Provably-secure quantum randomness expansion with untrusted homodyne detection secure against quantum side-information

Ignatius W. Primaatmaja[1], Jianran Zhang[2], Jing Yan Haw[2], Raymond Ho[2], Gong Zhang[2], Chao Wang[2], Charles C.-W. Lim[1,2]

[1] Centre for Quantum Technologies, [2] Department of Electrical & Computer Engineering
National University of Singapore

Key message: homodyne-based QRNGs have the following practical advantages...

chip-based implementation

fast (high bandwidth)

cost-effective

room temperature (no cooling required)

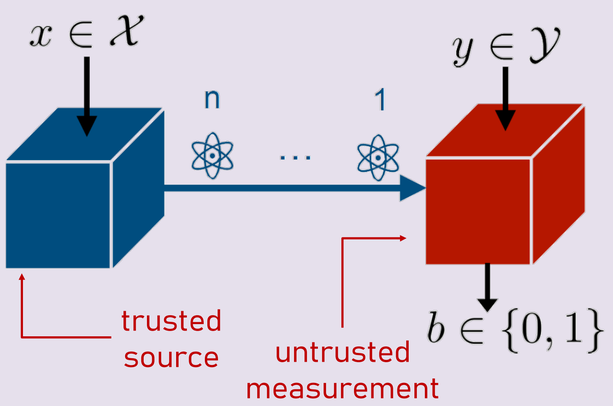
But on the other hand, it is...

complicated (i.e., difficult to model accurately)

Why untrusted measurement?

- The complexity of homodyne detector makes it difficult to characterise.
- An adversary could bias the measurement outcome of the homodyne detector. [For example, see Smith et al., *P.R. Applied* **15**, 044044 (2021)]

Protocol



For key generation round:
Set $|\psi_x\rangle = |\alpha\rangle$ and measure P-quadrature

For each (x, y):
Set a winning condition $b_{x,y}$.

In the ***parameter estimation*** step, we estimate the winning frequency.
Abort if it deviates too much from the expected winning probability.

Some homodyne/heterodyne-based semi-DI-QRNGs

Reference	source	measurement	side information
Marangon et al., *PRL* (2017)	untrusted ☺	trusted ☹	quantum ☺
Michel et al., *P.R. Applied* (2018)	untrusted ☺	trusted ☹	quantum ☺
Avesani et al., *Nat. Comms.* (2018)	untrusted ☺	trusted ☹	quantum ☺
Rusca et al., *Appl. Phys. Lett.* (2020)	energy 😐	untrusted ☺	classical 😐
Avesani et al., *P.R. Applied* (2021)	energy 😐	untrusted ☺	classical 😐
This work*	**trusted ☹**	**untrusted ☺**	**quantum ☺**

Randomness certification

Assumptions:

1. Quantum theory is correct.
2. Alice has a characterised source of quantum states.
3. Bob could securely store his measurement outcomes.
4. Alice and Bob have some trusted and private random seed.

NOTE: we do not assume the measured states to be i.i.d.

Method:

$p(b|x,y)$ —SDP (Wang et al., npj QI **5**, 17 (2019))→ $P_g(B_i|E)$ —EAT (Brown et al., IEEE Trans. on Info. Theory **66**, 2964 (2019))→ $H_{min}^{\epsilon}(\vec{B}|E)$

expected behaviour

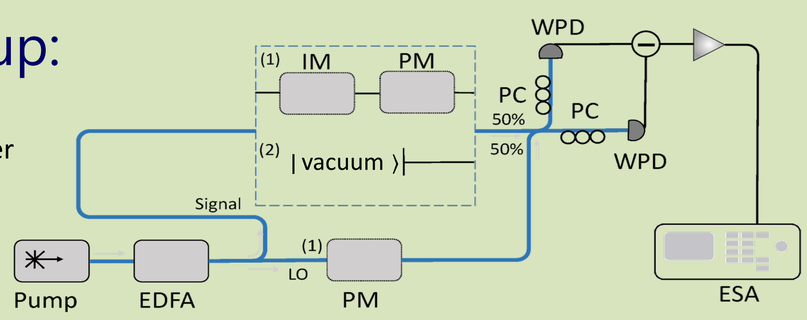
Eve's single round guessing probability

conditional smooth min entropy

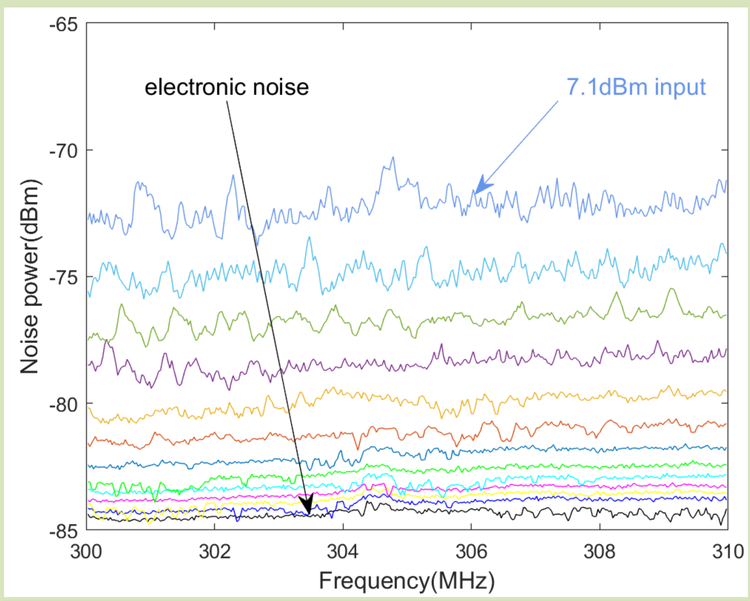
Experimental setup and characterisations

