ETSI/IQC Quantum Safe Cryptography Event

Assessment of device-dependent quantum random number generators

Christopher Chunnilall

christopher.chunnilall@npl.co.uk

15/02/2023

Applications of Randomness

Security & Defence

- Cryptography & Secure Communication

Finance

- Device Authentication & Secure Transactions

Healthcare

- Randomized medical trials & population sampling

Scientific Research

- Simulations & fundamental Experiments

Entertainment & Sport

- Lotteries & gambling

UNIVERSITY of York

Key Criteria

- For information security, it is crucial that the random numbers are:

Unbiased

Outputs are all equally likely

Unpredictable

Outputs are unique and knowledge of a subsequence cannot improve the ability to predict earlier or subsequent sequences

Types of RNGs

BSI categorisation of RNGs
2 Sep 2022 – Version 2.35 – DRAFT]

A Proposal for Functionality Classes for Random Number Generators

Version 2.35 - DRAFT

Matthias Peter
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

September 2, 2022

DRNG
Deterministic random-number generator (uses a deterministic algorithm)

PTRNG
Physical random-number generator (uses a physical source of entropy [noise])

NPTRNG
Non-physical random-number generator (uses a non-physical source of entropy [noise])

and hybrids

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

Types of RNGs

BSI categorisation of RNGs
2 Sep 2022 – Version 2.35 – DRAFT]

A Proposal for Functionality Classes for Random Number Generators

Version 2.35 - DRAFT

Matthias Peter
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Werner Schindler
Bundesamt für Sicherheit in der Informationstechnik (BSI)

September 2, 2022

5.4 (Para 937):

Quantum noise source. Quantum RNGs exploits physical phenomena that contain randomness according to the laws of quantum mechanics. This document does not distinguish between quantum entropy and entropy from physical phenomena based on other physical models. The AIS 31 considers quantum RNGs as PTRNGs already because of the digitization mechanism that transfers the analog data to raw random numbers.

https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Certification/Interpretations/AIS_31_Functionality_classes_for_random_number_generators_e.pdf

Quantum random number generators

NPL

Output generated from a fundamentally random quantum process

Examples:

- Single photons incident on a beamsplitter
- Spontaneous emission of light

Security and unpredictability derived from laws of physics

- QRNGs permit thorough and accurate physical modelling and testing
- Increased knowledge of process $\not\rightarrow$ increased predictability
- Classical noise can be removed through modelling

