Unit 11: No clone in quantum

Tzu-Chieh Wei
C. N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, State University of New York at Stony Brook, Stony Brook, NY 11794-3840, USA
(Dated: August 12, 2022)

In this unit, we discuss no cloning of quantum states, non-orthogonal state discrimination, quantum tomographic tools, and quantum cryptography: quantum key distribution from transmitting qubits and from shared entanglement.

Learning outcomes: You'll be able to understand why no cloning actually helps to distribute secret keys.

I. INTRODUCTION

Classical information can be copied and this seems to be obvious. We make zerox copies of papers, copy files, record music, etc. However, in the quantum world, copying is generally not possible, i.e.,

$$|\alpha\rangle|\text{blank}\rangle \not\to |\alpha\rangle|\alpha\rangle.$$

This is referred to as no cloning [1–3]. It can be easily proved by contradiction. Assume that one could copy via some unitary process,

$$|\alpha\rangle|\text{blank}\rangle \longrightarrow |\alpha\rangle|\alpha\rangle,$$
$$|\beta\rangle|\text{blank}\rangle \longrightarrow |\beta\rangle|\beta\rangle,$$

where we use $|\text{blank}\rangle$ to denote some reference state just like a blank paper in the classical world. However, the unitary operation preserves the overlap, and thus we have

$$\langle\alpha|\beta\rangle = \langle\alpha|\beta\rangle^2 \to \langle\alpha|\beta\rangle = 0 \text{ or } 1.$$

This does not hold in general, and thus cloning is not possible in general. However, we see that when $\langle\alpha|\beta\rangle = 0$ or 1 holds, they are either orthogonal or identical and behave like classical states, and can be cloned.

One consequence of cloning is that it would allow to distinguish non-orthogonal states with certainty. Suppose we can copy quantum states, then a state $|\alpha\rangle$ would become $|\alpha\rangle^{\otimes n}$ and two orthogonal states could be copied so that the copied states become orthogonal for large enough n,

$$\langle\alpha|\beta\rangle^n \to 0,$$

and therefore, they could be distinguished.

On the other hand, deterministic discrimination of non-orthogonal states, if possible, could be used to perform cloning of non-orthogonal states! This can be understood as follows. Suppose classical description of two states is known, but don't know which one is given. If one could uniquely determine which, one could then produce as many copies (given its description is known).

Self-consistently, neither cloning nor deterministic non-orthogonal discrimination is possible, so there is no contradiction.

II. STATE DISCRIMINATION

We know that non-orthogonal states cannot be distinguished or discriminated with unit success probability. But how well can we distinguish these states? Imagine there are two one-qubit states which may not be orthogonal: ψ_1 and ψ_2, which appears with equal probability. For simplicity, one can take

$$|\psi_1\rangle = |0\rangle,\ |\psi_2\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle,\ \text{with}\, 0 \le \theta \le \pi/2.$$

The key question is: what is the best strategy to distinguish these two states?

This question needs to be clarified. We will consider (i) to maximum overall success probability (a.k.a. minimum-error) and (ii) to maximize the unambiguous discrimination.

FIG. 1. Cloning is not possible for quantum information.

A. Minimum-error discrimination

We will design an orthogonal basis for such a measurement,

$$|v_1\rangle = \cos\phi|0\rangle + \sin\phi|1\rangle,\ |v_2\rangle = -\sin\phi|0\rangle + \cos\phi|1\rangle.$$

Then we will assign that if the outcome is v_1 then we declare it is ψ_1; we declare it is ψ_2 if the outcome is v_2; see illustration in Fig. 2b. However, we need to note that this scheme is not un-ambiguous, i.e., even if v_1 is detected, the state can still be ψ_2. So we want to maximize the success probability,

$$P(\phi) = \frac{1}{2}|\langle v_1|\psi_1\rangle|^2 + \frac{1}{2}|\langle v_2|\psi_2\rangle|^2 = \frac{1}{2}\cos^2\phi + \frac{1}{2}\sin^2(\theta-\phi).$$

This probability is easily maximized,

$$\max \text{ at } \phi = -(\pi/2-\theta)/2 : \max P = (1+\sin\theta)/2.$$

In general, there is the so-called Helstrom bound [4] that gives an lower bound on the error for arbitrary distribution for the two states (p_1, p_2),

$$P_{\text{err}} \geq \frac{1}{2}(1-\sqrt{1-4p_1p_2|\langle\psi_1|\psi_2\rangle|^2}).$$

The case we have $(p_1, p_2) = (1/2, 1/2)$ is a special case.

