UNIVERSITY OF GDANSK

INTERNATIONAL CENTRE FOR THEORY OF QUANTUM TECHNOLOGIES

Quantum Random Number Generators

Marcin Pawłowski

NARODOWE CENTRUM NAUKI

European Funds Smart Growth

Republic of Poland

FNP Foundation for Polish Science

European Union European Regional Development Fund

CECC 2020, Zagreb, 24-26.06.20

Outline

- Current Qunatum RNGs
- The need for self-testing
- History of device independent protocols
- Quantum nonlocality
- Self-testing QRNGs

Current Quantum RNGs

Classical

- Thermal noise from a resistor, amplified to provide a random voltage source.[12]
- Avalanche noise generated from an avalanche diode, or Zener breakdown noise from a reverse-biased Zener diode.
- Atmospheric noise, detected by a radio receiver attached to a PC (though much of it, such as lightning noise, is not properly thermal noise, but most likely a chaotic phenomenon).

Quantum

- Shot noise, a quantum mechanical noise source in electronic circuits. A simple example is a lamp shining on a photodiode. Due to the uncertainty principle, arriving photons create noise in the circuit. Collecting the noise for use poses some problems, but this is an especially simple random noise source. However, shot noise energy is not always well distributed throughout the bandwidth of interest. Gas diode and thyratron electron tubes in a crosswise magnetic field can generate substantial noise energy (10 volts or more into high impedance loads) but have a very peaked energy distribution and require careful filtering to achieve flatness across a broad spectrum.[8]
- A nuclear decay radiation source, detected by a Geiger counter attached to a PC.
- Photons travelling through a semi-transparent mirror. The mutually exclusive events (reflection/transmission) are detected and associated to ‘0’ or ‘1’ bit values respectively.
- Amplification of the signal produced on the base of a reverse-biased transistor. The emitter is saturated with electrons and occasionally they will tunnel through the band gap and exit via the base. This signal is then amplified through a few more transistors and the result fed into a Schmitt trigger.
- Spontaneous parametric down-conversion leading to binary phase state selection in a degenerate optical parametric oscillator.[9]
- Fluctuations in vacuum energy measured through homodyne detection.[10][11][*third-party source needed*]

Source: *Wikipedia*

INTERNATIONAL CENTRE FOR THEORY OF QUANTUM TECHNOLOGIES

Current Quantum RNGs

Classical

•Thermal noise from a resistor, amplified to provide a random voltage source.[12]

•Avalanche noise generated from an avalanche diode, or Zener breakdown noise from a reverse-biased Zener diode.

•Atmospheric noise, detected by a radio receiver attached to a PC (though much of it, such as lightning noise, is not properly thermal noise, but most likely a chaotic phenomenon).

Quantum

•Shot noise, a quantum mechanical noise source in electronic circuits. A simple example is a lamp shining on a photodiode. Due to the uncertainty principle, arriving photons create noise in the circuit. Collecting the noise for use poses some problems, but this is an especially simple random noise source. However, shot noise energy is not always well distributed throughout the bandwidth of interest. Gas diode and thyratron electron tubes in a crosswise magnetic field can generate substantial noise energy (10 volts or more into high impedance loads) but have a very peaked energy distribution and require careful filtering to achieve flatness across a broad spectrum.[8]

•A nuclear decay radiation source, detected by a Geiger counter attached to a PC.

•Photons travelling through a semi-transparent mirror. The mutually exclusive events (reflection/transmission) are detected and associated to '0' or '1' bit values respectively.

•Amplification of the signal produced on the base of a reverse-biased transistor. The emitter is saturated with electrons and occasionally they will tunnel through the band gap and exit via the base. This signal is then amplified through a few more transistors and the result fed into a Schmitt trigger.

•Spontaneous parametric down-conversion leading to binary phase state selection in a degenerate optical parametric oscillator.[9]

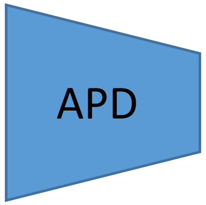
•Fluctuations in vacuum energy measured through homodyne detection.[10][11][*third-party source needed*]

Source: *Wikipedia*

Current Quantum RNGs

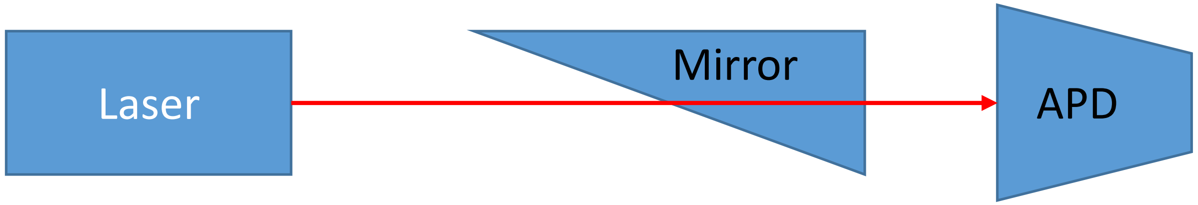
Classical

• Avalanche noise generated from an avalanche diode, or Zener breakdown noise from a reverse-biased Zener diode.



