New perspectives on Quantum Information Theory

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona

Taller de Altas Energías, Barcelona, September 2010

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.

(Einstein, Planck, Bohr, Schrödinger, Heisenberg,…, first half of the XX century).

↔

Information Theory: mathematical formalism describing how information can be stored, processed and transmitted.

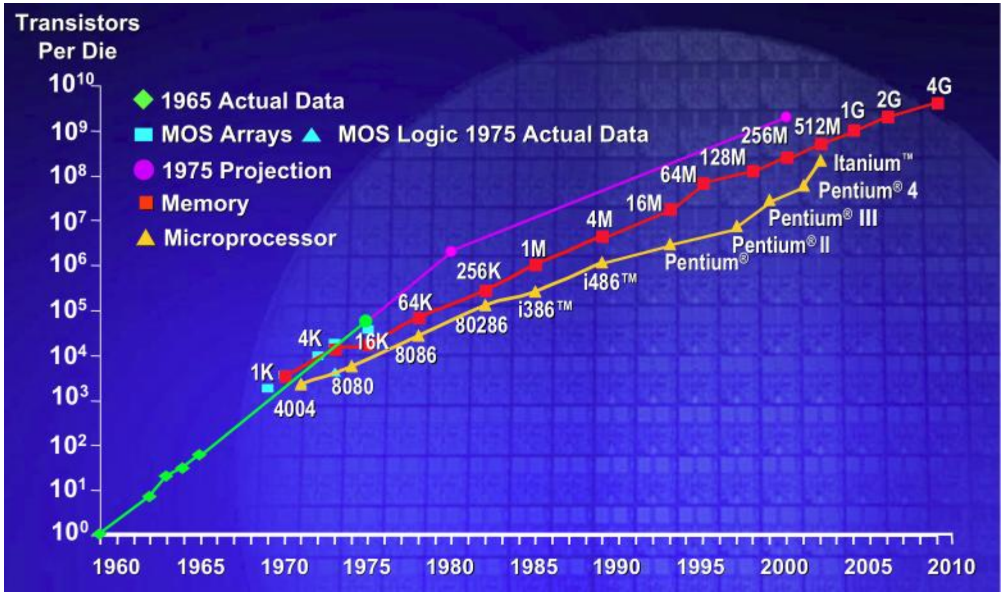
(Shannon, 1950).

Why now?

Quantum Information Theory

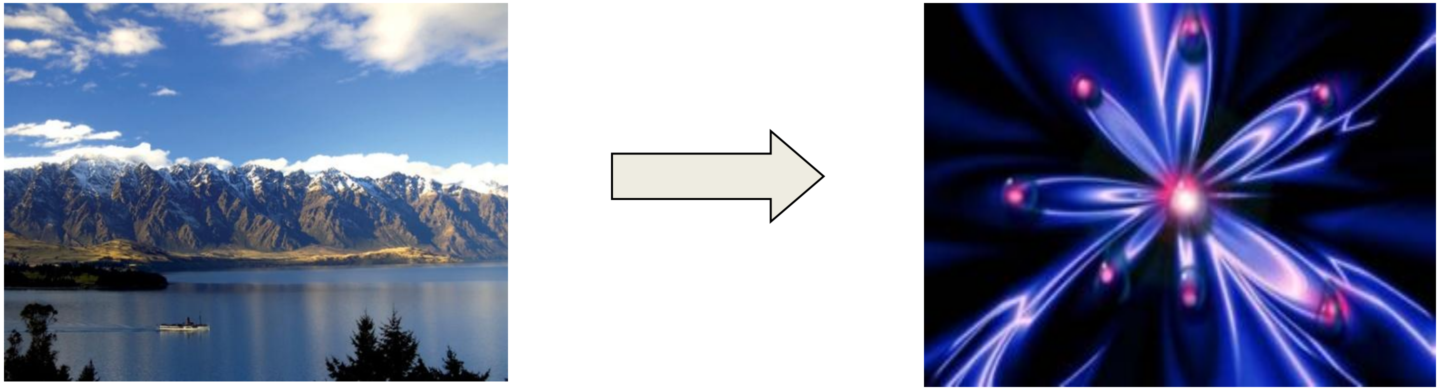
Current technological progress on devices miniaturization leads to a scenario where information is encoded on quantum particles, such as atoms or photons.

- Moore’s Law: information-device size decreases exponentially with time.
- Information is encoded in fewer and fewer atoms.
- It is very plausible that quantum effects will manifest in the near future.



Quantum Information Theory

What happens when we encode information in the quantum world?



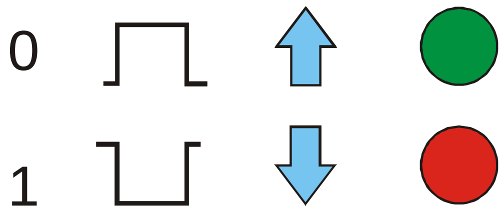
Novel information applications become possible when using information encoded on quantum states, e.g. more powerful computers and secure communication.

