1 Abstract

The no-cloning theorem has always been a hot topic in quantum theorem: As an impossibility result, this theorem precludes attempts to communicated faster than light and reinforces the security of several quantum cryptography protocol. In this survey, I will briefly introduce the history of quantum no-cloning theorem—how the thesis was invented, how did it get its name; And i would also discuss the hitherto progress on no-cloning theorem, several approach of none-perfect cloning on non-orthogonal states as well as the application of quantum no-cloning theorem in quantum cryptography and quantum information.

This survey incorporates the lecture "Quantum Information Amplifiers Beyond the No-Cloning Theorem" given by Prof. Giulio Chiribella and "Quantum cryptography" given by Prof. Xiongfeng Ma.

2 Introduction

It has always been a remarkable question that whether a given quantum states can be duplicated. The answer may look obviously positive, since we are using cloning scheme all around in our daily life: from copying data between computers to copying others homework. However, the answer to the quantum cloning problem is in general the opposite: There’s provably no way to replicate an arbitrarily given quantum state unless some error tolerance is allowed.

This assertion seems ludicrous, since if quantum states can not be cloned without error, how come we are still capable of doing perfectly cloning in our everyday life? (Since Physicians cherish the proposition that all the information carriers are quantum\footnote{5}.) However, the quantum no-cloning theorem merely states the fact of the ineligibility of cloning arbitrarily quantum states, what it does not obstacle is the possibility of cloning a subsets of all quantum states, for example, linear independent states: The theorem that we can actually do perfect cloning on orthogonal states is shown by W.H. Zurerk et al\footnote{7}, which is exactly how we implement immaculate cloning in our daily life.

Having said this, one may begin to wonder what is the behavior of quantum cloning machine on a given subset of quantum states instead of all the states in a universal Hilbert space. This observation involves the definition of quantum cloning machine. In general, there are two types of quantum cloning machines: The deterministic (build through unitary operators) and the probabilistic (through reversible evolution as well as measurement). Well the probabilistic cloning machine would possibly abort during the execution, it can produce perfect copies with non-negligible probability. On the contrary, the deterministic cloning machine, although in most case behaves better than probabilistic ones, could never replicate non-orthogonal states perfectly.

The history of quantum no-cloning theorem is shown in section 3, the definition of no-cloning theorem and several related theorems are given in section 4, the relationship between no-cloning theorem with quantum cryptography and no-signaling is presented in section 5, my comments would be introduced in section 6.

3 History of non-cloning theorem

As the saying goes, failure is the key to success: The quantum non-cloning theorem is originated in a wrong assertion: in 1982, Nick Herbert\footnote{8} publish a paper on the possibility of using Superluminal Communicator...
and quantum measurement to communicate faster than light. Interestingly, the editor of that journal, albeit
knowing that this theorem must be wrong because it violates the basic principle of special relativity, decided
to publish this paper in order to enhance the public understanding of quantum physics.

Herbert’s scheme is done as the following steps:

**Steps 3.1 (Communicate faster than light).**

1. Alice prepare an entangle state $|\Phi\rangle = \sum_i |\alpha_i\rangle \otimes |\beta_i\rangle$.
2. Alice send the marginal state $|B\rangle$ of $|\Phi\rangle$ on $H_B$ to Bob, through an laser gain tube, which Herbert
   asserted that it could replicate $|B\rangle$ to $|B\rangle \otimes |B\rangle$.
3. Alice take choose a bit from $\{0, 1\}$, if its 0, then Alice measure the entangle state on $H_A$ on plane
   polarized basis, otherwise measure it on circularly polarized photons.
4. Bob could detect which kind of measurement Alice used with his local measurement.

Not long after Herbert’s publication, Zurek[7] publish a paper called "a single quantum cannot be cloned"
on nature, sheerly refuted Herberts theorem by showing that the vital part in H’s experiment: to replicate
quantum states, is impossible. The conclusion of Zurek’s paper is given by that no deterministic cloning
machine (especially, the laser gain tube) can not implement perfect cloning on no-orthogonal states: The
Herbert experiment may success in some case, but the laser tube would produce as many noise as the copies,
which would greatly vitiate the success probability of the experiment to the extend that in average, Alice
can not pass any information about her private bits to Bob.

