Quantum Random Number Generation based on Vertical-Cavity Surface-emitting lasers

Marcos Valle-Miñón[1], Ana Quirce[1], Angel Valle[1], and Jaime Gutiérrez[2]

1. Instituto de Física de Cantabria (CSIC-Univ. Cantabria), Santander, Spain
2. Dpto. Matemática Aplicada y CC. Computación, Univ. Cantabria, Spain

Outline

- Introduction
- Experiment for Quantum random number generation
- Post-processing and results of statistical test
- Stochastic model of the entropy source

Introduction

Random number generators extensively used in Cryptography

Deterministic algorithms: PRNG
Physical entropy sources: TRNG

Quantum random number generator (QRNG): randomness stems in Quantum Mechanics

QRNG necessary for Quantum Key Distribution (QKD)

Most comercial and research QKD use semiconductor lasers

F. Xu… J. W Pan, Reviews of Modern Physics, 2020
T. K. Paraiso,…, A.J. Shields, Adv. Quantum Technol. 2021

Most of QRNGs: Quantum optics

QRNG: Single-photon detection methods
Multi-photon

Single-Photon: two-path splitting of single photons

T. Jennewein…A. Zeilenger, Rev. Sci. Inst. 2000.

Multi-photon: phase noise in pulsed semiconductor lasers

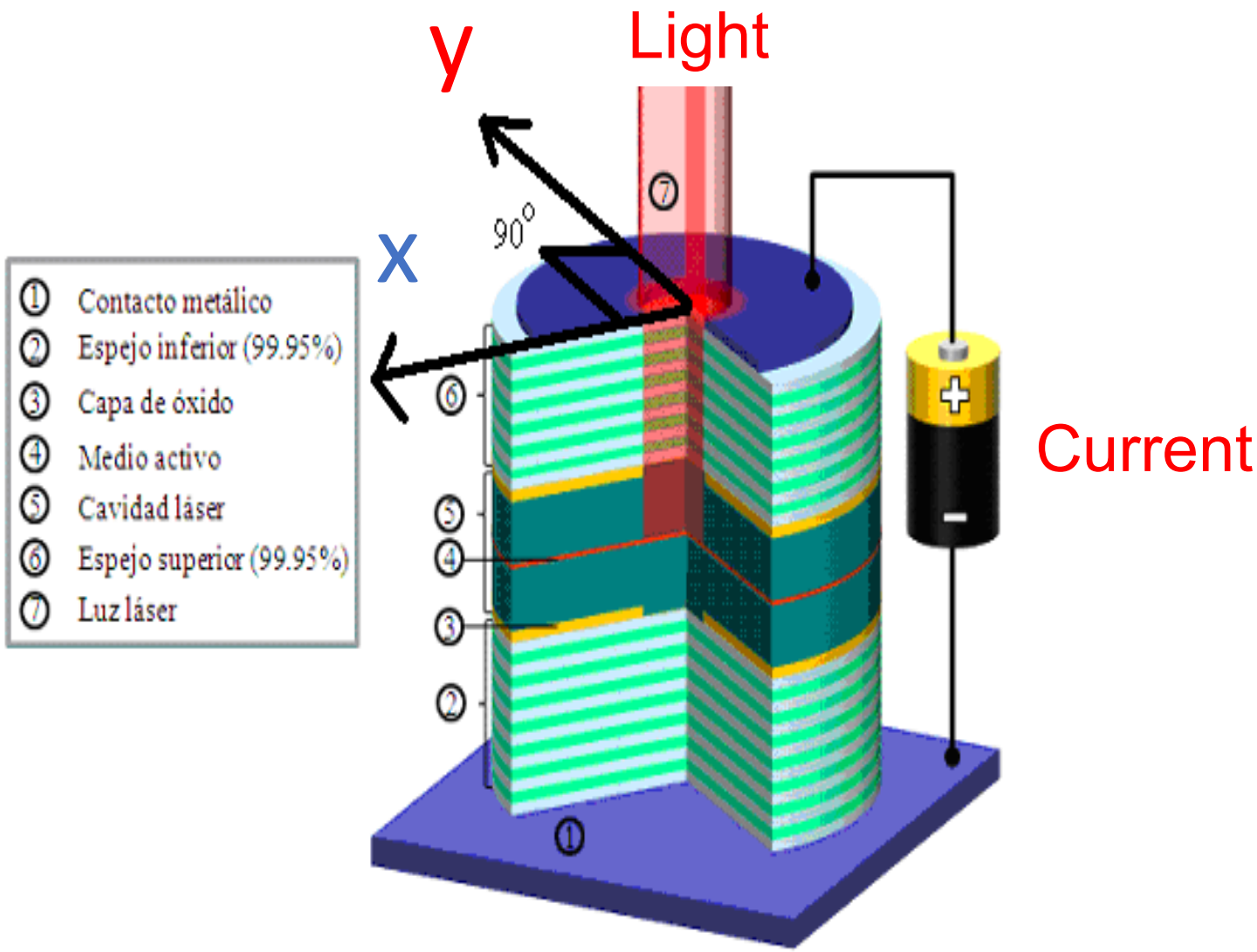
C. Abellan…,M. Mitchel, Opt. Exp. 2014.

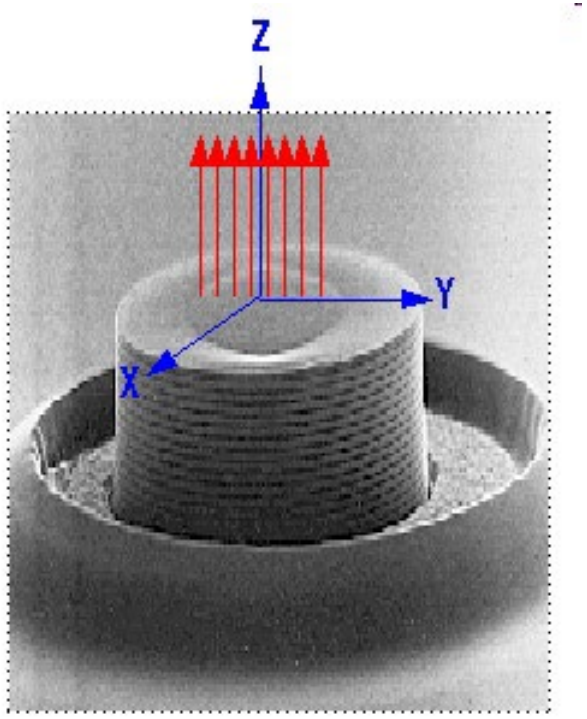
QRNG obtained by excitation of linearly polarized modes of a pulsed semiconductor laser (VCSEL)

A. Quirce, A. Valle, Opt. Exp. 2022.

The experiment

Laser: semiconductor laser called VCSEL (Vertical cavity surface emitting laser)

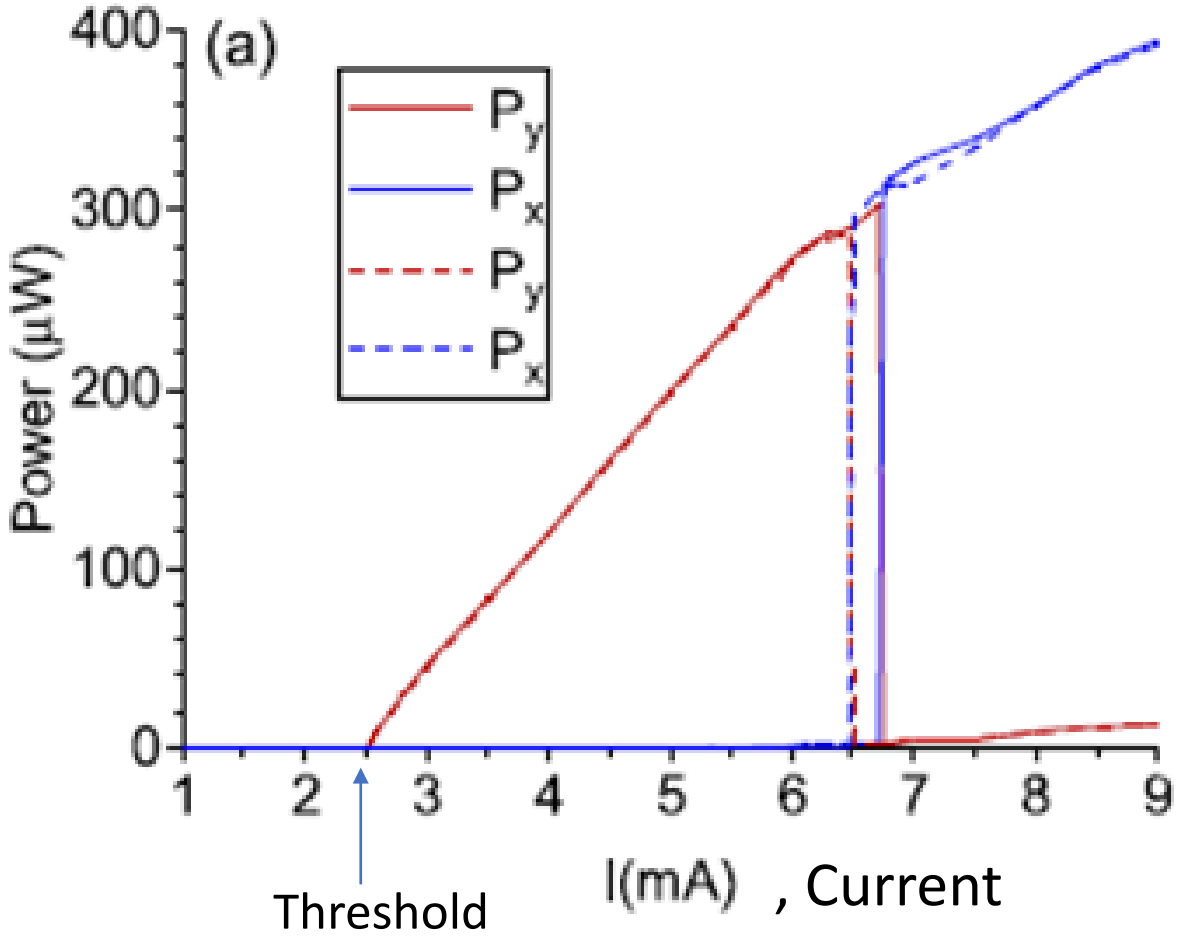




They are microlasers: a few microns dimensions in all directions

When current increases: y-emission to x-emission (Polarization switching)

