

Device-Independent Quantum Information Processing (DIQIP)

Maciej Demianowicz

ICFO-Institut de Ciències Fotòniques, Barcelona (Spain)



Coordinator of the project: Antonio Acín (ICFO, ICREA professor)

Some coordinates

- Starting date of the project: September 1, 2011,
- Kick-off meeting in Geneva, November 23-25, 2011,
- First-year meeting in Barcelona, June 13-15, 2012, organized together with the EU STREP Project Quantum Computer Science (QCS),
- Second-year meeting in Paris, May 14-17, 2013, joint meeting with QCS and EU STREP Project Quantum Algorithms (QALGO),
- *Next meeting in Bruxelles, May 13-16, 2014, joint with QALGO.*

Quantum Information Theory

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

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.

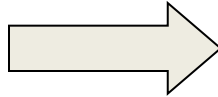


Information Theory:

set of laws describing
how information can
be manipulated.

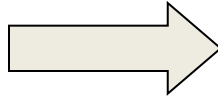
Quantum Information Theory

What happens when we encode information in the quantum world?



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

vs

physical security

Computational security

It is easy to generate the factors and then compute the product.

What about the other direction?

One-way functions: *easy* in one direction, *hard* in the opposite.

Computational security

It is easy to generate the factors and then compute the product.

What about the other direction?

One-way functions: *easy* in one direction, *hard* in the opposite.

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



Computational security

It is easy to generate the factors and then compute the product.

What about the other direction?

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 is easy, the enemy can break the protocol!

Is factorization really a hard problem?!

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

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!**

$30790518401361202507 = 4575351673 \times 6729650659$



P. W. Shor

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!**

$30790518401361202507 = 4575351673 \times 6729650659$



P. W. Shor

A quantum computer allows for the efficient factorization of large numbers.

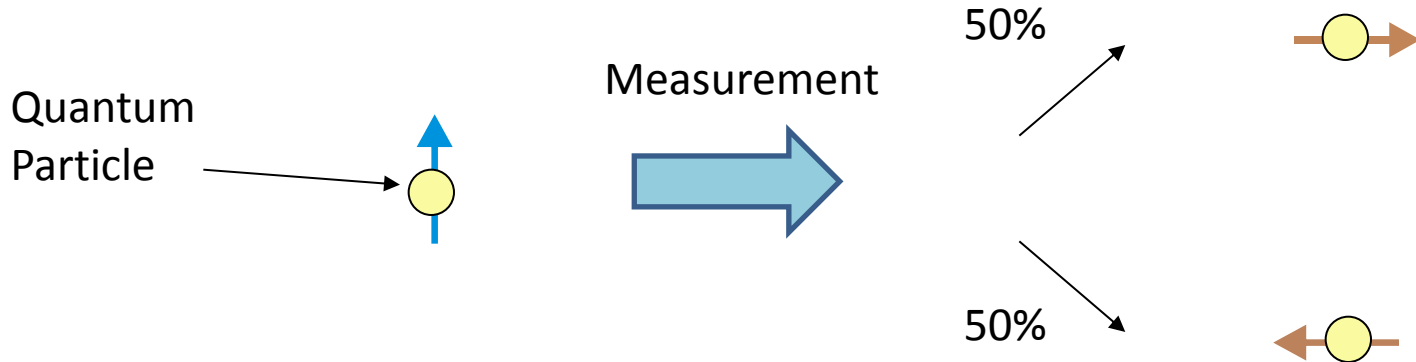
Which problems are easy for a quantum computer?

Heisenberg Uncertainty Principle

Quantum Theory only predicts the *probabilities of outcomes*.

