

Device-Independent Quantum Information Processing

Antonio Acín

ICREA Professor at ICFO-Institut de Ciències Fotòniques, Barcelona

Chist-Era kick-off seminar, March 2012, Warsaw, Poland



Quantum Information Theory

Quantum Information Theory studies how to manipulate and transmit information encoded on quantum particles.

Quantum Mechanics:

set of laws describing
the Physics of the
microscopic world.

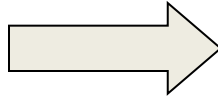


Information Theory:

set of laws describing
how information can
be manipulated.

Quantum Information Theory

What happens when we encode information in the quantum world?



Novel information applications become possible when using information encoded on quantum states, e.g. more powerful computers and secure communication.

Computational security

- Standard Classical Cryptography schemes are based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- Even with this assumption, the security is unproven. E.g.: factoring is believed to be a hard problem.
- Quantum computers sheds doubts on the long-term applicability of these schemes, e.g. Shor's algorithm for efficient factorization.

Quantum Computation

Quantum computer: device able to manipulate information encoded on quantum particles. These devices allow one to solve computational problems in a much more efficient way than a classical computer.

Shor's algorithm (1994): factorization problem.

$6 = 3 \times 2$ Easy!

$30790518401361202507 = 4575351673 \times 6729650659$



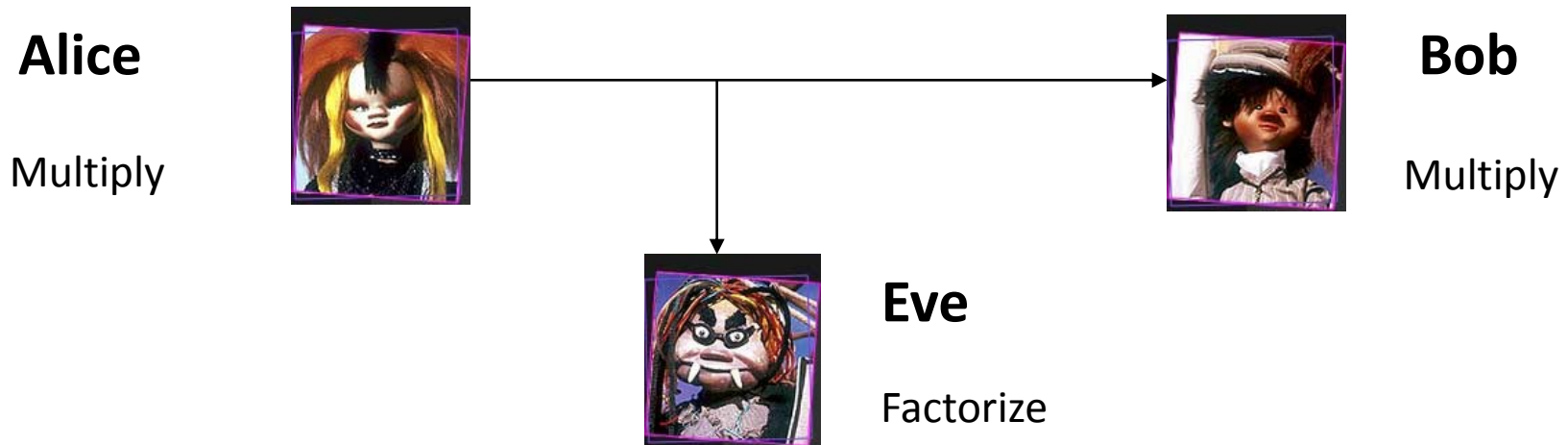
A quantum computer allows the efficient factorization of large numbers.

Which problems are easy for a quantum computer?

Computational security

It was easy to generate the factors and then compute the product.
One-way functions: easy in one direction, hard in the opposite.