The Quantum Bit

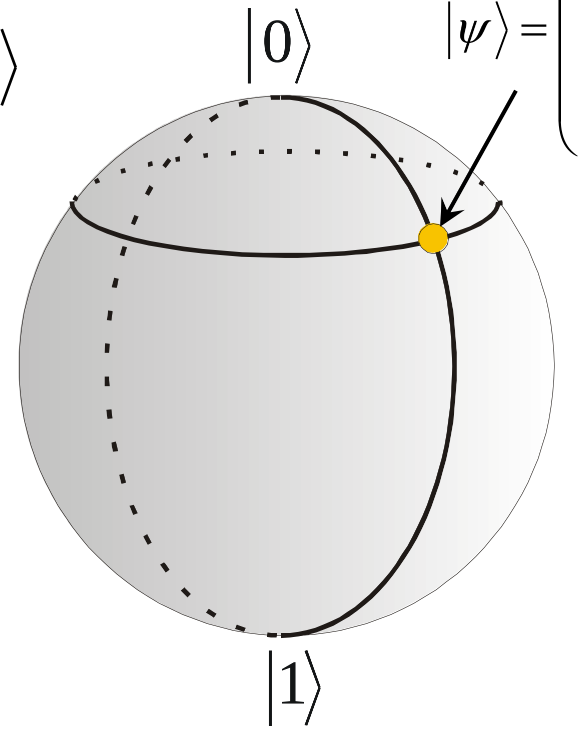
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

The classical bit

The classical bit can take two values, the so-called logical 0 and 1. Examples of realizations of a bit are:



All these realizations encode the same amount of information: one bit.

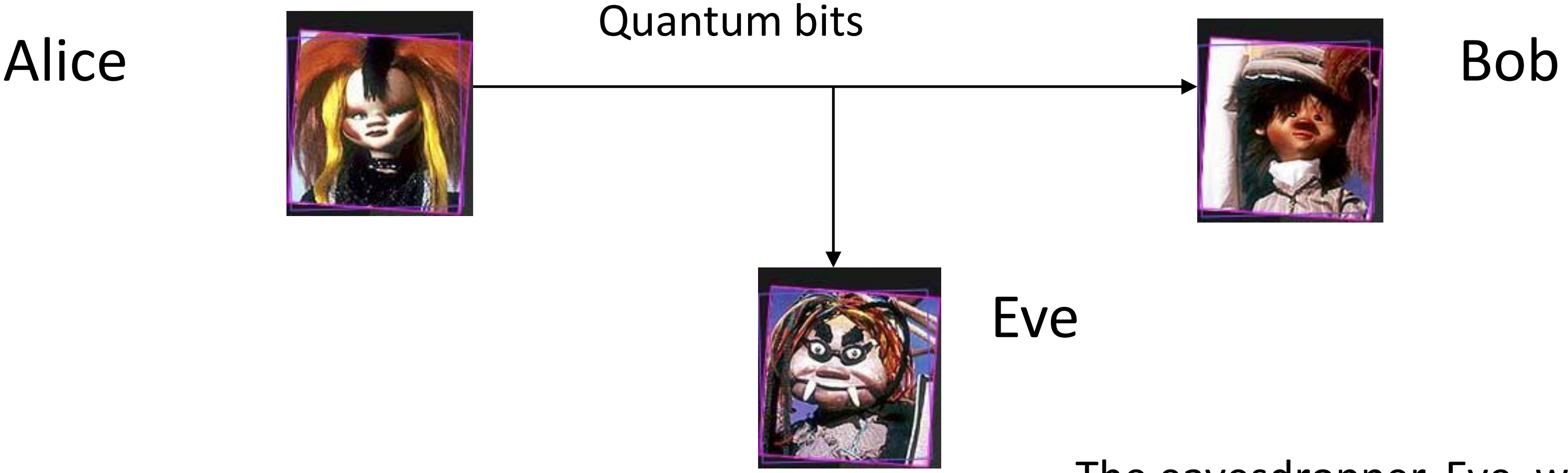


$$|\psi\rangle = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)e^{i\varphi} \end{pmatrix}$$

The quantum bit or qubit can be represented by a point on the so-called Bloch sphere. The poles are associated to the states $|0\rangle$ and $|1\rangle$. Any superposition of these two states generates a unique point on this sphere. Therefore, any quantum bit can be specified by means of two angles, that is, two real numbers.

Quantum Cryptography

Heisenberg uncertainty principle → Secure cryptography!



Alice

Quantum bits

Bob

Eve

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

Bennett

Brassard

Ekert

Classical Cryptography

- 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 Cryptography

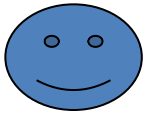
- Quantum Cryptography protocols are based on physical security.
- Assumption: Quantum Mechanics offers a correct physical description of the devices.
- No assumption is required on the eavesdropper’s power, provided it does not contradict any quantum law.
- Using this (these) assumption(s), the security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

