

Device-Independent Quantum Information Processing (DIQIP)

Antonio Acín

ICREA Professor at ICFO-Institut de Ciències Fotoniques, Barcelona

Project Start Date: 1 September 2011

Chist-Era meeting, 18 March 2015, Madrid, Spain

Quantum Information Theory

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

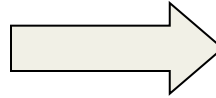
Quantum Mechanics:
set of laws describing
the Physics of the
microscopic world.



Information Theory:
set of laws describing
how information can
be manipulated.

Quantum Information Theory

What happens when we encode information on quantum particles?



Novel information applications become possible thanks to quantum effects, e.g. more powerful computers and secure cryptography.

Change of paradigm: **physics matters!**

Quantum cryptography: unbreakable private information exchange exploiting quantum effects.

Quantum Cryptography: a new form of 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. Alternatively: the assumption for security is that factoring is hard.
- Quantum computers sheds 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.

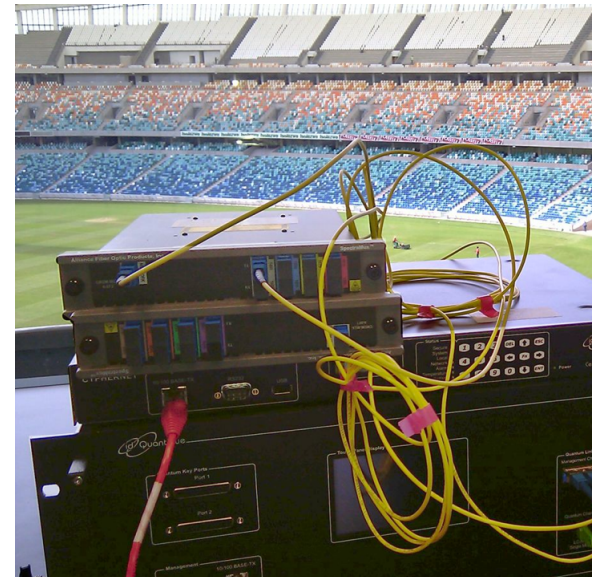
Quantum Cryptography: you can buy it!

- Quantum cryptography is a commercial product.



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.

Theory

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Quantum hacking

Quantum hacking attacks break the implementation, not the principle.

Theory

- Prepare states in a Hilbert space of dimension two.
- Measure observables in the same space, e.g. spin-1/2 measurements.

Implementation

- Prepare states using an attenuated laser source.
- Measure polarization of light using single-photon detectors.

Moral: the unavoidable mismatch between theoretical requirements and implementation is an important weakness in quantum information protocols, especially in adversarial scenarios.



chist-era

Certification and trust

Can You Trust NIST?

Revelations that the NSA undermined the U.S. standards agency leave cryptographers feeling queasy

By Lily Hay Newman

Posted 9 Oct 2013 | 14:00 GMT

Share | Email | Print



Photo-illustration: Randi Silberman Klett

The National Institute of Standards and Technology (NIST) has an image problem. Last month, revelations surfaced indicating that the National Security Agency (NSA) may have planted a vulnerability in a widely used NIST-approved encryption algorithm to facilitate its spying activities. And cryptographers are also questioning subtle changes that might weaken a new security algorithm called Secure Hash

Algorithm-3, or SHA-3. Encryption experts say NIST's reputation has been seriously undermined but that the security community would like to continue using it as a standards body if it can show that it has reformed.



Certification and trust

Can You Trust NIST?

Revelations that the NSA undermined the U.S. standards agency leave cryptographers feeling queasy

By Lily Hay Newman

Posted 9 Oct 2013 | 14:00 GMT

[Share](#) | [Email](#) | [Print](#)



Photo-illustration: Randi Silberman Klett

The National Institute of Standards and Technology (NIST) has an image problem. Last month, revelations surfaced indicating that the National Security Agency (NSA) may have planted a vulnerability in a widely used NIST-approved encryption algorithm to facilitate its spying activities. And cryptographers are also questioning subtle changes that might weaken a new security algorithm called Secure Hash

Algorithm-3, or SHA-3. Encryption experts say NIST's reputation has been seriously undermined but that the security community would like to continue using it as a standards body if it can show that it has reformed.