The proof given by Zurek can be written within 300 characters, however, the simple form belies the the
deep idea behind it. One maybe curious about why such straightforward theorem hadn’t been bring about
until the year 1982 given that human beings are doing data copy for thousands of years. The answer is
definitely not due to the inept of quantum physic, since the proof only involves the basic linear algebraic
formulas and fundamental quantum physic that had been available for nearly a half century. It is the idea
of viewing quantum physic in a information way that perplexed the precursors and delayed the discovery of
no-cloning theorem to 1982.

Form then on, the no-cloning theorem began to prevail in all aspects of quantum physics due to its
direct application on quantum information, quantum cryptography and no-signaling theorem. The problems
related to no-cloning theorem can be generalized into the following categories:

**Category 3.1 (No-cloning theorem).**

1. The fidelity problem: Since no perfect cloning can be implement, then how well close to perfect can we
   clone.
2. The probabilistic cloning: Clone states using unitary gates in cooperation with measurements.
3. The applications of no-cloning theorem. (no-cloning theorem with computational limitations)

The first and second category will be discussed in the following section, the third one would be put into
consideration in the 5th section.

4 No-cloning theorem: Propositions and Results

**Proposition 4.1 (No-cloning theorem[6]).** No quantum device can be constructed which outputs $|\psi\rangle|\psi\rangle$, given $|\psi\rangle$, for arbitrary $|\psi\rangle$.

This version of no-cloning theorem is the most general one, which holds for any quantum device (whether
deterministic or non-deterministic). And it only holds for the cloning of all possible states. However, if we
restrict the device to be deterministic, a stronger theorem can be stated:

**Proposition 4.2 (No-cloning theorem for deterministic device[6]).** No unitary operator can be constructed
which outputs $|\psi\rangle|\psi\rangle, |\phi\rangle|\phi\rangle$ when given $|\psi\rangle, |\phi\rangle$ respectively, for two non-orthogonal states $|\psi\rangle$ and $|\phi\rangle$.

The above two theorems hold for pure states, in 1996, H. Barnum et al extend the extant no-cloning
theorems to more general quantum states: the mixed state. This marvelous theorem, as given in their paper,
could be stated in a primitive way:
Proposition 4.3 (No-cloning theorem for mixed state\(^{[10]}\)). Given a general mixed state for a quantum system, there are no physical means for broadcasting that state onto two separate quantum systems, even when the state need only be reproduced marginally on the separate systems.

The aforementioned several impossibilities results of perfect quantum cloning did not close the book of cloning theorem, in fact, it sprint out bunch of results in non-perfect cloning that can be generalized into the following categories:

**Category 4.1.**
1. copying arbitrarily state with error tolerance.
2. copying a subset of quantum states perfectly.
3. copying a subset of quantum states with error.
4. copying quantum states with limited computational power.

The first attempt of copying quantum states with error was postulated by V. Buzek and M. Hillery\(^{[7]}\) when they noticed the limits of Wootters and Zurek’s previous proposition on the impossibility of perfect cloning: The computation process in quantum computer is not one hundred percent accurate by itself; In quantum cryptography, a protocol is secure not in the sense that an adversary can not always steal useful information, but that the adversary should be able to steal information only in very rare cases. All the above aspects repudiate the use of perfect no-cloning. Only by studying no-cloning theorem with error tolerance can we provide feasible auxiliary tools for the most general quantum computation and quantum cryptography.

Proposition 4.4 (Copying arbitrarily state with error tolerance). Suppose we have a quantum machine \(Q\) that execute the following operation:

1. \(|0\rangle_a|Q\rangle_x \rightarrow |0\rangle_a|0\rangle_b(\Omega_0)_{ab}x + |0\rangle_a|1\rangle_b|Y_0\rangle_x + \sum_{ij}a_{ij}|0\rangle_a|0\rangle_b|Y_j\rangle_x\)
2. \(|1\rangle_a|Q\rangle_x \rightarrow |1\rangle_a|1\rangle_b|Q_1\rangle_{ab}x + |0\rangle_a|1\rangle_b|Y_1\rangle_x\)

In which \(|Y_0\rangle = |Y_1\rangle = \xi\), \(|\Omega_0\rangle = |Q_1\rangle = |\langle Y_0\rangle| = |\langle Y_1\rangle\rangle = \frac{1}{\sqrt{2}}\).