Quantum

• Photons travelling through a semi-transparent mirror. The mutually exclusive events (reflection/transmission) are detected and associated to ‘0’ or ‘1’ bit values respectively.

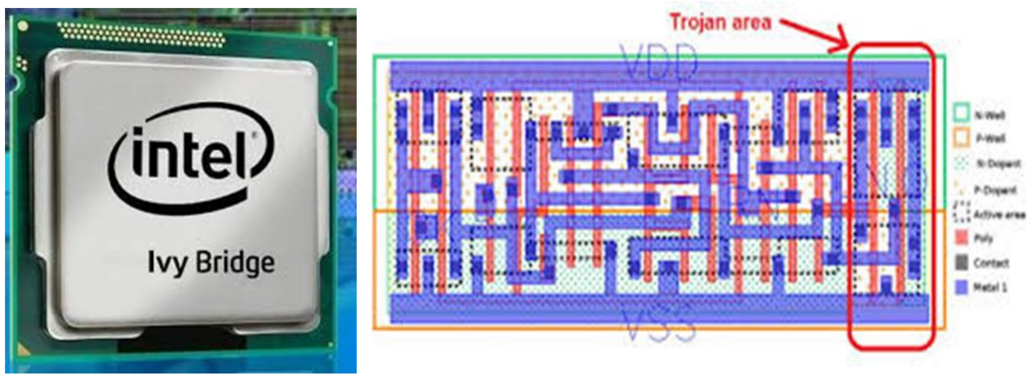


The need for self-testing

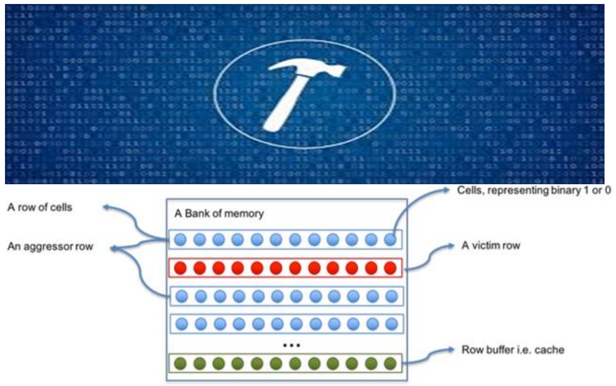
Dishonest vendor

Dishonest designer and/or certifier

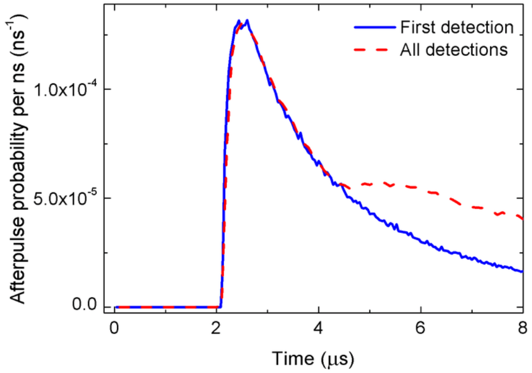
Dishonest manufacturer



Dishonest subcontractor



Smart hacker



DOI: 10.1080/09500340.2012.690050

Smart scientist

INTERNATIONAL CENTRE FOR THEORY OF QUANTUM TECHNOLOGIES

History of device independent protocols

Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, Valerio Scarani,
„*Device-independent security of quantum cryptography against collective attacks*”,
Phys. Rev. Lett. 98, 230501 (2007):

„This intuition has been around for some time [2, 11, 12].”

[2] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[11] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. 68, 557 (1992).
[12] D. Mayers, A. Yao, Quant. Inf. Comput 4, 273 (2004).