Types of QRNGs

Device independent → Bell inequality violation

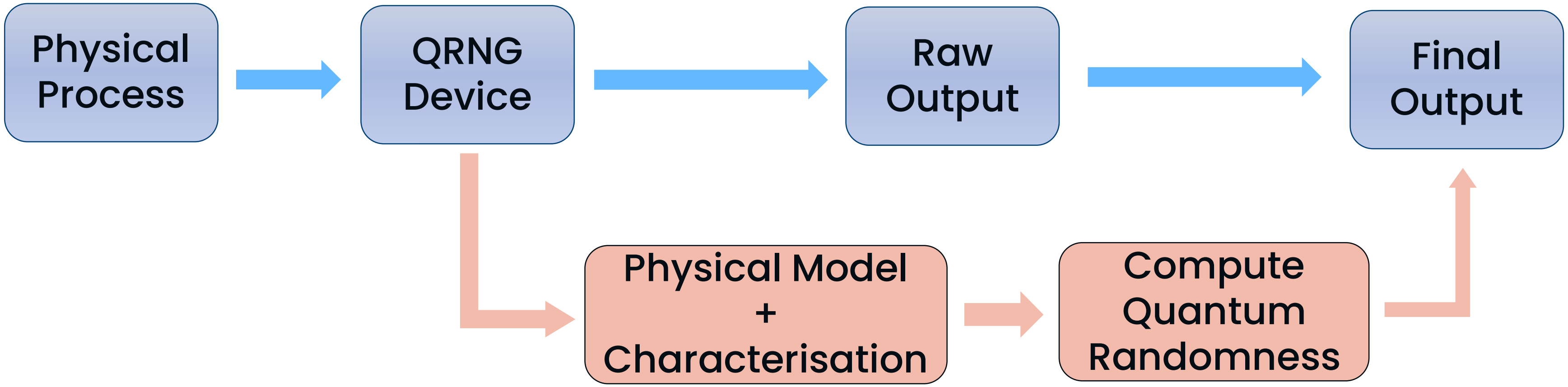
Device dependent → no universal tests →

quantum entropy source
device properties
entropy quantification
randomness extraction

Statistical tests cannot confirm "quantumness" of the source, nor randomness of the numerical output

Herrero-Collantes & Garcia-Escartin, Rev. Mod. Phys. 89, 015004 (2017)

