Trust, Security and Quantumness

Damian Markham

Leonardo Disilvestro

Vedran Dunjko (Innsbruck)

Petros Wallden (Edin.)

Elham Kashefi

Alexandru Gheorghiu (Edin.)

cnrs

PCQC

UPMC SORBONNE UNIVERSITÉS

Where does quantum advantage come from?

- (tells us something interesting about the universe...?)
- How to exploit it more!
- How to protect fragile quantum features
- How to optimise

Quantum computing

- Its definitely entanglement!
  - entanglement needed for speedup [Josza '97]
  - speedup with pseudo mixed states [Linden Popescu '91]
  - low entanglement is classical [Vidal '08]
  - too much entanglement is bad! [Gross../Bremner... '08]
- No, its definitely discord!
  - speedup with no entanglement needs discord [Datta, Shaji, Caves '08]
  - Almost all states have discord [Ferraro et al '10]
- No, no, no, its definitely certainly all about contextuality!
  - contextuality needed MBQC [Anders Browne / Raussendorf '09]
  - contextuality needed magic state [Howard et al '12]
  - not needed for separation [Hoban et al '14]

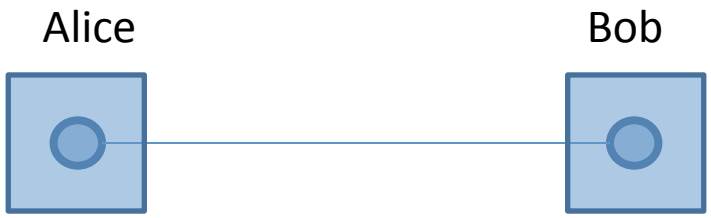
Quantum key distribution

- Heisenberg Uncertainty
- Entanglement
- Non-locality
- Steering
- ...

Key insight: different level of trust / assumptions require different levels of 'quantumness'

C. Branciard et al, _PRA 2012

Non-locality and trust



EPR '35: where does randomness come from?

- Bell: no LHV model exists violating inequality
- If there is no law of nature that can predict the outcomes of the measurement, neither can an Eavesdropper! [Ekert '91]

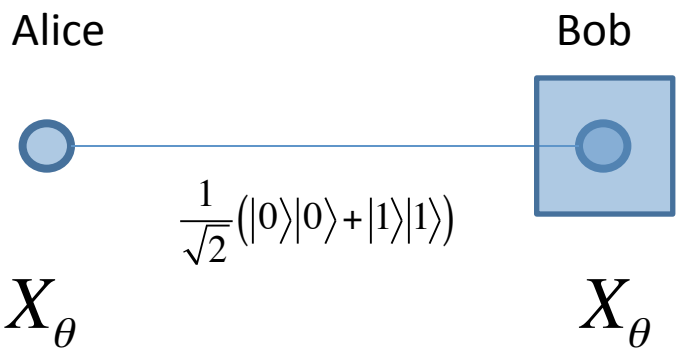
-> crucially Bell's theorem does not use QM!

- device independent QKD! [Colbeck '06, Acin...]

Steering and trust

- Schrodinger: Bob performing measurements can 'steer' Alice's system
- Alice can check correlations by measuring her system (*knows* the measurements she makes!)
- One sided device independent

Steering and trust



Protocol

- Alice asks Bob to measure X_θ

θ →

- Bob sends Alice result

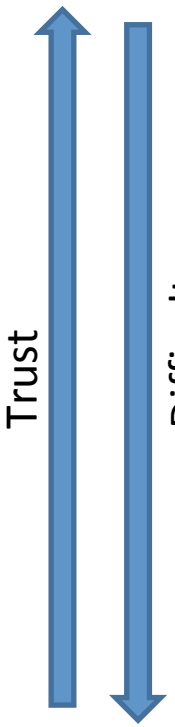
← ± 1

- Alice measures X_θ

-> if results match ACCEPT

no match FAIL

Different degrees of trust



Alice Bob

- **QKD**

Alice and Bob fully trust their devices (know measurements)

- 1-sided DI-QKD

Alice fully trusts her device, Bob does not (only knows his statistics)

Steering

- Fully DI-QKD

Neither Alice nor Bob trust their devices (only know statistics)