Using Polarization switching in VCSELs for random number generation



Experimental set-up for pulsed VCSELs

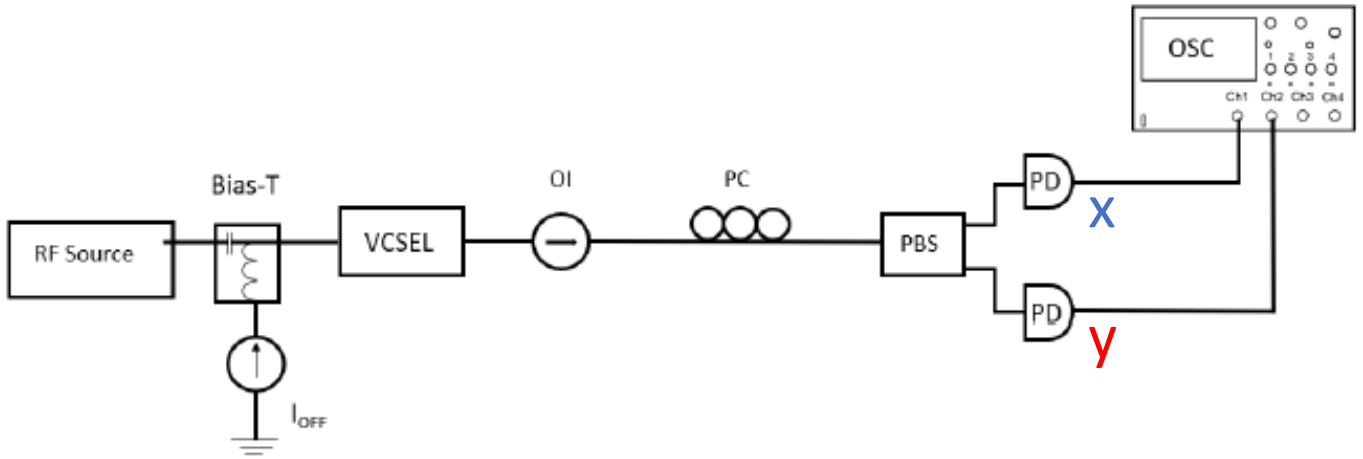
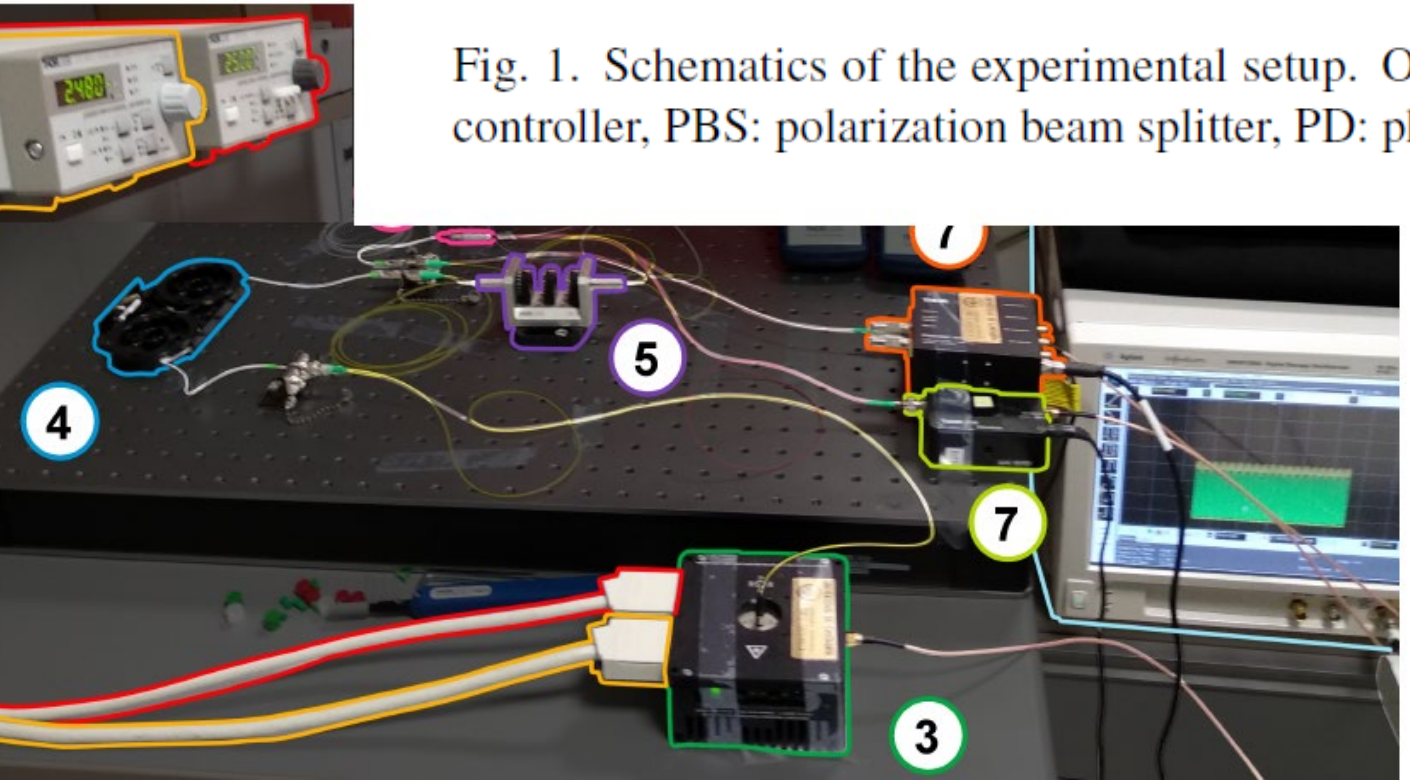


Fig. 1. Schematics of the experimental setup. OI: optical isolator, PC: polarization controller, PBS: polarization beam splitter, PD: photodetector, OSC: oscilloscope.



We apply pulses of current:

Large current 5 ns
Small current: 5 ns

Pulses of light

Current modulation from below to above threshold value

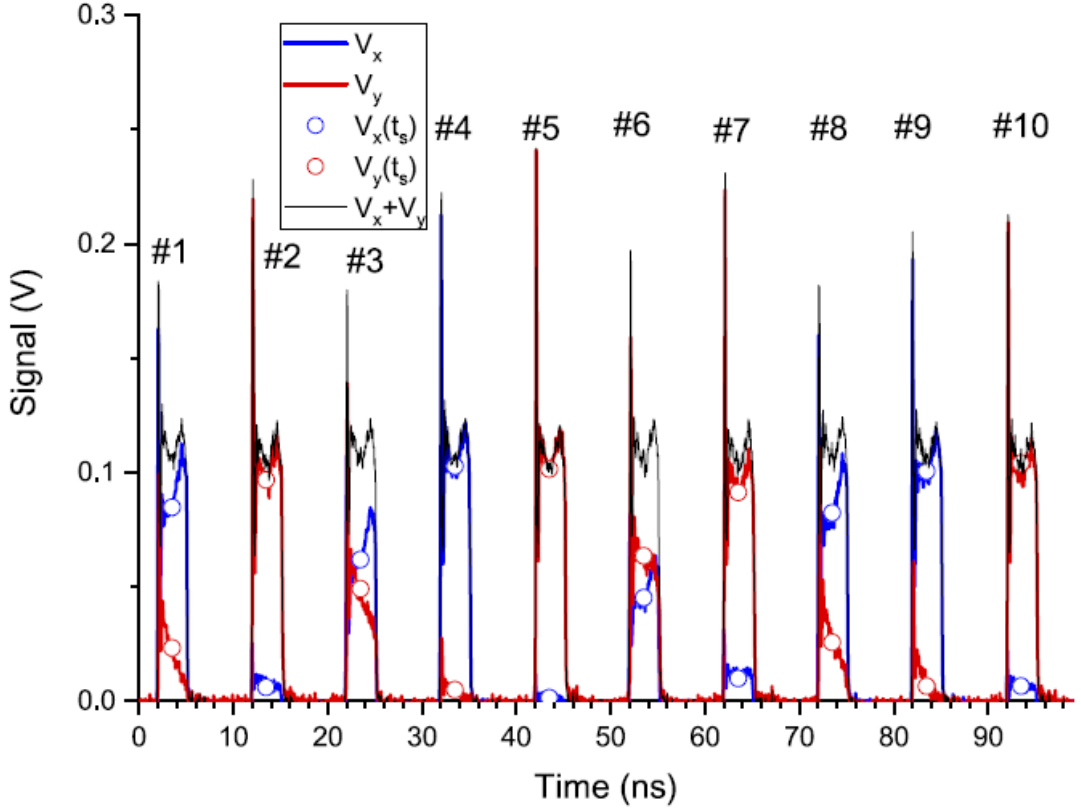
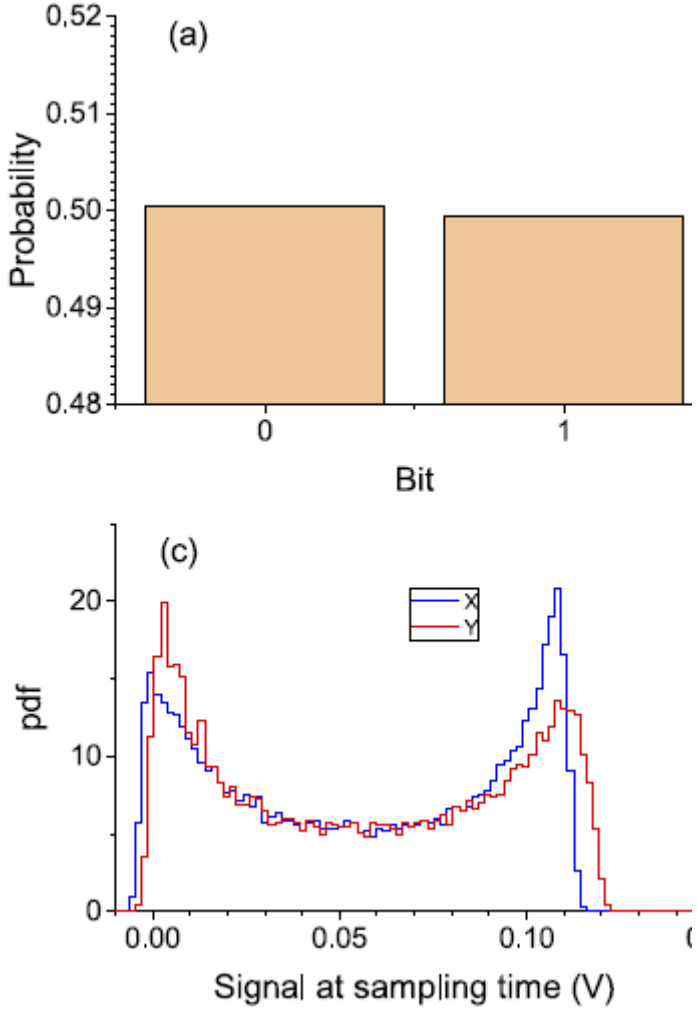


Fig. 3. Experimental time traces of the signals corresponding to the *x*-polarization (blue line), *y*-polarization (red line), and total power (black line). The signals at the sampling time are also plotted with symbols. In this figure I_{off} = 2.5 mA, V_{on} = 1.3 V, and t_s = 3.5 ns.

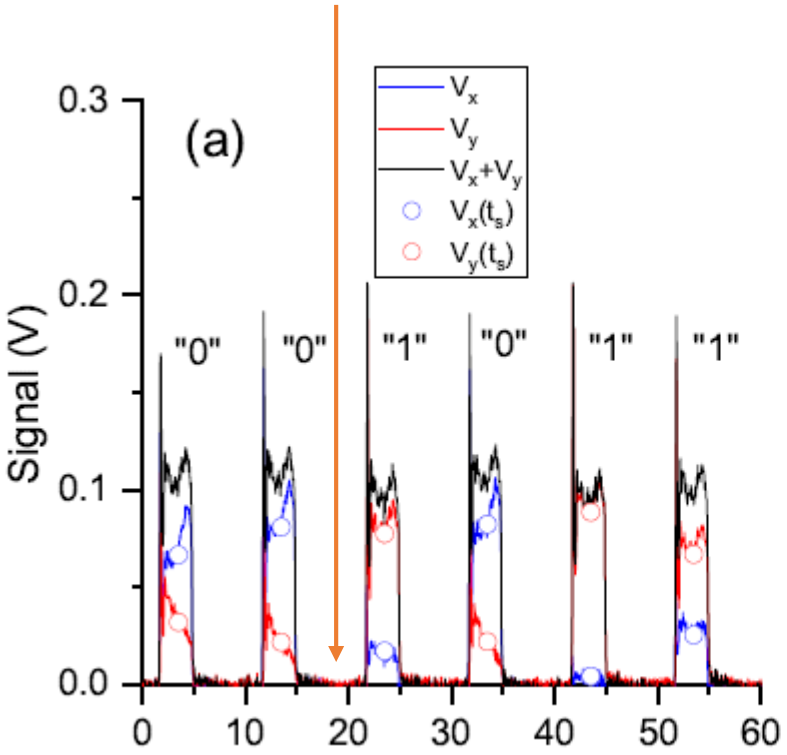
Random excitation of x and y polarizations

