Quantum Information Processing with Real-world Devices

Jean-Daniel Bancal

UNIVERSITÉ DE GENÈVE

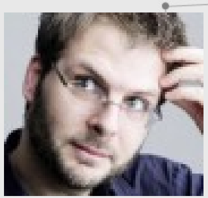
CEA Saclay, May 2020

Where do I come from?

2007 - 2012	PhD with Prof. Gisin, Group of Applied Physics, Geneva
2012 - 2015	Research Fellow, Center for Quantum Technologies, Singapore
2015 - 2018	Research Assistant, Quantum Optics Theory Group, Basel

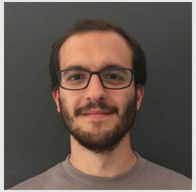
Currently (since 2019)

Maître Assistant in the Quantum Correlations group of Prof. Brunner, Geneva

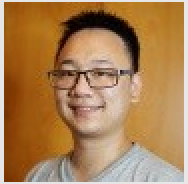


Working closely with

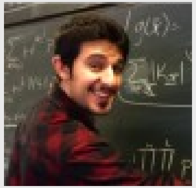
Marie Ioannou (PhD)
Semi-DI QKD



Davide Rusca (PhD)
Finite statistics

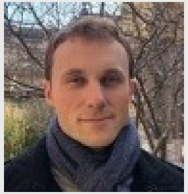


Cai Yu (postdoc)
Multipartite nonlocality,
Entangled sets



Armin Tavakoli (PhD)
Mutually unbiased bases

Ivan Šupić (postdoc)
Multipartite nonlocality



Alastair Abbott (Postdoc)
Semi-definite programming

Collaborations

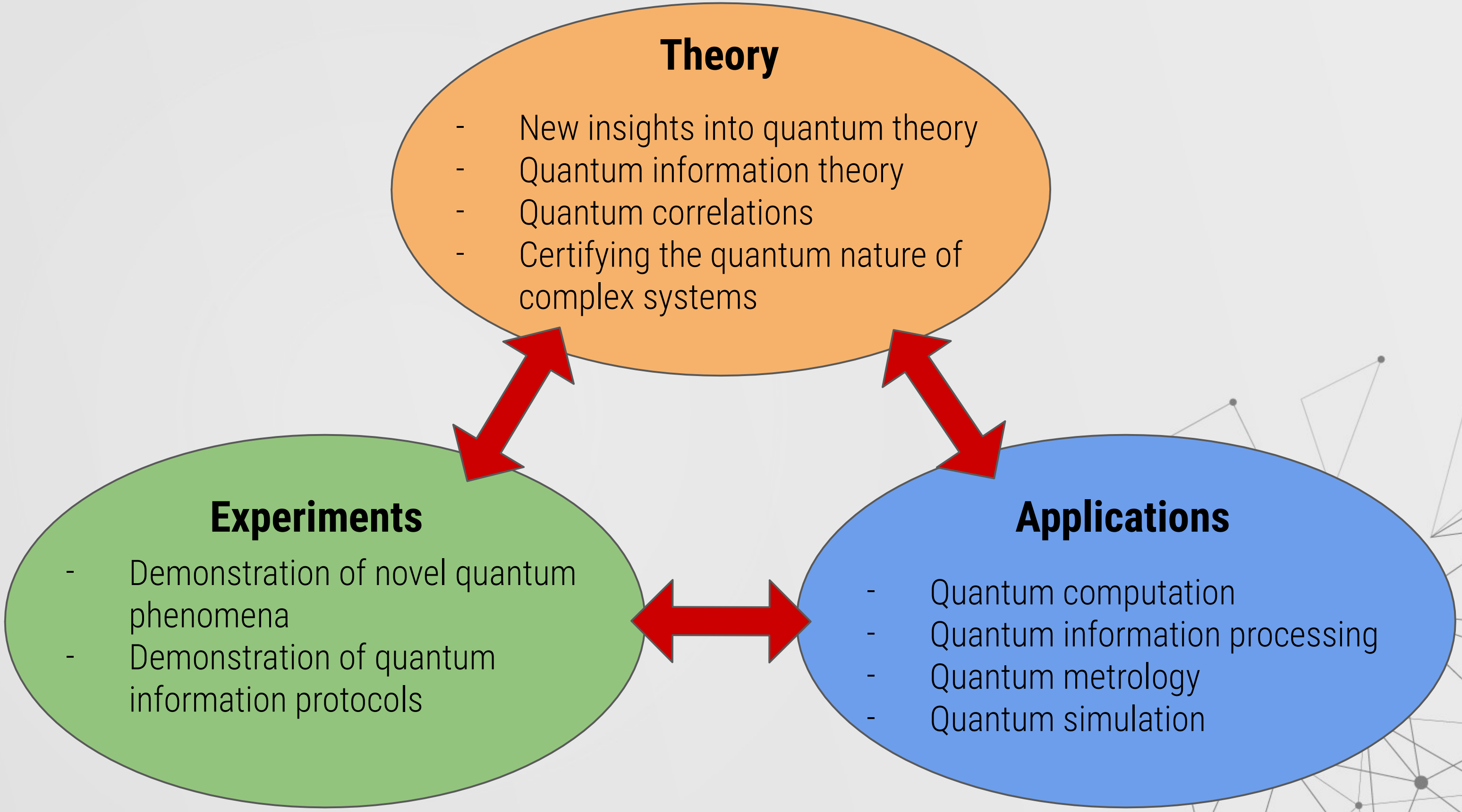
Theory groups

Acín (Barcelona) PRA‘19
Arnon-Friedman (UC Berkley) NJP‘19
Augusiak (Warsaw) PRA’19
Branciard (Grenoble) JPA’12
Dür (Innsbruck) PRL‘19
Gühne (Siegen) PRL’13
Kaniewski (Warsaw) arXiv‘19
Lewenstein (Barcelona) PRA’19
Liang (Tainan) PRA‘18
Martin-Martinez (Waterloo) PRA‘16
McKague (Brisbane) PRA‘16
Navascués (Vienna) PRL’14
Pironio (Bruxelles) NJP‘16
Popescu (Bristol) Nature Comm.‘20
Renner (Zurich) arXiv’20
Spekkens (Perimeter Institute) arXiv’20
Sangouard (CEA Saclay) Quantum‘20
Scarani (Singapore) PRL’18
Vertesi (Hungary) PRL’14