B. Unambiguous discrimination

In this second case, we want to know excatly what states we have unambigously. However, it is not possible to succeed with unit probability so we need to maximize the probability of unambiguous discrimination. This means that we can use three non-negative operators M_1, M_2 and M_3 that correspond to must-be state 1, must-be state 2, and 'don't know', respectively.

Since there are only two states, if we choose an operator proportional to projector orthogonal to ψ_2, then if the corresponding detector clicks, we know it must come from the state ψ_1, etc. Thus, we can define that three operators as follows,

$$M_1 = c|\psi_2^\perp\rangle\langle\psi_2^\perp|,\ M_2 = c|\psi_1^\perp\rangle\langle\psi_1^\perp|,\ M_3 = I - M_1 - M_2,$$

where we allows a constant c (the weight in the unambiguous discrimination), but we want it to be as large as possible, and it is constrained by

$$M_3 = I - c(-\sin\theta|0\rangle + \cos\theta|1\rangle)(-\sin\theta\langle 0| + \cos\theta\langle 1|) - c|1\rangle\langle 1| \geq 0.$$

We thus obtain the success probability

$$P_{\text{success}} = \frac{1}{2}\text{Tr}(|\psi_1\rangle\langle\psi_1|\cdot M_1) + \frac{1}{2}\text{Tr}(|\psi_2\rangle\langle\psi_2|\cdot M_2),$$

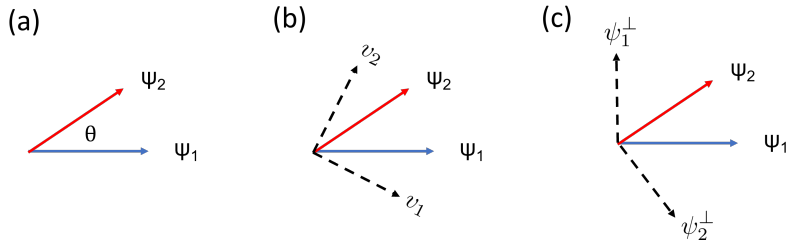


FIG. 2. State discrimination: (a) two non-orthogonal state; (b) minimum error (or maximum probability) discrimination; (c) optimal unambiguous discrimination.

which gives,

$$[P_{\text{success}} = c\frac{1}{2}|\langle 0|(-\sin\theta|0\rangle + \cos\theta|1\rangle|^2 + c\frac{1}{2}\langle 1|(\cos\theta|0\rangle + \sin\theta|1\rangle|^2 = c\sin^2\theta \leq 1 - \cos\theta.$$

In the last equality, we have used the fact

$$\max_{M_3 \geq 0} \; c = 1/(1+\cos\theta).$$

For the moment, we leave the detailed derivation to the readers.

For earlier discussions on state discrimination, see Refs. [5–7]. For later development, see, e.g. Refs. [8, 9]. In addition to uneven distribution, one can also consider more than two states and mixed states. But these are beyond the scope of this course.

III. PUBLIC KEY CRYPTOGRAPHY

We have discussed no cloning and no perfect discrimination of non-orthogonal states, and we will see that this can be useful for secure communication. But why do we want to use quantum properites to perform secure communication? One reason is that current public key cryptography using e.g. RSA can be broken by Shor's quantum factoring algorithm [10].

Let us re-cap the RSA crypo scheme below.

- Choose two different large prime numbers p and q; define $N = pq$.
- $\Phi = (p-1)(q-1)$ is a number coprime with N and less than N.
- Choose e coprime with Φ and compute $d = e^{-1}(\text{mod}\,(\Phi)$ or $ed = 1(\text{mod}\,\Phi)$.
- Broadcast public key e and number N.
- Other party encodes message a (assume coprime to N) to be $b = a^e(\text{mod}\,N)$ and we can decode it by $b^d = a^{(ed)} = a \cdot a^{n\Phi} = a(\text{mod}\,N)$, noting that $a^\Phi = 1(\text{mod}\,N)$.
- We can identify ourselves by encoding our signature s to be $t = s^d(\text{mod}\,N)$, everyone can verify it by decoding $t^e = s(\text{mod}\,N)$.