If $V_x(t_s)>V_y(t_s)$ → "0" bit

If $V_x(t_s)\leq V_y(t_s)$ → "1" bit

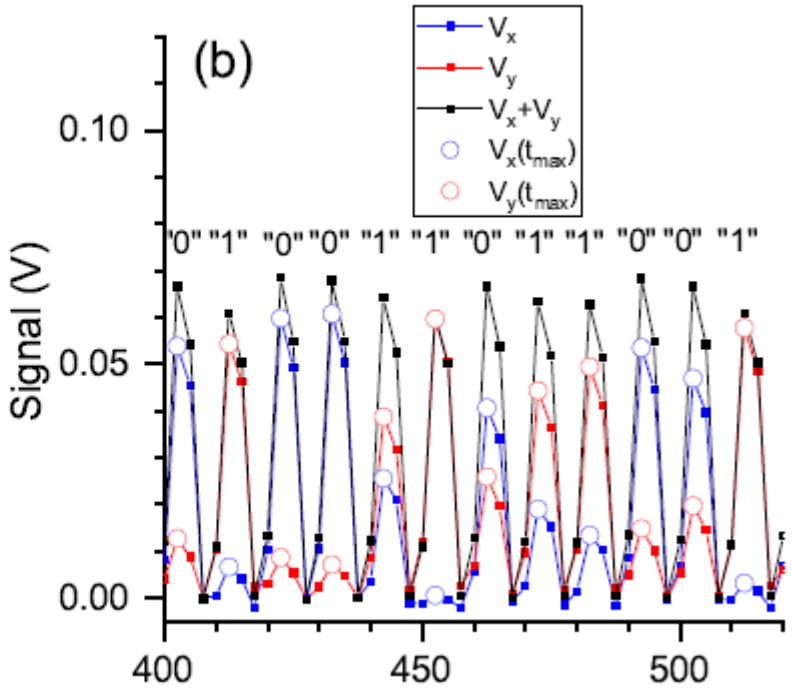


Spontaneous emission noise causes random excitations



1 random bit each 400 values

High resolution acquisition mode



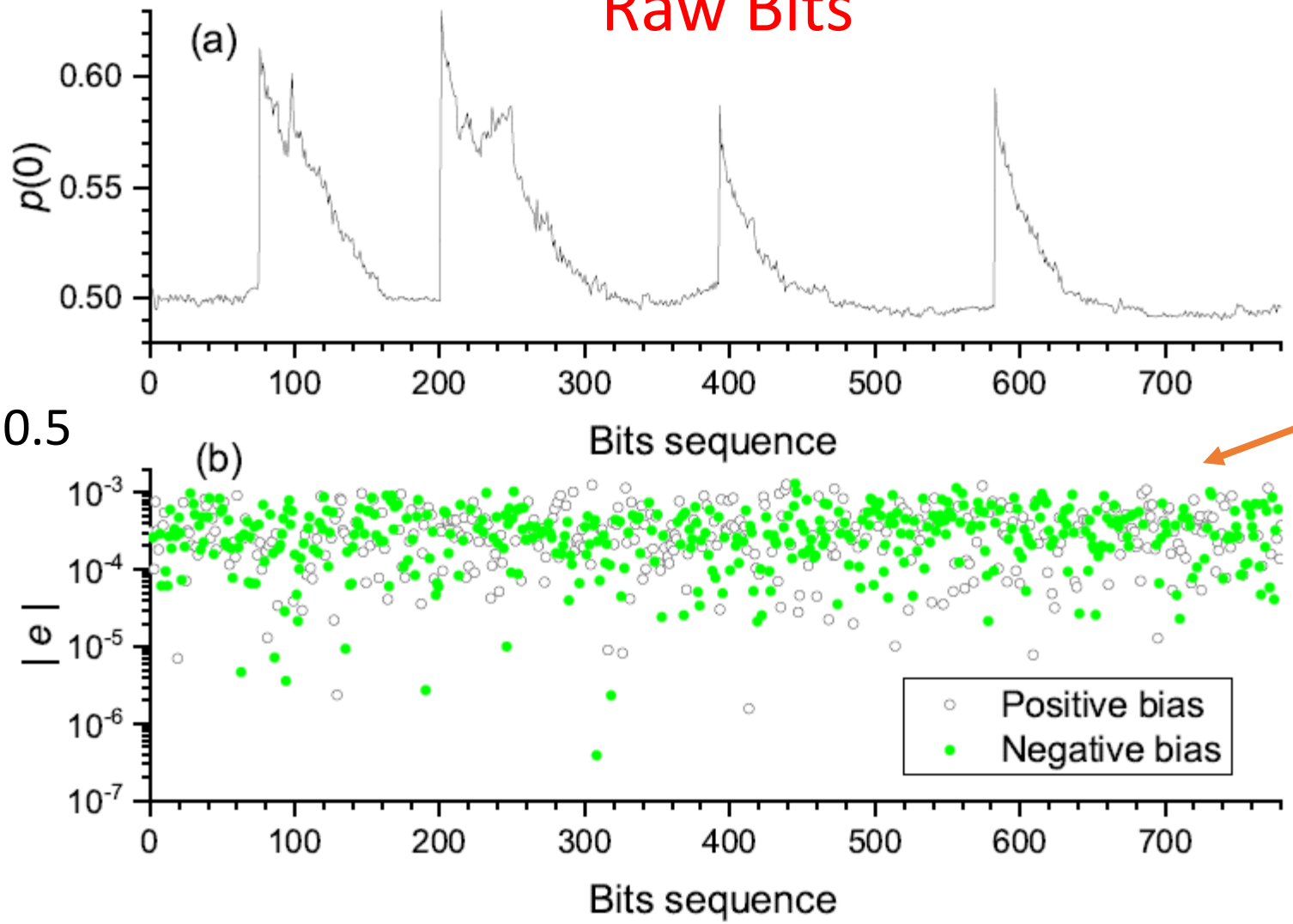
1 random bit each 4 values

↓

enough random bits for passing statistics tests

Post-processing and results of statistical test

Raw Bits



Bias, e=p(0) - 0.5

Von-Neumann Post-processing

01 → 0
10 → 1
00 → no bit
11 → no bit

But low throughput ~ 1/4

Fig. 3. (a) $p(0)$ obtained from the raw data bits, and (b) modulus of the bias obtained with the Von Neumann post-processing, for each of the bit sequences.

Post-processing with [n,k,d] linear codes (BCH)

Theorem 1 [31] *Let G be a linear corrector mapping n bits to k bits. Then the bias of any non zero linear combination of the output bits is less or equal than $2^{d-1}e^d$, where d is the minimal distance of the linear code constructed by the generator matrix G.*

P. Lacharme, Int. W. Fast Softw. Encryp., 2008.

As suggested in [30] we use the efficient $[n, k, d]$-BCH codes defined over the finite field $GF(2)$ and where $n + 1$ is a power of 2. For the raw input bits $(x_{n-1}, \ldots, x_0)$, the output $(y_{k-1}, \ldots, y_0)$ is obtained as:

input output

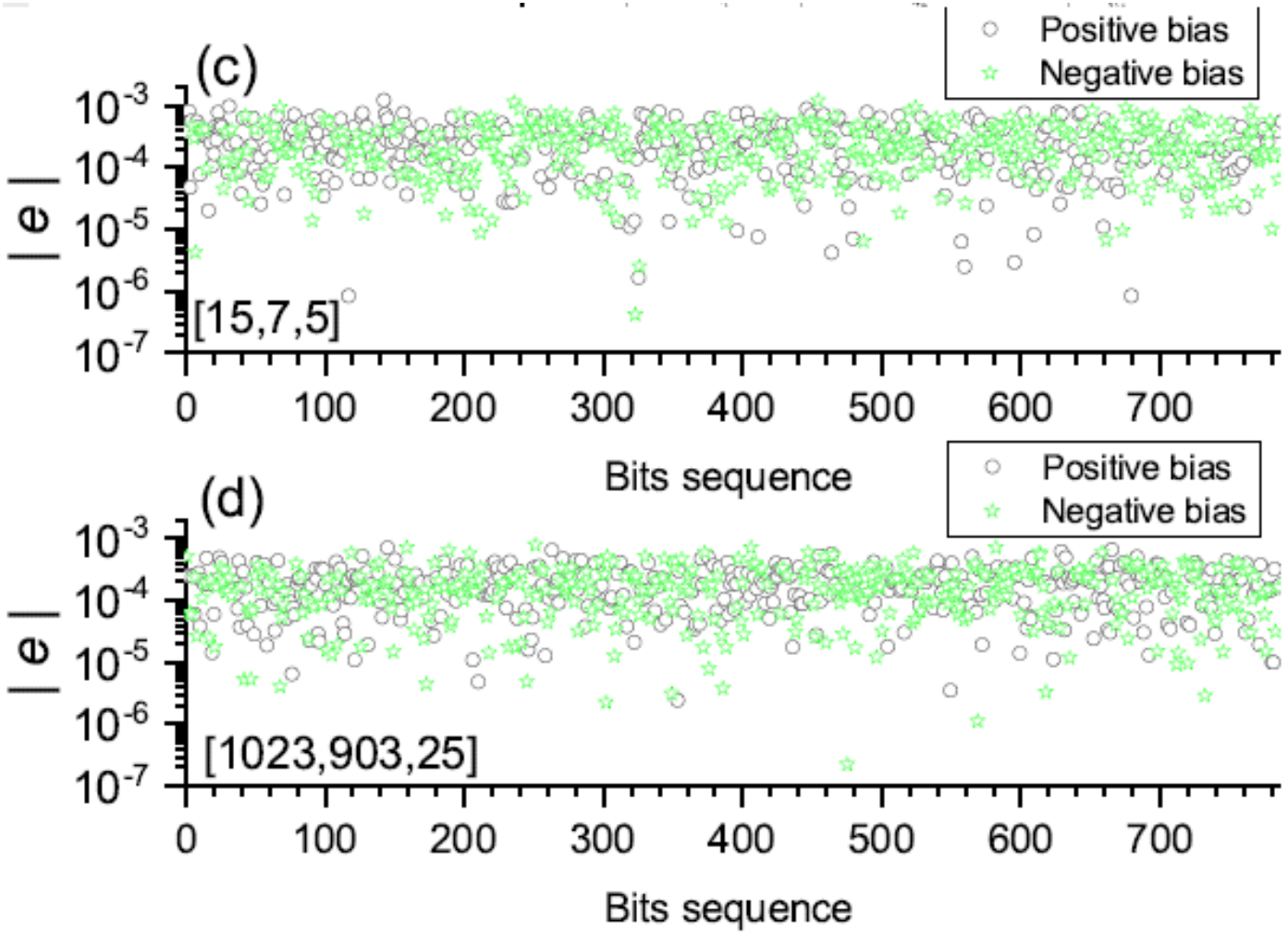
$$\begin{pmatrix} g_{n-k} & \ldots\ldots\ldots & g_0 & 0\ldots\ldots 0 \\ 0 & g_{n-k} & \ldots\ldots\ldots g_0 & 0\ldots\ldots 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0\ldots\ldots & 0 & g_{n-k} & \ldots\ldots g_0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_0 \end{pmatrix} = \begin{pmatrix} y_{k-1} \\ y_{k-2} \\ \vdots \\ y_0 \end{pmatrix}$$

n bits k bits

and $g(x) = g_{n-k}x^k + \cdots + g_1x + g_0$ is the cyclic generator polynomial of the $[n, k, d]$-BCH code.

For instance the BCH code with parameters $[15, 7, 5]$ has as generator cyclic polynomial $x^8 + x^7 + x^6 + x^4 + 1$.