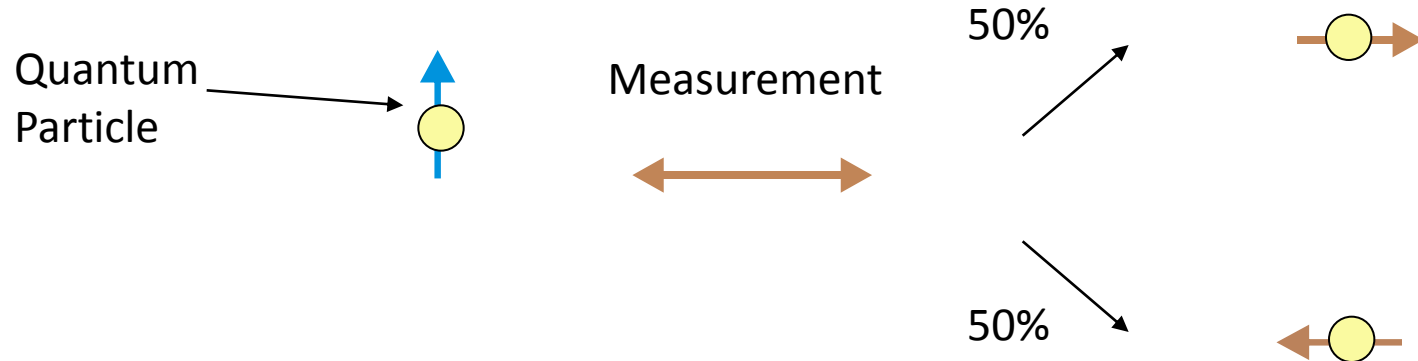
Many cryptographic schemes, such as RSA, are based on the factorization problem.



If factorization becomes easy, the enemy can break the protocol!

Heisenberg Uncertainty Principle

Quantum Theory only predicts the probabilities of outcomes.

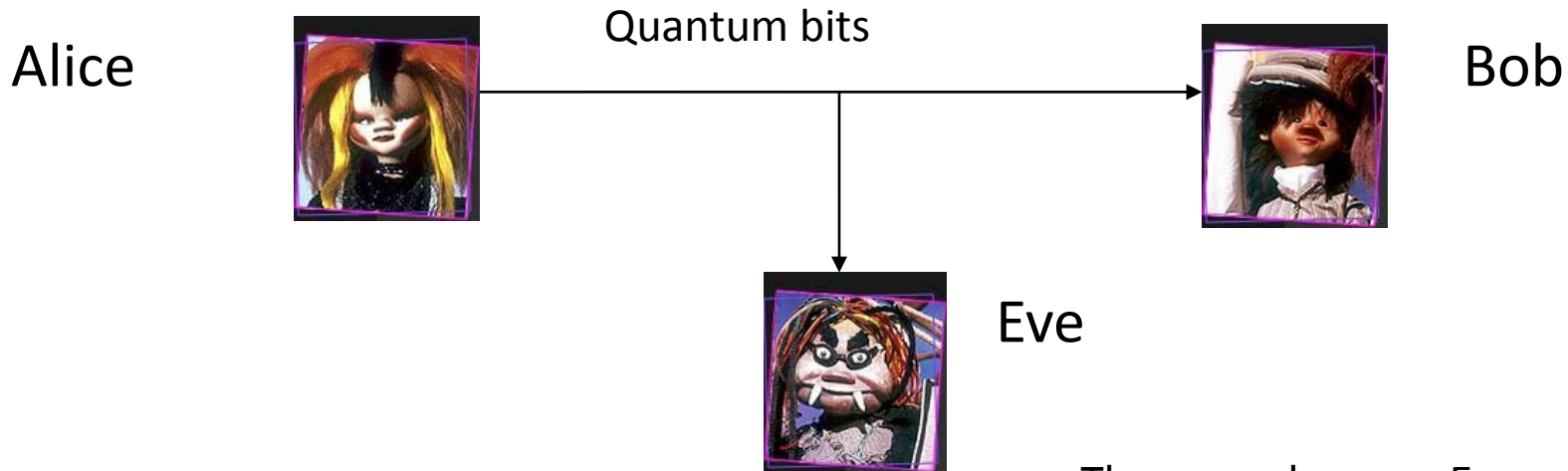


The measurement process modifies the state of the particle!