Stop using NSA-influenced code in our products, RSA tells customers

Firm "strongly recommends" customers stop using RNG reported to contain NSA backdoor.

by Dan Goodin - Sept 20 2013, 1:43am RDT

GOVERNMENT | PRIVACY | 83

Officials from RSA Security are advising customers of the company's BSAFE toolkit and Data Protection Manager to stop using a crucial cryptography component in the products that were recently revealed to contain a backdoor engineered by the National Security Agency (NSA).

An advisory sent to select RSA customers on Thursday confirms that both products by default use something known as Dual EC_DRBG when creating cryptographic keys. The specification, which was approved in 2006 by the National Institute of Standards and Technology (NIST) and later by the International Organization for Standardization, **contains a backdoor that was inserted by the NSA**, *The New York Times* reported last week. RSA's advisory came 24 hours after Ars asked the company if it intended to warn BSAFE customers about the deliberately crippled pseudo random number generator (PRNG), which is so weak that it undermines the security of most or all cryptography systems that use it.

NSA LEAKS

NSA moves from bugging German Chancellor to bugging German ministers

Clapper: We should have disclosed NSA bulk data collection in 2001

New Snowden docs show NSA, GCHQ spied on WikiLeaks, Pirate Bay users

NSA let Snowden crawl all over its intranet unchecked

Report: NSA bulk metadata program doesn't cover cellphones

[View all...](#)



chist-era

Certification and trust

Can You Trust NIST?

Revelations that the NSA undermined the U.S. standards agency leave cryptographers feeling queasy

By Lily Hay Newman

Posted 9 Oct 2013 | 14:00 GMT

[Share](#) | [Email](#) | [Print](#)



Photo-illustration: Randi Silberman Klett

The National Institute of Standards and Technology (NIST) has an image problem. Last month, revelations surfaced indicating that the National Security Agency (NSA) may have planted a vulnerability in a widely used NIST-approved encryption algorithm to facilitate its spying activities. And cryptographers are also questioning subtle changes that might weaken a new security algorithm called Secure Hash

Algorithm-3, or SHA-3. Encryption experts say NIST's reputation has been seriously undermined but that the security community would like to continue using it as a standards body if it can show that it has reformed.

Stop using NSA-influenced code in our products, RSA tells customers

Firm "strongly recommends" customers stop using RNG reported to contain NSA backdoor.

by Dan Goodin - Sept 20 2013, 1:43am RDT

GOVERNMENT PRIVACY 83

Officials from RSA Security are advising customers of the company's BSAFE toolkit and Data Protection Manager to stop using a crucial cryptography component in the products that were recently revealed to contain a backdoor engineered by the National Security Agency (NSA).

An advisory sent to select RSA customers on Thursday confirms that both products by default use something known as Dual EC_DRBG when creating cryptographic keys. The specification, which was approved in 2006 by the National Institute of Standards and Technology (NIST) and later by the International Organization for Standardization, **contains a backdoor that was inserted by the NSA**, *The New York Times* reported last week. RSA's advisory came 24 hours after Ars asked the company if it intended to warn BSAFE customers about the deliberately crippled pseudo random number generator (PRNG), which is so weak that it undermines the security of most or all cryptography systems that use it.

NSA LEAKS

NSA moves from bugging German Chancellor to bugging German ministers

Clapper: We should have disclosed NSA bulk data collection in 2001

New Snowden docs show NSA, GCHQ spied on WikiLeaks, Pirate Bay users

NSA let Snowden crawl all over its intranet unchecked

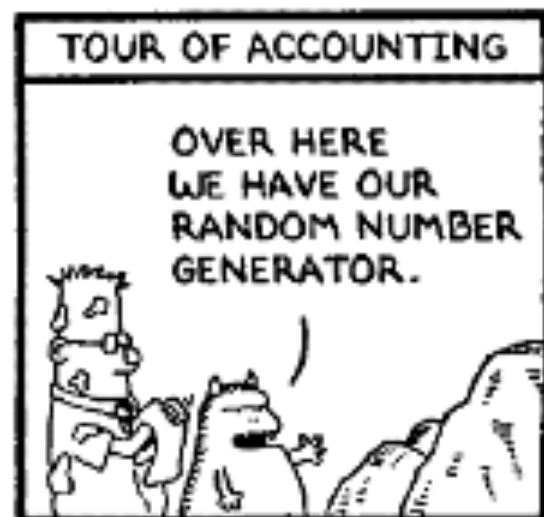
Report: NSA bulk metadata program doesn't cover cellphones