Bell non-locality

C. Branciard et al, _PRA 2012

Different degrees of trust

Trust

Difficulty

Alice

Bob

Alice and Bob fully trust their devices (know measurements)

- **QKD**
- **Ent. Witnesses**
- **Quantum channel authentication**
- **Secure secret sharing (practical authentn)**

Alice fully trusts her device, Bob does not (only knows his statistics)

- 1-sided DI-QKD
- **1-sided DI ent. verification**
- **FK verified blind universal QC**

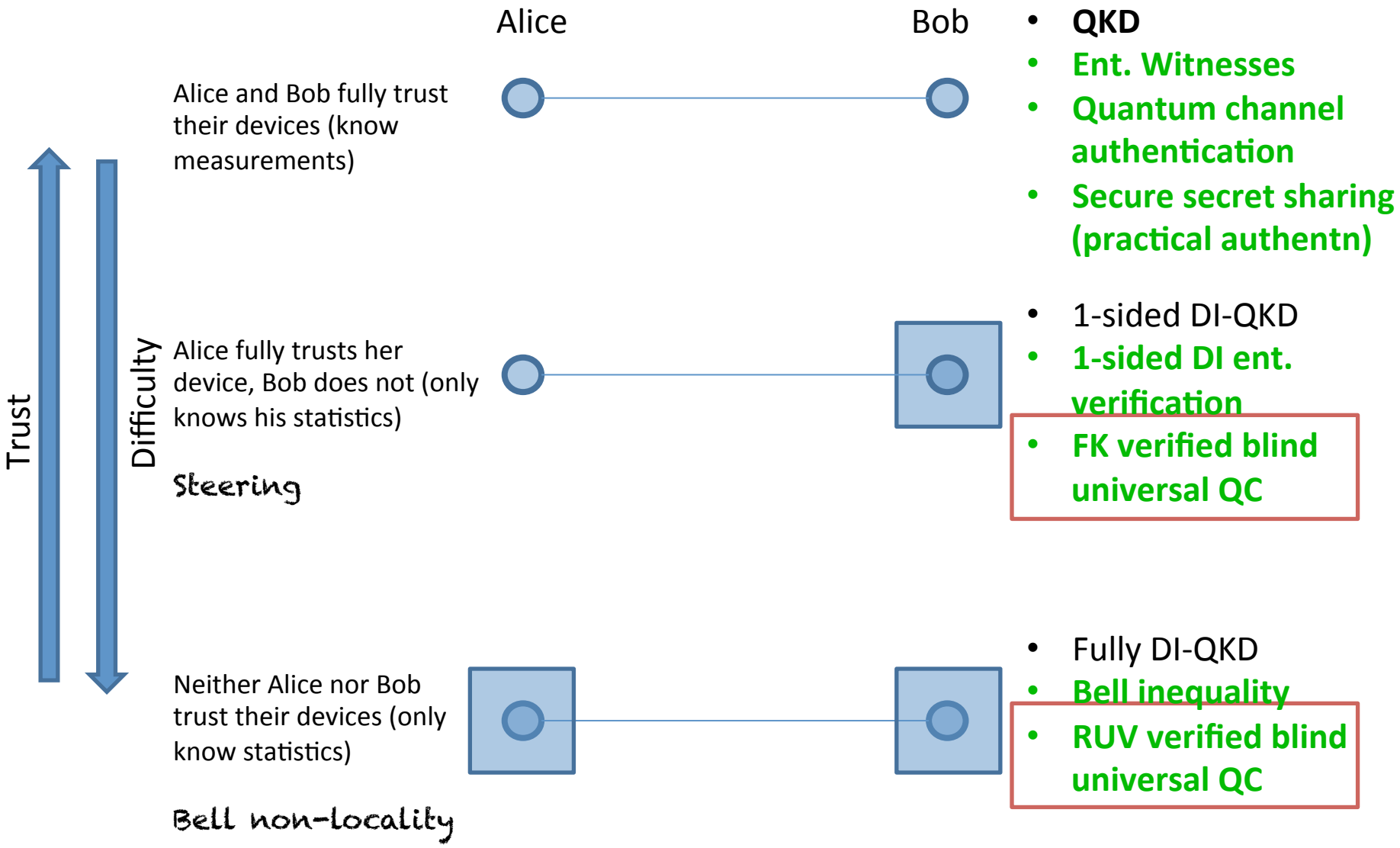
Steering

Neither Alice nor Bob trust their devices (only know statistics)