↓

„Self-testing”

History of device independent protocols

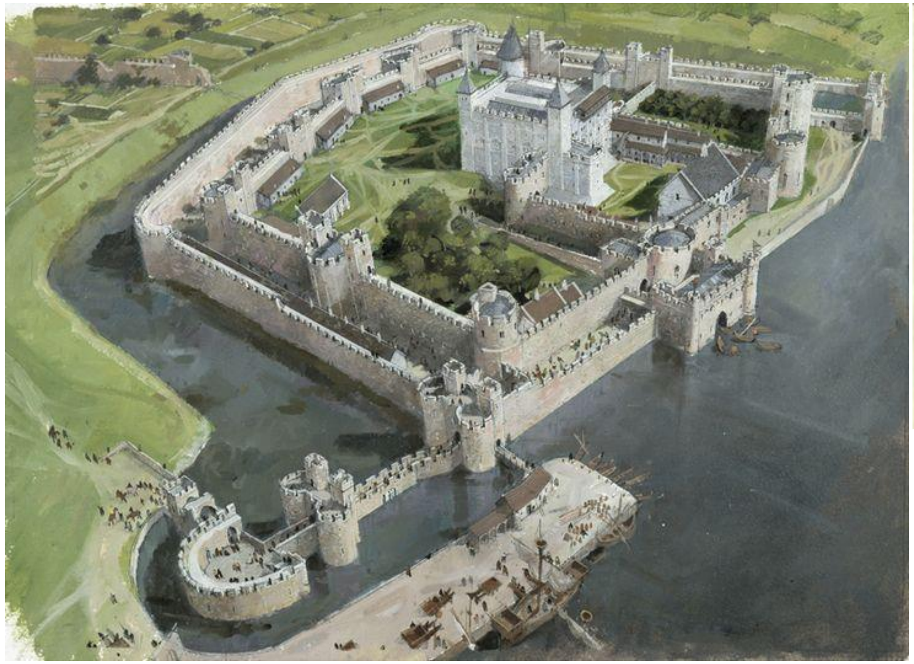
<u>1715 A.D.:</u>

"George, by the Grace of God, King of Great Britain, France and Ireland, Defender of the Faith, etc."

"Louis XIV, by the Grace of God, King of France and of Navarre"

History of device independent protocols

1715 A.D.:



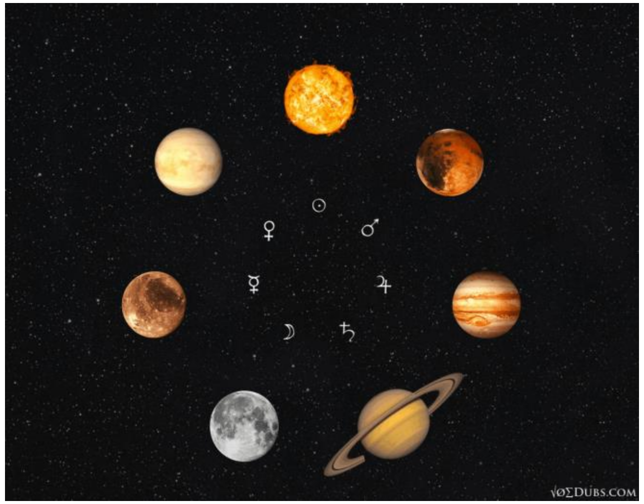
Tower of London

Sir Issac Newton

History of device independent protocols

1715 A.D.:

Security proof



Gold is the densest

Estimate of coin density

Lower bound on gold content

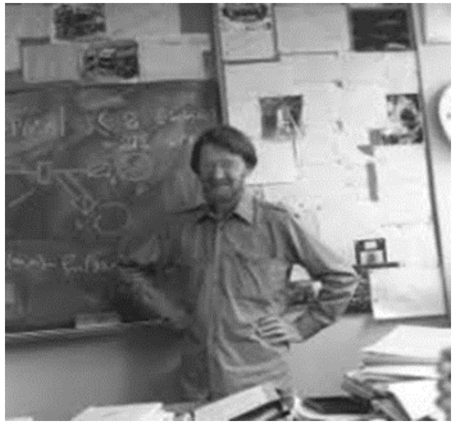
History of device independent protocols

	Intangible quality	Proof	Measurable parameter
1715 A.D.:	Value of a coin	Alchemy	Density
2020 A.D.:	Entropy of a string of numbers	Quantum Physics	Nonlocality, noncompatiblity, etc.