[View all...](#)

Is trust always needed? Can trust be certified?



chist-era



© 2001 United Feature Syndicate, Inc.





chist-era



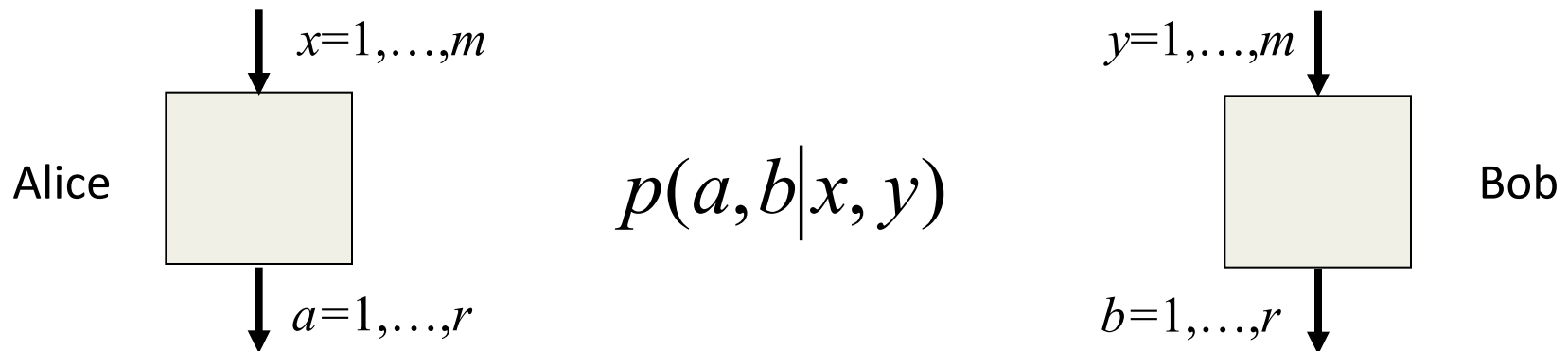
Can the presence of randomness be guaranteed by any physical mechanism?

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?

A solution to the hacking problem

Device-Independent Quantum Key Distribution



Protocols that establish a secure key only from the observed correlations and without making any assumption about the internal working of the devices used to obtain these correlations.

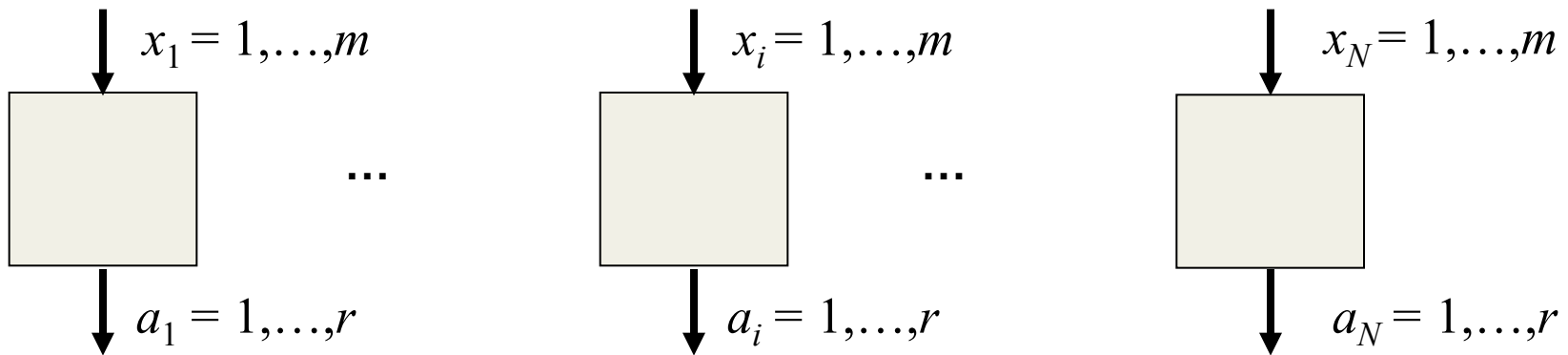
A. Acín *et al.*, Phys. Rev. Lett. 98, 230501 (2007)

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.