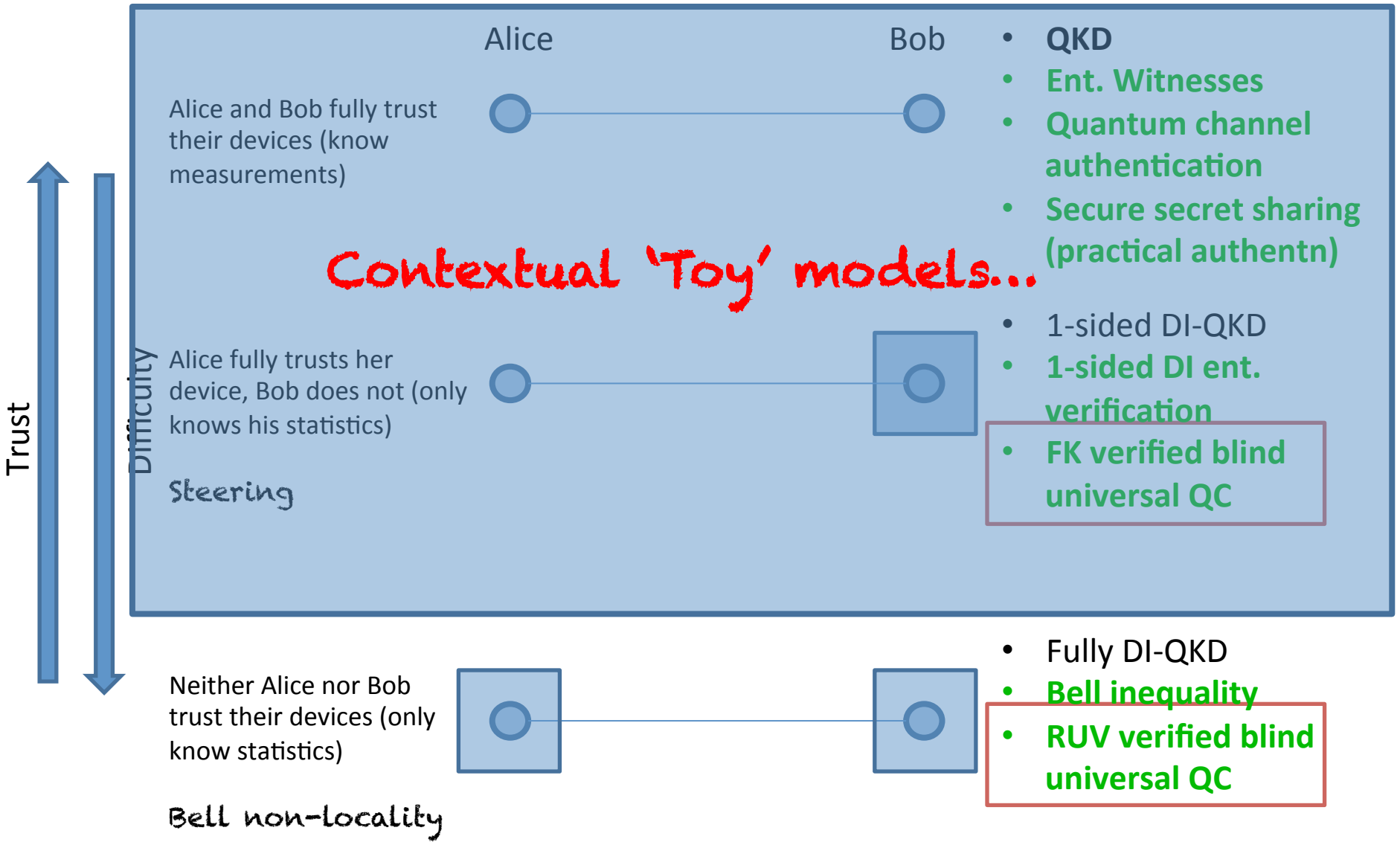
- Fully DI-QKD
- **Bell inequality**
- **RUV verified blind universal QC**

