevents exact duplication of arbitrary quantum states, while quantum cloning protocols explore approximations. These approximations are vital in quantum information science, affecting quantum communication, memory, and computing, while preserving information without exact copying.