DI quantum information processing

Develop a new form of **quantum information theory** in a scenario where the users' devices are just seen as (quantum) **black boxes** processing classical information. The resulting protocols have **self-certification**.



Observed correlations

$$p(a_1, \dots, a_N | x_1, \dots, x_N)$$

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

Principal Investigator	Organisation	Country	Expertise
Antonio Acin (Coordinator)	ICFO-The Institute of Photonic Sciences	Spain	Physics, quantum communication, quantum non-locality
Maciej Lewenstein	ICFO-The Institute of Photonic Sciences	Spain	Physics, entanglement theory, many-body physics
Nicolas Gisin	GAP-Optique, University of Geneva	Switzerland	Physics, quantum communication, implementations of qit
Renato Renner	ETH Zurich	Switzerland	Physics, quantum cryptography, quantum information theory
Stefan Wolf	USI Lugano	Switzerland	Computer science, quantum and classical cryptography
Sophie Laplante	LIAFA, Paris 7	France	Computer science, quantum communication complexity
Serge Massar	Université Libre de Bruxelles	Belgium	Physics, quantum non-locality, implementations of qit
Sandu Popescu	University of Bristol	United Kingdom	Physics, foundations of quantum physics, quantum non-locality
Jonathan Barrett	University of Oxford	United Kingdom	Physics, foundations of quantum physics, quantum communication

What we planned 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

Quantum nonlocality does not imply entanglement distillability

- In 1999, Peres conjectured that nonlocal correlations could only be observed on quantum states with distillable entanglement. If true, the conjecture would mean that bound entangled states would be useless for any quantum information protocols that require nonlocality.
- The conjecture was a long-standing open question in the field.
- One of the highlights of DIQIP is to prove that Peres conjecture is false. Vertesi and Brunner identified a bound entangled state that violates a Bell inequality.

UNIGE: T. Vertesi, N. Brunner, *Disproving the Peres conjecture by showing Bell nonlocality from bound entanglement*, Nature Communications 5, 5297 (2014)

What we did

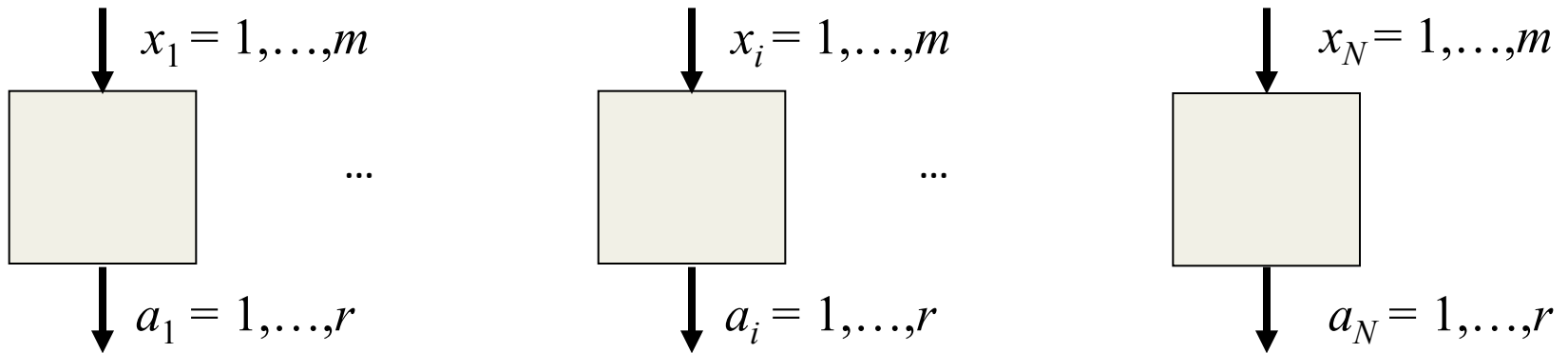
Complexity aspects of non-local games

- Nonlocality enables two parties to win specific games with probabilities strictly higher than allowed by any classical theory. Nevertheless, all known such examples consider games where the two parties have a common interest, since they jointly win or lose the game.
- Can quantum non-locality offer an advantage in a scenario where the two parties have conflicting interests?
- The question was answered in the affirmative by presenting a simple conflicting interest game, where quantum strategies outperform classical ones. The game has a fair quantum equilibrium with higher payoffs for both players than in any fair classical equilibrium.
- Finally, the quantum advantage was experimentally demonstrated using a commercial entangled photon source.