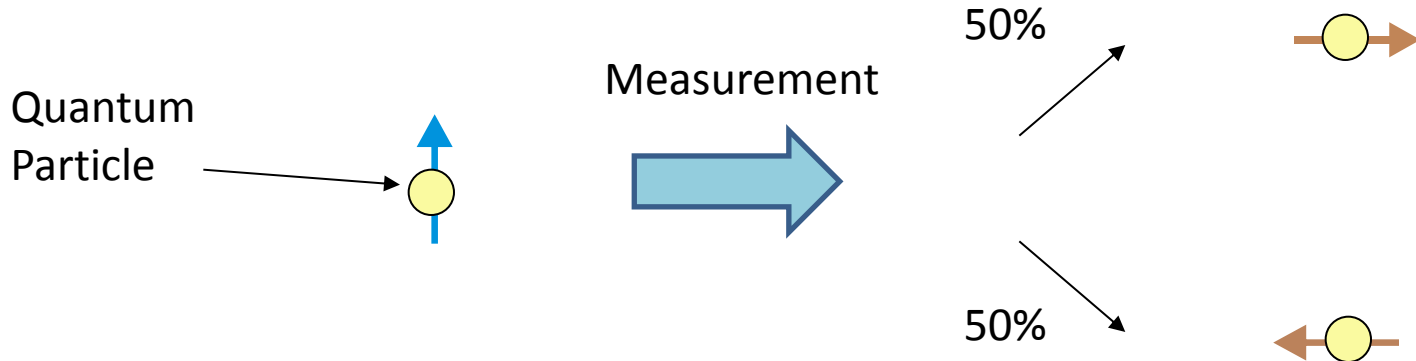
Heisenberg Uncertainty Principle

Quantum Theory only predicts the *probabilities of outcomes*.



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!

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.



C. H. Bennett



G. Brassard



A. Ekert

Standard Cryptography

- Standard Classical Cryptography schemes are based on **computational security**,
- *Assumption 1*: eavesdropper computational power is limited,
- *Assumption 2*: factoring is assumed to be a hard problem,
- Quantum computers shed doubts on the long-term applicability of these schemes, e.g. Shor's algorithm for efficient factorization.

Standard Cryptography



- Standard Classical Cryptography schemes are based on **computational security**,
- *Assumption 1*: eavesdropper computational power is limited,
- *Assumption 2*: factoring is assumed to be a hard problem,
- Quantum computers shed doubts on the long-term applicability of these schemes, e.g. Shor's algorithm for efficient factorization.

Quantum Cryptography: a new form of security

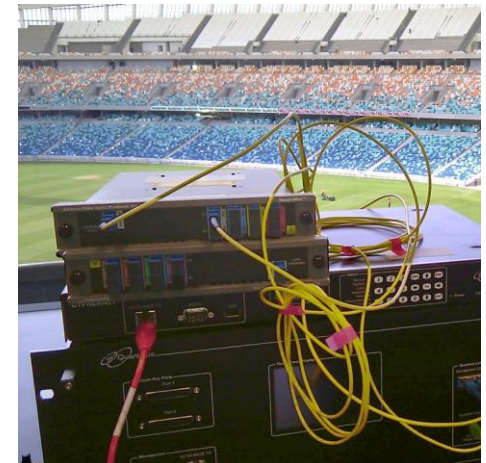
- Quantum Cryptography protocols are based on **physical security**,
- *Assumption*: Quantum Mechanics offers a correct physical description of the devices,
- **No assumption** is required on the eavesdropper's power, provided it does not contradict any quantum law,
- Using this (these) assumption(s), the security of the schemes *can* be proven.

Quantum Cryptography: you can buy it!

- Quantum cryptography is a commercial product.



- 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



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.

Quantum hacking

Quantum hacking attacks break the implementation, ***not*** the principle.



Single-photon source

Quantum hacking

Quantum hacking attacks break the implementation, ***not*** the principle.



Single-photon source



Quantum channel

Quantum hacking

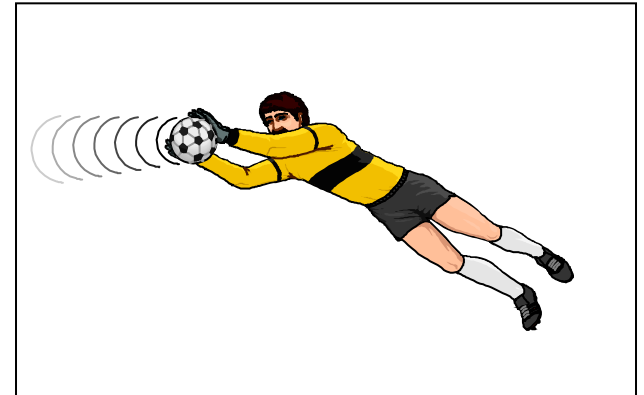
Quantum hacking attacks break the implementation, ***not*** the principle.



Single-photon source



Quantum channel



Single-photon detector

Quantum hacking

Quantum hacking attacks break the implementation, **not** the principle.