Assessment process



Homemade QRNG

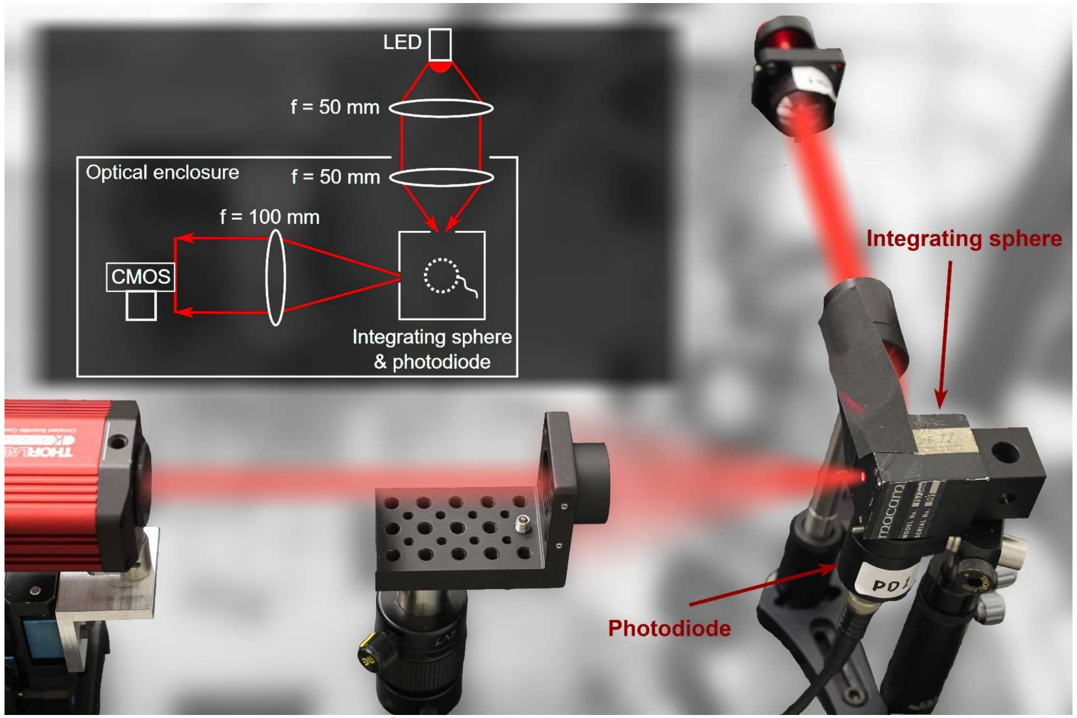
UNIVERSITY *of York*

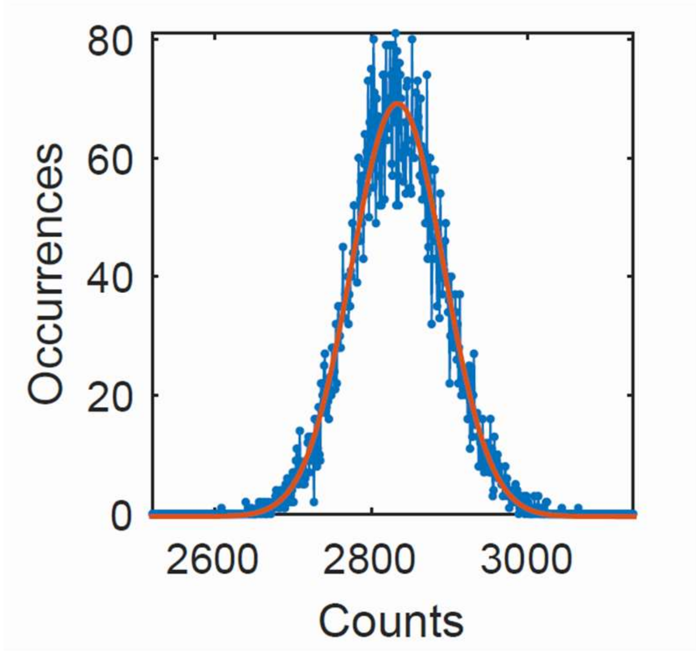
Device

PHYSICAL REVIEW X 4, 031056 (2014)

Quantum Random Number Generation on a Mobile Phone

Bruno Sanguinetti,* Anthony Martin, Hugo Zbinden, and Nicolas Gisin
Group of Applied Physics, University of Geneva, Genève 4, CH-1211, Switzerland
(Received 2 May 2014; revised manuscript received 25 July 2014; published 29 September 2014)

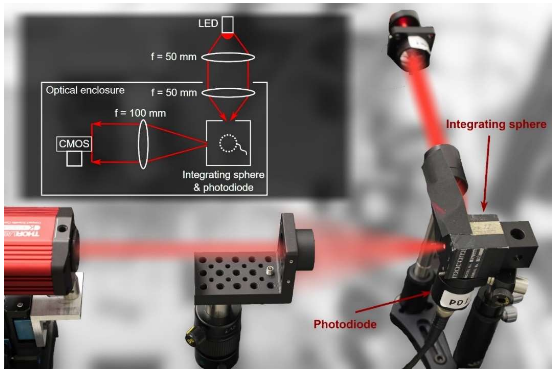




Assembled from commercial off-the-shelf components

UNIVERSITY of York

Model



- Spontaneous emission of single photons (e-h+ pair)
- Independent propagation in linear medium
- Detection at a single pixel
- Probability p_i of i^{th} e-h+ pair at LED creating a free electron at the detector pixel

<u>Number of charges released in pixel (n_e) is sum of N independent Bernoulli random trials</u>

n_e follows a Poisson binomial distribution $\sim$ Poisson distribution

$$P(n_e) = \sum_{\substack{X\in\{0,1\}^N \\ |X|_1 = n_e}} \prod_i^N (1-p_i)^{(1-X_i)}\, {p_i}^{X_i} \qquad X = \begin{bmatrix}0\\1\\1\end{bmatrix} \rightarrow p(n_e) = (1-p_1)(p_2)(p_3)$$

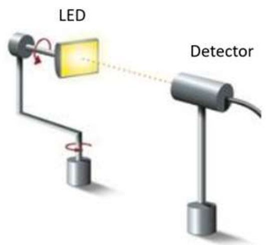
Error δP in this approximation (Le Cam's theorem): $\overline{n_e} = \sum_{i=1}^N p_i \qquad \delta P < 2\sum_{i=1}^N {p_i}^2$

Do not need to specify LED emission distribution

Metrology

Cannot measure N, but can measure rate of photon emission N_{ph} – proxy (underestimate)

