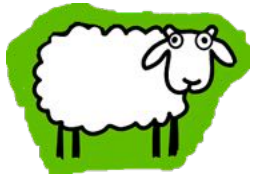
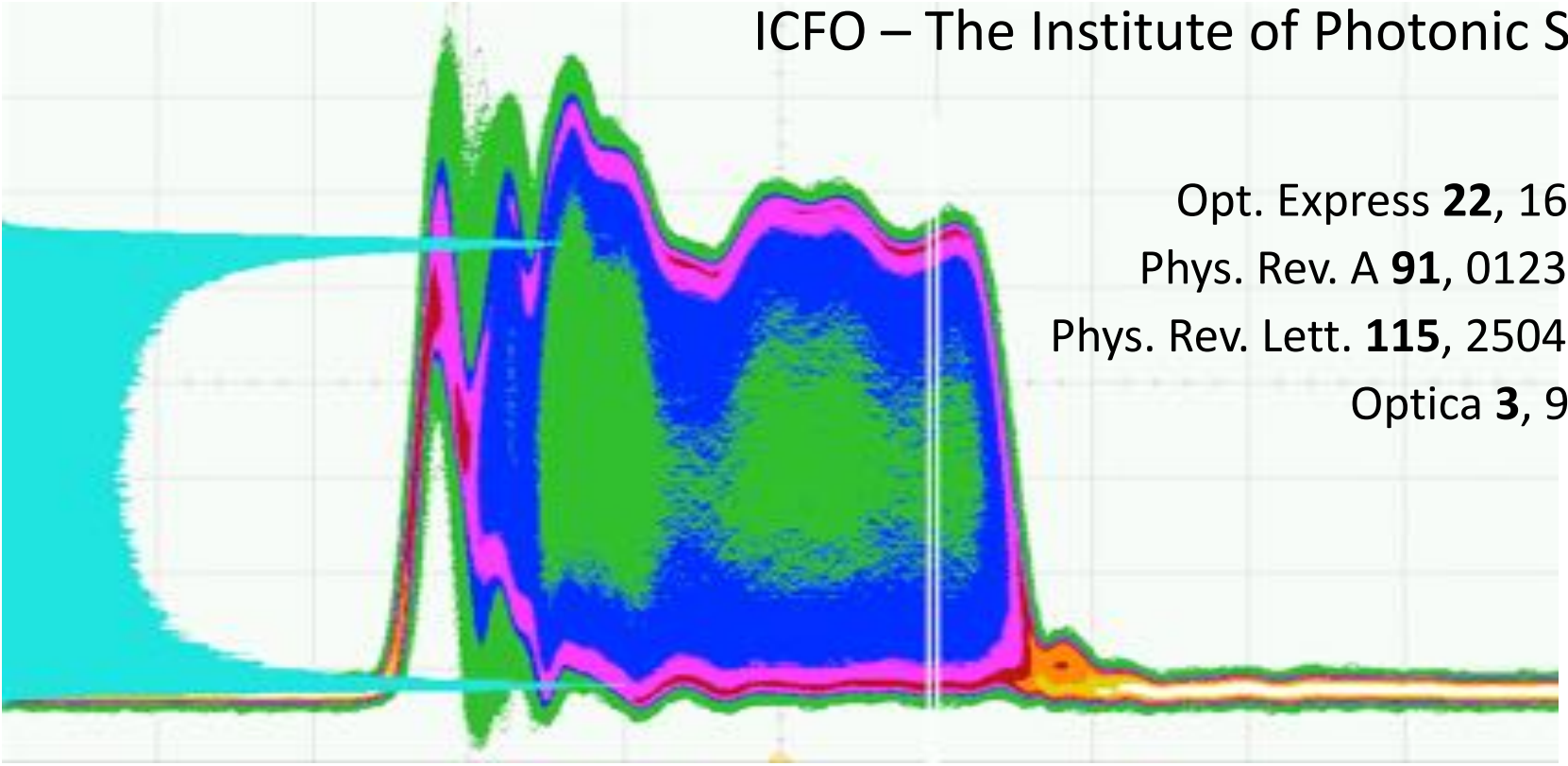
Metrological approach to quantum random number generation (and a QRNG on a chip)



Morgan W. Mitchell
ICFO – The Institute of Photonic Sciences

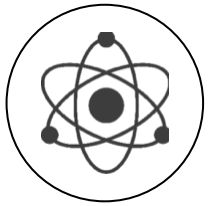


Opt. Express **22**, 1645 (2014)
Phys. Rev. A **91**, 012314 (2015)
Phys. Rev. Lett. **115**, 250403 (2015)
Optica **3**, 989 (2016)

Applications of randomness

communications and data security

high-performance computing



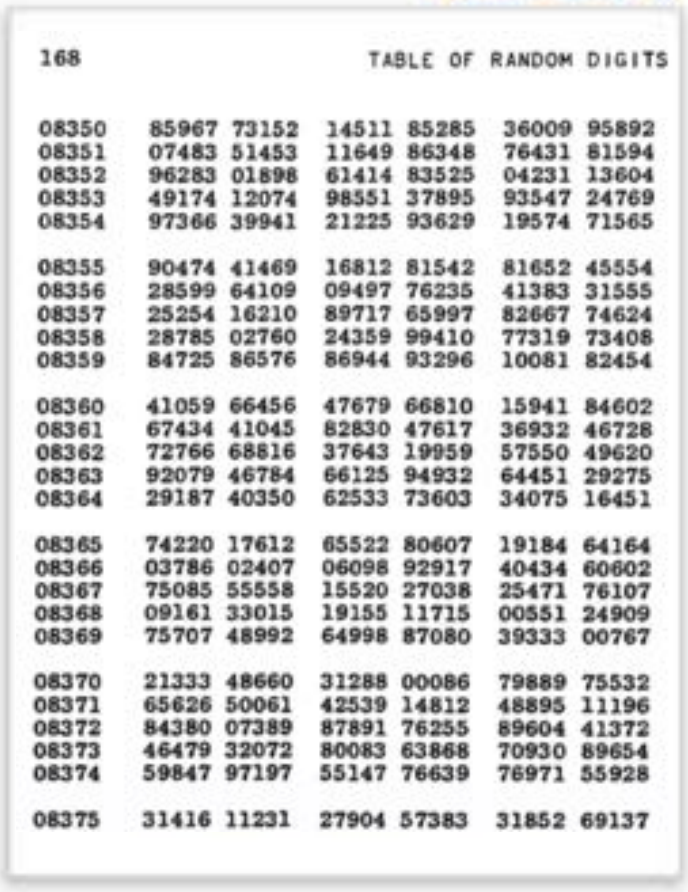
fundamental physics

A Million Random Digits with 100,000 Normal Deviates

by The RAND Corporation (Author)

682 customer reviews

Look inside



168 TABLE OF RANDOM DIGITS

08350	85967	73152	14511	85285	36009	95892
08351	07483	51453	11649	86348	76431	81594
08352	96283	01898	61414	83525	04231	13604
08353	49174	12074	98551	37895	93547	24769
08354	97366	39941	21225	93629	19574	71565
08355	90474	41469	16812	81542	81652	45554
08356	28599	64109	09497	76235	41383	31555
08357	25254	16210	89717	65997	82667	74624
08358	28785	02760	24359	99410	77319	73408
08359	84725	86576	86944	93296	10081	82454
08360	41059	66456	47679	66810	15941	84602
08361	67434	41045	82830	47617	36932	46728
08362	72766	68816	37643	19959	57550	49620
08363	92079	46784	66125	94932	64451	29275
08364	29187	40350	62533	73603	34075	16451
08365	74220	17612	65522	80607	19184	64164
08366	03786	02407	06098	92917	40434	60602
08367	75085	55558	15520	27038	25471	76107
08368	09161	33015	19155	11715	00551	24909
08369	75707	48992	64998	87080	39333	00767
08370	21333	48660	31288	00086	79889	75532
08371	65626	50061	42539	14812	48895	11196
08372	84380	07389	87891	76255	89604	41372
08373	46479	32072	80083	63868	70930	89654
08374	59847	97197	55147	76639	76971	55928
08375	31416	11231	27904	57383	31852	69137

published 1955, re-issued 2001

Top positive review

See all 489 positive reviews ›

1,890 people found this helpful

almost perfect

By a curious reader on October 26, 2006

Such a terrific reference work! But with so many terrific random digits, it's a shame they didn't sort them, to make it easier to find the one you're looking for.

There is no such thing as a random number – there are only methods to produce random numbers.

John von Neumann

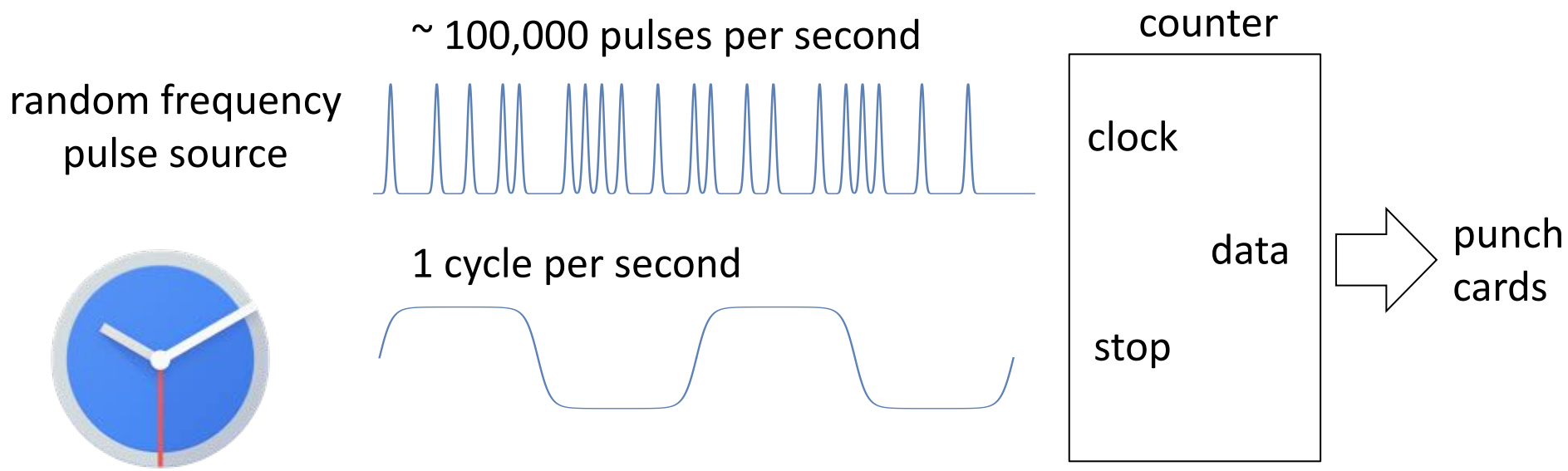
HISTORY OF RAND'S RANDOM DIGITS - SUMMARY