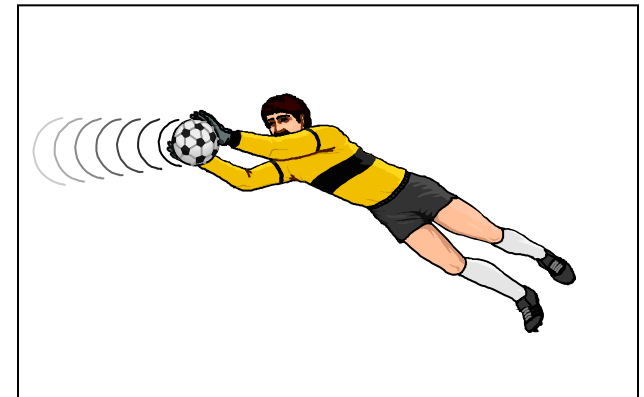


~~Single photon source~~

Attenuated laser source



Quantum channel



~~Single photon detector~~

Realistic APD detector

The problem

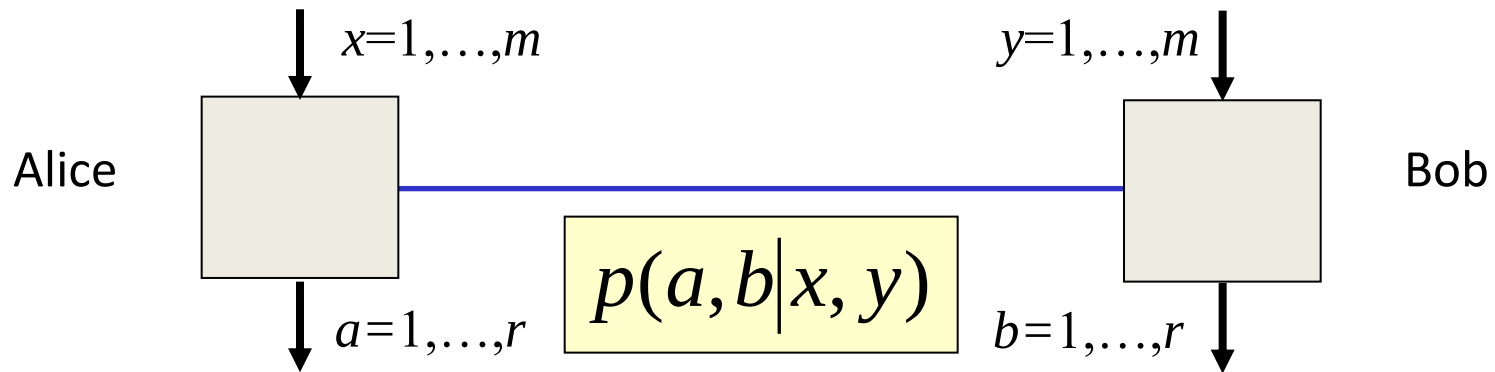
How can one assess the level of security provided by real-life implementations of quantum key distribution, or more generally, quantum information protocols, which will inevitably differ in inconspicuous ways from the idealized, theoretical description?

Device-Independent Quantum Information Processing (DIQIP)

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.