Experimental groups

Blatt (Innsbruck) Nature Phys.’13
Eschner (Saarbrücken) NJP’13
Kurtsiefer (Singapore) PRL‘18
Laurat (LKB) PRL‘13
Martin (Nice) arXiv’19
Romero (Brisbane) JPA‘16
Weinfurter (Munich) arXiv‘18
Treutlein (Basel) Science‘16
Zbinden (Geneva) PRL’15

Overview of my research



Outline

1 Introduction to quantum correlations

2 Genuine randomness and black-box certification

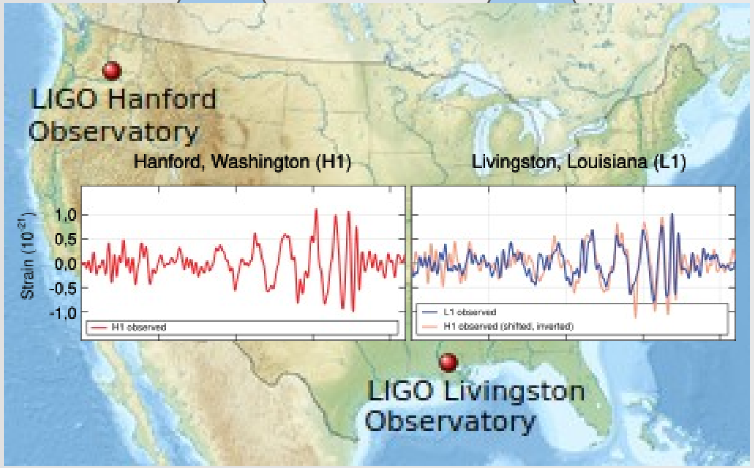
3 Certification of future devices

Correlations

A **B**

H H

H H



Two possible explanations:

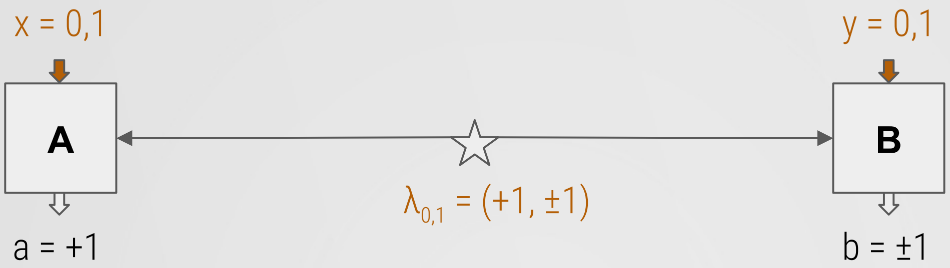
- Direct causal influence

$$\mathbf{A} \Longrightarrow \mathbf{B}$$

- Common cause

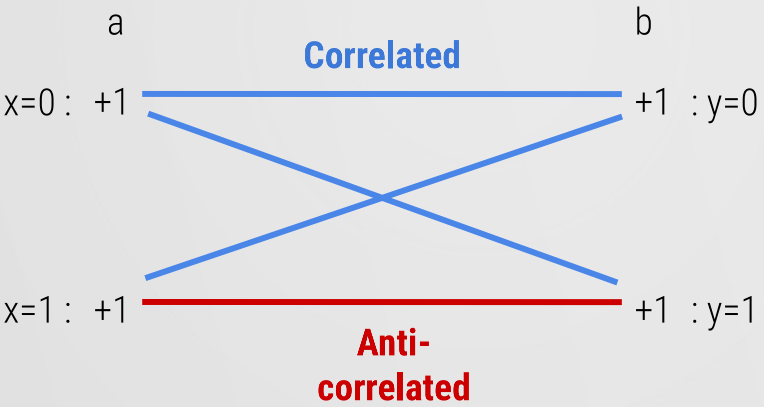
$$\mathbf{A} \Longleftarrow \lambda \Longrightarrow \mathbf{B}$$

Local correlations



(Anti)-correlated results

-> any correlation possible



With settings, all statistics are not achievable

CHSH Inequality: $S = \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle$

Non-local correlations

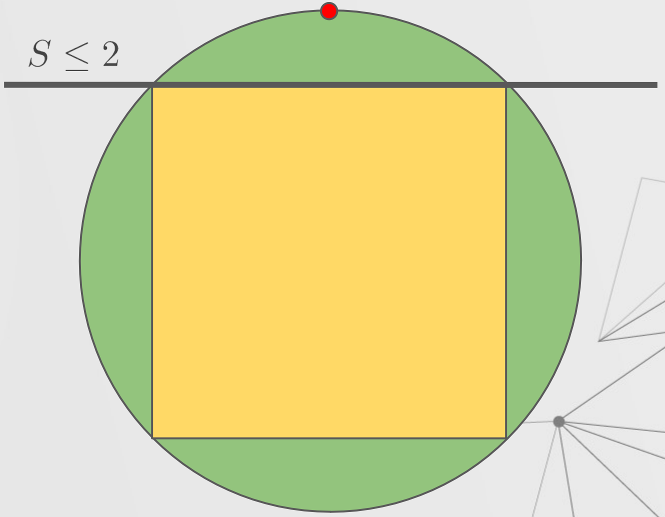
Characterize possible behaviors $P(a, b|x, y)$

