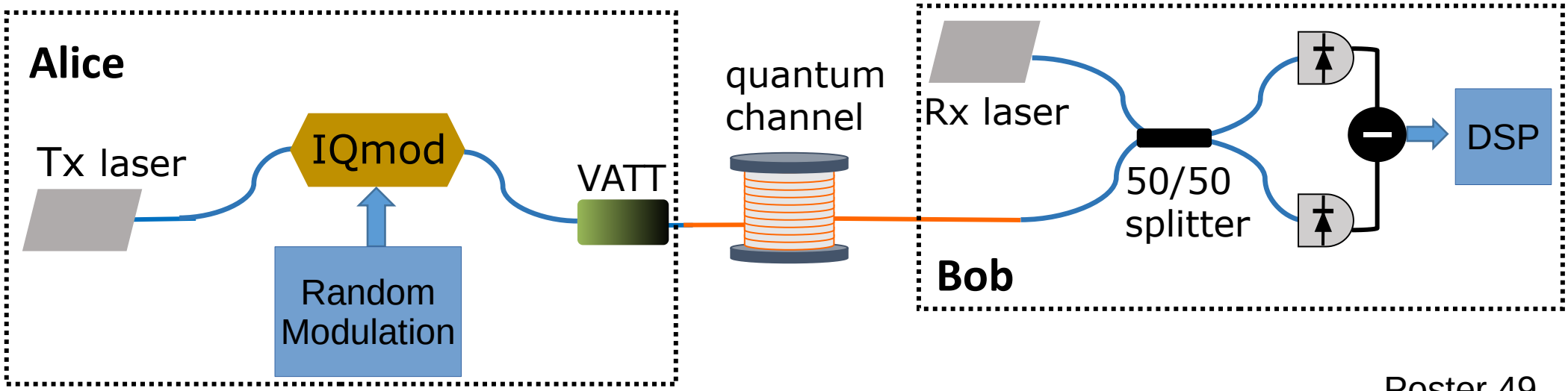
Vacuum fluctuations quantum random number generator with non-iid samples

Tobias Gehring et al.

Secure heterodyne-based quantum random number generator at 17 Gbps

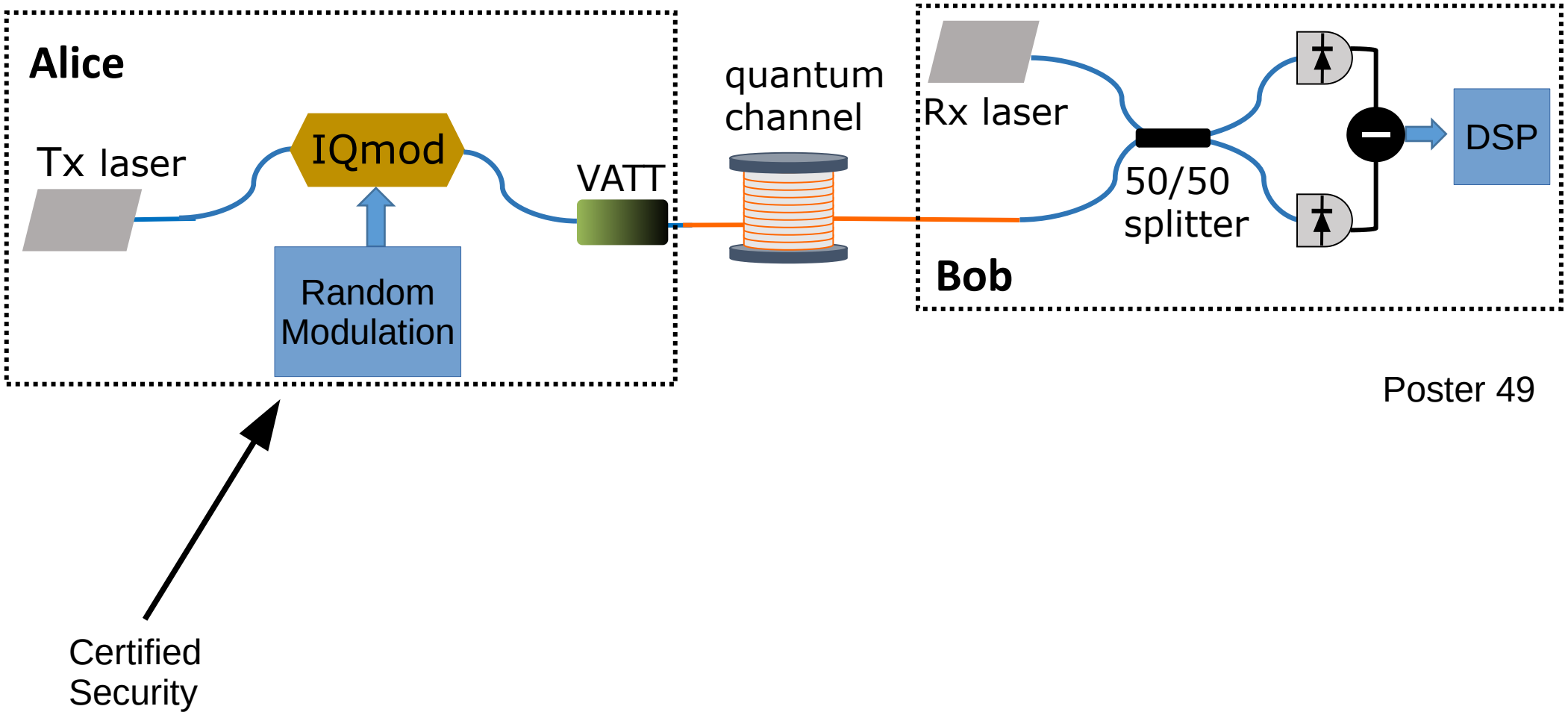
Marco Avesani et al.