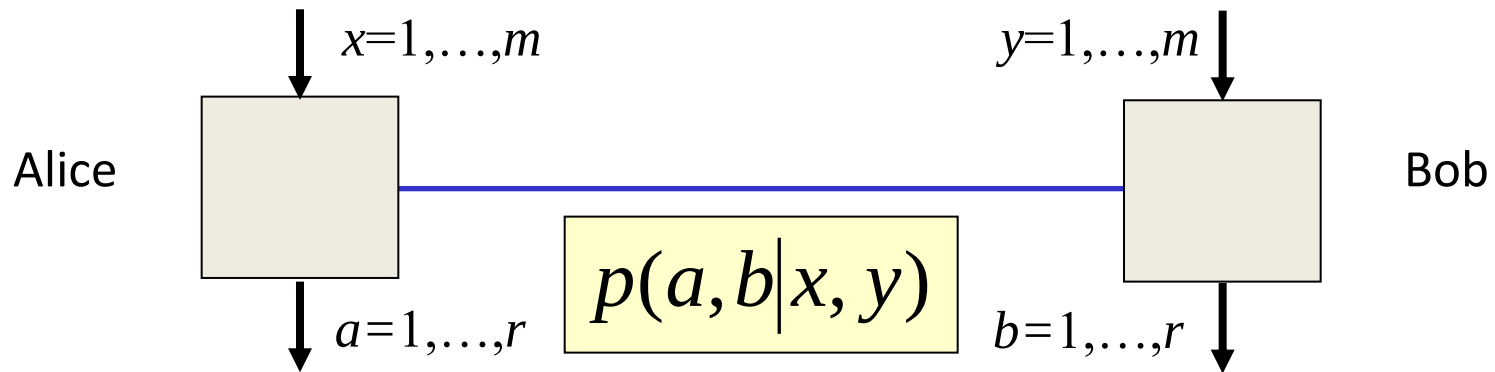
Scenario

Distant parties performing m different measurements of r outcomes.



Scenario

Distant parties performing m different measurements of r outcomes.



Goal: to perform an information task, e.g. to distribute a secret key, only from the observed correlations between devices, $p(a, b|x, y)$.

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

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.

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	Oxford	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.

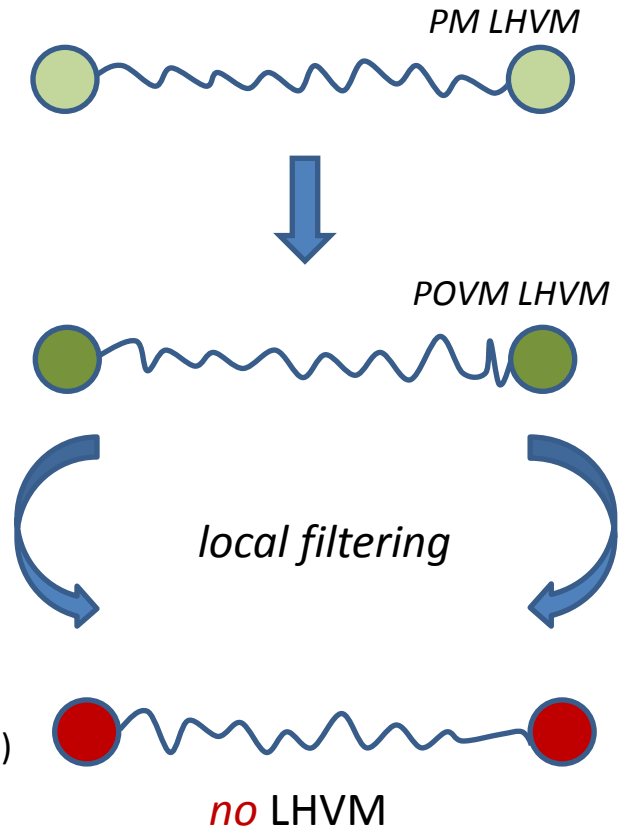
What we did

Characterization of multipartite non-locality

First example of *genuine* hidden nonlocality:

- hidden – filtering (sequence of measurements) is required to reveal nonlocality of a state,
- *genuine* – original state has a model for arbitrary general measurements (called POVMs)

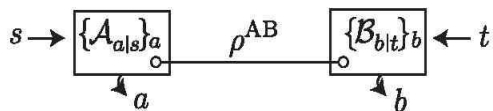
(previous constructions showed this effect for states with models only for a restricted class of measurements, projective measurements – PMs)



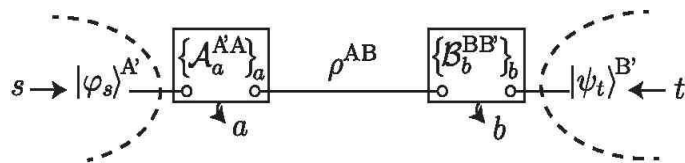
What we did

Complexity aspects of non-local games

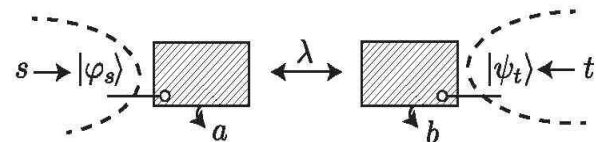
Standard Bell scenario (with classical inputs)



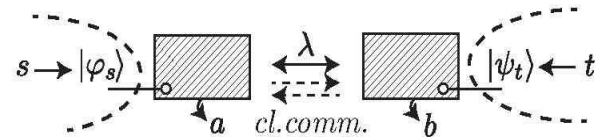
Quantum Input scenario



QI scenario simulation using LOSR



QI scenario simulation using LOCC



No-go result:

In the quantum input (QI) framework it is **impossible** to simulate *any* entangled state using shared randomness (SR) and even *unrestricted* classical communication (CC).