- Convex set
- Boundaries are Bell inequalities

Quantum correlations are nonlocal:

$$P(a, b|x, y) = \langle \psi_{AB} | A_{a|x} \otimes B_{b,y} | \psi_{AB} \rangle$$

$$|\psi_{AB}\rangle = (|00\rangle + |11\rangle)/\sqrt{2} \quad \rightarrow S = 2\sqrt{2}$$



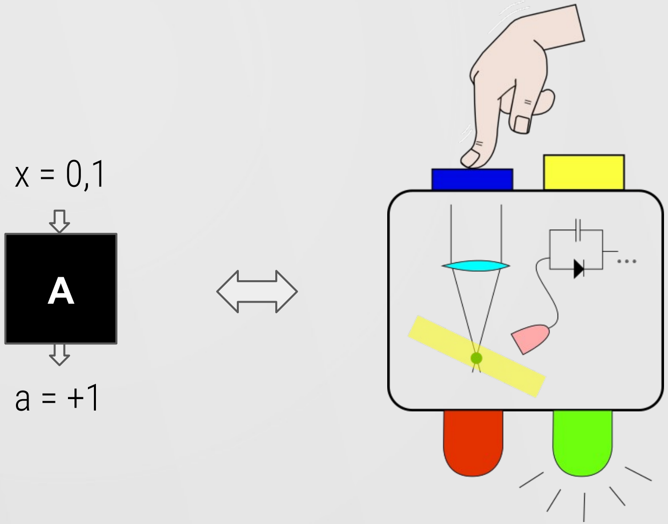
Black-box approach

Assumptions:

- Separation between the parties
- Choice of settings independent of λ

Non-assumptions:

- What are the relevant degrees of freedom
- How the outcomes are actually produced
- Amount of systematic errors



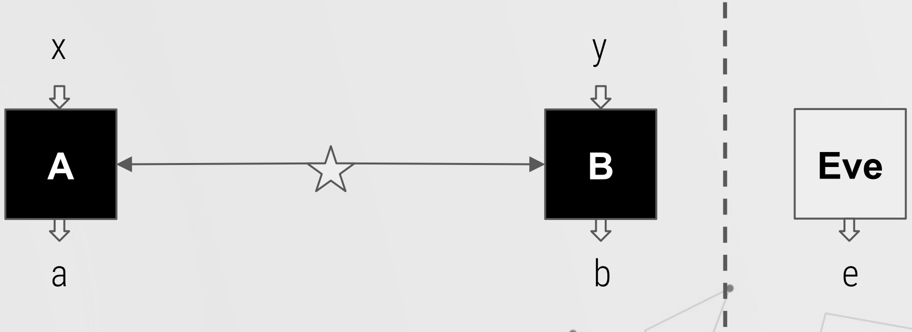
2

Genuine Randomness and Black-box Certification

Genuine Randomness

Is this bit string random : 0010111?

- Random for whom?
- Processes can be random

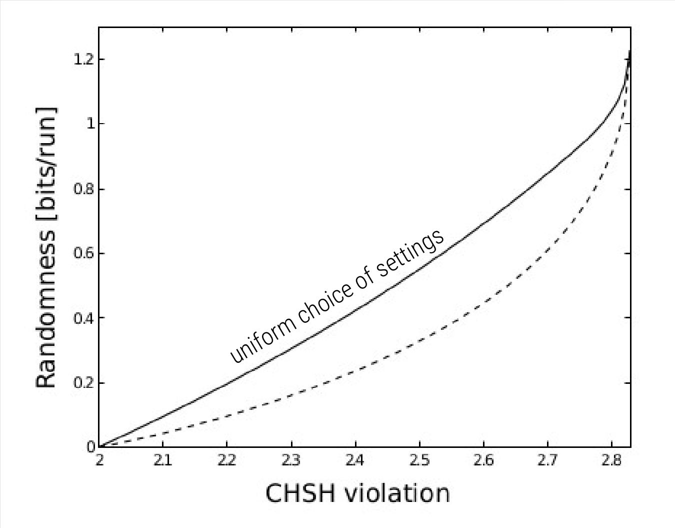


The adversary is given full knowledge about the devices

Prior knowledge λ cannot explain the outcomes ⟺ The adversary cannot guess the outcomes

Colbeck '06, Pironio et al., Nature'10

Randomness quantified



Randomness can be quantified by

$$H_{\min} = -\log_2(P_{\text{guess}})$$

In presence of side information λ, we have the decomposition

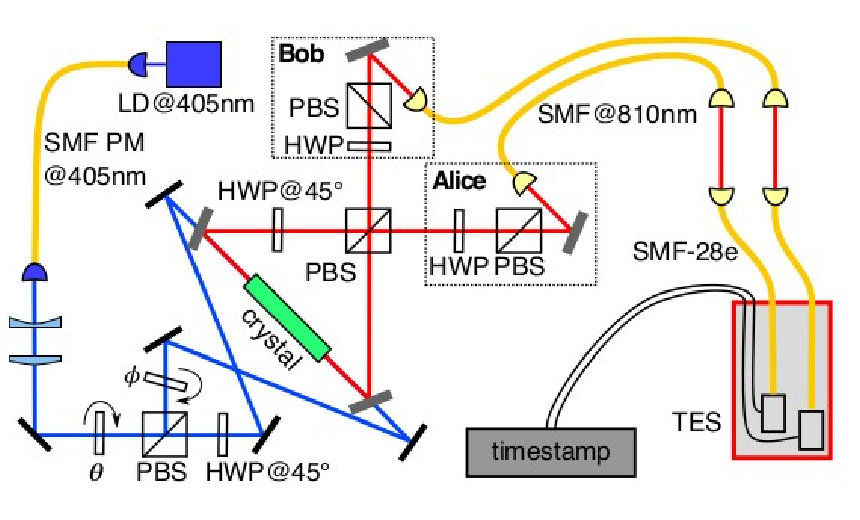
$$P(a,b|x,y) = \sum_{\lambda} q_\lambda P(a,b|x,y,\lambda)$$