$N_{ph} \sim 7.1 \times 10^{15}\ s^{-1}$



Incident photon rate on pixel

Pixel $\leq 5.85\ \mu m \times 5.85\ \mu m$

$n_{ph} \leq 7 \times 10^5\ s^{-1}$

$$\overline{q_i} = \frac{\overline{n_{ph}}}{N} < 10^{-10}$$

$$\delta P < 3 \times 10^{-4}$$

Average photon detection efficiency over all arriving photons: $\eta < 1$

$p_i = \eta\, q_i$

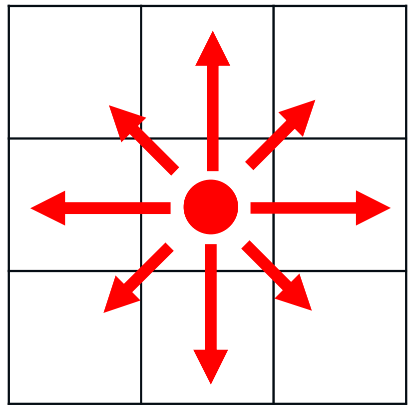
Since $\eta < 1$, n_e will be even better modelled by a Poisson distribution than n_{ph}

Dark counts

Assume a random variable, independent of n_e, accessible to an adversary

Cross-talk
Ignore cross-talk of dark counts

Consider only nearest-neighbour effects
Cross-talk $< 4 \times 10^{-3}$
Negligible



Amplification and ADC conversion

Untrusted noise

Photoexcitation of electrons (n_e)
Poisson distribution

Fixed detection efficiency below full well limit

Conversion to voltage

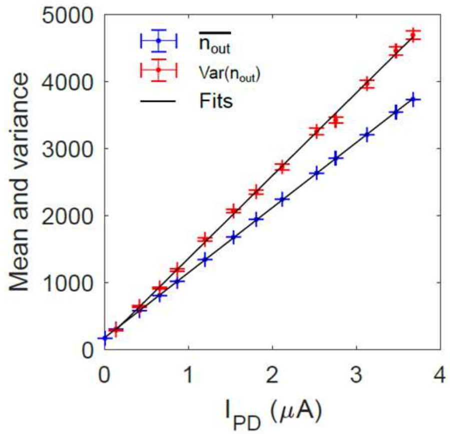
Voltage amplification

12-bit ADC conversion (n_{out})

$$n_{out} = B[g(n_e' + n_d) + C_1]$$

After cross-talk

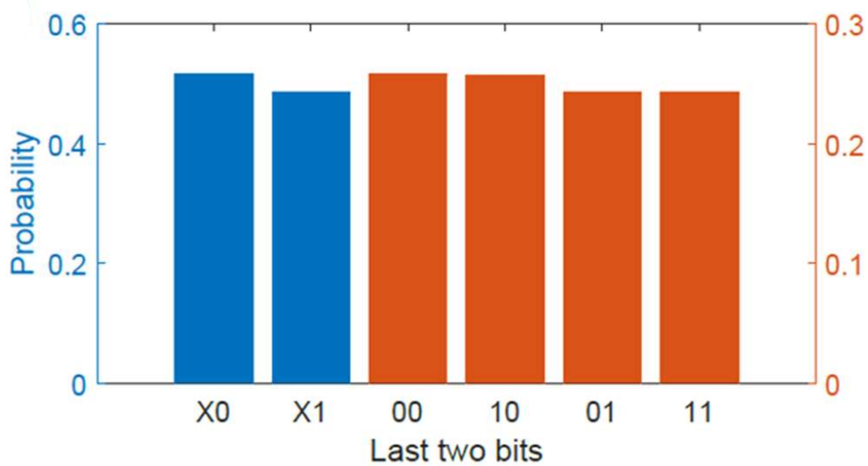
Classical *noise* (uncorrelated with n_e)