Quantum Information Theory

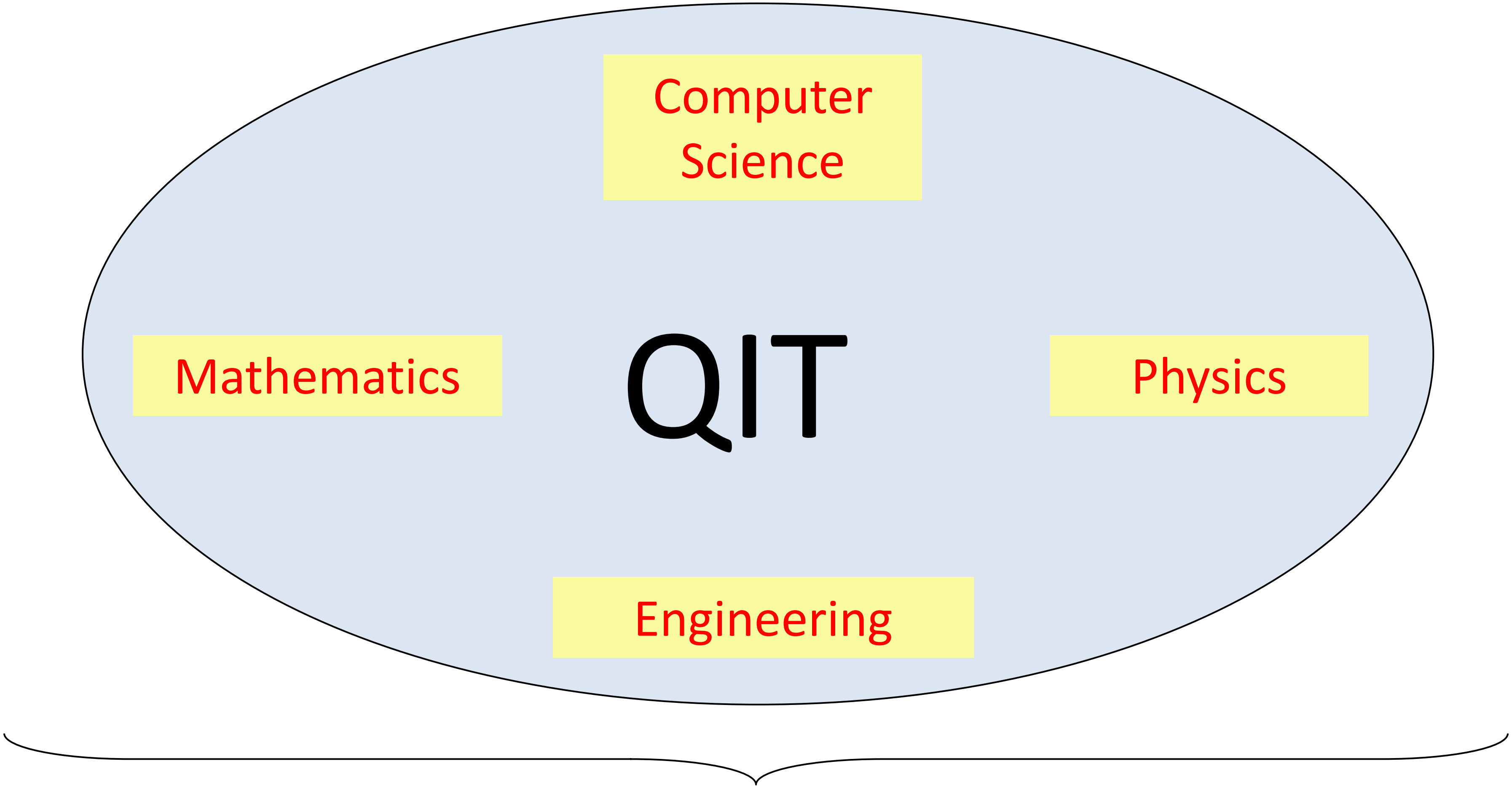
1. Quantum Mechanics goes often against our classical intuition.
2. Standard probability theory does not apply.
3. Quantum paradoxes are useful: the more quantum, the better!!

Quantum Cryptography is one of the best examples of this change of paradigm.

- Heisenberg principle: the state of a system cannot be measure without perturbing it.
- Let's use this property to guarantee the security of information transmission → any eavesdropper attempting to read the information will be limited by the Heisenberg principle!



Quantum Information Theory



Computer Science

Mathematics

QIT

Physics

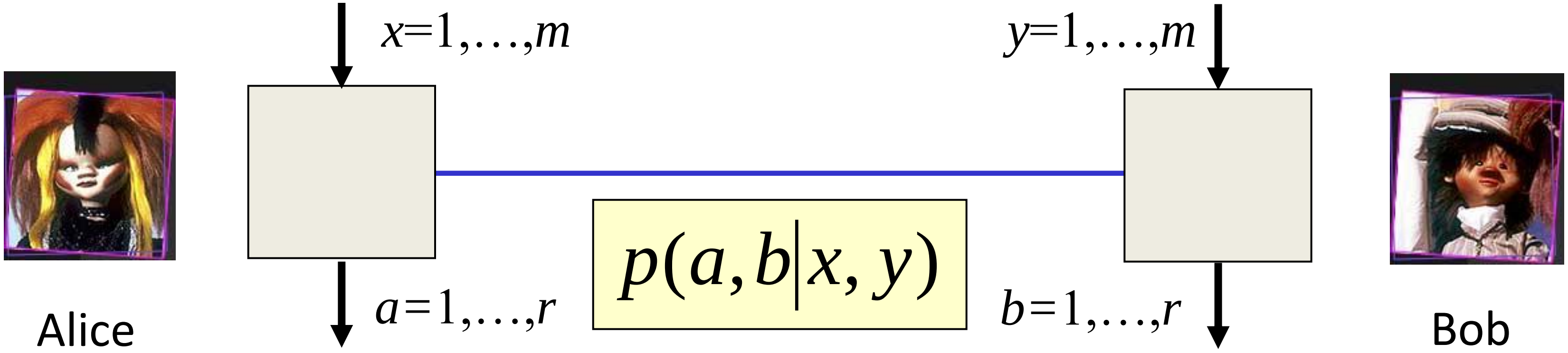
Engineering

Very inter-disciplinary line of research

Quantum Correlations and Device-Independent Quantum Information Processing

Scenario

Distant parties performing *m* different measurements of *r* outcomes.



x=1,…,m

y=1,…,m

$p(a,b|x,y)$

a=1,…,r

b=1,…,r

Alice

Bob

Vector of $m^2\, r^2$ positive components satisfying m^2 normalization conditions

$$p(a,b|x,y|) = \underbrace{\left(p(1,1|1,1), p(1,2|1,1), \ldots, p(r,r|1,1)\right.}_{\sum_{a,b=1}^{r} p(a,b|x,y) = 1 \quad \forall x,y}\left., \ldots, p(r,r|m,m)\right)$$

Physical Correlations

Physical principles translate into limits on correlations.

