Quantum information encoded on Quantum Operations

Estimation, characterization, engineering of QO's

Giacomo Mauro D'Ariano

Quantum Optics & Information Group

http://www.qubit.it

Istituto Nazionale di Fisica della Materia, Unità di Pavia

Dipartimento di Fisica "A. Volta", via Bassi 6, I-27100 Pavia, Italy

Dept. of Electrical and Computer Engineering, Northwestern University, Evanston, IL 60208

Research group/collaborations

G. M D'Ariano,

C. Macchiavello (univ. researcher),

M. G. A. Paris (INFM researcher),

M. Sacchi (INFM postdoc),

O. Rudolph (ATESIT postdoc),

S. Virmani (EQUIP postdoc),

P. Lo Presti (phd student),

R. Mecozzi (graduated),

F. Buscemi (graduated)

Founded by ATESIT

Partly supported by:

EQUIP, MURI (US).

- COLLABORATIONS

F. De Martini (Roma La Sapienza),

P. Kumar and H. Yuen (Northwestern University)

Research group/collaborations

G. M D'Ariano,

C. Macchiavello (univ. researcher),

M. G. A. Paris (INFM researcher),

M. Sacchi (INFM postdoc),

⇒ O. Rudolph [separability criteria]

S. Virmani (EQUIP postdoc),

P. Lo Presti (phd student),

R. Mecozzi (graduated),

F. Buscemi (graduated)

Founded by ATESIT

Partly supported by:

EQUIP, MURI (US).

- COLLABORATIONS

F. De Martini (Roma La Sapienza),

P. Kumar and H. Yuen (Northwestern University)

Research group/collaborations

⇒ **G. M D'Ariano,**

C. Macchiavello (univ. researcher),

⇒ **M. G. A. Paris** (INFM researcher),

M. Sacchi (INFM postdoc),

O. Rudolph (ATESIT postdoc),

S. Virmani (EQUIP postdoc),

⇒ **P. Lo Presti** (phd student),

⇒ **R. Mecozzi** (graduated),

⇒ **F. Buscemi** (graduated)

Founded by ATESIT

Partly supported by:

EQUIP, MURI (US).

- **COLLABORATIONS**

⇒ **F. De Martini** (Roma La Sapienza),

⇒ **P. Kumar and H. Yuen** (Northwestern University)

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \longrightarrow \frac{\mathrm{E}(\rho)}{\mathsf{Tr}[\mathrm{E}(\rho)]}$$

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \longrightarrow \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \rightarrow \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is
  1. linear

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \rightarrow \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is
  1. linear
  2. trace-decreasing

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \to \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is
  1. linear
  2. trace-decreasing
  3. completely positive

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \to \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is
  1. linear
  2. trace-decreasing
  3. completely positive
- The normalization $\mathrm{Tr}[\mathrm{E}(\rho)] \leq 1$ is the probability that the transformation occurs.

Main problems and motivations

Main focus on QO's instead of quantum states

- QO are the most general state change in quantum mechanics

$$\rho \to \frac{\mathrm{E}(\rho)}{\mathrm{Tr}[\mathrm{E}(\rho)]}$$

- The QO E is a map on traceclass operators that is
  1. linear
  2. trace-decreasing
  3. completely positive
- The normalization $\mathrm{Tr}[\mathrm{E}(\rho)] \leq 1$ is the probability that the transformation occurs.
- Encoding on QO's: given a fixed input state ρ, the message m is encoded on it via $\rho \to \mathrm{E}_m(\rho)$. Anonymous $\rho \equiv$ encryption.

Anonymous state encryption

-  transmits $|\varphi_A\rangle \in$ H (known only to her) to 

Anonymous state encryption

-  transmits $|\varphi_A\rangle \in$ H (known only to her) to 

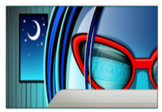
- Depending on the message m that  wants to send to , he modulates $|\varphi_A\rangle$ with a unitary U_m^B and sends $U_m^B|\varphi_A\rangle$ to 

Anonymous state encryption

-  transmits $|\varphi_A\rangle \in$ H (known only to her) to 
- Depending on the message m that  wants to send to , he modulates $|\varphi_A\rangle$ with a unitary U_m^B and sends $U_m^B|\varphi_A\rangle$ to 
- From knowledge of $|\varphi_A\rangle$ and openly known U_m^B,  decrypts m.

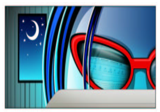
Anonymous state encryption

-  transmits $|\varphi_A\rangle \in$ H (known only to her) to 
- Depending on the message m that  wants to send to , he modulates $|\varphi_A\rangle$ with a unitary U_m^B and sends $U_m^B|\varphi_A\rangle$ to 
- From knowledge of $|\varphi_A\rangle$ and openly known U_m^B,  decrypts m.

$\Rightarrow$ Without knowing $|\varphi_A\rangle$,  cannot tell m without significant error.

Anonymous state encryption

-  transmits $|\varphi_A\rangle \in$ H (known only to her) to 
- Depending on the message m that  wants to send to , he modulates $|\varphi_A\rangle$ with a unitary U_m^B and sends $U_m^B|\varphi_A\rangle$ to 
- From knowledge of $|\varphi_A\rangle$ and openly known U_m^B,  decrypts m.

$\Rightarrow$ Without knowing $|\varphi_A\rangle$,  cannot tell m without significant error.

$\Rightarrow$ The function $f : m \rightarrow U_m^B$ can be regarded as a quantum one-way function with trapdoor information given by the knowledge of the actual input state $|\varphi_A\rangle$.

The Quantum Bit Commitment

- Anonymous states also used for the QBC.

The Quantum Bit Commitment

- Anonymous states also used for the QBC.

⇒ Dispute Yuen versus Lo-Chau-Mayers on whether there are unconditional secure QBC protocols

The Quantum Bit Commitment

- Anonymous states also used for the QBC.

$\Rightarrow$ Dispute Yuen versus Lo-Chau-Mayers on whether there are unconditional secure QBC protocols

- For non aborting protocols any multistep commitment can be reduced to a single step:

The Quantum Bit Commitment

- Anonymous states also used for the QBC.

⇒ Dispute Yuen versus Lo-Chau-Mayers on whether there are unconditional secure QBC protocols

- For non aborting protocols any multistep commitment can be reduced to a single step:

1.  prepares the Hilbert space H with the anonymous state $|\varphi\rangle \in$ H. He then sends H to  .

The Quantum Bit Commitment

- Anonymous states also used for the QBC.

⇒ Dispute Yuen versus Lo-Chau-Mayers on whether there are unconditional secure QBC protocols

- For non aborting protocols any multistep commitment can be reduced to a single step:

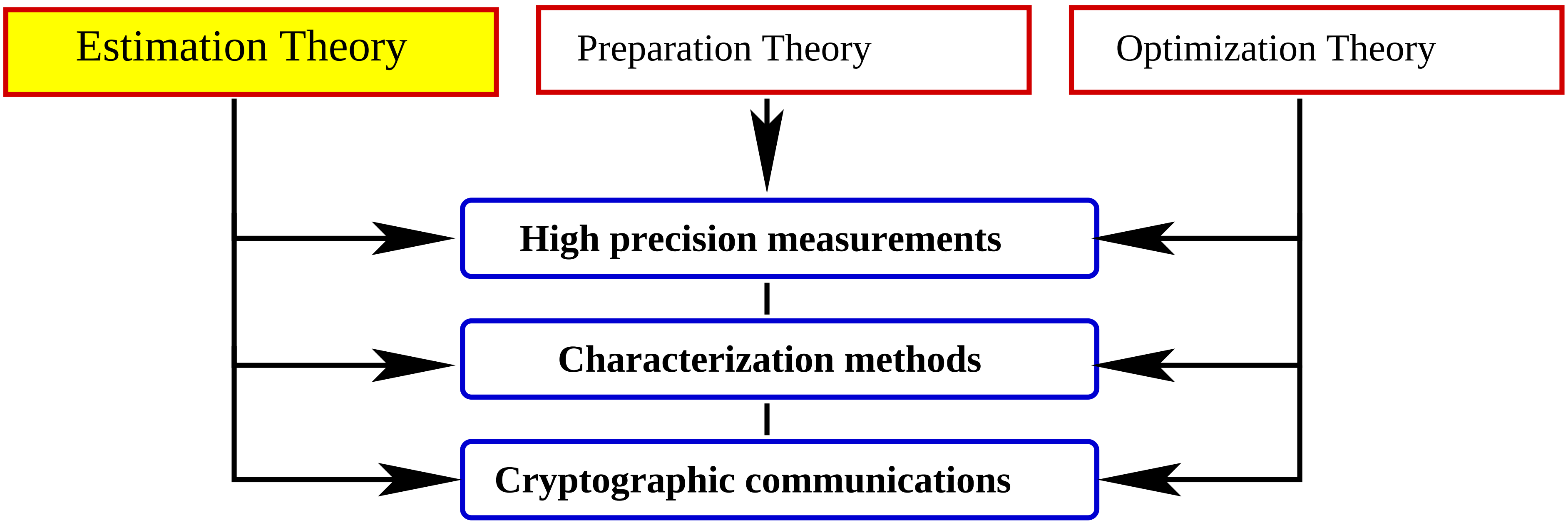
  1.  prepares the Hilbert space H with the anonymous state $|\varphi\rangle \in$ H. He then sends H to  .
  2.  modulates the value b of the committed bit on a QO acting on the anonymous state $|\varphi\rangle$ and sends the output back to  .