Post-processing with [n,k,d] BCH codes



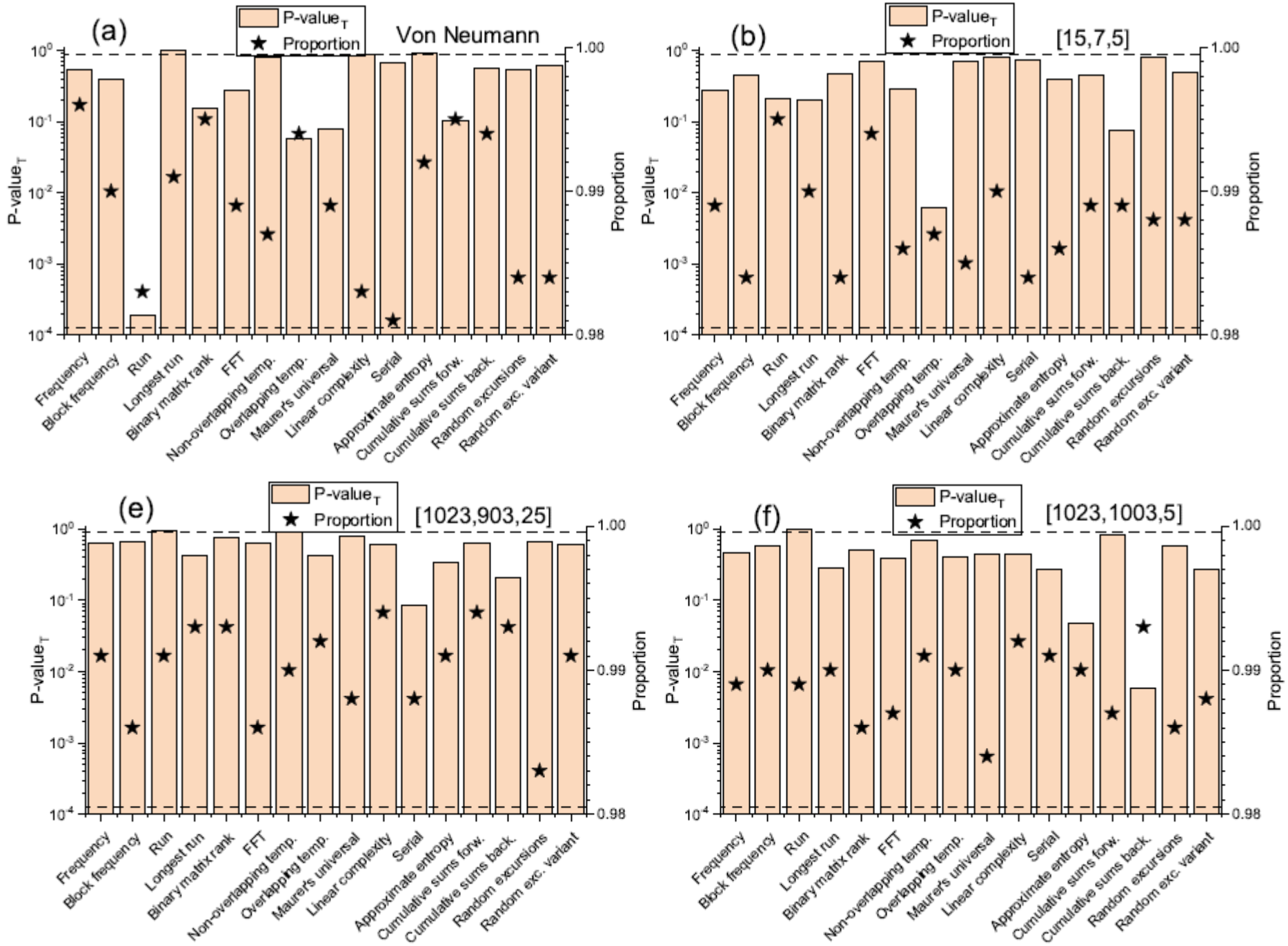

(a)
Von Neumann
(b)
[15,7,5]
(e)
[1023,903,25]
(f)
[1023,1003,5]
P-value$_T$
Proportion
Frequency
Block frequency
Run
Longest run
Binary matrix rank
FFT
Non-overlapping temp.
Overlapping temp.
Maurer's universal
Linear complexity
Serial
Approximate entropy
Cumulative sums forw.
Cumulative sums back.
Random excursions
Random exc. variant

Table 1. Post-processing and NIST test results for different post-processing methods

Post-processing	Output bias	Rate	< P-value$_T$ >	< Prop >	σ_{Prop}
Von Neumann	-3.1 $\times 10^{-5}$	0.2479	0.4737	0.9892	0.0050
[15,7,5]	-1.4 $\times 10^{-8}$	0.4666	0.4446	0.9880	0.0033
[255,107,45]	-2.2 $\times 10^{-5}$	0.4196	0.4204	0.9885	0.0035
[511,484,7]	8.2 $\times 10^{-6}$	0.9472	0.4103	0.9906	0.0022
[1023,903,25]	9.0 $\times 10^{-6}$	0.8827	0.5865	0.9903	0.0032
[1023,1003,5]	8.4 $\times 10^{-6}$	0.9804	0.4513	0.9889	0.0024

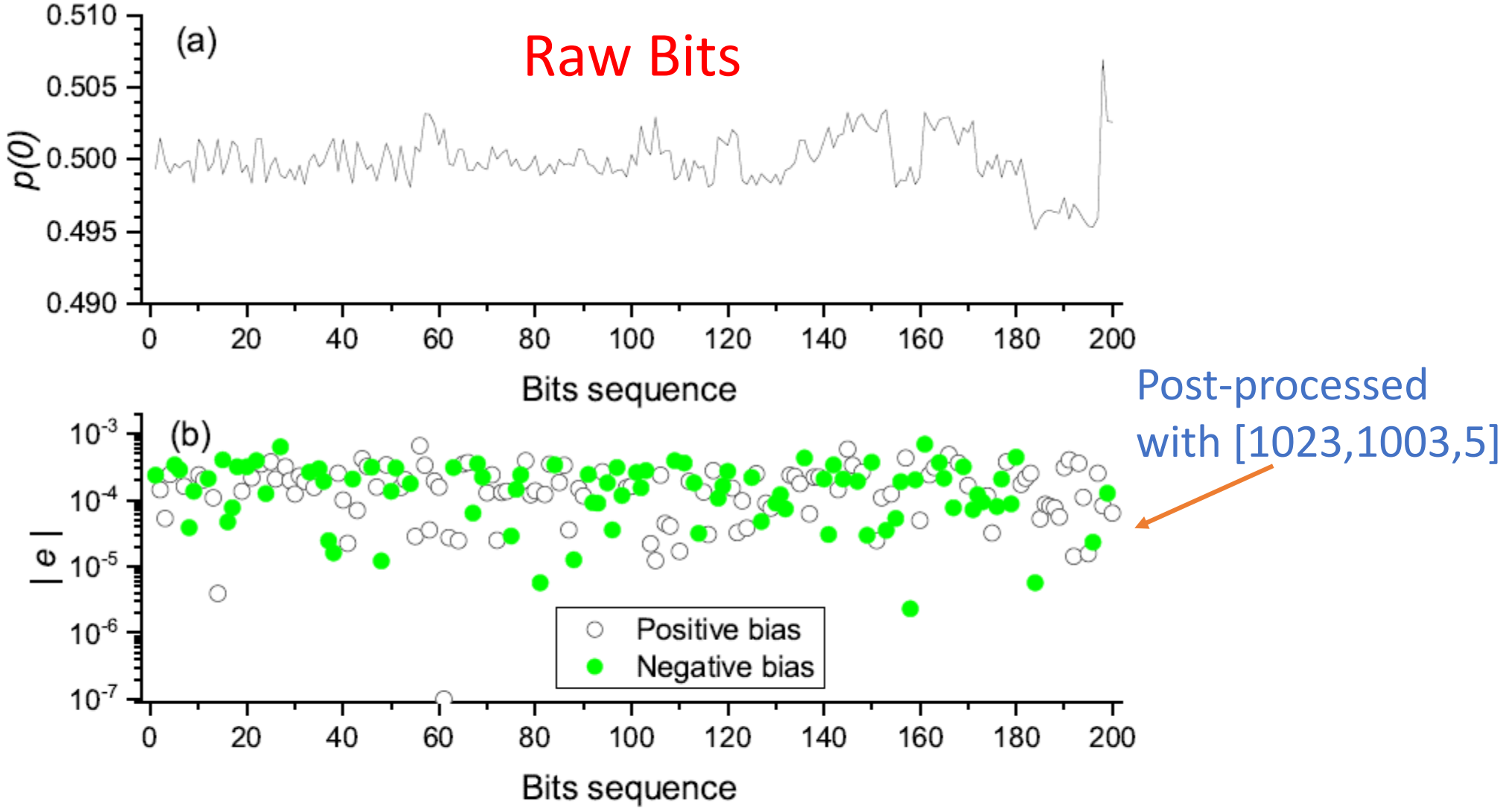


Fig. 5. (a) $p(0)$ obtained from the selected raw data bits, and (b) modulus of the bias obtained with the [1023,1003,5] post-processing, for each of the bit sequences.