The need for random numbers



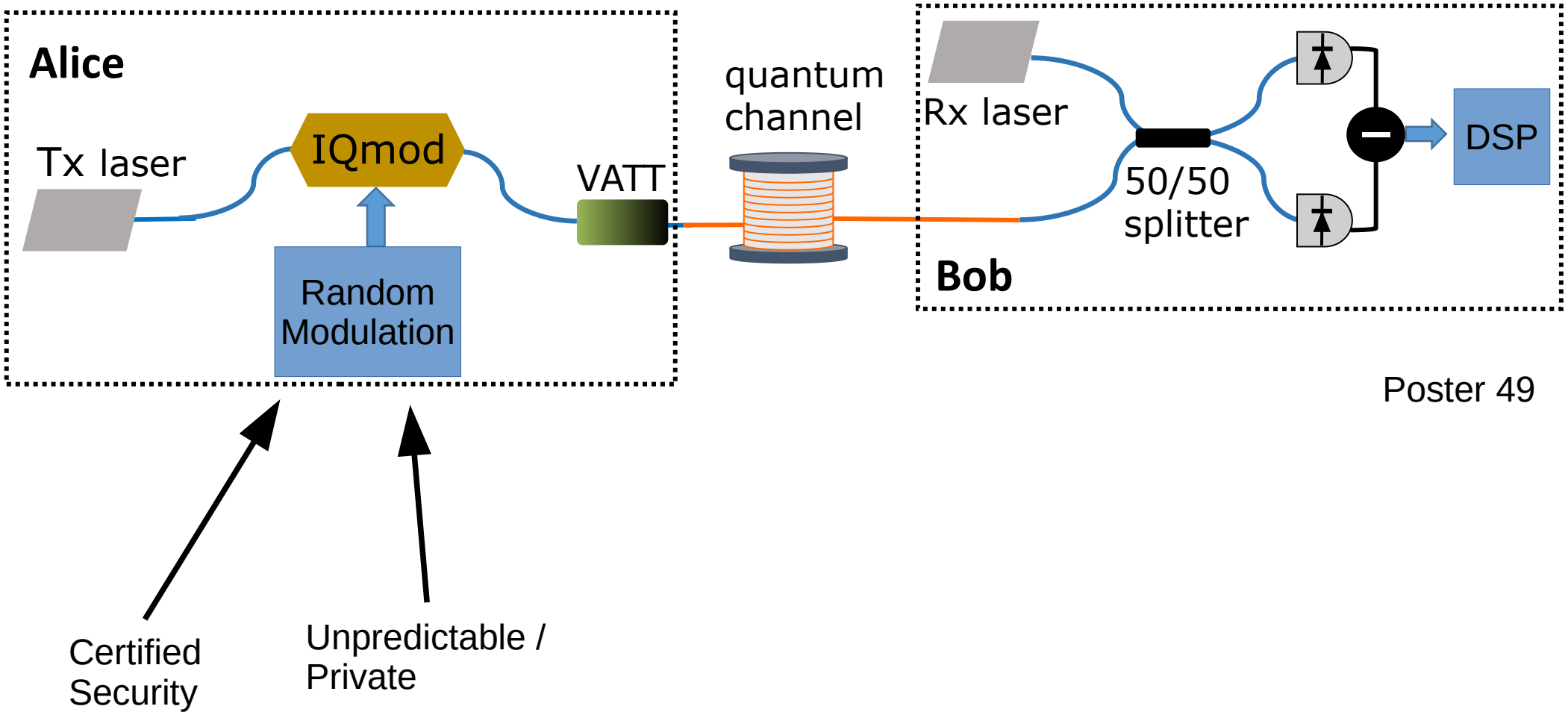
Poster 49

The need for random numbers



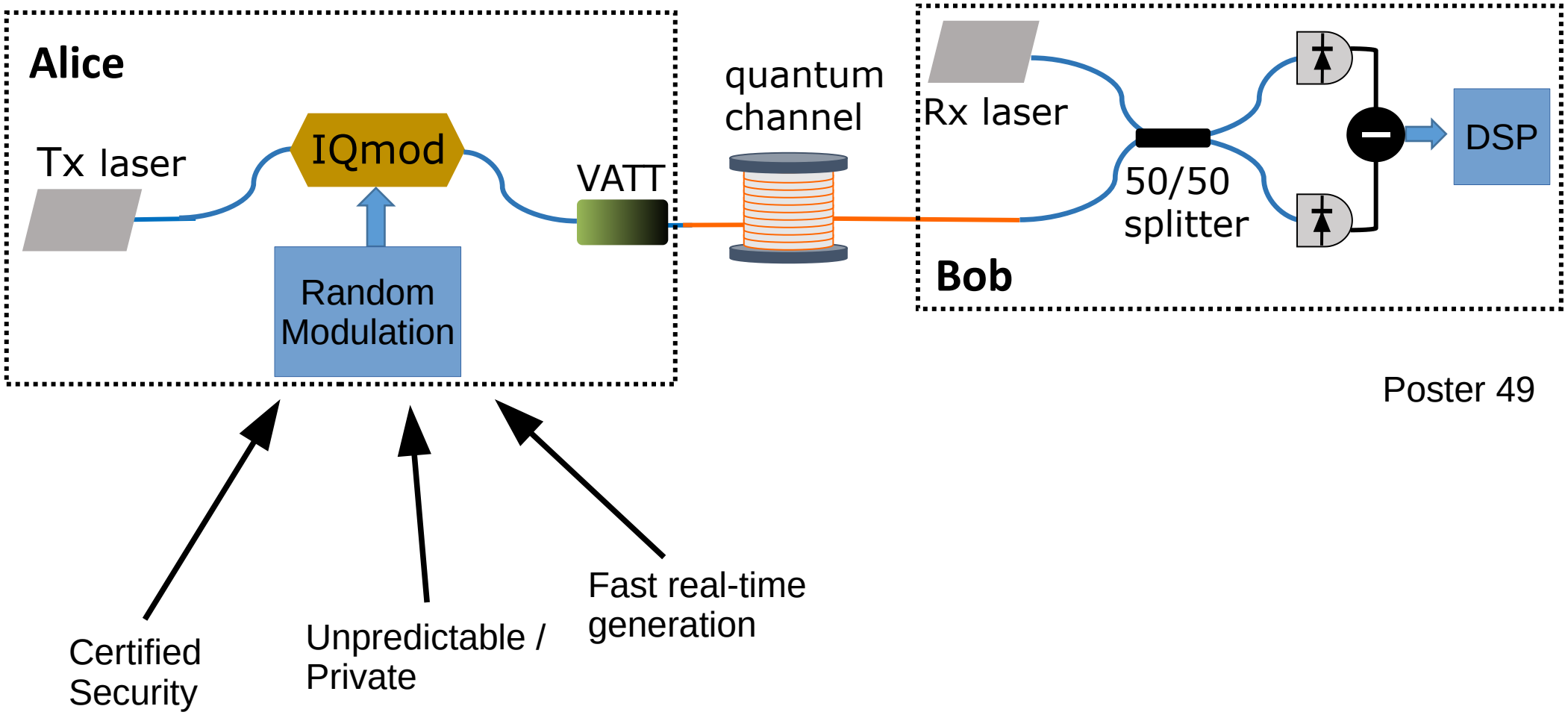
Poster 49

The need for random numbers



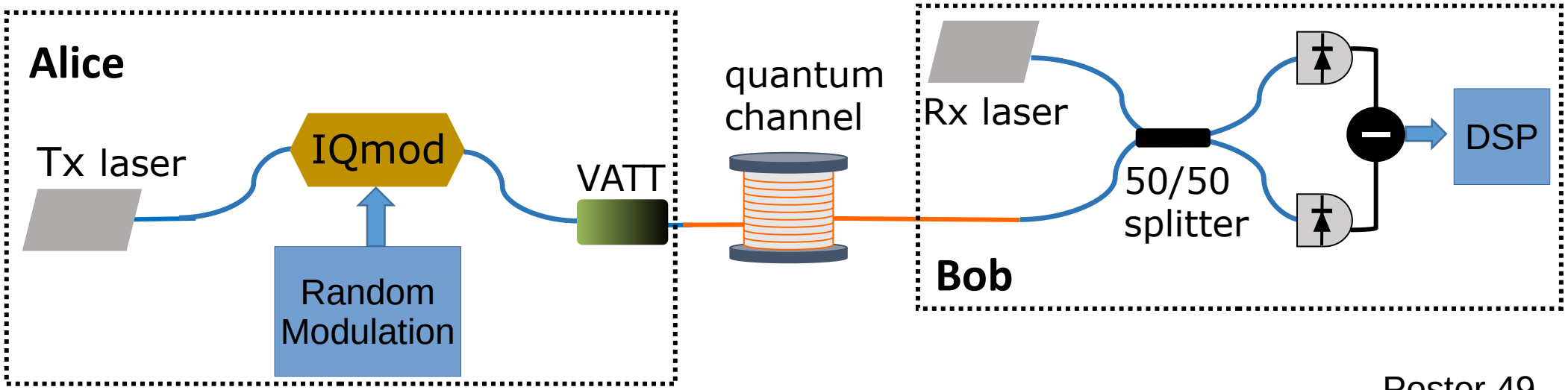
Poster 49

The need for random numbers



Poster 49

The need for random numbers



Poster 49

Certified Security

Unpredictable / Private

Fast real-time generation

Many other applications:

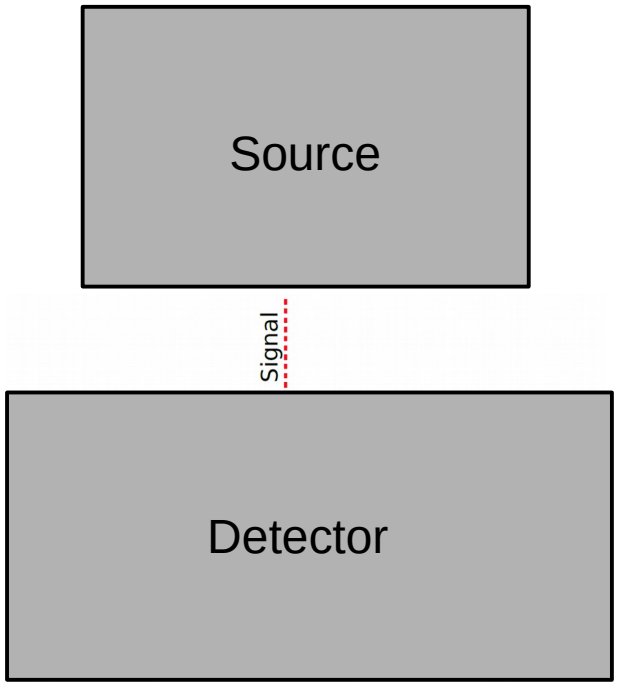
- Simulations
- Gambling
- Classical Key Generation
- etc

Randomness Certification

How can one guarantee that the random numbers are truly random?

Randomness Certification

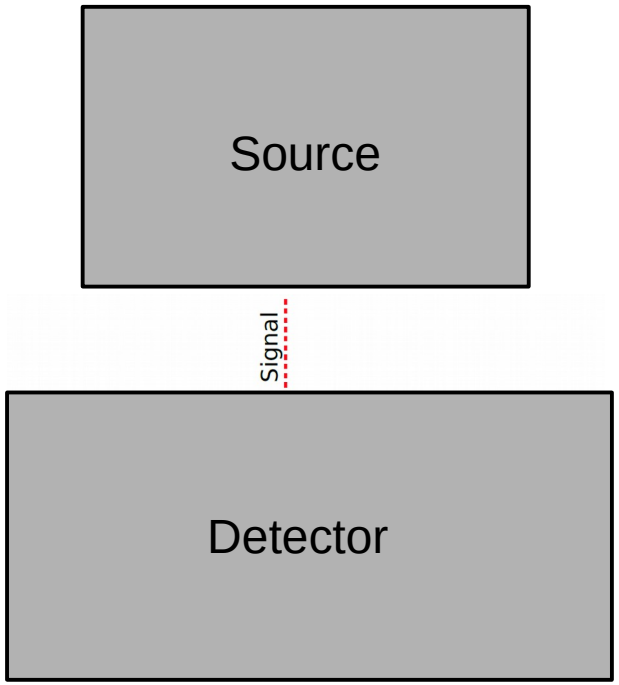
How can one guarantee that the random numbers are truly random?



