A semi-device-independent framework based on natural physical assumptions
and its application to random number generation

T. Van Himbeeck, E. Woodhead, N. Cerf, R. García-Patrón, S. Pironio

arXiv:1612.06828

AQIS 2017 – 4-8 September 2017

There exist vulnerabilities in quantum cryptography, successfully exploited by quantum hackers

Scholar

About 359 results (**0.06** sec)

Articles
Case law
My library

Any time
Since 2017
Since 2016
Since 2013
Custom range...

Sort by relevance
Sort by date

include patents
include citations

Create alert

Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems
Y Zhao, CHF Fung, B Qi, C Chen, HK Lo - Physical Review A, 2008 - APS
Abstract Quantum-key-distribution (QKD) systems can send quantum signals over more than 100 km standard optical fiber and are widely believed to be secure. Here, we show experimentally a technologically feasible attack—namely, the time-shift attack—against a
Cited by 384 Related articles All 9 versions Cite Save

Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack
JZ Huang, C Weedbrook, ZQ Yin, S Wang, HW Li... - Physical Review A, 2013 - APS
Abstract The security proofs of continuous-variable quantum key distribution are based on the assumptions that the eavesdropper can neither act on the local oscillator nor control Bob's beam splitter. These assumptions may be invalid in practice due to potential
Cited by 47 Related articles All 8 versions Cite Save

Hacking commercial quantum cryptography systems by tailored bright illumination
L Lydersen, C Wiechers, C Wittmann, D Elser... - Nature ..., 2010 - nature.com
... For example, RSA public key cryptography has been subject to extensive scrutiny, which has led to the discovery of effective attacks based on implementation loopholes 25 . In our view, **quantum hacking** is an indication of the mature state of QKD rather than its insecurity. ...
Cited by 558 Related articles All 21 versions Cite Save

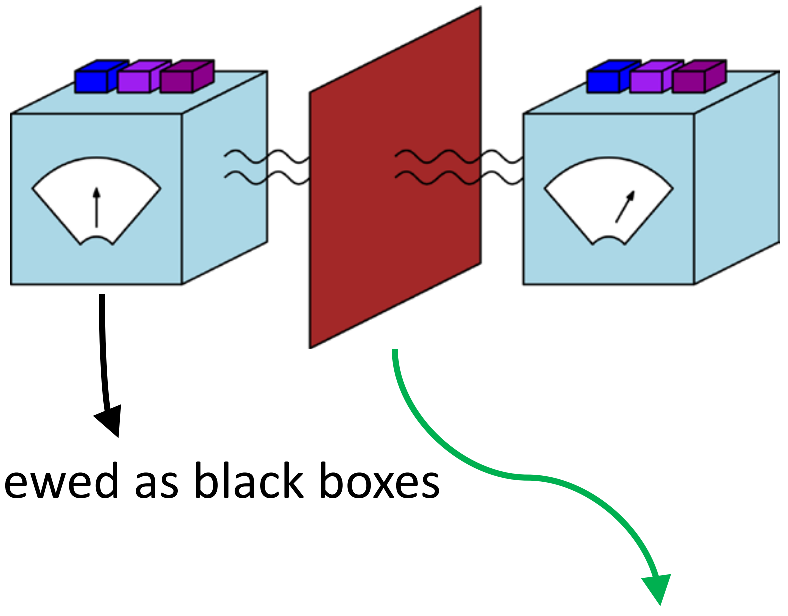
Quantum hacking on quantum key distribution using homodyne detection
JZ Huang, S Kunz-Jacques, P Jouguet, C Weedbrook... - Physical Review A, 2014 - APS
Abstract Imperfect devices in commercial quantum key distribution systems open security loopholes that an eavesdropper may exploit. An example of one such imperfection is the wavelength-dependent coupling ratio of the fiber beam splitter. Utilizing this loophole, the
Cited by 21 Related articles All 5 versions Cite Save

Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors
H Weier, H Krauss, M Rau, M Fürst... - New Journal of ..., 2011 - iopscience.iop.org
Cited by 96 Related articles All 9 versions Cite Save

[HTML] Optimised **quantum hacking** of superconducting nanowire single-photon detectors
MG Tanner, V Makarov, RH Hadfield - Optics express, 2014 - osapublishing.org
We explore bright-light control of superconducting nanowire single-photon detectors (SNSPDs) in the shunted configuration (a practical measure to avoid latching). In an

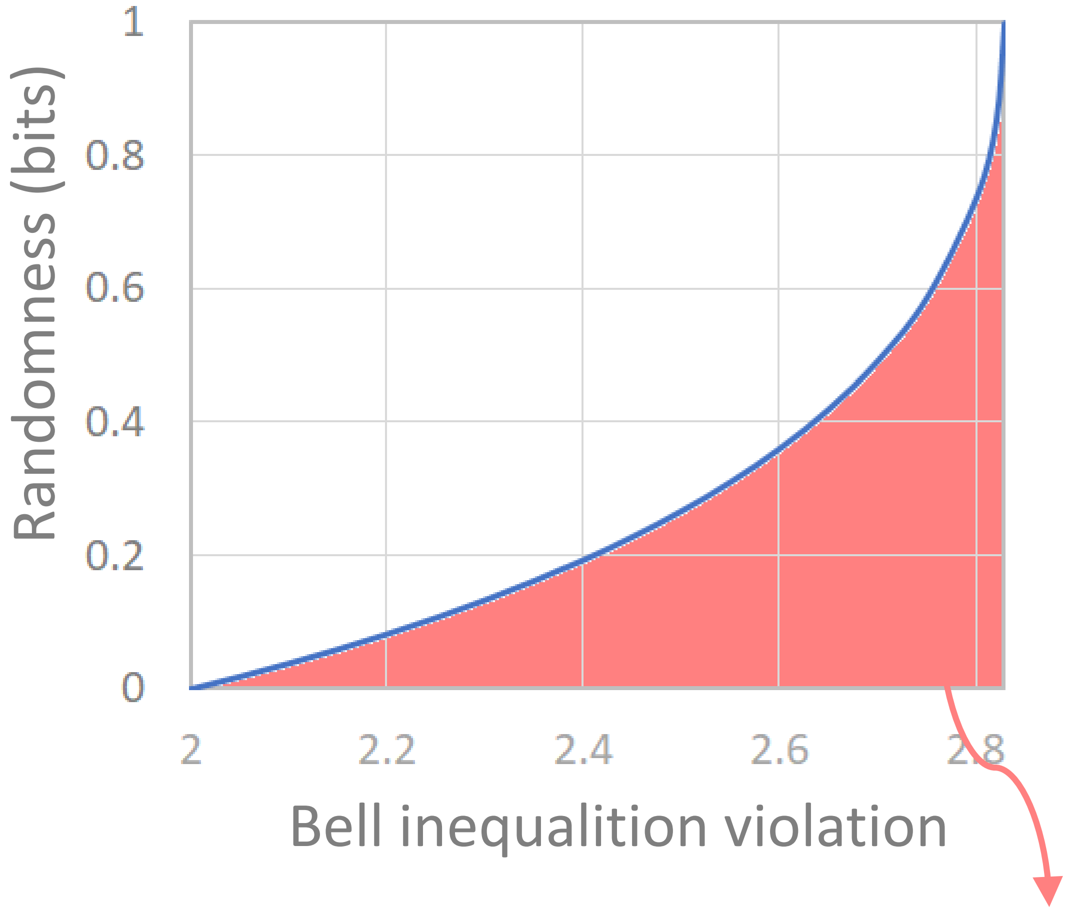
These attacks exploit a mismatch between the theoretical model used to prove security and the actual implementation

Device-independent quantum cryptography



Devices viewed as black boxes

A single natural physical assumption



Region not allowed by quantum theory if devices do not communicate

This approach can be used to certify the security of RNG and QKD protocols, or even the performance of quantum computers.

Usual, “device-dependent” quantum cryptography

Based on a detailed characterization of the devices

Semi-device-independent quantum cryptography

Based on a few assumpions. Devices are partly untrusted.

E.g.:

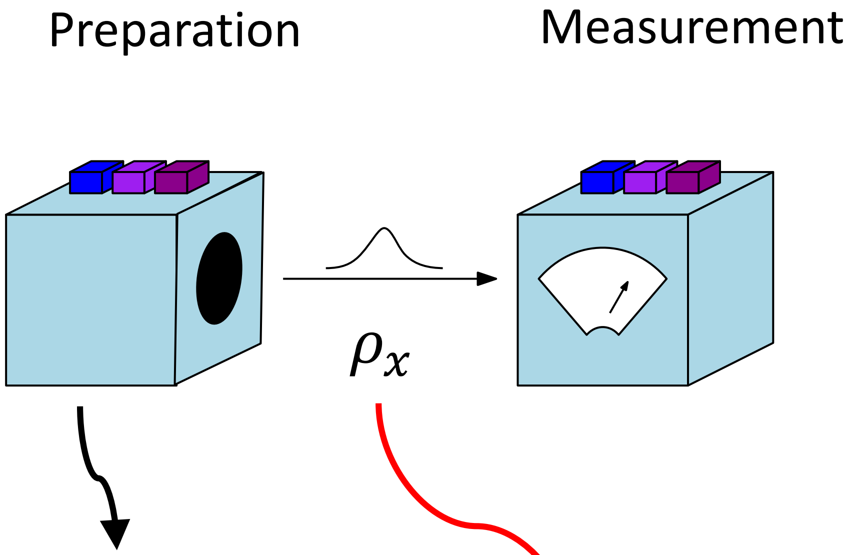
- Measurement-device-independence
- One-sided quantum cryptography
- Source-independent QRNG
- Qubit assumption
- Source & measurement independence
- …

Advantage: higher rate, easier to implement than fully device-independent protocols

Fully “device-independent” quantum cryptography

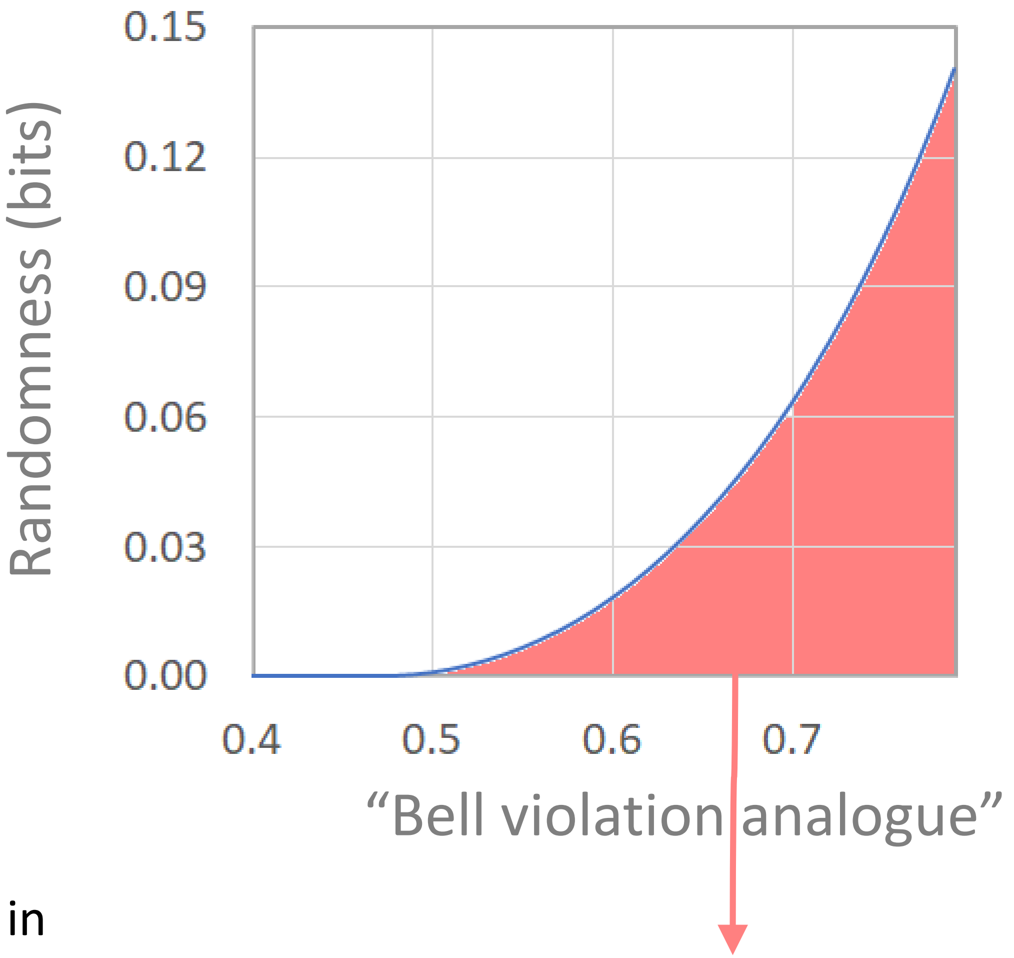
Based on minimal assumptions. Devices can be untrusted.

