Secure heterodyne-based QRNG at 17 Gbps

Marco Avesani¹ Davide G. Marango¹*, Giuseppe Vallone¹,², Paolo Villoresi¹,²

¹ Department of Information Engineering, Università degli Studi di Padova
² Istituto di Fotonica e Nanotecnologie, CNR, Padova
* Now at Toshiba CRL

QCrypt 2018, Shanghai

arXiv:1801.04139
Tradeoffs in QRNG

Based on N. Brunner, QCrypt2015
Tradeoffs in QRNG

- Reach up to 68 Gbps
- Need to trust every element
- Side-information leakage if deviation from the model


Based on N. Brunner, QCrypt2015
Tradeoffs in QRNG

- Reach up to 68 Gbps
- Need to trust every element
- Side-information leakage if deviation from the model

- Security certified by nonlocality
- No assumptions: black box devices
- Complex and slow: 181 bps

Device-Independent

Security / Paranoia

A good compromise?

Weaker assumptions

Semi Device-Independent

[5-8]

Device-Independent

Security / Paranoia

Gbps

Speed

bps

Based on N. Brunner, QCrypt2015

References:
Our goal!

Based on N. Brunner, QCrypt2015
Source Device-Independent scenario: the protocol

Eve has **full control** on the **source**: she and Alice can share any bipartite states at each round.

- Valid for any set of POVM implemented by Alice
- The POVM are **trusted**, but don’t need to be **ideal**
- The key element is the **quantum conditional min-entropy**, $H_{\min}(X | \mathcal{E})$: it takes into account **quantum side-information for a single-shot**
- Use the **Leftover Hashing Lemma** to get the secure numbers [1]

Randomness estimation (for CV systems)

The amount of private randomness is given by:

\[ H_{\text{min}}(X|\mathcal{E}) = -\log_2(P_{\text{guess}}(X|\mathcal{E})) \]

\[ P_{\text{guess}}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \text{Tr}[\Pi_A^x \tau_\beta] d\beta \]

s.t. \( \rho_A = \int p(\beta) \tau_\beta d\beta \)

Represents Eve’s probability of correctly guessing Alice’s output.
Randomness estimation (for CV systems)

The amount of private randomness is given by:

\[ H_{min}(X|\mathcal{E}) = -\log_2(P_{\text{guess}}(X|\mathcal{E})) \]

Represents Eve's probability of correctly guessing Alice's output.

\[ P_{\text{guess}}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \text{Tr}[\Pi_A^x \tau_\beta] d\beta \]

All possible decompositions of Alice state.

Not useful for projective measurements, but for overcomplete POVM...
Randomness estimation for Heterodyne detection

Heterodyne POVM = \[ \Pi = \frac{1}{\pi} |\alpha\rangle\langle \alpha| \]

**Overcomplete** set POVM, projection on coherent states
Heterodyne POVM = \( \Pi = \frac{1}{\pi} |\alpha\rangle\langle \alpha| \)

**Overcomplete** set POVM, projection on coherent states
Randomness estimation for Heterodyne detection

Heterodyne POVM = \( \Pi = \frac{1}{\pi} |\alpha\rangle\langle\alpha| \)

**Overcomplete** set POVM, projection on coherent states
Randomness estimation for Heterodyne detection

Heterodyne POVM = \[ \Pi = \frac{1}{\pi} |\alpha\rangle\langle\alpha| \]

**Overcomplete** set POVM, projection on coherent states
Randomness estimation for Heterodyne detection

Heterodyne POVM = $\Pi = \frac{1}{\pi} |\alpha\rangle \langle \alpha |$

**Overcomplete** set POVM, projection on coherent states
Randomness estimation for Heterodyne detection

Heterodyne POVM = \( \Pi = \frac{1}{\pi} |\alpha\rangle \langle \alpha| \)

**Overcomplete** set POVM, projection on coherent states

The **overlap** of the POVM introduces randomness!
Randomness estimation for Heterodyne detection