Device-Independent

Randomness Certification

How can one guarantee that the random numbers are truly random?

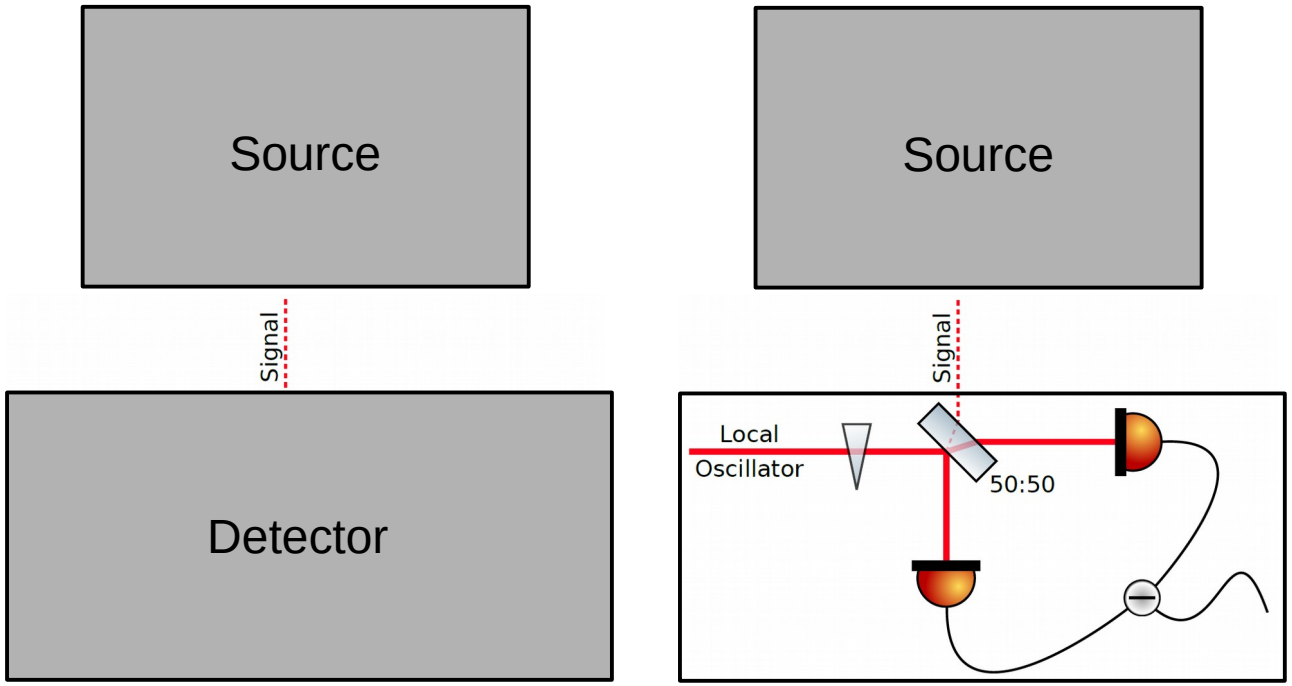


Device-Independent

More assumptions

Randomness Certification

How can one guarantee that the random numbers are truly random?



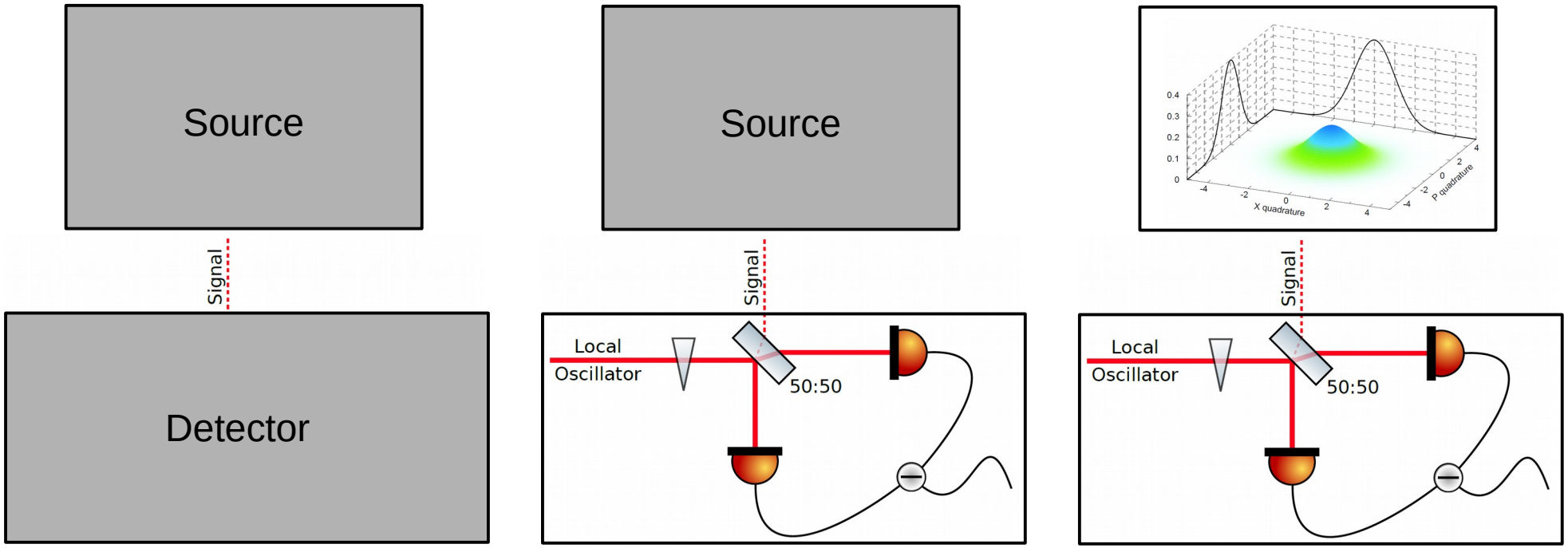
Device-Independent

Source-Independent

More assumptions

Randomness Certification

How can one guarantee that the random numbers are truly random?



Device-Independent

Source-Independent

Device Dependent

More assumptions

Vacuum fluctuations quantum random number generator with non-iid samples

Tobias Gehring[1], Arne Kordts[1], Dino Solar Nikolic[1], Nitin Jain[1], Cosmo Lupo[2], Stefano Pirandola[2], Thomas B. Pedersen[3], Ulrik L. Andersen[1]

1) Department of Physics, Technical University of Denmark, Denmark

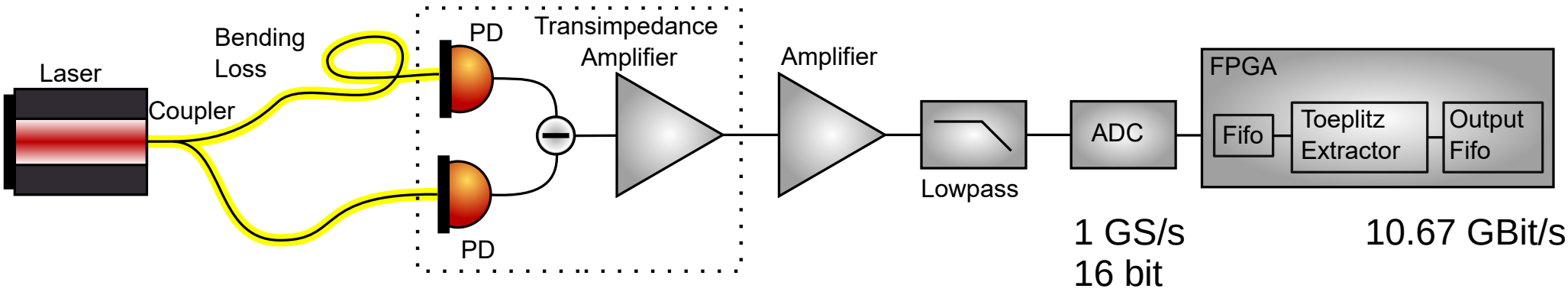
2) Department of Computer Science, University of York, UK