Heisenberg uncertainty principle: the measurement process perturbs the state of a quantum system.

Quantum Cryptography

Heisenberg uncertainty principle → Secure cryptography!



The eavesdropper, Eve, when measuring the particles, introduces noise, errors, in the channel and is detected by the honest parties.



Bennett



Brassard



Ekert

Quantum Cryptography: a new form of security

- Standard Cryptography is based on computational security.
Quantum Cryptography is based on physical security.
- Assumption: eavesdropper computational power is limited.
Quantum Mechanics offers a correct physical description of the devices.
- Even with this assumption, the security is unproven.
- No assumption is required on the eavesdropper's power, provided it does not contradict any quantum law.
E.g.: factoring is believed to be a hard problem.
- Quantum computers sheds doubts on the long-term applicability of these schemes, e.g. Shor's algorithm for efficient factorization.
- Using this (these) assumption(s), the security of the schemes can be proven.

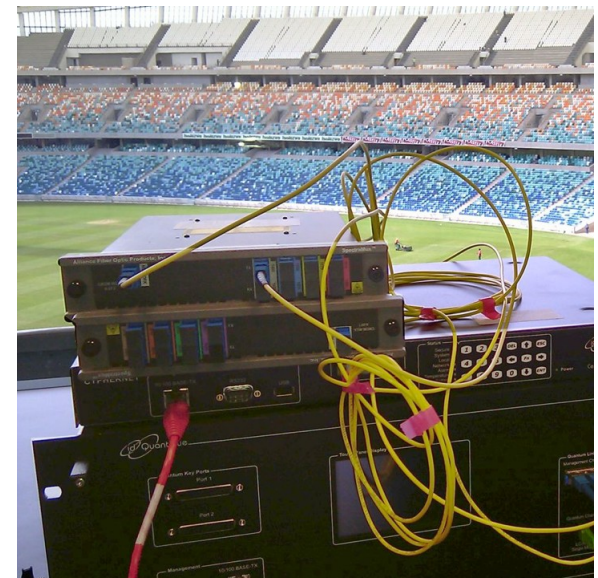
Quantum Cryptography: you can buy it!

- Quantum cryptography is a commercial product.



Ribordy

- In 2007, it was used to secure part of the vote counting in a referendum in the canton of Geneva.
- The Quantum Stadium: in 2010, in collaboration with the University of Kwazulu-Natal, South Africa, it was used to encrypt a connection in the Durban stadium during the World Cup.



Quantum hacking

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Published online 29 August 2010 | Nature | doi:10.1038/news.2010.436

News

Hackers blind quantum cryptographers

Lasers crack commercial encryption systems, leaving no trace.

Zeeya Merali

How come?!



Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

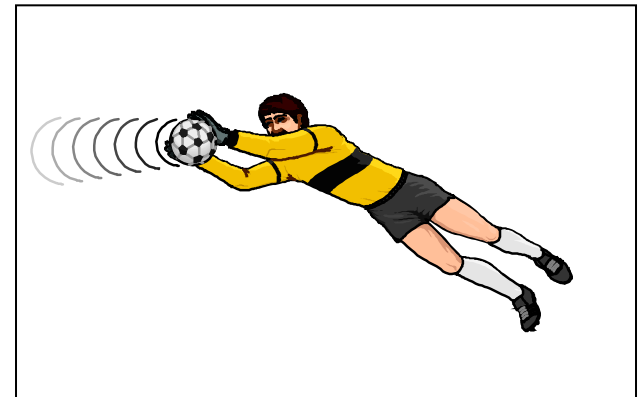


~~Single photon source~~

Attenuated laser source



Quantum channel



~~Single photon detector~~

Realistic APD detector

The problem

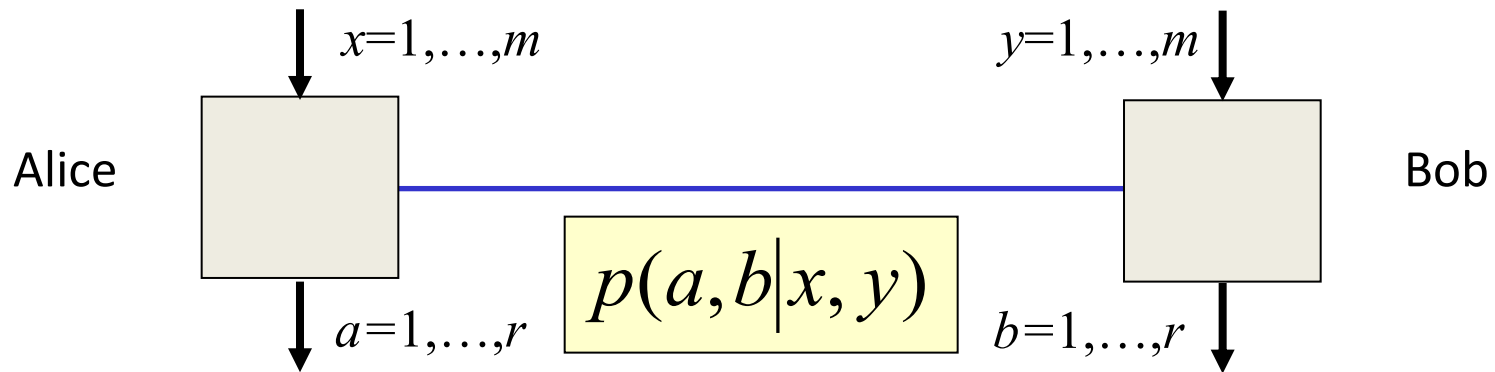
How can one assess the level of security provided by real-life implementations of quantum key distribution, or more generally, quantum information protocols, which will inevitably differ in inconspicuous ways from the idealized, theoretical description?

Device-Independent Quantum Information Processing

Device-Independent Quantum Information Processing represents a new paradigm for quantum information processing: the goal is to design protocols to solve relevant information tasks without relying on any assumption on the internal working of the devices used in the protocol.

Scenario

Distant parties performing m different measurements of r outcomes.



Goal: to perform an information task, eg to distribute a secret key, only from the observed correlations between devices, $(\quad | \quad)$.

Standard Quantum Information applications are not device-independent: they crucially rely on the details of states and measurements used in the protocol.

Physical Correlations

Physical principles translate into limits on correlations.

1) **Classical correlations:** correlations established by classical means.

$$p(a,b|x,y) = \sum_{\lambda} p(\lambda) p(a|x,\lambda) p(b|y,\lambda)$$

These are the standard “EPR” correlations. Independently of fundamental issues, these are the correlations achievable by classical resources. Bell inequalities define the limits on these correlations.

Physical Correlations

2) **Quantum correlations:** correlations established by quantum means.

$$p(a, b|x, y) = \text{tr}(\rho_{AB} M_a^x \otimes M_b^y)$$

$$\sum_a M_a^x = I$$

$$M_{a'}^x M_a^x = \delta_{a'a} M_a^x$$

3) **No-signalling correlations:** correlations compatible with the no-signalling principle, i.e. the impossibility of instantaneous communication.

$$\sum_b p(a, b|x, y) = p(a|x)$$

Quantum non-locality

- The set of quantum correlations is strictly larger than the set of classical correlations.
- This is because of the existence of non-local quantum correlations, that is, quantum correlations that violate a Bell inequality. These inequalities are satisfied by classical correlations
- If some correlations do not violate any Bell inequality, then there exists a classical model for them. Thus, no improvement can be expected over Classical Information Theory.
- Any protocol should be built from non-local correlations. Quantum non-locality is the resource for DIQIP.
- DIQIP can be understood as the use of non-locality as a resource for information processing.