$$\overline{n_{out}} = g\,\overline{n_e};$$

$$Var(n_{out}) = g^2\,\overline{n_e}$$

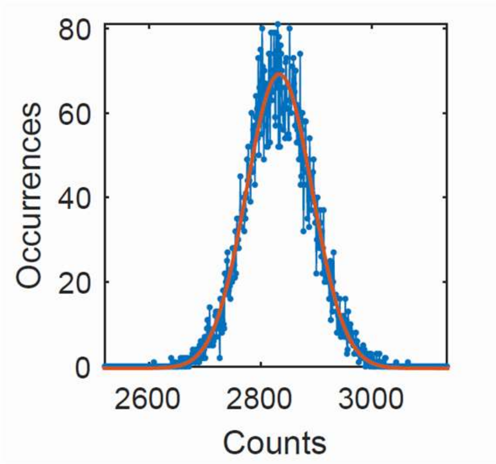
$g \sim 1.19$: uniqueness property satisfied

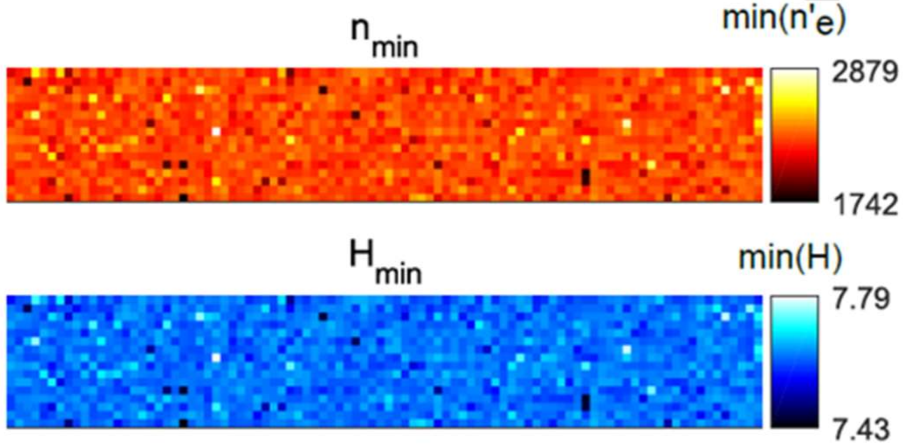


UNIVERSITY *of York*

Extractable randomness

Number of bits that can be extracted from raw output of a pixel:





Extracted random sequence using Toeplitz hash algorithm

Ke Guo, T Hebdige, R Colbeck, and C Chunnilall, In preparation, 2023

Next steps

NPL

- Apply methodology to prototype and commercial QRNG devices
- Seed an assessment process – aligned with existing standards

AQURAND
ASSURANCE OF QUANTUM RANDOM NUMBER GENERATORS

http://www.aqurand.org

Cambridge Quantum | Crypta Labs | KETS | nu QUANTUM | QD Quantum Dice | TOSHIBA

NPL National Physical Laboratory | University of York | University of Kent | National Cyber Security Centre

QUANTUM COMMUNICATIONS HUB | IDQ | NPL National Physical Laboratory | University of York

QRANGE

Part of the Quantum Flagship

University of York

Summary

- Assessment process for QRNGs, combining theoretical modelling with physical characterisation.

- Demonstrated process with ‘homemade’ device
- Extracted random sequence using Toeplitz hash algorithm
- (Passed NIST, TESTU01 statistical tests)

- Approach is compatible with existing standards
- Enables rigorous testing

- AQuRand project – 6 vendors pursuing this approach

cf. Gras et al., Phys. Rev. Applied, 15, 054048 (2021)

Acknowledgements

NPL

UNIVERSITY of York

Ke Guo
[York, NPL]

Tom Hebdige
[York]

Roger Colbeck
[York]

Christopher Chunnilall
[NPL]

Department for Business, Energy & Industrial Strategy

FUNDED BY BEIS

QUANTUM COMMUNICATIONS HUB

AQuRAND
ASSURANCE OF QUANTUM RANDOM NUMBER GENERATORS

The National Physical Laboratory is operated by NPL Management Ltd, a wholly-owned company of the Department for Business, Energy and Industrial Strategy (BEIS).

Questions?