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

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

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.

For a finite number of measurements and results, these correlations define a polytope, a convex set with a finite number of extreme points.

Physical Correlations

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

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

$$\sum_a M_a^x = 1$$

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

The set of quantum correlations is again convex, but not a polytope, even if the number of measurements and results is finite.

Physical Correlations

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

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

The set of no-signalling correlations defines again a polytope.

Bell

$$\boxed{C \subset Q \subset NS}$$

Popescu-Rohrlich

Characterization of Quantum Correlations

Motivation

Is $p(a,b|x,y)$ a quantum probability?

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

$$\sum_a M_a^x = 1$$

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

Example:

$$p(a,b|0,0) = p(a,b|0,1) = p(a,b|1,0) = \frac{1}{8}\left(2+\sqrt{3}, 2-\sqrt{3}, 2-\sqrt{3}, 2+\sqrt{3}\right)$$

$$p(a,b|1,1) = (0.245, 0.255, 0.255, 0.245)$$

Are these correlations quantum?

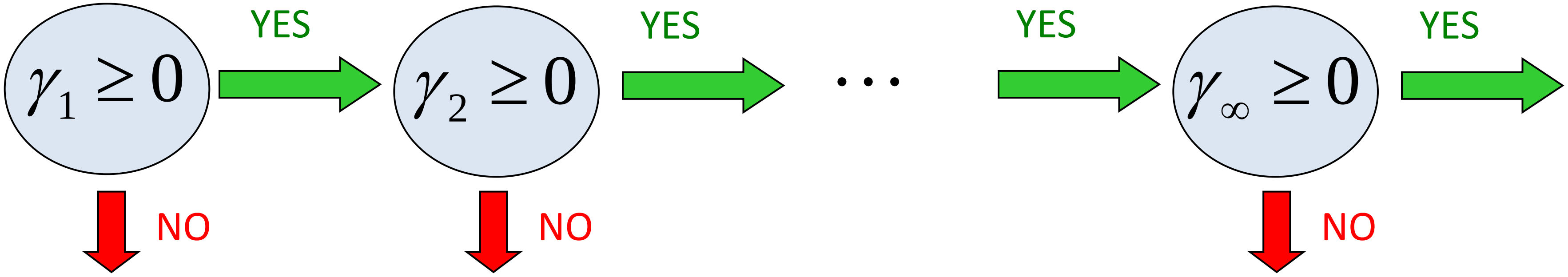
Motivation

- What are the allowed correlations within our current description of Nature?
- How can we detect the non-quantumness of some observed correlations? Quantum analogues of Bell inequalities.
- What are the limits on correlations associated to the quantum formalism?
- To which extent Quantum Mechanics is useful for information tasks?

Previous work by Tsirelson

Hierarchy of necessary conditions

Given a probability distribution $p(a,b|x,y)$, we have defined a hierarchy consisting of a series of tests based on semi-definite programming techniques allowing the detection of supra-quantum correlations.



The hierarchy is asymptotically convergent.

Device-Independent Quantum Key Distribution

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.~~

Is there a protocol for secure QKD based on $p(a,b|x,y)$ without requiring any assumption on the devices?

Motivation

- The fewer the assumptions for a crytpographic protocol → the stronger the security.
- Device-Independent QKD represents the strongest form of quantum cryptography. It is based on the minimal number of assumptions.
- It may be useful when considering practical implementations. If some correlations are observed → secure key distribution. No security loopholes related to technological issues.

Bell inequality violation

Bell inequality violation is a necessary condition for security

If the correlations are local: $p(a,b|x,y) = \sum_{\lambda} p(\lambda) p(a|x,\lambda) q(b|y,\lambda)$

A perfect copy of the local instructions can go to Eve.

BHK, PRL 95; Ekert 91

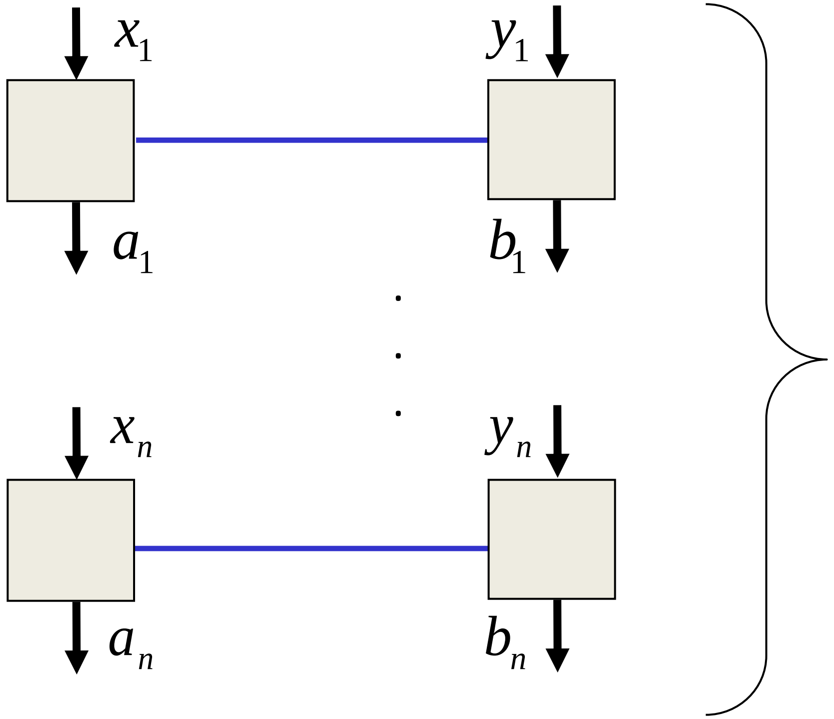
Any protocol should be built from non-local correlations.