Main problems and motivations

Main focus on QO's instead of quantum states

Main problems and motivations

Main focus on QO’s instead of quantum states

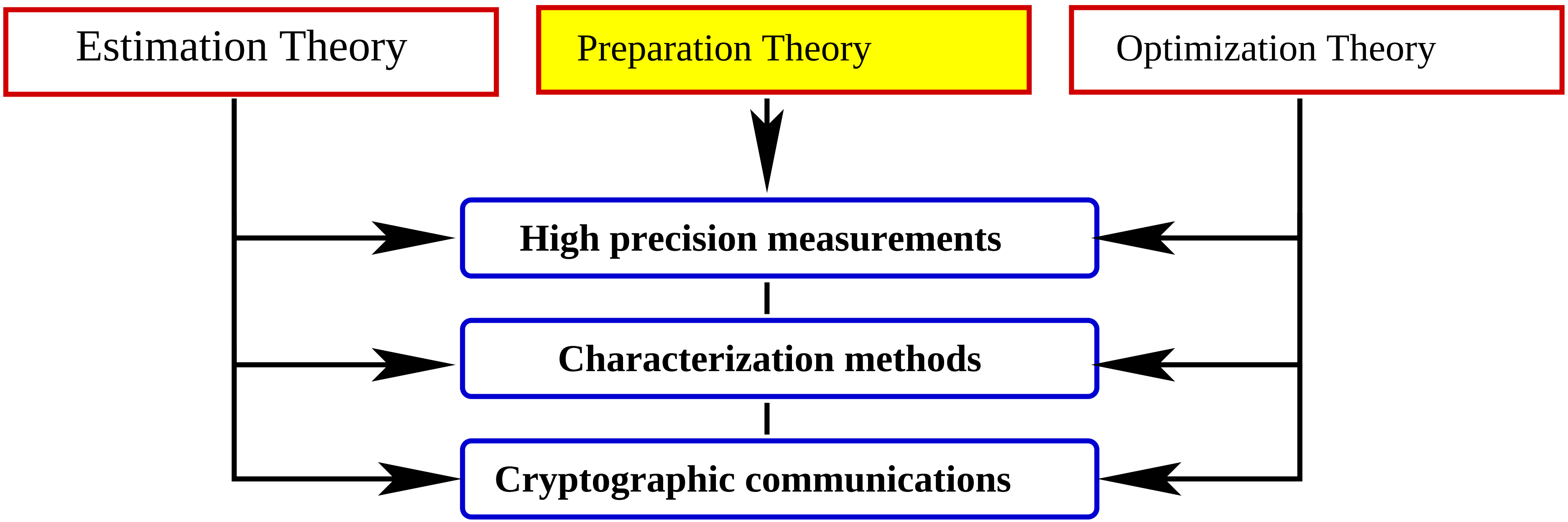


Discrimination among QO’s, POVM’s for estimating QO’s, tomographic characterization

Mayers, PRL **78** 3414 (1997); Lo and Chau, PRl **78** 3410 (1997),H. P. Yuen, quant-ph/0109055 –

Main problems and motivations

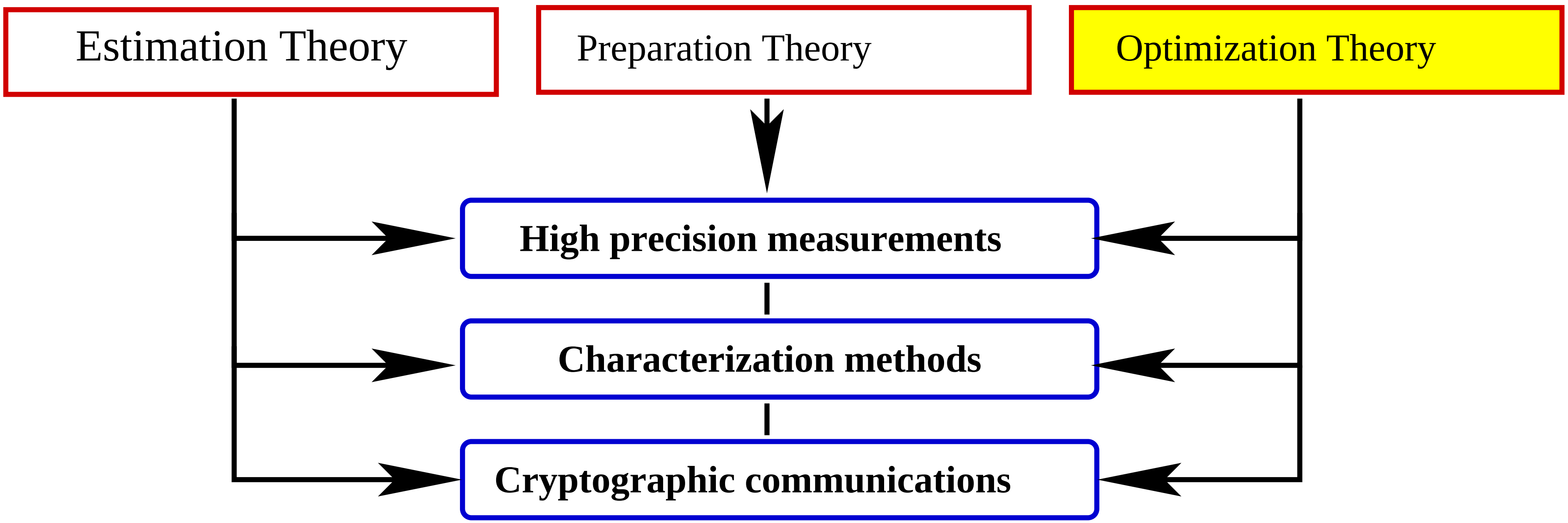
Main focus on QO’s instead of quantum states



Which apparatuses for achieving a QO −−> Classification of unitary extensions of QO’s, ...

Main problems and motivations

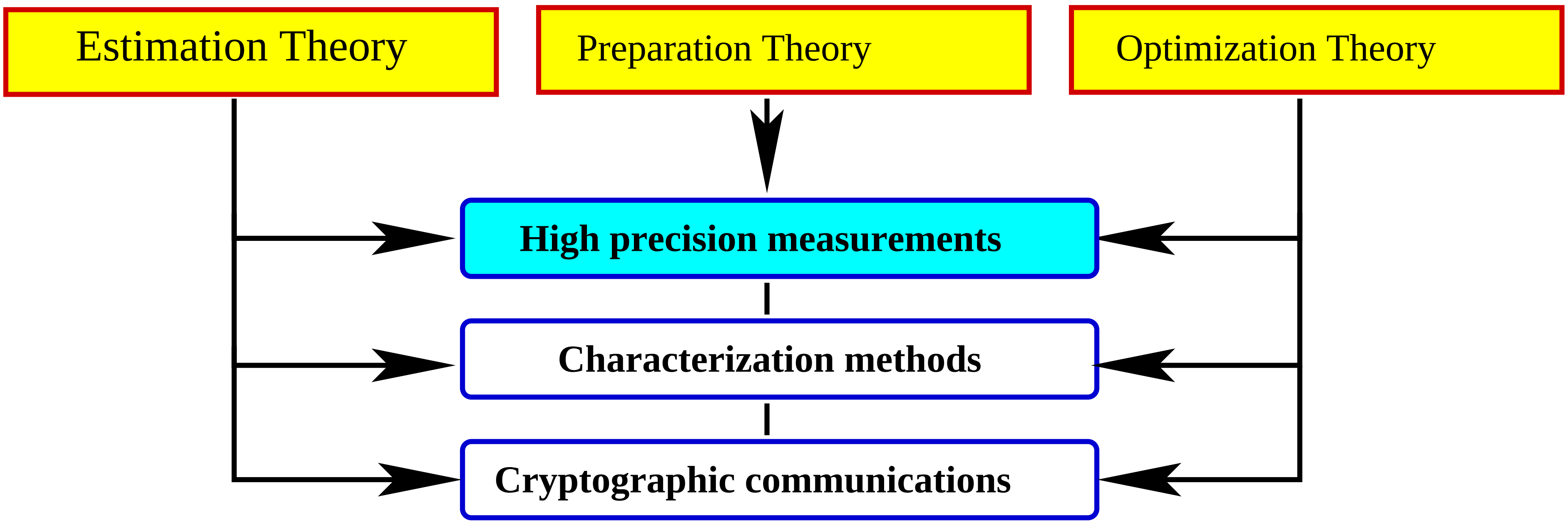
Main focus on QO's instead of quantum states



Which is the optimal QO to achieve a given purpose [in terms of a cost function]

Main problems and motivations

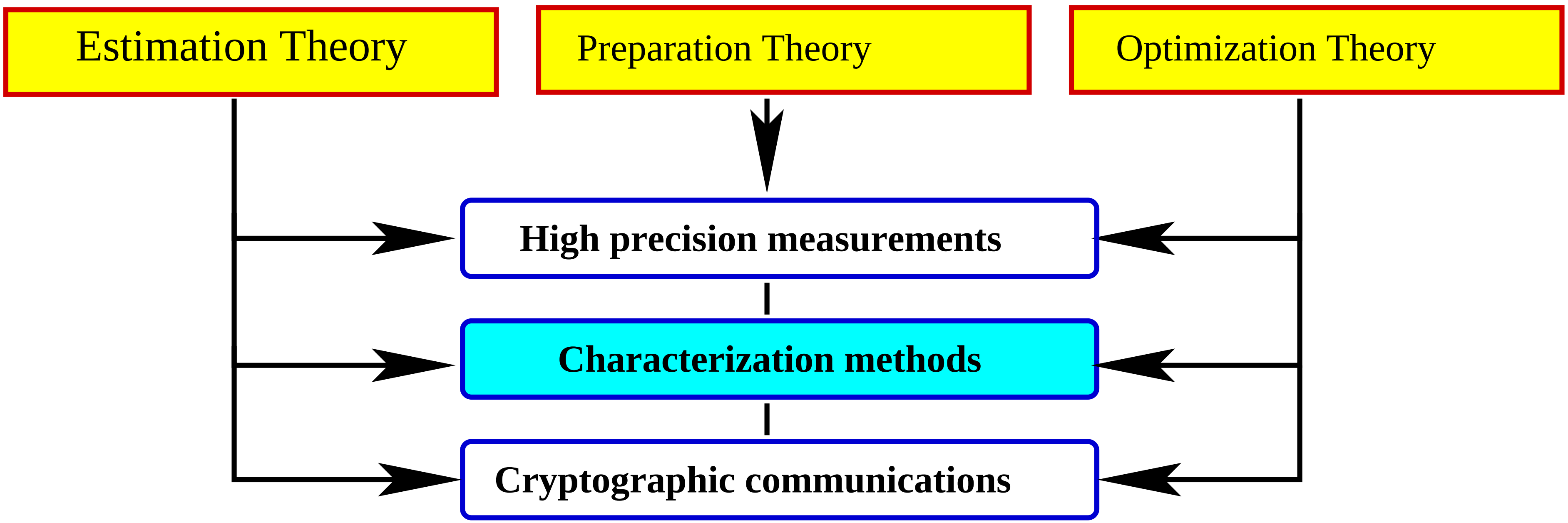
Main focus on QO’s instead of quantum states



Measurements can be always regarded as the estimation of parameters of a set of QO’s

