instituto de telecomunicações

IT-Aveiro

QRNG from Vacuum States

Optical Networking

Background and challenges

- Why are random numbers important?

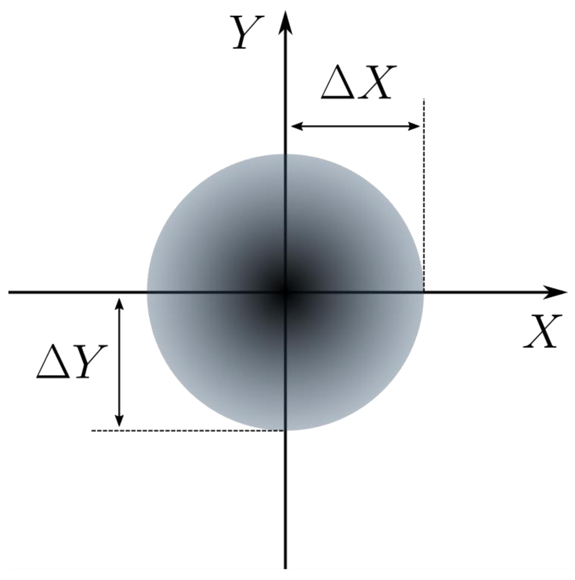
They are necessary for a range of applications: cryptography, numeric simulations, lotteries, fundamental physics tests (Bell experiment)…

- Why quantum?

Quantum physics is supported by a probabilistic theory that is fundamentally random, thus it can generate truly random numbers, that are completely unpredictable and which cannot be reproduced.

- From where can we extract quantum randomness?

The quadratures of a vacuum state are truly random.

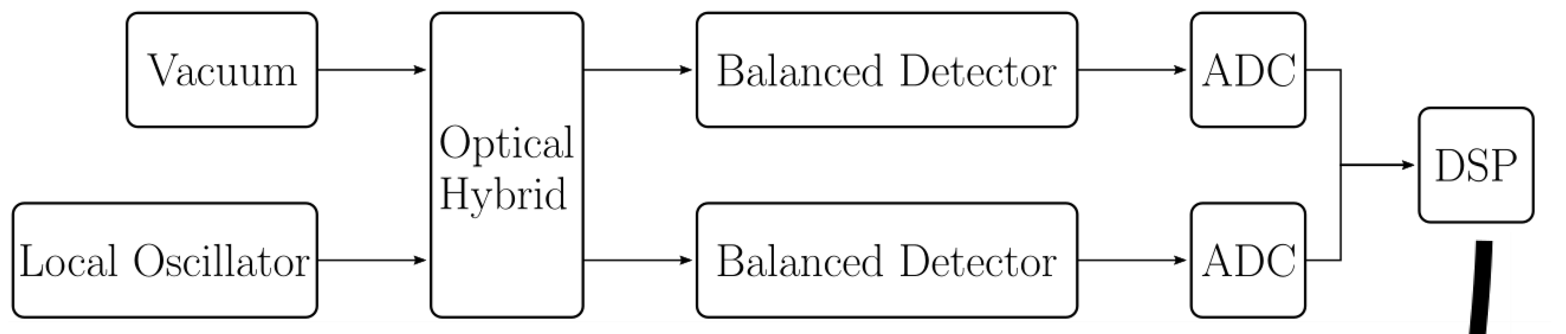


- What challenges do we have?