Semi-device-independent protocols based on an energy constraint



Devices viewed as black boxes…

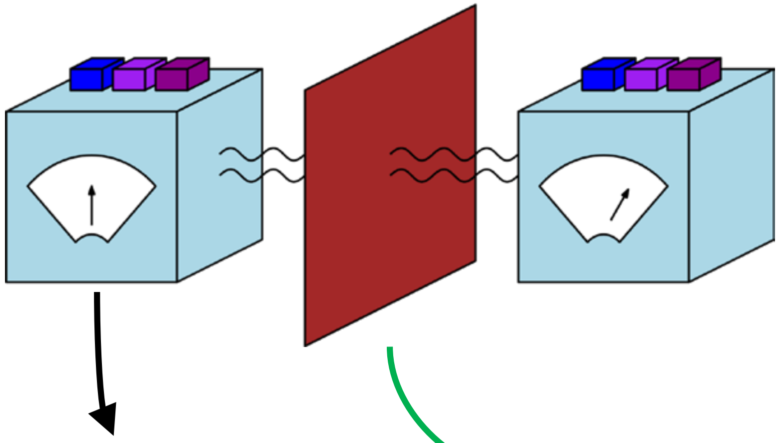
… except for a single assumption:
ρ_x are optical signals close to the vacuum:
$\langle 0|\rho_x|0\rangle \geq \omega$



Region not allowed by quantum theory
if prepared states satisfy the energy constraint

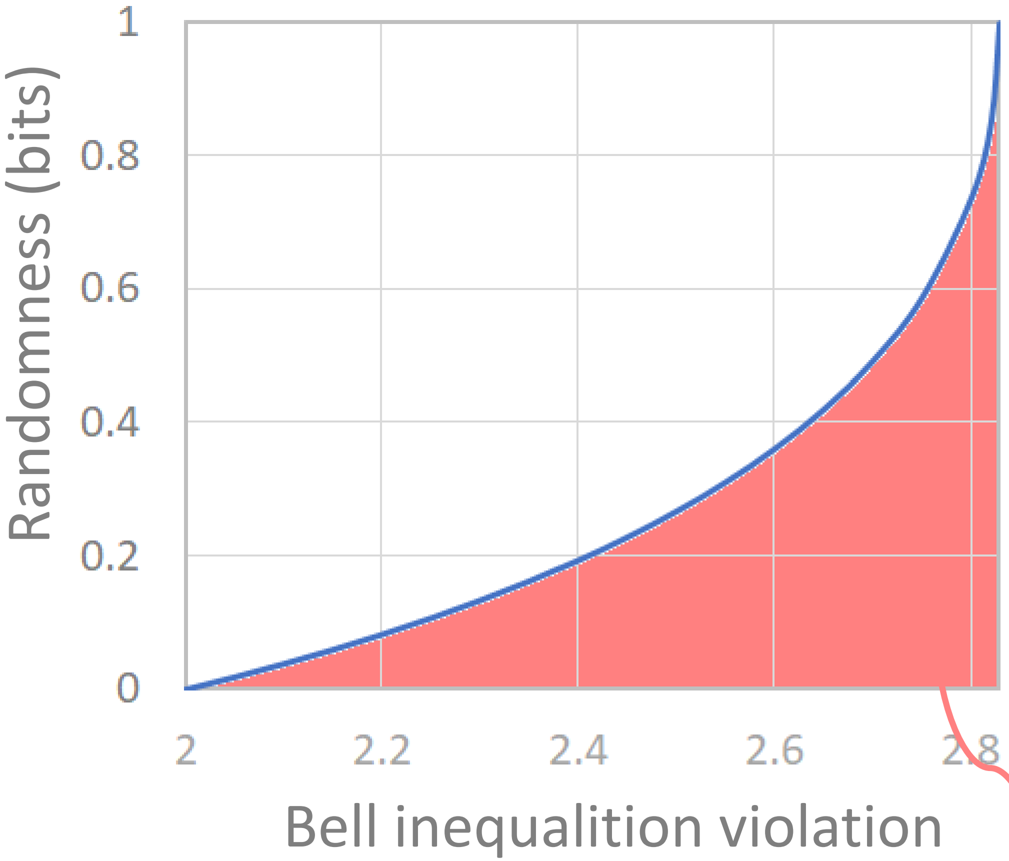
This assumption is sufficient to guarantee that devices behave in a genuinely quantum way.
In particular, it allows for secure RNG protocols.
Hopefully, it can also be used for QKD

Device-independent quantum cryptography



Devices viewed as black boxes

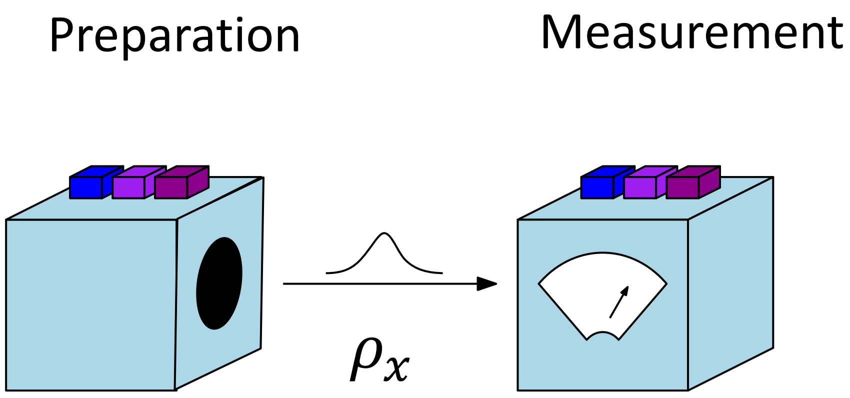
A single natural physical assumption



Region not allowed by quantum theory if devices do not communicate

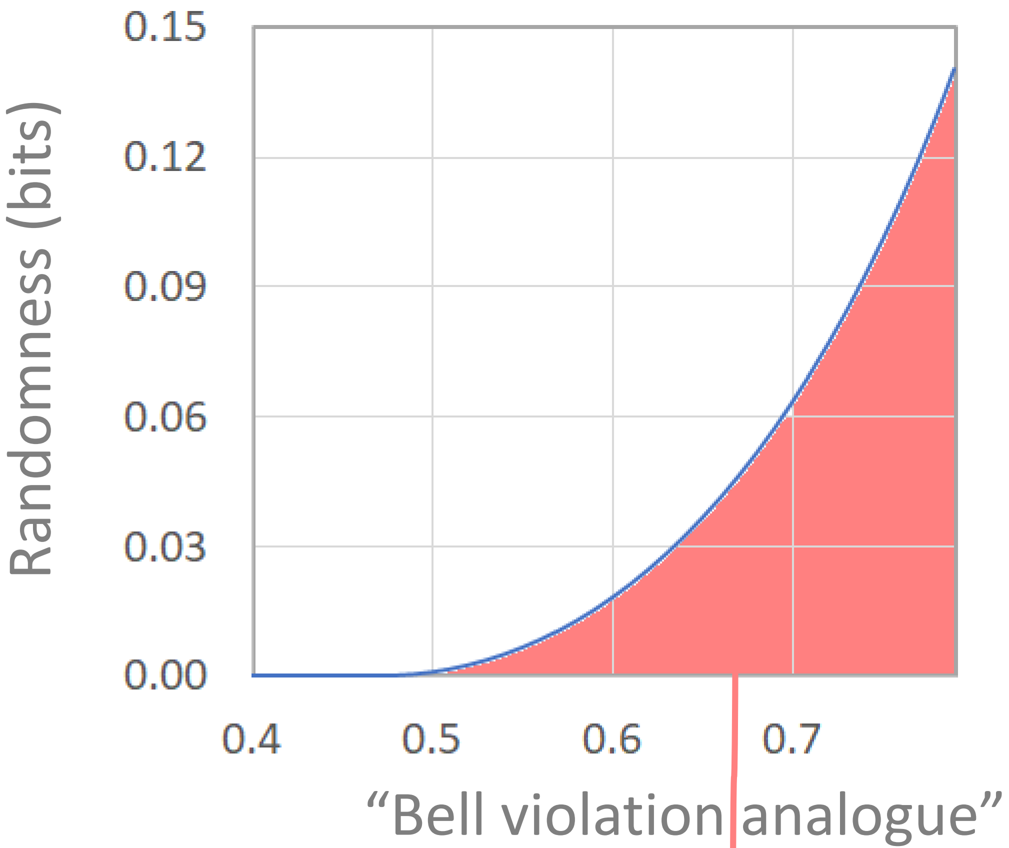
This approach can be used to certify the security of RNG and QKD protocols, or even the performance of quantum computers.

Semi-device-independent protocols based on an energy constraint



Devices viewed as black boxes…

… except for a single assumption:
ρ_x are optical signals close to the vacuum:
$\langle 0|\rho_x|0\rangle \geq \omega$



Region not allowed by quantum theory
if prepared states satisfy the energy constraint

This assumption is sufficient to guarantee that devices behave in a genuinely quantum way.
In particular, it allows for secure RNG protocols.
Hopefully, it can also be used for QKD

Usual, “device-dependent” quantum cryptography

Based on a detailed characterization of the devices

Semi-device-independent quantum cryptography

Based on a few assumpions. Devices are partly untrusted.

E.g.:

- Measurement-device-independence
- One-sided quantum cryptography
- Qubit assumption
- Source & measurement independence
- …
- Energy constraint

Fully “device-independent” quantum cryptography

Based on minimal assumptions. Devices can be untrusted.

