Secure heterodyne-based QRNG at 17 Gbps

Marco Avesani[1] Davide G. Marangon[1*], Giuseppe Vallone[1,2], Paolo Villoresi[1,2]

[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

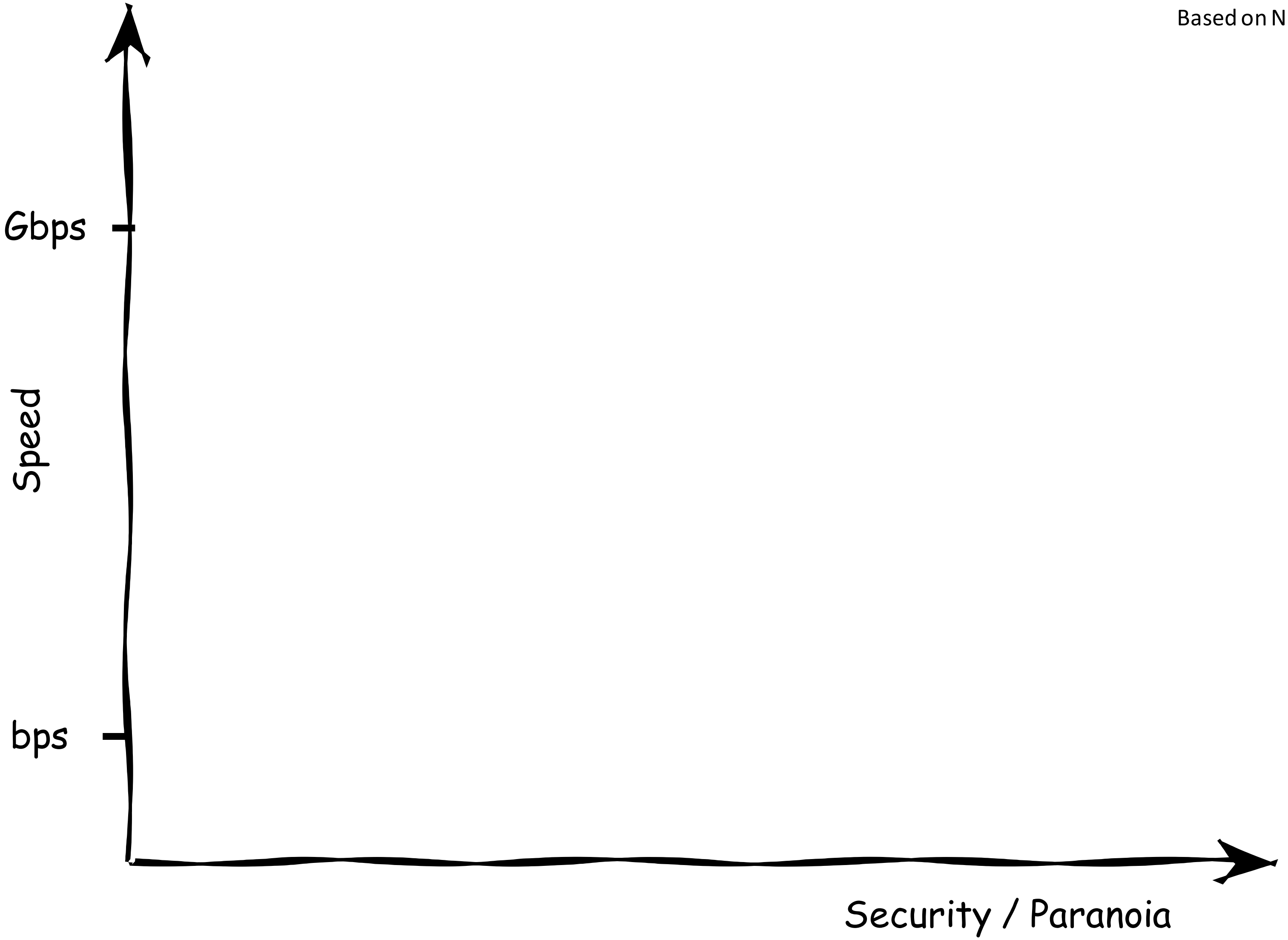
arXiv:1801.04139

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

UNIVERSITÀ DEGLI STUDI DI PADOVA

Tradeoffs in QRNG

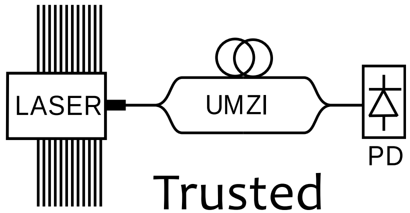
Based on N.Brunner, QCrypt2015



Tradeoffs in QRNG

Based on N.Brunner, QCrypt2015

Gbps



Trusted
[1][2]

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

Speed

bps

Security / Paranoia

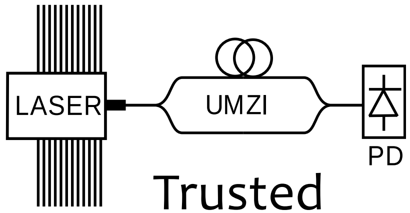
[1] C. Abellán *et al.*, *Opt. Express*, 22, 1645,(2014).
[2] Y. Q. Nie *et al.*, *Rev. Sci. Instrum.*, 86, 6,(2015.)