Security proof of the protocol

We can prove the security of the protocol against any attack under the assumption that measurements have a tensor product structure.

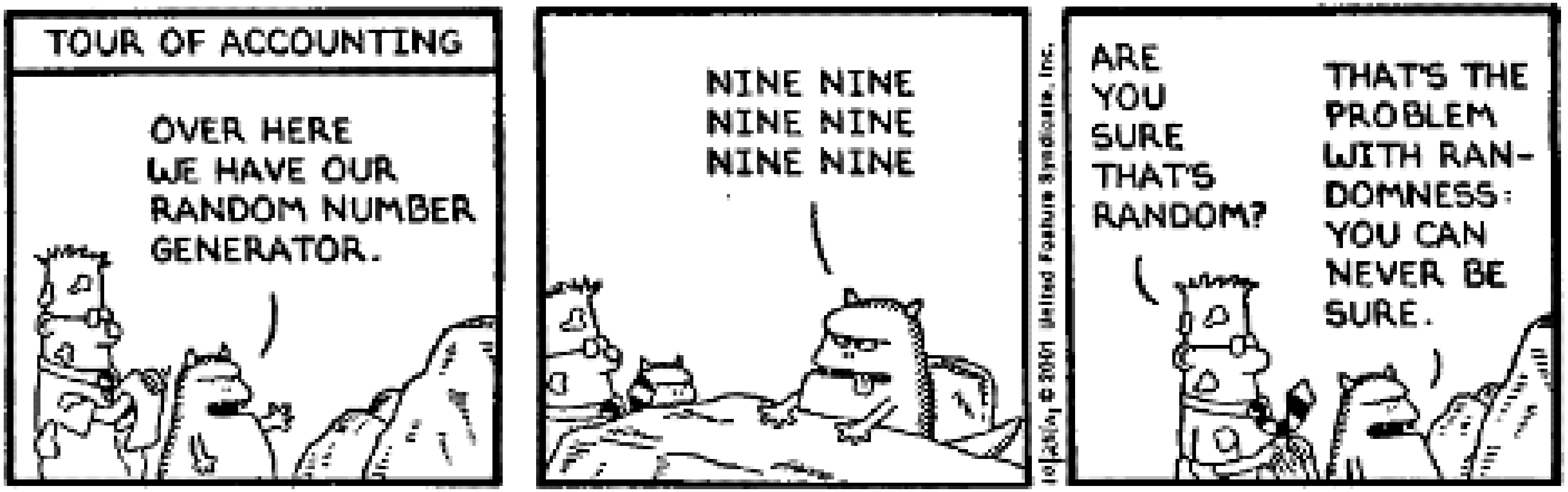
Masanes PRL09

$$P(\vec{a},\vec{b}|\vec{x},\vec{y}) = tr(\rho_{A_1 \ldots A_n B_1 \ldots B_n} M_{a_1}^{x_1} \otimes \ldots \otimes M_{a_n}^{x_n} \otimes M_{b_1}^{y_1} \otimes \ldots \otimes M_{b_n}^{y_n})$$



This assumption can be physically satisfied when the symbols are generated by different devices.

Device-Independent Randomness Generation


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
NINE NINE NINE NINE NINE NINE
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.
10/25/01 © 2001 United Feature Syndicate, Inc.

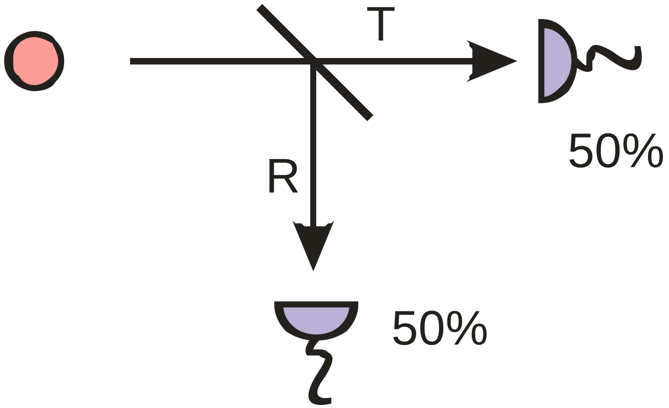
Can the presence of randomness be guaranteed by any physical mechanism?

Randomness tests

- Good randomness is usually verified by a series of statistical tests.
- There exist chaotic systems, of deterministic nature, that pass all existing randomness tests. Uchida et al., Nat. Phot. 2, 728 (2008)
- Do these tests really certify the presence of randomness?

Known solutions

- Classical Random Number Generators (CRNG): all of them are of deterministic Nature.
- Quantum Random Number Generators (QRNG): all the existing solution require some knowledge of the devices. The provider has to be trusted.