3) Cryptomathic A/S, Denmark

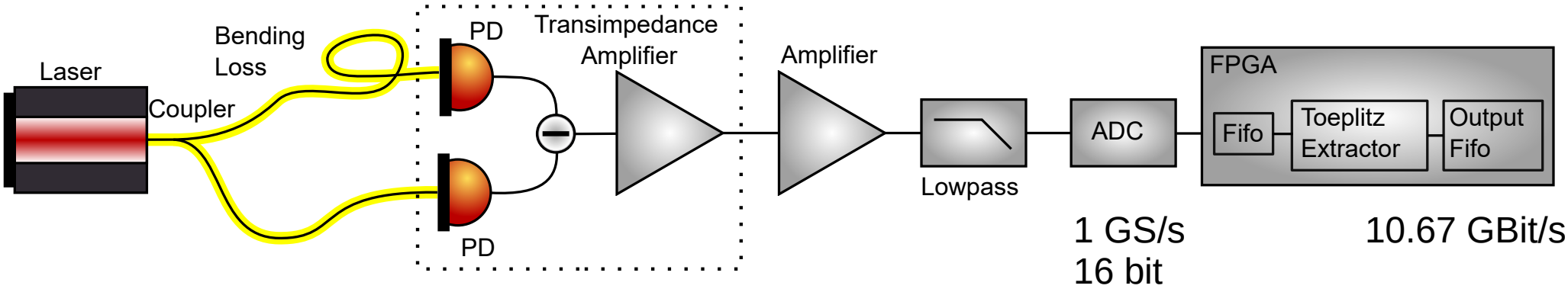
Innovationsfonden

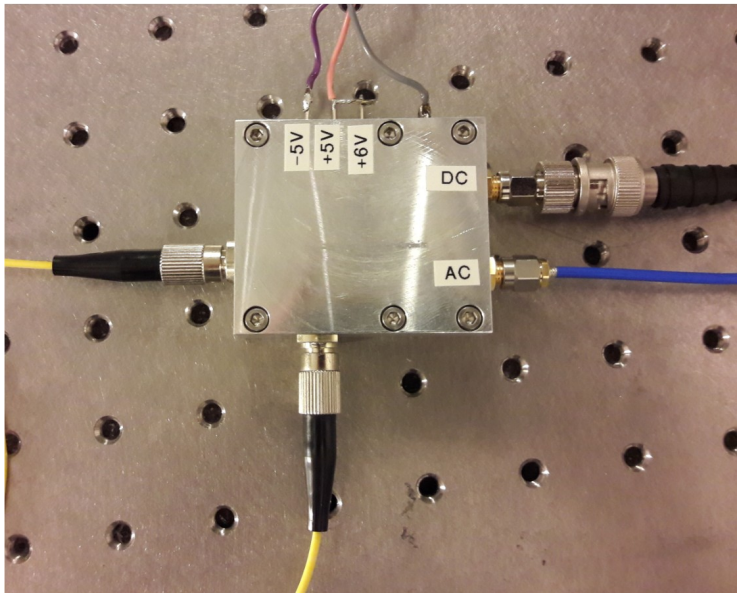
Qubiz
Quantum Innovation Center

Experimental Setup

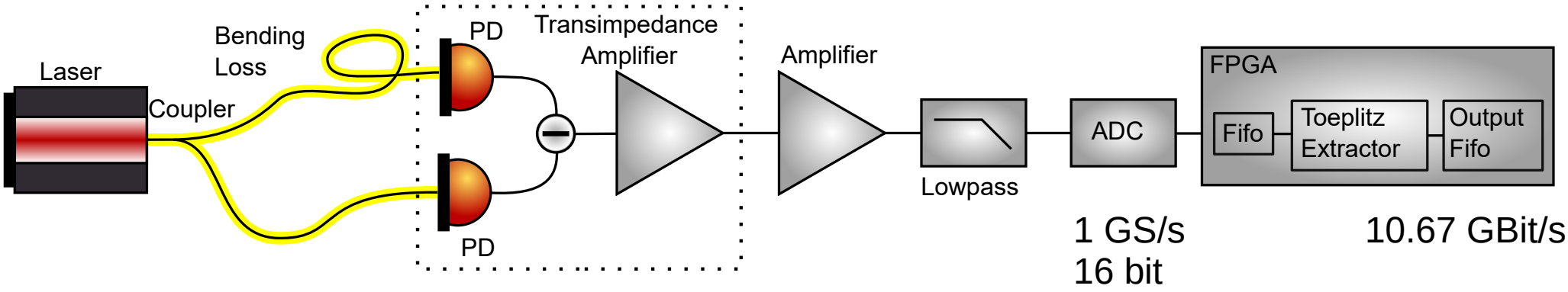


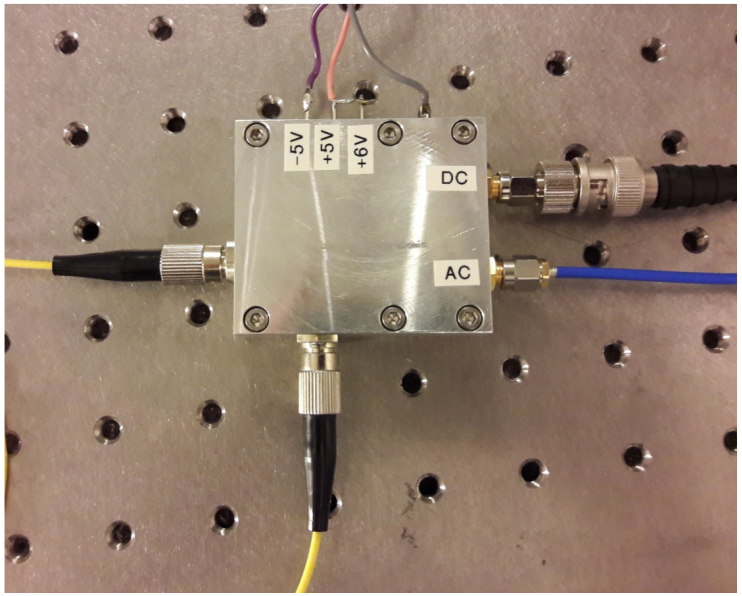
Experimental Setup

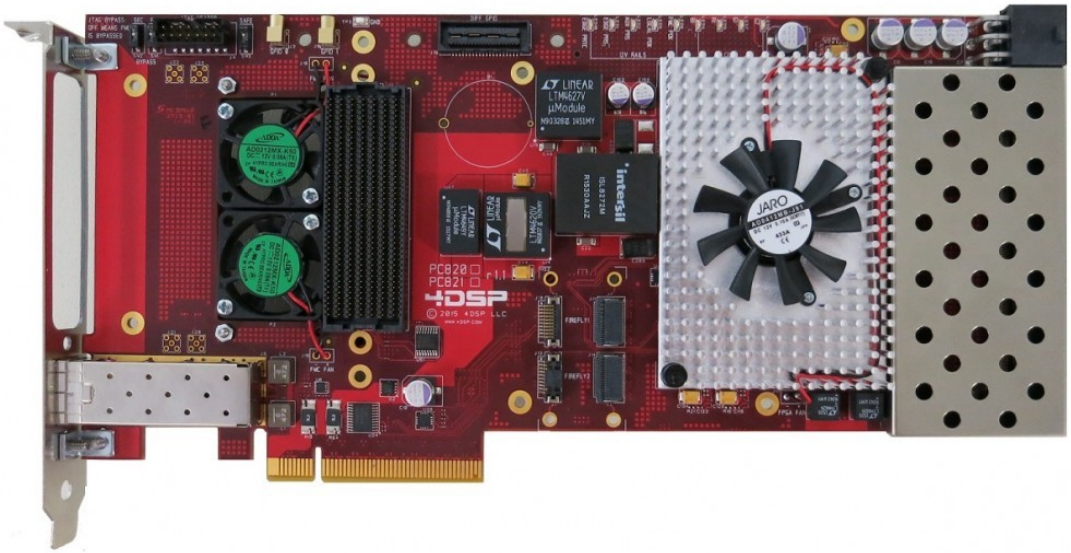




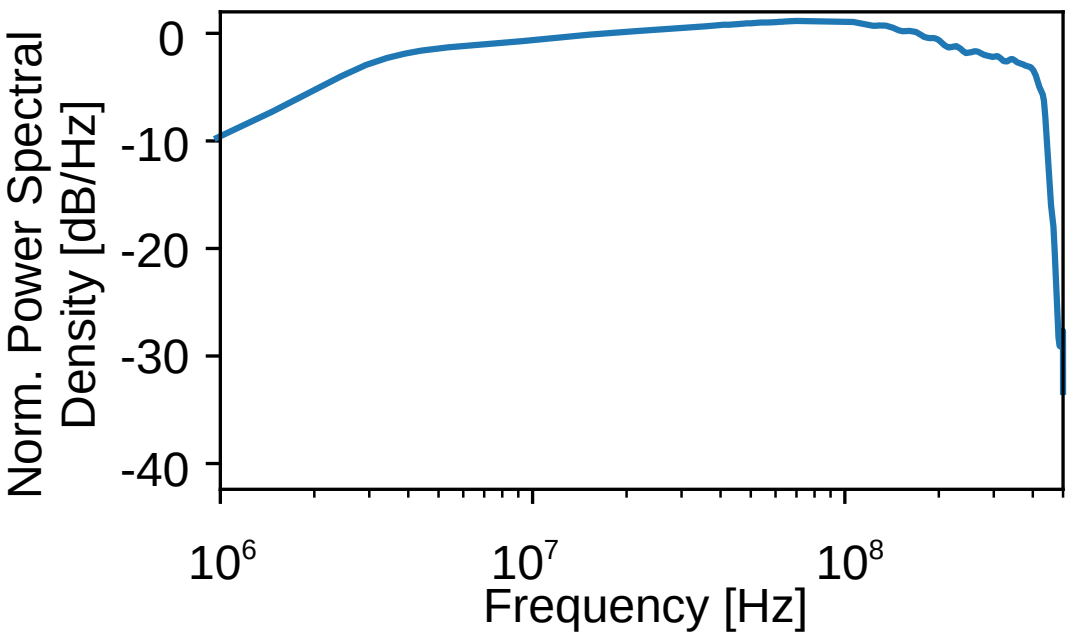
Experimental Setup

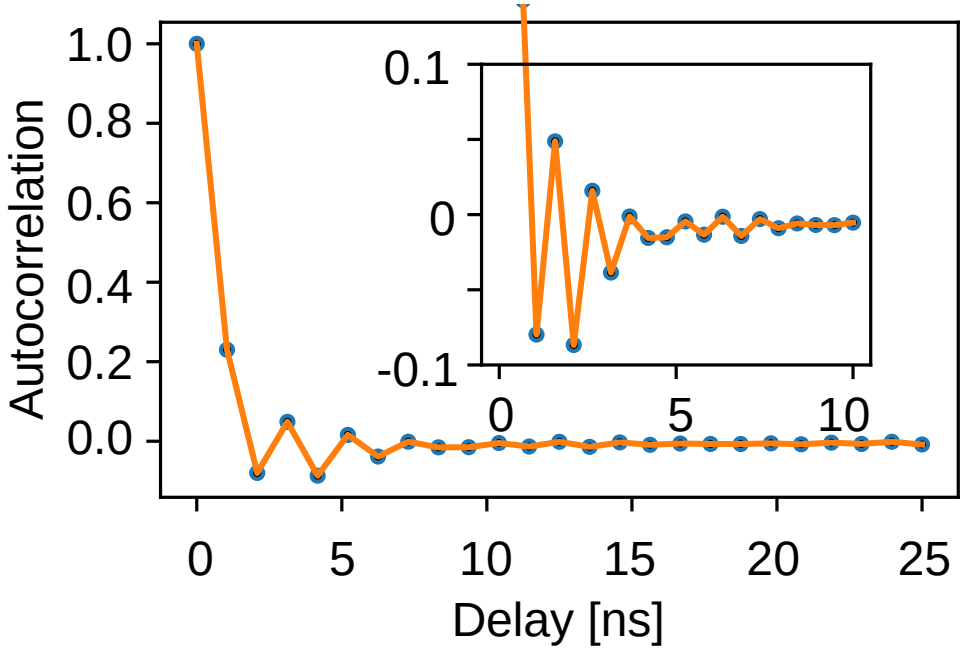




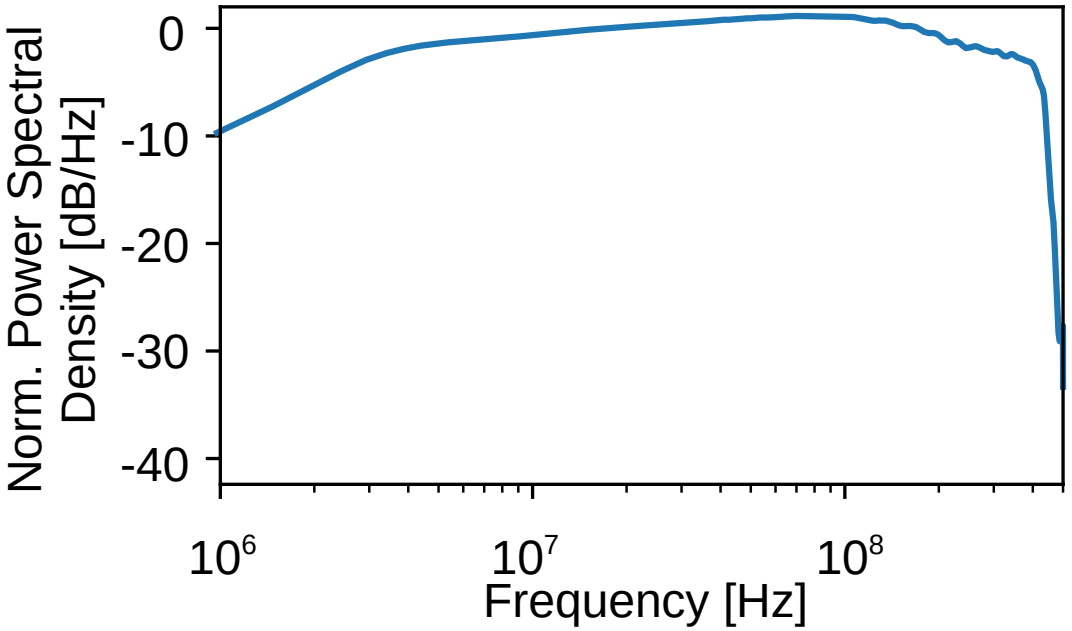


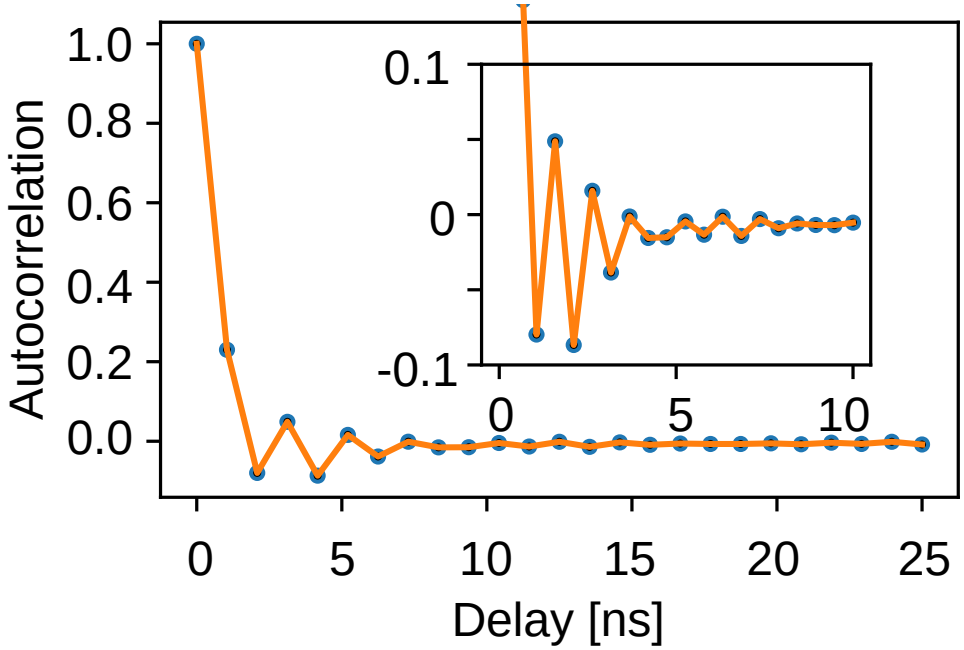
Correlated Samples





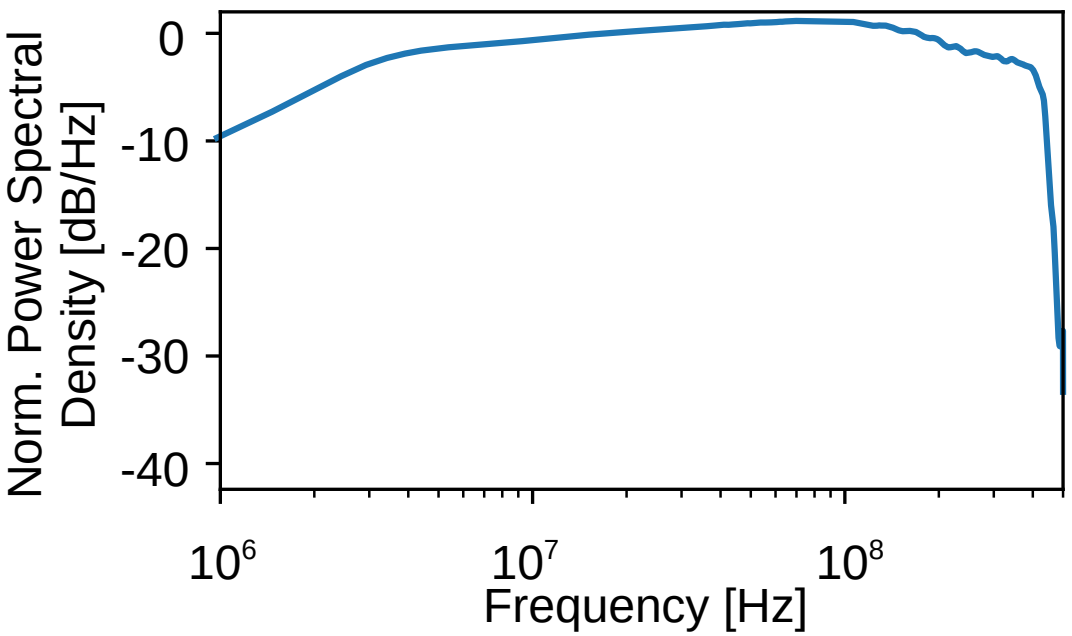
Correlated Samples

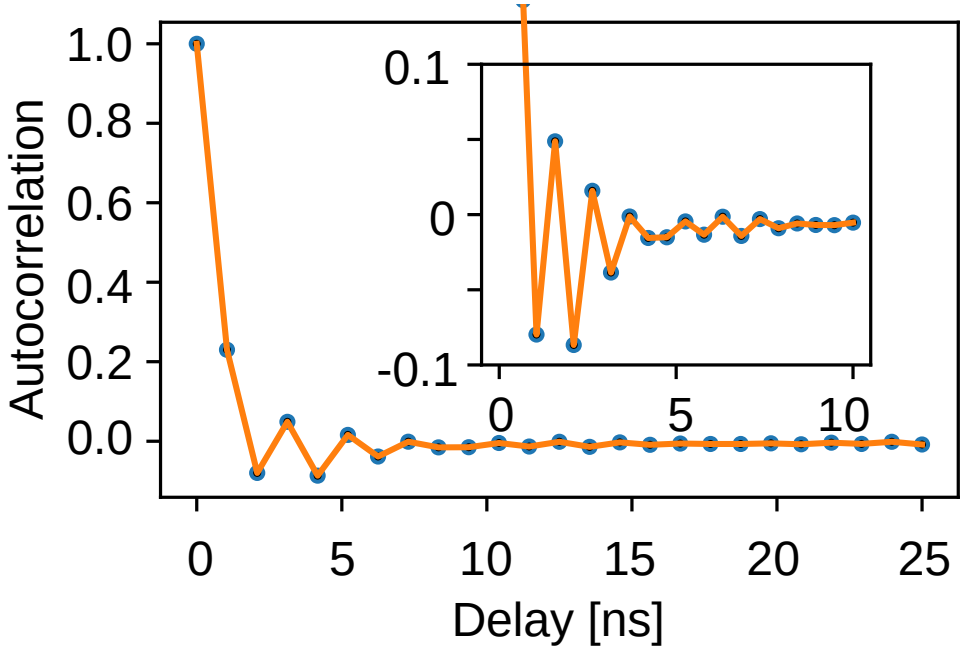




Samples are not independently distributed!

Correlated Samples