Main problems and motivations

Main focus on QO’s instead of quantum states

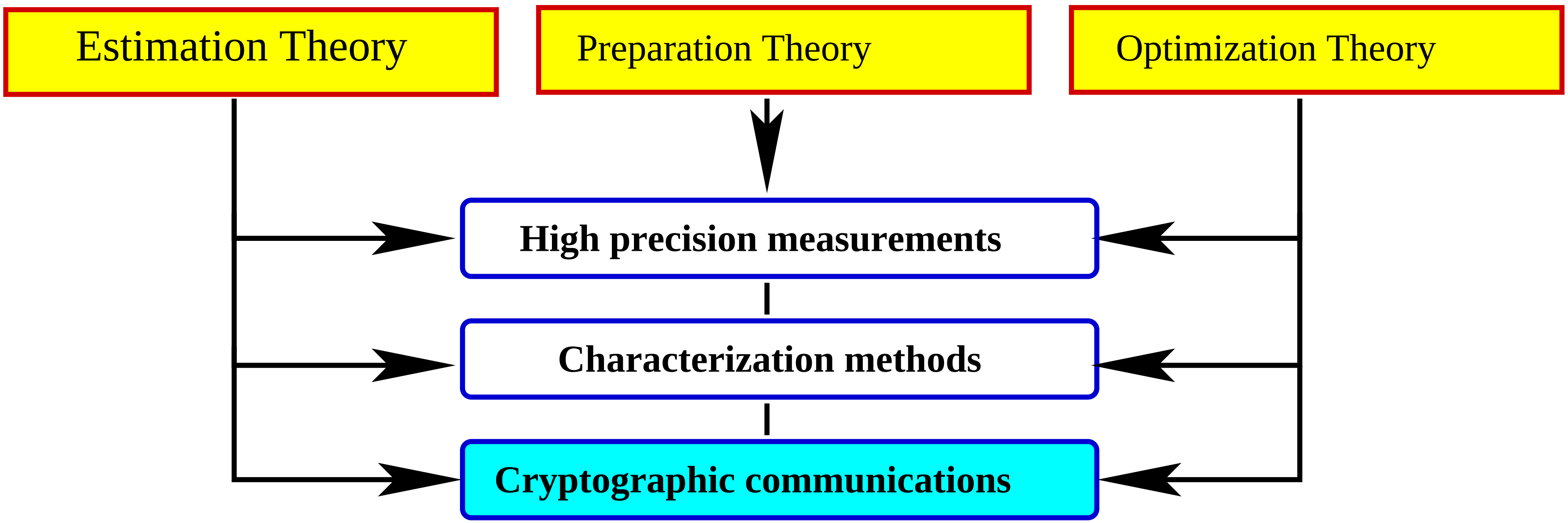


We need to characterize completely quantum mechanically the new devices for QIT

Mayers, PRL **78** 3414 (1997); Lo and Chau, PRl **78** 3410 (1997),H. P. Yuen, quant-ph/0109055 –

Main problems and motivations

Main focus on QO's instead of quantum states



Quantum cryptography with anonymous states = encoding information on maps

Mayers, PRL **78** 3414 (1997); Lo and Chau, PRl **78** 3410 (1997),H. P. Yuen, quant-ph/0109055 –

Main results on QO theory

1) Optimal discrimination between QO's (unitary)

2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano, and P. Lo Presti, M. G. A. Paris, Phys. Rev. Lett. 87 270404 (2001)

Main results on QO theory

1) Optimal discrimination between QO’s (unitary)

2) Tomographic characterization of QO’s using entangled input

3) Classification of all unitary extensions of QO’s, extremal QO’s and POVM’s

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D’Ariano, and P. Lo Presti, Phys. Rev. Lett. 86, 4195 (2001)
Collaboration with F. De Martini (Roma): tomography of a single qubit device

Main results on QO theory

1) Optimal discrimination between QO's (unitary)

2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano and F. Buscemi (unpublished)
G. M. D'Ariano, P. Lo Presti, and R. Mecozzi (unpublished)

Main results on QO theory

1) Optimal discrimination between QO’s (unitary)

2) Tomographic characterization of QO’s using entangled input

3) Classification of all unitary extensions of QO’s, extremal QO’s and POVM’s

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D’Ariano, QCM&C 2002, Boston (preprint available)

Optimal discrimination of QO's

Optimal discrimination of QO's

1) Optimal discrimination between QO's (unitary)

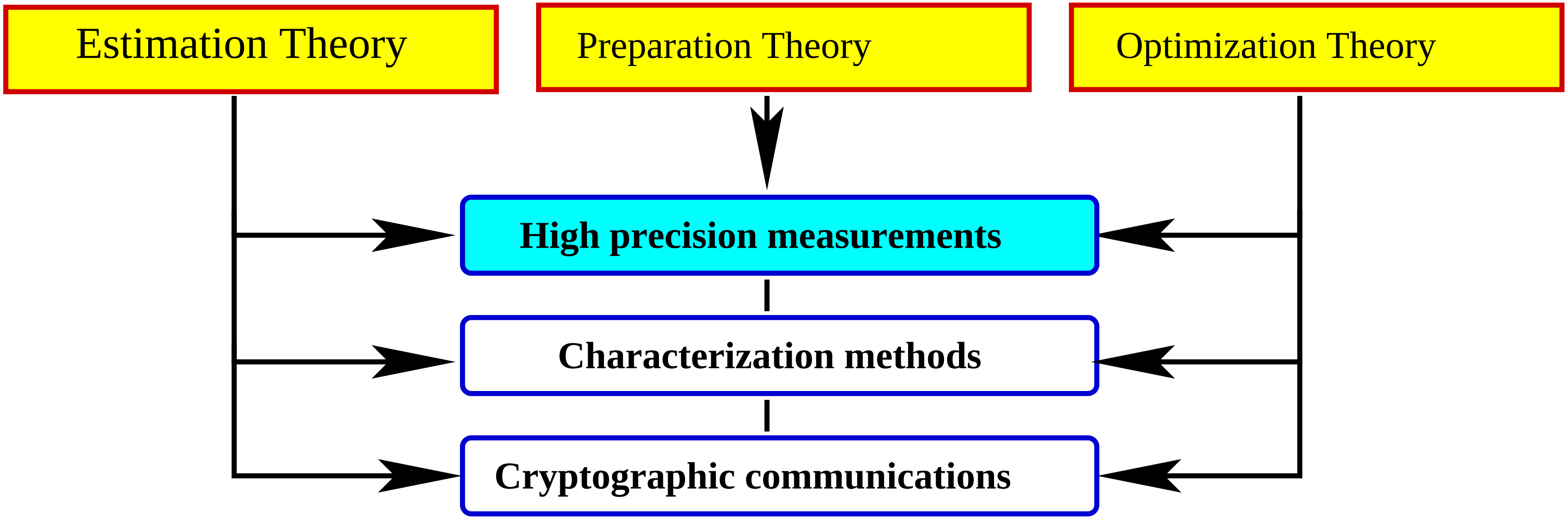
2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano, and P. Lo Presti, M. G. A. Paris, Phys. Rev. Lett. 87 270404 (2001)

Optimal discrimination of QO's



Measurements can be always regarded as the estimation of parameters of a set of QO's

Optimal discrimination of QO's

- Optimization over:

Optimal discrimination of QO's

- Optimization over:
  1. the detection scheme

Optimal discrimination of QO's

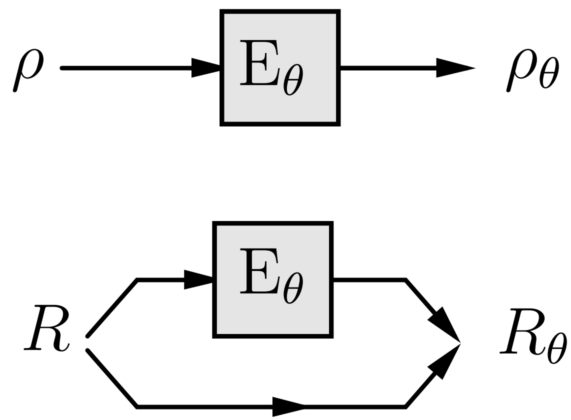
- Optimization over:
  1. the detection scheme
  2. the input state

Optimal discrimination of QO's

- Optimization over:
  1. the detection scheme
  2. the input state
- The use of an entangled input state R is considered, with the unknown transformation E_θ acting locally only on one side of the entangled state: $R \to R_\theta = \mathrm{E}_\theta \otimes \mathrm{I}(R)$.

Optimal discrimination of QO's

- Optimization over:
  1. the detection scheme
  2. the input state
- The use of an entangled input state R is considered, with the unknown transformation E_θ acting locally only on one side of the entangled state: $R \to R_\theta = \mathrm{E}_\theta \otimes \mathrm{I}(R)$.



Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.

Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:

Optimal discrimination of QO’s

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:
  1. the entangled state is equivalent to many input states in “quantum parallel”;

Optimal discrimination of QO’s

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:
  1. the entangled state is equivalent to many input states in “quantum parallel”;
  2. precision increases with the dimension of the input space.

Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.

- Reasons:

  1. the entangled state is equivalent to many input states in "quantum parallel";
  2. precision increases with the dimension of the input space.

     Extreme examples:

Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:
  1. the entangled state is equivalent to many input states in "quantum parallel";
  2. precision increases with the dimension of the input space.

     Extreme examples:
     - Discrimination of $I, \sigma_x, \sigma_y, \sigma_z \leftrightarrow$ Bell measurement;

Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:
  1. the entangled state is equivalent to many input states in "quantum parallel";
  2. precision increases with the dimension of the input space.

     Extreme examples:
     - Discrimination of $I, \sigma_x, \sigma_y, \sigma_z \leftrightarrow$ Bell measurement;
     - Estimation of $\alpha \in \mathbb{C}$ of $D(\alpha) \leftrightarrow$ breaching the 3dB noise;

Optimal discrimination of QO's

- Result: the entangled configuration performs better, in increasing the precision of the measurement.
- Reasons:
  1. the entangled state is equivalent to many input states in "quantum parallel";
  2. precision increases with the dimension of the input space.

  Extreme examples:
  - Discrimination of $I, \sigma_x, \sigma_y, \sigma_z \leftrightarrow$ Bell measurement;
  - Estimation of $\alpha \in \mathbb{C}$ of $D(\alpha) \leftrightarrow$ breaching the 3dB noise;
  - Covariant discrimination: the Holevo bound is increased exactly by the amount of entanglement of the input state.

Optimal discrimination of QO's

Moreover:

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;
2. An entangled input improves the measurement stability.

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;

2. An entangled input improves the measurement stability.

   Example: measurement of $x \in \mathbb{R}$ of $D(xe^{i\phi})$. Squeezed vs twin beam inputs. Sensitivity:

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;

2. An entangled input improves the measurement stability.

   Example: measurement of $x \in \mathbb{R}$ of $D(xe^{i\phi})$. Squeezed vs twin beam inputs. Sensitivity:

   - dramatically decreases for mismatched squeezing;

G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87** 270404 (2001)

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;

2. An entangled input improves the measurement stability.

   Example: measurement of $x \in \mathbb{R}$ of $D(xe^{i\phi})$. Squeezed vs twin beam inputs. Sensitivity:

   - dramatically decreases for mismatched squeezing;
   - is independent on ϕ for twin beams.

G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87** 270404 (2001)

Optimal discrimination of QO's

Moreover:

1. An entangled input improves the measurement in the presence of noise [below a "quantum" threshold]

   Example: heterodyne measurement of $\alpha \in \mathbb{C}$ of $D(\alpha)$ in the presence of Gaussian noise, for $\overline{n} < 1$;

2. An entangled input improves the measurement stability.

   Example: measurement of $x \in \mathbb{R}$ of $D(xe^{i\phi})$. Squeezed vs twin beam inputs. Sensitivity:

   - dramatically decreases for mismatched squeezing;
   - is independent on ϕ for twin beams.

3. One has the phenomenon of perfect discrimination between any two unitaries with a finite number N of copies of the QO (compare with *state* discrimination).

G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87** 270404 (2001) –

Discrimination between unitaries

- Optimal error prob. in discrimination of $U_1|\psi\rangle$ and $U_2|\psi\rangle$

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right],$$

Discrimination between unitaries

- Optimal error prob. in discrimination of $U_1|\psi\rangle$ and $U_2|\psi\rangle$

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right],$$

- Optimum input states $|\psi\rangle$ minimize the overlap $|\langle\psi|U_2^\dagger U_1|\psi\rangle|$.