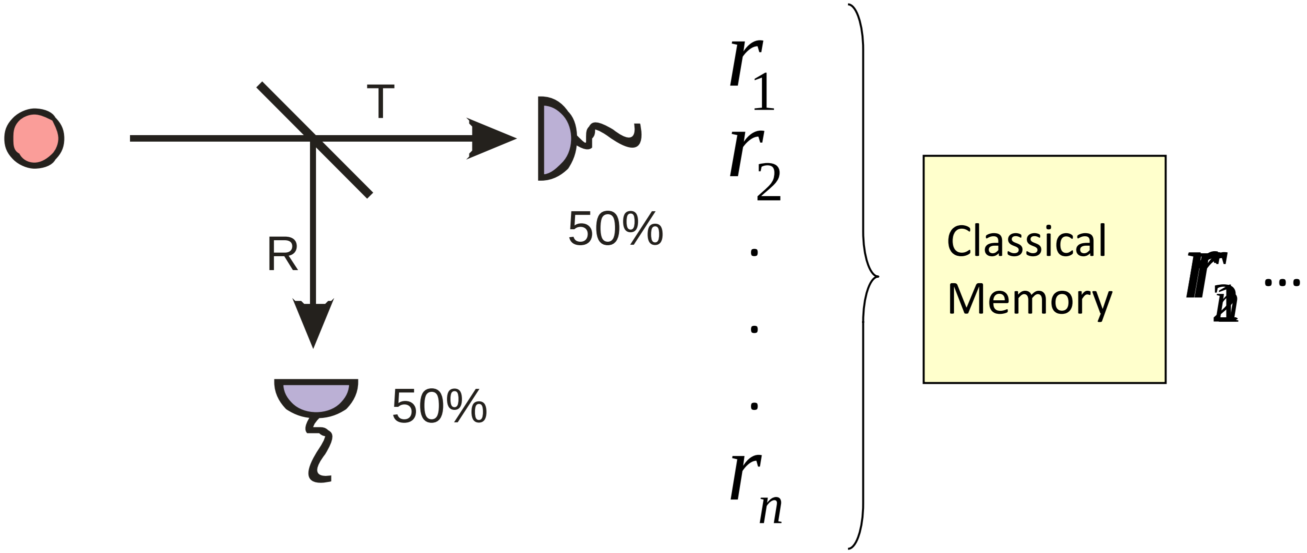


The standard quantum solution crucially depends on the details of the device used for the random number generation.

- In any case, all the solutions guarantee the randomness using standard statistical randomness tests.

Private Randomess

- Many applications require private randomness.
- Untrusted scenario: can one be sure that nobody has a deterministic model for the observed randomness?