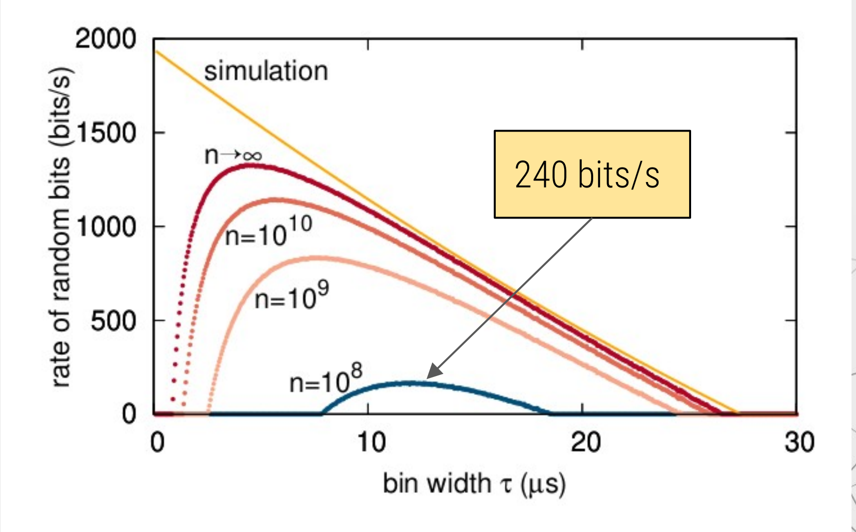
The average guessing probability can be expressed as

$$P_{\text{guess}} = \sum_{x,y} p(x,y) \sum_{\lambda} q_\lambda \max_{a,b} P(a,b|x,y,\lambda)$$

Bancal et al., NJP'14

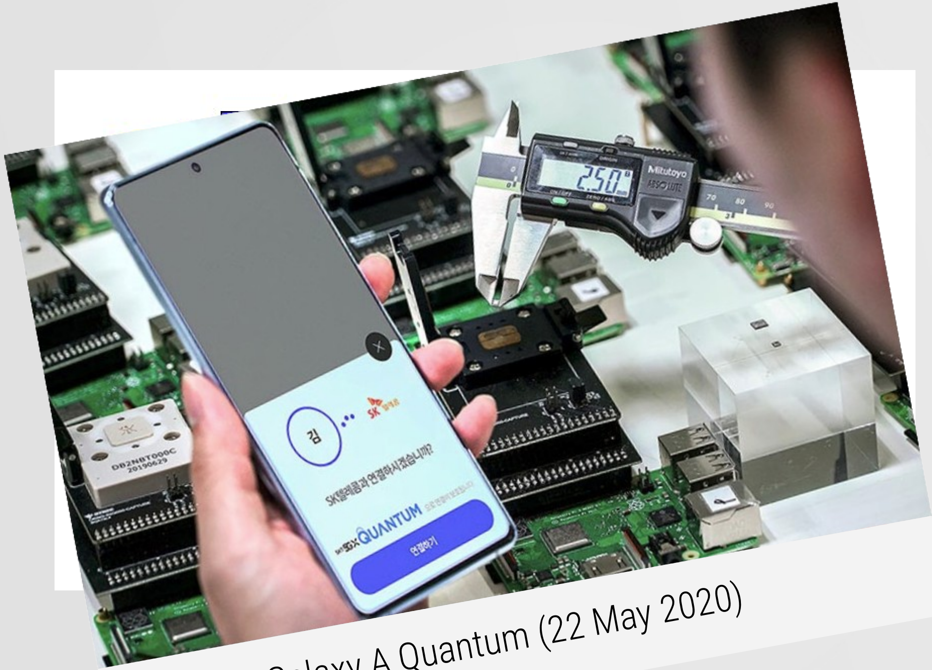
High-speed experimental randomness with a continuous SPDC source





Shen, Lee, Le Phuc, Bancal et al., PRL'18

High-speed experimental randomness with a continuous SPDC so…



Samsung Galaxy A Quantum (22 May 2020)

30

l., PRL'18


https://beacon.nist.gov/home

NIST National Institute of Standards and Technology U.S. Department of Commerce

Beacon Record

URI: https://beacon.nist.gov/beacon/2.0/chain/1/pulse/907848

Version: Version 2.0

Cipher Suite: 0: SHA512 hashing and RSA signatures with PKCSv1.5 padding

Period: 60000 milliseconds

Certificate Hash: 02288edbdc04bdeeb1c8140a41a1ad40ab2ea7ad27fdd316946f3ec5aff1a712
9f1fb5078202d75d42c201878b06d79c45bf37adb55f83aa213200834792b1da
View

Chain Index: 1

Pulse Index: 907848

Time: 2020-05-28T17:08:00.000Z

Local Random Value: 6EF99249CB437314FC787847C35BDE0703808A03942FCF3FEA979CB1FD7E944B
B905E4EE91921E74F36966F9C376F3FF898EE463FCB30F8664BF5F6696C44F60