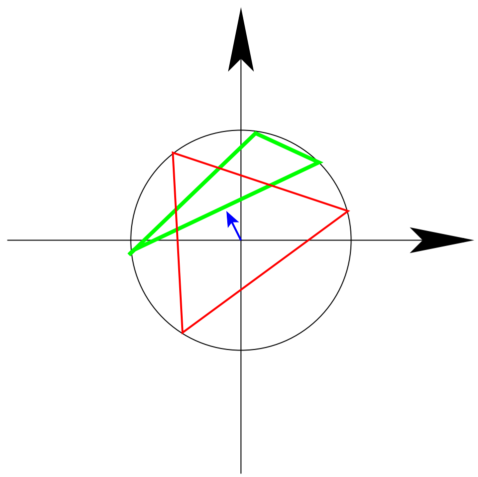
G. M. D'Ariano, P. Lo Presti, and M. G. A. Paris, Phys. Rev. Lett. **87** 270404 (2001) –

Discrimination between unitaries

- Optimal error prob. in discrimination of $U_1|\psi\rangle$ and $U_2|\psi\rangle$

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right],$$

- Optimum input states $|\psi\rangle$ minimize the overlap $|\langle\psi|U_2^\dagger U_1|\psi\rangle|$.
- Minimum overlap: $\min_{||\psi||=1} |\langle\psi|U_2^\dagger U_1|\psi\rangle| = r(U_2^\dagger U_1)$,

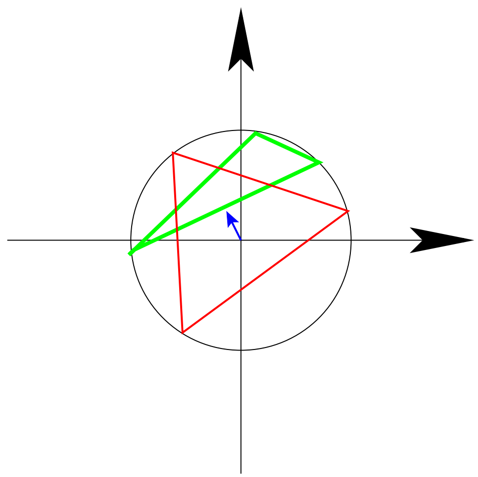


Discrimination between unitaries

- Optimal error prob. in discrimination of $U_1|\psi\rangle$ and $U_2|\psi\rangle$

$$P_E = \frac{1}{2}\left[1 - \sqrt{1 - |\langle\psi|U_2^\dagger U_1|\psi\rangle|^2}\right] ,$$

- Optimum input states $|\psi\rangle$ minimize the overlap $|\langle\psi|U_2^\dagger U_1|\psi\rangle|$.
- Minimum overlap: $\min_{||\psi||=1} |\langle\psi|U_2^\dagger U_1|\psi\rangle| = r(U_2^\dagger U_1)$,



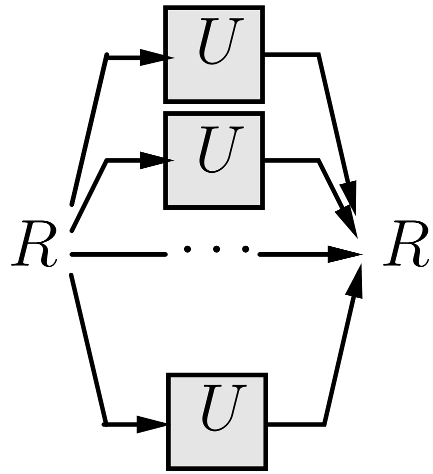
- Perfect discrimination: the poligon encircles the origin.

Discrimination between unitaries

- Available N copies of the unitary transformation $U = U_{1,2}$ and a N-partite entangled state as follows

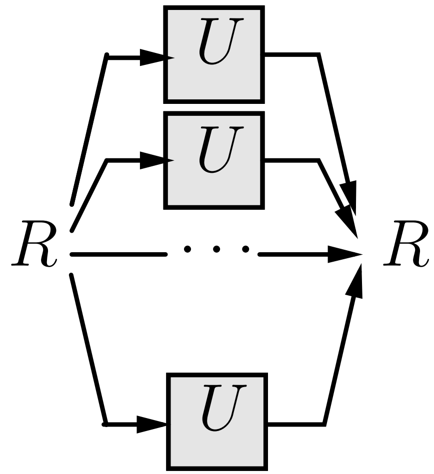
Discrimination between unitaries

- Available N copies of the unitary transformation $U = U_{1,2}$ and a N-partite entangled state as follows



Discrimination between unitaries

- Available N copies of the unitary transformation $U = U_{1,2}$ and a N-partite entangled state as follows

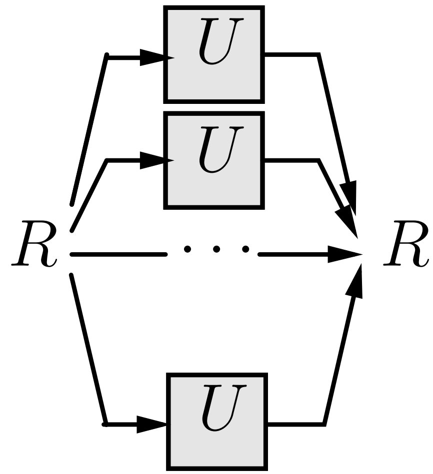


- Angular spread $\Delta(W)$ of the spectrum of W. One has

$$\Delta(W^{\otimes N}) = N\Delta(W) \text{ mod } 2\pi.$$

Discrimination between unitaries

- Available N copies of the unitary transformation $U = U_{1,2}$ and a N-partite entangled state as follows



- Angular spread $\Delta(W)$ of the spectrum of W. One has

$$\Delta(W^{\otimes N}) = N\Delta(W) \text{ mod } 2\pi.$$

- Conclusion: *the discrimination is always exact for sufficiently large* N! [see also Acín, quant-ph/0102064].

Tomography of a quantum device

Tomography of a quantum device

1) Optimal discrimination between QO's (unitary)

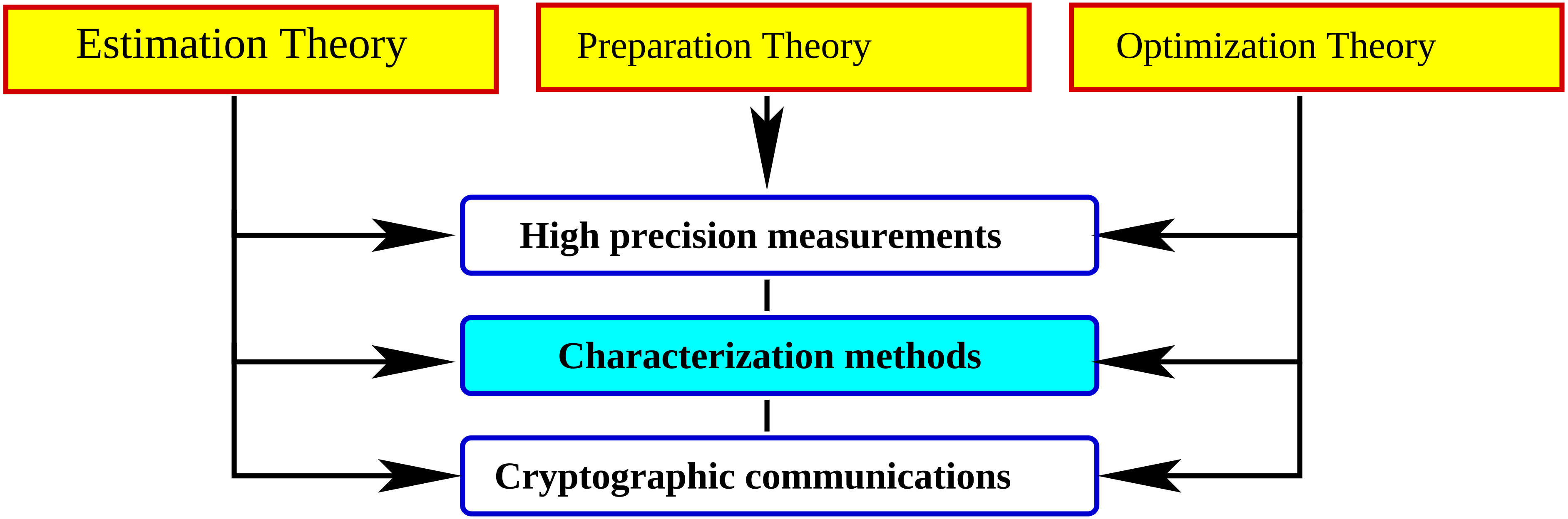
2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano, and P. Lo Presti, Phys. Rev. Lett. 86, 4195 (2001)
Collaboration with F. De Martini (Roma): tomography of a single qubit device

Tomography of a quantum device



We need to characterize completely quantum mechanically the new devices for QIT

Tomography of a quantum device

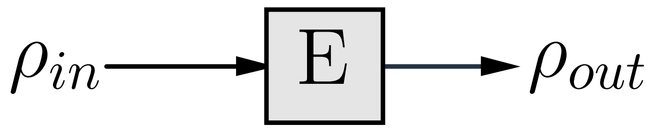
- How to achieve a complete characterization of a quantum device?

Tomography of a quantum device

- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.

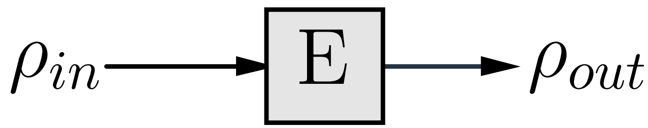
Tomography of a quantum device

- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.



Tomography of a quantum device

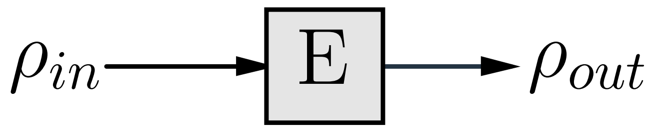
- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.



- In quantum mechanics the inputs and outputs are density operators $\Rightarrow$ we need to run all the following inputs

Tomography of a quantum device

- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.

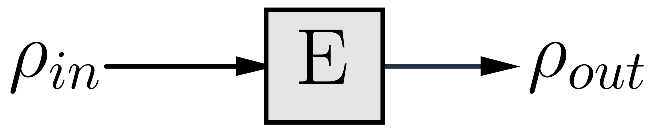


- In quantum mechanics the inputs and outputs are density operators $\Rightarrow$ we need to run all the following inputs
  - $|n\rangle, \qquad n = 0, 1, 2, \ldots,$

G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **86** 4195 (2001) –

Tomography of a quantum device

- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.