Given that RSA can be broken by quantum computers, is there any classical secure communication? Indeed, the so-called "one-time pad" is secure if the length is as long as the message and is used only once; see Fig. 3. A key question will be how to generate these one-time pads, which is discussed in the next section.

IV. QUANTUM CRYPTOGRAPHY

The goal is to establish a random sequence between Alice and Bob.

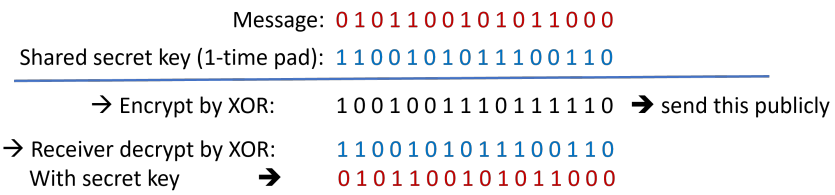
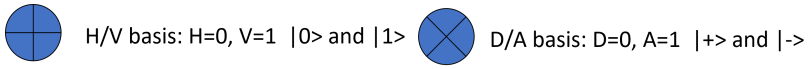


FIG. 3. Illustration of the one-time pad.

A. BB84

Given physical transmission of quantum bits is via photons (e.g. using polarizations as encoding), we list the possible bit encoding for the BB84 protocol below (invented by Bennett and Brassard [11]),



The protocol exploits the non-orthogonality between $|0\rangle$ and $|+\rangle$ (or $|1\rangle$ and $|-\rangle$). For each bit 0 or 1, Alice randomly selects between the two bases 0/1 or $+/-$. Bob at his end needs to measure in the same basis in order to have correlated bits. This means half of the time, the bases will not match.

- Alice randomly selects a random sequence, e.g. 0101011... For each bit (0 or 1) she randomly selects H/V or D/A basis, e.g. HVDVDAV....
- For each bit Bob randomly selects a basis H/V or D/A to measure, e.g. [H/V][D/A][H/V][H/V][D/A][H/V][D/A]. Suppose Bob measures: H D V V D H D.
- They openly compare bases (not results), and keep results when measured in the same basis, e.g. HVD...=010...
- They can compare a subset of results to make sure the security.

Attacking QKD? We now consider possible attacks to crack the QKD. First let us consider the "intercept-and-resend" attack. The eavesdropper Eve performs measurement on the intercepted photon (from Alice) in a randomly chosen basis H/V or D/A and resends a new photon to Bob according to her measurement result.

When Alice and Bob happen to use the same basis: If Eve uses the correct basis (50% of the time), then both she and Bob will decode Alice's bit value correctly. In this case, no error is introduced by Eve. If Eve uses the wrong basis (50% of the time), then both she and Bob will have random measurement results. Because Alice and Bob have 50% of using the same basis, the overall quantum bit error rate (QBER) is 25%. Naively, if the detected QBER in reality is close to this value, then the communication channel is not secure. Specifically, If QBER >14.6% then QKD is not secure; if QBER <12.4% it is secure; see, e.g., Ref. [12].

An important advantage of this QKD scheme is that once a QKD session is over, no classical "transcript" exists for Eve to keep since the communication is quantum. In contrast, in the public key crptography, Eve can copy encrypted messages and wait until private key is broken to decrypt the messages.

QKD has been applied, e.g. in the bank transaction and government communication. It was even used to encrypt security communications in the 2007 Swiss election and the 2010 World Cup; see `https://www.scientificamerican.com/article/swiss-test-quantum-cryptography/` and `https://www.prweb.com/releases/2010/05/prweb3998874.htm`.

Making keys more secure. Alice and Bob can further perform two classical steps to increase correlation between their key strings and reduce mutual information with Eve.

- Information reconciliation: error-correction conducted over a public channel (e.g. using parity check).
- Privacy amplification: a procedure for Alice and Bob to distill a common private key from a raw key about which Eve might have partial information.

In the latter step, Alice and Bob employ local randomness by using universal hash functions G, which map the set of n-bit strings A to the set of m-bit strings B, such that for any distinct $a_1, a_2 \in A$, when g is chosen uniformly at random from G, then the probability that $g(a_1) = g(a_2)$ is at most $1/|B|$.