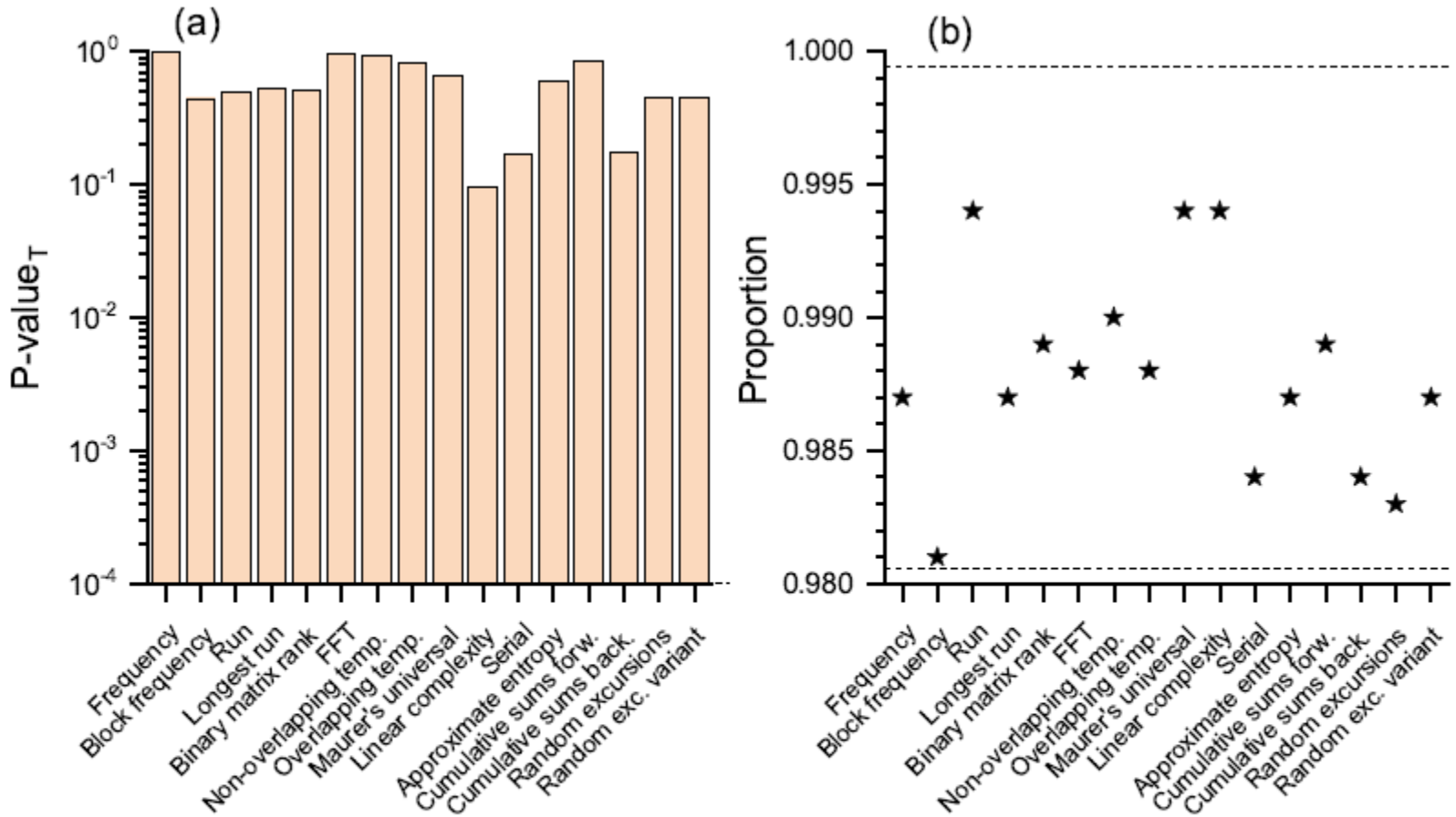


Fig. 6. NIST test results for the [1023,1003,5] post-processing of the selected raw data of Fig. 5. (a) P-value$_T$, and (b) proportions of sequencies that pass the tests

Stochastic model of the entropy source

Stochastic differential equations

Variables: $E_x(t), E_y(t)$
$D(t)$, $n(t)$

Parameters: k, γ_a .....
(Measured for the specific laser)

ξ_+ and ξ_+: Gaussian White noises

$$\frac{dE_x}{dt} = -(\kappa + \gamma_a)E_x - i(\kappa\alpha + \gamma_p)E_x + \kappa(1 + i\alpha)(DE_x + inE_y) + \left(\sqrt{\frac{R_+}{2}}\xi_+(t) + \sqrt{\frac{R_-}{2}}\xi_-(t)\right) \quad (1)$$

$$\frac{dE_y}{dt} = -(\kappa - \gamma_a)E_y - i(\kappa\alpha - \gamma_p)E_y + \kappa(1 + i\alpha)(DE_y - inE_x) + i\left(\sqrt{\frac{R_-}{2}}\xi_-(t) - \sqrt{\frac{R_+}{2}}\xi_+(t)\right) \quad (2)$$

$$\frac{dD}{dt} = \frac{I(t)}{e\,(N_{th} - N_t)} - R(D) - \gamma[D(|E_x|^2 + |E_y|^2) + in(E_yE_x^* - E_xE_y^*)] \quad (3)$$

$$\frac{dn}{dt} = -\gamma_s n - \gamma[n(|E_x|^2 + |E_y|^2) + iD(E_yE_x^* - E_xE_y^*)] \quad (4)$$

where

$$R_\pm = \beta_{SF}\gamma\left[(D \pm n) + \frac{G_N N_t}{2\kappa}\right] \quad (5)$$

$$R(D) = A\left(D + D_t\right) + B\left(D + D_t\right)^2 + C\left(D + D_t\right)^3 \quad (6)$$

Teoría

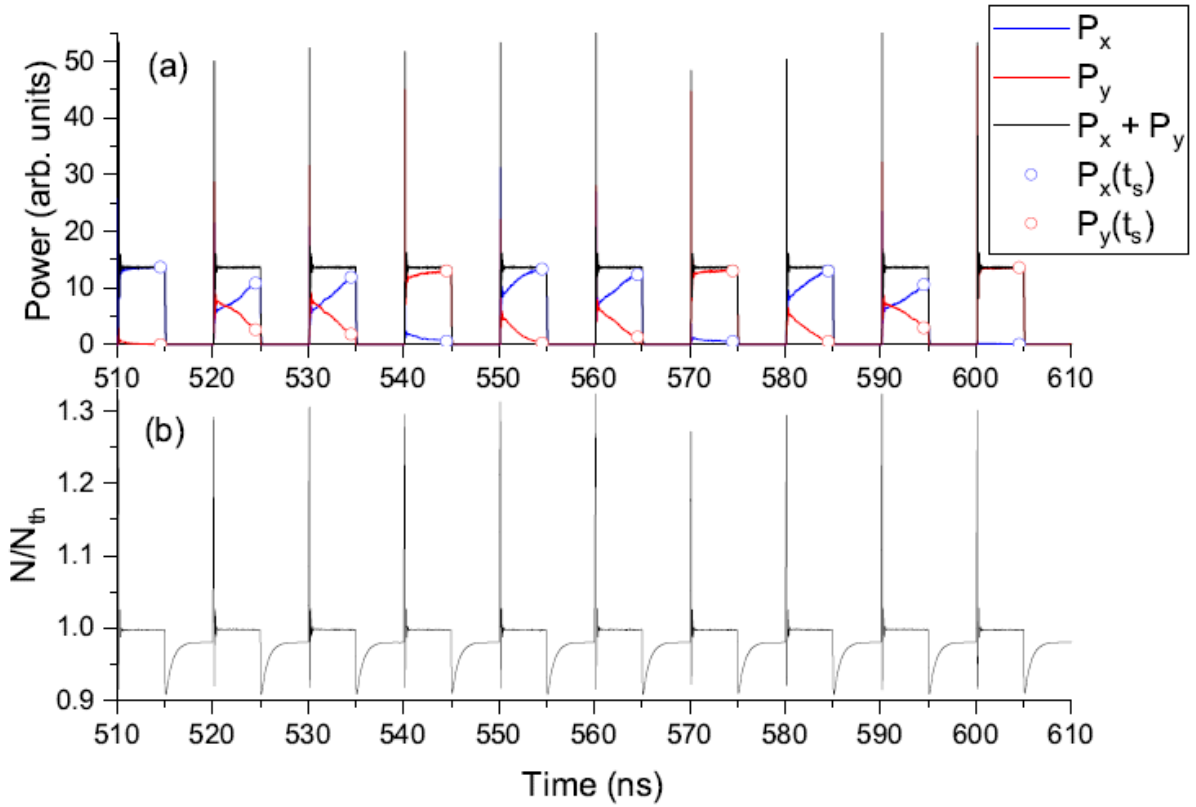


Fig. 3. (a) Simulated time traces of the power of x (blue line) and y (red line) polarization modes. The total power is also plotted with black line. (b) Simulated time traces of the ratio between the carrier number and carrier number at threshold. The modulation frequency is 100 MHz, I_{on} = 15.8 mA (V_{on} = 1.3 V), I_{off} = 2.5mA, γ_a = −0.013 ns^{-1}, and t_s=4.5 ns.

Experimento

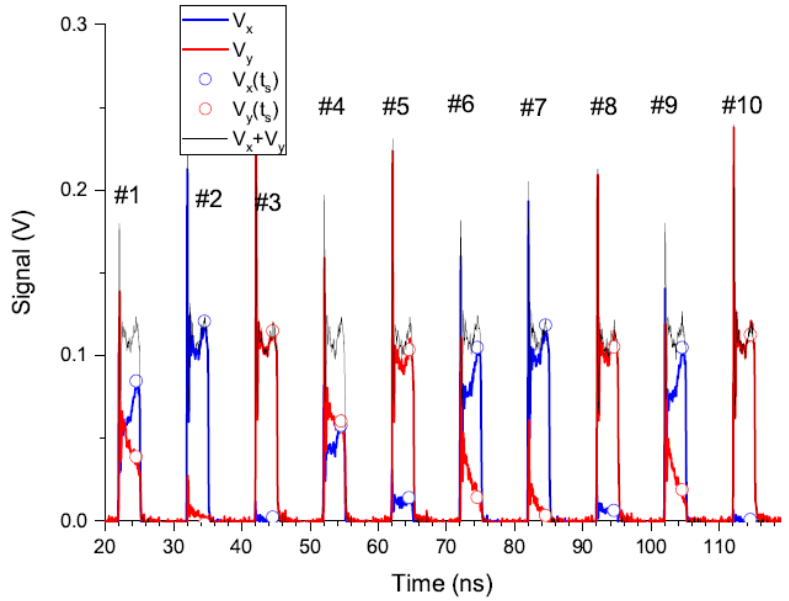


Fig. 1. Experimental time traces of the signals corresponding to the x-polarization (blue line), y-polarization (red line), and total power (black line). The signals at the sampling time are also plotted with symbols. In this figure I_{off} = 2.5 mA, V_{on} = 1.3 V, and t_s = 4.5 ns.