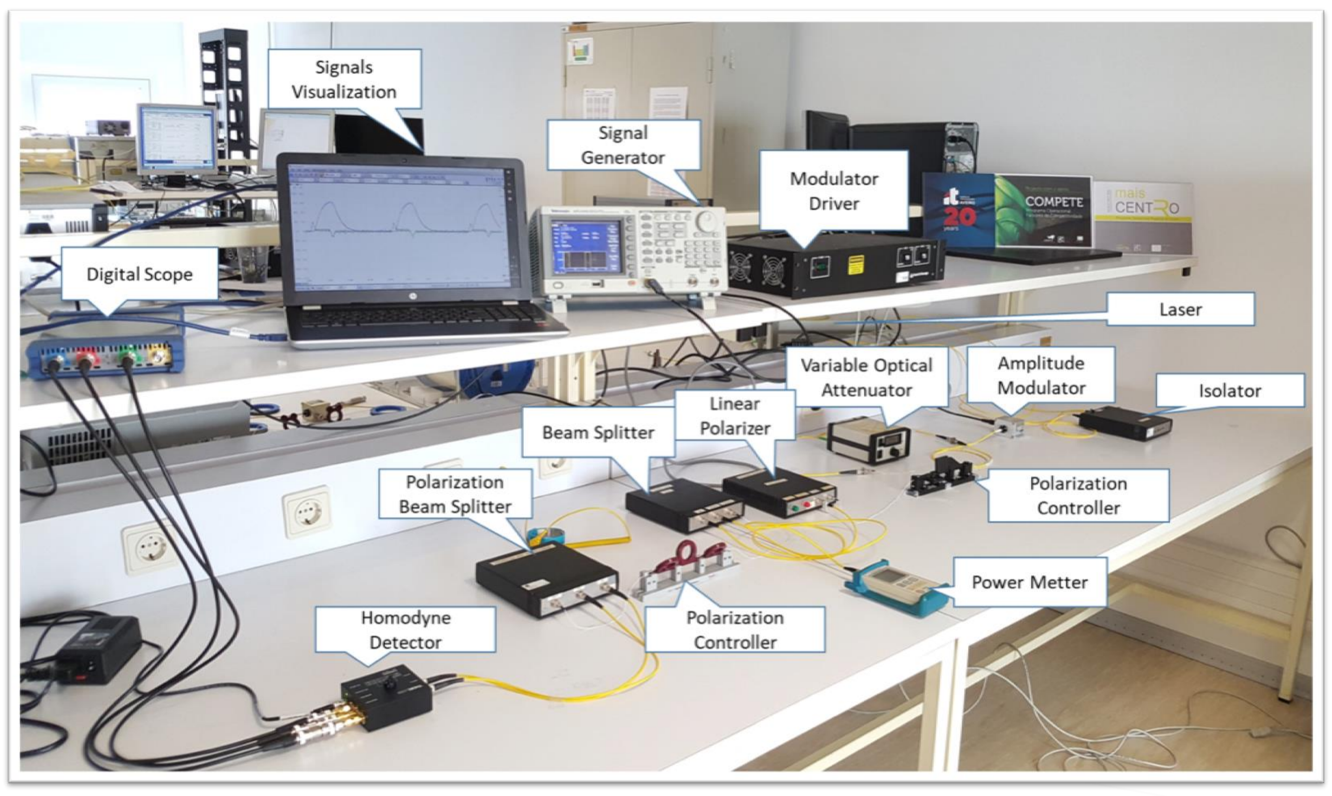
To recover the truly random vacuum state quadrature fluctuation we need to reject all sources of classical noise.