Bell non-locality

Different degrees of trust



Different degrees of trust

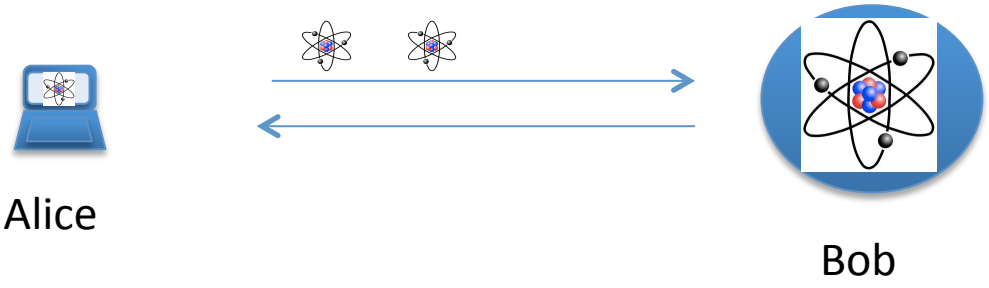


Verified Universal Quantum Computation

- Alice has small / no quantum power
  Bob has universal QC
- Wants to 'delegate' a computation to Bob such that
  - Bob gets no information of the computation (Blind)
  - Alice can be sure Bob does it (verified)

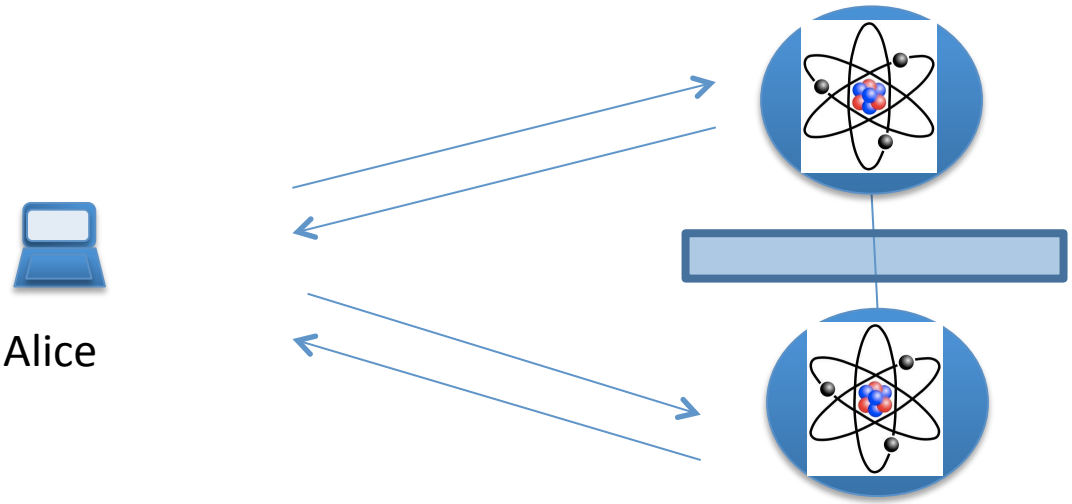
Verified Universal Quantum Computation

- A weakly quantum Alice [Fitzsimons Kashefi'12]



Blind prepare and measure test

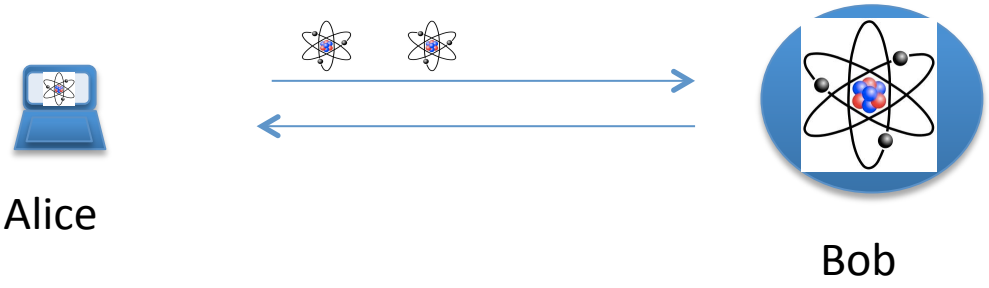
- A classical Alice, two non-communicating Bobs
[Reichardt, Unger, Vazirani '13]