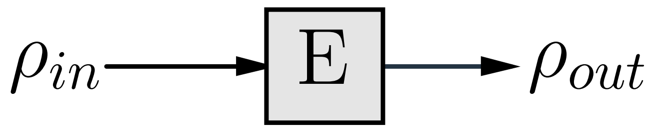


- In quantum mechanics the inputs and outputs are density operators $\Rightarrow$ we need to run all the following inputs
  - $|n\rangle, \qquad n = 0, 1, 2, \ldots,$
  - $\frac{1}{\sqrt{2}}(|n'\rangle + \kappa|n''\rangle), \qquad \kappa = \pm 1, \pm i,\ n, n' = 0, 1, 2, \ldots$

G. M. D'Ariano and P. Lo Presti, Phys. Rev. Lett. **86** 4195 (2001) –

Tomography of a quantum device

- How to achieve a complete characterization of a quantum device?
- Answer (brute force): by scanning a *basis* of possible inputs, and measuring the corresponding outputs.



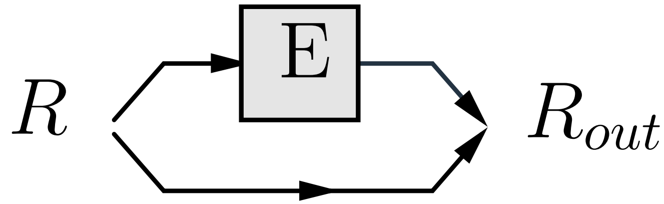
- In quantum mechanics the inputs and outputs are density operators $\Rightarrow$ we need to run all the following inputs
  - $|n\rangle, \qquad n = 0, 1, 2, \ldots,$
  - $\frac{1}{\sqrt{2}}(|n'\rangle + \kappa|n''\rangle), \qquad \kappa = \pm 1, \pm i, \; n, n' = 0, 1, 2, \ldots$
- However, the availability of a basis of states in the lab is a very hard technological problem.

Tomography of a quantum device

- **Quantum parallelism of entanglement**: a single entangled input state R is equivalent to scanning all states in parallel.

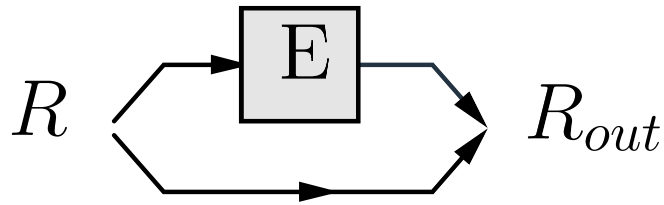
Tomography of a quantum device

- **Quantum parallelism of entanglement**: a single entangled input state R is equivalent to scanning all states in parallel.



Tomography of a quantum device

- **Quantum parallelism of entanglement**: **a single entangled input state R is equivalent to scanning all states in parallel.**

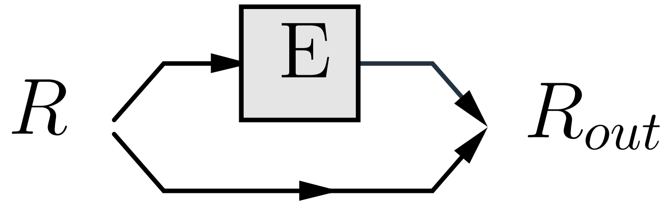


- The setup is expressed as the quantum operation

$$R_{out} = \mathrm{E} \otimes \mathrm{I}(R).$$

Tomography of a quantum device

- **Quantum parallelism of entanglement**: **a single entangled input state R is equivalent to scanning all states in parallel.**



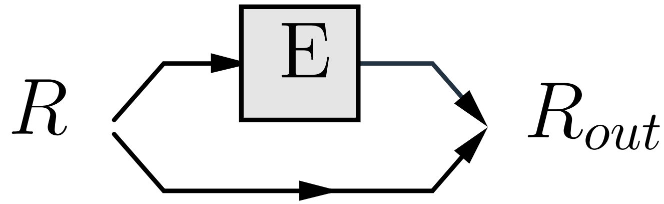
- The setup is expressed as the quantum operation

$$R_{out} = \mathrm{E} \otimes \mathrm{I}(R).$$

- For fixed *faithful* state R the output state R_{out} is in one-to-one correspondence with the QO of the device E.

Tomography of a quantum device

- **Quantum parallelism of entanglement: a single entangled input state R is equivalent to scanning all states in parallel.**



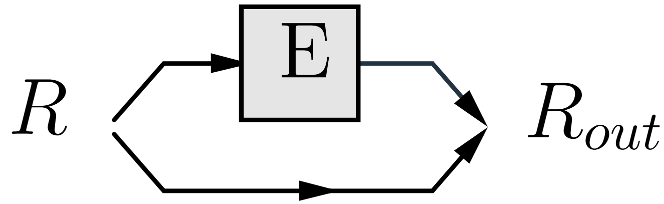
- The setup is expressed as the quantum operation

$$R_{out} = \mathrm{E} \otimes \mathrm{I}(R).$$

- For fixed *faithful* state R the output state R_{out} is in one-to-one correspondence with the QO of the device E.
- But now entangled states are easily available in the lab via parametric downconversion of vacuum!

Tomography of a quantum device

- **Quantum parallelism of entanglement: a single entangled input state R is equivalent to scanning all states in parallel.**



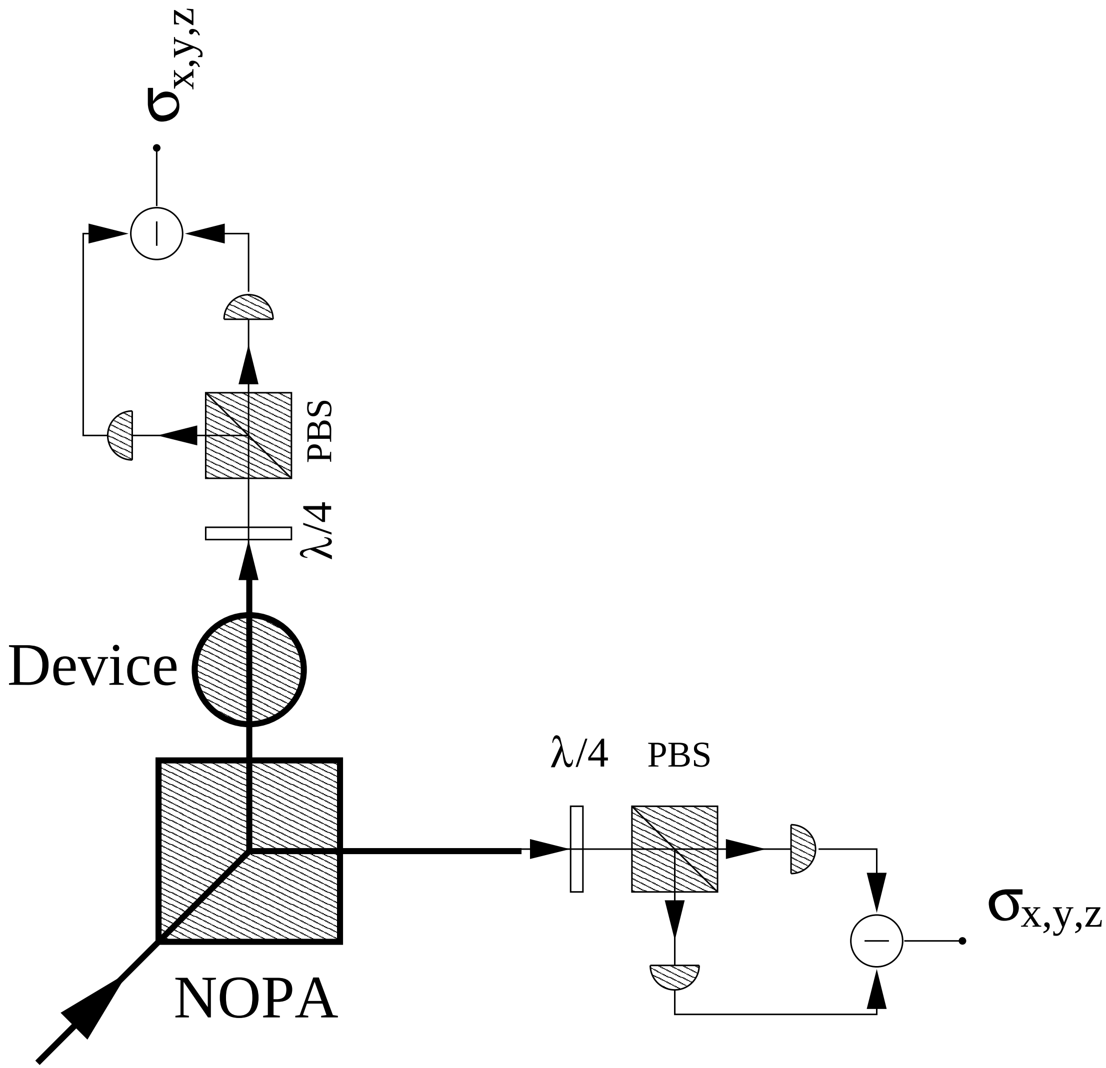
- The setup is expressed as the quantum operation

$$R_{out} = \mathrm{E} \otimes \mathrm{I}(R).$$

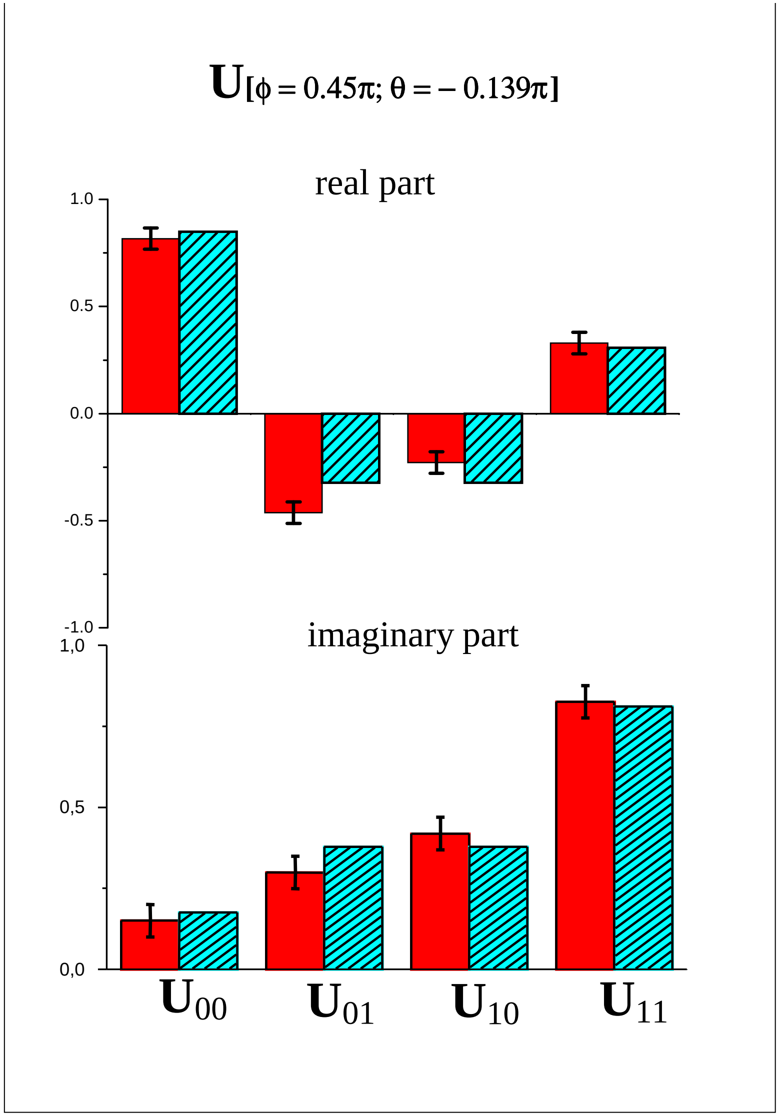
- For fixed *faithful* state R the output state R_{out} is in one-to-one correspondence with the QO of the device E.
- But now entangled states are easily available in the lab via parametric downconversion of vacuum!
- The method is very robust to noise [a state remains faithful under almost any kind of noise, e. g. depolarizing, etc].