Tradeoffs in QRNG

Based on N.Brunner, QCrypt2015

Speed

Gbps

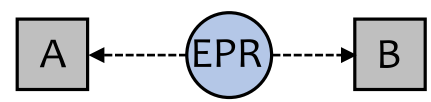


Trusted
[1][2]

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

bps

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



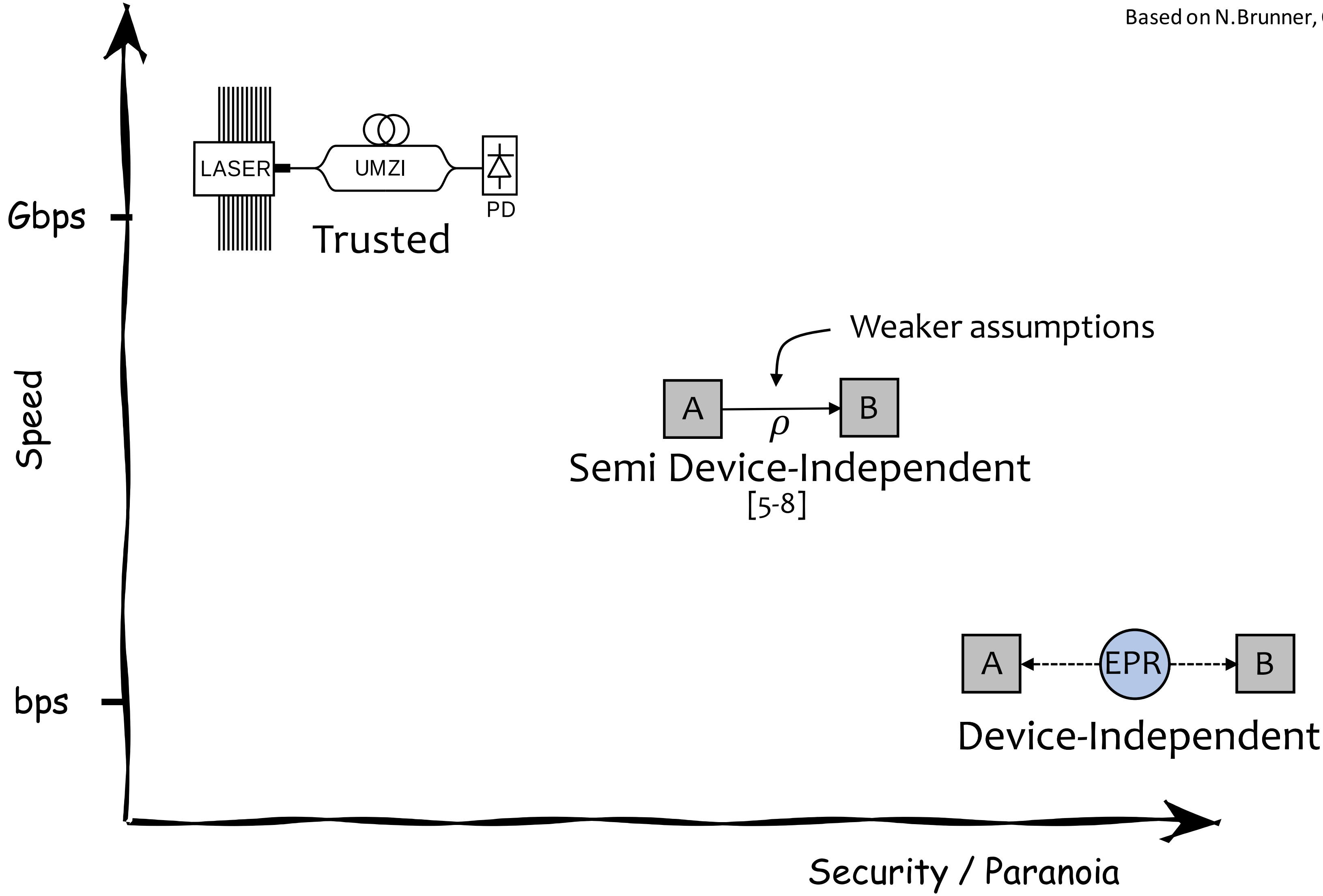
Device-Independent
[3][4]

Security / Paranoia

[1] C. Abellán *et al.*, *Opt. Express*, 22, 1645,(2014).
[2] Y. Q. Nie *et al.*, *Rev. Sci. Instrum.*, 86, 6,(2015.)
[3] Y. Liu *et al.*, arXiv:1807.09611v2, 2018.
[4] P. Bierhorst *et al.*, *Nature*, 556,7700, (2018).

A good compromise?