Outline

- Why semi-device-independent quantum cryptography?
- Motivation for our energy constraint assumption
- Results

Outline

- Why semi-device-independent quantum cryptography?
- Motivation for our energy constraint assumption
- Results

Even full DI requires non-trivial assumptions

Usual, “device-dependent” quantum cryptography

Semi-device-independent quantum cryptography

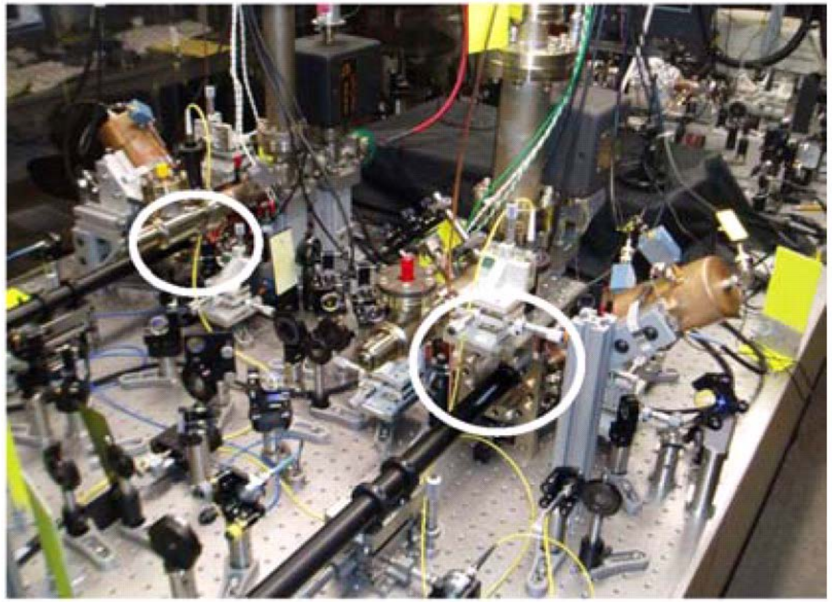
Fully “device-independent” quantum cryptography

- Laser power is limited

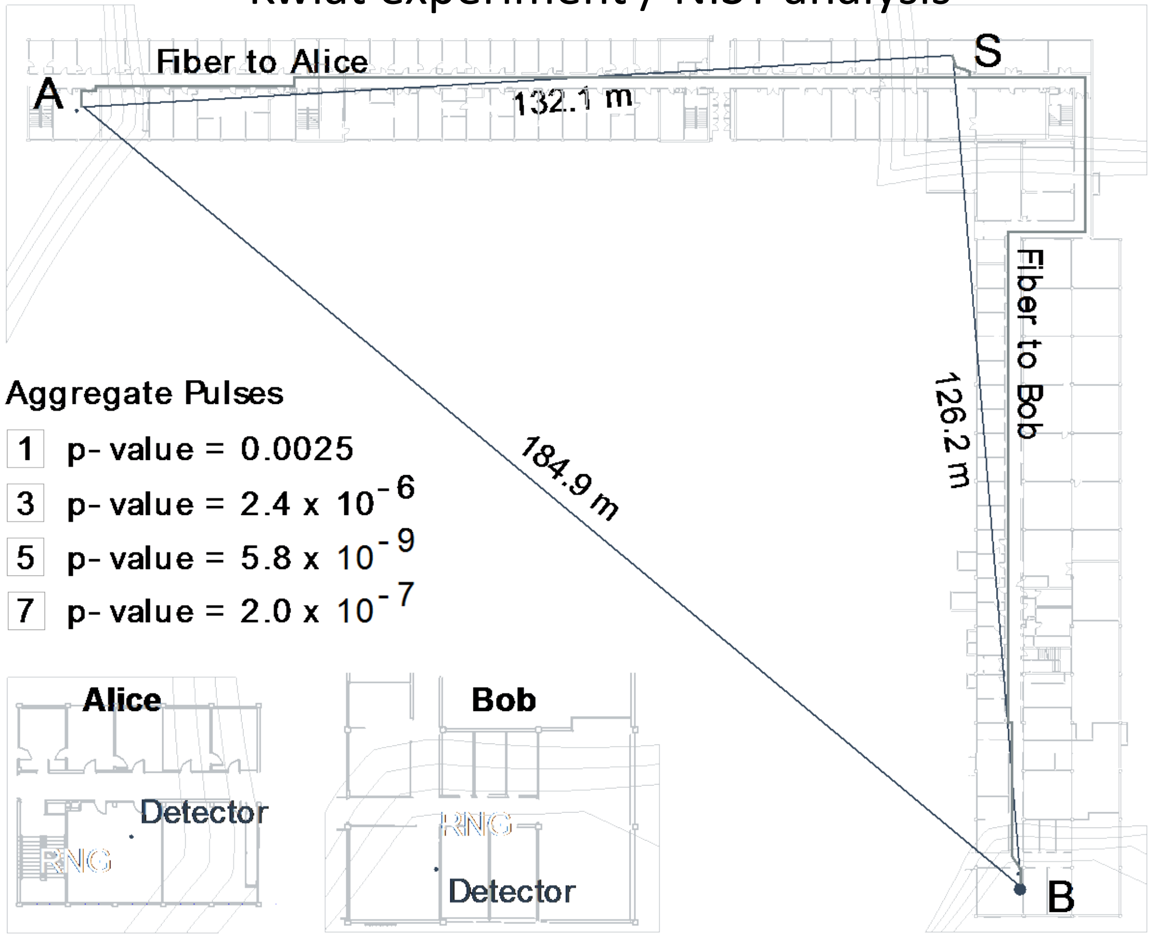
- Electronics and classical computers are trusted
- No information leakage
- GPS are accurate
- …

DI RNG implementations

Monroe experiment

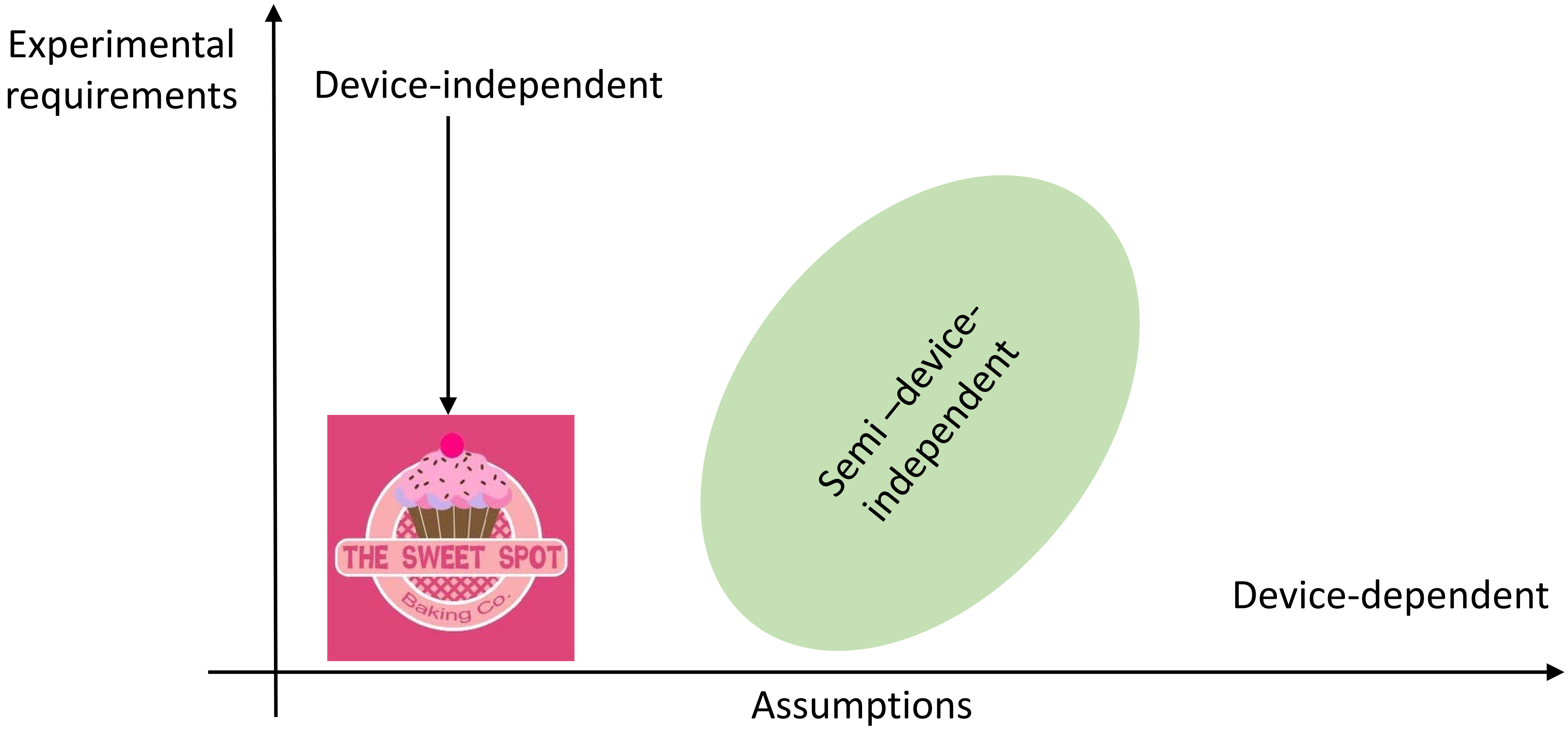


Kwiat experiment / NIST analysis

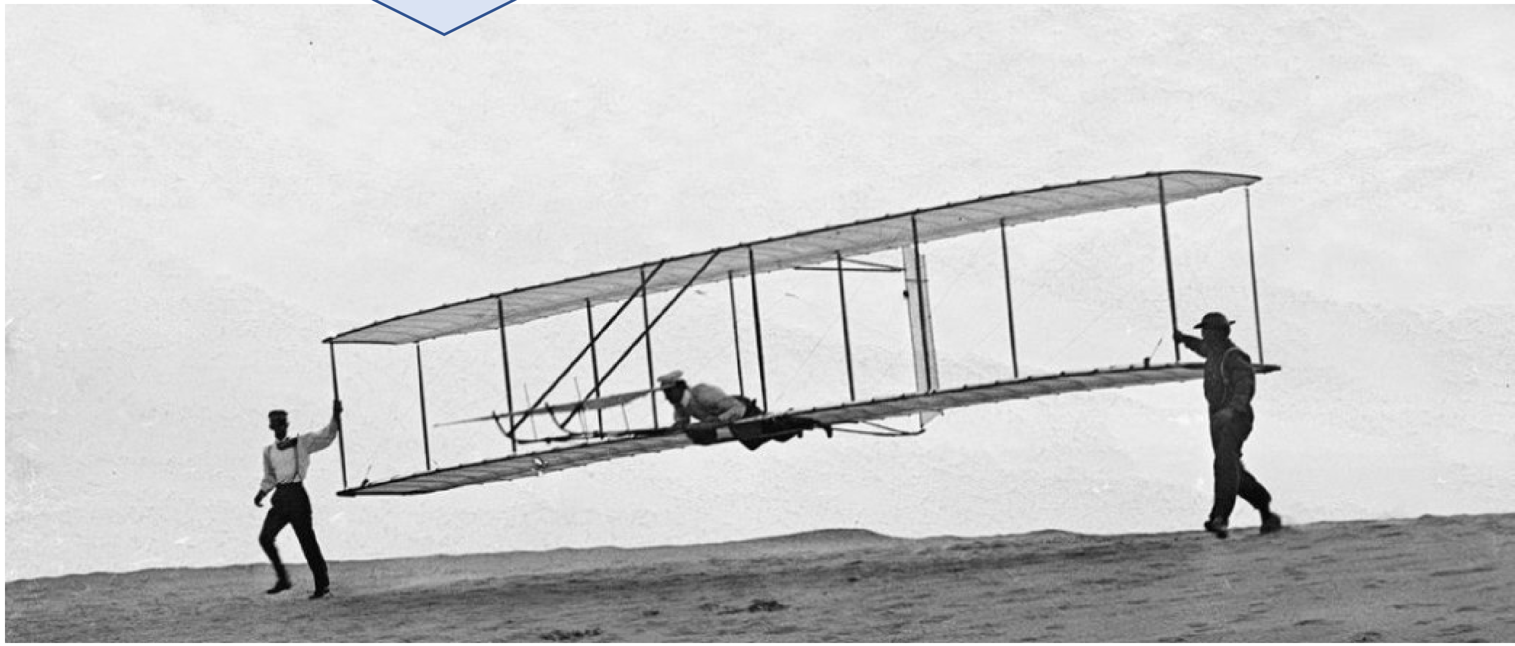


we extracted 256 bits, certified to be uniform to within 0.001.