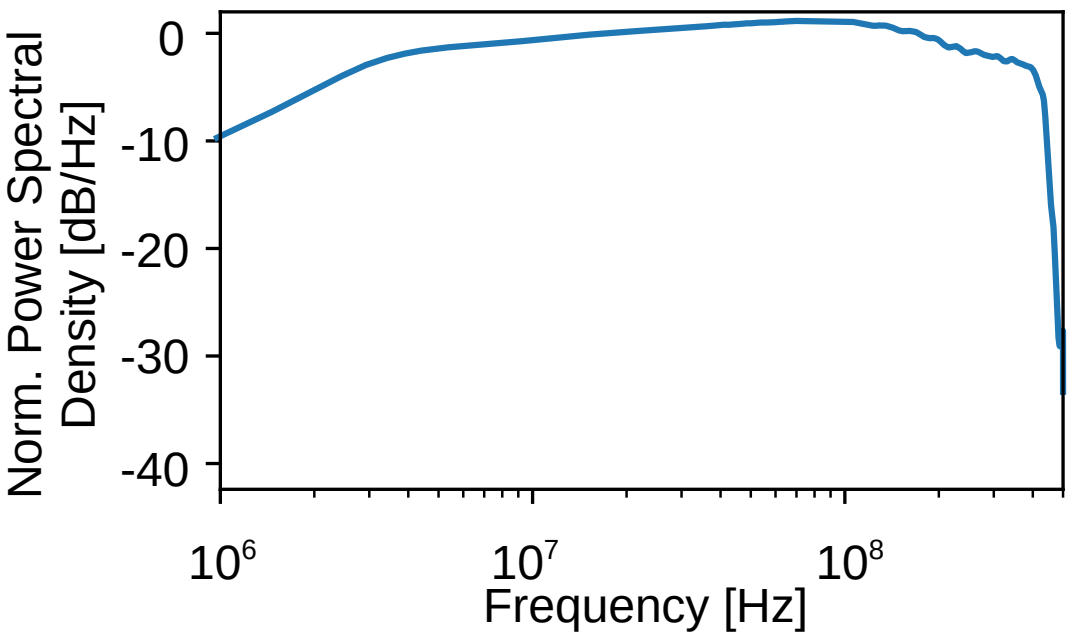


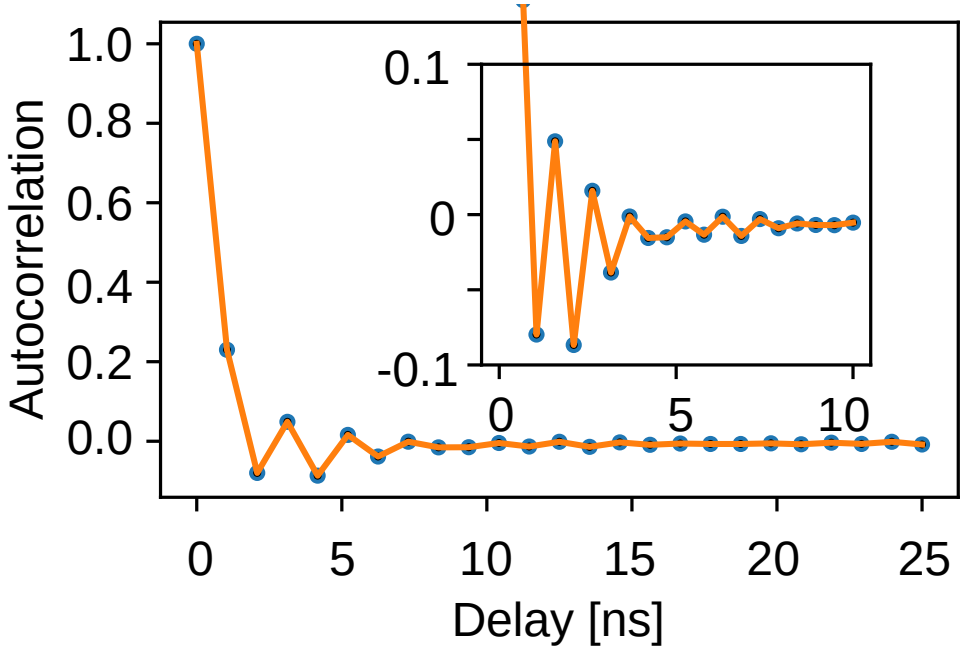


Samples are not independently distributed!

Idea: Map non-i.i.d. into i.i.d. process

Correlated Samples





Samples are not independently distributed!

Idea: Map non-i.i.d. into i.i.d. process

Conditional variance describes variance of virtual i.i.d. process

$$\sigma_X^2 = \frac{1}{2\pi e} 2^{\frac{1}{2\pi}\int_0^{2\pi} d\lambda \log[2\pi e f_X(\lambda)]}$$

Power spectral density of the signal

Metrological characterization

- Min-Entropy model has three parameters:

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal
  - Conditional variance of the excess noise

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal
  - Conditional variance of the excess noise
- Characterize all of them with confidence intervals

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal
  - Conditional variance of the excess noise

- Characterize all of them with confidence intervals
- Take the minimum min-entropy which is compatible with the confidence intervals

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal
  - Conditional variance of the excess noise

} "Simple"

- Characterize all of them with confidence intervals
- Take the minimum min-entropy which is compatible with the confidence intervals

Metrological characterization

- Min-Entropy model has three parameters:
  - Variance of the signal
  - Conditional variance of the signal

