Applications of Non-Cloning Theorem: Approximate Cloning Machine and Quantum Protocols

Daniil Volkov(PH, MA), Yonglong Zhan (PH)
Advisor: Professor P.K. Aravind (PH), Professor Darko Volkov (MA)

Introduction

- Quantum cryptography allows two distant parties to create a secret key by exchanging quantum particles. Information is encoded in the values of the spin of the particles.
- An eavesdropper cannot decipher the information encoded in the states perfectly without disturbing it in an uncontrollable way.
- Approximate cloning machines use a variety of methods to produce imperfect clones that allow an eavesdropper to obtain useful information about the key being exchanged.
- This report studies the Buzek-Hillery 1→ 2 cloning machine and an N → M generalization of it. A particular type of attack launched with a 1→ 2 machine is also studied.

No-Cloning Theorem

This is a fundamental theorem of quantum cryptography which states that it is impossible to produce a perfect clone of an arbitrary quantum state while preserving the original state undisturbed. Two alternative proofs of the theorem have been given, one by **Wootters and Zurek** and the other by **Dieks.** Both proofs are simple and use only the unitarity of quantum operations performed on a closed system.

This result has two important implications:
1. An eavesdropper cannot make a perfect copy of a transmitted particle and so is limited in her ability to learn about the information encoded in it.
2. An eavesdropper corrupts the state of the transmitted particle and so risks detection.

Fidelity

Fidelity is a measure of the quality of the clone produced. If $\boldsymbol{\varphi}$ is the state being cloned and $\boldsymbol{\rho_j}$ is the density matrix of one of the clones produced, the fidelity is defined as

$$F_j = \langle \varphi | \rho_j | \varphi \rangle \quad , \qquad j = 1,2, \dots, M$$

The clones must be described by a density matrix because they are entangled with each other and the cloning machine. All the machines we consider produce identical clones.

Buzek-Hillery(BH) Cloning Machine

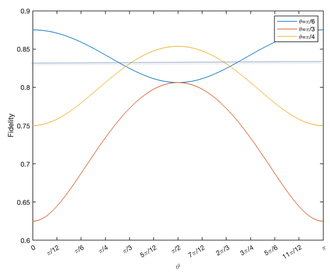
The **Buzek-Hillery** machine is a $\mathbf{1 \rightarrow 2}$ cloning machine that performs a unitary transformation on the input state, a blank state and the machine state, converting the input and blank states into two approximate copies of the input state that are entangled with the state of the machine.

The fidelity of a generalized version of the Buzek-Hillery machine, studied in this MQP, is given by

$$\boldsymbol{F = \frac{1}{2} + \frac{cos(\theta)\sqrt{2sin^2(\theta)sin^2(\vartheta)+cos^2(\theta)cos^3(\vartheta)}}{2}}$$

where θ describes the nature of the machine and ϑ is a parameter characterizing the input state.

For the usual BH machine, $\theta = cos^{-1}\left(\sqrt{\frac{2}{3}}\right)$ and F = $\frac{5}{6}$



The three curves show F as a function of the input state parameter $\boldsymbol{\vartheta}$ for machines with three different values of θ and the flat line is the BH machine. The other machines can outperform BH for some states but only BH has a uniform fidelity for all states.

Generalized N → M cloning machines

These machines take as their input an arbitrary state of a d-state quantum system (or "qudit").

They take N identical states as input and produce M > N identical (but imperfect) copies as output.

An approach due to Werner allows the fidelity of the machine to be derived without a detailed knowledge of its internal structure. The expression is

$$F = \frac{N}{M} + \frac{M-N}{M}\frac{N+1}{N+d}$$

For d = 2, N = 1, M = 2 we find F = 5/6 -- the BH machine!

Background on Incoherent Attack

In the BB84 protocol, Alice and Bob measure the percentage of errors in the bit string they share after the sifting phase. If it exceeds a certain critical value D, they acknowledge that the key either had too much noise or was compromised by an eavesdropper Eve. If things go smoothly, they shrink their key by a factor R to obtain a secret key. The values of D and R are given by the security criterion of Csiszar and Korner:

$$R = I(A:B) - min\{I(A:E), I(B:E)\}$$

A is Alice, B is Bob, E is Eve and I is the mutual information.

Optimal Incoherent Attack with an Ancilla

In an optimal incoherent attack with an ancilla, Eve tries to maximize her knowledge of I(A:E) and I(B:E). She uses a cloning machine due to Niu and Griffiths that entangles the input state with two qubits each initially in the blank state. By suitable measurements on these two qubits after the sifting phase, Eve can make I(A:E) = I(B:E) and also maximize their values. This can be done while limiting the error rate in the key to 14.6%.

Conclusion

- We carried out a detailed analysis of a generalized version of the Buzek-Hillery machine that produces two imperfect copies of an arbitrary state of a qubit.
- We used an approach due to Werner to study more general types of cloning machine that can take N identical copies of a d-state system as input and produce M > N imperfect copies of it.
- We showed that under a certain type of incoherent attack the BB84 protocol is safe if the error rate is less than 14.6%.
- More sophisticated attacks can have 11.1% crit. error

References

1. V. Buzek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. Physical Review A, 54(3):1844–1852, 1996.
2. W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. Nature, 299(5886):802–803, 1982. 49
3. M. Keyl and R. F. Werner. Optimal cloning of pure states, testing single clones. Journal of Mathematical Physics, 40(7):3283–3299, 1999
4. Valerio Scarani, Sofyan Iblisdir, Nicolas Gisin, and Antonio Ac´ın. Quantum cloning. Reviews of Modern Physics, 77(4):1225–1256, 2005.