in [18], which is titled "XOR 3" and consists of a total of 182, 161, 215 trials, acquired in 30 min of running the experiment, improving on the approximately one month duration of data

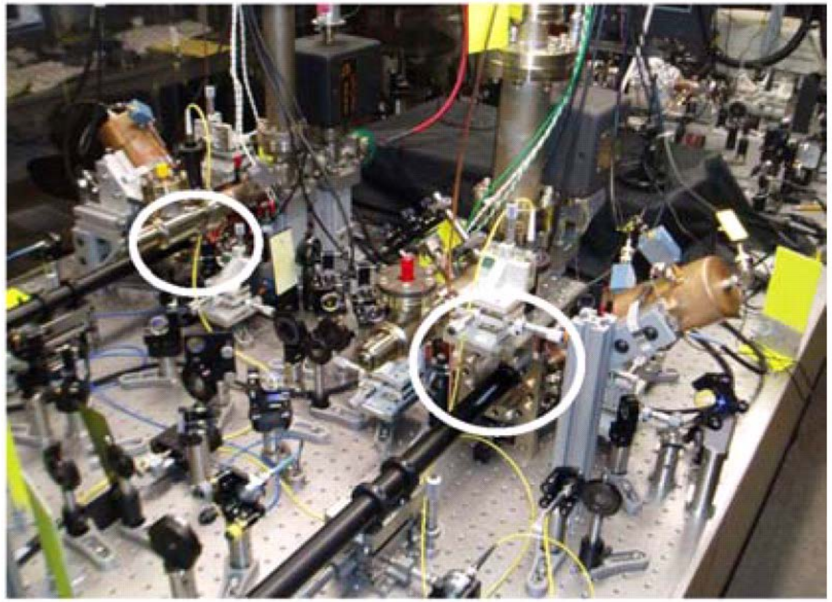

Experimental requirements
Device-independent
THE SWEET SPOT
Baking Co.
Semi –device-independent
Device-dependent
Assumptions

Don’t waste time developing cars: in the future planes will be easy to build, common, and affordable.

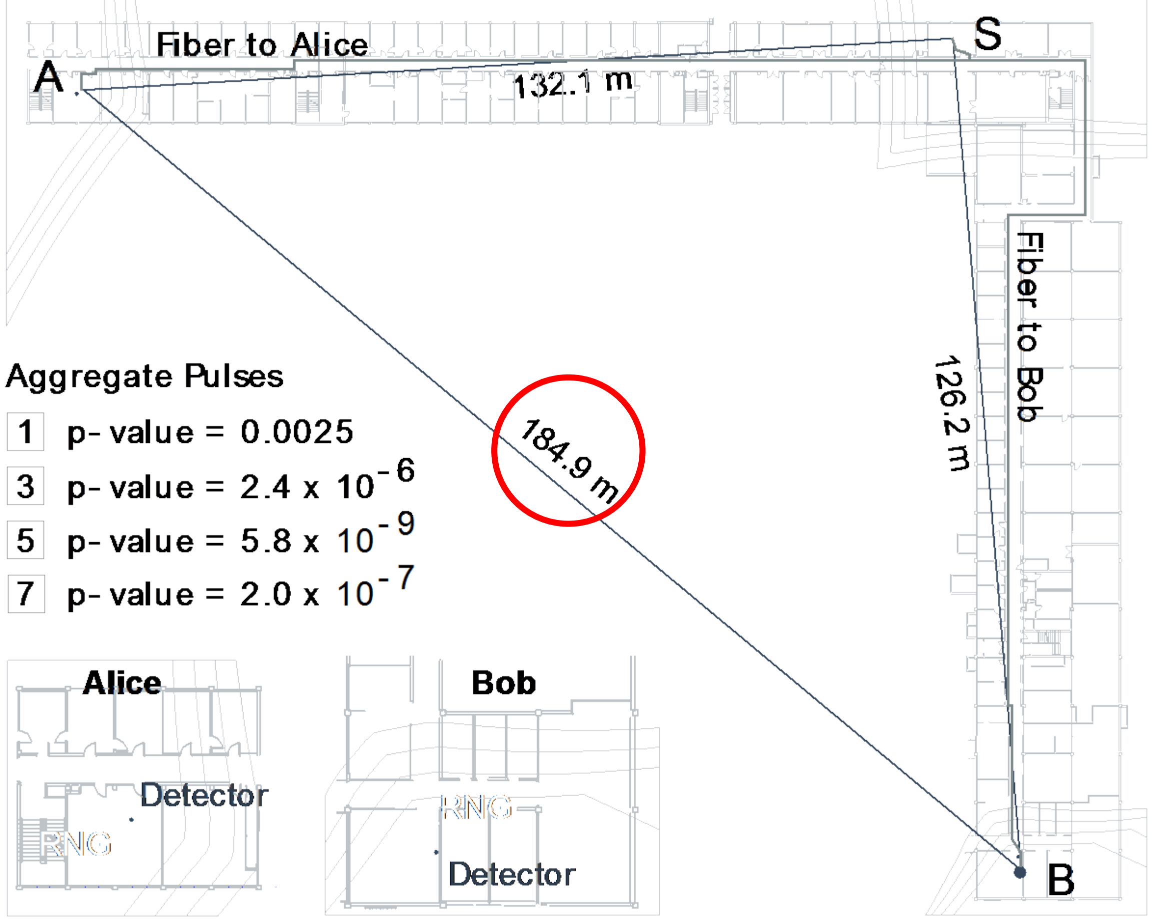


DI RNG implementations

Monroe experiment



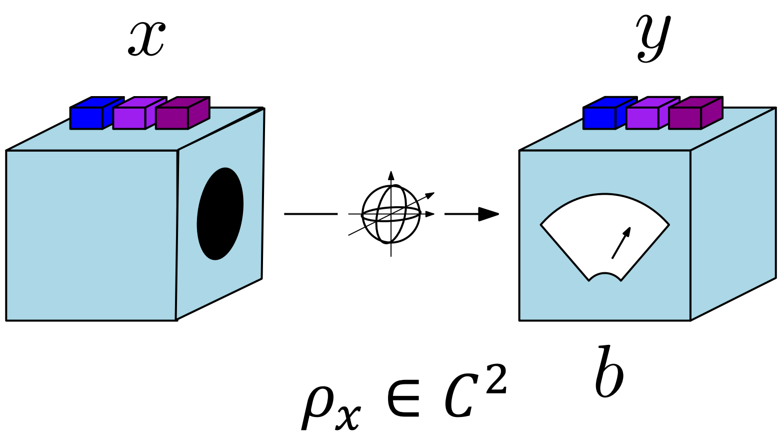
Kwiat experiment / NIST analysis



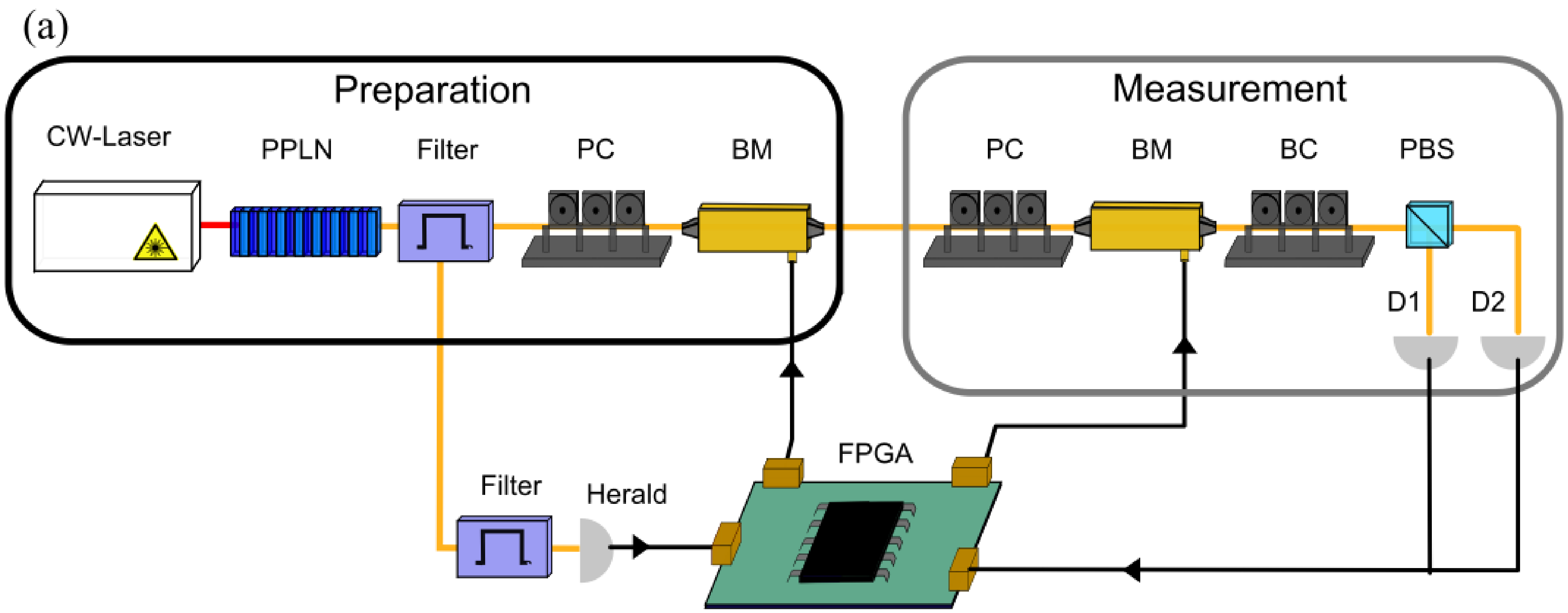
we extracted 256 bits, certified to be uniform to within 0.001.

in [18], which is titled "XOR 3" and consists of a total of 182, 161, 215 trials, acquired in 30 min of running the experiment, improving on the approximately one month duration of data

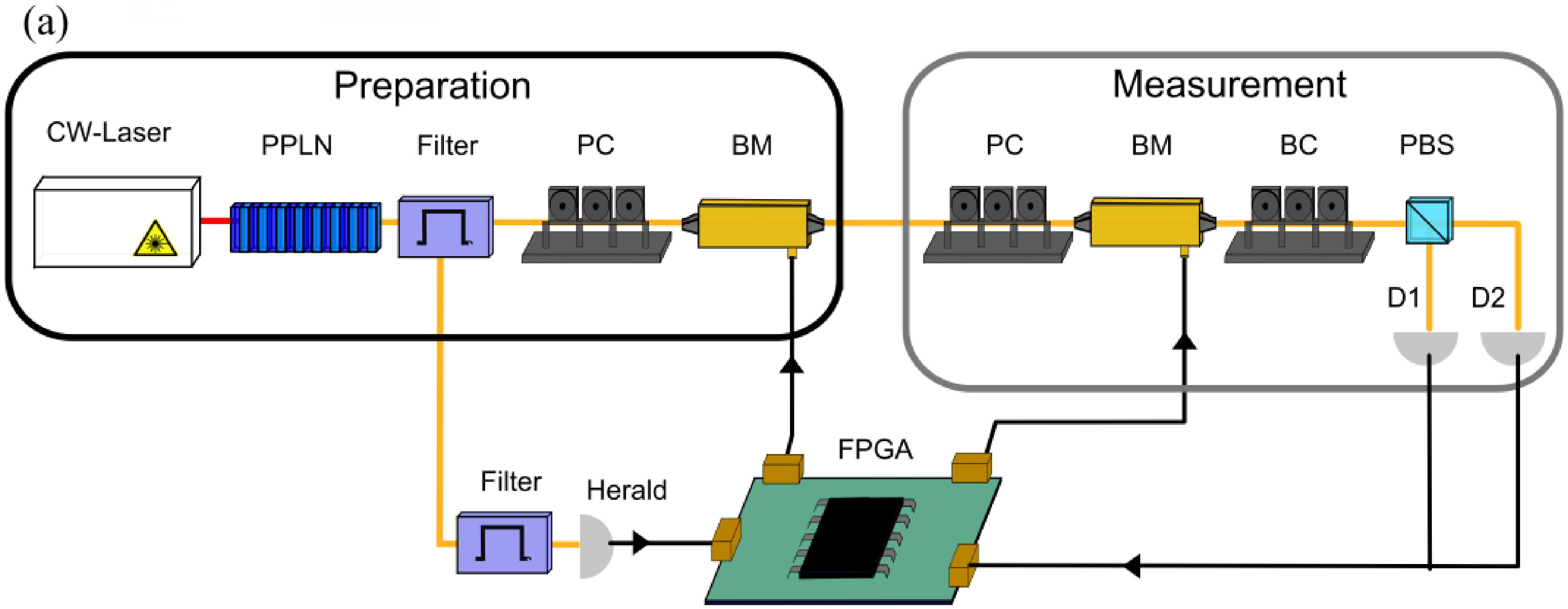
Semi-DI protocols based on a qubit assumption