Device-Independent QKD

Standard QKD protocols based their security on:

1. Quantum Mechanics: any eavesdropper, however powerful, must obey the laws of quantum physics.
2. No information leakage: no unwanted classical information must leak out of Alice's and Bob's laboratories.
3. Trusted Randomness: Alice and Bob have access to local random number generators.
4. Knowledge of the devices: Alice and Bob require some control (model) of the devices.

There are protocols for secure QKD based on $p(a, b|x, y)$ without requiring any assumption on the devices.

The project

Device-Independent Quantum Information Processing represents a new paradigm for quantum information processing: the goal is to design protocols to solve relevant information tasks without relying on any assumption on the devices used in the protocol. For instance, protocols for device-independent key distribution aim at establishing a secret key between two honest users whose security is independent of the devices used in the distribution. Contrary to standard quantum information protocols, which are based on entanglement, the main resource for device-independent quantum information processing is quantum non-locality. Apart from the conceptual interest, device-independent protocols offer important advantages from an implementation point of view: being device-independent, the realizations of these protocols, though technologically challenging, are more robust against device imperfections. Current and near-future technology offer promising perspectives for the implementation of device-independent protocols.

The project structure

- **Study of non-local quantum correlations:** The goal is to study quantum correlations in general, with an emphasis on non-local correlations. We will consider different approaches to tackle this question. In particular, we will study non-local quantum correlations from an information perspective, identifying information-based principles that are able to characterize this set of correlations.
- **Device-independent quantum information processing:** Here, the goal is to exploit non-local correlations for information processing. We will mostly work in the device-independent scenario, where the presence of non-local correlations is a necessary ingredient. We want to improve the analysis of the existing device-independent applications and derive protocols for new tasks.
- **Towards experimental implementations of device-independent protocols:** Finally, we plan to consider how all these ideas could be experimentally tested and how device-independent protocols can be adapted to present and near-future technology. This is a theory project and, as such, no experiments are planned. However, we expect to have close interaction with experimental groups and potentially collaborate with them in the demonstration of these concepts.

Who we are

Partner Number	Country	Institution/ Department	Name of the group leader	Name of other personnel participating in the project
1 <i>Coordinator</i>	Spain	ICFO-The Institute of Photonic Sciences (ICFO)	Antonio Acín	Maciej Lewenstein Lluís Masanes
2	Switzerland	GAP-Optique, ETH (GAP-ETH)	Nicolas Gisin	Renato Renner Stefan Wolf Yeong-Cherng Liang
3	France	Laboratoire de Recherche en Informatique (LRI)	Sophie Laplante	Julia Kempe Iordanis Kerenidis Frédéric Magniez Miklos Santha
4	Belgium	Université Libre de Bruxelles / Laboratoire d'Information Quantique (ULB)	Serge Massar	Stefano Pironio Jonathan Silman Ross Duncan Unknown (PhD or post-doc)
5	UK	University of Bristol (UoB)	Sandu Popescu	Noah Linden Andreas Winter Nicolas Brunner
6	UK	Royal Holloway, University of London (RH)	Jonathan Barrett	