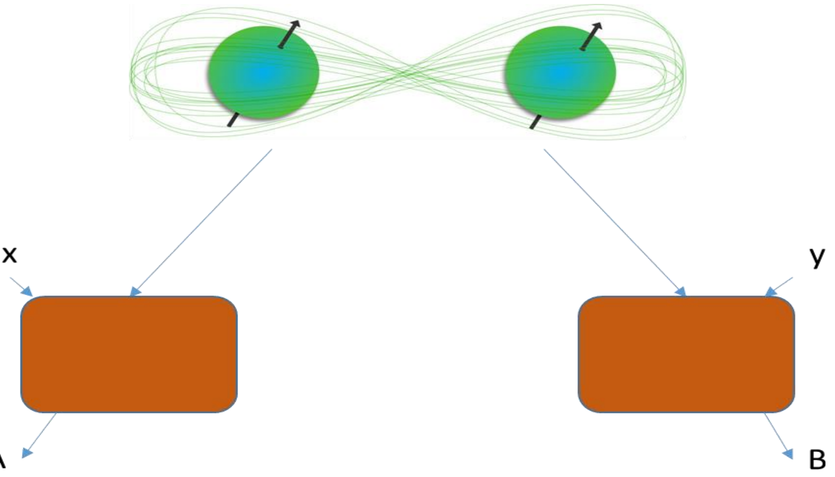
Assumptions:

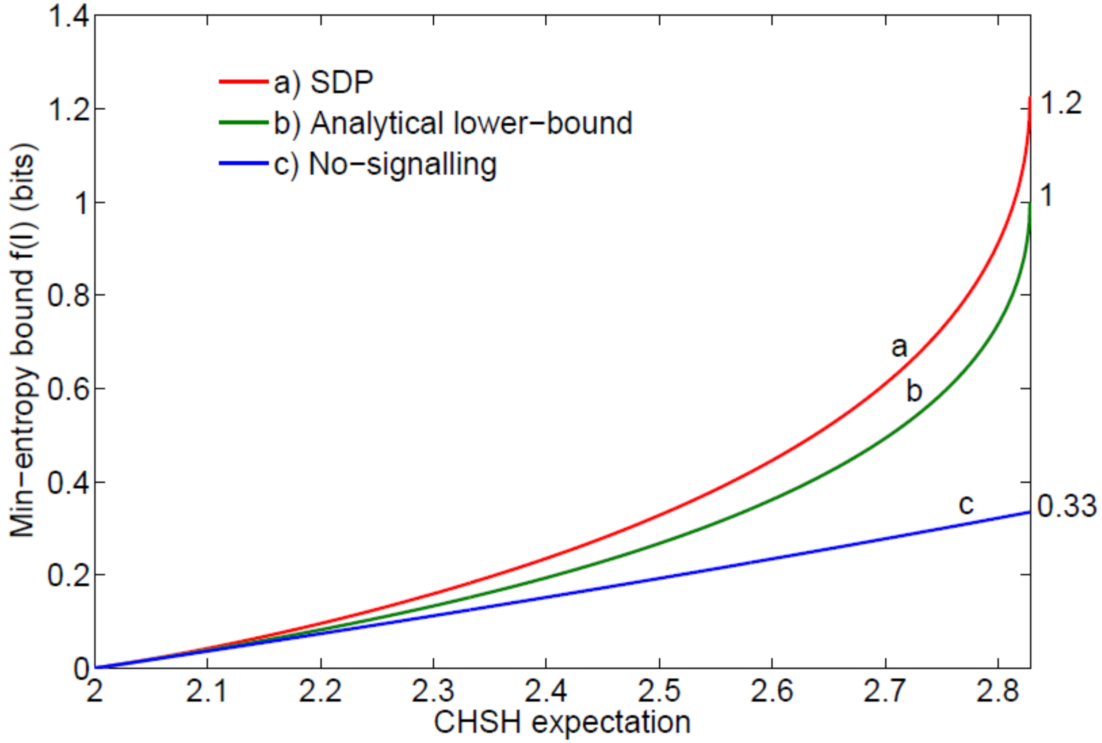
1. **Adversary has better technology and unlimited funds**
2. **Adversary is limited only by the laws of Nature**