George W. Brown

P-113

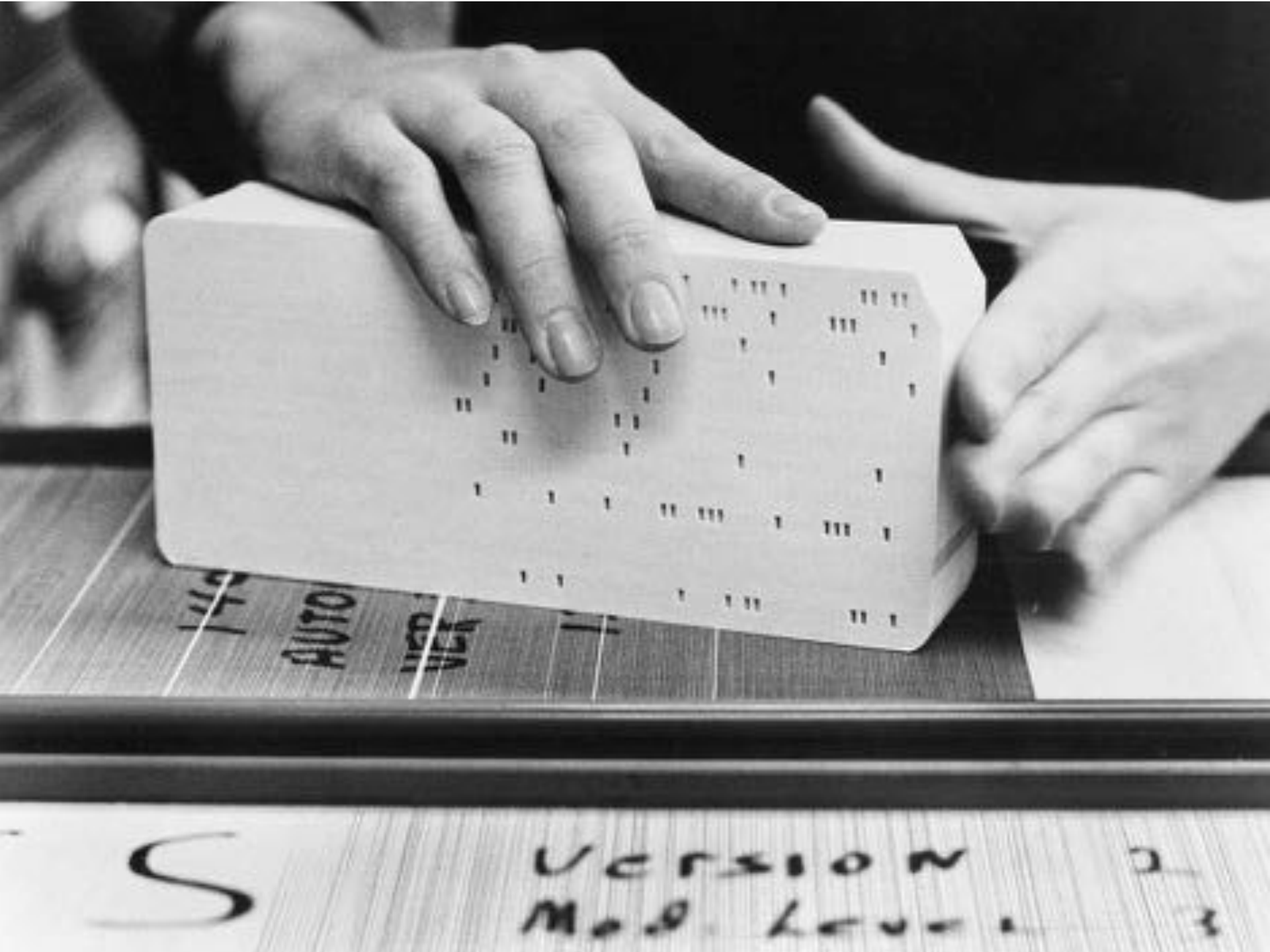
June 1949

—The RAND Corporation
• SANTA MONICA • CALIFORNIA—



PRODUCTION OF THE RANDOM DIGITS

The random digits in this book were produced by rerandomization of a basic table generated by an electronic roulette wheel. Briefly, a random frequency pulse source, providing on the average about 100,000 pulses per second, was gated about once per second by a constant frequency pulse. Pulse standardization circuits passed the pulses through a 5-place binary counter. In principle the machine was a 32-place roulette wheel which made, on the average, about 3000 revolutions per trial and produced one number per second. A binary-to-decimal converter was used which converted 20 of the 32 numbers (the other twelve were discarded) and retained only the final digit of two-digit numbers; this final digit was fed into an IBM punch to produce finally a punched card table of random digits.


AUTO

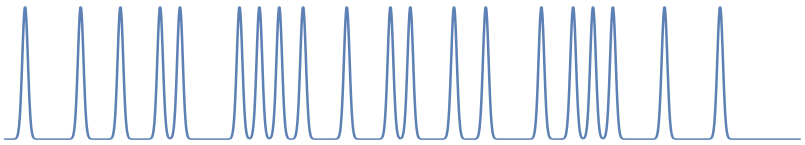
	BLOCK 1		BLOCK 2	
	χ^2	*Probability*	χ^2	*Probability*
Frequency (9 d.f.*)	6.0	.74	21.0	.02
Odd-even (1 d.f.)	3.0	.09	7.0	<.01
Serial (81 d.f.)	78.7	.55	105.6	.03

recently “tuned up” one month later

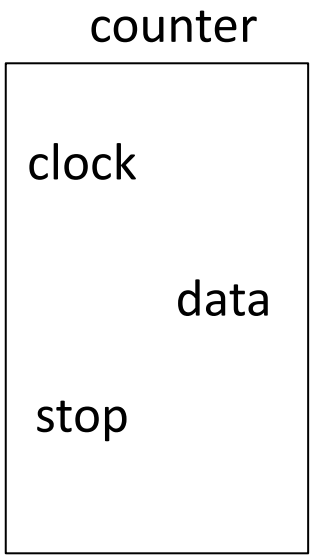
Production from the original machine showed statistically significant biases, and the engineers had to make several modifications and refinements of the circuits before production of apparently satisfactory numbers was achieved. The basic table of a million digits was then produced during May and June of 1947. This table was subjected to fairly exhaustive tests and it was found that it still contained small but statistically significant biases. For example, the following table‡ shows the results of three tests (described later) on two blocks of 125,000 digits:

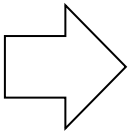
random frequency pulse source

~ 100,000 edges per second



1 cycle per second

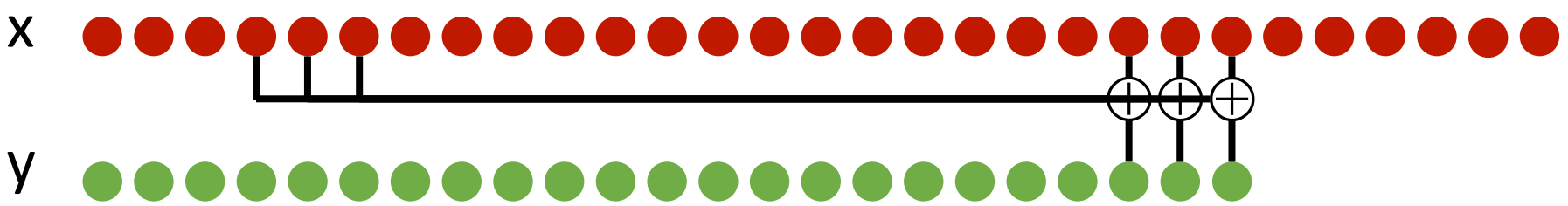




punch cards

Observation: need to worry about your conversion to stable data, even if your basic source is completely random.

$$y_i = (x_i + x_{i-50}) \mod 10$$



At this point we had our original million digits, 20,000 I.B.M. cards with 50 digits to a card, with the small but perceptible odd-even bias disclosed by the statistical analysis. It was now decided to rerandomize the table, or at least alter it, by a little roulette playing with it, to remove the odd-even bias. We added (mod 10) the digits in each card, digit by digit, to the corresponding digits of the previous card.

The derived table of one million digits was then subjected to the various standard tests, frequency tests, serial tests, poker tests, etc. These million digits have a clean bill of health and have been adopted as RAND's table of random digits.

168 TABLE OF RANDOM DIGITS

08350	85967 73152	14511 85285	36009 95892
08351	07483 51453	11649 86348	76431 81594
08352	96283 01898	61414 83525	04231 13604
08353	49174 12074	98551 37895	93547 24769
08354	97366 39941	21225 93629	19574 71565
08355	90474 41469	16812 81542	81652 45554
08356	28599 64109	09497 76235	41383 31555
08357	25254 16210	89717 65997	82667 74624
08358	28785 02760	24359 99410	77319 73408
08359	84725 86576	86944 93296	10081 82454
08360	41059 66456	47679 66810	15941 84602
08361	67434 41045	82830 47617	36932 46728
08362	72766 68816	37643 19959	57550 49620
08363	92079 46784	66125 94932	64451 29275
08364	29187 40350	62533 73603	34075 16451
08365	74220 17612	65522 80607	19184 64164
08366	03786 02407	06098 92917	40434 60602
08367	75085 55558	15520 27038	25471 76107
08368	09161 33015	19155 11715	00551 24909
08369	75707 48992	64998 87080	39333 00767
08370	21333 48660	31288 00086	79889 75532
08371	65626 50061	42539 14812	48895 11196
08372	84380 07389	87891 76255	89604 41372
08373	46479 32072	80083 63868	70930 89654
08374	59847 97197	55147 76639	76971 55928
08375	31416 11231	27904 57383	31852 69137

★★★☆☆ **Weirdest sudoku book ever**

By John Peter O'connor on October 6, 2012

Format: Paperback

This has got to be the most useless set of sudoku puzzles ever.

In my copy of the book, all of the puzzles were already filled in which I find really annoying and what is worse, most of them have been filled in wrongly.

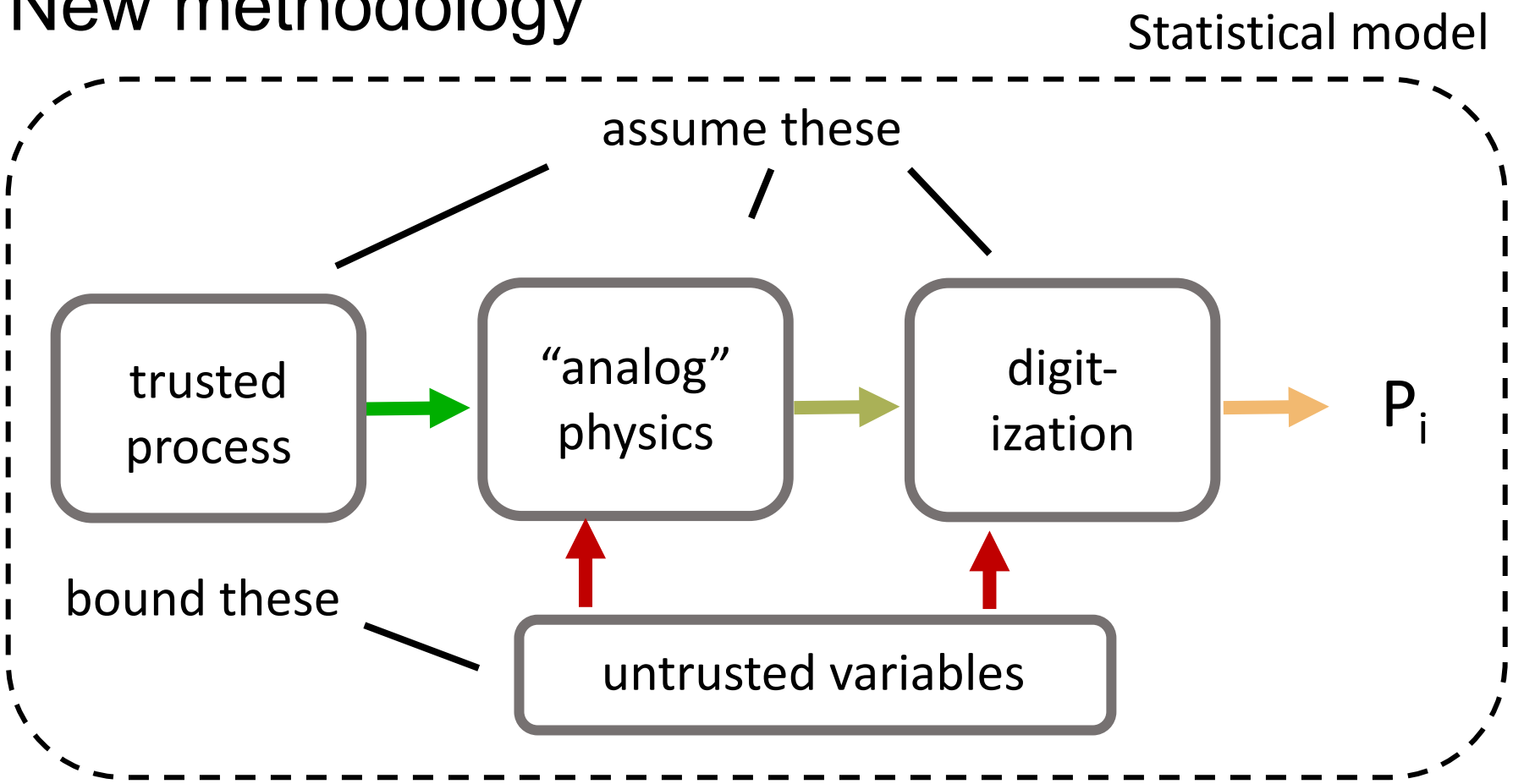
physical RNG strategy in 1949

1) Make a device that you think should be random.
2) Use statistical tests to assess how random it really is
3) Massage the data until they pass the tests.