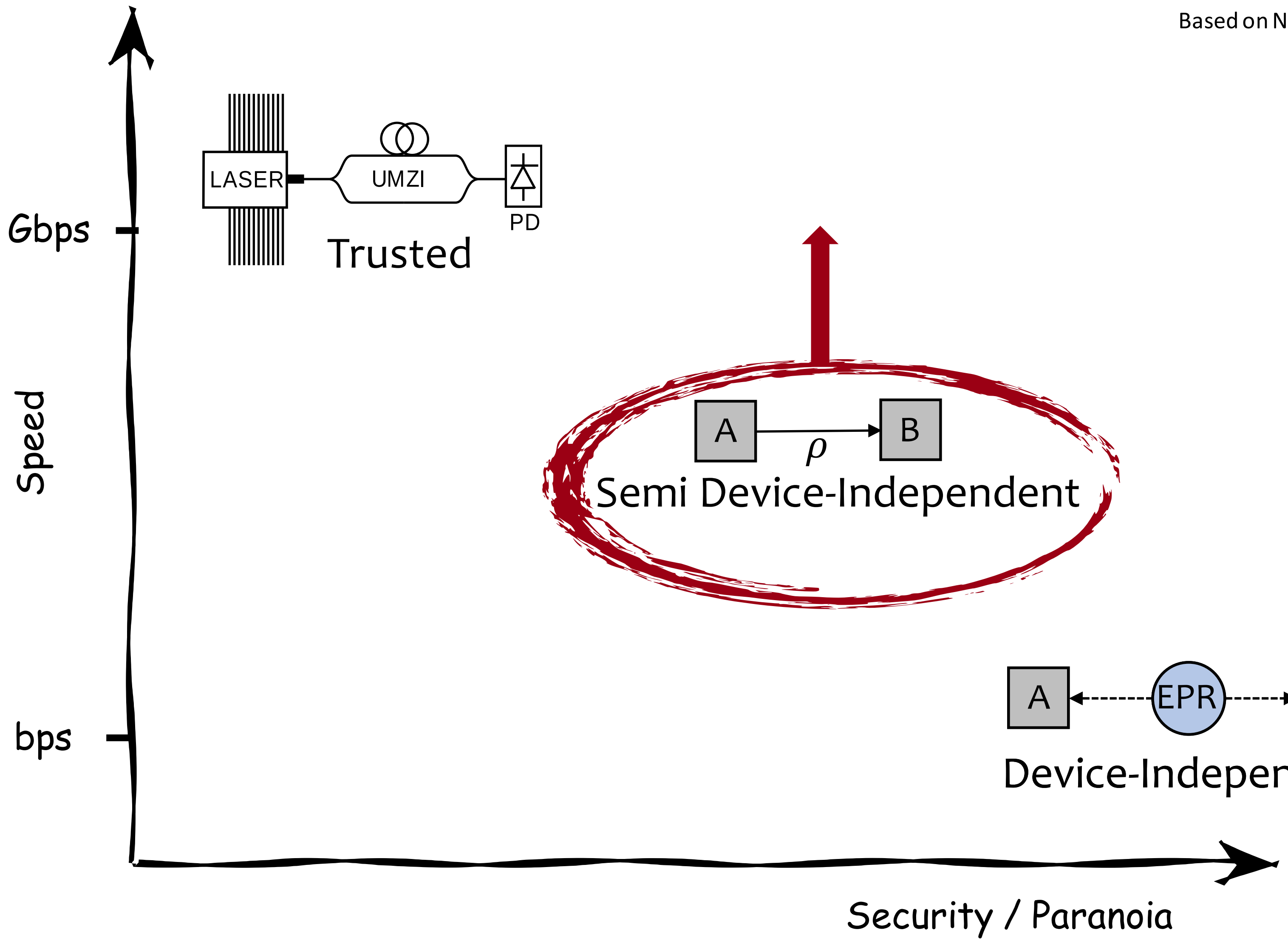
Based on N.Brunner, QCrypt2015



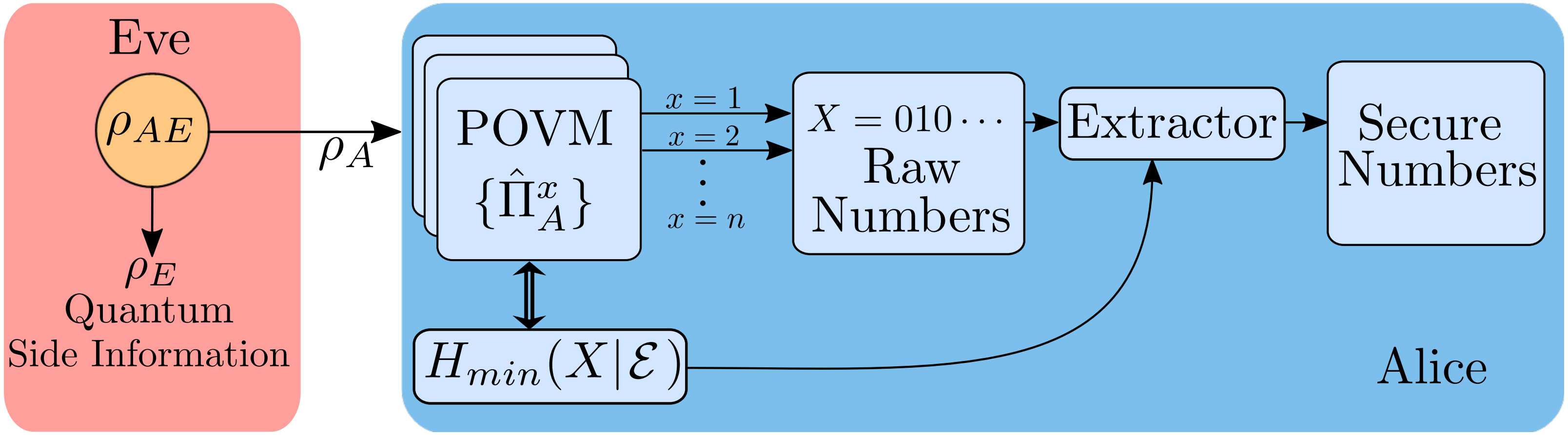
[5] T. Lunghi et al., Phys. Rev. Lett., 114, 150501, (2015).
[6] D. G. Marangon et al., Phys. Rev. Lett., 118, 060503, (2017).
[7] J. B. Brask et al., Phys. Rev. Appl., 7, 54018, (2017).
[8] T. Van Himbeeck, et al., Quantum, 1, 33, (2017)

Our goal!