Semi-DI protocols based on a qubit assumption



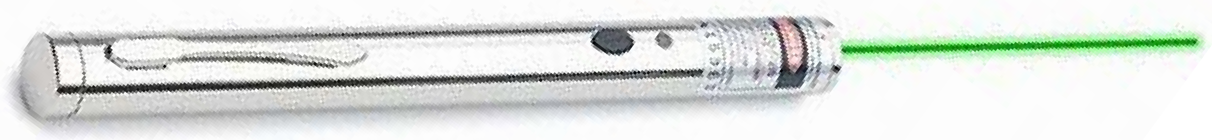
Mismatch between model used for security proof and implementation!



Qubit assumption is an idealization.

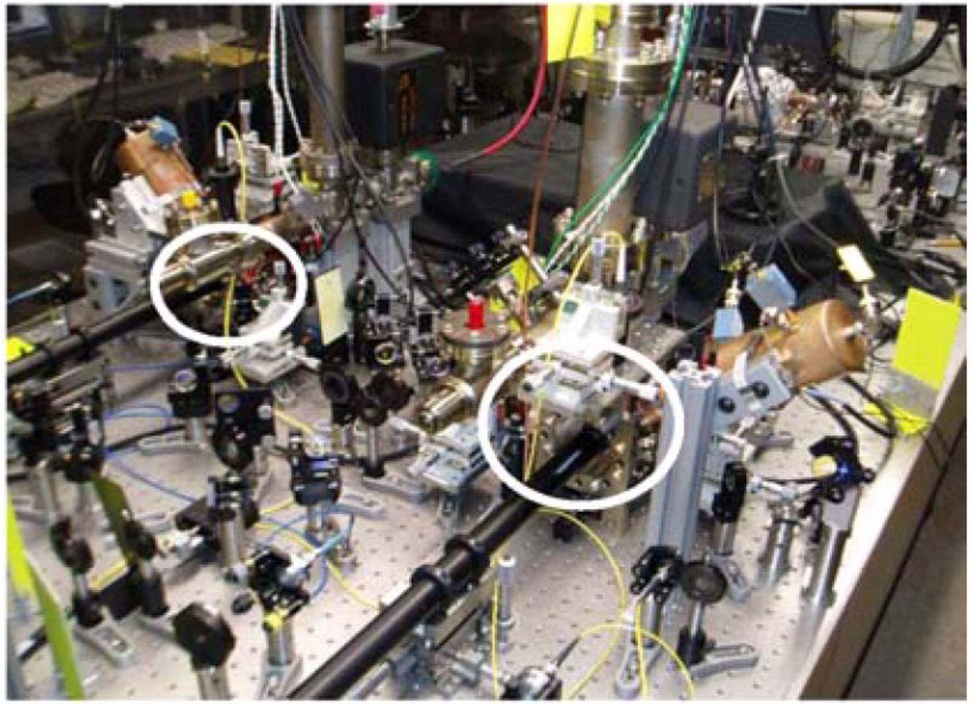
→ Shows that it is important to choose well the assumptions.

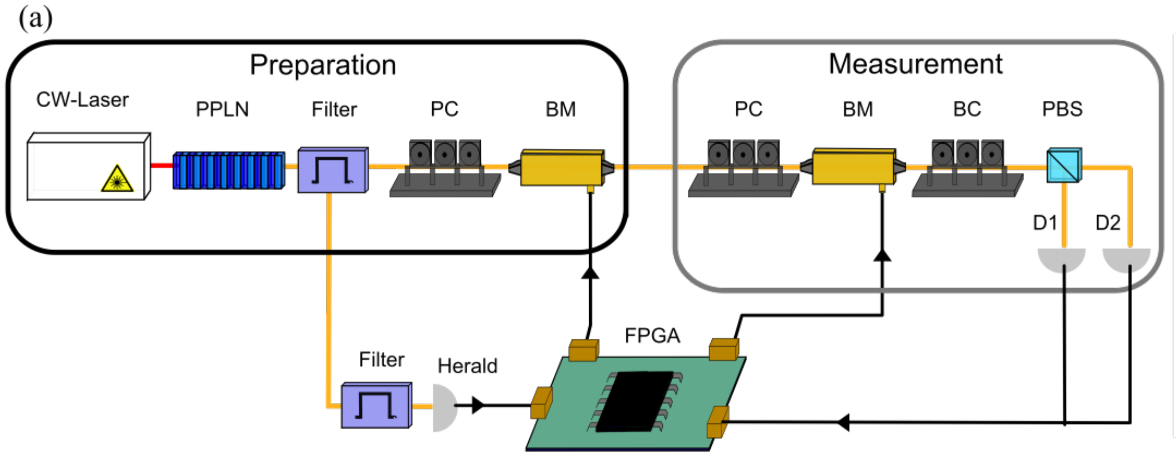

MPD
PDM series



$$\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle + \cdots$$

Click with prob $1 - \alpha^2$
No-click with prob α^2

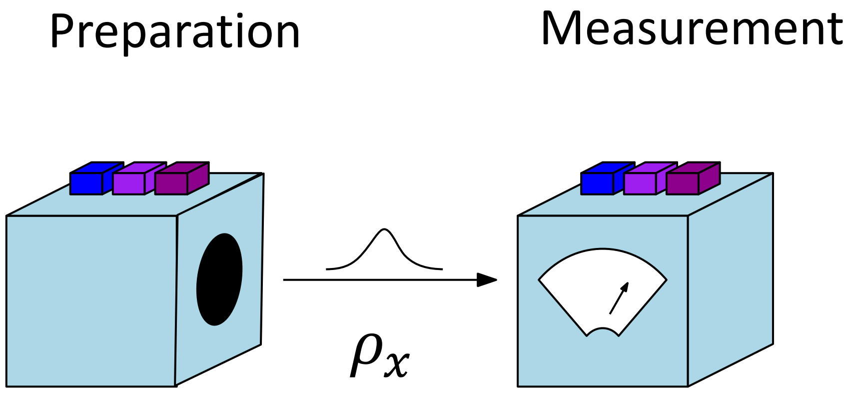



(a)
Preparation
CW-Laser
PPLN
Filter
PC
BM
Measurement
PC
BM
BC
PBS
D1
D2
FPGA
Filter
Herald

Outline

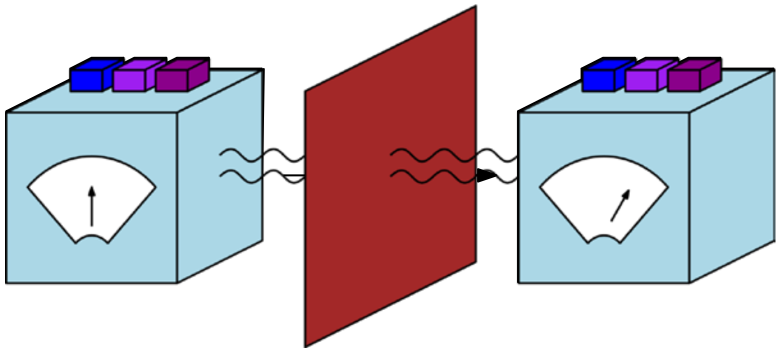
- Why semi-device-independent quantum cryptography?
- Motivation for our energy constraint assumption
- Results

Semi-device-independent protocols based on an energy constraint



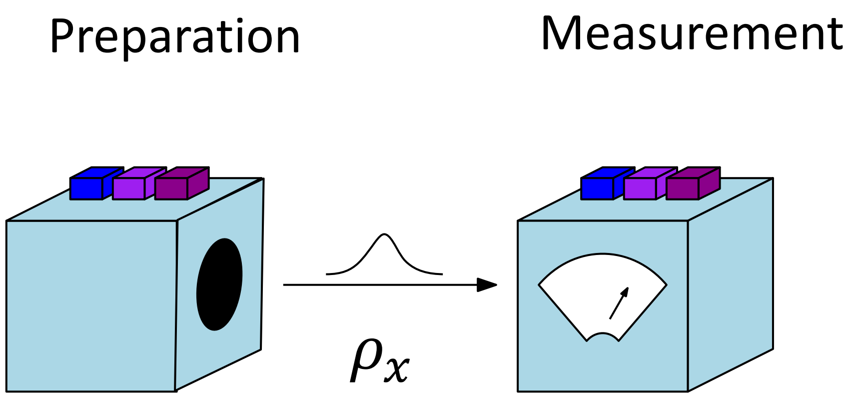
Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

Semi-device-independent protocols based on an energy constraint



Assumption: no-communication
$\leftrightarrow \langle 0|\rho_x|0\rangle = 1$

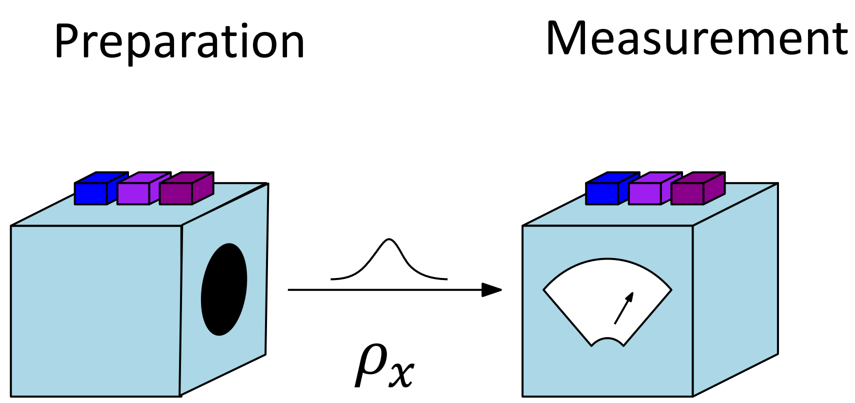
Semi-device-independent protocols based on an energy constraint



Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols

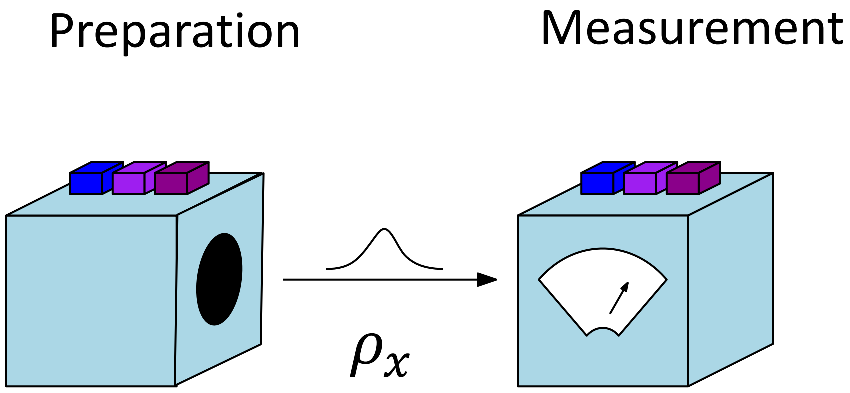
Semi-device-independent protocols based on an energy constraint



Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

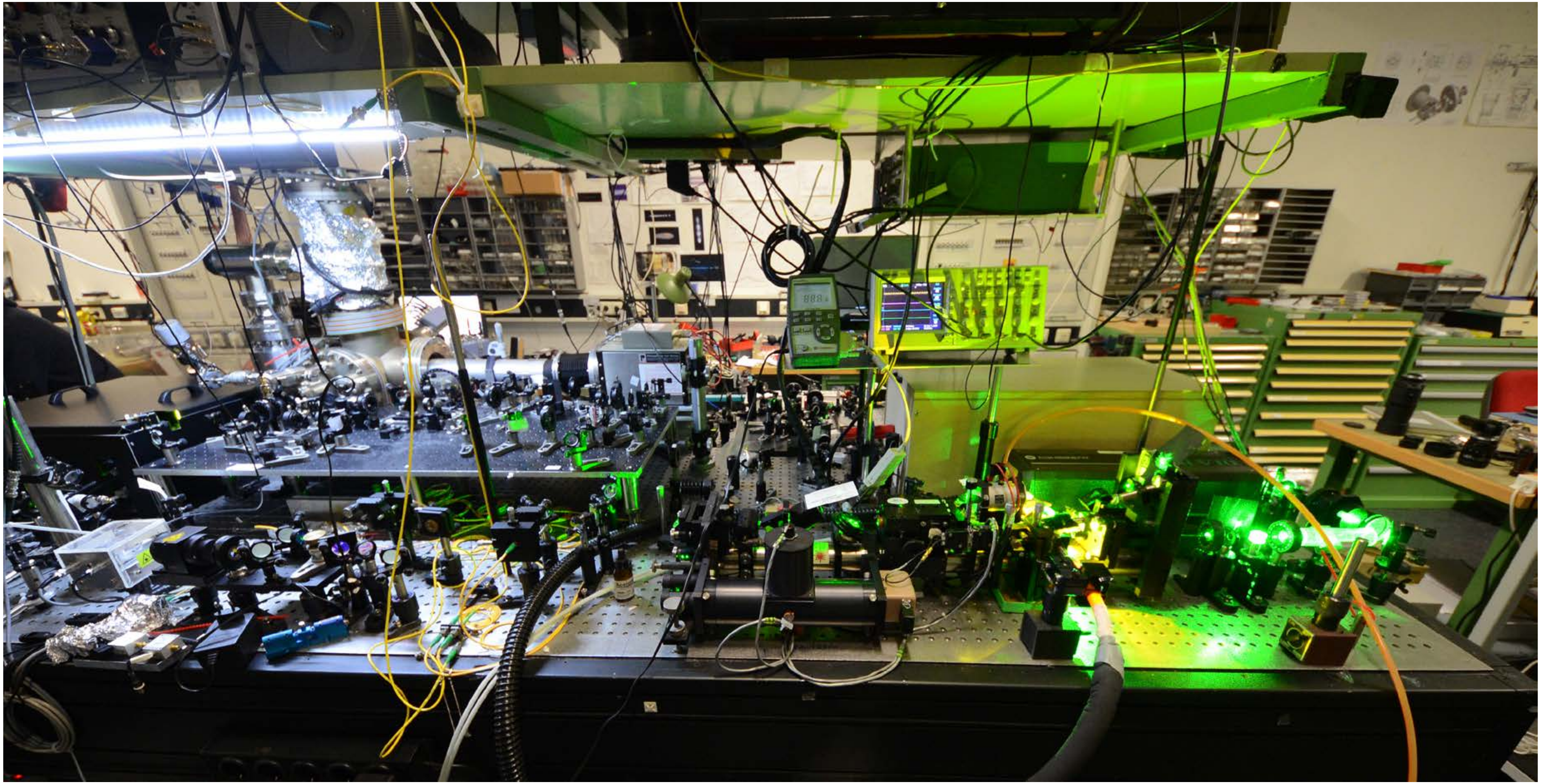
- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.

Semi-device-independent protocols based on an energy constraint

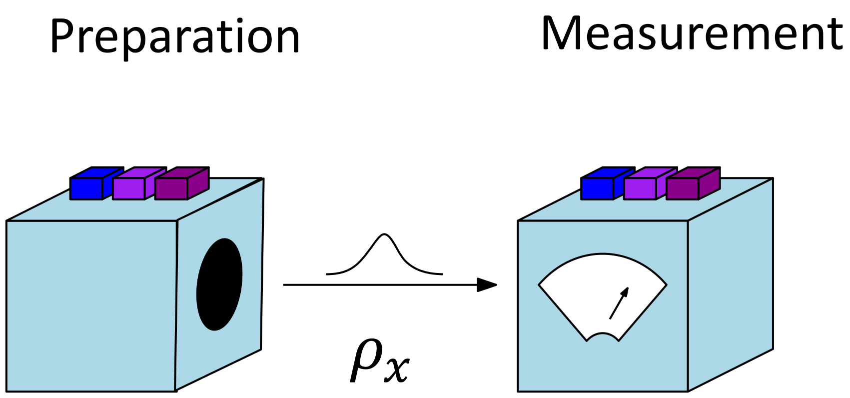


Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.



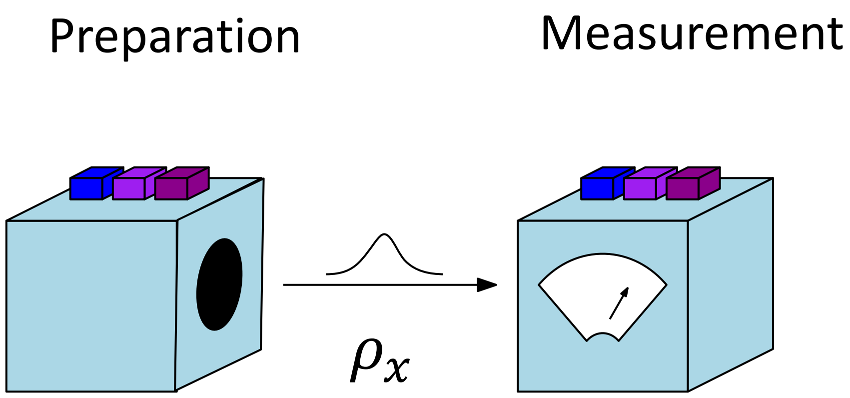
Semi-device-independent protocols based on an energy constraint



Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.

Semi-device-independent protocols based on an energy constraint



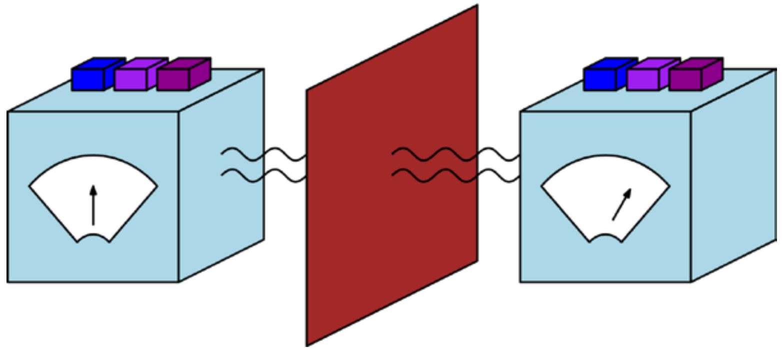
Assumption: $\langle 0|\rho_x|0\rangle \geq \omega_x$

- Natural relaxation of the no-communication assumption of full DI protocols
- The appropriate space to describe quantum optics experiments is the Fock space of several quantum optical modes. In this context, it is natural to bound the average number of photons.
- This is an assumption anyway made in many quantum optics experiments in which attenuated laser sources are used.
- It is directly related to simple characteristics of the device components (laser power, attenuator) and robust to device imperfections.
- It could be directly monitored (calibrated power meter) or enforced (optical fuse).

Outline

- Why semi-device-independent quantum cryptography?
- Motivation for our energy constraint assumption
- Results

No-communication assumption

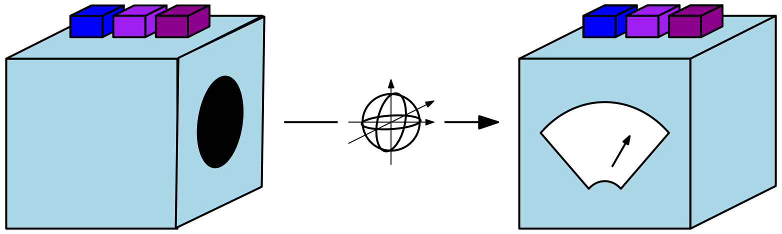


↓

Violation of Bell inequalities

$Q > C$

Qubit assumption

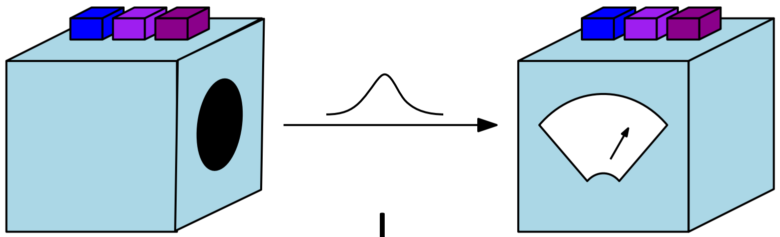


↓

Violation of “dimension witnesses”

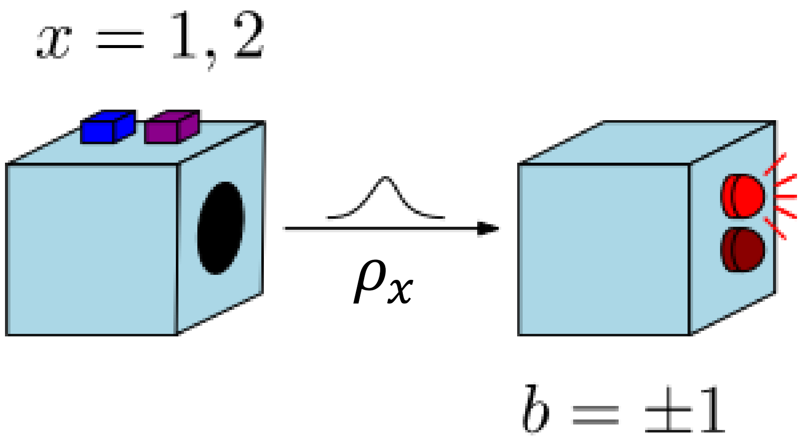
$Q > C$

Energy constraint assumption



↓

$Q > C$??