Quantum nonlocality



J.S. Bell

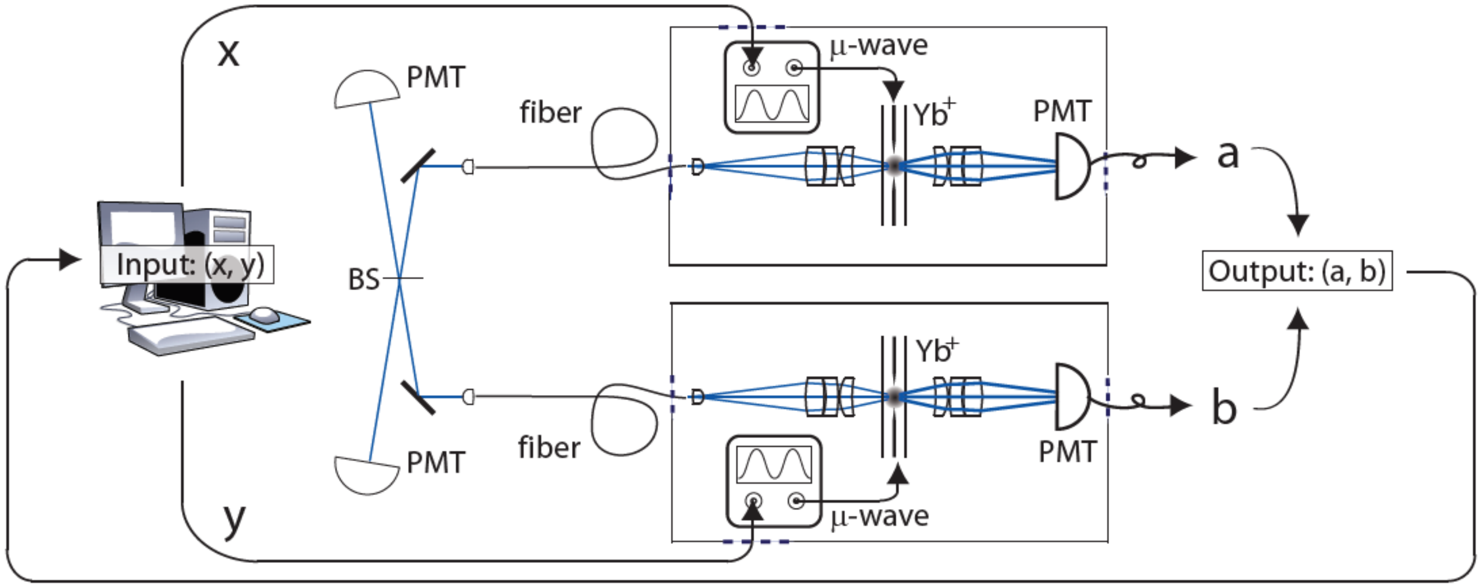




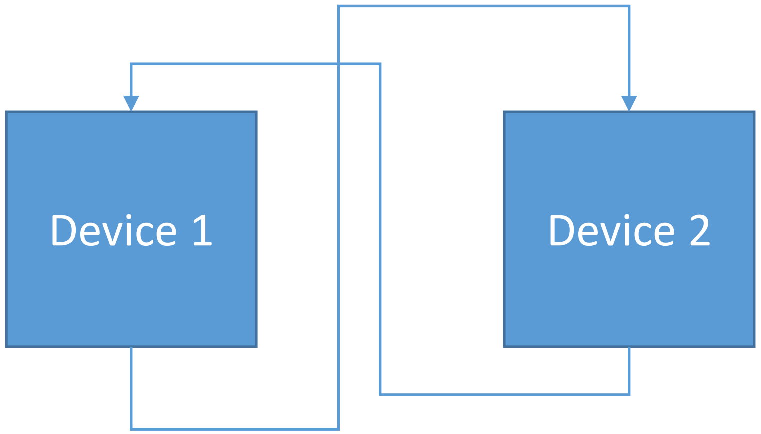
S. Pironio, et. al., Nature 464, 1021 (2010)