This establishes a *new* feature of entanglement.

What we did

Information principles and quantum correlations

Q: Could we explain correlations within the framework of hidden influences?

Ans: **No**, v – causal models for quantum correlations lead to signalling

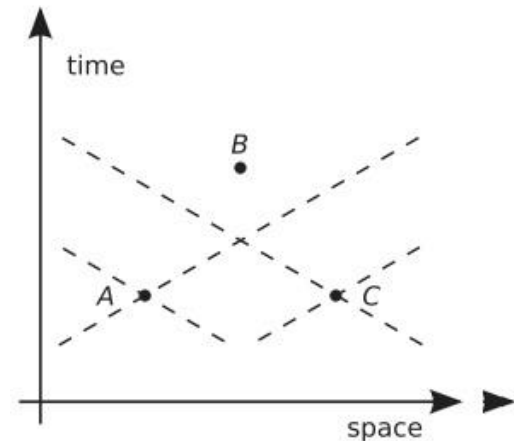
In other words, influences aiming at explaining quantum nonlocality *cannot* remain hidden and *can* be exploited to superluminal signalling.

Previously known results:

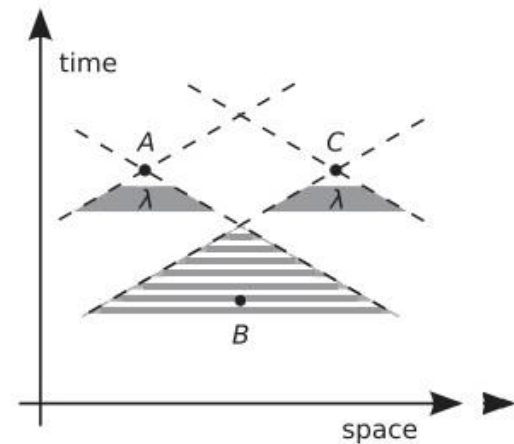
- bipartite – experimental
(lower bounds on the speed),
- tripartite - ??
- four partite - theoretical.

Closing the gap:

First example of a tripartite quantum state violating the hidden-influence constraints.



(a) The unconditioned time ordering



(b) The conditioned time ordering

What we plan to do

Device-independent quantum information processing

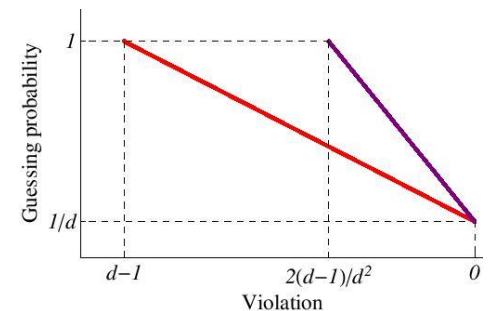
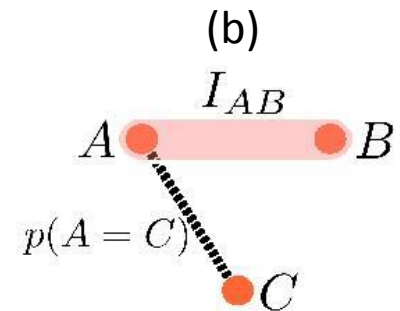
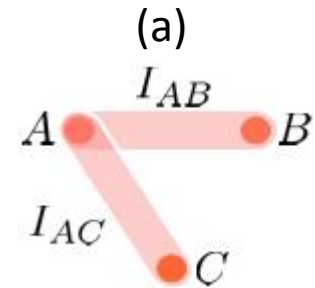
Tasks	
T2.1	Trade-off between non-locality and randomness (ICFO; ULB) Here we want to establish quantitative relations between the amount of randomness and non-locality in quantum systems. How does randomness scale with a Bell violation, or with the number of parties? The use of the SDP hierarchy will 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 did

Trade-off between non-locality and randomness

- physical principles impose bounds on the way correlations can be distributed among parties
-> **monogamies**,
- usual monogamy relations (a) involve a single feature of a state (entanglement, nonlocality),
- novel monogamy relations* (b) tightly relate the amount of nonlocality to the classical correlations an external party can share with outcomes of any measurement performed by the parties,
- they give us bounds on the guessing probability **better** than the ones **previously known**.