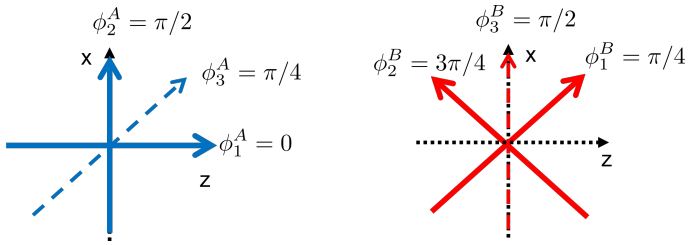
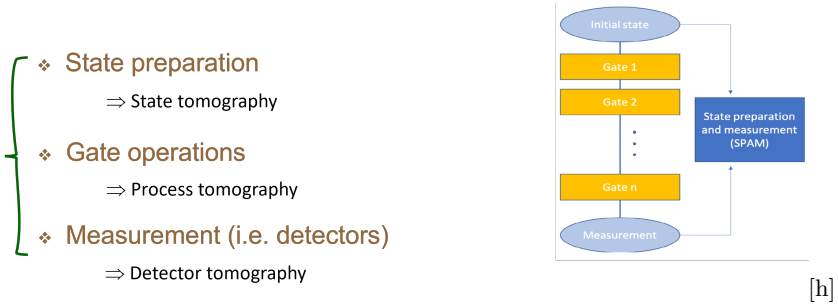


FIG. 4. Illustration of the Bell-inequality test and Ekerlt's protocol for secret key distribution.



[h]

FIG. 5. Illustration of the three quantum tomographic tools.

B. Ekert's protocol

We have used the singlet state in the Bell-inequality violation,

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

and the measurement set up is in Fig. 4 if Alice and Bob measure their particles along either their axis 1 or 2. Ekert realized that adding one more measurement axis (labeled 3 at each location), one could achieve QKD and test its security [13].

In particular, measurement using (A3,B1) and (A2,B3) gives anticorrelation and this allows the two parties to establish common secret keys. To ensure security, they use other measurement combinations to test the violation of the Bell inequality. The higher the violation, the better the security.

C. Six-state (Singapore) protocol

Will add later...

V. QUANTUM TOMOGRAPHIC TOOLS

In this section, we discuss things that are not directly related to no-cloning, but rather tools that allow us to characterize quantum states, processes and detection. These are called quantum state tomography (QST) [14, 15], quantum process tomography (QPT) [16, 17], and quantum detector tomography (QDT) [18], respectively. Other tools that are of use include quantum gate set tomography, randomized benchmarking, and quantum volume, and we will discuss the latter topics if time permits.

A. Quantum state tomography

The goal of QST is to estimate an unknown state, given multiple copies. Let us first illustrate with a one qubit state,

$$\rho = \frac{1}{2}(I + \vec{r}\cdot\vec{\sigma}) = \frac{1}{2}(I + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z),$$

where

$$r_j = \mathrm{Tr}(\rho\sigma_j) = \mathrm{Tr}(\rho|0_j\rangle\langle 0_j|) - \mathrm{Tr}(\rho|1_j\rangle\langle 1_j|),$$

and we have use the notation $\sigma_j|0/1_j\rangle = \pm|0/1_j\rangle$. This means that we need to measure the probabilities of the following projectors

$$|0\rangle\langle 0|, |1\rangle\langle 1|, |+\rangle\langle +|, |-\rangle\langle -|, |+i\rangle\langle +i|, |-i\rangle\langle -i|.$$

Since $\mathrm{Tr}(\rho|0_j\rangle\langle 0_j|) + \mathrm{Tr}(\rho|1_j\rangle\langle 1_j|) = 1$, the number of projectors needed to measure can be further reduced to just 3. The one-qubit QST is illustrated in Fig. 6.

Two-qubit QST. The above consideration can be easily generalized to two and multiple qubits. For two qubits, we use the decomposition,

$$\rho_{2-\mathrm{qubit}} = \frac{1}{4}\sum_{\mu,\nu=0,x,y,z} r_{\mu\nu}\sigma_\mu \otimes \sigma_\nu,$$

where $\sigma_0 \equiv I$ and

$$r_{\mu\nu} = \mathrm{Tr}(\rho_{2-\mathrm{qubit}}\sigma_\mu \otimes \sigma_\nu).$$

The above expression for $r_{\mu\nu}$ indicates that measurement will be done in coincidence, i.e. in the product basis. More n-qubit QST, n-qubit coincidence needs to be measured and the number of operators needed to measure scale exponentially with n, and it becomes very costly as n becomes large.