External Source Id: 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

External Status Code: 0

External Value: 0000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000

Previous Output: A0E82B833C96AD20AE5EEEDBB5D03C13CCED09E39AA7C0B705AA4771C5BBE16A
7CD09E3E80401BDCBB7C876472B4D29BB3952731876CD4BDCA1093119ECE679B

Hour: 446B716C67ED76CF100BB347DB4790B7AB6A2D996D6F7A34AAF80587A38B9CF3
6A1EEF8DCA83052867B4996ECA167472495B846DC67AAF3EF39C900F7DE3B8B7

Day: 9BDF5B27B70681A493DB1CFA5D722B4A2135B2D8D9E33693FE5F03EF48C279DA
E08EDEF3D9FC1B06F3201CD03F387320BE423C3AAEE0888CD9B49641BA2B214E

Month: F0DE2F2606CA3AA287F99AB1308EEE5C5857816EF60EDDD7B57DD28E5A7BF531
04BE2A1ACFC48654E1124AB7ECC60FD449F5505C93F44F3BB8FCEACF512D9DF7

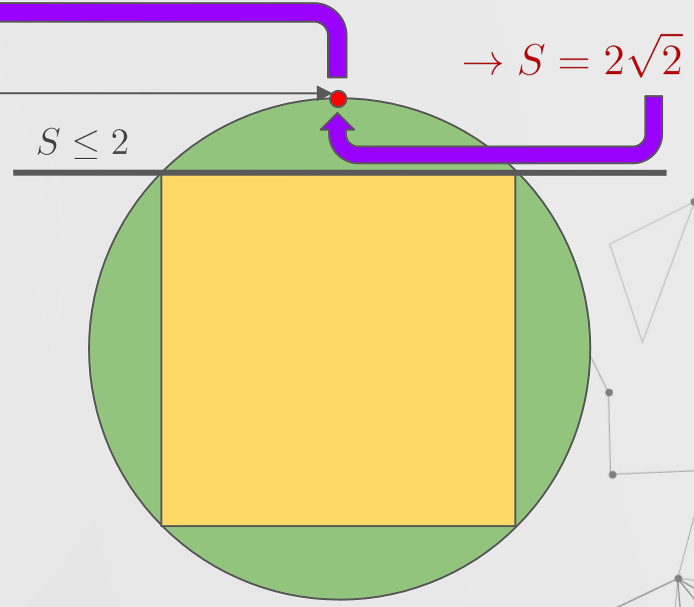
Year: CBC9AA97CDD5954218C585C89B061F356EF5F4158622C7CB38FBC317CA69C7AB
E9E4379D4738B1076F7671C916C78AD0167A9ADB5A53E0CB20CC7F3D38736857

Precommitment Value: 4DA748C2D801FCB5FC5BF44FB39E6C376C17105270E8C91B8E8AD9A719CF58F9
3B86D23D4CBEB2561B158D0D0FC21D5BD0F3D652B08FB2ED8547A821915ED359

Signature: 8614C6BD74CE69E7104FFC3DB3F12D062E181861FE8CFECAB0A3C92C5A70DE70

The other way around

$$|\psi_{AB}\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$$

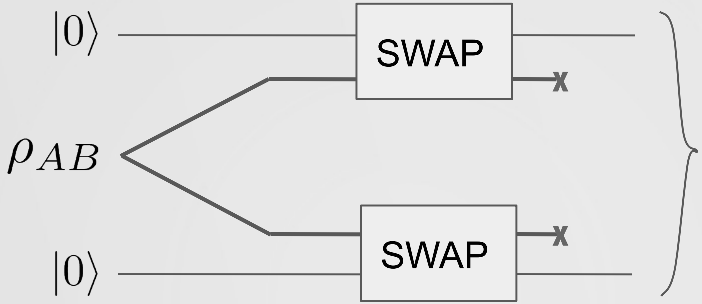


Black-box certification: Mayers, Yao, QIC'04

- Blind tomography
- Calibration ab initio
- Robust — Yang, Vertesi, Bancal et al., PRL'14
- Generic (multiple states, measurements, operations) — Bancal et al., PRL'18, Sekatski, Bancal et al., PRL'18, Wagner, Bancal et al., Quantum'20

Black-box certification

Idea: extract the desired part of the state in trusted registers Yang, Vertesi, Bancal et al., PRL'14



$$\rho_{\text{SWAP}} \leftrightarrow |\phi^+\rangle$$

How to construct a SWAP operator for an uncharacterized device?

$$U = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes A_0$$

$$V = \mathbb{I} \otimes \frac{\mathbb{I} + A_1}{2} + \sigma_x \otimes \frac{\mathbb{I} - A_1}{2}$$

Black-box certification

The swapped state can be described in terms of moments : $\langle \prod_i A_{x_i} \prod_j B_{y_j} \rho_{AB} \rangle$

$$\rho_{\mathrm{SWAP}} = \mathrm{Tr}_{AB}\left((\mathbf{S}_{AA'} \otimes \mathbf{S}_{BB'}) \left(\rho_{AB} \otimes |00\rangle_{A'B'}\langle 00|\right) (\mathbf{S}_{AA'} \otimes \mathbf{S}_{BB'})^\dagger \right)$$

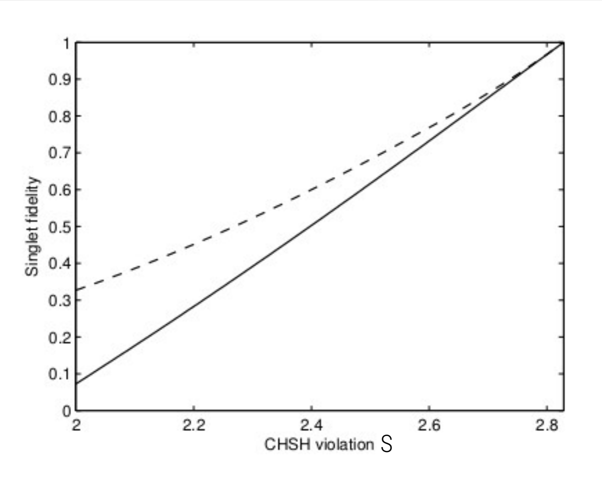
Quantum moments can be characterized by semi-definite programming