Based on N.Brunner, QCrypt2015



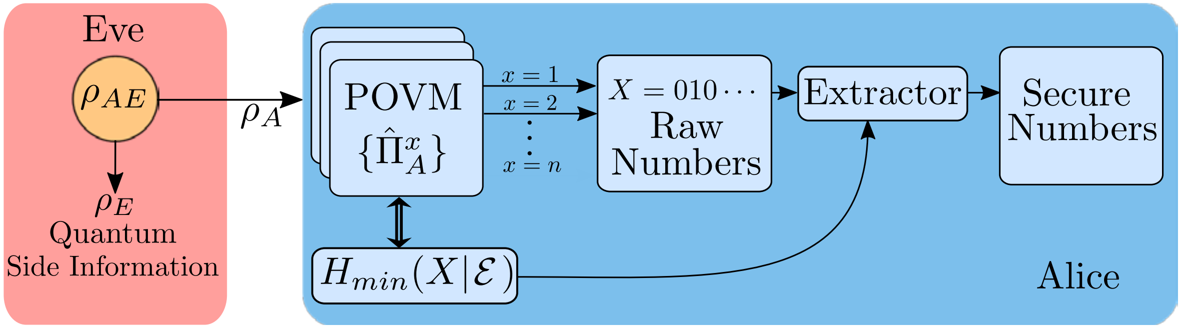
Source Device-Independent scenario: the protocol



- Eve has **full control** on the **source:** she and Alice can share **any** bipartite sates 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]

[1] M. Tomamichel, IEEE Trans. Inf. Theory, 57, (2011)

Randomness estimation (for CV systems)



The amount of private randomness is given by: $H_{min}(X|\mathcal{E}) = -\log_2(P_{guess}(X|\mathcal{E}))$

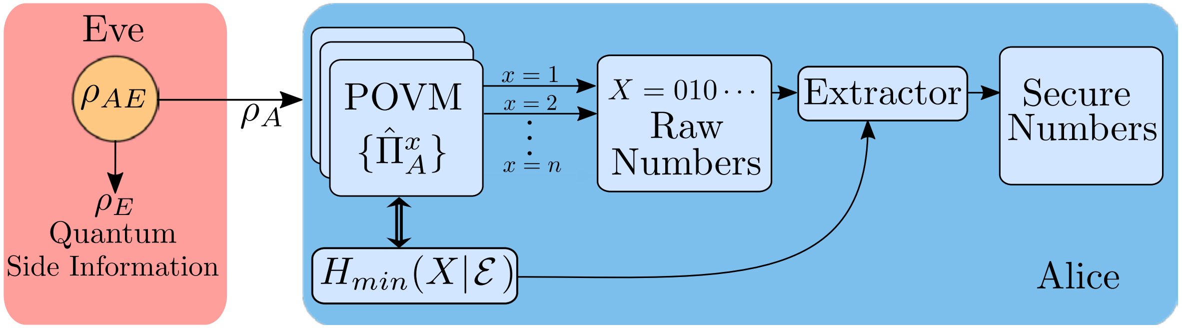
$$P_{guess}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \mathrm{Tr}[\Pi_A^x \tau_\beta]d\beta$$

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

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

All possible decompositions of Alice state

Randomness estimation (for CV systems)



The amount of private randomness is given by: $\boxed{H_{min}(X|\mathcal{E}) = -\log_2(P_{guess}(X|\mathcal{E}))}$

$$\boxed{P_{guess}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \mathrm{Tr}[\Pi_A^x \tau_\beta]d\beta}$$ s.t. $\rho_A = \int p(\beta)\tau_\beta d\beta$

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

All possible decompositions of Alice state

$$P_{guess}(X|\mathcal{E}) \leq \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_{x,\tau_w \in \mathcal{H}_A} \mathrm{Tr}[\Pi_A^x \tau_w]d\beta \leq \boxed{\max_{x,\tau_w \in \mathcal{H}_A} \mathrm{Tr}[\Pi_A^x \tau_w]}$$

Not useful for projective measurements, but for **overcomplete POVM**….

Randomness estimation for Heterodyne detection

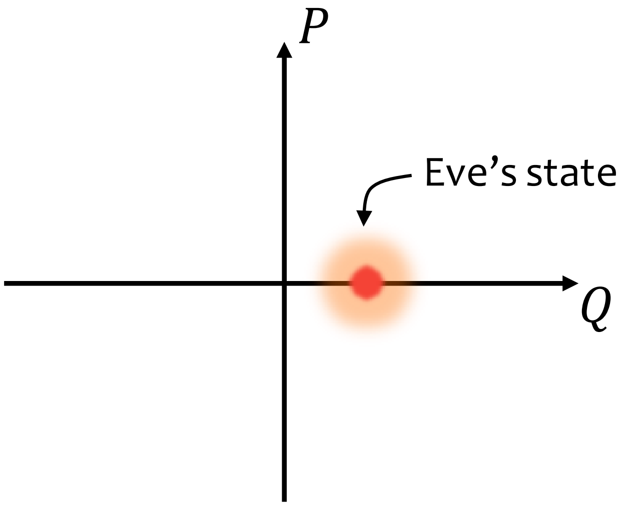
Heterodyne POVM = $\Pi = \frac{1}{\pi}|\alpha\rangle\langle\alpha|$

Overcomplete set POVM, projection on coherent states

Randomness estimation for Heterodyne detection

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

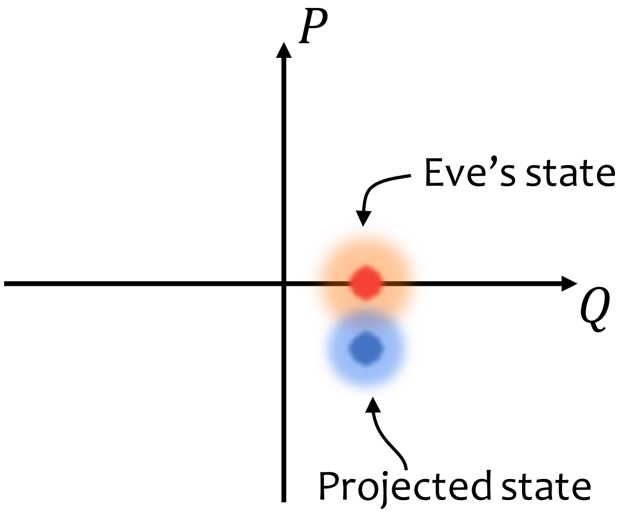
Overcomplete set POVM, projection on coherent states