Augusiak *et al.*, arXiv: 1307.6390



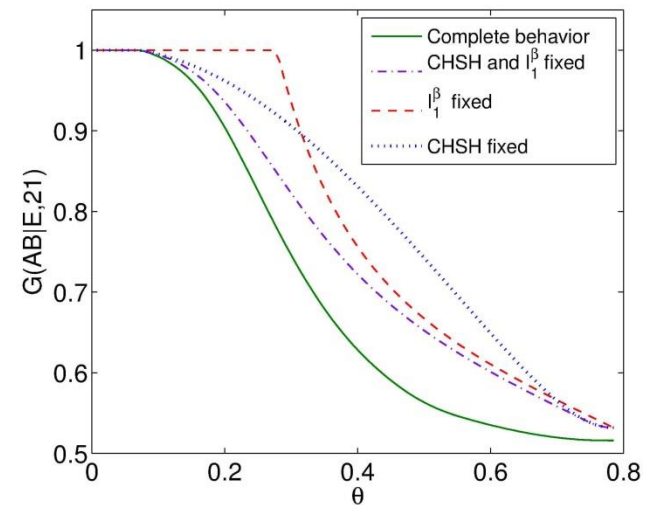
What we did

Improved DIQKD protocol

The set of data obtained in a Bell experiment is much richer than the mere value of the violation of some Bell inequality.

Q: is this additional data useful? **YES!**

- systematically taking into account the complete statistics one can obtain the device independent guessing probability (DIGP),
- for any set of nonlocal correlations there exists an optimal Bell inequality for certifying maximal amount accessible randomness.



What we did

Better security proofs for DIQKD

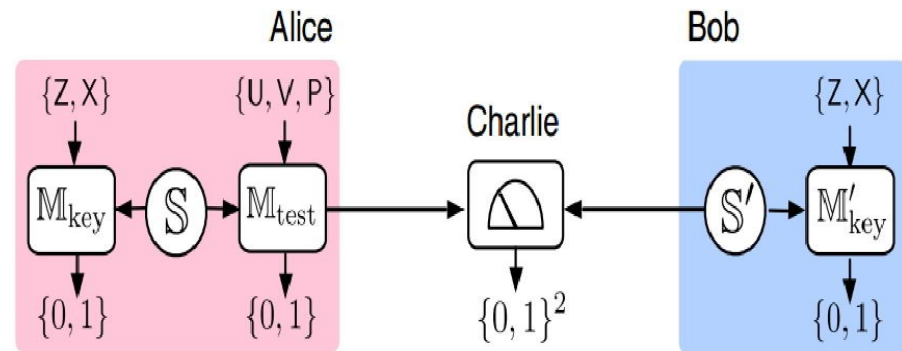
Novel approach to DIQKD:

Bell test is performed *locally* on two causally independent devices in Alice's laboratory



the detection loophole is avoided

Security proof uses a relation between the local CHSH test and a variant of the entropic uncertainty relation for smooth entropies.



What we plan to do

Towards experimental implementations of device-independent protocols

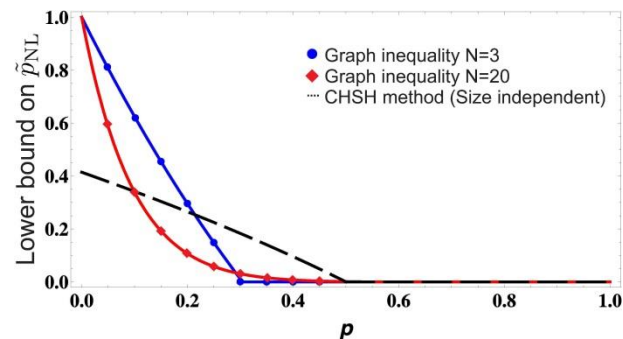
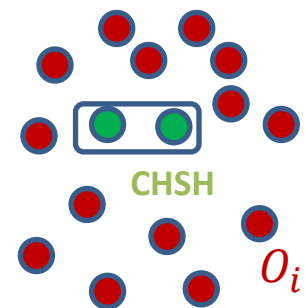
Tasks	
T3.1	Bell tests more robust against noise or detection inefficiencies (UoB; GAP-ETH, ULB, ICFO, LRI) Here we will study the design of Bell tests more robust against imperfections, especially for device-independent applications. We will consider different scenarios by changing the number of measurement 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.