ß=P(A=B|x=0,y=0)+P(A=B|x=1,y=0)+P(A=B|x=0,y=1)-P(A=B|x=1,y=1)≤2

Quantum nonlocality

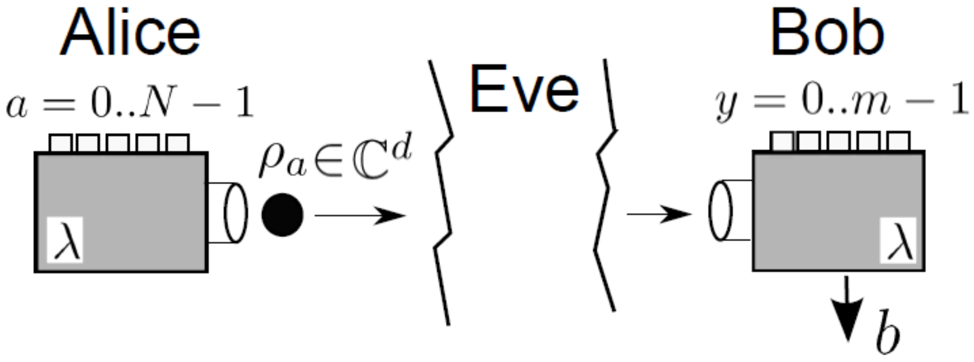


S. Pironio, et. al., Nature 464, 1021 (2010)

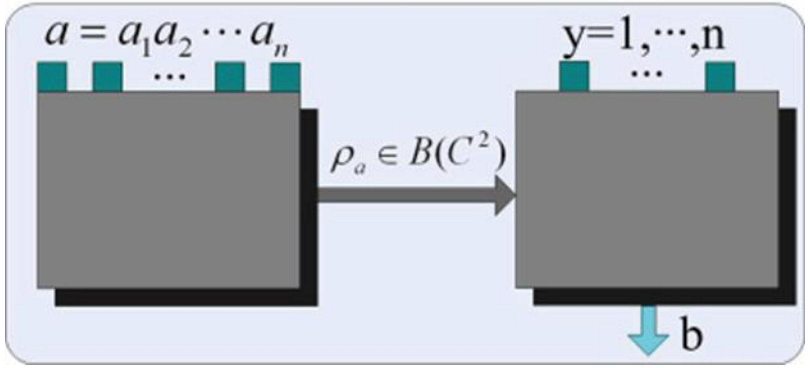


C.A. Miller, Y. Shi, Journal of the ACM, Vol. 63, Issue 4, Article No. 33 (2016)

Self-testing QRNGs: Semi-device independent



M. Pawłowski, N. Brunner, "Semi-device-independent security of one-way quantum key distribution", Phys. Rev. A **84**, 010302(R) (2011).

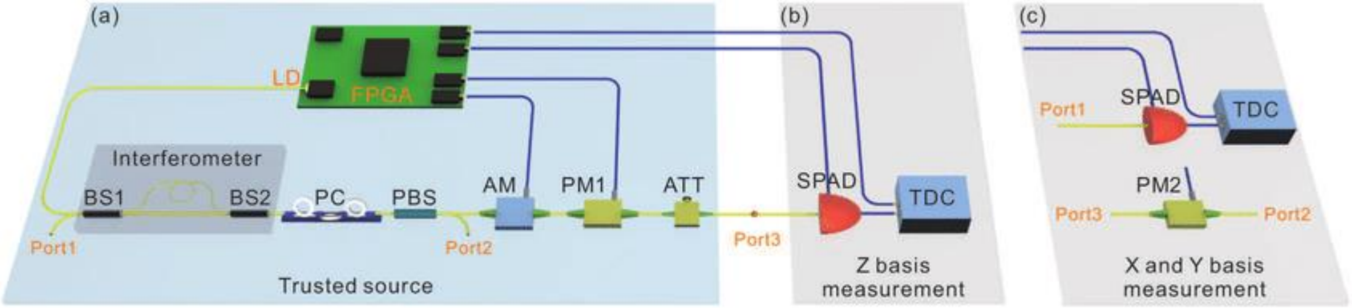


H-W Li, Z-Q Yin, Y-C Wu, X-B Zou, S. Wang, W. Chen, G-C Guo, Z-F Han, Phys. Rev. A. **84** ,034301 (2011).

H-W. Li, M. Pawłowski, Z-Q. Yin, G-C. Guo, Z-F. Han, Phys. Rev. A **85**, 052308 (2012).

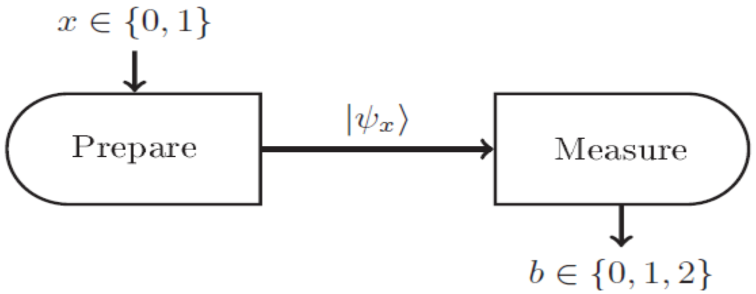
Self-testing QRNGs: Semi-device independent