LRI: A. Pappa *et al.*, *Nonlocality and Conflicting Interest Games*, Phys. Rev. Lett. 114, 020401 (2015)

What we did

Information principles and quantum correlations



$$p(a_1, \dots, a_N | x_1, \dots, x_N)$$

Local orthogonality: first example of an intrinsically multipartite principle for correlations. It detects supra-quantum correlations for which any bipartite principle fails.

ICFO+ETH: T. Fritz *et al.*, *Local Orthogonality as a multipartite principle for correlations*, Nature Communications 4, 2263 (2013)

What we planned to do

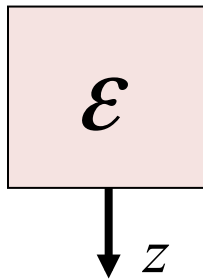
Device-independent quantum information processing

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

Randomness amplification: task that aims at producing arbitrarily pure random bits from a source of imperfect random bits.



$$\frac{1}{2} - \varepsilon \leq \Pr(z = 0 | \text{rest}) \leq \frac{1}{2} + \varepsilon$$

Goal: to distill a source of smaller ε from many uses of the initial source. Full randomness amplification means that ε can be made arbitrarily small.

Classically: impossible.

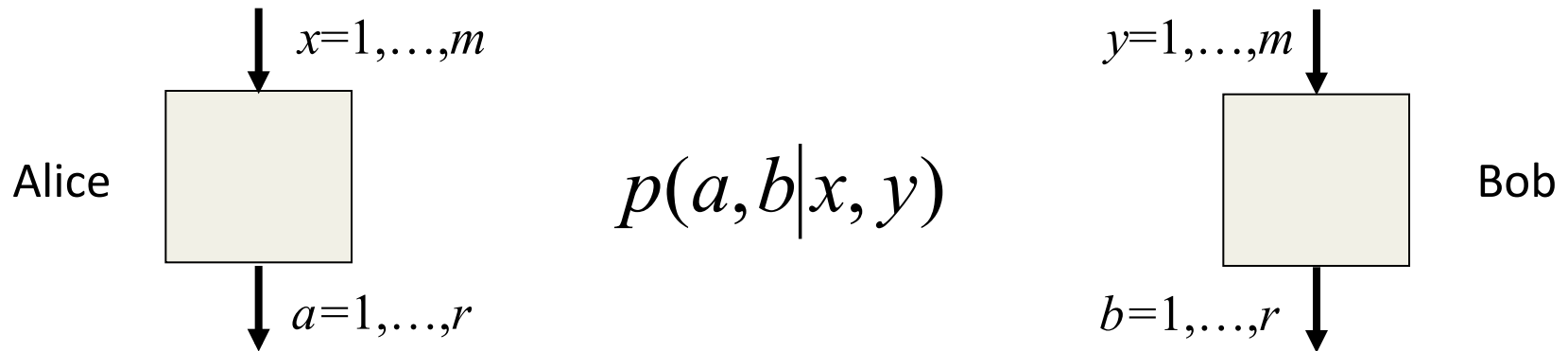
Quantumly: possible [1]. In fact, arbitrarily small amounts of randomness can be fully amplified [2].

ETH: R. Colbeck and R. Renner, *Free randomness can be amplified*, Nature Physics 8, 450 (2012)

ICFO: R. Gallego *et al.*, *Full randomness from arbitrarily deterministic events*, Nature Communications 4, 2654 (2013)

What we did

Improved DIQKD protocol



What's the optimal way of estimating randomness from the observed correlations?