physical RNG strategy in ~ 2010

1) device -> quantum process
2) “frequency tests etc.” -> Diehard(er), NIST, Crush, TestU01
3) ”a little roulette playing” -> randomness extraction

New methodology

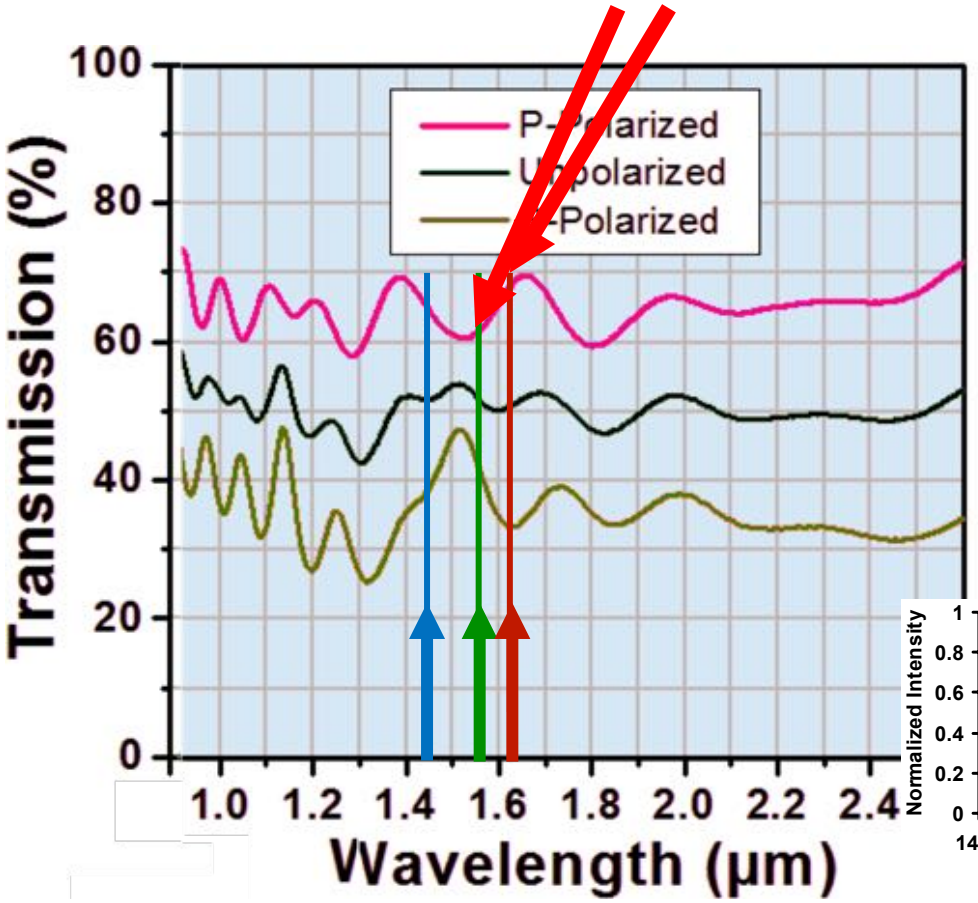


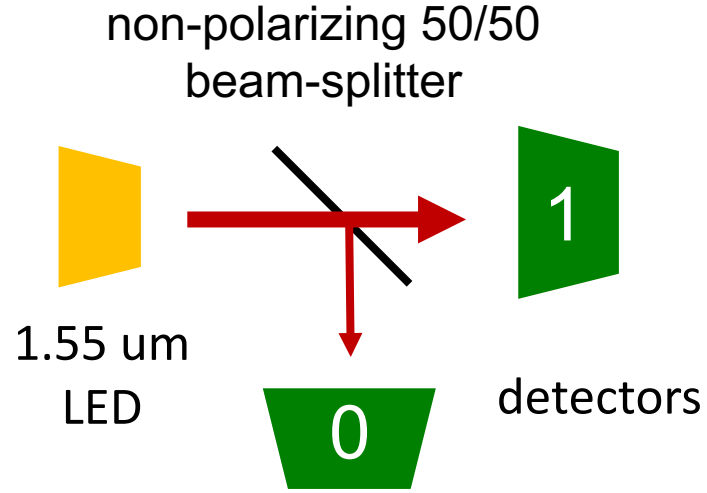
Inspired in metrology, e.g. precision spectroscopy

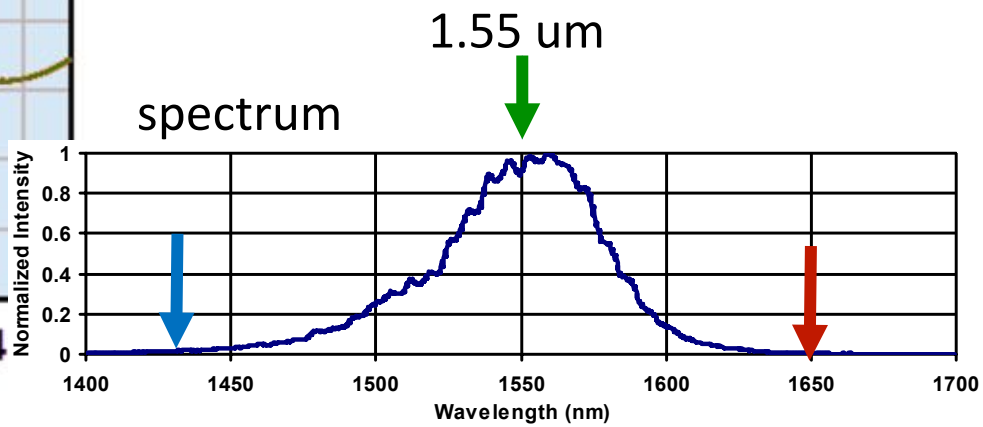
Mitchell et al. "Strong guarantees in ultrafast quantum random number generation" Physical Review A, 2015

Hypothetical example

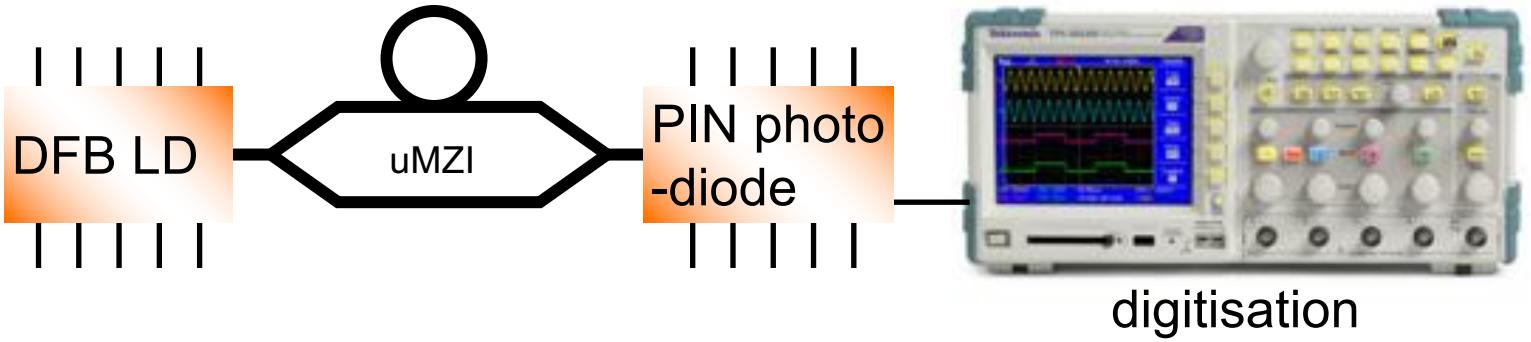
$$P(d=1) < 0.63$$







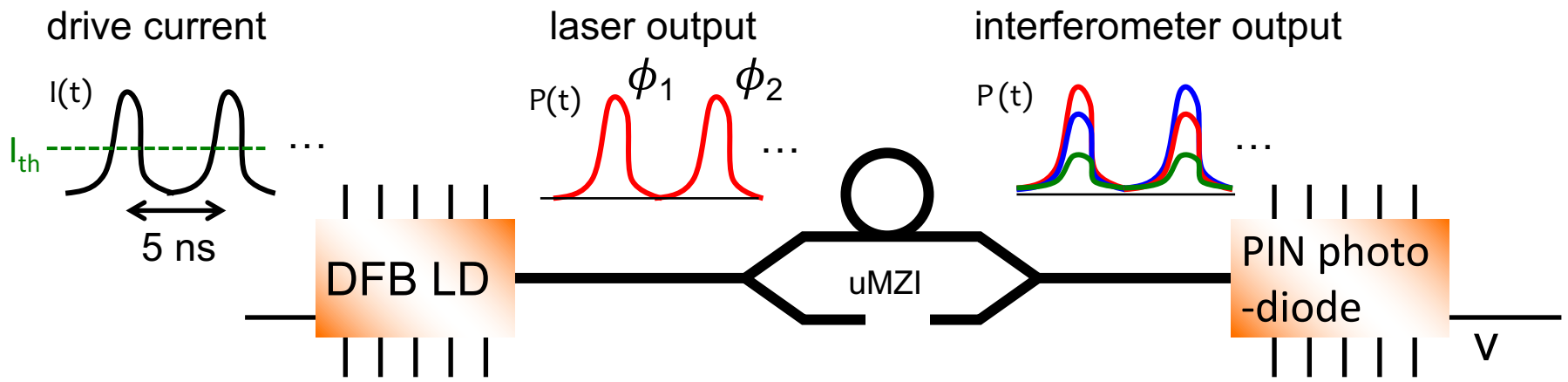
phase diffusion randomness generation

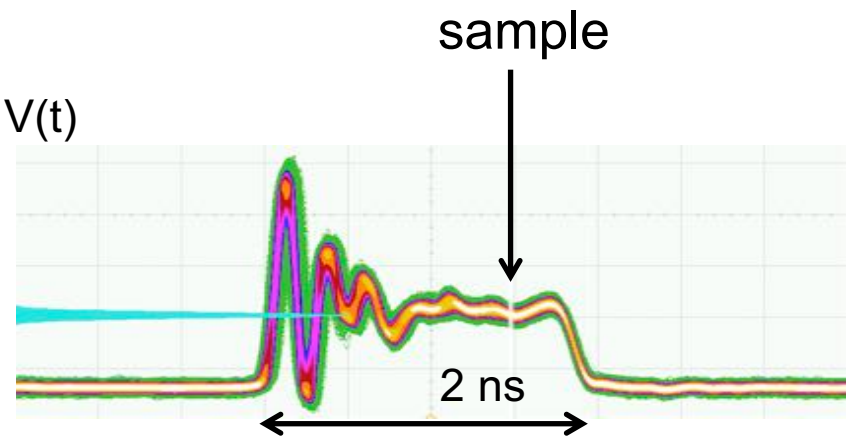


Macroscopic signals, high-speed + low noise

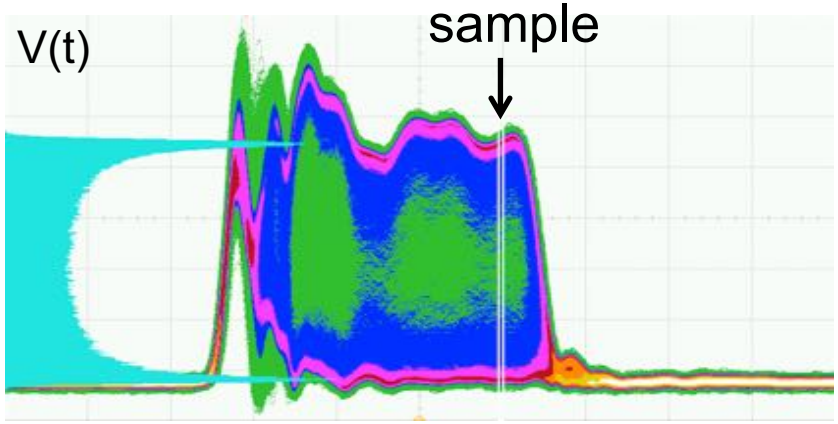
ICFO	1.1 Gbps	Jofre, et al. Opt. Express 2011
Toronto	6 Gbps	Xu, et al. Opt. Express 2012
ICFO	43 Gbps	Abellán, et al. Opt. Express 2014
Toshiba	20/80* Gbps	Yuan, et al. Appl. Phys. Lett. 2014
Hefei	68 Gbps	Nie, et al. Rev. Sci. Inst. 2015
		*randomness not claimed
ICFO	photonic IC	Abellán, et al. Optica 2016