Measurment device independent QRNG



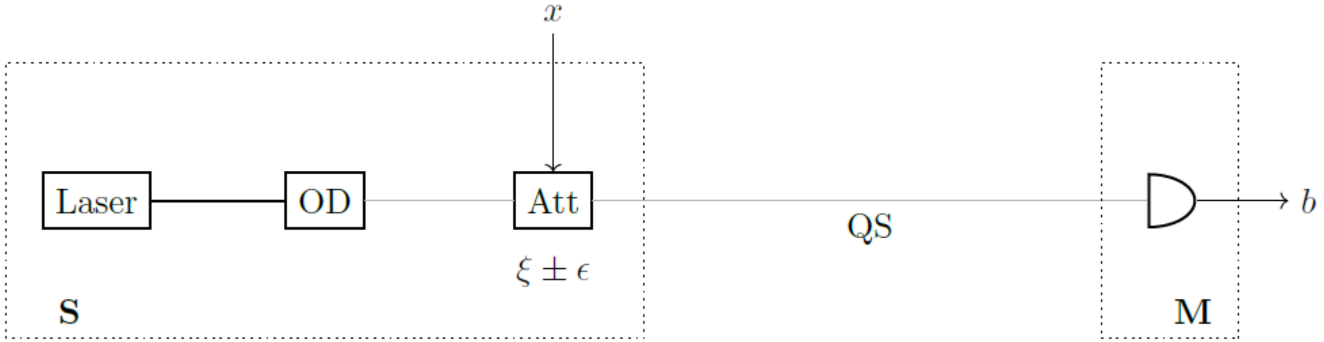
Y.-Q. Nie, et. al., Experimental measurement-device-independent quantum random number generation, Physical Review A, 94 (2016).