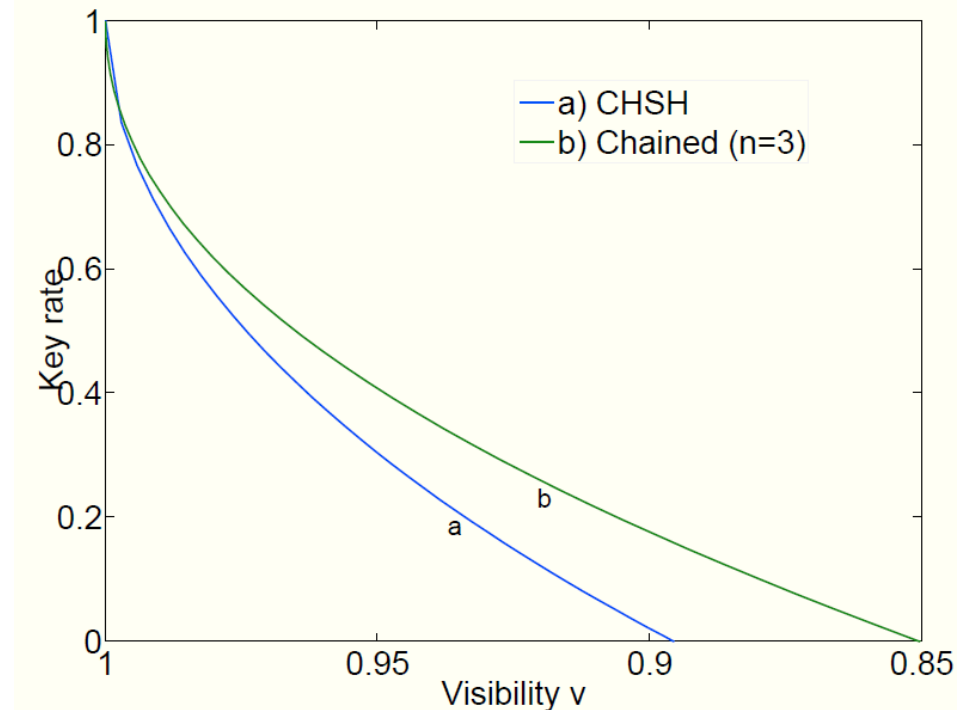
Tools for optimal randomness estimation → better key rates from the same correlations.

ULB: O. Nieto-Silleras, S. Pironio, J. Silman, *Using complete measurement statistics for optimal device-independent randomness evaluation*, New J. Phys. 16, 013035 (2014)

What we did

Better security proofs for DIQKD

- New proof valid for any Bell inequality and that, contrary to previous approaches, requires only two devices.
- It assumes that Eve has no long-term quantum memory.
- The obtained key rates are comparable to standard QKD.



ULB+ICFO+ETH: S. Pironio, L. Masanes, A. Leverrier, A. Acin, *Security of device-independent quantum key distribution in the bounded-quantum-storage model*, Phys. Rev. X 3, 031007 (2013)

What we planned 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

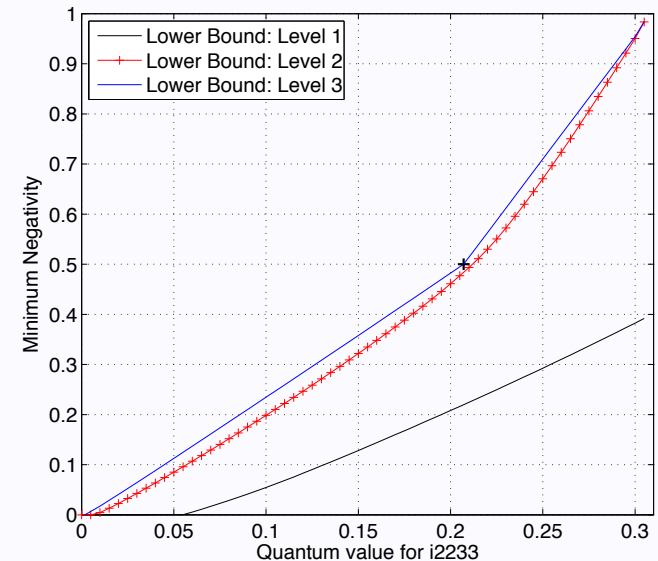
We more robust entanglement quantifiers based on Bell tests.

Device-independent entanglement quantification etc.