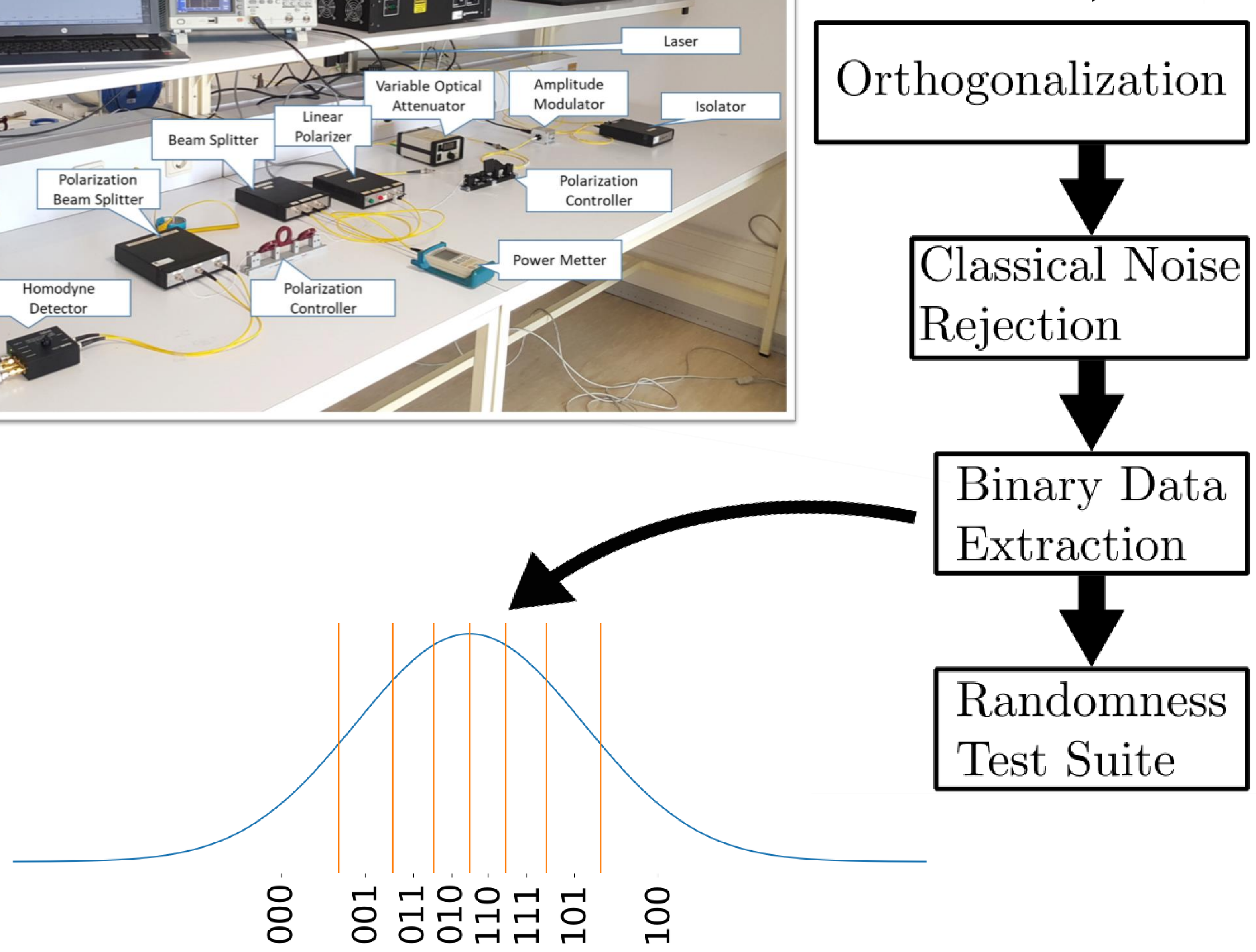
Description and main innovation

- We can perform homodyne measurements on the vacuum states to obtain the X and Y quadratures of the vacuum state.
- By performing dual homodyne measurements we effectively double the bit rate of the system.