What we plan to do

Study of non-local quantum correlations

Tasks	
T1.1	Characterization of multipartite non-locality (RH; ULB, GAP-ETH, ICFO, UoB) The goal is to improve our understanding of quantum non-locality and genuine multipartite non-locality in the scenario consisting of more than two parties. We will study the simulation of quantum states by classical resources, the extension of techniques such as bilocality to this scenario or the relation among the possible definitions of genuine multipartite non-locality.
T1.2	Complexity aspects of non-local games (LRI; ULB, ICFO) The goal is to study communication and non-local boxes as a measure of how non-local, or non-quantum, a particular distribution is. We will also use communication complexity techniques to determine how big the gaps are among the different families of correlations. A second objective is to study the complexity of quantum multipartite games from the perspective of multi-prover systems with entanglement.
T1.3	Information principles and quantum correlations (UoB; ICFO, ULB, RH) The goal is to compare the different information-based principles which bound the set of quantum correlations, in order to see whether some ordering among them can be established or how much of the quantum structure they can each recover. We will also compare them at different levels of the SDP hierarchy for quantum correlations.

What we plan to do

Device-independent quantum information processing

Tasks	
T2.1	Trade-off between non-locality and randomness (ICFO; ULB) Here we want to establish quantitative relations between the amount of randomness and non-locality in quantum systems. How does randomness scale with a Bell violation, or with the number of parties? The use of the SDP hierarchy will be crucial in this part.
T2.2	Improved DIQKD protocols (ULB; GAP-ETH, ICFO, RH) Our objective is to study better DIQKD protocols, even under the present security proofs. We will consider other Bell inequalities, relaxations of the original fully device-independent scenario based on bilocality or bounded adversary models, or two-way communication techniques.
T2.3	Better security proofs for DIQKD (GAP-ETH; ULB, ICFO, RH) Our goal is to establish stronger security proofs, enlarging the existing ones to more practical situations. The main objective is to understand how memory effects can be incorporated in these proofs. At the moment, we identify three possible approaches to solve this issue based on smooth entropies, martingale theory or uncertainty relations.

What we plan to do

Towards experimental implementations of device-independent protocols

Tasks	
T3.1	Bell tests more robust against noise or detection inefficiencies (UoB; GAP-ETH, ULB, ICFO, LRI) Here we will study the design of Bell tests more robust against imperfections, especially for device-independent applications. We will consider different scenarios by changing the number of measurement and outcomes, the dimension of the involved particles or the type of measurements. We will also consider new approaches to quantum non-locality based on networks and entanglement swapping.
T3.2	Detection and simulation of quantumness in many-body systems (ICFO; ULB, GAP-ETH) The goal will be study the application of our theoretical formalism to many-body systems. We will design device-independent witnesses for genuine multipartite entanglement. We also plan to propose novel few- and many-body systems to test the “quantumness” of temporal correlations.
T3.3	Feasibility studies for DI protocols (GAP-ETH; ULB,ICFO) We will consider experimental implementations of device-independent protocols with technology available today or in the near future. Physical systems considered will include trapped atoms, superconducting qubits, photons. In the latter case, we will consider the role of losses and how this problem can be solved using noiseless amplifiers or non-demolition quantum measurements. Finally, we will study hybrid scenarios where components of the implementation – e.g. detectors – are trusted.

Some numbers

- Starting date of the project: September 1st 2011
- Kick-off meeting in Geneva, 23-25 November 2011
- First-year meeting in Barcelona in June 2012. It will be organized together with the EU STREP Project Quantum Computer Science (QCS).
- **Cut: no coordination money.** No conference, as initially planned.
- 13 works have already appeared. At the moment, they are most under review, but available on-line.
- 5 of these works have been published or accepted for publication, 3 of them in Physical Review Letters.
- 9 of these works are collaborations among members of the consortium.