Heterodyne POVM = \( \Pi = \frac{1}{\pi} |\alpha\rangle\langle\alpha| \)

**Overcomplete** set POVM, projection on coherent states

The **overlap** of the POVM introduces randomness!

\[
P_{\text{guess}}(X|\mathcal{E}) \leq \max_{x, \tau_w \in \mathcal{H}_A} \text{Tr}[\Pi_A^x \tau_w] = \max_{\alpha, \tau_w \in \mathcal{H}_A} \frac{1}{\pi} \text{Tr}[|\alpha\rangle\langle\alpha| \tau_w] = \max_{\alpha, \tau_w \in \mathcal{H}_A} Q_{\tau_w}(\alpha) = \frac{1}{\pi}
\]

\[Q_\rho(\alpha)\] Is the Husimi Q-Function and is **always bounded** \(0 \leq Q_\rho(\alpha) \leq \frac{1}{\pi}\) [1]

Randomness estimation for Heterodyne detection

Heterodyne POVM = \( \Pi = \frac{1}{\pi} |\alpha\rangle\langle\alpha| \)

**Overcomplete** set POVM, projection on coherent states

The **overlap** of the POVM introduces randomness!

\[
P_{\text{guess}}(X|\mathcal{E}) \leq \max_{x,\tau_w \in \mathcal{H}_A} \text{Tr}[\Pi_A^x \tau_w] = \max_{\alpha,\tau_w \in \mathcal{H}_A} \frac{1}{\pi} \text{Tr}[|\alpha\rangle\langle\alpha|\tau_w] = \max_{\alpha,\tau_w \in \mathcal{H}_A} Q_{\tau_w}(\alpha) = \frac{1}{\pi}
\]

\( Q_\rho(\alpha) \) is the Husimi Q-Function and is **always bounded** \( 0 \leq Q_\rho(\alpha) \leq \frac{1}{\pi} \) [1]

Taking into account finite measurement resolution in the phase space

\[
P_{\text{guess}}(X|\mathcal{E}) \leq \frac{\delta P \delta Q}{\pi} \quad \longrightarrow \quad H_{\text{min}}(X|\mathcal{E}) = \log_2 \left( \frac{\pi}{\delta P \delta Q} \right)
\]

Key differences

- **No input randomness** required!
- Randomness **doesn’t depend on the measured statistics**. The **structure of the POVM** allows to bound the randomness a priori.
- Great simplification for real-time extractors
- Single-shot entropy measure + no estimations \( \rightarrow \) **no finite size effects**

\[ H_{\text{min}}(X|\mathcal{E}) = \log_2 \left( \frac{\pi}{\delta P \delta Q} \right) \]

The experimental implementation

- The source is **untrusted**: we use the simplest, the vacuum $|0\rangle$
- **The heterodyne detection (or double homodyne)** samples the two quadratures using a reference Local Oscillator (LO): **1550 nm** ECL laser
- The **LO is measured in real-time** to compensate for fluctuation
- For detection, two balanced InGaS detectors (**1.6 GHz BW**) are
- The two **quadrature** RF signals are **digitalized** by an **10 bit 4Ghz Oscilloscope** at 10 Gsps in burst mode, then filtered
- **Electronic noise** is treated as noise on the source: **not trusted**
- Finally, a **Toeplitz Randomness Extractor** calibrated on the min-entropy is used to **extract** the secure numbers

$$H_{\min}(X|\mathcal{E}) = \log_2 \left( \frac{\pi}{\delta P \delta Q} \right)$$

Z = 01010100001
Secure generation rate:

Resolution: 10-bit $\delta Q = (14,05 \pm 0,02) \cdot 10^{-3}$, $\delta P = (14,14 \pm 0,02) \cdot 10^{-3}$