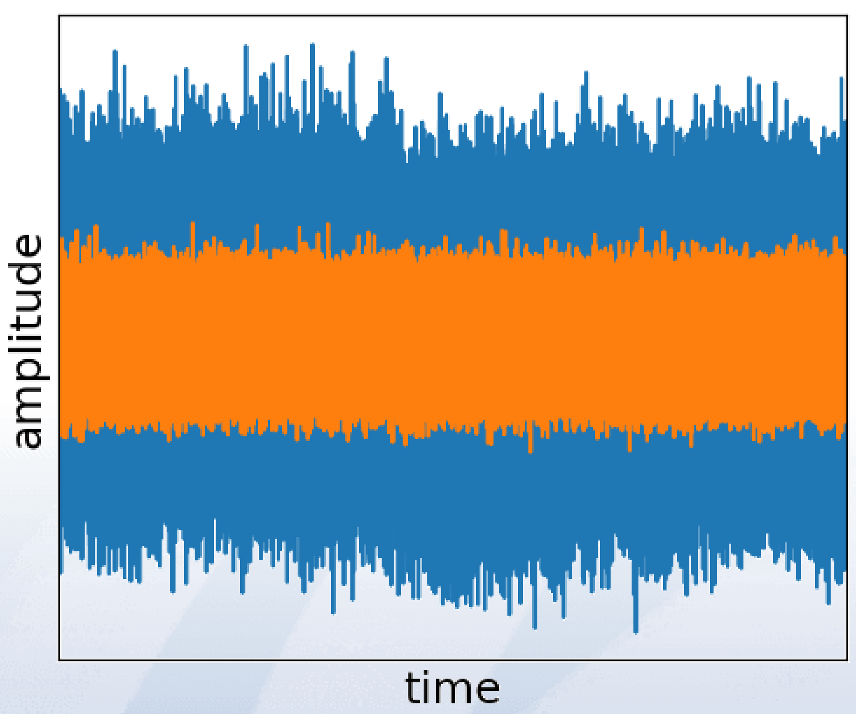
- Practical inaccuracies mean that isolating the X and Y quadratures is a challenge, this can be accomplished through DSP.
- In the literature, classical noise is avoided by using very high quality lasers in a very carefully tuned system. We intend to achieve the same results with a more simplistic system with the help of DSP.

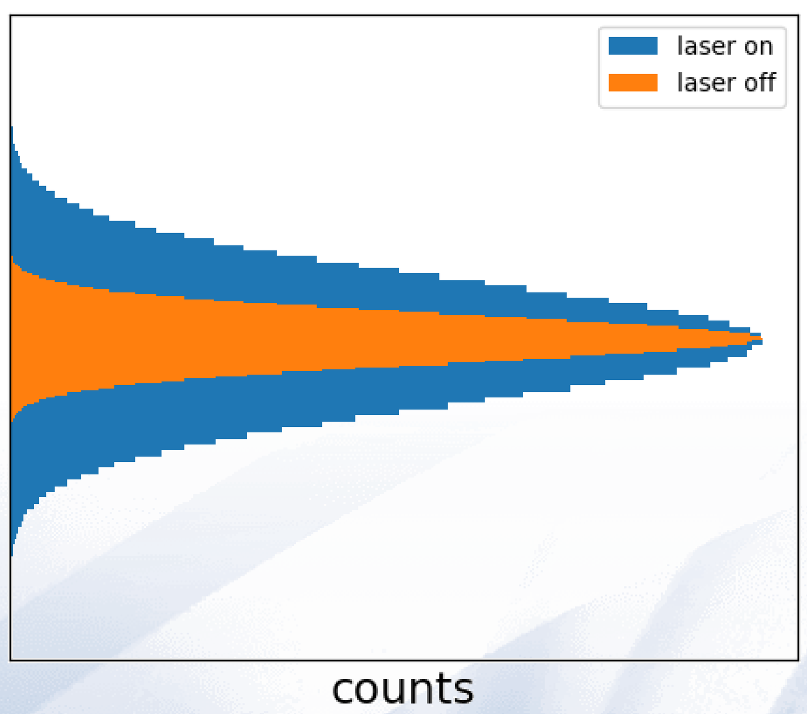




- Since the burden for classical noise rejection is on the DSP stage, our system is easily made self calibrating.

Achievements





- We are able to generate quantum based random numbers in real-time at a rate of 100 MHz.
- The generated numbers have passed most tests under the NIST suite in an offline setting.
- We have already prepared a real time acquisition and testing suite based on LabView.

TÉCNICO LISBOA · UNIVERSIDADE DE COIMBRA · altice labs · UNIVERSIDADE DA BEIRA INTERIOR · IPL · U.PORTO · NOKIA · ISCTE IUL Instituto Universitário de Lisboa

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA
UID/EEA/50008/2013

universidade de aveiro