Randomness estimation for Heterodyne detection

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

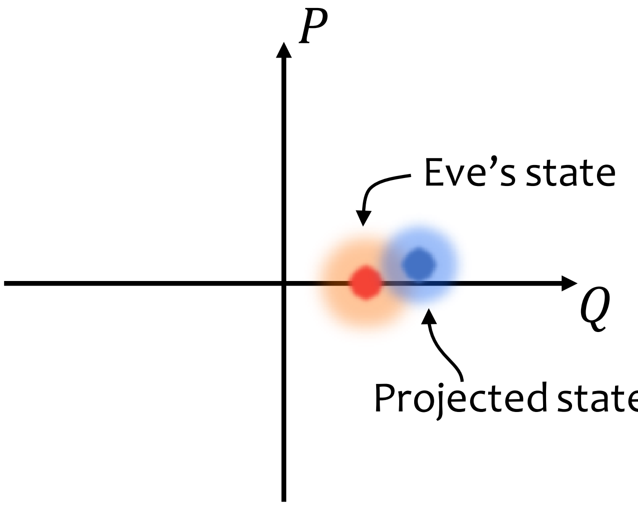
Overcomplete set POVM, projection on coherent states



Randomness estimation for Heterodyne detection

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

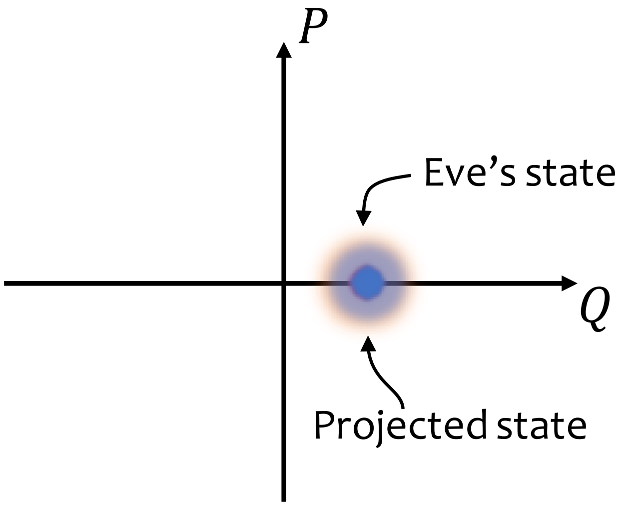
Overcomplete set POVM, projection on coherent states



Randomness estimation for Heterodyne detection

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

Overcomplete set POVM, projection on coherent states

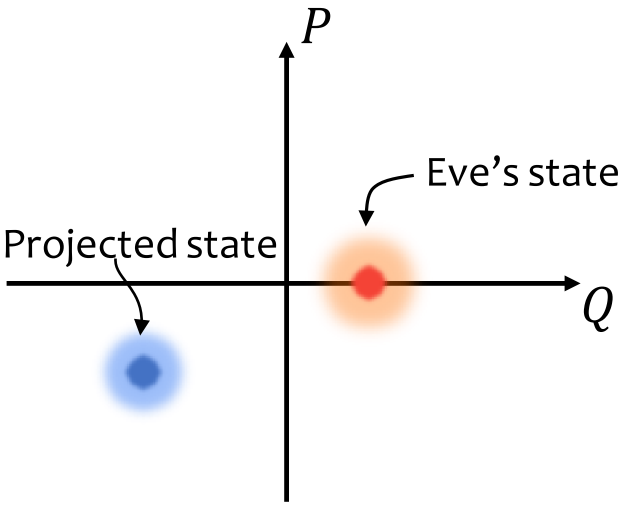


Randomness estimation for Heterodyne detection

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

Overcomplete set POVM, projection on coherent states

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

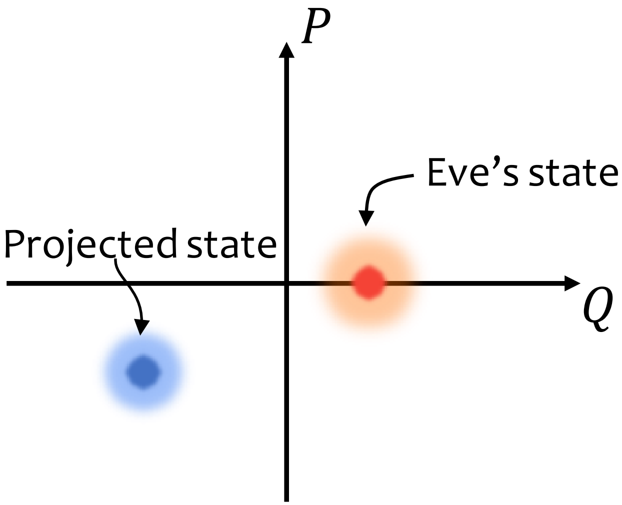


Randomness estimation for Heterodyne detection

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

Overcomplete set POVM, projection on coherent states

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



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

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

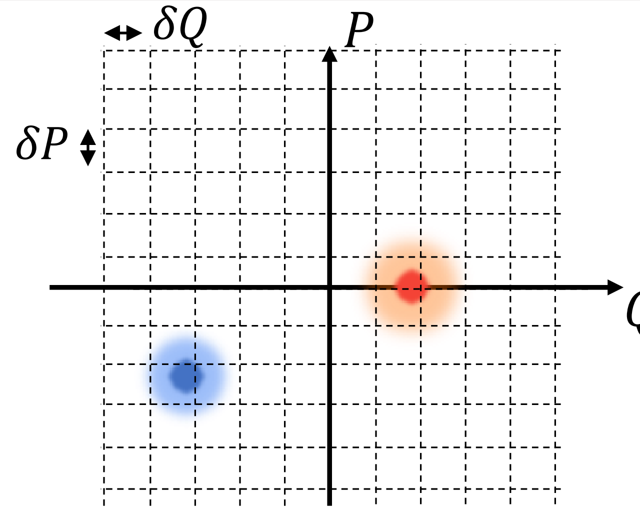
[1] U. Leonhardt, Measuring the Quantum State of Light

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!