Minimal state overlap assumption



W. Shi, Y. Cai, J. Bohr Brask, H. Zbinden, N. Brunner, Phys. Rev. A 100, 042108 (2019).

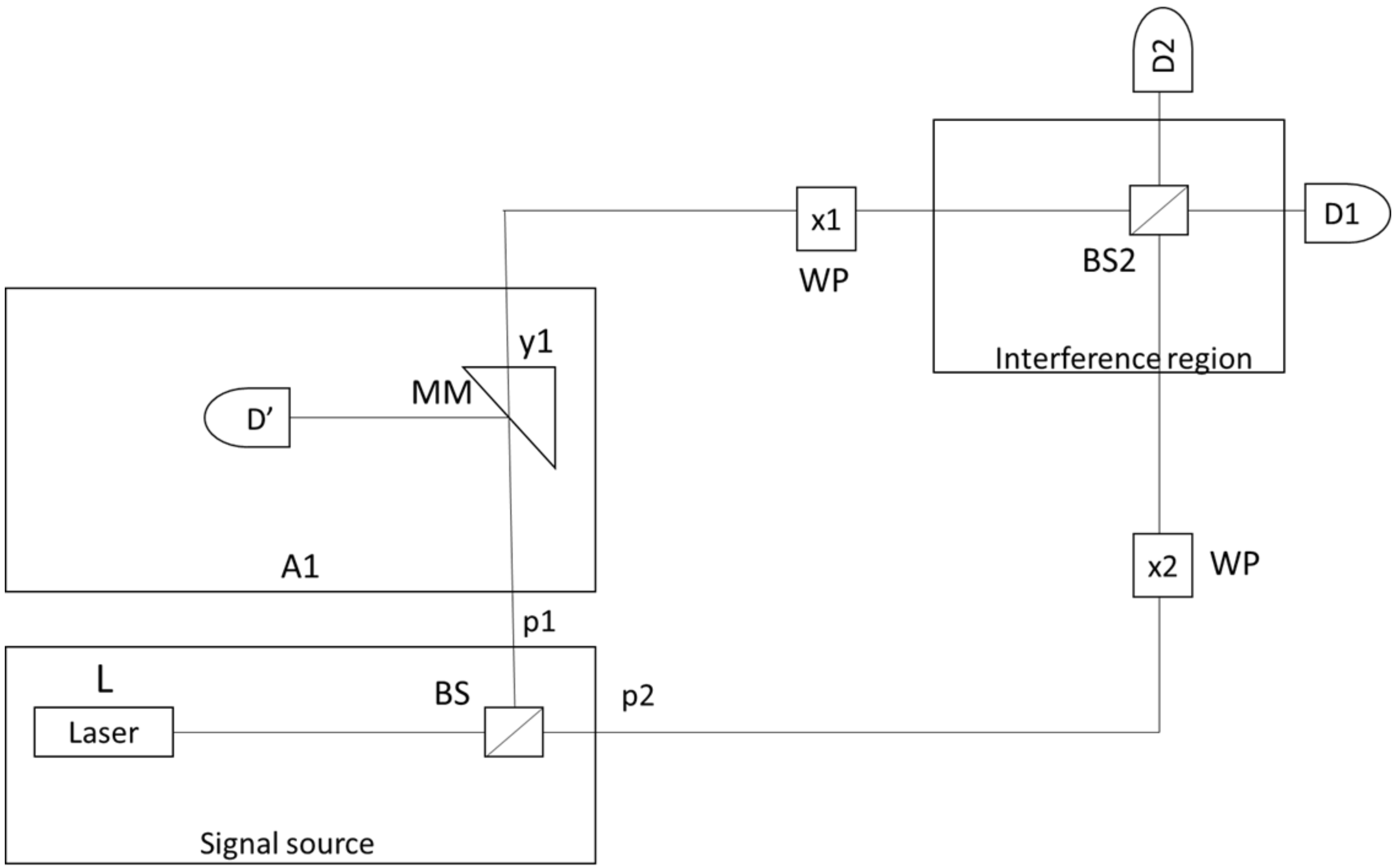
Mean value assumption

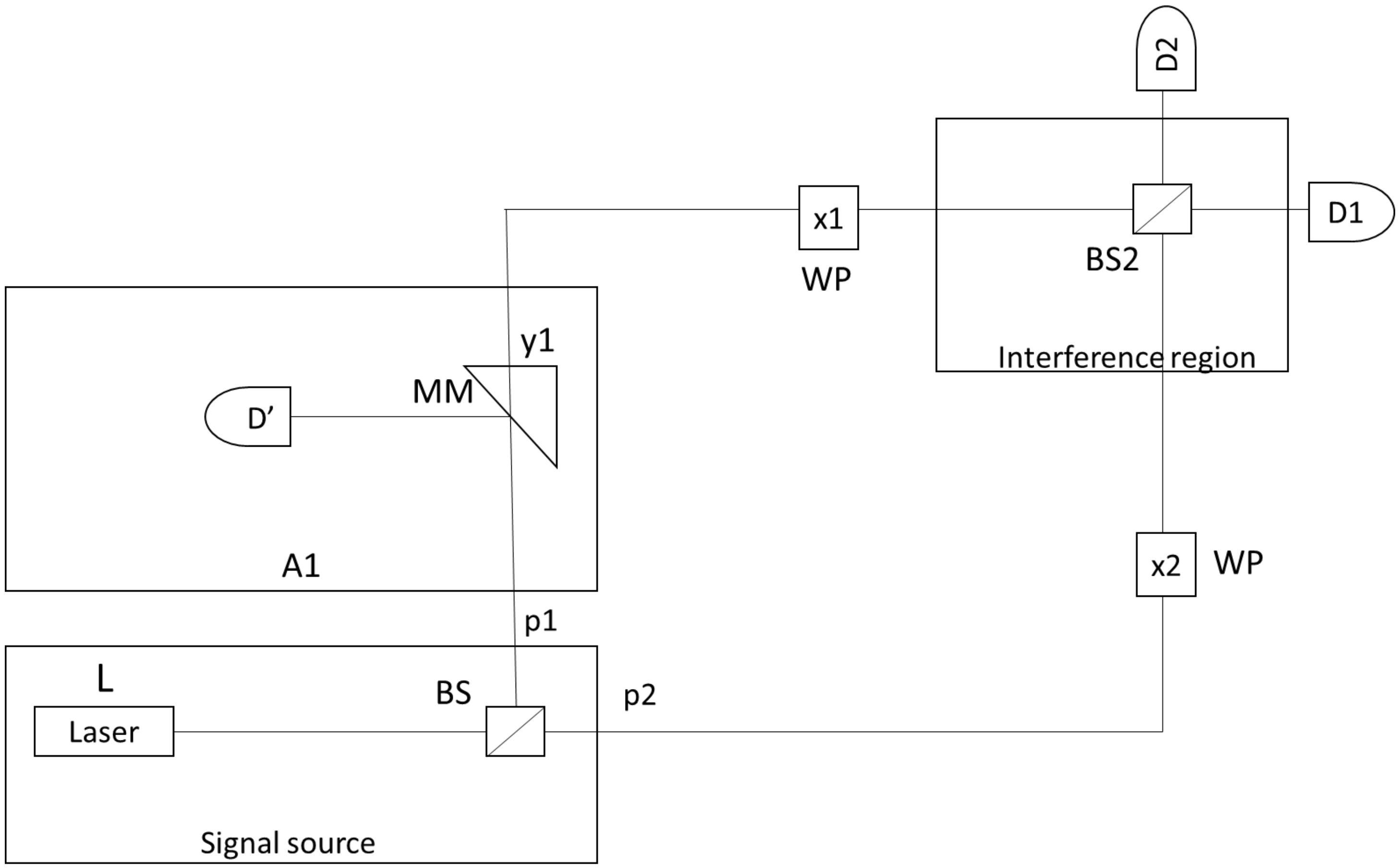


T. Van Himbeeck, et. al., Quantum 1, 33 (2017).

INTERNATIONAL CENTRE FOR THEORY OF QUANTUM TECHNOLOGIES

Self-testing QRNGs: Semi-device independent




D2
D1
x1
WP
BS2
Interference region
y1
MM
D'
A1
x2
WP
p1
L
BS
p2
Laser
Signal source