Min-entropy: $H_{\text{min}}(X|\mathcal{E}) \geq 13,949$ bits per sample

Effective sampling rate: 1.25 GSp/s

Secure rate: $R \geq 1.25 \cdot 10^9 \cdot H_{\text{min}}(X|\mathcal{E})$ bits

$R \geq 17,42$ Gbps
Conclusions & Outlook

Theory:
• We have proposed a new Source Device-Independent protocol valid for any Discrete and Continuous variable POVM
• The protocol doesn’t require any external randomness
• Security doesn’t depend on the measured data
• Non-asymptotic

Experiment:
• Simple experimental setup
• Used only commercial off-the-shelves components
• Performance are almost on par of the best Trusted QRNG

Outlook:
• Real-time filtering and extraction
• Weaken the assumptions on the measurements
Thank you for the attention!

Secure heterodyne-based quantum random number generator at 17 Gbps

arXiv:1801.04139
Backup
Calibration

Calibration is necessary to **link** the measured variances in **Volts** to the quantities in the **phase space**

The relation is given by

\[ \sigma_{q}^2 = \frac{\sigma_V^2}{k \cdot P_{LO}} \]

Where \( k \) is the angular coefficient given by the linear regression, while the intercept is linked to the electronic noise and is not trusted.

In our case:

\[
\begin{align*}
    m_1 &= (2.783 \pm 0.005 \cdot 10^{-2} \frac{V^2}{W}) \\
    q_1 &= (1.526 \pm 0.005 \cdot 10^{-5} V^2) \\
    m_2 &= (2.748 \pm 0.004 \cdot 10^{-2} \frac{V^2}{W}) \\
    q_2 &= (1.419 \pm 0.004 \cdot 10^{-5} V^2)
\end{align*}
\]
Filtering & Autocorrelation

The electric signals coming from the balanced detectors are sampled at 10 GSps and digitally filtered using a brick-wall filter.

We keep a 1.25 GHz window centered around 875 MHz to improve the SNR. The gap is always higher than 9.6 dB.

Filtering in the spectral domain induces correlation in the time domain, as expected from Wiener-Khinchin.

Correlation is removed, downsampling at 1.25 GSps, matching the first zero of the autocorrelation.
Finite resolution POVM

Every practical Heterodyne POVM has a finite resolution:

\[ \hat{\Pi}_{m,n} = \int_{m\delta_q}^{(m+1)\delta_q} dRe(\alpha) \int_{n\delta_p}^{(n+1)\delta_p} dIm(\alpha) \hat{\Pi}_\alpha \]

\[ P_{\text{guess}}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \text{Tr}[\Pi_{m,n}^{\delta} \tau_\beta] d\beta \]

Is a well defined probability....

In the limit \( \delta_q \delta_p \to 0 \) we get the differential quantum min-entropy

\[ h_{\text{min}}(X|\mathcal{E}) = \lim_{\delta_q \delta_p \to 0} [H_{\text{min}}(X|\mathcal{E}) + \log_2(\delta_q \delta_p)] \]

\[ p_{\text{guess}}(X|\mathcal{E}) = 2^{-h_{\text{min}}(X|\mathcal{E})} \]

Which is a probability density function.
The expression of the guessing probability is equivalent to the one introduced in [1]

\[
P_{\text{guess}}(X|\mathcal{E}) = \max_{\{\hat{E}_\beta\}} \sum_x P_X(x) \text{Tr} \left[ (\hat{E}_\beta \rho_x^E) \right]
\]

Intuitively, the states \(\hat{t}_\beta\) can be seen as the reduced post-measurement states that Eve sends to Alice after having applied her POVM \(\hat{E}_\beta\) on the bipartite state

\[
\hat{t}_\beta = \frac{\text{Tr}_E \left[ (1_A \otimes \hat{E}_\beta) \rho_{AE} \right]}{\text{Tr} \left[ (1_A \otimes \hat{E}_\beta) \rho_{AE} \right]}
\]

Side-Information

Trusted model

Eve controls the source

They have the same output statistics, and Alice cannot distinguish between the two

The **privacy** of the random numbers is completely **compromised**!