Then the behavior of this cloning machine could be derived as:

On input \(a|0\rangle + b|1\rangle\),

\[
D_{ab}^{(2)} = Tr[\rho_{ab}^{input} - \rho_{ab}^{ideal}]^2 = U_{11}^2 + 2U_{12}^2 + 2U_{13}^2 + U_{22}^2 + 2U_{23}^2 + U_{33}^2
\]

In which \(U_{11} = a^4 - a^2(1 - 2\xi), U_{12} = \sqrt{2}ab[a^2 - \frac{1}{2}(1 - 2\xi)], U_{13} = a^2b^2, U_{22} = 2a^2b^2 - 2\xi, U_{23} = \sqrt{2}ab[b^2 - \frac{1}{2}(1 - 2\xi)], U_{33} = b^4 - b^4(1 - 2\xi).\)

Looking ugly, the above result is the first attempt of human being to manipulate the behavior of an arbitrary quantum cloning machine in the scope of error and probability. From then on, began the long trek of non-perfect no-cloning theorem.

Paradoxically, the next breakthrough in quantum no-cloning theorem is a possibility result: in the year 1997 our professor Lu-Ming Duan contrive a quantum copying machine that can copy a set of linear independent states perfectly using a unitary-reduction process (a probabilistic cloning scheme)

Proposition 4.5 (Clone two non-orthogonal states). If \(|A\rangle\) and \(|B\rangle\) are two non-orthogonal states on a Hilbert space \(\mathcal{H}\), then there exists a unitary operation \(U\) and a measurement \(M\) such that

1. \(|A\rangle\underline{U}M|A\rangle\)
2. \(|B\rangle\underline{U}M|B\rangle\)


Proposition 4.6 (Clone linear independent states\(^{[4]}\)). There exists a unitary operation \(U\) and probe \(|P_i\rangle\) such that

\[
U(|\Psi_i\rangle|\Sigma\rangle|P_0\rangle) = \sqrt{\eta}|\Psi_i\rangle|\Psi_i\rangle|P_0\rangle + \sum_{j=1}^{n} c_{ij}|\Psi_{AB}\rangle|P_j\rangle
\]

if and only if \(|\{\Psi_i\}\rangle\) are linear independent.
This construction, fundamentally different from Zurek’s deterministic device by making measurement on $|P_0\rangle$ to extract the copies, gives us a hunch on the power of probabilistic cloning machine: Proposition 4.2 has precluded any deterministic quantum device (merely unitary operator) to produce perfect copies of non-orthogonal states. However, if we modifies our constraint on quantum device to allow certain measurement, we are able to (as shown in Proposition 4.6) enhance the copying behavior to handle linear independent states.

The term if and only if in this proposition sounds perfect, however, the proposition itself is not strong enough due to the incompatibility with error in the whole theorem. The error itself, although sounds inconsequential in quantum copying machine at the first glance, has a great impact on the amelioration of cloning behavior of quantum machines. For instance, the resent result of Prof Guilio\[11\] provides the following result:

Proposition 4.7.

(1). No deterministic process can reliably replicate the states \{e^{i\theta H}|\phi\rangle, \theta \in \mathbb{R}\} at a rate larger than 1.
(2). No physical process can perfectly replicate the states \{e^{i\theta H}|\phi\rangle, \theta \in \mathbb{R}\} at a rate larger than 1.
(3). There exists a physical process can reliably (with negligible error) replicate the quantum states \{e^{i\theta H}|\phi\rangle, \theta \in \mathbb{R}\} at a arbitrarily close to 2 rate, the rate 2 is optimal.