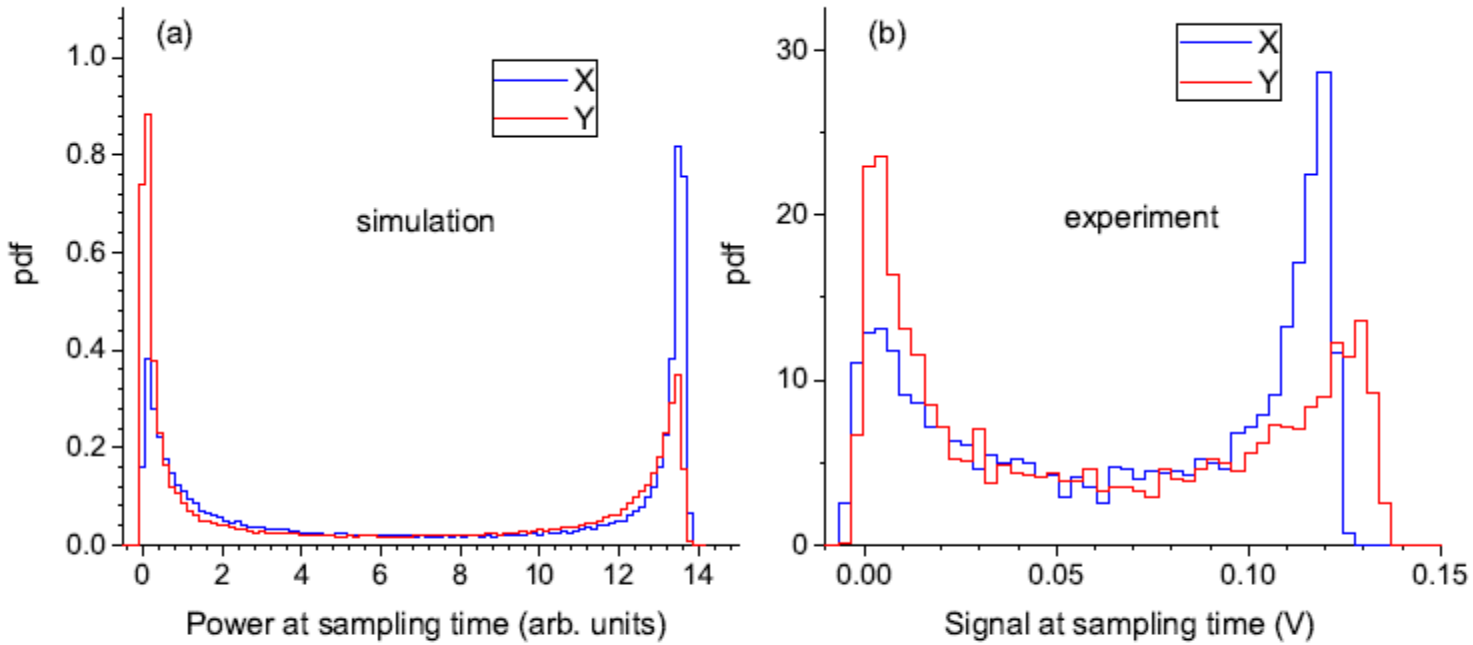


Fig. 4. (a) Theoretical and (b) experimental histograms of x and y signals at t_s= 4.5 ns. The modulation frequency is 100 MHz, I_{on} = 15.8 mA (V_{on} = 1.3 V), I_{off} = 2.5mA, $\gamma_a = -0.013$ ns^{-1}, and $\gamma_P = 103.34$ ns^{-1}.

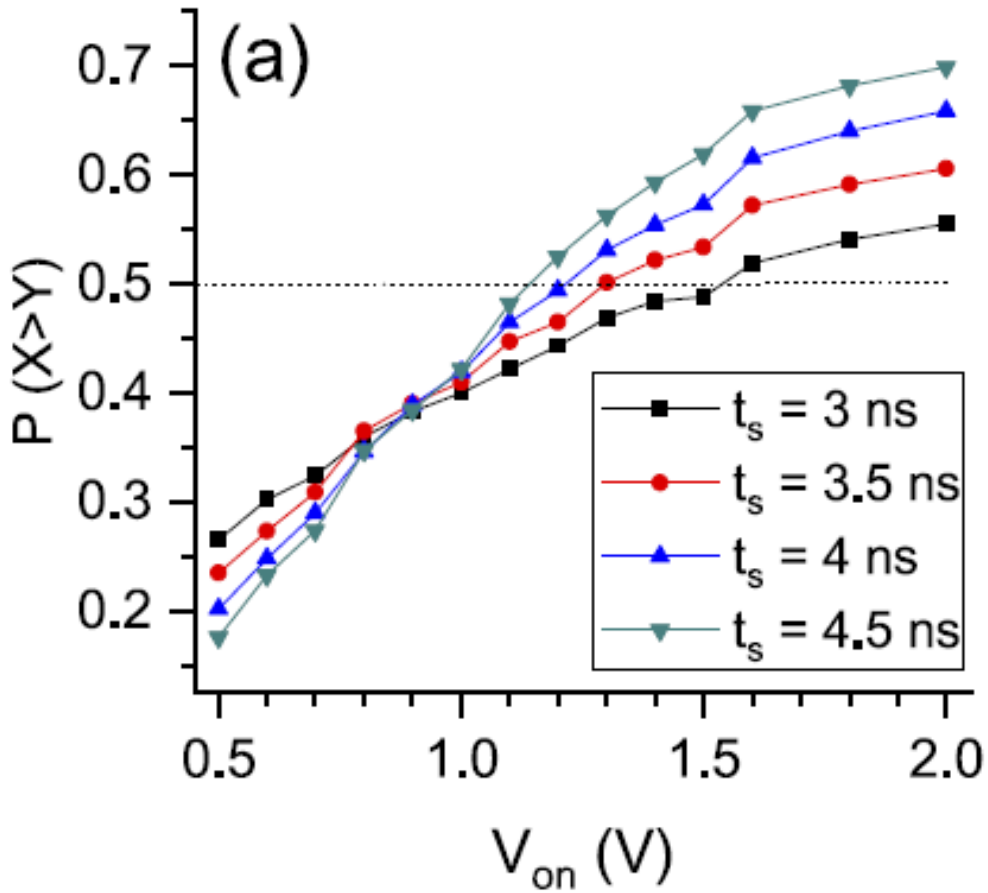
CONCLUSIONS

Random bits obtained from the excitation of linearly polarized modes in pulsed VCSELs fully pass the NIST statistical tests.

NIST test are passed even if small variations of the modulation conditions or temperature appear, providing appropriate post-processing

Post-processing with [n,k,d]-BCH codes with large n and k are the best choice to simultaneously improve throughput and randomness.

First steps in modelling the entropy source


(a)
0.7
0.6
0.5
0.4
0.3
0.2
P (X>Y)
0.5
1.0
1.5
2.0
V_on (V)
t_s = 3 ns
t_s = 3.5 ns
t_s = 4 ns
t_s = 4.5 ns

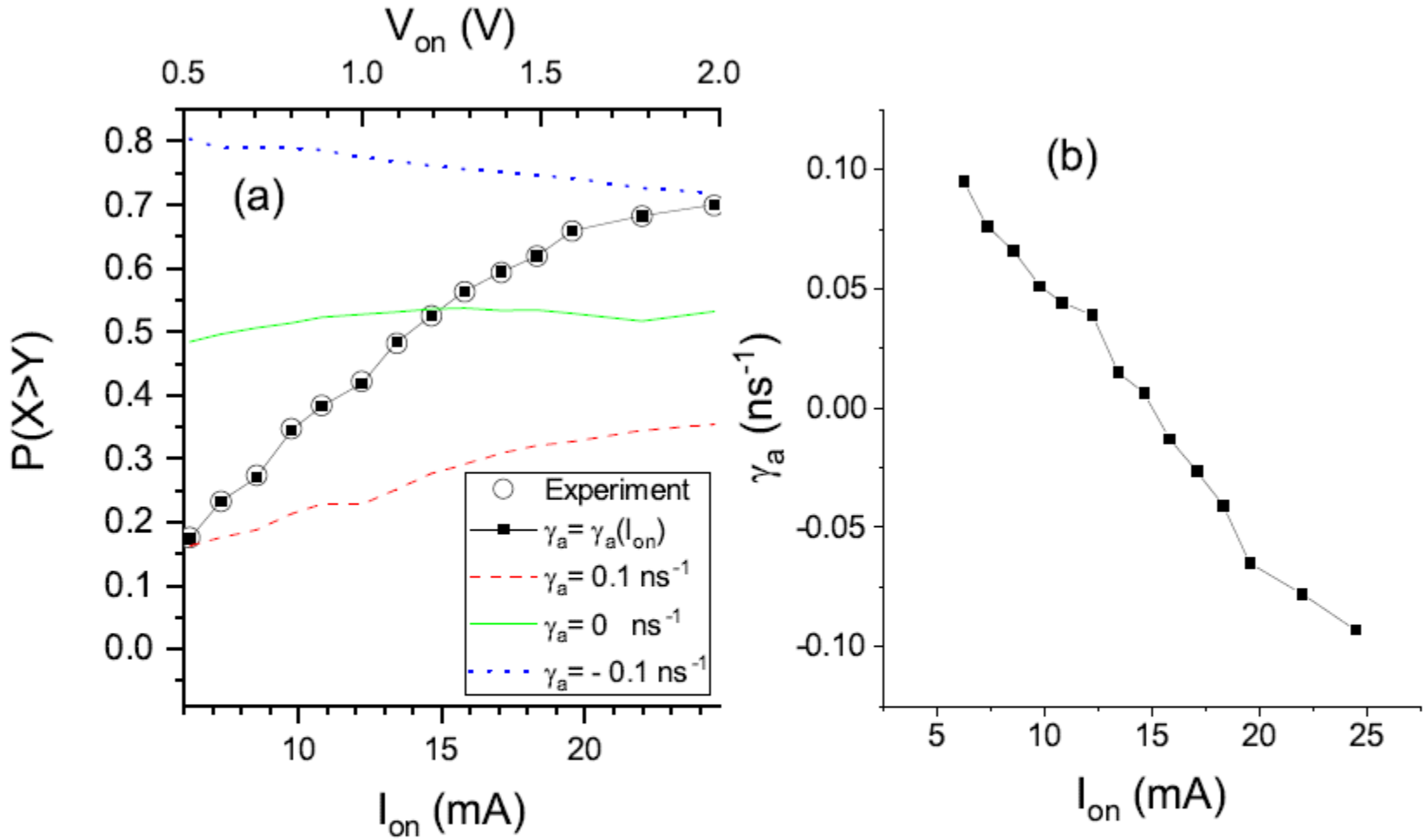


Fig. 2. (a) Probability of excitation of the $x-$ polarization as a function of I_{on} and V_{on} for $t_s = 4.5$ ns. Experimental and simulated values are plotted with circles and solid line, respectively. (b) Linear dichroism as a function of I_{on} for which the simulated results of part (a) are obtained.