Experimental setup:

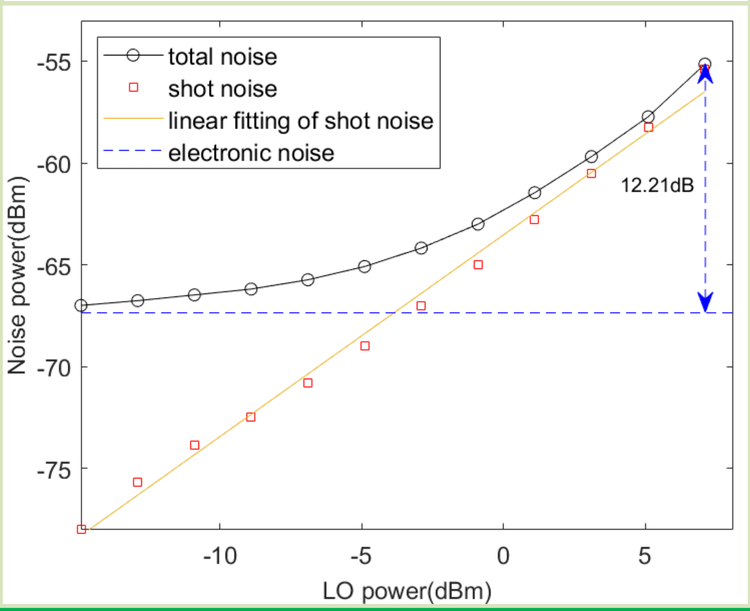
Legends:
EDFA: erbium-doped fibre amplifier
IM: intensity modulator
PM: phase modulator
PC: polarisation controller
WPD: waveguide-coupled photodiode
ESA: electronic spectrum analyser



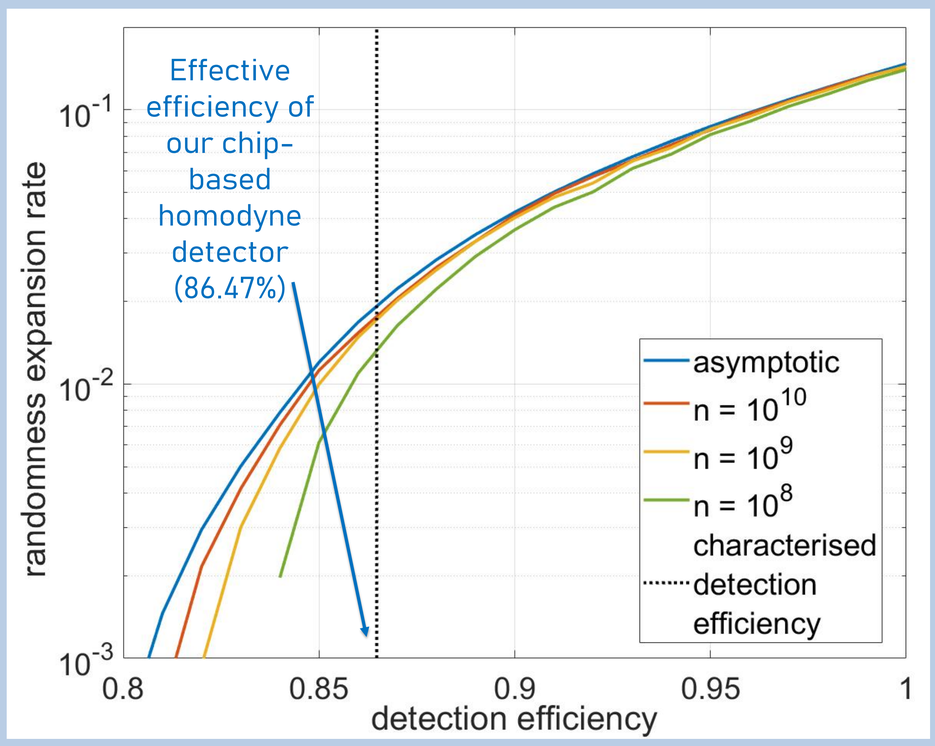
Noise spectrum



Clearance



Main result: randomness expansion rate



16-QAM protocol: positive net randomness expansion with block length of $>10^8$

Security parameters:

$\epsilon_{com} = 10^{-4}$
$\epsilon_{sound} = 10^{-8}$

If you have further questions, you can drop me an email at **william_primaatmaja@u.nus.edu**

Centre for Quantum Technologies

NUS National University of Singapore