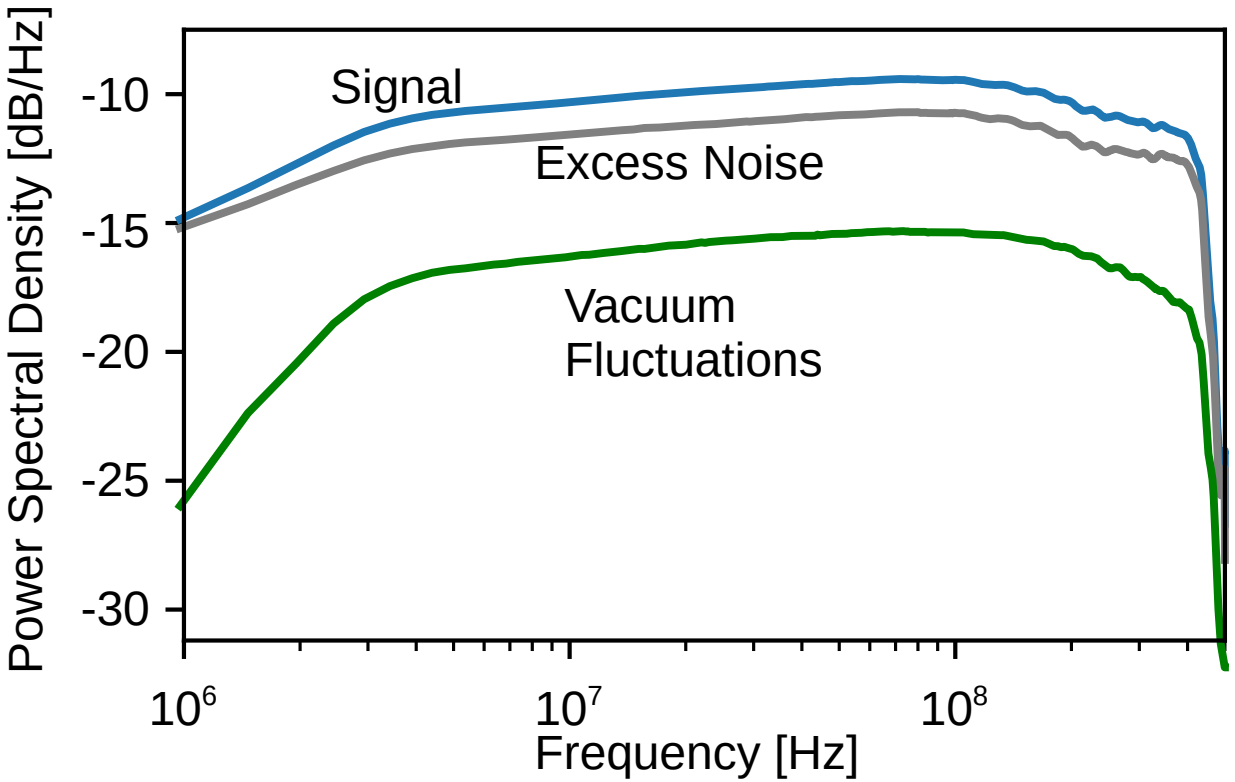
  } "Simple"

  - Conditional variance of the excess noise

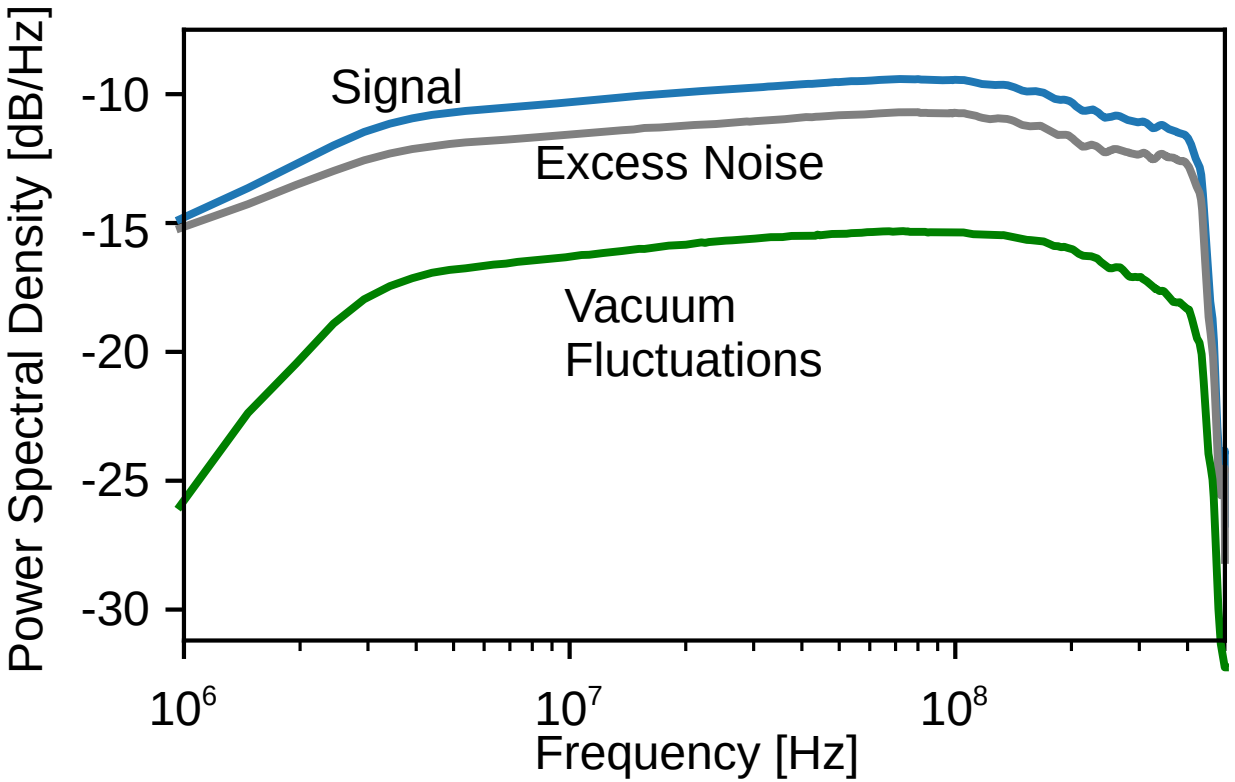
  } "Hard"

- Characterize all of them with confidence intervals
- Take the minimum min-entropy which is compatible with the confidence intervals