accelerated phase-diffusion RNG





single-arm output



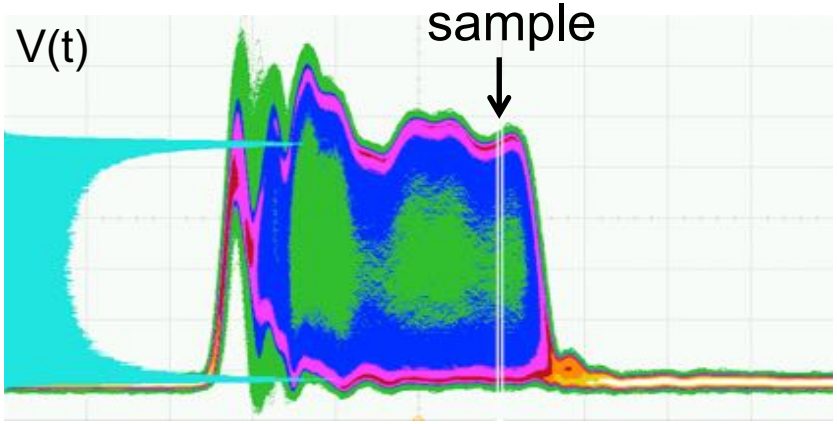
interferometer output

arcsine distribution

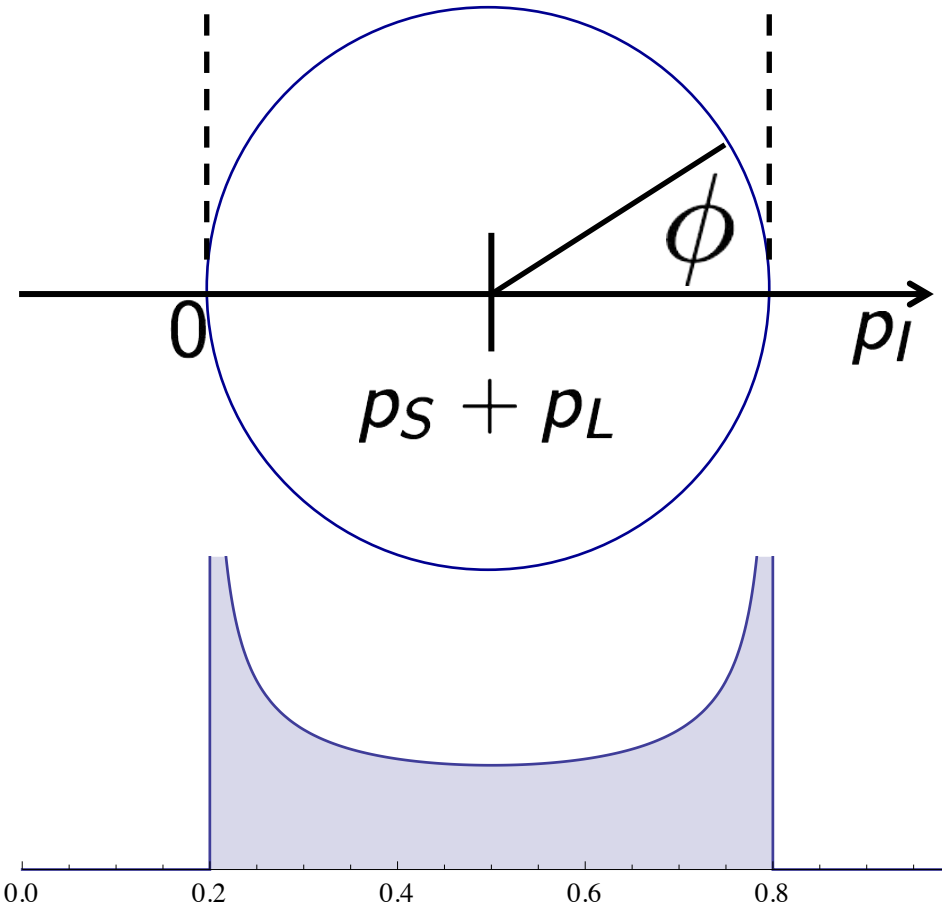
$$p_I(t) = p_S(t) + p_L(t) + 2\sqrt{p_S(t)p_L(t)}\cos\phi(t)$$

short path

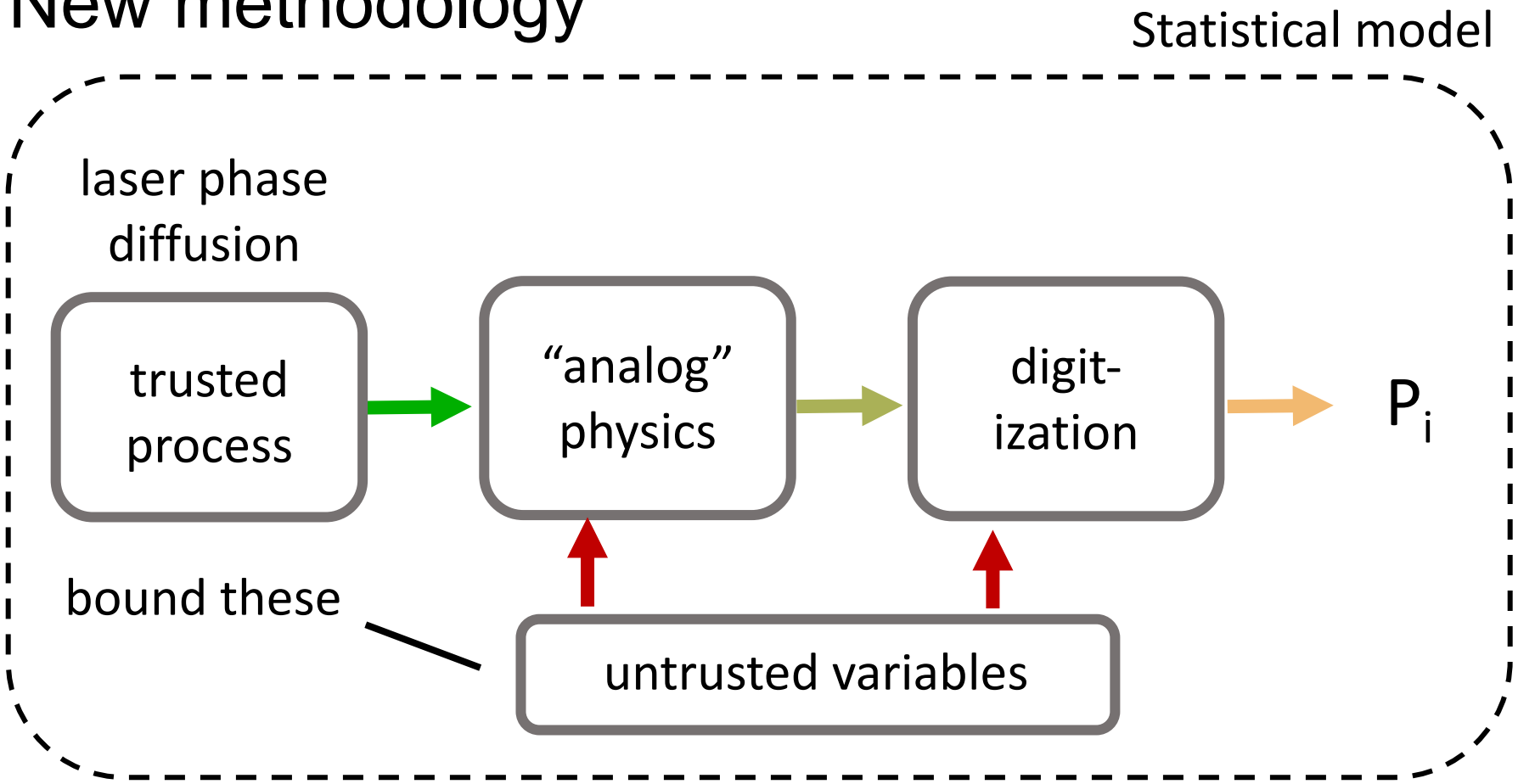
long path



interferometer output



New methodology

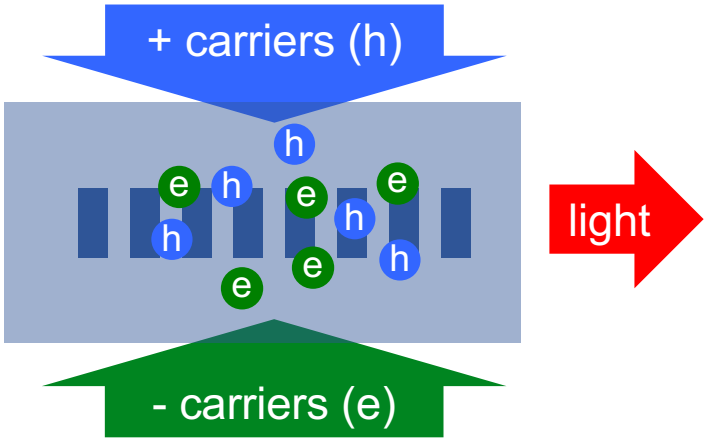


Inspired in metrology, e.g. precision spectroscopy

Mitchell et al. "Strong guarantees in ultrafast quantum random number generation" Physical Review A, 2015

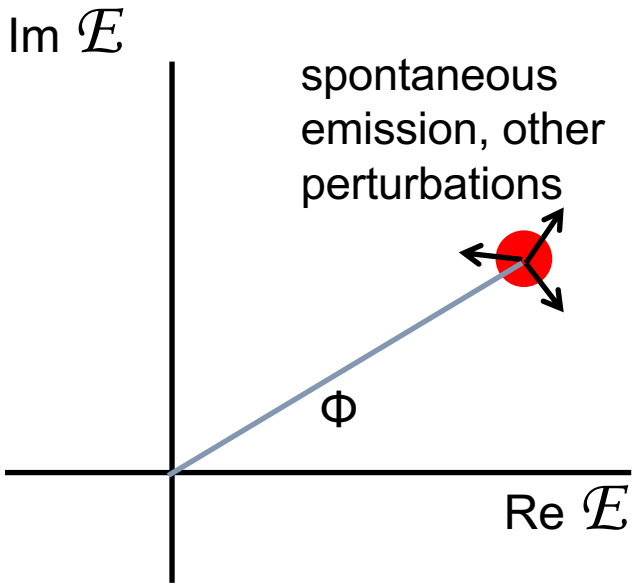
Phase diffusion driven by spontaneous emission