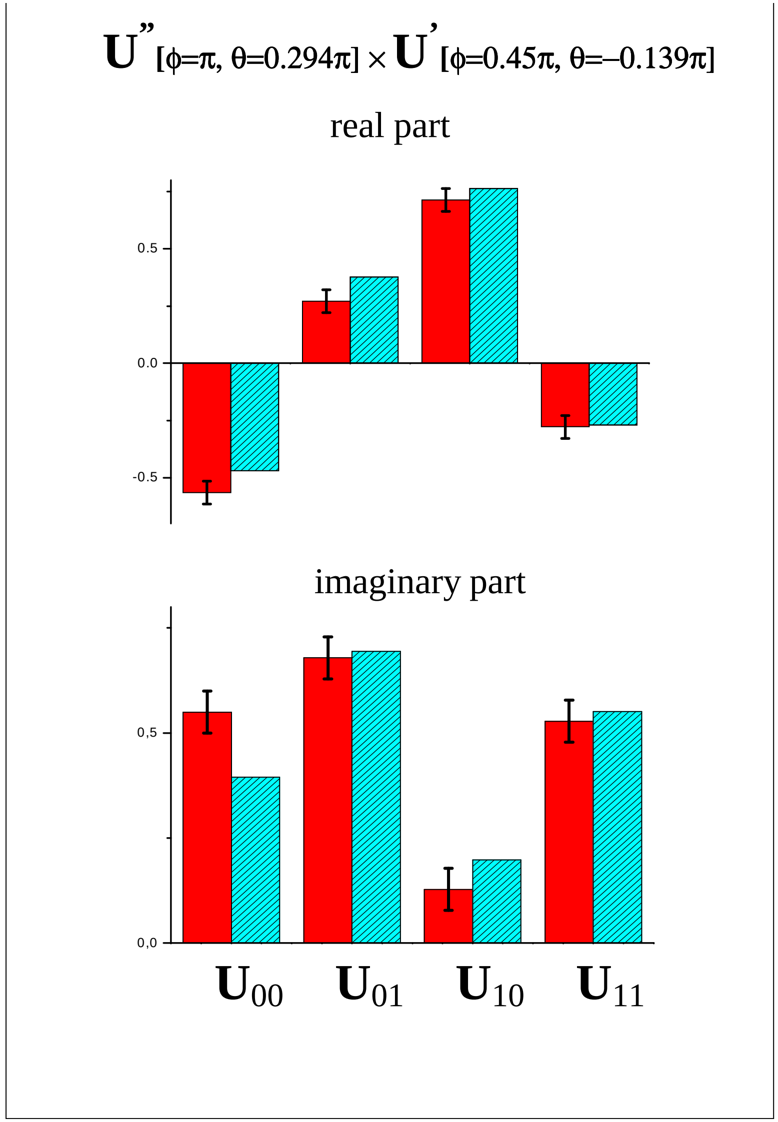
G. M. D'Ariano and P. Lo Presti, unpublished –

Tomography of a qubit device



Tomography of a qubit device

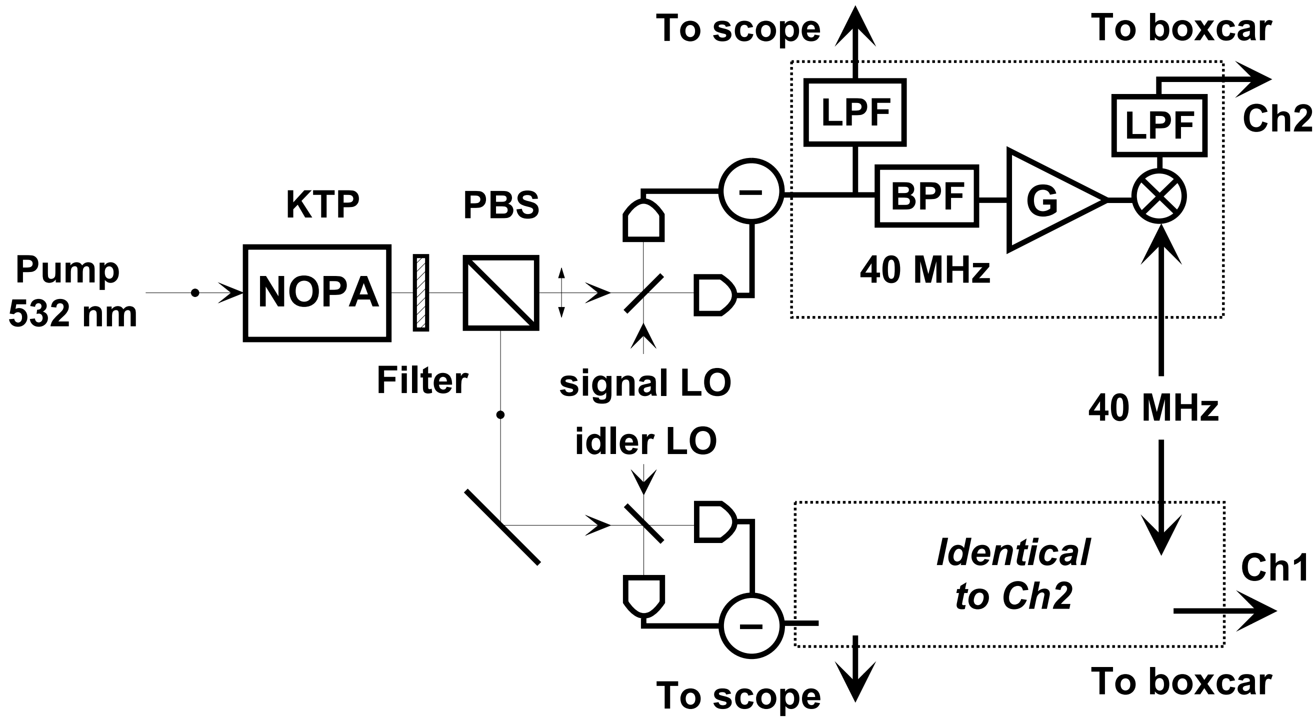




F. De Martini, G. M. D’Ariano, A. Mazzei, and M. Ricci, quant-ph/ – [17/32]

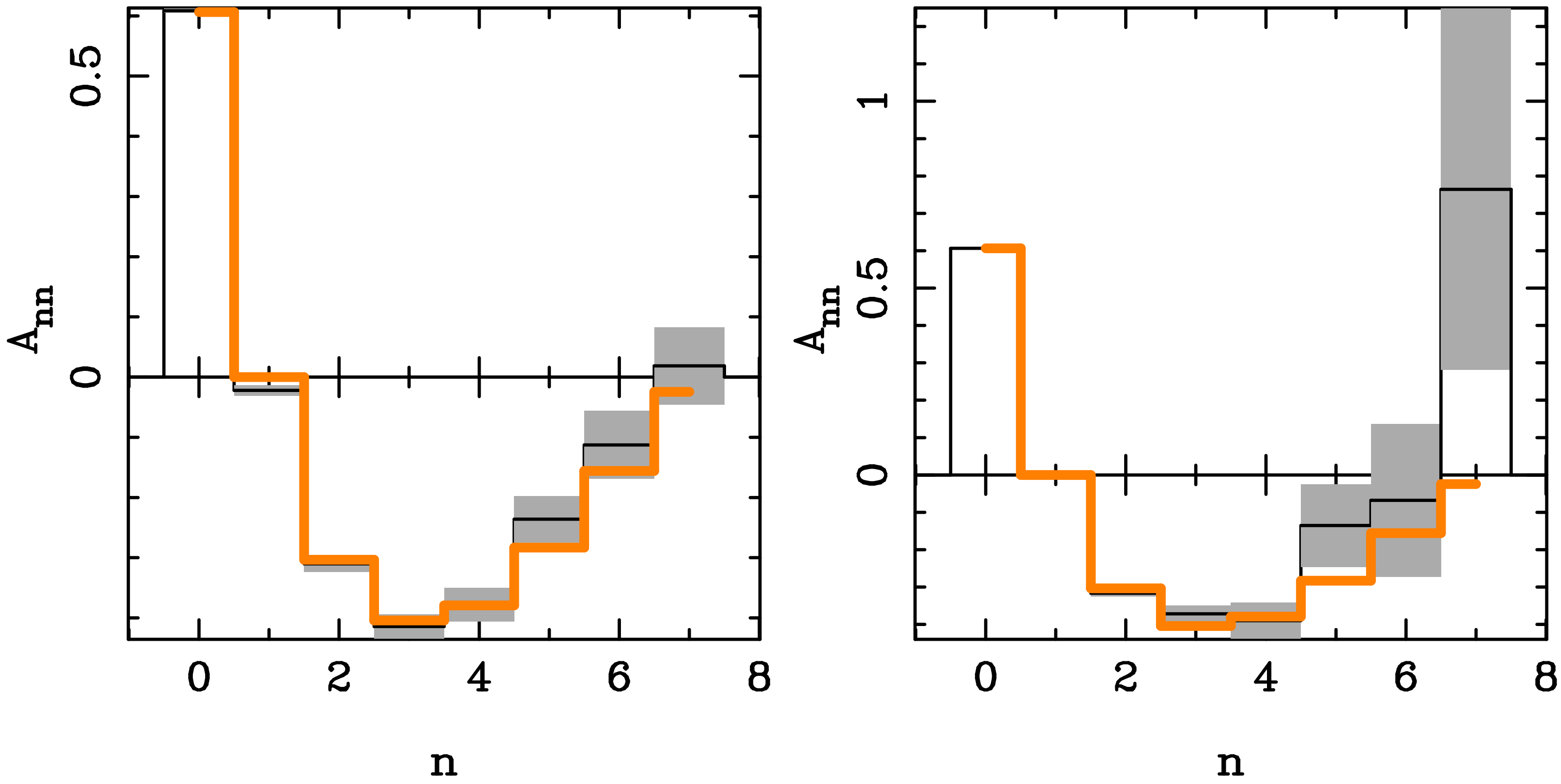
Tomography of a cv device

- Feasibility study for tomography of a displacer



Tomography of a cv device

- Feasibility study for tomography of a displacer



Left: $z = 1$, $\bar{n} = 5$, $\eta = 0.9$, and 150 blocks of 10^4 data have been used. Right: $z = 1$, $\bar{n} = 3$, $\eta = 0.7$, and 300 blocks of $2 \cdot 10^5$ data have been used.