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

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

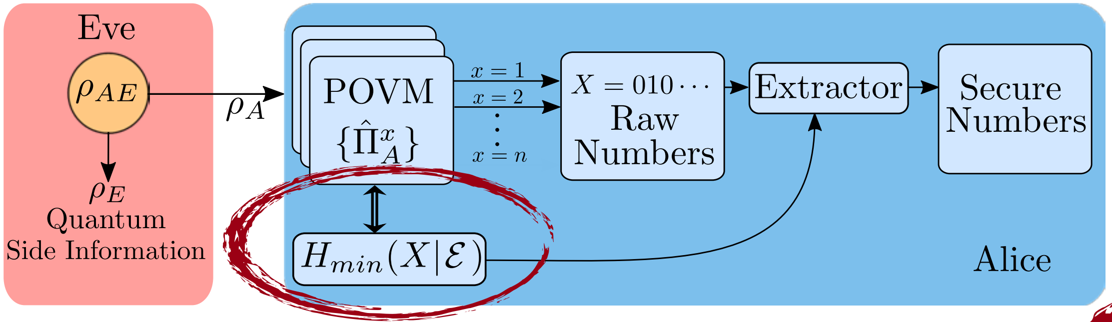
Taking into account finite measurement resolution in the phase space

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

[1] U. Leonhardt, Measuring the Quantum State of Light

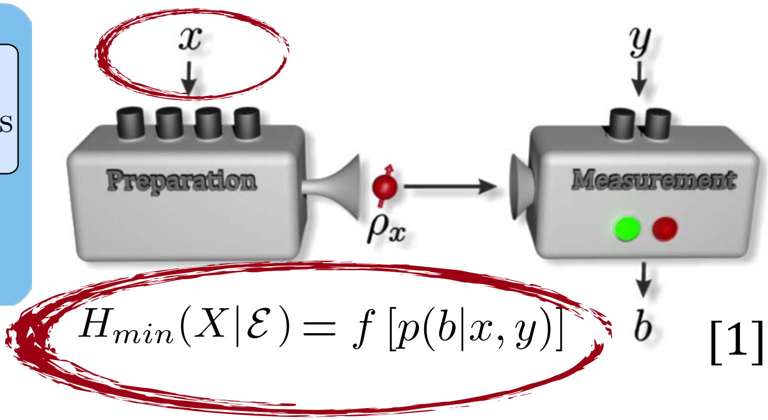
Key differences

Source Device-Independent



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

Typical Semi Device-Independent

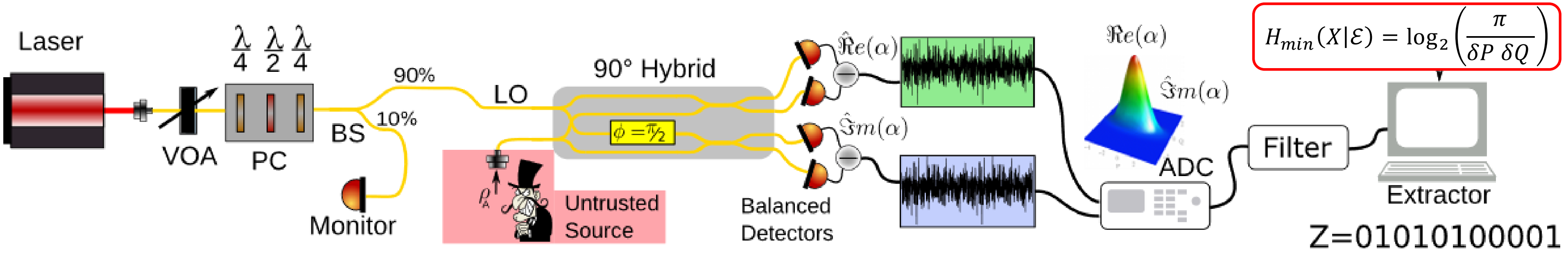


[1]

- **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 $\longrightarrow$ **no finite size effects**

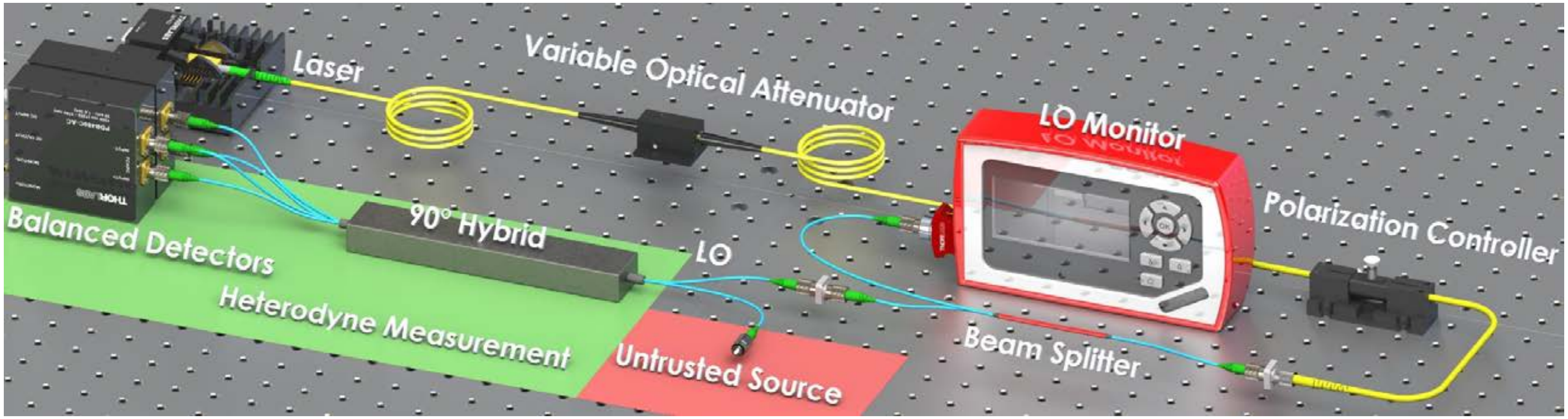
[1] T. Lunghi et al., Phys. Rev. Lett., 114, 150501, (2015).