Distributed feedback laser



single spatial mode
single frequency mode

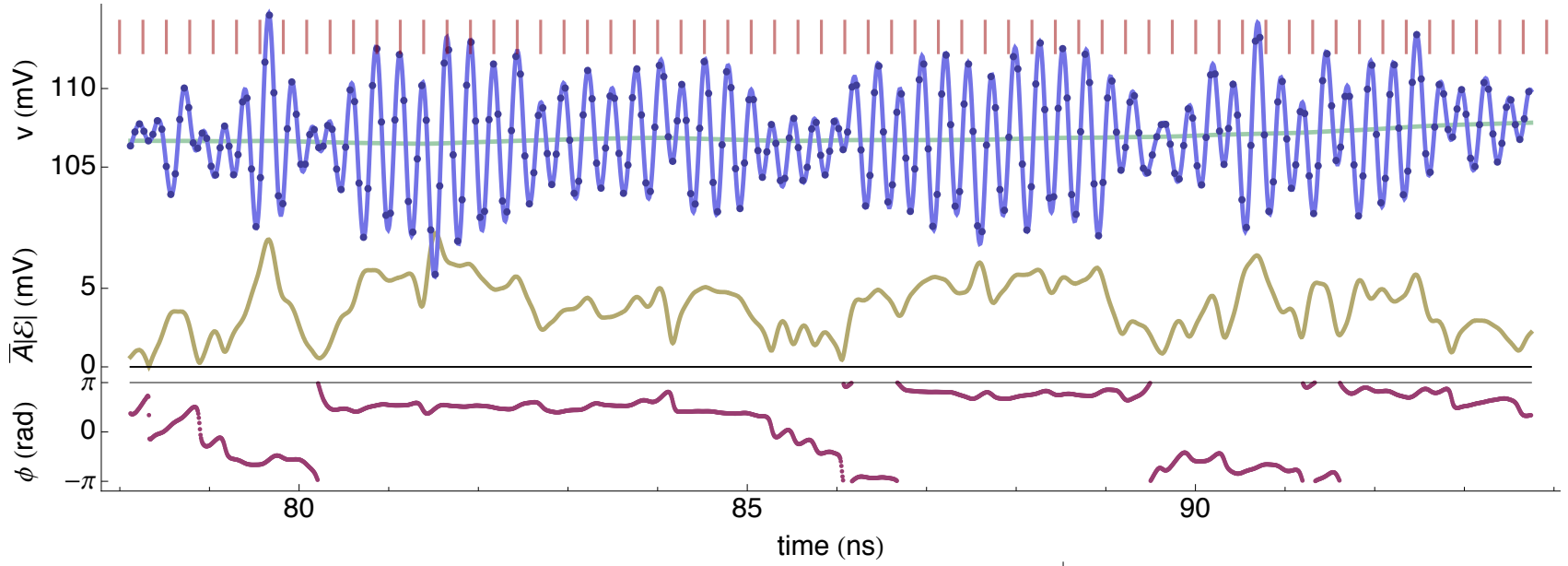
Intra-cavity field

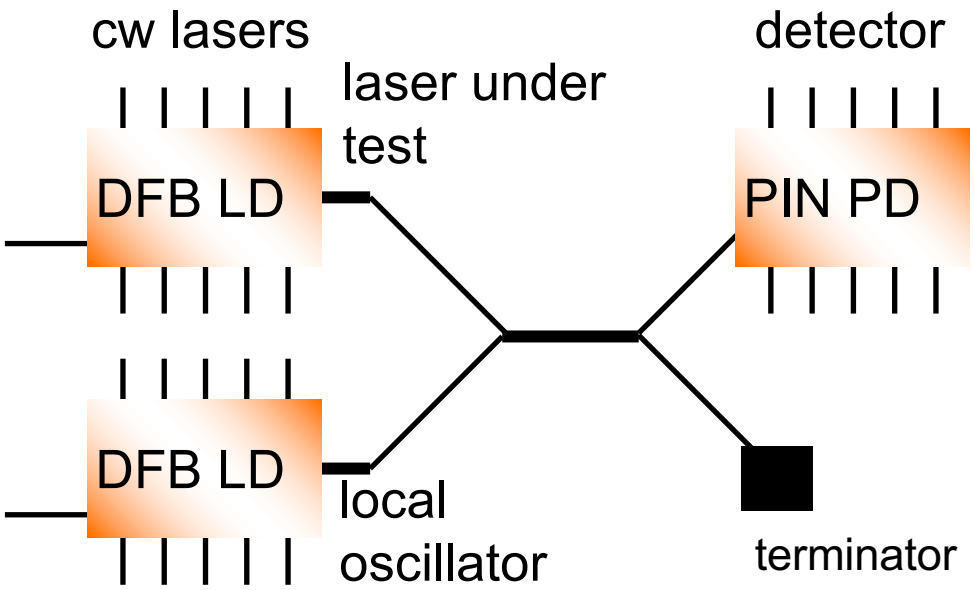


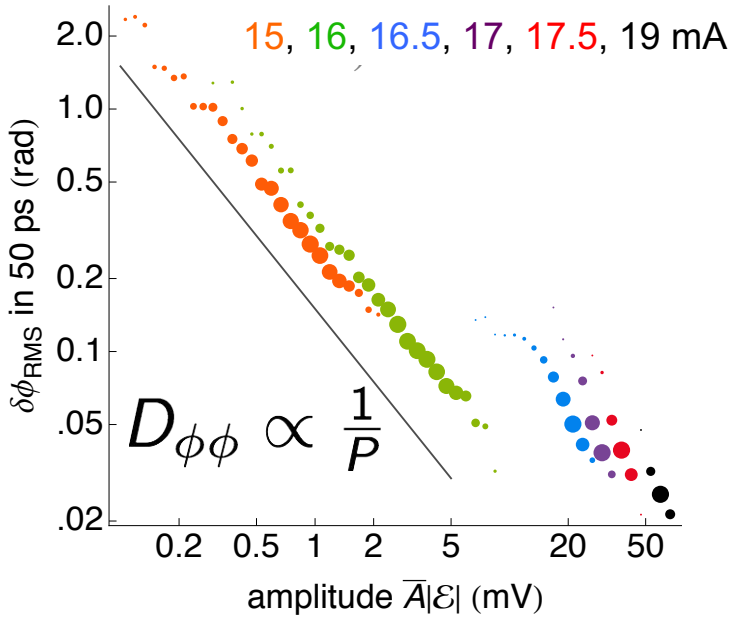
diffusion rate due to spontaneous emission