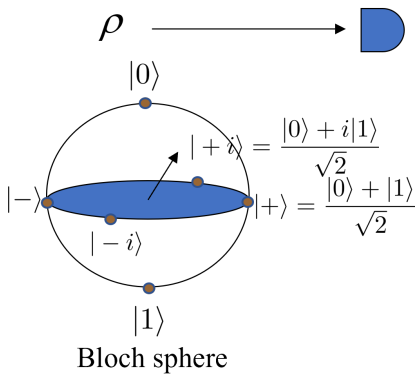


FIG. 6. Illustration of the one-qubit state tomography.

B. Quantum process tomography

From measuring a limited number of different input states (but unlimited supply of each), is it possible to predict the result for a general input state? This is the goal of QPT, as illustrated in Fig. 7. This is possible as any quantum process is linear and if one knows how the process acts on the finite number of complete matrix elements, then by linearity one knows the action on any linear combination.

Specifically, if we know the how the element $|j\rangle\langle k|$ is transformed,

$$\mathcal{E} : |j\rangle\langle k| \to \sum_\mu E_\mu |j\rangle\langle k| E_\mu^\dagger = \mathcal{E}(|j\rangle\langle k|),$$

then we can deduce the transformation on $a_{jk}|j\rangle\langle k|$,

$$\mathcal{E} : \sum_{jk} a_{jk}|j\rangle\langle k| \to \sum_{jk} a_{jk}\mathcal{E}(|j\rangle\langle k|).$$

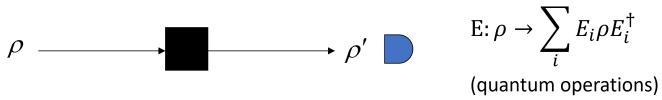


FIG. 7. Illustration of the quantum process tomography. The black box represents certain process and it turns the input ρ into the output ρ'.

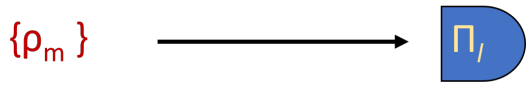


FIG. 8. Illustration of the quantum detector tomography.

But how can we obtain the action on $|j\rangle\langle k|$? Let us answer this by an example of one qubit. Arbitrary $|j\rangle\langle k|$ can be expressed in some linear combination of projectors, as illustrated below,

$$|0\rangle\langle 1| = |+\rangle\langle +| + i|+i\rangle\langle +i| = \frac{1+i}{2}|0\rangle\langle 0| - \frac{1+i}{2}|1\rangle\langle 1|, |1\rangle\langle 0| = |+\rangle\langle +| - i|+i\rangle\langle +i| = \frac{1-i}{2}|0\rangle\langle 0| - \frac{1-i}{2}|1\rangle\langle 1|.$$

This is called the standard QPT. There are also slightly varied approaches, e.g. using entangled pairs or correlated but unentangled pairs and let one part of the pairs undergo the process and perform the full tomography on the output pairs. These are called entanglement-assisted PT and ancilla assisted PT. For experimental demonstrations, see, e.g., Ref. [17].

C. Quantum detector tomography

We have seen some idea of this in measurement mitigation. The quantum detector tomography allows us to correct measuremet statistics. Here we explain what QDT is; the key idea is illustrated in Fig. 8.

The assumption is that we have an informationally complete set of test states $\{\rho_m\}$ be prepared with error much smaller than the error in the measurement or detection. The goal is to infer when detector outcome l clicks, what exactly is measured? As we learned earlier, this detector click should corresponds to some non-negative operator π_l that describes the POVM associated with the click.

This was proposed almost two decades ago, but some recent application in QDT comes from characterizing photon detectors. More recent application is the measurement error mitigation.

We will illustrate the idea by one qubits and it can be straightforwardly generalized to multiple-qubit detectors. We assume we have the capability to prepare with high fidelity the states

$$\rho_m = \{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |+i\rangle, |-i\rangle\},$$

and these can be easily prepared, e.g. on many quantum computers, via simple gate operations, which are of high fidelity. Our task is then to determine the POVM operators $\{\pi_0, \pi_1\}$ corresponding to the two outcomes 0 and 1, respectively. in this case, we have $\pi_0 + \pi_1 = I$, so the two are not independent.

