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
The need for random numbers

Poster 49
The need for random numbers

Certified Security

Unpredictable / Private
The need for random numbers

Certified Security
Unpredictable / Private
Fast real-time generation
The need for random numbers

Many other applications:

- Simulations
- Gambling
- Classical Key Generation
- etc
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?

Source

Detector

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?

- **Source-Independent**
  - More assumptions

- **Device-Independent**

- **Device Dependent**
  - Local Oscillator
  - Signal
  - 50:50

- **Source**
Vacuum fluctuations
quantum random number
generator with non-iid samples

Tobias Gehring¹, Arne Kordts¹, Dino Solar Nikolic¹, Nitin Jain¹,
Cosmo Lupo², Stefano Pirandola², Thomas B. Pedersen³,
Ulrik L. Andersen¹

1) Department of Physics, Technical University of Denmark, Denmark
2) Department of Computer Science, University of York, UK
3) Cryptomathic A/S, Denmark
Experimental Setup

Vacuum fluctuations quantum random number generator with non-iid samples
Vacuum fluctuations quantum random number generator with non-iid samples
Experimental Setup

Vacuum fluctuations quantum random number generator with non-iid samples
Vacuum fluctuations quantum random number generator with non-iid 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

Vacuum fluctuations quantum random number generator with non-iid samples
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

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

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

  \[
  \{\text{Simple}\}
  \]

- 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
  - Conditional variance of the excess noise

  } “Simple”

  } “Hard”

- Characterize all of them with confidence intervals

- Take the minimum min-entropy which is compatible with the confidence intervals
Metrological-Grade Characterization

Vacuum fluctuations quantum random number generator with non-iid samples
Vacuum fluctuations quantum random number generator with non-iid samples

Metrological-Grade Characterization

Vacuum fluctuations given by Schottky shot noise

Power Spectral Density [dB/Hz]

Signal

Excess Noise

Vacuum Fluctuations

Frequency [Hz]

10^6 10^7 10^8
Vacuum fluctuations quantum random number generator with non-iid samples

Metrological-Grade Characterization

Vacuum fluctuations given by Schottky shot noise

Power Spectral Density [dB/Hz]

Signal

Excess Noise

Vacuum Fluctuations

Frequency [Hz]

10^6

10^7

10^8

-10

-15

-20

-25

-30

Vacuum Fluctuations given by Schottky shot noise

<table>
<thead>
<tr>
<th>Power</th>
<th>Meter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Laser</th>
</tr>
</thead>
<tbody>
<tr>
<td>99%</td>
</tr>
</tbody>
</table>

(Local Oscillator)

10^6

10^7

10^8

FPGA

DDR4 RAM

Lowpass

20 dB

Attenuator

ADC

Vacuum fluctuations quantum random number generator with non-iid samples
Vacuum fluctuations quantum random number generator with non-iid samples

Metrological-Grade Characterization

Vacuum fluctuations given by Schottky shot noise

\[ \hbar \omega_L \frac{\text{TF}(\Omega)}{P_{\text{sig}}} \]

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

Vacuum Fluctuations

Excess Noise

Signal

Power Spectral Density [dB/Hz]

Frequency [Hz]

-10
-15
-20
-25
-30

10^6
10^7
10^8

10^6
10^7
10^8

Vacuum Fluctuations

Excess Noise

Signal

Power Spectral Density [dB/Hz]

Frequency [Hz]

10^6
10^7
10^8

Lowpass

Attenuator

FPGA

DDR4 RAM

Power Meter

Coupler

Bending Loss

Transimpedance Amplifier

Amplifier

ADC

Vacuum fluctuations quantum random number generator with non-iid samples
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: $\epsilon_{PE} = 10^{-12}$

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

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