Input-output statistics

$P(b|x) = Tr[\rho_x M_b]$ or $P(b|x) = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M_b^\lambda]$

Equivalent to knowledge of the bias of b given x:

$E_x = P(b = 1|x) - P(b = -1|x)$

$E_x = Tr[\rho_x M]$ or $E_x = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M^\lambda]$

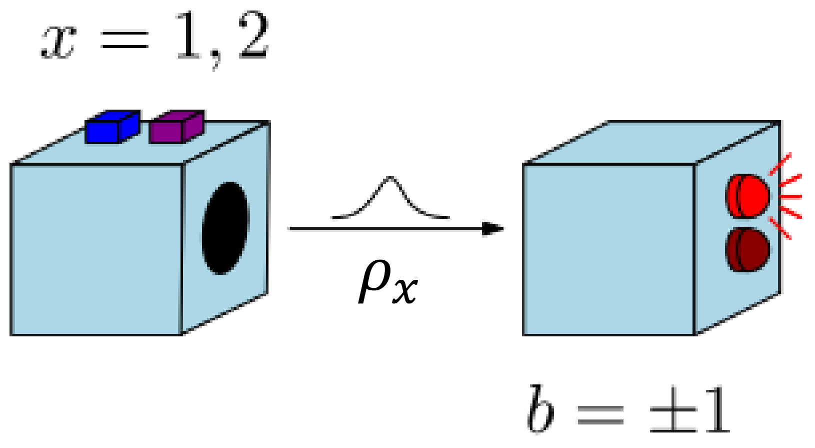
Output of devices is non-trivial if b is correlated to x

Amount of correlations can be measured by quantity

$$E_- = (E_1 - E_2)/2$$

Probability to guess correctly x given b is $\frac{1}{2} + \frac{|E_-|}{2}$

- b does not depend on x: $E_- = 0$
- b fully correlated to x: $|E_-| = 1$



Input-output statistics

$P(b|x) = Tr[\rho_x M_b]$ or $P(b|x) = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M_b^\lambda]$

Equivalent to knowledge of the bias of b given x:

$E_x = P(b = 1|x) - P(b = -1|x)$

$E_x = Tr[\rho_x M]$ or $E_x = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M^\lambda]$

Output of devices is non-trivial if b is correlated to x

Amount of correlations can be measured by quantity

$$E_- = (E_1 - E_2)/2$$

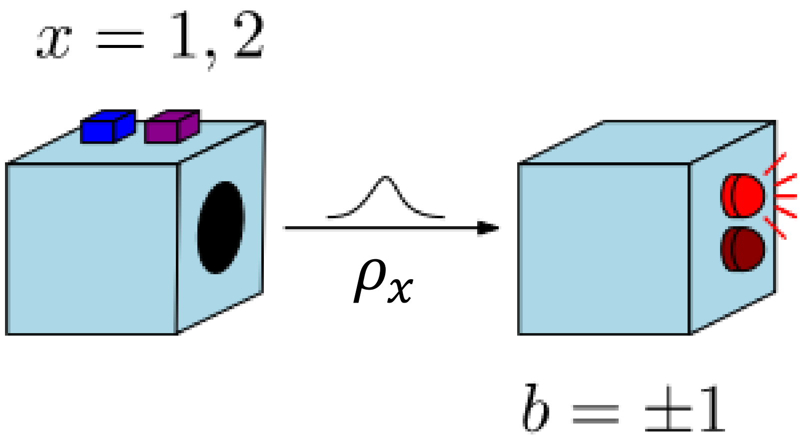
Probability to guess correctly x given b is $\frac{1}{2} + \frac{|E_-|}{2}$

- b does not depend on x: $E_- = 0$
- b fully correlated to x: $|E_-| = 1$

Assumption

Energy constraint:

$\langle 0| \sum_\lambda p_\lambda \rho_x^\lambda |0\rangle \geq w_x$



<u>Input-output statistics</u>

$P(b|x) = Tr[\rho_x M_b]$ or $P(b|x) = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M_b^\lambda]$

Equivalent to knowledge of the bias of b given x:

$E_x = P(b = 1|x) - P(b = -1|x)$

$E_x = Tr[\rho_x M]$ or $E_x = \sum_\lambda p_\lambda Tr[\rho_x^\lambda M^\lambda]$

Output of devices is non-trivial if b is correlated to x

Amount of correlations can be measured by quantity

$$E_- = (E_1 - E_2)/2$$

Probability to guess correctly x given b is $\frac{1}{2} + \frac{|E_-|}{2}$

- b does not depend on x: $E_- = 0$
- b fully correlated to x: $|E_-| = 1$

<u>Assumption</u>

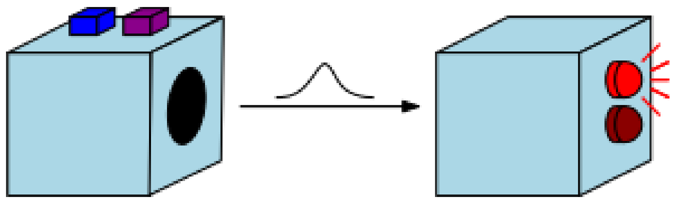
Energy constraint:

$\langle 0| \sum_\lambda p_\lambda \rho_x^\lambda |0\rangle \geq w_x$

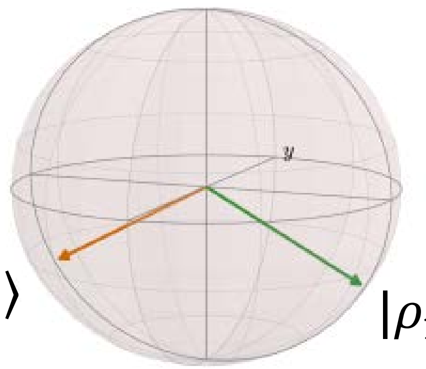
or

$$\sum_\lambda p_\lambda Tr[H\rho_x^\lambda] \leq 1 - w_x$$

Maximal value for E_- given $w_1 = w_2 = w$?



- $w = 1 \rightarrow E_- = (E_1 - E_2)/2 = 0$
- $w = 1/2 \rightarrow |\rho_{1,2}\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$
  $\rightarrow E_- = (E_1 - E_2)/2 = 1$
- $\frac{1}{2} \leq w \leq 1$ arbitrary
  $|\rho_1\rangle = \sqrt{w}|0\rangle + \sqrt{1-w}|\phi_1\rangle$
  $|\rho_2\rangle = \sqrt{w}|0\rangle + \sqrt{1-w}|\phi_2\rangle$



Scalar product minimal if $|\phi_1\rangle = -|\phi_2\rangle = |1\rangle$

$$\Rightarrow |\rho_{1,2}\rangle = \sqrt{w}|0\rangle \pm \sqrt{1-w}|1\rangle$$

Best distinguishing measurement: $M = \sigma_x$

→ We find the inequality $E_- = \frac{E_1 - E_2}{2} \leq 2\sqrt{w(1-w)}$

According to quantum strategies: $E_- = \frac{E_1 - E_2}{2} \leq 2\sqrt{w(1-w)} = \mathrm{Q}_{\max}$
Maximal value for "classical" strategies?

How to define "classical" strategies?
One possibility:

"classical" strategies = "deterministic" strategies (or convex combinations thereof)

$E_x = \sum_\lambda p_\lambda E_x^\lambda$ with $E_x^\lambda = \pm 1$

Let's be more conservative and compare $Q_{\max}$ to strategies where only E_1 is deterministic

$E_1 = \sum_\lambda p_\lambda E_1^\lambda$ with $E_1^\lambda = \pm 1$, no constraint on E_2

→ If $Q_{\max} > D_{\max}$ → the output of $x = 1$ is random (even to adversary with arbitrary knowledge of the devices)

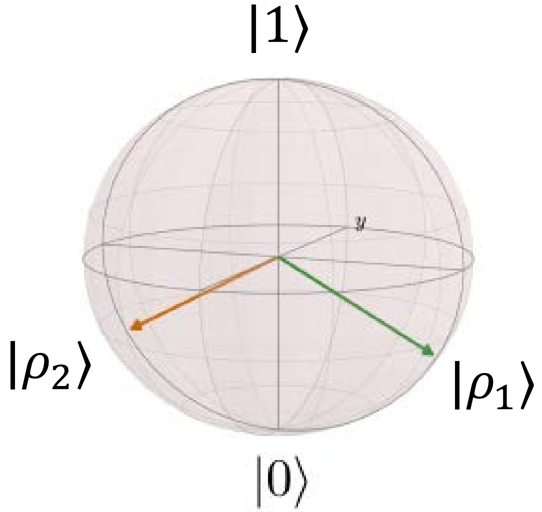
$$E_1 = \langle\rho_1|M|\rho_1\rangle = 1 \implies M = 2|\rho_1\rangle\langle\rho_1| - I$$

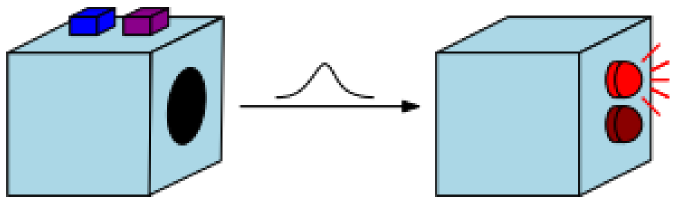
$$\implies E_2 = \langle\rho_2|M|\rho_2\rangle = 2|\langle\rho_2|\rho_1\rangle|^2 - 1$$

$$\implies E_- = \frac{E_1 - E_2}{2} = 2 - 2\,|\langle\rho_2|\rho_1\rangle|^2$$

Minimal value of $|\langle\rho_2|\rho_1\rangle|^2$ given w

$$\implies E_- \leq 4w(1-w) = D_{\max}$$



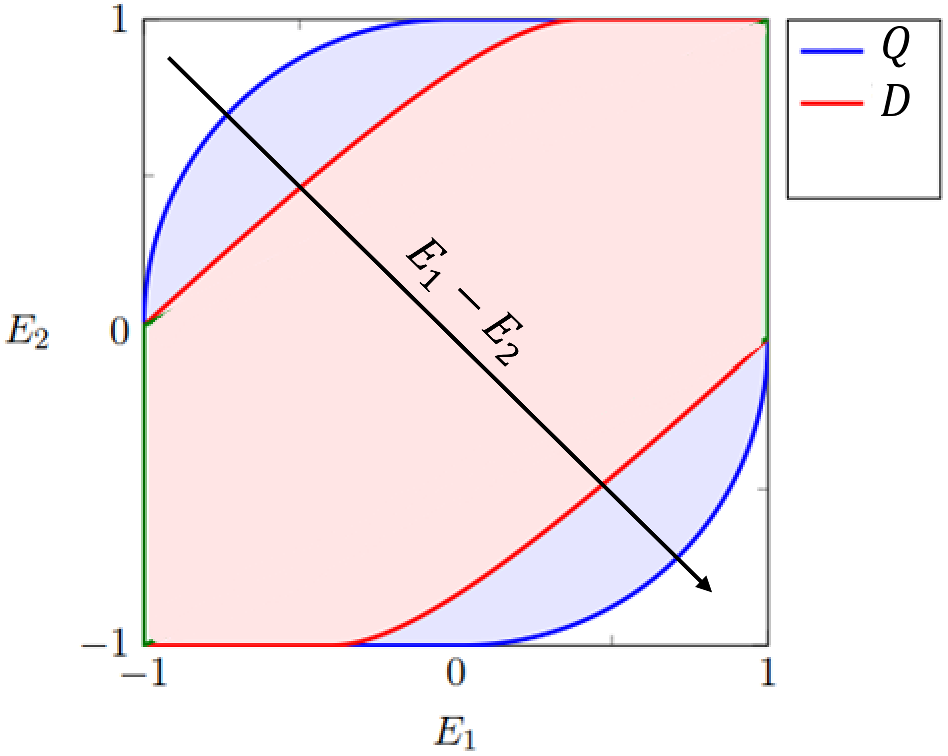


Assumption

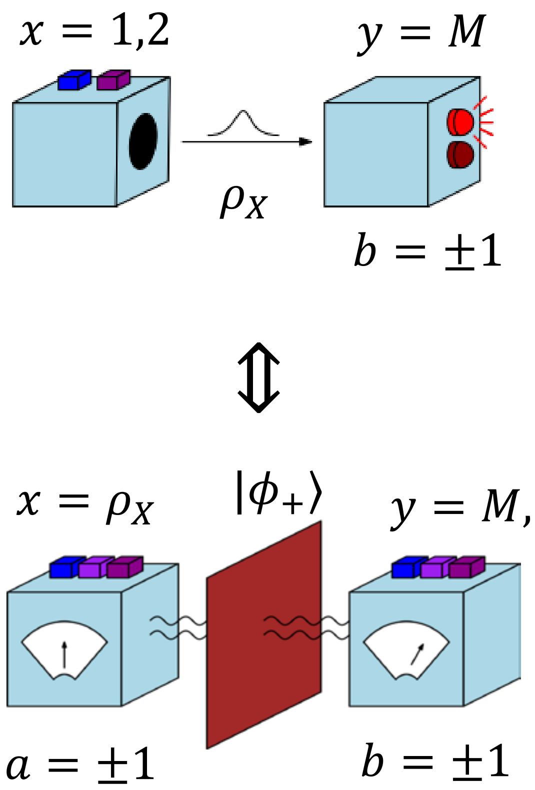
Energy constraint:
$\langle 0| \sum_\lambda p_\lambda \, \rho_x^\lambda |0\rangle \geq w_x$