D'Ariano and Lo Presti, PRL **86** 4195 (2001); Vasilyev, Choi, Kumar, and D'Ariano, PRL **84** 2354 (2000) –

Classification of QO extensions

Classification of QO extensions

1) Optimal discrimination between QO's (unitary)

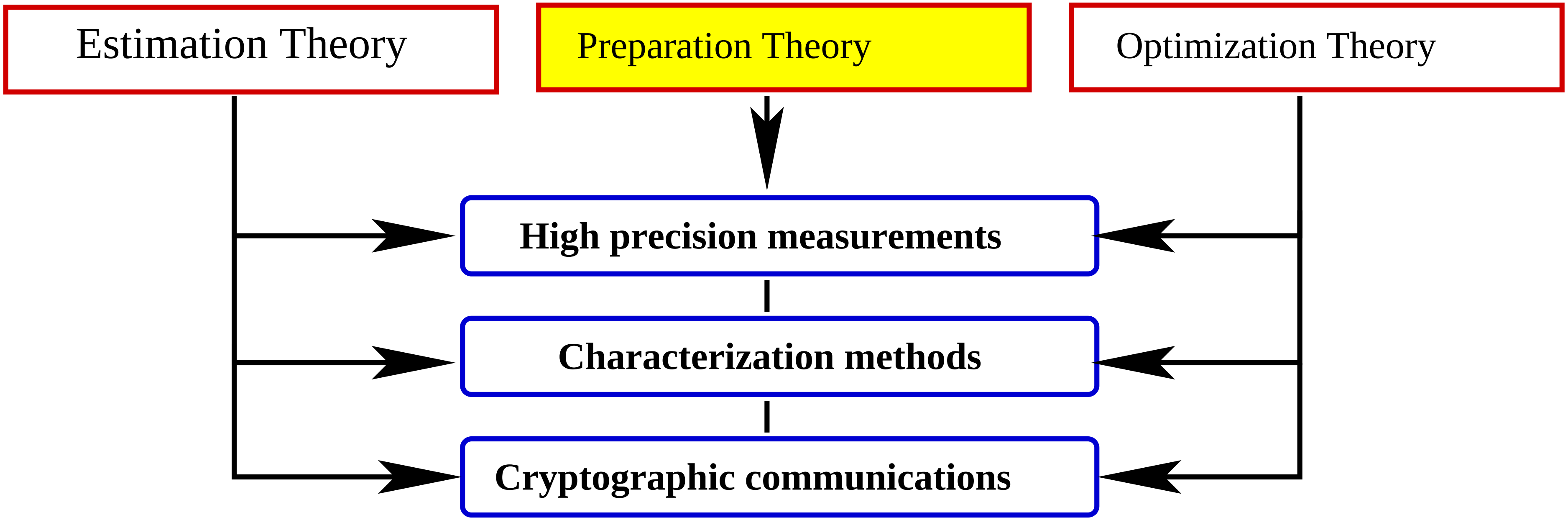
2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano and F. Buscemi (unpublished)
G. M. D'Ariano, P. Lo Presti, and R. Mecozzi (unpublished)

Classification of QO extensions



Which apparatuses for achieving a QO −−> Classification of unitary extensions of QO’s, ...

Classification of QO extensions

- Problem: Which unitary transformations, ancillas, etc. can be used to achieve a given QO?

Classification of QO extensions

- Problem: Which unitary transformations, ancillas, etc. can be used to achieve a given QO?
- The most general unitary extensions of a QO is of the form

$$\mathrm{E}(\rho) = \mathrm{Tr}_{\mathsf{F}}\{(I_{\mathsf{K}} \otimes \Sigma_{\mathsf{F}})U[|\phi\rangle\langle\phi|_A \otimes (\rho_{\mathsf{H}} \oplus O_{\mathsf{D}})]U^\dagger\},$$

Classification of QO extensions

- Problem: Which unitary transformations, ancillas, etc. can be used to achieve a given QO?
- The most general unitary extensions of a QO is of the form

$$\mathrm{E}(\rho) = \mathrm{Tr}_{\mathsf{F}}\{(I_{\mathsf{K}} \otimes \Sigma_{\mathsf{F}})U[|\phi\rangle\langle\phi|_A \otimes (\rho_{\mathsf{H}} \oplus O_{\mathsf{D}})]U^\dagger\},$$

where we have all these different Hilbert spaces:

Classification of QO extensions

- Problem: Which unitary transformations, ancillas, etc. can be used to achieve a given QO?
- The most general unitary extensions of a QO is of the form

$$\mathrm{E}(\rho) = \mathrm{Tr}_{\mathsf{F}}\{(I_{\mathsf{K}} \otimes \Sigma_{\mathsf{F}}) U [|\phi\rangle\langle\phi|_A \otimes (\rho_{\mathsf{H}} \oplus O_{\mathsf{D}})] U^\dagger\},$$

where we have all these different Hilbert spaces:

-

Symbol	Hilbert space	Symbol	Hilbert space
$\mathsf{H} \oplus \mathsf{D}$	Input system space	D	Conservation law constraint
A	Preparation ancilla	F	Measurement ancilla
$\mathrm{Rng}(\Sigma_{\mathsf{F}}) \subseteq \mathsf{F}$	Range of Σ_{F}	K	Output system space

Classification of QO extensions

- Problem: Which unitary transformations, ancillas, etc. can be used to achieve a given QO?
- The most general unitary extensions of a QO is of the form

$$\mathrm{E}(\rho) = \mathrm{Tr}_{\mathsf{F}}\{(I_{\mathsf{K}} \otimes \Sigma_{\mathsf{F}})U[|\phi\rangle\langle\phi|_A \otimes (\rho_{\mathsf{H}} \oplus O_{\mathsf{D}})]U^\dagger\},$$

where we have all these different Hilbert spaces:

Symbol	Hilbert space	Symbol	Hilbert space
$\mathsf{H} \oplus \mathsf{D}$	Input system space	D	Conservation law constraint
A	Preparation ancilla	F	Measurement ancilla
$\mathrm{Rng}(\Sigma_{\mathsf{F}}) \subseteq \mathsf{F}$	Range of Σ_{F}	K	Output system space

- $(\mathsf{H} \oplus \mathsf{D}) \otimes \mathsf{A} \simeq \mathsf{K} \otimes \mathsf{F}, \qquad \left(\mathrm{rank}(\mathrm{E}) + \left\lfloor \frac{\mathrm{rank}(I_{\mathsf{H}} - \mathrm{E}^\tau(I_{\mathsf{K}}))}{\dim(\mathsf{K})} \right\rfloor\right) \dim(\mathsf{K}) \geq \dim(\mathsf{H})$

Classification of QO extensions

- All Kraus decompositions $\{E_i\}$ must satisfy the majorization relation with respect to the canonical one $\{K_j\}$

$$[\|E_i\|_2^2] \prec [\|K_j\|_2^2].$$

Classification of QO extensions

- All Kraus decompositions $\{E_i\}$ must satisfy the majorization relation with respect to the canonical one $\{K_j\}$

$$[\|E_i\|_2^2] \prec [\|K_j\|_2^2].$$

- Therefore, we have a constraint which must be satisfied by the unitary operator U in order to achieve the QO E

$$\{(I_{\mathsf{K}} \otimes \langle\sigma_i|_{\mathsf{F}})U(|\phi\rangle_{\mathsf{A}} \otimes I_{\mathsf{H}})\} = E_i,$$

Classification of QO extensions

- All Kraus decompositions $\{E_i\}$ must satisfy the majorization relation with respect to the canonical one $\{K_j\}$

$$[\|E_i\|_2^2] \prec [\|K_j\|_2^2].$$

- Therefore, we have a constraint which must be satisfied by the unitary operator U in order to achieve the QO E

$$\{(I_{\mathsf{K}} \otimes \langle\sigma_i|_{\mathsf{F}})U(|\phi\rangle_{\mathsf{A}} \otimes I_{\mathsf{H}})\} = E_i,$$

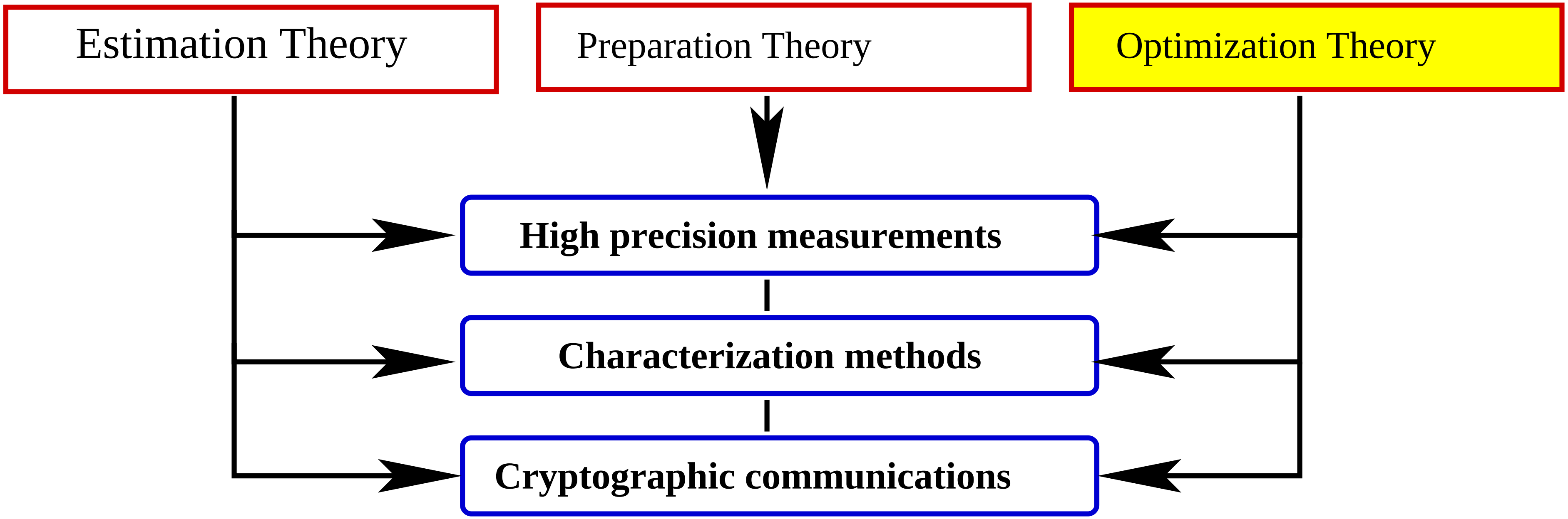
where $\Sigma_{\mathsf{F}} = \sum_i |\sigma_i\rangle\langle\sigma_i|_{\mathsf{F}}$, and

$$\dim \mathsf{F} \geq \mathrm{rank}(\Sigma_{\mathsf{F}}) \geq \mathrm{rank}(\mathrm{E}).$$

Extremal QO's and POVM's

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's



Which is the optimal QO to achieve a given purpose [in terms of a cost function]

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's

- Useful in optimization problems;

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's

- Useful in optimization problems;
- Extremal QO's [classified by Choi (1975)] $K_i^\dagger K_j$ linearly independent.