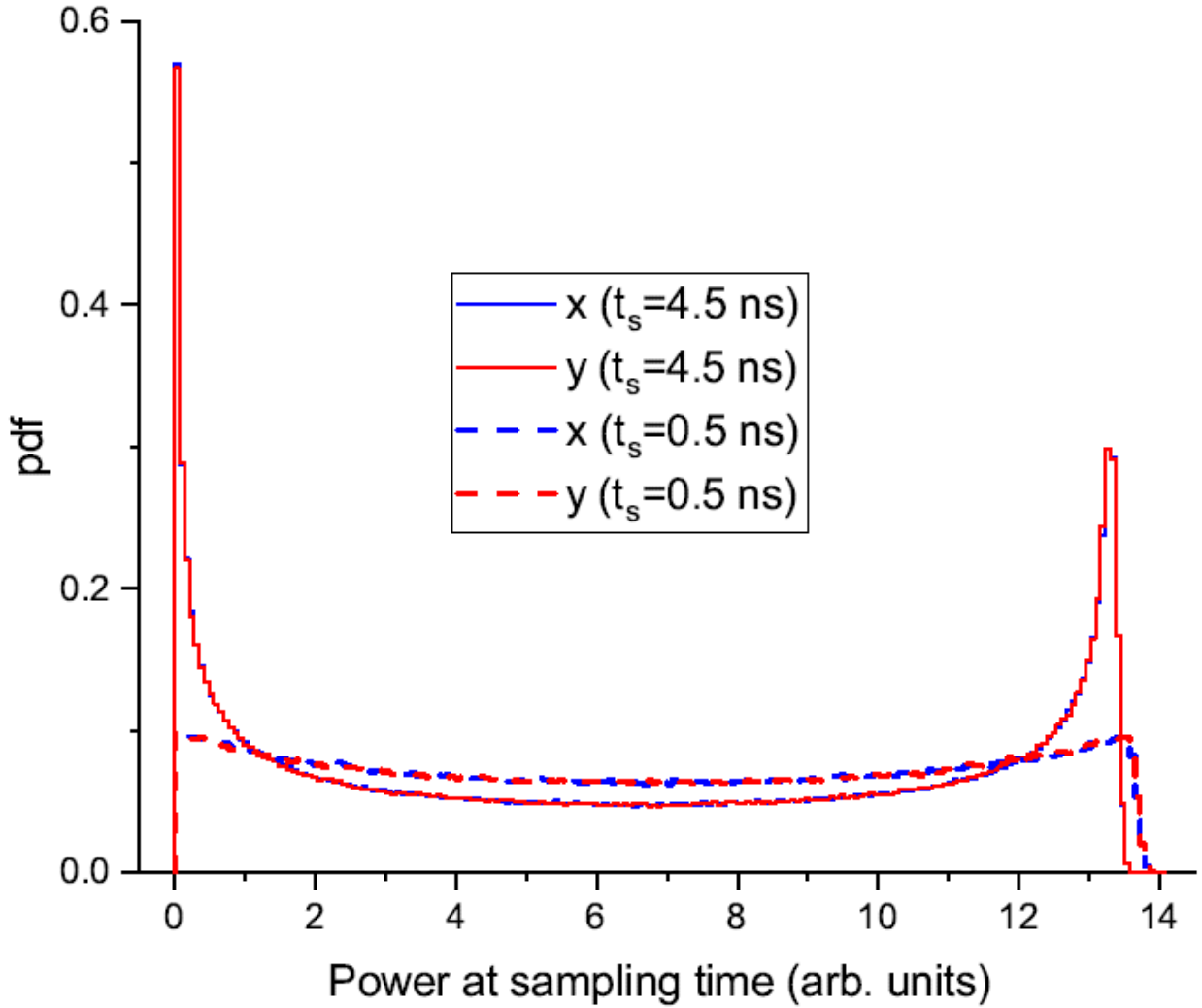


Fig. 5. Theoretical histograms of $x-$ and $y-$power at two sampling times, t_s=0.5 ns, and t_s=4.5 ns. The modulation frequency is 100 MHz, I_{on} = 15.8 mA, I_{off} = 2.5mA, $\gamma_a = 0\ \text{ns}^{-1}$, $\gamma_p = 0\ \text{ns}^{-1}$.

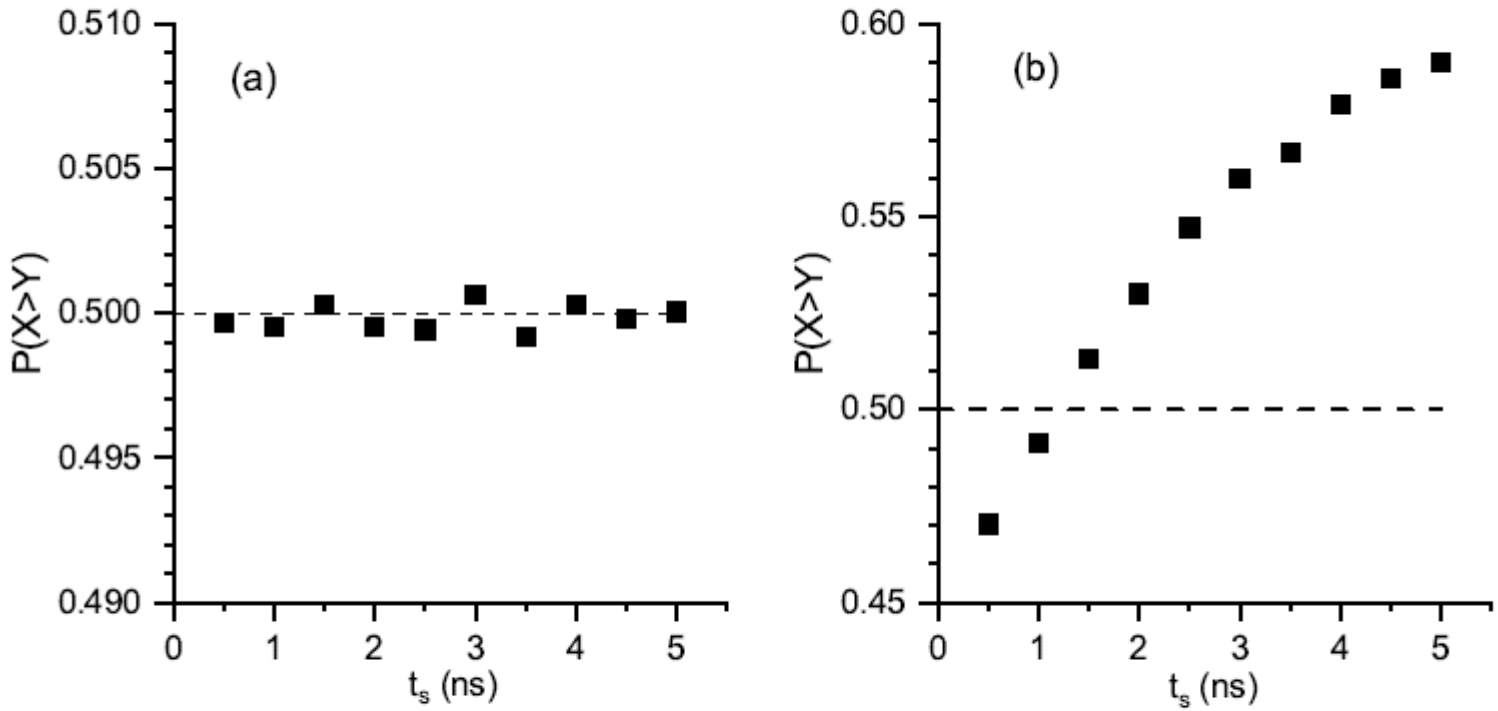


Fig. 6. Probability of excitation of the $x-$polarization as a function of the sampling time for (a) $\gamma_a = 0\ \mathrm{ns}^{-1}$, $\gamma_p = 0\ \mathrm{ns}^{-1}$, and (b) $\gamma_a = -0.013\ \mathrm{ns}^{-1}$, $\gamma_p = 103.34\ \mathrm{ns}^{-1}$. The modulation frequency is 100 MHz, $I_{\mathrm{on}} = 15.8$ mA, $I_{\mathrm{off}} = 2.5mA$.