What we did

Bell tests more robust against noise or detection efficiencies

CHSH method for multipartite states subject to local noise:

- efficiently calculable bounds for the tolerable noise threshold or the nonlocal content,
- in many cases significantly tighter estimates than from any other known method, e.g.:
 - N-qubit GHZ states under local dephasing are nonlocal throughout the whole dephasing dynamics,
 - for N-qubit graph states, size independent and exponentially tighter (as N increases) estimate of the nonlocal content.



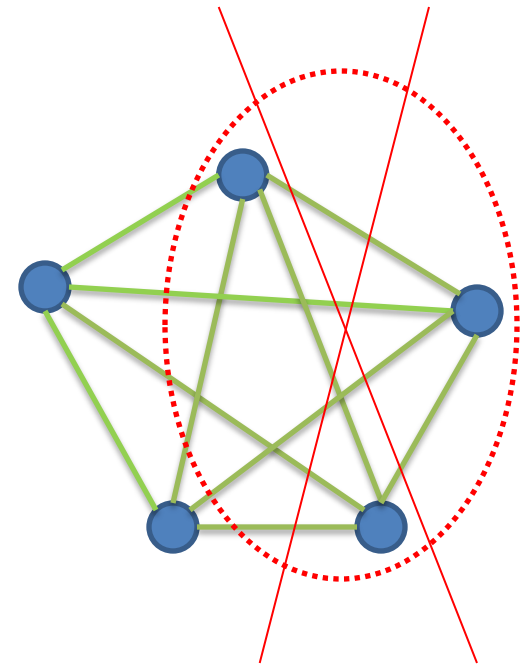
What we did

Detection and simulation of quantumness in many-body systems

High-order correlation functions are *not* easily accessible in experiments...

Q: Can we circumvent this obstacle and use only two body correlators to detect nonlocality in many-body systems? YES!

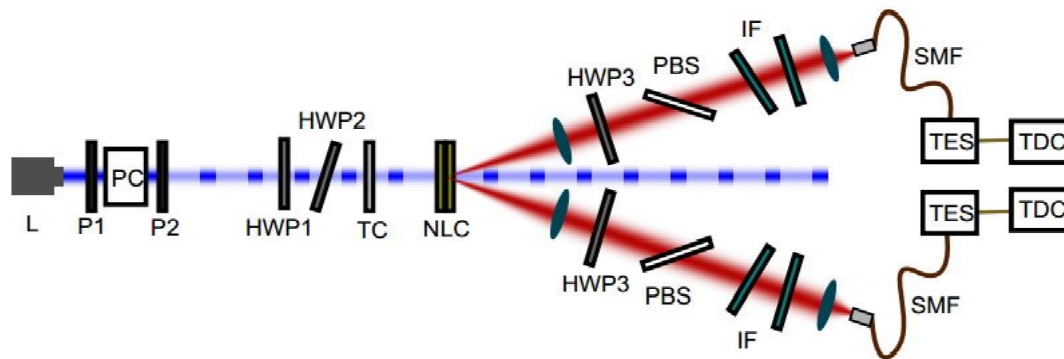
- *explicit* construction of Bell inequalities from **one-** and **two-body** correlation functions for an arbitrary number of parties,
- the obtained inequalities are violated by some of the Dicke states, which arise naturally in many-body physics (as the ground states of the two-body Lipkin-Meshkov-Glick Hamiltonian).



What we did

Feasibility studies for DI protocols

First genuinely detection-loophole-free Bell experiment with photons has been carried out.



The results open promising perspectives for device independent quantum information processing. In particular, for device independent randomness expansion (DIRE):

- previously reported rate of generation of private random bits – 1.5×10^{-5} bits/s,
- with the new method: 0.4 bits/s!

Some numbers...

Second year of the project:

- 45 publications (23 already published and 22 submitted) + 2 conference proceedings : 1 Nature Physics, 3 Nature Communications, and 5 Physical Review Letters,
- 13 articles were multi-partner (of two and sometimes even three partners in the consortium), which shows the strong collaboration among the different partners.

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 modelling 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 during the first two years. More to come!