- Lower bounding negativity directly from Bell inequality violation, e.g.

$$N(\rho_{AB}|S_{CHSH} = v) = \frac{v - 2}{4(\sqrt{2} - 1)}$$

- (Genuine) Negativity bound also gives lower bound on Hilbert space dimension and structure on multipartite entanglement.
- A converging hierarchy of semidefinite programs can be used to compute quantum bounds obtainable from PPT states.



UNIGE: T. Moroder et al., *Device-independent entanglement quantification and related applications*, Phys. Rev. Lett. 111, 030501 (2013)

What we did

Detection and simulation of quantumness in many-body systems



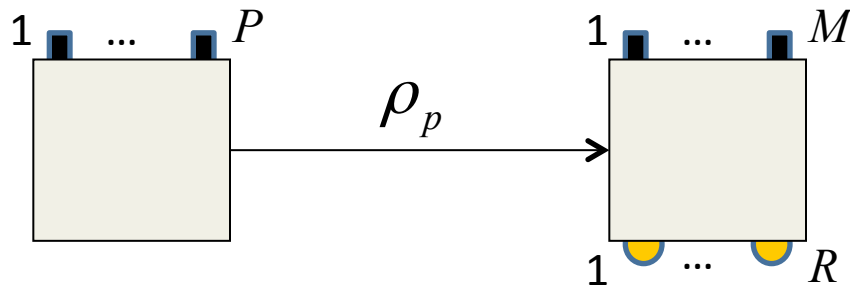
- Do many-body quantum states exhibit non-local correlations? Yes, they do, when all possible measurements are considered.
- Standard and feasible measurements in a many-body context measure correlations only between a few (say two) particles. Do quantum states exhibit non-locality for these measurements and any number of particles? YES!
- The Bell inequality violations can be estimated by standard global-spin observables
- Tools for the experimental detection of non-locality of big quantum systems.

ICFO: J. Tura et al., *Detecting non-locality of many-body quantum states*, Science 344, 1256 (2014)

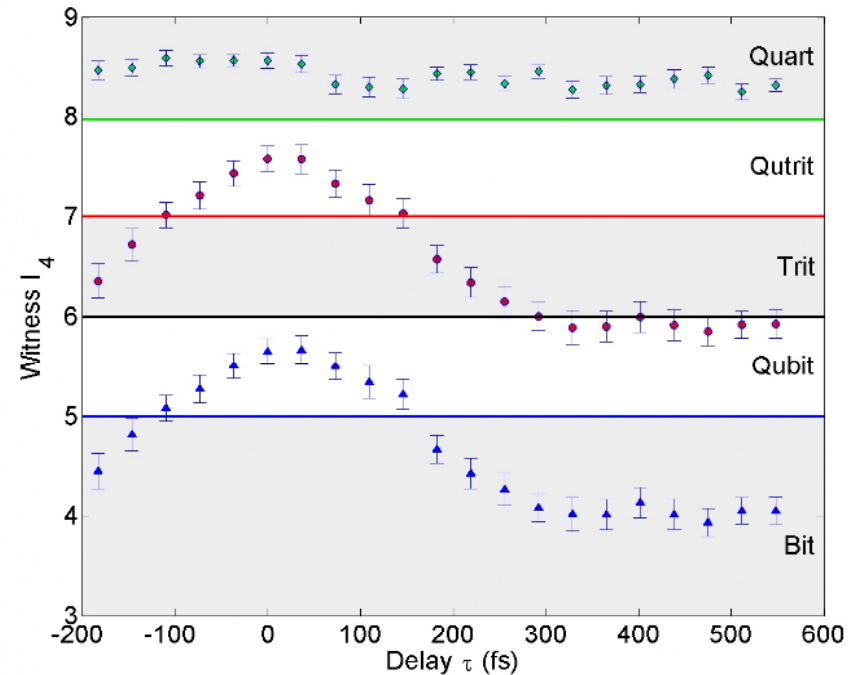
What we did

Feasibility studies for DI protocols

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



$$P(r|m, p) = \text{tr}(\rho_p M_r^m)$$



ICFO+UoB: M. Hendrych *et al.*, *Experimental estimation of the dimension of classical and quantum systems*, Nature Physics 8, 588 (2012)

Project meetings

- Starting date of the project: September 1st 2011
- Kick-off meeting in Geneva, 23-25 November 2011
- First-year meeting in Barcelona, 13-15 June 2012. It was organized together with the EU STREP Project Quantum Computer Science (QCS).
- Second-year meeting in Paris, 14-17 May 2013. It was again organized together with the EU STREP Project Quantum Computer Science (QCS).
- Third-year meeting in Brussels, 13-16 June 2014. It was organized together with the EU STREP Project Quantum Algorithms (QALGO).
- **Cut: no coordination money.** No conference, as initially planned.