The booming of rate from 1 to 2 is extremely significant compares with the error we have to sacrifice when using reliable replication. In fact, the error generated by the physical process could be ignored when taking to application as quantum computation or quantum cryptography.

The optimality of rate 2 is due to a notorious and vexing limitation in quantum physic:

Proposition 4.8 (Heisenberg Limit ).

Whenever one tries to estimate the value of a parameter characterizing a physical process, the variance of the estimate will decrease at most as \(\frac{1}{N^2}\), where \(N\) is the number of times that the process is probed.

Ironically, in classical case, the very elegant Chernoff bound states the following result:

Proposition 4.9 (Chernoff bound, classical case). \(\{X_i\}_{i=1}^{n}\) are i.i.d random variables, with each \(X_i \in [0,1]\), then

\[
E[|\frac{1}{n} \sum_{i=1}^{n} X_i - E[X_i]| > \varepsilon] < 2e^{-2\varepsilon^2 n}
\]

The variance of the estimate will decrease at the speed \(e^{-poly(N)}\).

The distinction between the above two propositions is a watershed of classical world and quantum world. The slower speed of convergence in quantum case exacerbate the sampling times required by a fairly accurate quantum experiment, however, it can contribute to a more secure environment in quantum cryptography which we would show in the next section.

As in the classical theoretical computer science, the better impossibility result (e.g. indistinguishability) can be created by restricting the computational power. In the traditional case, well the informational security would occurs only when the key length is equal to the message length, if we restrict the adversary computational power to be within a mathematical limitation, we can achieve (under some reasonable assumptions) computational security with much smaller key length. The same phenomenon can happen in quantum cryptography due to the better no-cloning theorem when the copying machine has only limit computational power.

Proposition 4.10 (No-cloning theorem with limited computational power\[15\]). Let $|\psi\rangle$ be an $n$-qubit pure state. Suppose we are given the initial state $|\psi\rangle^\otimes k$ for some $k \geq 1$ as well as an oracle $U_\psi$ such that $U_\psi|\psi\rangle = -|\psi\rangle$ and $U_\psi|\phi\rangle = |\phi\rangle$ whenever $\langle \phi | \psi \rangle = 0$. Then to prepare a state $\rho$ such that

\[
\langle \psi |^{k+1} \rho | \psi \rangle^{k+1} > p
\]

We need

\[
\Omega \left( \frac{\sqrt{2p}p}{k \log k} - k \right)
\]

many queries to $U_\psi$. 

4
The above theorem is magnificent: If we only consider the cloning machine without computational limits, the state $|\psi\rangle^\otimes k$ can be copied to $|\psi\rangle^\otimes k+1$ almost perfectly with an auxiliary unitary operator $U_\psi$. However, the number of query to $U_\psi$ is exponential in order to implement fairly good copying. It is impossible to attach one $|\psi\rangle$ to $|\psi\rangle^\otimes k$ if we confine the computational power of the copying machine to be polynomial. The constriction ”polynomial” is not a sever weaken to the proposition since we are merely using machines that run in polynomial time with respect to the input length in our everyday life.

While recent researchers are more and more intriguing in the area of probabilistic cloning theorem with error, there are still lots of open problems in this area:

**Open Problems 4.1.**

1. Are the parameters in theoretical quantum no-cloning theorem optimal?
2. Can we give constructions for unclonable quantum ID cards or quantum proofs? How do these function- alities relate to money and copy-protection?
3. What can we say about information-theoretically se- cure quantum copy-protection, in the regime where the number of copies of the quantum program is assumed to be small?

# 5 No-cloning theorem: Applications

The direct application of no-cloning theorem is quantum information amplification: If we are able to copy two quantum states $|\phi\rangle, |\psi\rangle$ of several times perfectly, we would be better distinguish the given input $|\phi\rangle, |\psi\rangle$. The following steps would give a toy example of how the quantum cloning theorem is related to the quantum information.