Blind Bell test

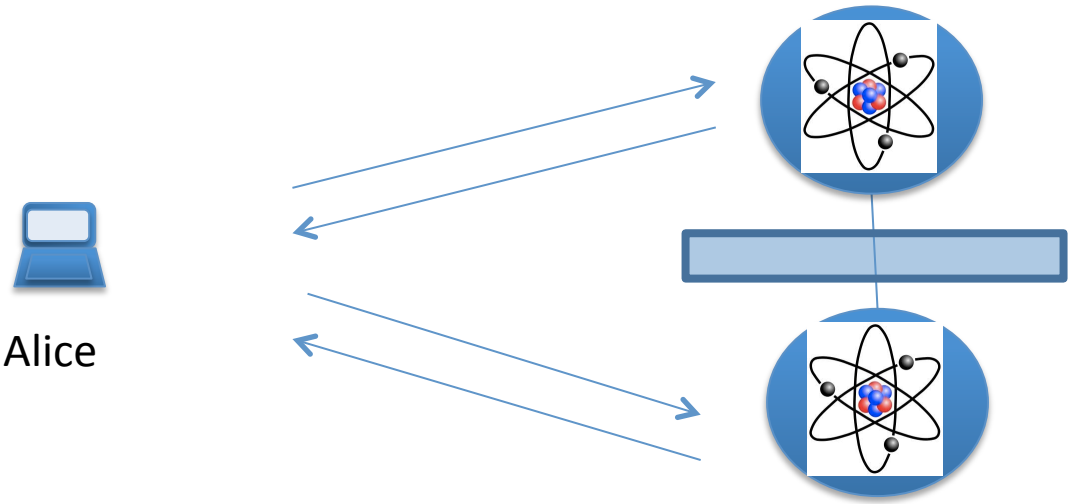
Verified Universal Quantum Computation

- A weakly quantum Alice [Fitzsimons Kashefi'12]



Blind prepare and measure test

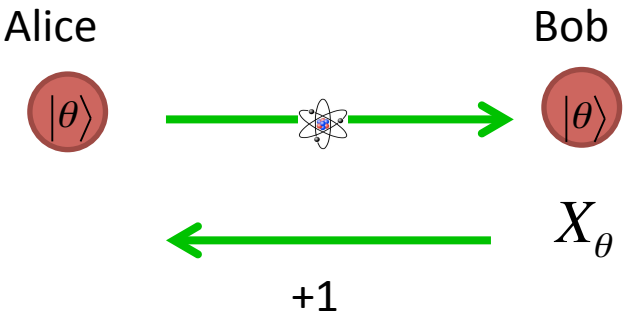
- A classical Alice, two non-communicating Bobs
[Reichardt, Unger, Vazirani '13]



Blind Bell test

Verified Universal Quantum Computation

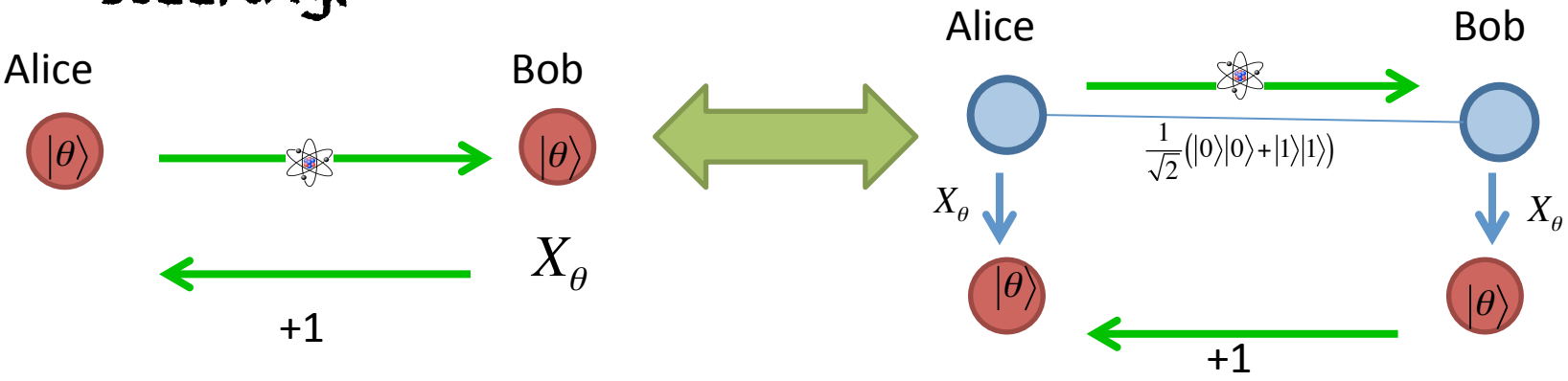
- FK hidden prepare and measure test is effectively steering.