Metrological-Grade Characterization

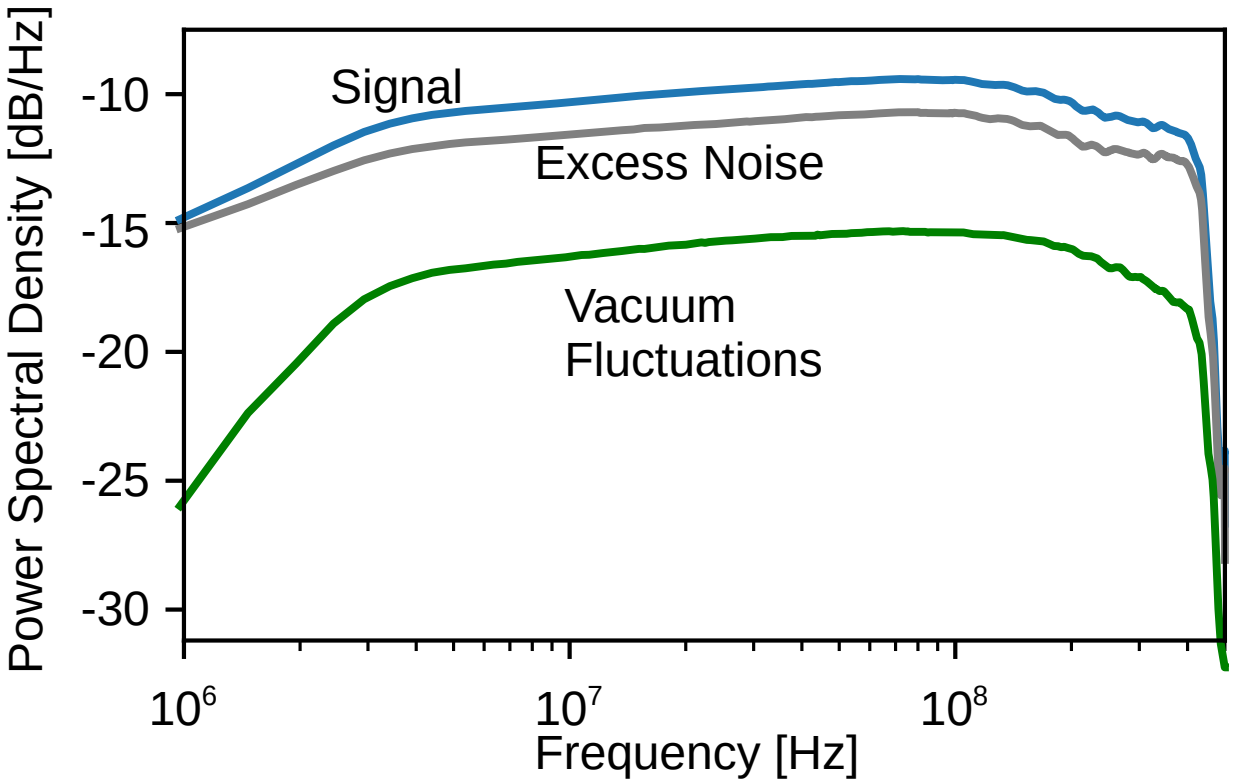


Metrological-Grade Characterization

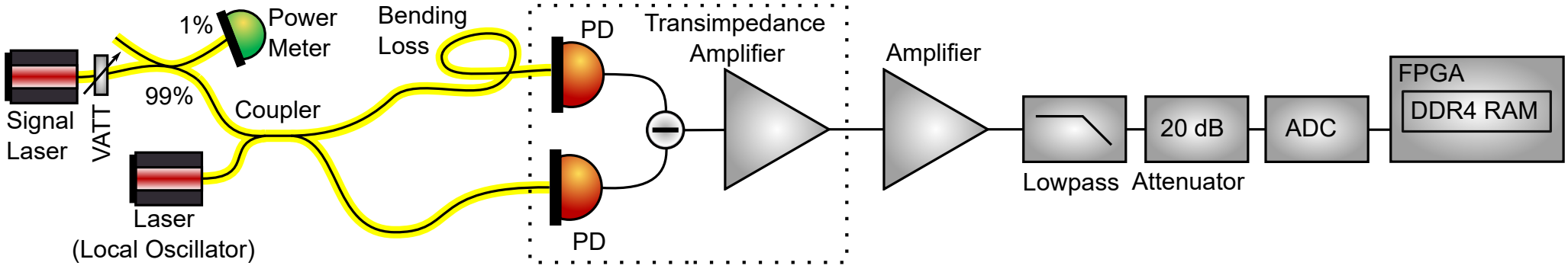


Vacuum fluctuations given by Schottky shot noise

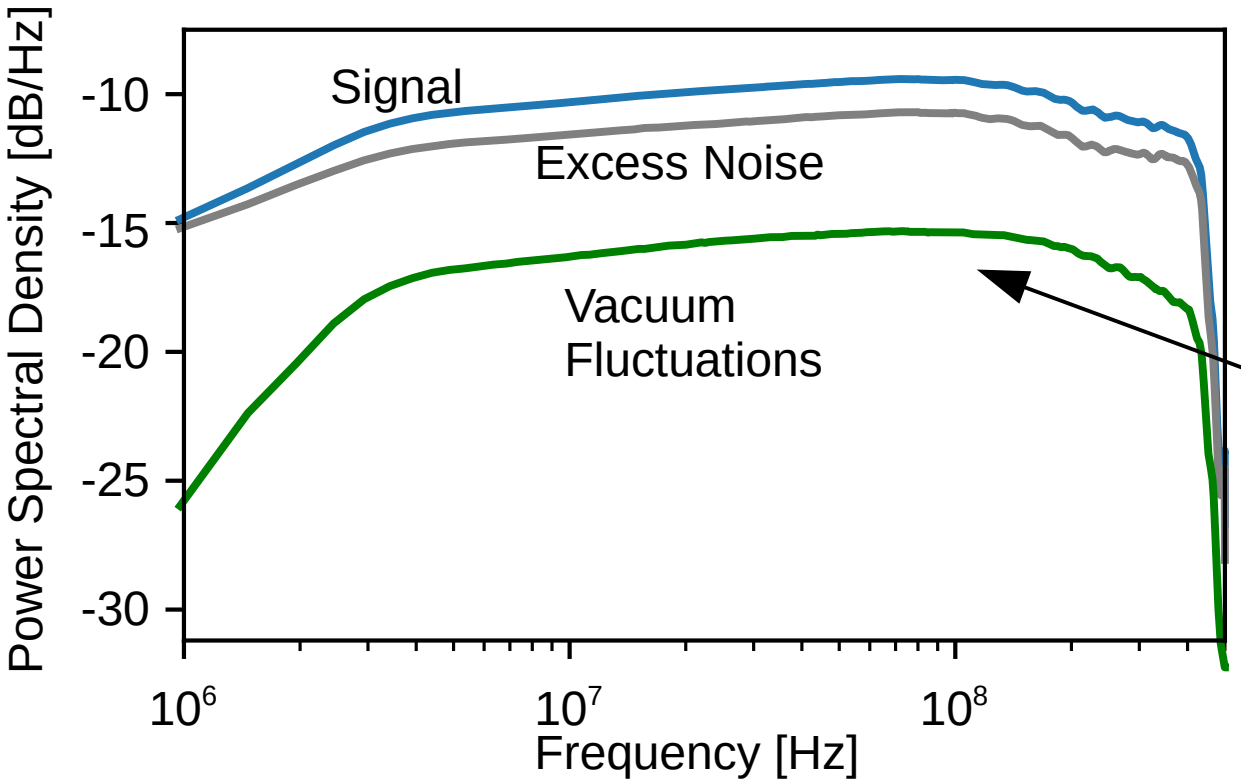
Metrological-Grade Characterization



Vacuum fluctuations given by Schottky shot noise



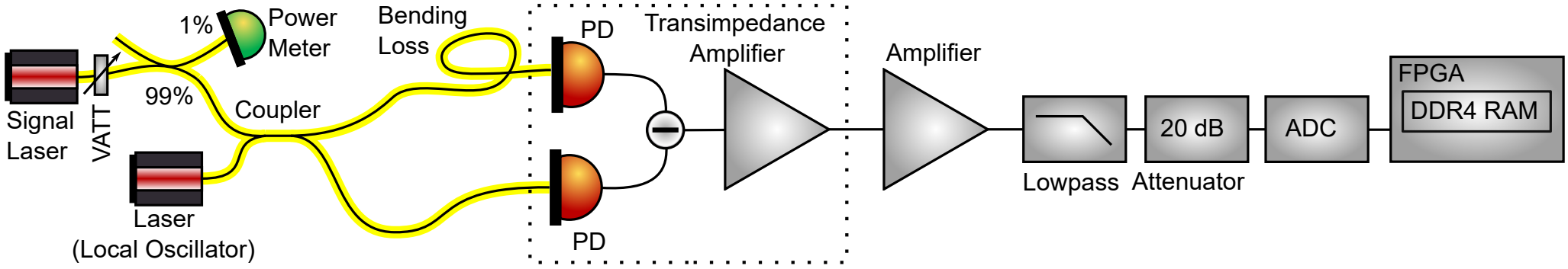
Metrological-Grade Characterization



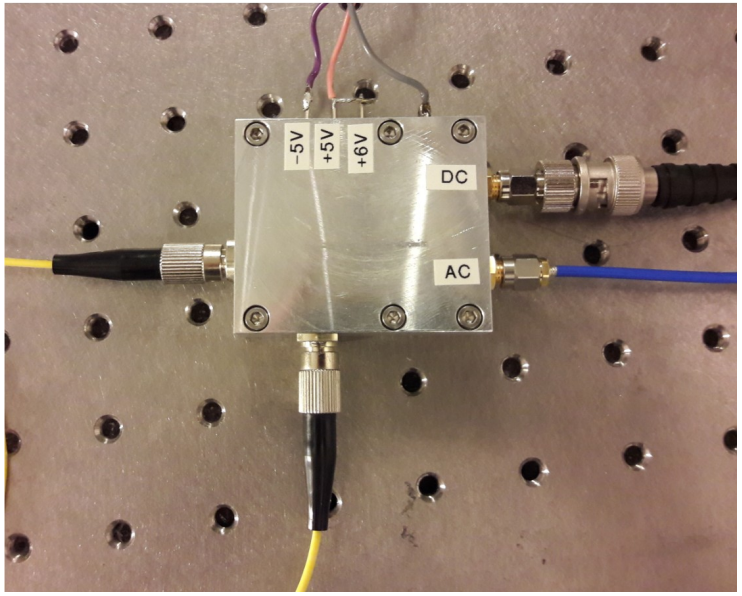
Vacuum fluctuations given by Schottky shot noise

$$\hbar\omega_L \frac{\mathrm{TF}(\Omega)}{P_{\mathrm{sig}}}$$

Lower bound as
- Visibility = 1
- Quantum efficiency = 1



Summary



Real-time QRNG suitable for high speed QKD

- Min-Entropy: 11.4 bit per 16 bit sample
- Real-time randomness extraction: 10.67 Gbit/s
- Metrological characterization: $\epsilon_{\mathrm{PE}} = 10^{-12}$

$$N\epsilon_{\mathrm{hash}} + \epsilon_{\mathrm{PE}} + \epsilon_{\mathrm{seed}} = N \cdot 10^{-36} + 10^{-12} + \epsilon_{\mathrm{seed}}$$

QRNG runs in the past

Outlook

- Where to get good seed bits from? DI-QRNG?
- Integration into a package suitable for QKD integration
- Online tests
- Power-on self-tests