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's

- Useful in optimization problems;
- Extremal QO's [classified by Choi (1975)] $K_i^\dagger K_j$ linearly independent.
- Physical meaning: they can be achieved with an indirect measurement scheme with faithful state reduction.

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's

- Useful in optimization problems;
- Extremal QO's [classified by Choi (1975)] $K_i^\dagger K_j$ linearly independent.
- Physical meaning: they can be achieved with an indirect measurement scheme with faithful state reduction.
- Extremal POVM's: classification of quantum and classical noise.

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

Extremal QO's and POVM's

- Useful in optimization problems;
- Extremal QO's [classified by Choi (1975)] $K_i^\dagger K_j$ linearly independent.
- Physical meaning: they can be achieved with an indirect measurement scheme with faithful state reduction.
- Extremal POVM's: classification of quantum and classical noise.
  - *Theorem:* A POVM $\{P_e\}_{e\in\mathsf{E}}$ with spectral resolution $P_e = \sum_i |v_i^{(e)}\rangle\langle v_i^{(e)}|$ is extremal if and only if the operators

$$|v_i^{(e)}\rangle\langle v_j^{(e)}|,\quad \text{for all events } e\in\mathsf{E},\ \text{and all } i,j$$

are linearly independent.

D'Ariano and Buscemi (unp.); D'Ariano, Lo Presti and Mecozzi (unp.); Parthasaraty, Inf. Dim. Anal. **2** 557 (1999)

The Quantum Bit Commitment

The Quantum Bit Commitment

1) Optimal discrimination between QO's (unitary)

2) Tomographic characterization of QO's using entangled input

3) Classification of all unitary extensions of QO's, extremal QO's and POVM's

4) Classification of all QBC protocols, and bounds for the probabilities of cheating

G. M. D'Ariano, QCM&C 2002, Boston (preprint available)

The Quantum Bit Commitment

- Commitment:  provides  with a piece of evidence that she has chosen a bit $b = 0, 1$ which she commits to him.
- Opening: Later  will open the commitment, revealing b to , and proving that it is indeed the committed bit with the evidence in Bob's possession, i. e.  will check the commited bit.

The Quantum Bit Commitment

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

The Quantum Bit Commitment

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

The Quantum Bit Commitment

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

The Quantum Bit Commitment

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

(3) The evidence should be *verifiable*, namely  must be able to check b unambiguously against the evidence in his possession.

The Quantum Bit Commitment

- Therefore, Alice and Bob should agree on a protocol which satisfies simultaneously the three requirements:

(1) The evidence should be *concealing*, namely  should not be able to retrieve b before the opening.

(2) The evidence should be *binding*, namely  should not be able to change b after the commitment.

(3) The evidence should be *verifiable*, namely  must be able to check b unambiguously against the evidence in his possession.

- Both parties are supposed to possess unlimited technology, and the protocol is said *unconditionally secure* if neither Alice nor Bob can cheat with significant probability of success as a consequence of physical laws.

The Quantum Bit Commitment

- Bit modulation: QO parametrized by $b = 0, 1$.

The Quantum Bit Commitment

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from H to K.

The Quantum Bit Commitment

- Bit modulation: QO parametrized by $b = 0, 1$.
- To make the protocol concealing and at the same time verifiable, the modulation is a choice between two ensembles of QO's $\{\mathrm{M}_j^{(b)}\}$ for $b = 0, 1$ from H to K.

  – j: secret parameter known only to  .

The Quantum Bit Commitment

-  has always the option of choosing j by preparing a secret-parameter space P in the state $|j\rangle$ and performing a QO on an extended Hilbert space which includes P.

The Quantum Bit Commitment

-  has always the option of choosing j by preparing a secret-parameter space P in the state $|j\rangle$ and performing a QO on an extended Hilbert space which includes P.
- Strictly trace-decreasing maps correspond to aborting protocols, namely when  doesn't succeed in achieving the QO the protocol is aborted.

The Quantum Bit Commitment

-  has always the option of choosing j by preparing a secret-parameter space P in the state $|j\rangle$ and performing a QO on an extended Hilbert space which includes P.
- Strictly trace-decreasing maps correspond to aborting protocols, namely when  doesn't succeed in achieving the QO the protocol is aborted.
- Since  has unlimited technology, she can always achieve the map *knowingly*, i. e. she has the option of achieving each QO as a *perfect pure measurement*.

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space A $\otimes$ P,

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space $\mathsf{A} \otimes \mathsf{P}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space $\mathsf{A} \otimes \mathsf{P}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on $\mathsf{F} \otimes \mathsf{P}$, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space $\mathsf{A} \otimes \mathsf{P}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on $\mathsf{F} \otimes \mathsf{P}$, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

(4) sending K to  .

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space $\mathsf{A} \otimes \mathsf{P}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on $\mathsf{F} \otimes \mathsf{P}$, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

(4) sending K to  .

- For aborting protocols we have an additional orthogonal projector Σ_{F}, whose rank generally depends on j and b.

The Quantum Bit Commitment

- Therefore  achieves the QO knowingly by:

(1) preparing ancilla and secret parameter space $\mathsf{A} \otimes \mathsf{P}$,

(2) performing a unitary transformation U on $\mathsf{H} \otimes \mathsf{A}$,

(3) performing a complete von Neumann measurement on $\mathsf{F} \otimes \mathsf{P}$, with $\mathsf{K} \otimes \mathsf{F} \simeq \mathsf{H} \otimes \mathsf{A}$ and outcome i,

(4) sending K to  .

- For aborting protocols we have an additional orthogonal projector Σ_{F}, whose rank generally depends on j and b.

$\Rightarrow$ For simplicity, we focus attention on non aborting protocols.

The Quantum Bit Commitment

- **Opening step:** In a *perfectly verifiable* protocol  tells b along with the *secret parameter* j and the *secret outcome* i to , who verifies the pure state $E^{(b)}_{ji}|\varphi\rangle \equiv E^{(b)}_{J}|\varphi\rangle$.

The Quantum Bit Commitment

- Opening step: In a *perfectly verifiable* protocol  tells b along with the *secret parameter* j and the *secret outcome* i to , who verifies the pure state $E_{ji}^{(b)}|\varphi\rangle \equiv E_J^{(b)}|\varphi\rangle$.

- Since the local QO's on K and F $\otimes$ P commute,  has the possibility of: first sending K to  and then performing the measurement on F $\otimes$ P at the very last moment of the opening! Before  launches her EPR cheating attack V on F $\otimes$ P!

The Quantum Bit Commitment

- Opening step: In a *perfectly verifiable* protocol  tells b along with the *secret parameter* j and the *secret outcome* i to  , who verifies the pure state $E_{ji}^{(b)}|\varphi\rangle \equiv E_J^{(b)}|\varphi\rangle$.

- Since the local QO's on K and F $\otimes$ P commute,  has the possibility of: first sending K to  and then performing the measurement on F $\otimes$ P at the very last moment of the opening! Before  launches her EPR cheating attack V on F $\otimes$ P!

- On the other side,  can try to discriminate between the two mixtures of QO's by launching his own EPR attach at the very beginning of the commitment, by entangling the anonymous state with a system in his possession.

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Symbol	Hilbert space	Symbol	Hilbert space
H	Anonymous state	K	Output
A	Preparation ancilla	P	Secret parameter
F	Measurement ancilla	R	Bob cheating space
$\mathrm{Rng}(\Sigma_F)$	Range of Σ_F (abortion)		

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Symbol	Hilbert space	Symbol	Hilbert space
H	Anonymous state	K	Output
A	Preparation ancilla	P	Secret parameter
F	Measurement ancilla	R	Bob cheating space
$\mathrm{Rng}(\Sigma_{\mathsf{F}})$	Range of Σ_{F} (abortion)		

- All alternate Kraus decompositions $\{E_J^{(b)}\}$ correspond to different openings.

Commitment: summary

- Classification of protocols $\equiv$ classifications of QO extensions

Symbol	Hilbert space	Symbol	Hilbert space
H	Anonymous state	K	Output
A	Preparation ancilla	P	Secret parameter
F	Measurement ancilla	R	Bob cheating space
$\mathrm{Rng}(\Sigma_{\mathrm{F}})$	Range of Σ_{F} (abortion)		

- All alternate Kraus decompositions $\{E_J^{(b)}\}$ correspond to different openings.

- Alice EPR-cheating transformation: unitary V on P $\otimes$ F: corresponds to change the Kraus decomposition from $\{E_J^{(0)}\} \to \{E_J^{(0)}(V)\}$

Bounds for cheating probabilities

$$P_c^A(V,\varphi) \geq \sqrt{1 - \sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2},$$

$$2P_c^B - 1 \leq \left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \leq \sqrt{\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2}.$$

Bounds for cheating probabilities

$$P_c^A(V,\varphi) \geq \sqrt{1 - \sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2},$$

$$2P_c^B - 1 \leq \left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \leq \sqrt{\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2}.$$

- However, it has not been proved that there is a V such that

$$\sum_J \left\| E_J^{(0)}(V) - E_J^{(1)} \right\|^2 \leq \omega\left(\left\| \mathrm{M}^{(1)} - \mathrm{M}^{(0)} \right\|_{cb} \right),$$

with $\omega(\varepsilon)$ vanishing with ε.

Summary

- Encoding information on QO's more general than on states:

Summary

- Encoding information on QO’s more general than on states:

⇒ it includes anonymous input states.

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.

Summary

- Encoding information on QO's more general than on states:

⇒ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

$\Rightarrow$ experiments.

Summary

- Encoding information on QO's more general than on states:

⇒ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

⇒ experiments.

- Classification of QO's unitary extensions:

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

$\Rightarrow$ experiments.

- Classification of QO's unitary extensions:

$\Rightarrow$ constraints for U corresponding to a QO;

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

$\Rightarrow$ experiments.

- Classification of QO's unitary extensions:

$\Rightarrow$ constraints for U corresponding to a QO;

$\Rightarrow$ extremal QO's and POVM's;

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

$\Rightarrow$ experiments.

- Classification of QO's unitary extensions:

$\Rightarrow$ constraints for U corresponding to a QO;

$\Rightarrow$ extremal QO's and POVM's;

- Classification of QBC protocols:

Summary

- Encoding information on QO's more general than on states:

$\Rightarrow$ it includes anonymous input states.

- Better distinguishability for QO's than for states.
- Tomography of QO's using entangled/faithful states:

$\Rightarrow$ experiments.

- Classification of QO's unitary extensions:

$\Rightarrow$ constraints for U corresponding to a QO;

$\Rightarrow$ extremal QO's and POVM's;

- Classification of QBC protocols:

$\Rightarrow$ bounds for the probabilities of cheating.