Navascués et al., PRL'07

$$\min_{\vec{x}} \langle \phi^+ | \rho_{SWAP} | \phi^+ \rangle$$

$$\text{s.t.} \sum_i f_i(a,b|x,y) x_i = P(a,b|x,y)$$

$$\sum_i F_i x_i \geq 0$$

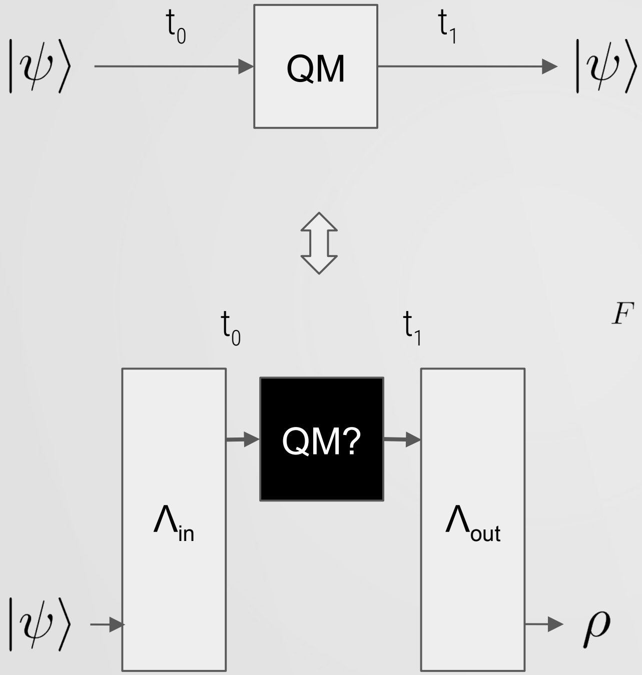


- The construction applies to arbitrary Hilbert space dimensions

- Results are robust by construction

Yang, Vertesi, Bancal et al., PRL'14

Certifying a quantum memory

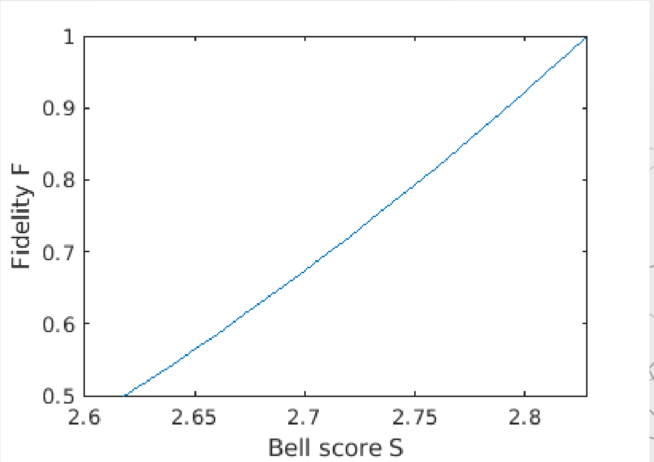


Decoherence decreases the Bell violation

No loss in violation => no decoherence

Sekatski, Bancal et al., PRL'18

$$F = \langle\psi|\rho|\psi\rangle \geq \frac{(12 + 8\sqrt{2} - (4 + 5\sqrt{2})S)^2}{64}$$



The device can be used instead of an ideal quantum memory with quantified impact.

3

Certification of Future Devices

Quantum computations

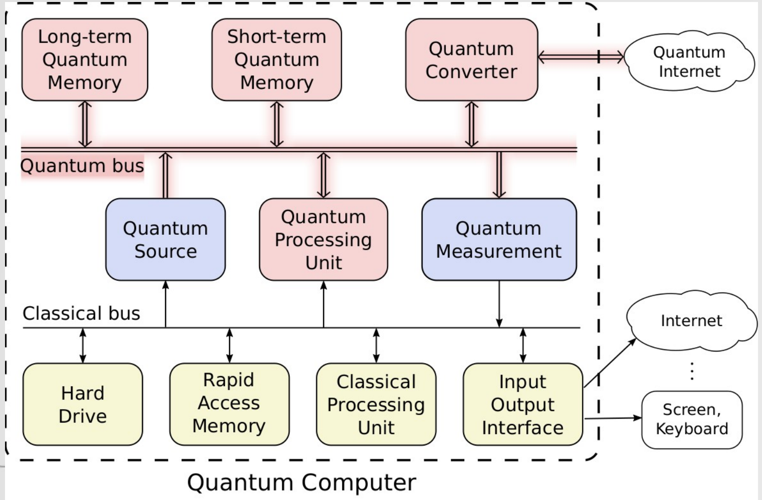
Potential of quantum computation:

- Factoring (breaks RSA) Shor, '95
- Combinatorial problems, QAOA (math) Google, arXiv'20
- Machine learning (quantum annealing) Biamonte et al., Nature'17
- …

Complexity advantage over classical computations Google, Nature'19

Can one trust the outcome of a quantum computer?