Study of non-local quantum correlations

The definition of multipartite nonlocality

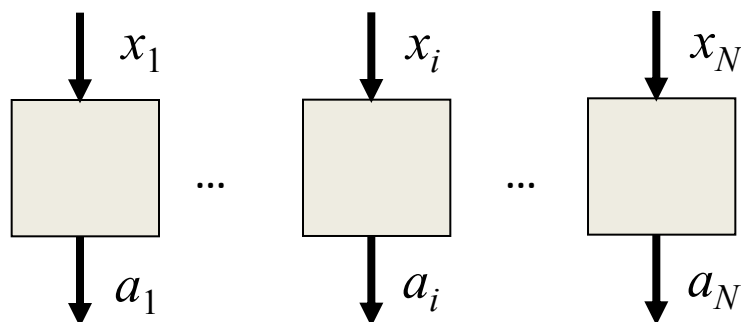
J. Barrett, S. Pironio, J.-D. Bancal, N. Gisin

RH+ULB+GAP

An operational framework for nonlocality

R. Gallego, L. E. Würflinger, A. Acín, M. Navascués

UoB+ICFO



When do N systems share multipartite non-local correlations?

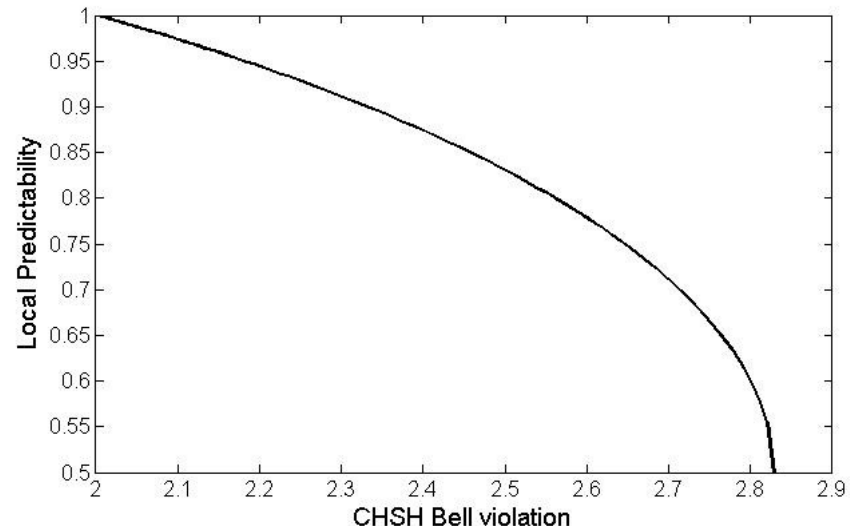
- These works question our current understanding of genuine multipartite non-locality, which is based on the pioneering works of Svetlichny.
- This standard approach is incompatible with an operational framework in which non-locality is seen as a resource for information processing.
- They provide new formulations for which consistency is recovered.

Device-independent quantum information processing

Security of practical private randomness generation

S. Pironio, S. Massar

Measurements on entangled quantum systems necessarily yield outcomes that are intrinsically unpredictable if they violate a Bell inequality. This property can be used to generate certified randomness in a device-independent way.

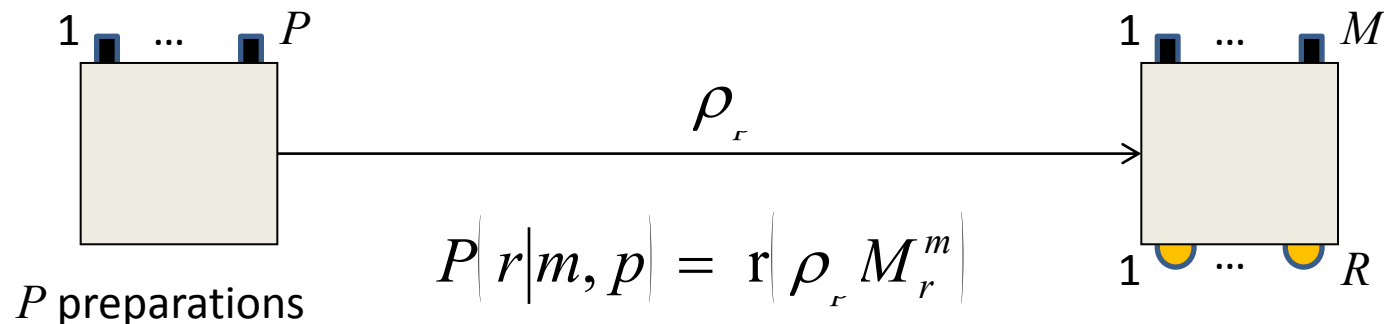


- It is argued in this work that in most real, practical situations, it is sufficient to show that the generated string is random with respect to an adversary that holds only classical-side information.
- The paper also gives a precise theoretical framework for practical device-independent randomness expansion.