$$D_{\phi\phi} \propto \frac{1}{P}$$

photon number

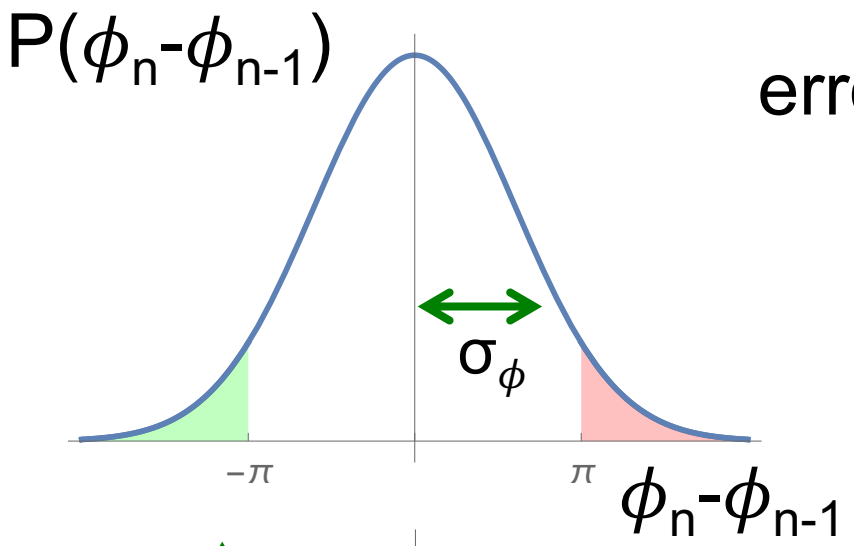


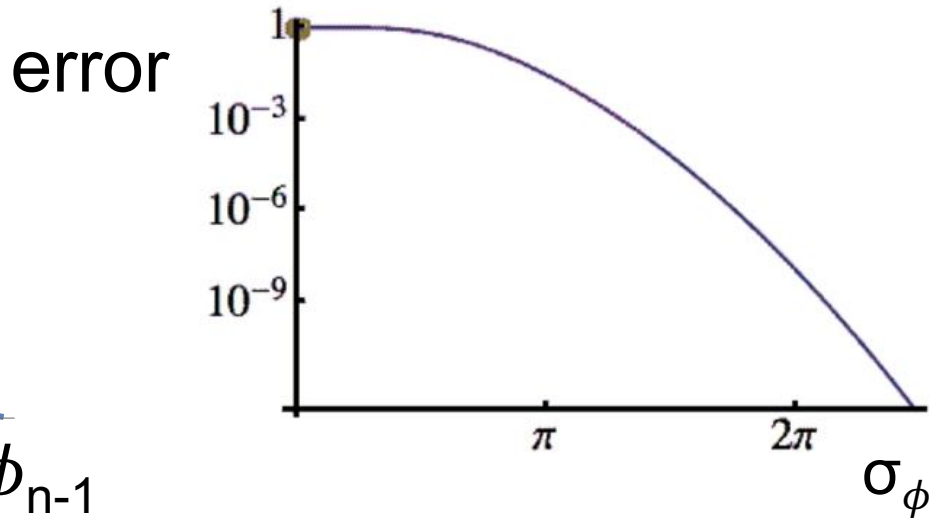


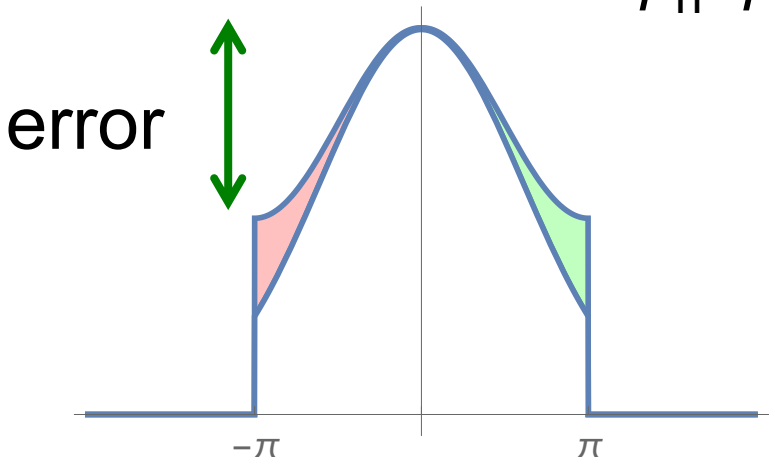


Morgan W. Mitchell, ICFO

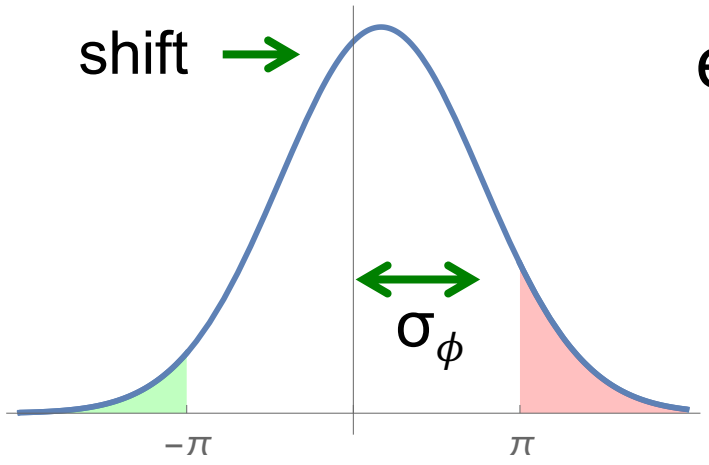
cyclic variables become very smooth

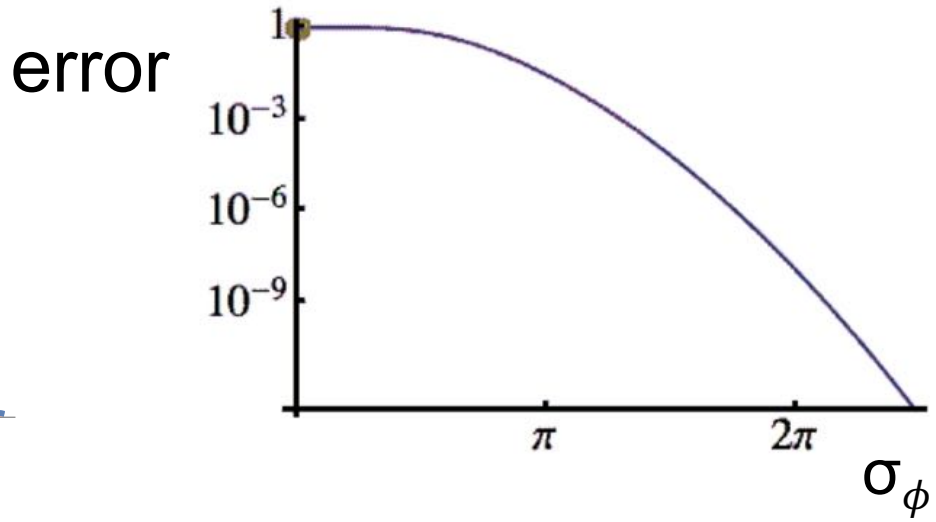


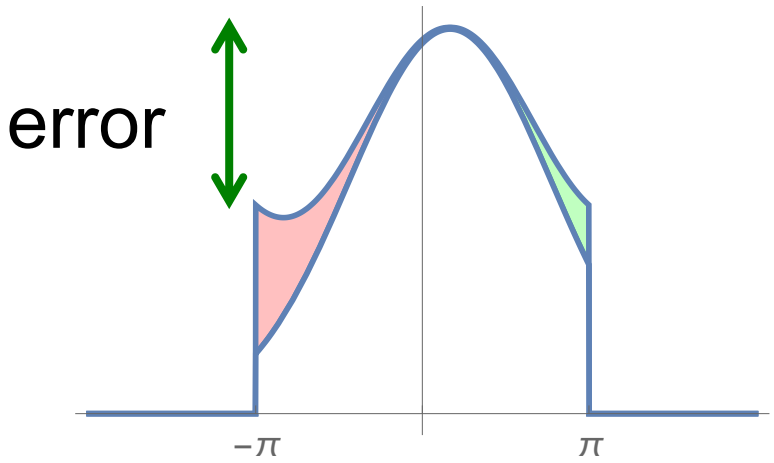




good phase + bad phase = good phase







“Analog physics”

$$p_I(t) = p_S(t) + p_L(t) + 2\sqrt{p_S(t)p_L(t)}\cos\phi(t)$$

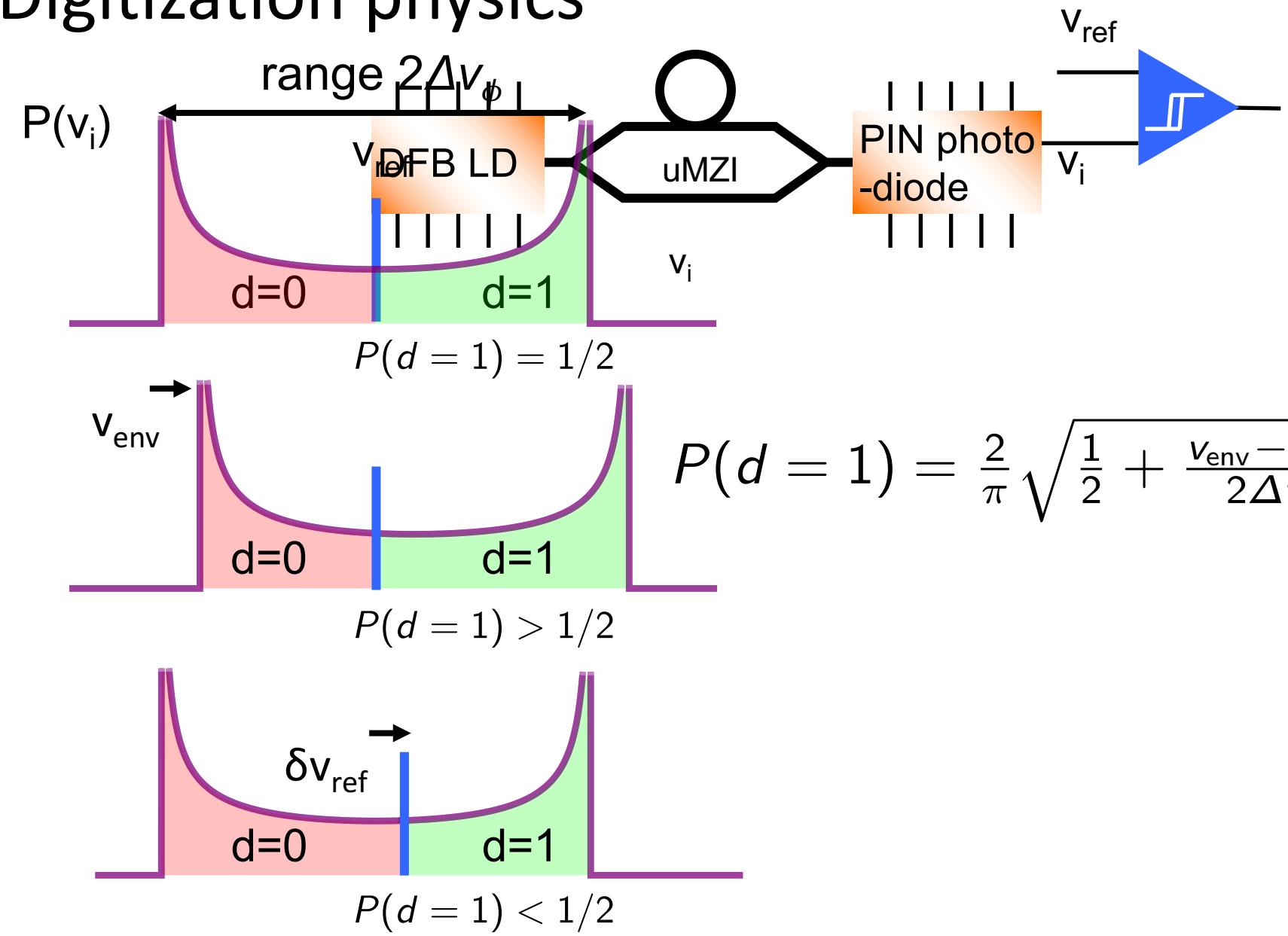
↓ finite speed of detector

$$v_I(t) = v_S(t) + v_L(t) + \underbrace{2\mathcal{V}\sqrt{v_S(t)v_L(t)}\cos\phi(t)}_{\text{trusted variable } v_\phi} + v_{h/o} + v_D$$

short path	long path	trusted variable v_ϕ range $\pm\Delta v_\phi$	hang-over	detector noise


1.93 V
1.43 V
930 mV
430 mV
-70 mV
-570 mV
-1.07 V
-1.57 V
-2.07 V
5.48 µs
5.50 µs
5.52 µs
5.54 µs
5.56 µs
5.58 µs
5.60 µs
5.62 µs
5.64 µs
5.66 µs
5.68 µs
20.0 ns/
5.5833000 µs
X1
X2
100.4 ns
100.9 ns
101.4 ns
101.9 ns
102.4 ns
102.9 ns
103.4 ns
103.9 ns
104.4 ns
104.9 ns
105.4 ns
500 ps/
102.8970 ns
Results
X1 102.397000 ns
X2 103.397000 ns
ΔX 1.000000 ns
1/ΔX 1.000000 GHz
Y1 -121.500 mV
Y2 -1.86000 mV
ΔY 119.640 mV
X Scale 241 hits/
X Offset 0 hits
Hist Mean 104.1 mV
Hist Std Dev 4.3 mV
Hist µ±1σ 70%
Hist µ±2σ 96%
Hist µ±3σ 100%
Hist p-p 35.2 mV
Hist Min 85.9 mV
Hist Max 121.1 mV
Bin Width 400 µV
Hist Median 103.9 mV
Hist Mode 103.1 mV
Hist Hits 26.080 khits
Hist Peak 962 hits

Digitization physics



$$P(d=1)=\frac{2}{\pi}\sqrt{\frac{1}{2}+\frac{v_{env}-\delta v_{ref}}{2\Delta v_\phi}}$$

Result of the statistical metrology

"bound" = 6 sigma
of observed variation

statistical model

$$P(d=1) = \frac{2}{\pi}\sqrt{\frac{1}{2} + \frac{v_{\text{env}} - \delta v_{\text{ref}}}{2\Delta v_\phi}}$$

← upper bound on this

← lower bound on this

upper bound on P(d)