r_1
r_2
.
.
.
r_n

Classical Memory

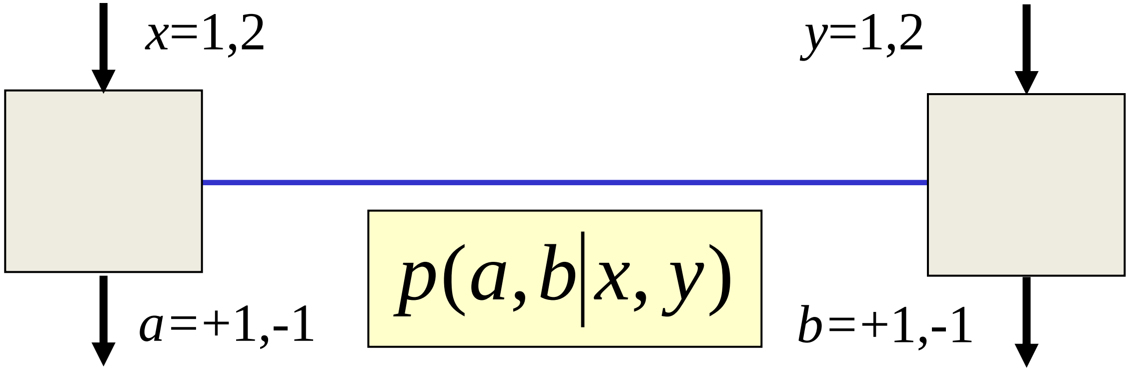
r_1 …

Random Numbers from Bell’s Theorem

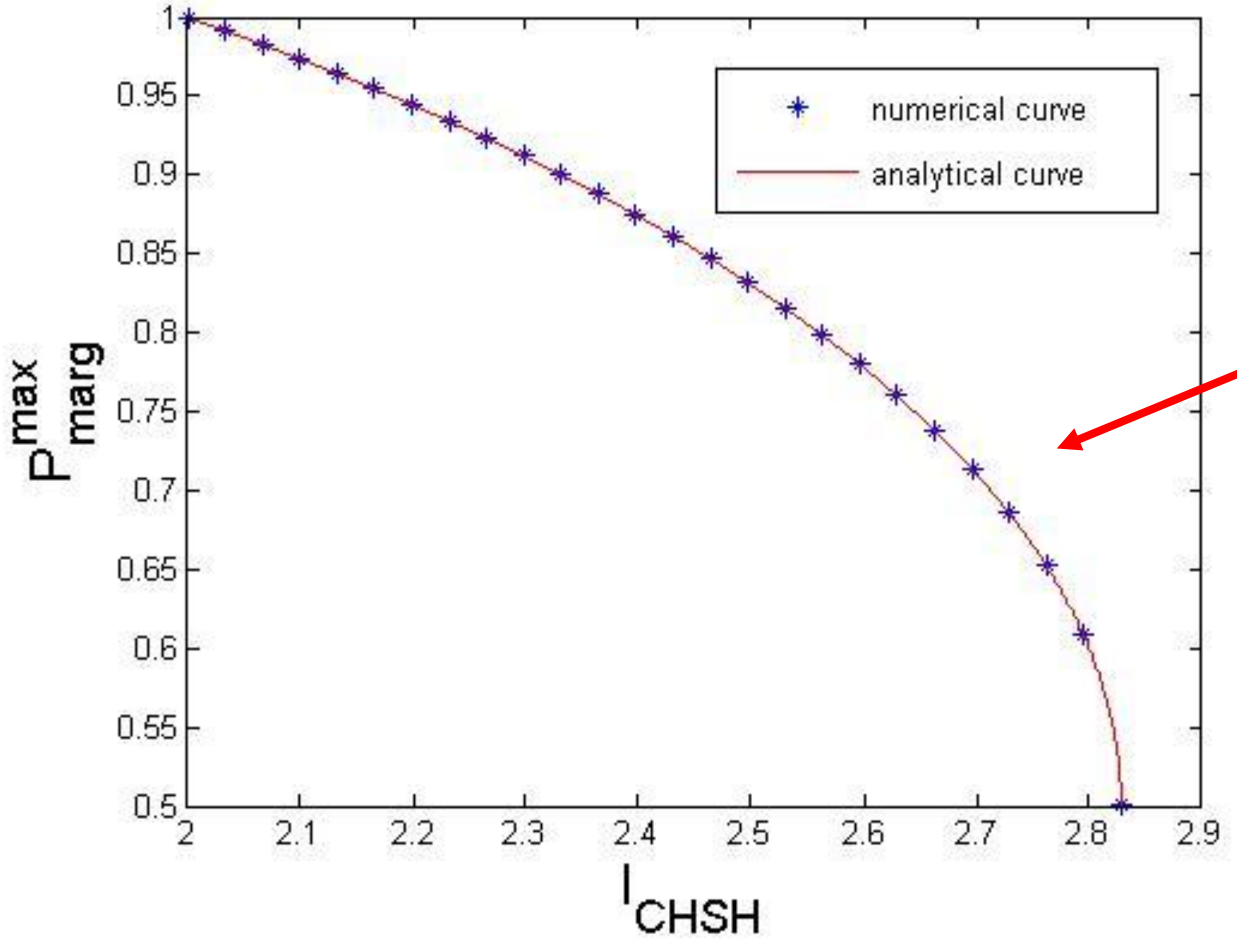
- Randomness can be certified in the quantum world by means of non-local correlations, i.e. the violation of a Bell inequality.
- The obtained randomness is private.
- It represents a novel application of Quantum Information Theory, solving a task whose classical realization is, at least, unclear.
- Our findings can be used to design Device-Independent Quantum Randomness Expanders.

Random Numbers from Bell's Theorem

We want to explore the relation between non-locality, measured by the violation β of a Bell inequality, and local randomness, quantified by the parameter $r = \max_{a,x} p(a|x)$. Clearly, if β =0 → r=1.

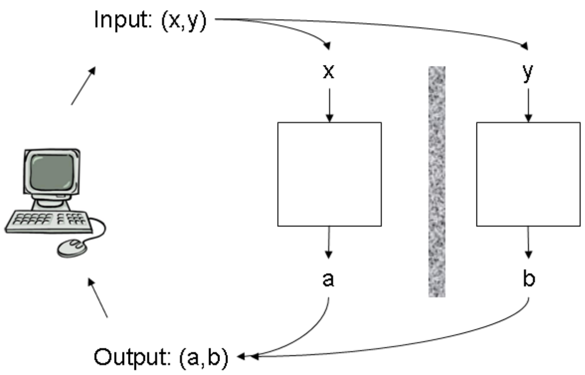


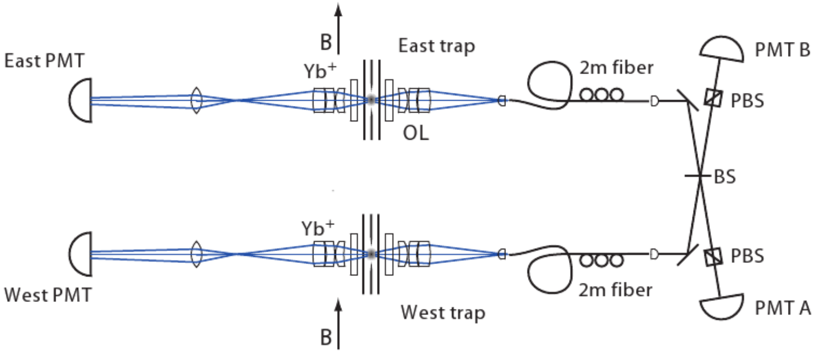
Results



All the region above the curve is impossible within Quantum Mechanics.