**Steps 5.1.**

1. Alice choose its private bit from $\{0,1\}$, and sends to Bob $|\psi\rangle$ if the bit is 0, otherwise sends to Bob state $|\phi\rangle$.
2. Bob, when receiving the states $|a\rangle$, use a quantum cloning machine to create copies $|a\rangle^\otimes N$, and take an measurement on the new state.
3. If $|\psi\rangle, |\phi\rangle$ are not orthogonal, Bob would increase the chance that he discovers the private bit of Alice.

The above toy example gives us a illustration on one of the major application of no-cloning theorem: The quantum information: We can view the no-cloning theorem as a bound on the accessible informations in the quantum information communication protocol–If we can not transfer more information than a given bound, we would not be able to clone the received states more than another bound. By this means, we would be able to restate the non-cloning theorem in a quantum information form, which is called the Holevo bound.

**Theorem 5.1** (Holevo bound[6]). Suppose Alice prepares a state $\rho_X$ where $X = 0,1,...,n$ with probabil- ity $p_0,...,p_n$. Bob performs a measurement described by POVM $\{E_y\} = \{E_0,...,E_m\}$ on that state, with measurement outcome $Y$. The Holevo bound states that for any such measurement Bob may do:

$$I(X;Y) \leq S(\rho) - \sum_x p_x S(\rho_x)$$

In which $\rho = \sum_x p_x \rho_x$.

The biggest application of quantum no-cloning theorem is the quantum cryptography:

It has always been a axiom in cryptography that the faster the computer is, the more secure a cryp- tographic protocol would be. This axiom may looks like a dumb since its easy for one to consider that quicker compute can break the protocol faster. The consideration itself is true, however, people who use this proposition to demerit the security of cryptographic protocol must not have taken the encryption time into their claims. The faster computer we have, the longer key we can generated within a fixed time interval, which would greatly enhance the security of protocol when the decryption takes longer time than encryption in asymptotic case.

Having said this, one may easily proclaim that the quantum computer provide the better cryptographic protocol than the classical computer can do, since quantum computer is provably faster than classical computer.
Ironically, one of the most powerful means of quantum computer in cryptography is to break the several generally used classical crypto protocols: In the year 1994, the prodigal shor[13] propose the following algorithm:

**Proposition 5.1.** There exists an quantum algorithm $A$ such that:

1. On input $N = pq$, in which $p, q$ are $n$-bit primes.
2. $A$ runs in time $O(n^2 \log n \log \log n)$
3. $A$ outputs $p, q$.

While the traditional believe that factoring can not be done within polynomial time is the footstone of a great number of generally used the crypto protocols, exemplified by RSA. Its not surprising to us that quantum computer are capable to break many classical crypto systems:

Here’s the list of classical crypto system that has or has not been broken by quantum computer:

These cryptosystems can be broken by quantum computers:

1) RSA public key encryption
2) Diffie-Hellman key-exchange
3) Elliptic curve cryptography
4) Buchmann-Williams key-exchange
5) Algebraically Homomorphic

And these cryptosystems (and also with some variants) are safe:

1) McEliece public key encryption
2) NTRU public key encryption
3) Lattice-based public key encryption

The ability of quantum computer to destroy crypto systems seems extreme, however, it is miserably inaptitude when dealing with encryption scheme that uses quantum computer and quantum bits. The power of quantum encryption scheme is rooted in no-cloning theorem: If an adversary can not even copied the encryption message from the receiver, how can he decode the message ever? The first quantum encryption scheme is proposed by Bennett and Brassard[0], which states that a secret key can be agreed by two parties, say, Alice and Bob, only through communication of quantum bits through a public quantum channel. The detail of the Algorithm is as follows:

**Steps 5.2.**

1. Alice encodes a bit of secret key in the state of a qubit.
2. With probability $\frac{1}{2}$, Alice encodes her bit in the basis $\{|0\rangle, |1\rangle\}$, i.e: She prepare the state $|0\rangle$ if her bit is 0 and prepare $|1\rangle$ otherwise.
3. With probability $\frac{1}{2}$ (otherwise), Alice encodes her bit in the basis $\{|+, |\rangle\}$.
4. She sends her qubit to Bob through a channel $C$ which is a non secure transmit channel controlled by an adversary Eva.
5. Bob, when getting the qubit from Alice, with probability $\frac{1}{2}$ measures it in the basis $\{|0\rangle, |1\rangle\}$ and probability $\frac{1}{2}$ in the basis $\{|+, |\rangle\}$.
6. Bob tells Alice the basis that he used to measure in an accurate but public channel. Then with probability $\frac{1}{2}$, Bob tells Alice the measurement result.
6.5. Bob and Alice abort the exchanging and deleted their previous private bits if they are using the same basis but the outcome of Bob’s measurement is different from Alice’s private bit.
(7). Bob accepts the measure result as his private bit in this round and Alice accepts her private bit if and only if Bob measured the qubit with the same basis as Alice’s preparing the qubit.

The security of this crypto system came from the no-cloning theorem: If Eva want to recover the private bits of Alice, he should be able to copy the qubit transmitted through the channel from Alice to Bob. However, if he manage to copy the qubit, due to no-cloning theorem, the successfully copy of Eva is at the expense of the quality of the qubit that reaches Bob, which could lead Alice and Bob to abort the exchanging process when they perform step 6.5.

This quantum key exchange protocol is provably to be secure against the most strong type of Man in the middle attack considering the computational power of the adversary or not, which makes the protocol appear to be perfect. However, it has a irredemably drawbacks if we take a close look at it: The protocol would do nothing but discard all the previous communication when detecting an error. However, the abortion is impolitic when the channel is noisy, or when the adversary (Eva) would be satisfied by only blocking the secret key generating process of Alice and Bob.

We can not denied the milestoneness of the $BB_84$ protocol to the development of quantum cryptography. As the first quantum crypto system, it opened the door of a commodious room in quantum physic for the future cryptographers.

The next giant step in quantum cryptography is based on the quantum no-cloning theorem for limited computational power quantum machines. As I have mentioned before, almost every extant crypto protocol is based on the assumption of the computational power of the adversary (as well as the encryption and decryption scheme). It is a direct application to incorporate the aforementioned non-cloning theorem of bounded computational machines into the quantum cryptography.

In computational based quantum cryptography, the two message exchanging parties (the user) and the third party are confined with only polynomial computational power, however, apart from the classical computational cryptography, the term "polynomial" here would refer to a more elaborated computational instrument: the quantum turing machine.

Definition 5.1 (Quantum Coins$^{[12]}$). A quantum money scheme with key size $n$ consists of the following:

1. A quantum circuit $B$ of size $O(poly(n))$ (the bank), which takes a string $s \in \{0,1\}^n$ (the secret key) as input, and produces a classical string $e_s$ (the public key) and mixed state $\rho_s$ (the banknote) as output.
2. A quantum circuit $A$ of size $O(poly(n))$ (the authenticator), which takes a string $e$ and state $\rho$ as input and either accepts or rejects.

The non-cloning theorem provides a preferable tool to handle quantum cryptography, however, its not yet powerful enough to produce type of negligible bounds as those in classical cryptography since we here not only seek for non-clonable quantum states, but for finding them efficiently as well: In classical crypto protocol, the existence of pseudorandom function is always assumed before the details of the protocol construction, as a counterpart, the existence of pseudorandom function against the quantum observer is the bedrock of computational quantum cryptography.

Proposition 5.2 (Pseudorandom function implies quantum security$^{[12]}$). If there exists a pseudorandom function family secure against quantum adversaries, then there exists a private-key quantum money scheme with perfect completeness and exponentially small soundness error.

6 Brief Conclusion

It is always astonishing to find out that such profound physic theorem-an arbitrary quantum states can not be copied, has such a simple, even naive form. Well the existence of the proof for non-cloning theorem is yet more jolting due to the fact that statement "quantum states can’t be copy" sounds like a rationale in our cosmos. Obviating the attempts to communicating faster then light well infuse a fresh blood in to the classical cryptograph, the non-cloning theorem is both a bane and a bless. Yet, no matter what words people would entitle it, one thing is certain: The era of Quantum would advent, and the non-cloning theorem would one day change the way we live, undeniably.
References