Certifying quantum computations



Quantum computers need to be certified in some sense

- Device-independent certification is the strongest possible certification

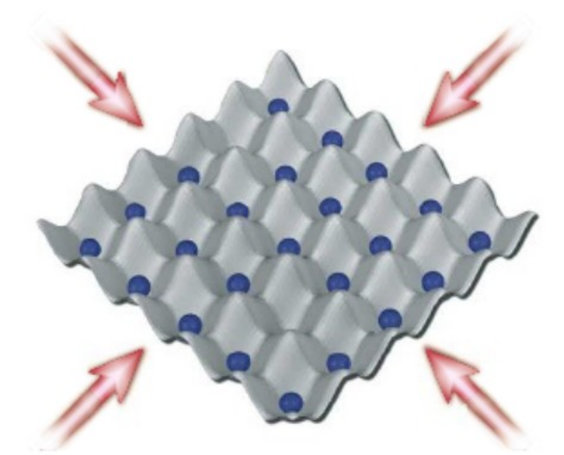
Proposal:

- Certify shallow circuits
  - Demonstrate quantum advantage
  - Suitable for many architectures
  - Device-independent tools readily apply:
    - CNOT and other gates already certified

Sekatski, Bancal et al., PRL'18

Quantum simulation

- Huge potential in multiple fields: Tacchino et al., arXiv'20
  - Chemistry
  - High energy physics
  - Condensed matter
  - …
- NISQ devices are already helpful -> near-term

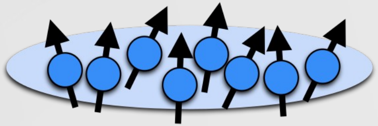


Bloch, Nature'08

Can one trust the outcome of a quantum simulator?

Quantum features in many-body systems

Quantum correlations play a key role in many-body systems



We recently demonstrated the presence of Bell correlations in a 480 atoms BEC

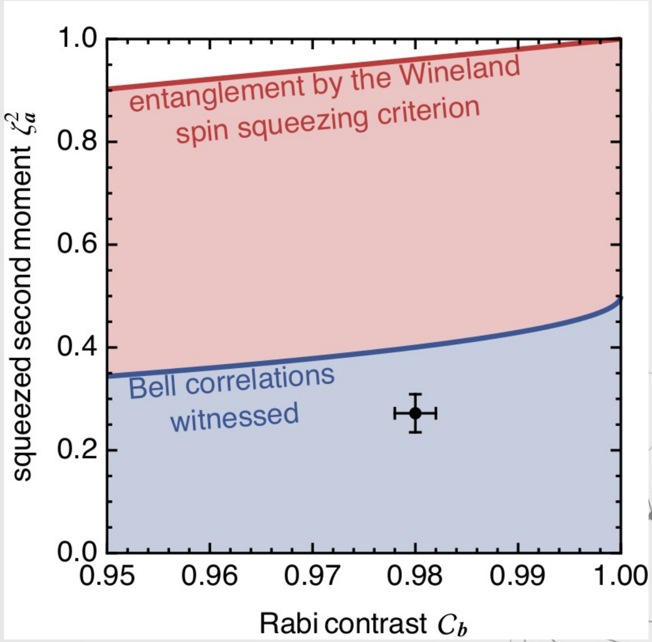
Next steps:

- Revealing quantumness in large systems require a lot of statistics — Bancal et al., PRL'17

- Quantification of genuinely multipartite Bell correlations needed
  - First results — Baccari, Tura, Fadel, Aloy, Bancal et al., PRL'19

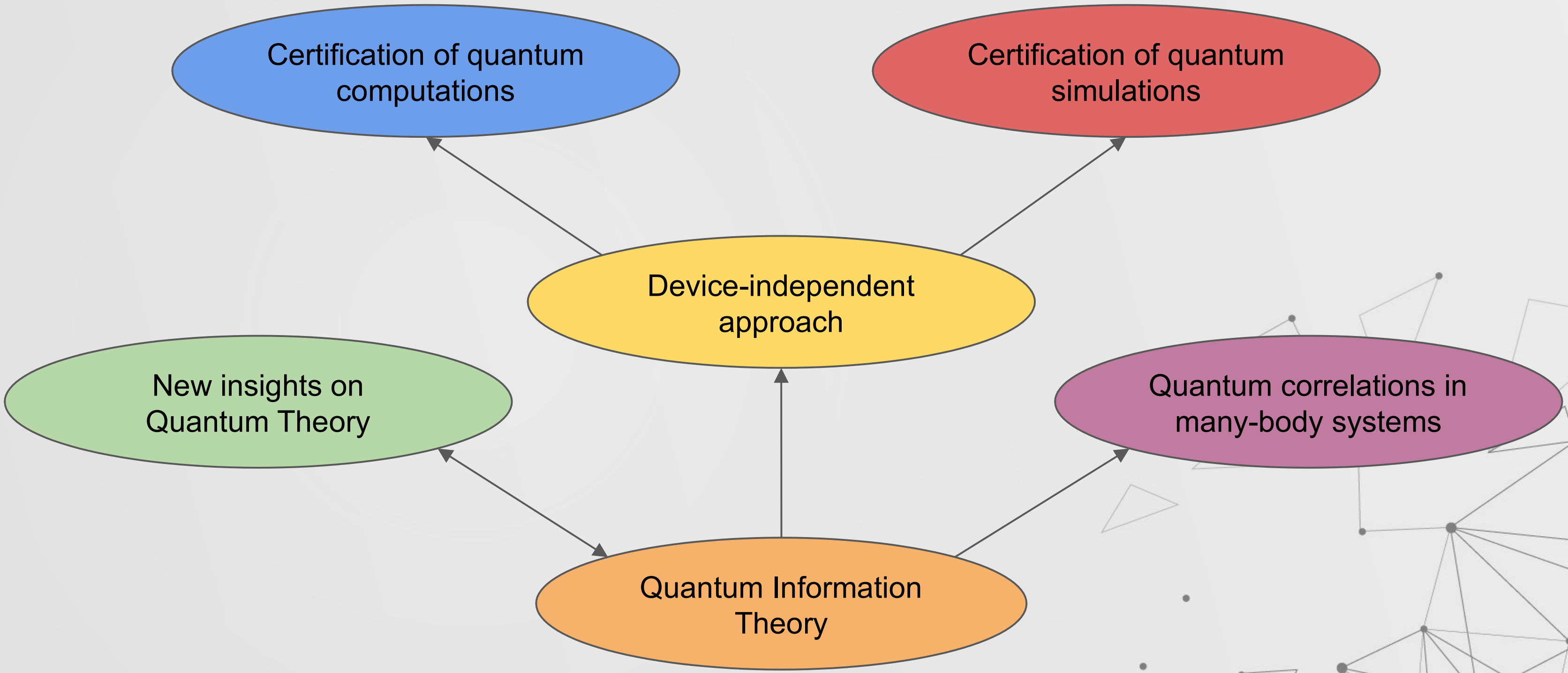
10 years of experience with nonlocality in multipartite systems