$$P(d=1) < \tfrac{1}{2}(1+\epsilon)$$

$$\epsilon = 0.12$$

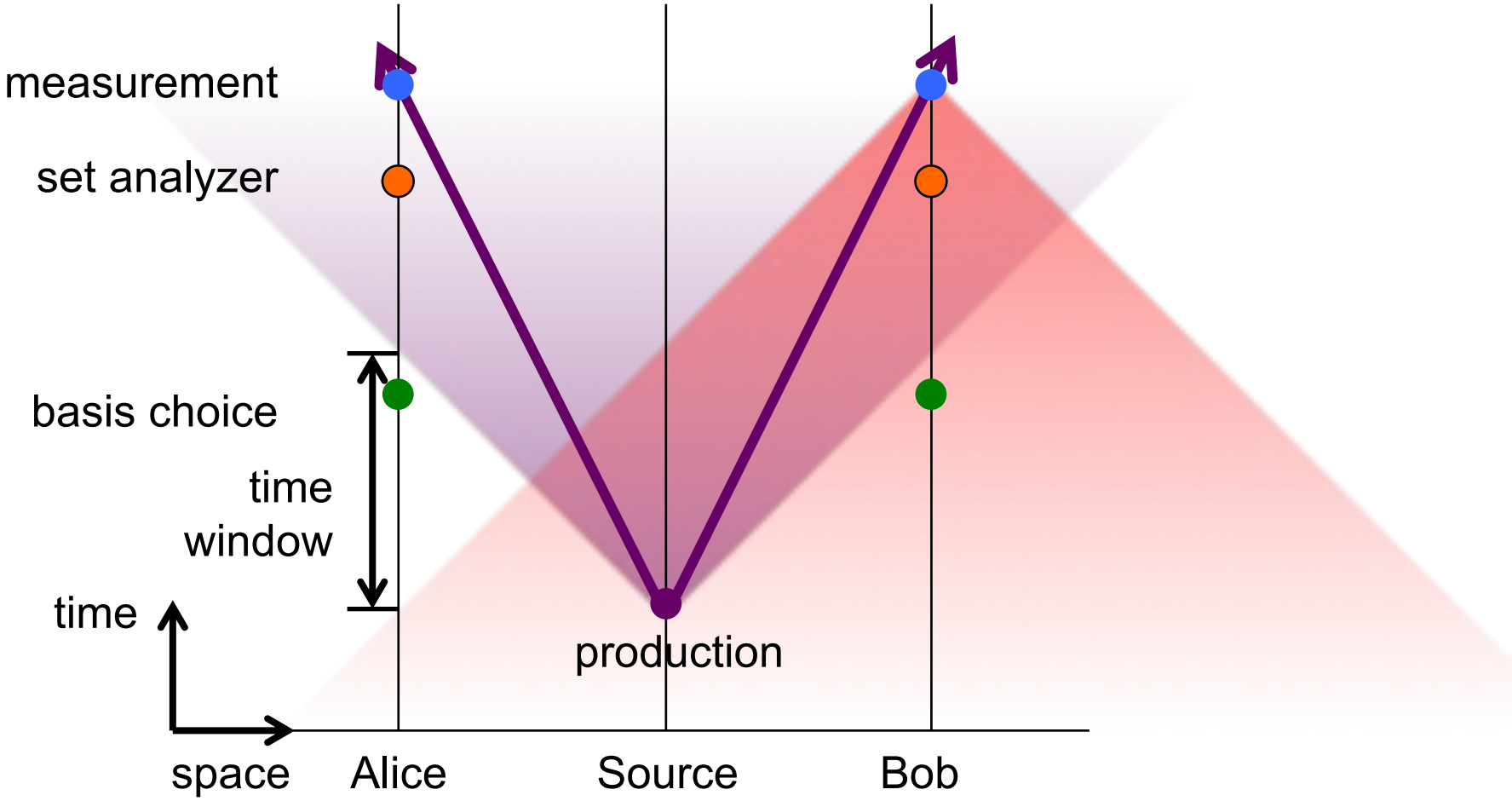
$$H_\infty > 0.83 \quad \text{bits}$$

Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

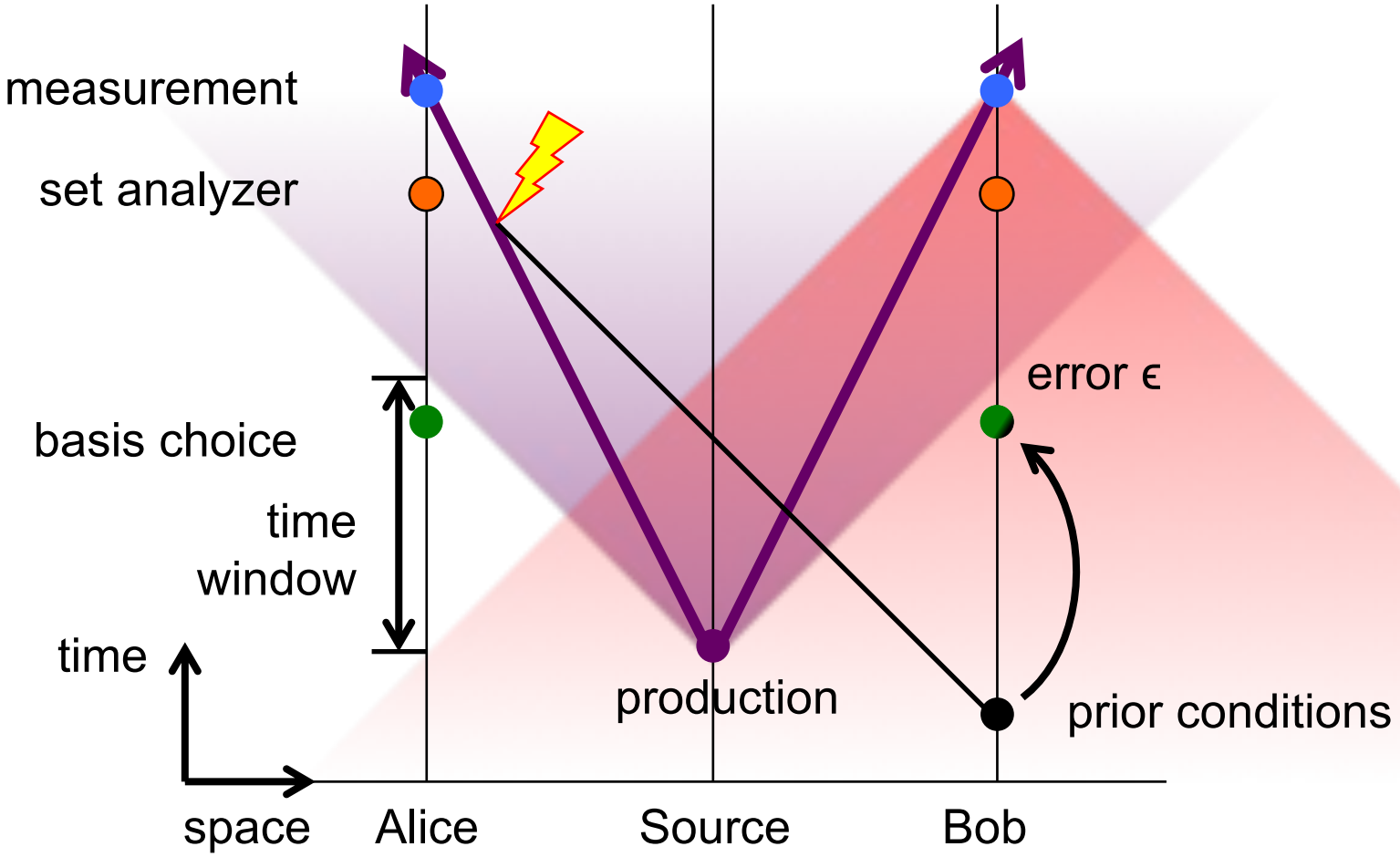
B. Hensen[1,2], H. Bernien[1,2]†, A. E. Dréau[1,2], A. Reiserer[1,2], N. Kalb[1,2], M. S. Blok[1,2], J. Ruitenberg[1,2], R. F. L. Vermeulen[1,2], R. N. Schouten[1,2], C. Abellán[3], W. Amaya[3], V. Pruneri[3,4], M. W. Mitchell[3,4], M. Markham[5], D. J. Twitchen[5], D. Elkouss[1], S. Wehner[1], T. H. Taminiau[1,2] & R. Hanson[1,2]

Nature, 29 Oct 2015

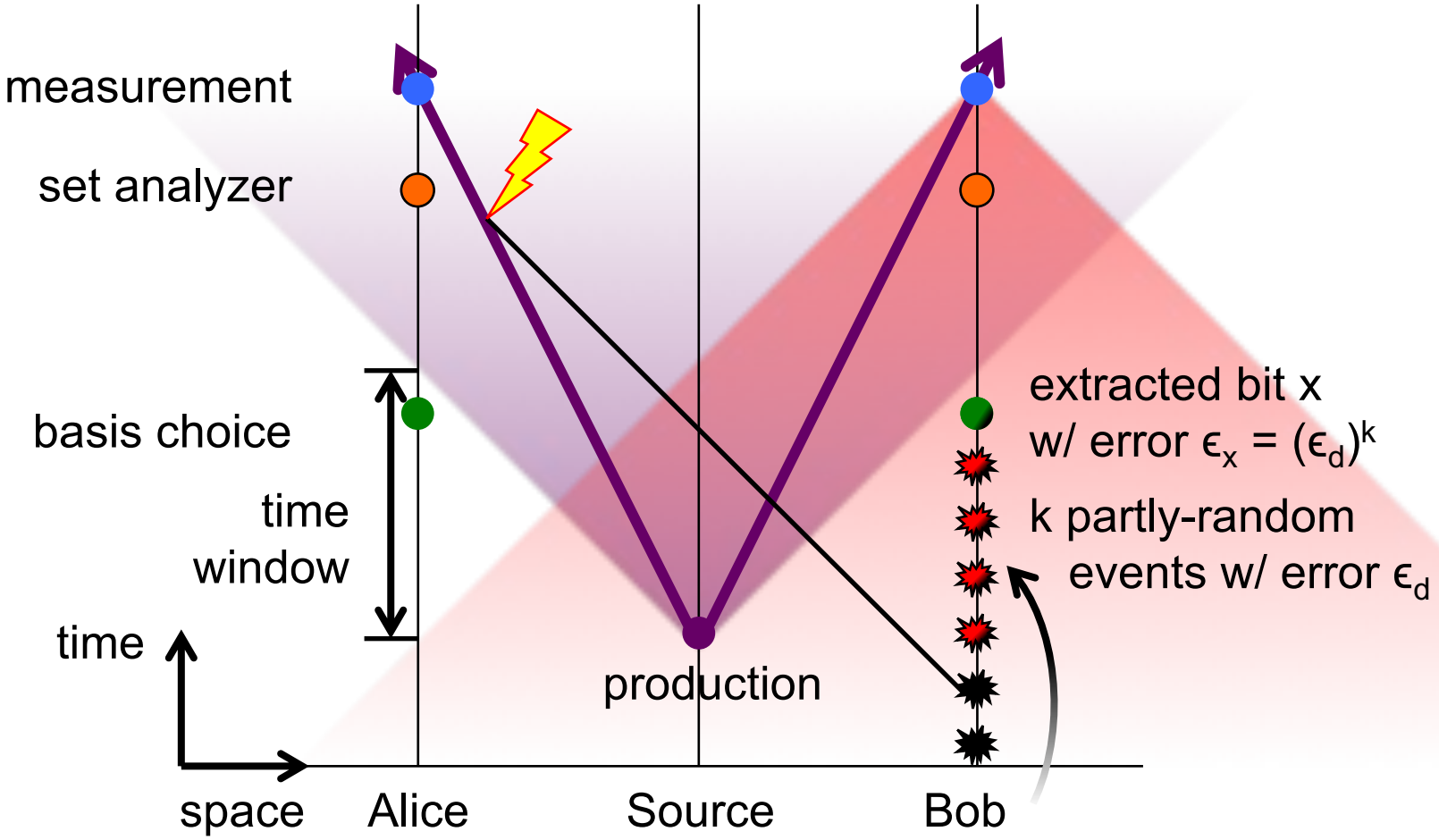
Bell test space-time loopholes



Bell test error tolerance



Bell test error tolerance




CML outputs
sync
LVTTL out
PLL control
ON
OFF
FRESH QUANTUM
RANDOM NUMBER
GENERATOR
ICFO
Institut
de Ciències
Fotòniques
ICFO

The New York Times

Sorry, Einstein. Quantum Study Suggests 'Spooky Action' Is Real.

By JOHN MARKOFF OCT. 21, 2015

Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometers
B. Hensen et al. Nature, 29 October 2015

A significant-loophole-free test of Bell's theorem with entangled photons
M. Giustina et al. Phys. Rev. Lett., 18 December 2015

A strong loophole-free test of local realism
L. Shalm et al. Phys. Rev. Lett., 18 December 2015

Generation of fresh and pure random numbers for loophole-free Bell tests
C. Abellan et al. Phys. Rev. Lett., 18 December 2015