The procedure is very simple: we prepare different states ρ_m and record the number of clicks f_{lm} by the detector outcome π_l. From the procedure, we have

$$p_{lm} = \mathrm{Tr}(\rho_m \pi_l) \approx \frac{f_{lm}}{\sum_{l'} f_{l'm}}.$$

Since the problem is linear, one can invert to find π_l from the probabilities. Fiurasek [PRA 64, 024102 (2001)] [19] provided a maximum-likelihood method that allows us to iteratively find π_l accurately. We will not describe the detail here but refer the readers to the paper for the procedure to process the data. For recent experimental results on superconducting qubits, see, e.g., Ref. [20], where the authors also describe how to used the characterized detectors to infer ideal measurement distribution.

VI. GATE QUALITY CHARACTERIZATION

to add soon...

A. Quantum volume

For quantum volume, we refer to Ref. [21].

B. Randomized benchmarking

For the earlier proposal of randomized benchmarking, we refer to Ref. [22].

VII. CONCLUDING REMARKS

In this unit, we have discussed no cloning of quantum states, non-orthogonal state discrimination, quantum tomographic tools, and quantum cryptography: quantum key distribution from transmitting qubits and from shared entanglement.

It is a good time to check whether you have achieved the following Learning Outcomes:
After this Unit, You'll be able to understand why no cloning actually helps to distribute secret keys.

Suggested reading: N&C 12.1, 12.6; Qb chap 3.12

---

[1] J. L. Park, The concept of transition in quantum mechanics, Foundations of physics **1**, 23 (1970).
[2] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).
[3] D. Dieks, Communication by epr devices, Physics Letters A **92**, 271 (1982).
[4] C. W. Helstrom, Quantum detection and estimation theory, Journal of Statistical Physics **1**, 231 (1969).
[5] I. D. Ivanovic, How to differentiate between non-orthogonal states, Physics Letters A **123**, 257 (1987).
[6] A. Peres, How to differentiate between non-orthogonal states, Physics Letters A **128**, 19 (1988).
[7] D. Dieks, Overlap and distinguishability of quantum states, Physics Letters A **126**, 303 (1988).
[8] U. Herzog and J. A. Bergou, Distinguishing mixed quantum states: Minimum-error discrimination versus optimum unambiguous discrimination, Phys. Rev. A **70**, 022302 (2004).
[9] M. Kleinmann, H. Kampermann, and D. Bruß, Unambiguous discrimination of mixed quantum states: Optimal solution and case study, Phys. Rev. A **81**, 020304 (2010).
[10] P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring, in *Proceedings 35th annual symposium on foundations of computer science* (Ieee, 1994) pp. 124–134.
[11] C. H. Bennett and B. G., Quantum cryptography: Public key distribution and coin tossing, Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing **175**, 8 (1984).
[12] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, Phys. Rev. A **72**, 032301 (2005).
[13] A. K. Ekert, Quantum cryptography based on bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[14] D. F. V. James, P. G. Kwiat, W. J. Munro, and A. G. White, Measurement of qubits, Phys. Rev. A **64**, 052312 (2001).
[15] G. M. D'Ariano, M. De Laurentis, M. G. Paris, A. Porzio, and S. Solimeno, Quantum tomography as a tool for the characterization of optical devices, Journal of Optics B: Quantum and Semiclassical Optics **4**, S127 (2002).
[16] I. L. Chuang and M. A. Nielsen, Prescription for experimental determination of the dynamics of a quantum black box, Journal of Modern Optics **44**, 2455 (1997).
[17] J. B. Altepeter, D. Branning, E. Jeffrey, T. C. Wei, P. G. Kwiat, R. T. Thew, J. L. O'Brien, M. A. Nielsen, and A. G. White, Ancilla-assisted quantum process tomography, Phys. Rev. Lett. **90**, 193601 (2003).
[18] A. Luis and L. L. Sánchez-Soto, Complete characterization of arbitrary quantum measurement processes, Phys. Rev. Lett. **83**, 3573 (1999).
[19] J. Fiurášek, Maximum-likelihood estimation of quantum measurement, Phys. Rev. A **64**, 024102 (2001).
[20] Y. Chen, M. Farahzad, S. Yoo, and T.-C. Wei, Detector tomography on ibm quantum computers and mitigation of an imperfect measurement, Phys. Rev. A **100**, 052315 (2019).
[21] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, Validating quantum computers using randomized model circuits, Phys. Rev. A **100**, 032328 (2019).
[22] J. Emerson, R. Alicki, and K. Życzkowski, Scalable noise estimation with random unitary operators, Journal of Optics B: Quantum and Semiclassical Optics **7**, S347 (2005).