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 a **Toeplitz Randomness Extractor** calibrated on the **min-entropy** is used to **extract** the secure numbers

Results



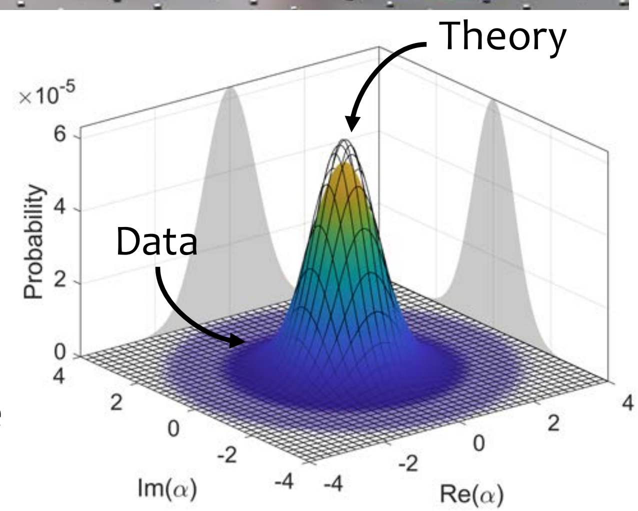
Secure generation rate:

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: $H_{min}(X|\mathcal{E}) \geq \mathbf{13,949}$ **bits** per sample

Effective sampling rate: $1.25\ GSps$

Secure rate: $R \ \geq 1{,}25 \cdot 10^{9} \cdot \ H_{min}\,(X|\mathcal{E})$ 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

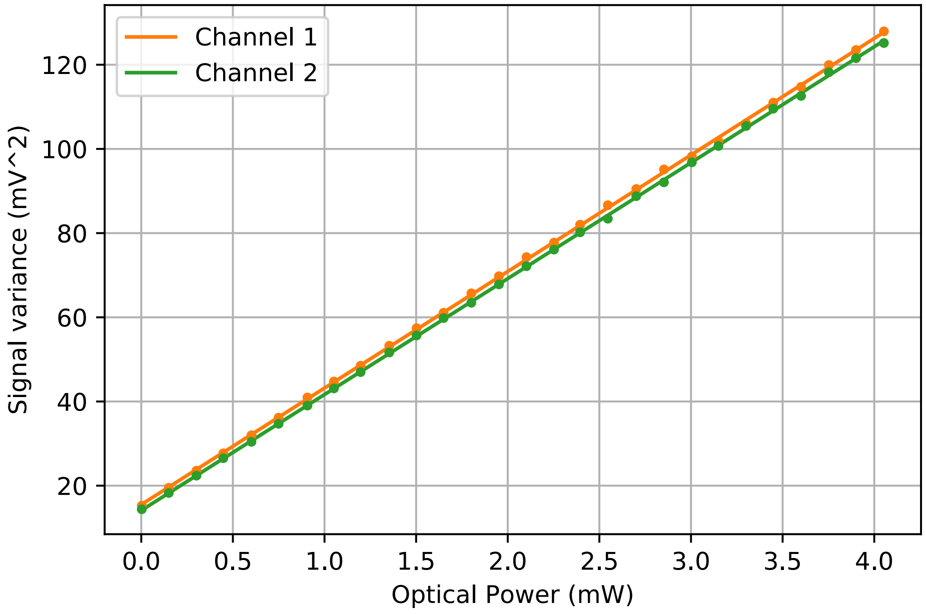
Calibration

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:

$$m_1 = (2.783 \pm 0.005 \cdot 10^{-2} \frac{V^2}{W})$$

$$q_1 = (1.526 \pm 0.005 \cdot 10^{-5}\ V^2)$$

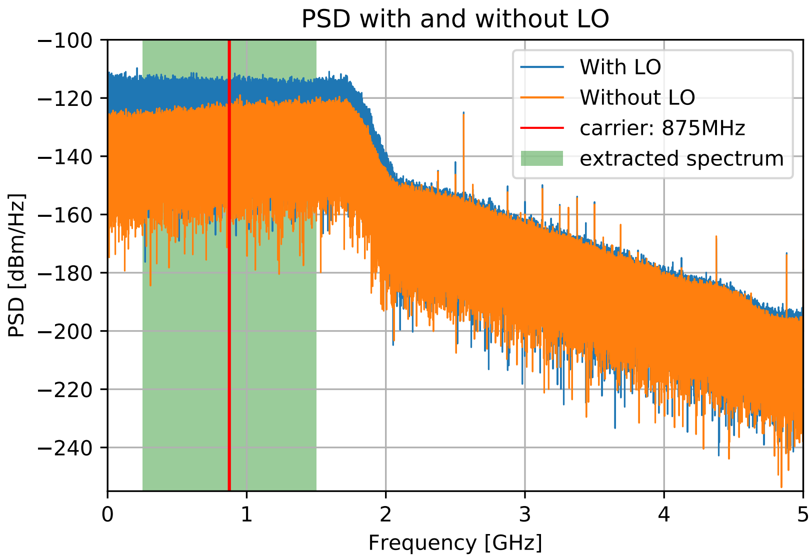
$$m_2 = (2.748 \pm 0.004 \cdot 10^{-2} \frac{V^2}{W})$$