- Alice prepares and sends a state $|\theta\rangle := \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$
- Asks Bob to measure it in X_θ
- Checks result!
  -> since blind, Bob doesn't know , can't cheat.

Verified Universal Quantum Computation

- FK hidden prepare and measure test is effectively steering.

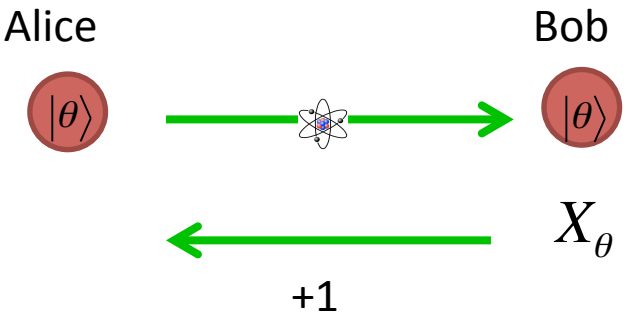


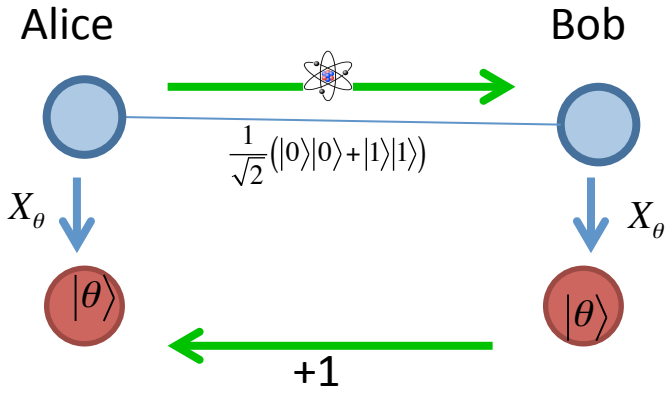
- Alice prepares and sends a state $|\theta\rangle := \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$
- Asks Bob to measure it in X_θ
- Checks result!
  -> since Blind, Bob doesn't know , can't cheat.

- Alice sends half an ME state
- Alice measures in X_θ and aks Bob to measure in X_θ
- Checks result match!

Verified Universal Quantum Computation

- FK hidden prepare and measure test is effectively steering.





- Alice prepares and sends a state $|\theta\rangle := \frac{|0\rangle + e^{i\theta}|1\rangle}{\sqrt{2}}$
- Asks Bob to measure it in X_θ
- Checks result!
  -> since blind, Bob doesn't know , can't cheat.

- Alice sends half an ME state
- Alice measures in X_θ and aks Bob to measure in X_θ
- Checks result match!

⇨ **Steering!** [Gheorghiu et al '15]

Verified Universal 'Toy' Computation...

Spekkens' Toy model [Spekkens '04]

- A totally 'classical' theory
  - explicit local hidden variables
  - access to them is limited
- Mimics many features of quantum mechanics
  - incompatible measurements
  - entanglement
  - steering
  - teleportation
  - QKD
- Has a 'stabiliser' like picture [Pusey '12]

We further show

[Disilvestro, M, arxiv1608.09012 '16]

Using stabiliser techniques

- Error correction and secret sharing
- No bit commitment
- Verified blind computation possible

Where to next

- 'spectrum' of toy theories: all based on limited access to information
  - Includes Gaussian Optics! [Bartlett et al '11]

- The efficiency game...
  - minimise 'amount' and 'type' of resources
  - genearlised resource theory

- Keep on going!
  Trust, security and quantumness...
  - verification of entanglement and other features
  - delegation of general quantum tasks:
    -> sensing
    -> simulation
    -> ...