Towards experimental implementations of device-independent protocols

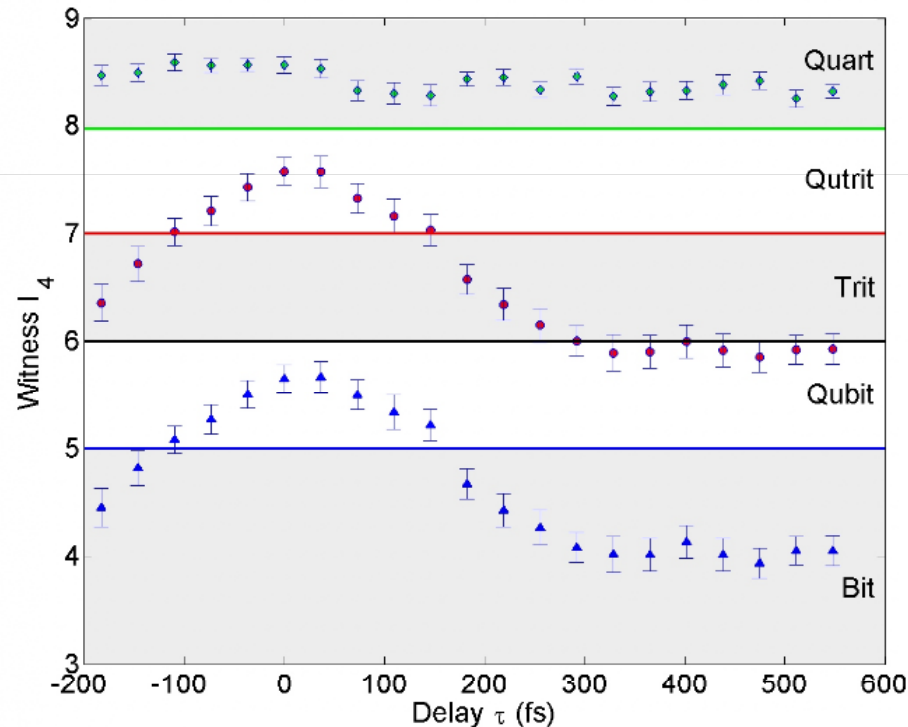
Experimental estimation of the dimension of classical and quantum systems
 M. Hendrych, *R. Gallego*, *N. Brunner*, M. Micuda, *A. Acín*, J. P. Torres
ICFO+UoB

Goal: to estimate the dimension of an unknown quantum (classical) system.



What's the minimal dimension of the mediating quantum particle needed to reproduce the observed correlations?

Towards experimental implementations of device-independent protocols



Polarization and orbital angular momentum was used to prepare states and perform measurements up to dimension four. The witness I_4 was estimated.

	Bit	Qubit	Trit	Qutrit	Quart
I_4	5	6	7	7.9689	9

Conclusions

- Device-independent quantum information processing is a new paradigm for quantum information processing whose main goal is to design information protocols that do not require any modeling of the devices.
- Quantum non-locality is the resource in the framework.
- DIQIP project aims at understanding and characterizing the possibilities and limitations of the new scenario.
- The main objectives of the project are: (i) the characterization of non-local quantum correlations, (ii) the use of these correlations for information protocols and (iii) the study of the feasibility of these protocols.
- Several significant results along these main goals have already been obtained in these months. More to come!