- $E_- = \frac{E_1 - E_2}{2}$
- If E_1 is deterministic, we have the "Bell inequality"
$$E_- \leq 4w(1-w) = D_{\text{max}}$$
- According to a general quantum strategy
$$E_- \leq 2\sqrt{w(1-w)} = Q_{\text{max}} = \sqrt{D_{\text{max}}} > \text{D}_{\text{max}}$$

More generally, it is possible to characterize completely the set of allowed values (E_1, E_2) for given energy bounds (w_1, w_2)



One nice way to do it:

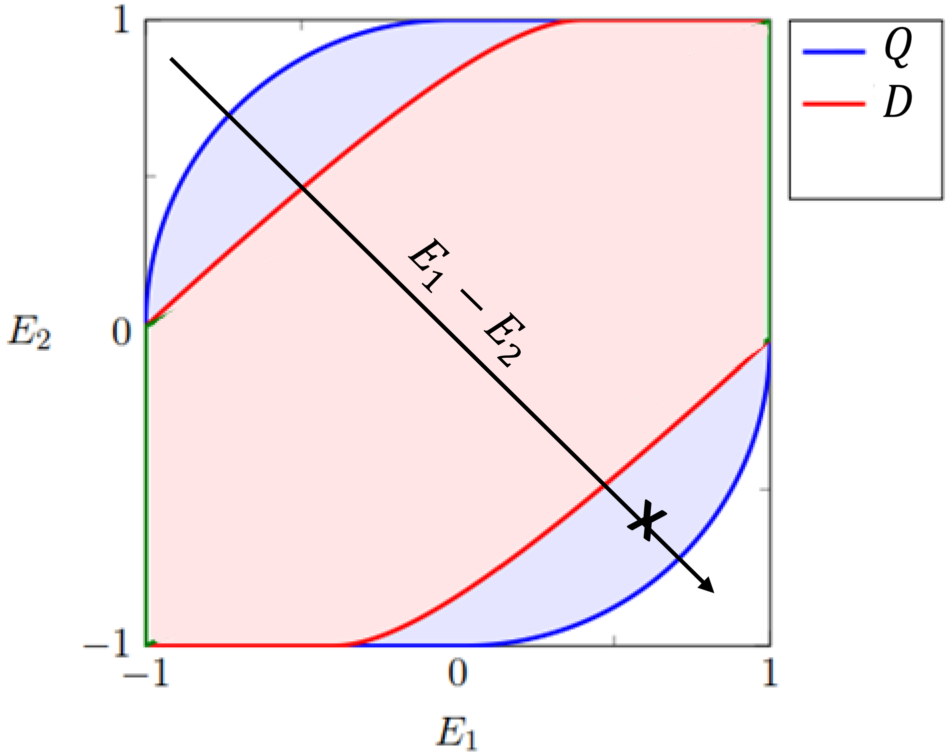


$E_x = Tr[\rho_x M]$
$w_x = Tr[\rho_x V]$

$\langle A_x M \rangle = E_x$
$\langle A_x V \rangle = w_x$

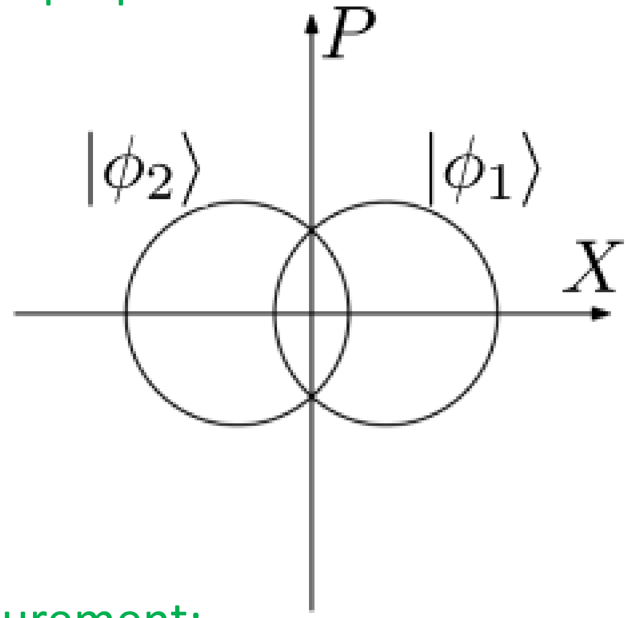
Given this characterization, one can also put rigorous bounds on the output entropy given (E_1, E_2)
→straightforward to build a RNG protocol where amount of randomness produced is evaluated assuming only the energy bound, but no other assumption on the devices.

How to produce “non-deterministic” correlations in the lab?



A practical implementation with gaussian states and homodyne measurements:

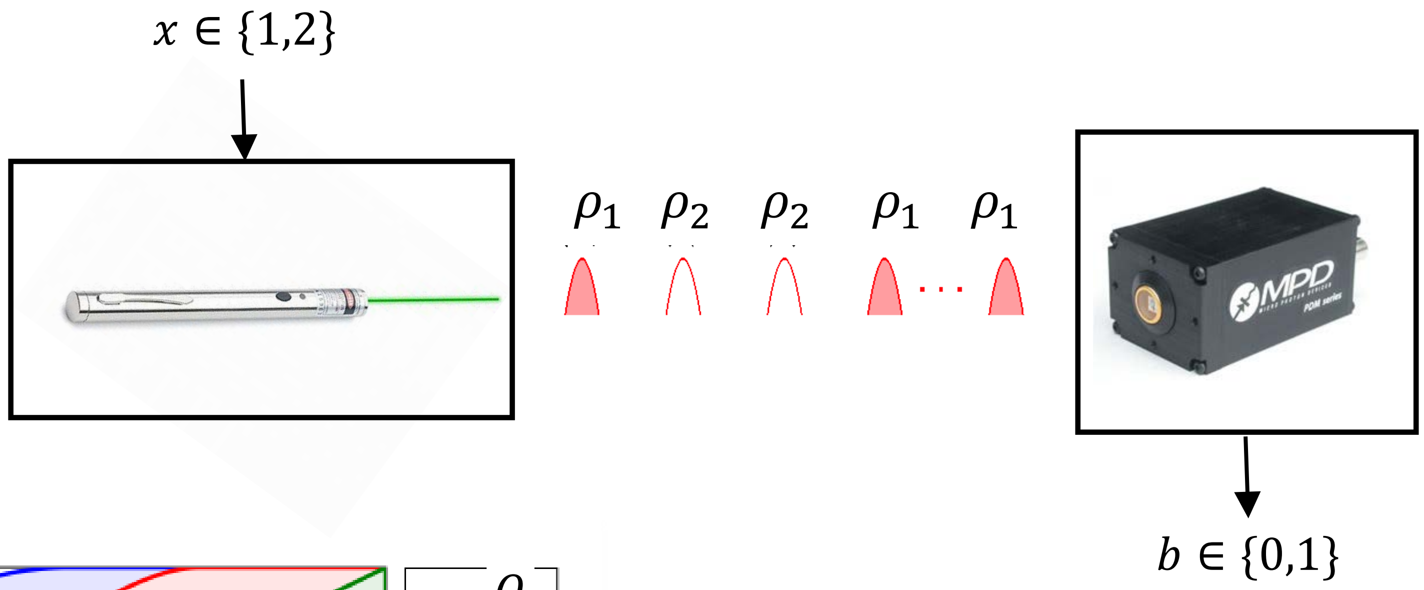
Source prepares:

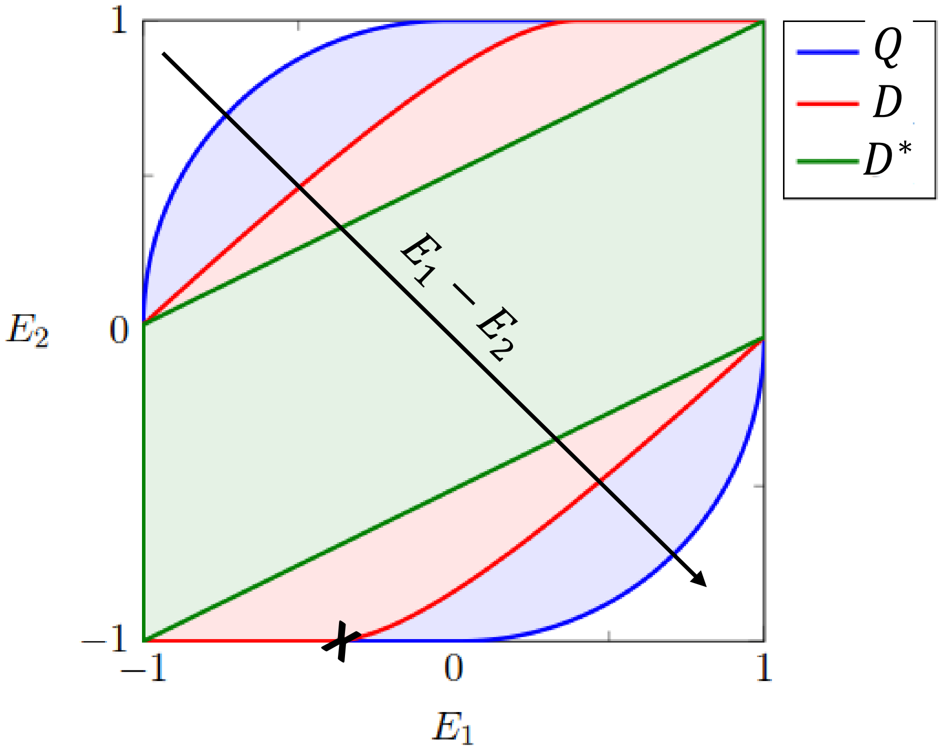


Measurement:

Homodyne measurement of X quadrature with b = sign(X)

A simpler implementation with a slightly stronger assumption





Average energy constraint:
$\langle 0| \sum_\lambda p_\lambda \rho_x^\lambda |0\rangle \geq w_x$

Peak energy constraint
$\langle 0| \rho_x^\lambda |0\rangle \geq w_x$ for all λ

Summary

- We propose to use a bound on the energy of optical signals as a unique assumption on which to prove the security of prepare-and-measure quantum cryptography protocol (with no other assumptions on the devices)
- We have shown that there is a gap between what can be achieved with very simple quantum implementations and deterministic strategies. This is equivalent to the violation of Bell inequalities in full DI protocols.
- These results immediately imply the existence of RNG protocols where the amount of randomness produced can be certified without making any assumptions about the devices except the energy assumption.

Open question

- Is the energy assumption sufficient to prove the security of a QKD protocol?
- We implicitly assumed that the preparation and measurement device did not share prior entanglement. Can this be relaxed?
- One extra motivation for the energy assumption is that it is in principle compatible with CV protocols for which no DI or semi-DI implementations have been introduced.
  Can we analyze the security of a genuinely CV protocol in a DI setting using the energy assumption?