Bancal et al., PRL'09 --- Zwerger, Dür, Bancal et al., PRL'19

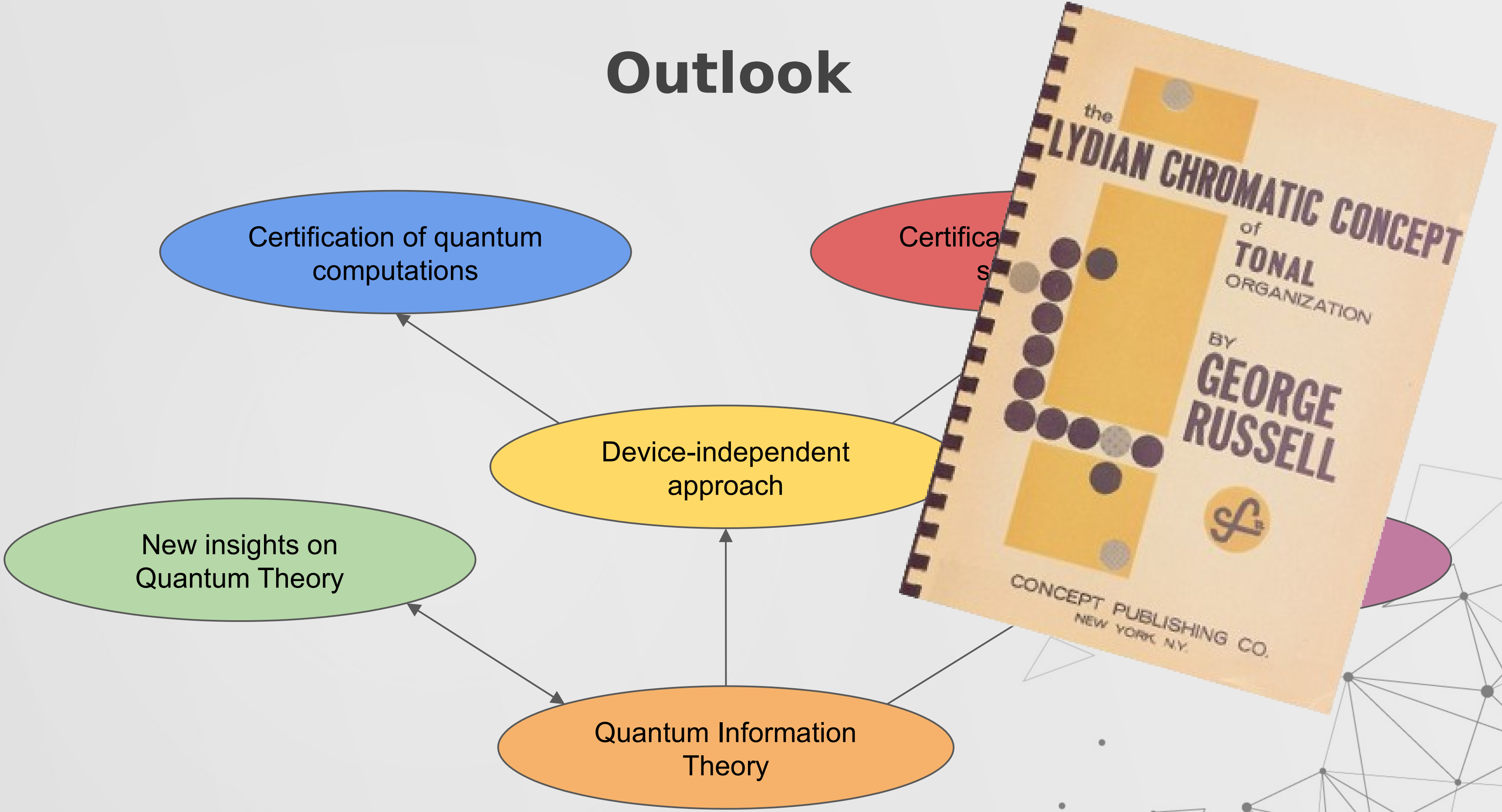


Schmied, Bancal et al., Science'16
Awarded P. Ehrenfest Price 2017
See also Tura et al., Science'14

Outlook


Certification of quantum computations
Certification of quantum simulations
Device-independent approach
New insights on Quantum Theory
Quantum correlations in many-body systems
Quantum Information Theory

Outlook


Certification of quantum computations
Certifica
Device-independent approach
New insights on Quantum Theory
Quantum Information Theory
the
LYDIAN CHROMATIC CONCEPT
of
TONAL
ORGANIZATION
BY
GEORGE RUSSELL
CONCEPT PUBLISHING CO.
NEW YORK N.Y.