Experimental realization





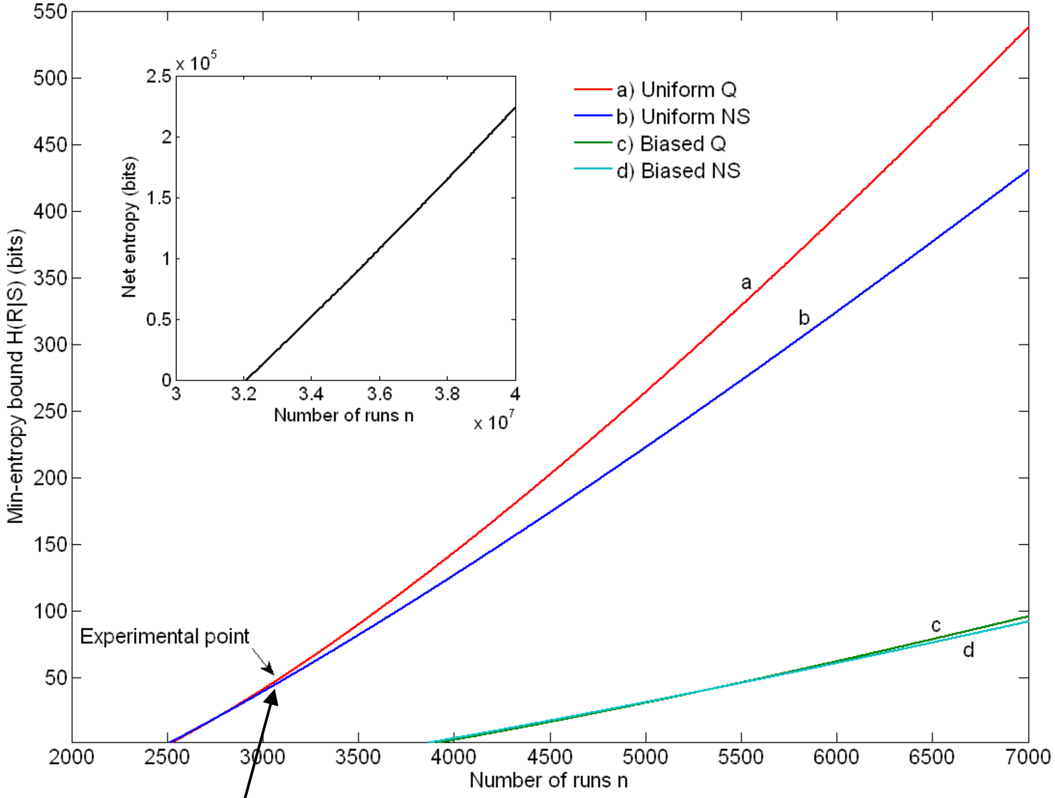
- In a completely untrusted scenario, the Bell test must be loophole-free.

- The setup allows for a detection-loophole-free Bell test but it does not close the locality loophole.

- However, our goal is to certify the generation of randomness. We “assume” that the experiment should be compatible with Quantum Mechanics.

- The experimental realization guarantees a tensor product structure of the measurements. This is all what we need to certify randomness.

Data analysis



- The observed CHSH parameter was equal to 2.4.
- The choice of inputs was fully random, each measurement with probability one half. No expansion!
- We plug this number into the previous formulae and compute the randomness generation curves.

The observed violation certifies the generation of 42 new random bits.

Concluding Remarks

Quantum correlations

- Hierarchy of necessary condition for detecting the quantum origin of correlations.
- Each condition can be mapped into an SDP problem.
- How does this picture change if we fix the dimension of the quantum system?
- Are all finite correlations achievable measuring finite-dimensional quantum systems?

Device-Independent QKD

- It seems possible to construct QKD protocols whose security does not require any assumption on the devices.
- Bell inequality violation is a necessary condition for security in this scenario.
- How to include memory effects?
- These techniques are useful for standard QKD.

Random Numbers from Bell Theorem

- Randomness can be certified in the quantum world by means of non-local correlations, i.e. the violation of a Bell inequality.
- The obtained randomness is private.
- Randomness can be quantified in a setup.
- Multipartite case?
- Link between randomness and non-locality?

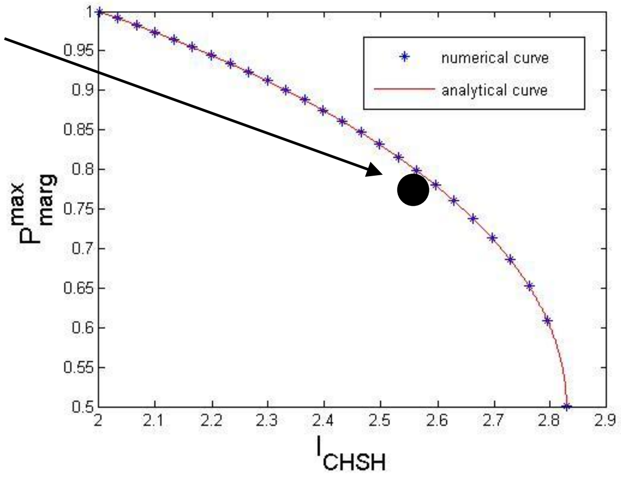
Take-home question

(C or Q)RNG

DIQRNE

Specifications: it passes all statistical randomness tests.

Specifications:



It won’t pass all the existing randomness tests!

Which device is more random?

References

- Quantum Correlations
  1. M. Navascues, S. Pironio and AA, Phys. Rev. Lett. 98, 010401 (2007)
  2. N. Brunner, S. Pironio, AA, N. Gisin, A. A. Methot and V. Scarani, Phys. Rev. Lett. 100, 210503 (2008)
  3. M. Navascues, S. Pironio and AA, New J. Phys. 10, 073013 (2008)
  4. S. Pironio, M. Navascues and AA, SIAM J. Optim. 20, 2157 (2010)

- Device-Independent QKD
  1. AA, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, Phys. Rev. Lett. 98, 230501 (2007)
  2. S. Pironio, AA, N. Brunner, N. Gisin, S. Massar and V. Scarani, New J. Phys. 11, 045021 (2009)
  3. L. Masanes, S. Pironio and AA, in preparation.

- Device-Independent Randomness Generation
  1. S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning and C. Monroe, Nature 464, 1021 (2010)