Some numbers

- 89 publications, 6 conference proceedings and 17 articles submitted for publication.
- 1 article in Science, 4 in Nature Physics, 6 in Nature Communications, 2 in Physical Review X and 25 Physical Review Letters.
- Although being a theoretical project, we collaborated in 7 experimental works.
- 29 publications involve collaborations withing DIQIP, usually of 2 nodes, but sometimes even 3.

What follows?

- ERC Consolidator Grant: “Quantum Information Theory with Black Boxes” (QITBOX). Starting date: 1 January 2014. PI: Antonio Acín.
- Templeton Project: Intrinsic Randomness in the Quantum World. PI: Antonio Acín (+ Maciej Lewenstein).
- SNSF Starting Grant: “Device-Independent Approach to Quantum Theory” (DIAQ). Starting Date: 1 September 2015. PI: Nicolas Brunner.
- We submitted a joint proposal with some of the partners in DIQIP + 3 experimental groups to the recent FET-Open call. Rejected, we will resubmit it by the end of the month.

Conclusions

- Device-independent quantum information processing is a new paradigm for quantum information processing whose main goal is to design quantum information protocols that do not require any modelling of the devices.
- The DIQIP project represented the first joint effort to understand the possibilities and limitations of this new scenario.
- The main success was to consolidate this novel paradigm at a European scale: strengthen and create collaborations, results in high-impact journals, talks in international conferences, first collaborations with experimentalists.
- Continuations of this effort is essential, the scenario is still in its infancy. Individual efforts have been secured (ERC-type grants), we are looking for joint projects.

Funding

N°	Partner	Person.months	Total costs	Percentage of requested budget
1	ICFO	41	137,540.41 €	≥ 100%
2	GAP-ETH-USI	28	114076.04 CHF	41.82%
3	LIAFA	3.5	110000 €	60%
4	ULB	12	33000 €	82%
5	UoB	2	14456 £	17%
6	Oxford	18	51709.50 £	98%

Funding

- 1) The total expenses of ICFO for the period September 2011 – December 2013 consists mainly of the salary contribution to two post-docs, Mathew Hobban and Maciej Demianowicz (€ 111,486.49). The other major expense charged in this project has been the traveling cost (€25,003.76), and the lowest expenditure has been realized in consumables (€1,050.16).
- 2) The total expenses of GAP for the period September 2011 – August 2014 consist mainly of the salary contribution for the PhD student, Mr. Gilles Pütz (CHF 106'766) and other miscellaneous expenses (CHF 5'289) such as traveling cost incurred in attending the DIQIP-QCS meeting at Paris and Brussels. Gilles Pütz is a common PhD student between Geneva and Zurich. He spent 20% of his time in Zurich, but his salary was fully paid via Geneva.
- 3) LIAFA has extended the contract to end in September 2015 due to delays in hiring a suitable postdoctoral researcher. A postdoc has started in August 2014 with a contract ending in July 2015.
- 4) The total expenses of ULB for the period September 2013 – August 2014 consists mainly of the salary contribution to one post-doc Damian Pitaula Garcia, who started working in January 2014. This is the expense reflected in the table. Moreover, researchers paid by other sources (permanent staff, postdocs, PhD students) have contributed to the project.
- 5) The total expenses of UoB for the period September 2012 – August 2014 consist mainly of the salary contribution for the post-doctoral researcher Ana Belen Sainz (£ 6547) and other miscellaneous expenses (£ 7909) such as traveling costs and consumables.
- 6) Expenses incurred by Oxford are to cover 60% salary of an 18 month postdoc (Dr Clare Horsman), who began in mid-Feb 2013, along with small amounts for consumables (£1095.60) and travel (£1789.75).