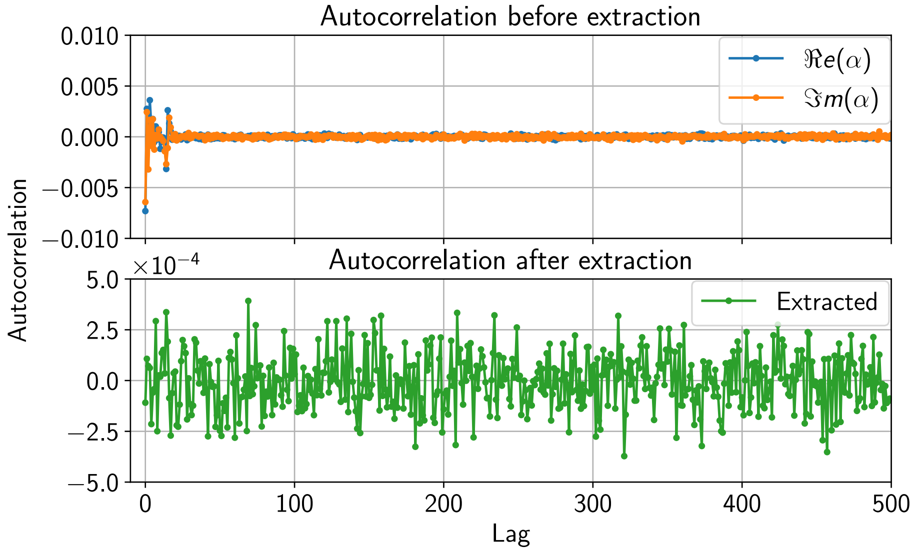
$$q_2 = (1.419 \pm 0.004 \cdot 10^{-5}\ V^2)$$

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:

$$\hat{\Pi}^{\delta}_{m,n} = \int_{m\delta_q}^{(m+1)\delta_q} dRe(\alpha) \int_{n\delta_p}^{(n+1)\delta_p} d\mathrm{Im}(\alpha) \quad \hat{\Pi}_{\alpha}$$

$$P_{guess}(X|\mathcal{E}) = \max_{\{p(\beta),\tau_\beta\}} \int p(\beta) \max_x \mathrm{Tr}\left[\Pi^{\delta}_{m,n}\tau_\beta\right] d\beta$$

Is a well defined probability….

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

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

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

Which is a probability density function

Guessing Probability

The expression of the guessing probability is equivalent to the one introduced in [1]

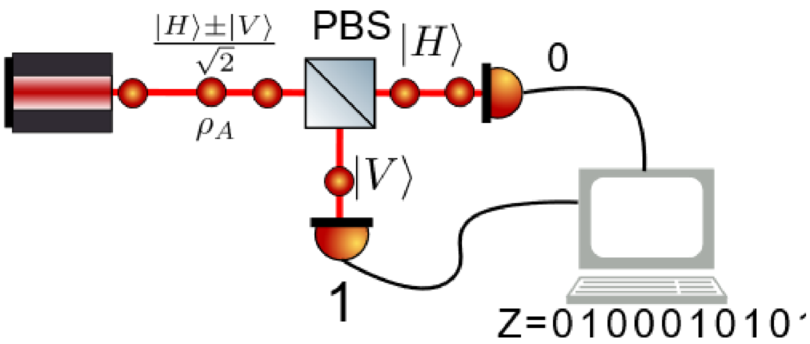
$$\mathrm{P_{guess}}(\mathrm{X}|\mathcal{E}) = \max_{\{\hat{E}_\beta\}} \sum_{x}^{d} P_X(x)\mathrm{Tr}\left[(\hat{E}_\beta)\rho_x^E\right]$$

Intuitively, the states $\hat{\tau}_\beta$ 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

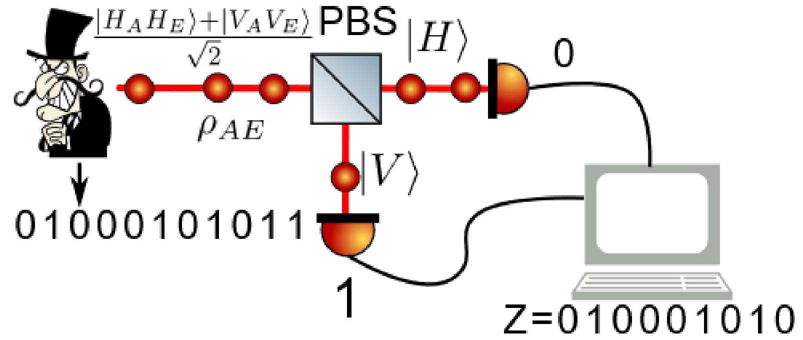
$$\hat{\tau}_\beta = \frac{\mathrm{Tr_E}\left[\left(1_A \otimes \hat{E}_\beta\right)\rho_{AE}\right]}{\mathrm{Tr}\left[\left(1_A \otimes \hat{E}_\beta\right)\rho_{AE}\right]}$$

[1] R. Konig et al, IEEE Transactions on Information theory 55.9 (2009)

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**!