Carlos Abellan

Waldimar Amaya

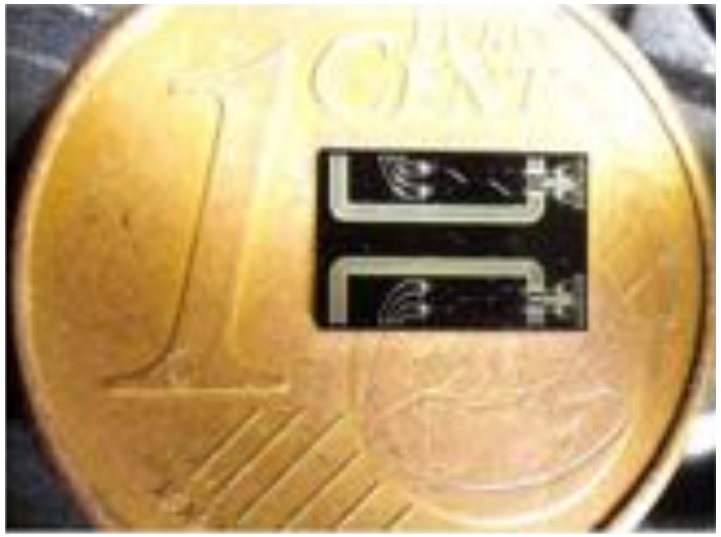
Morgan W. Mitchell, ICFO

optica

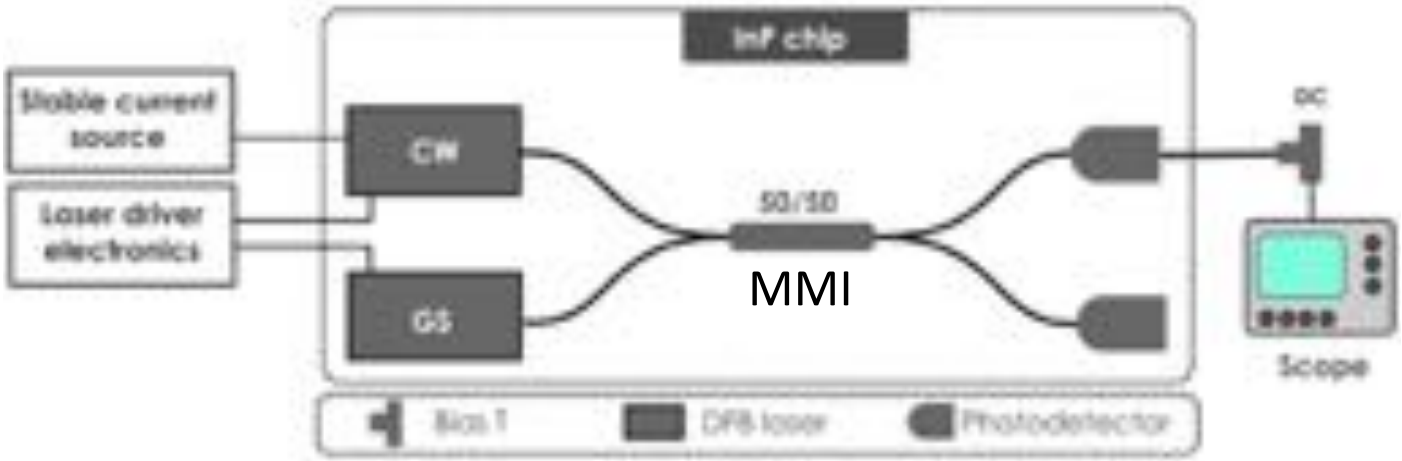
Quantum entropy source on an InP photonic integrated circuit for random number generation

Carlos Abellan,[1,*] Waldimar Amaya,[1] David Domenech,[2] Pascual Muñoz,[2,3] Jose Capmany,[2,3] Stefano Longhi,[4] Morgan W. Mitchell,[1,5] and Valerio Pruneri[1,5,6]

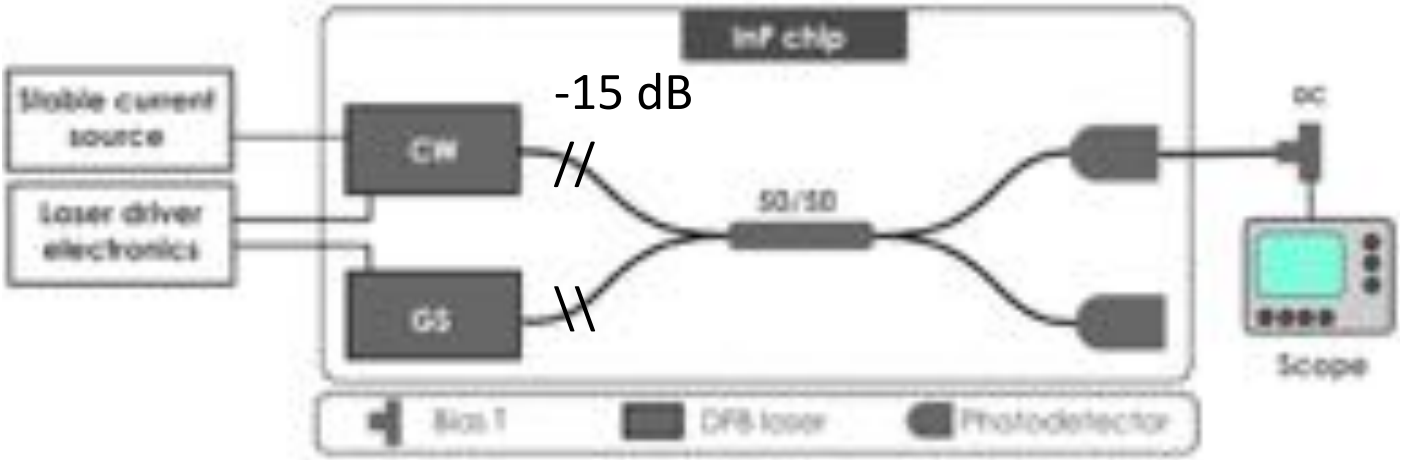
2016

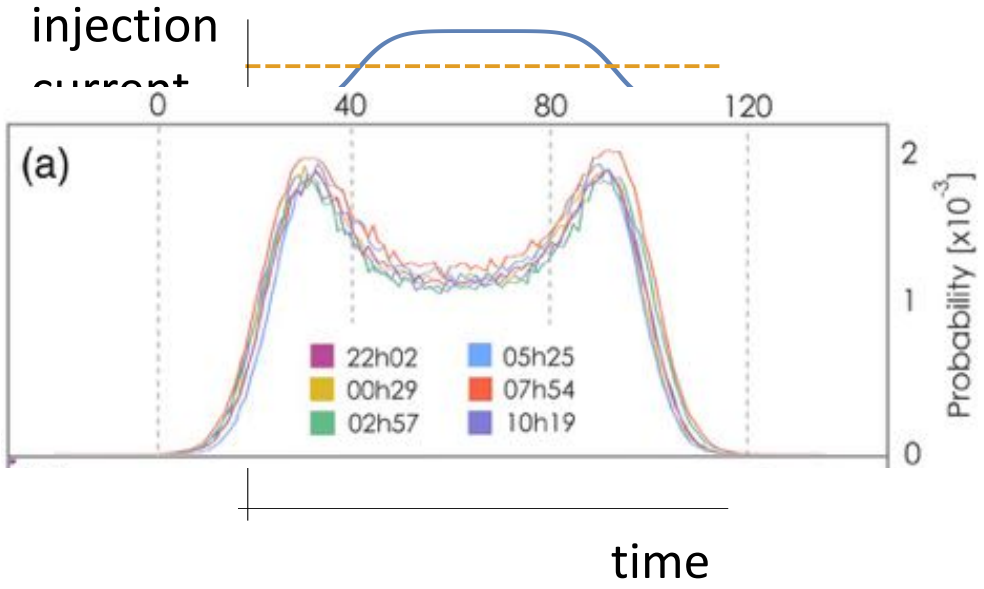


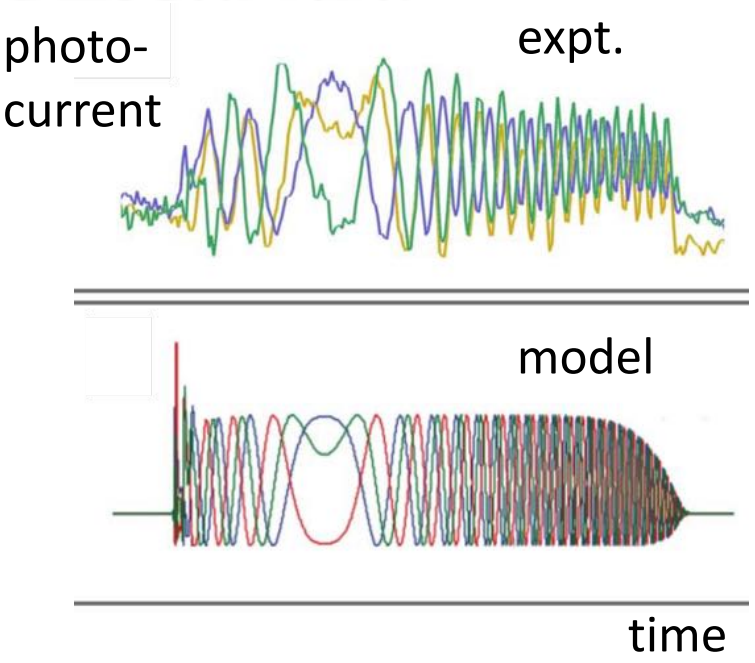
Device design



Two-laser strategy







Conclusions and outlook

Methodology for rigorous experimental justification of quantum randomness claims.

High-speed randomness generation, up to 43 Gbps.

Integration in InP using a two-laser strategy.

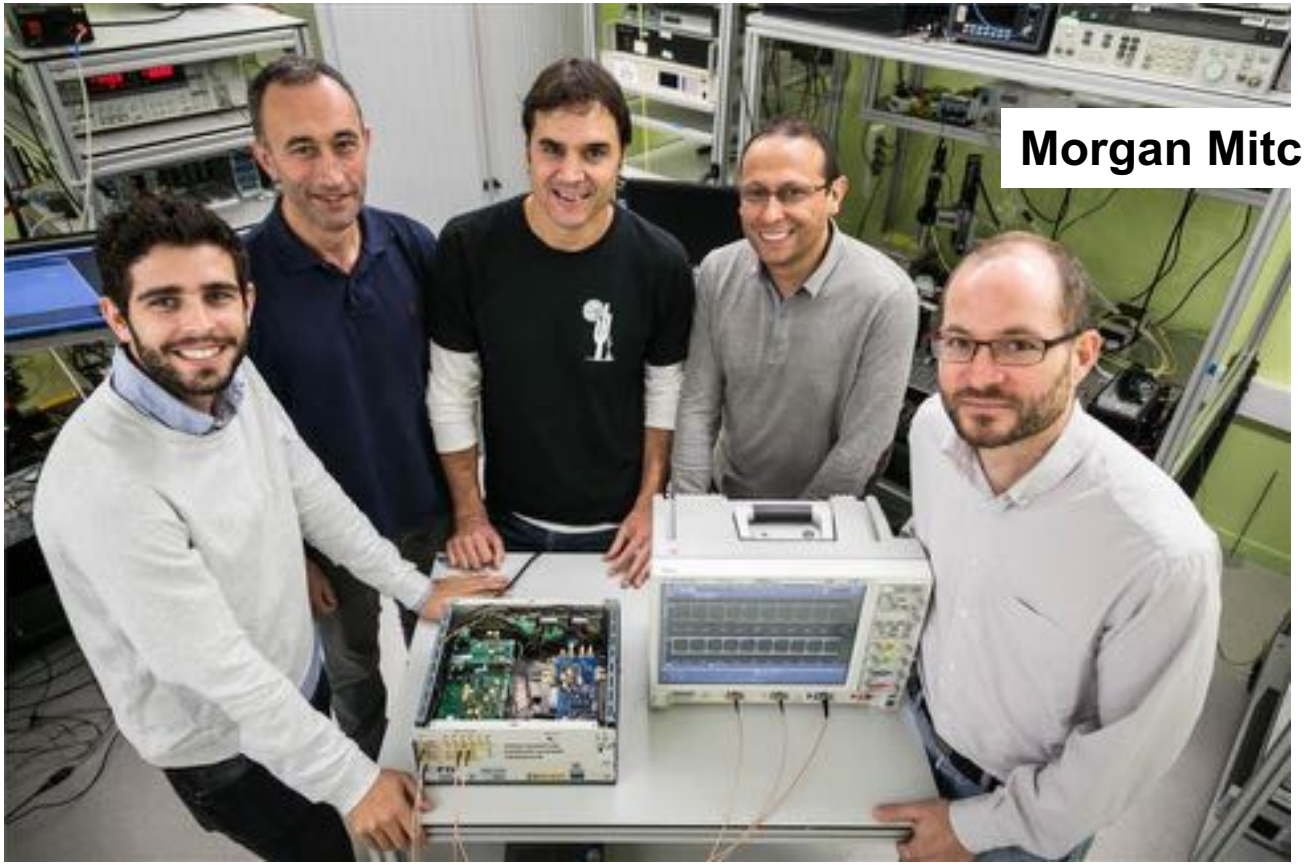
Ongoing work

Rigorous modeling/characterization of the two-laser problem.

ICFO QRNG Collaboration

Valerio Pruneri Daniel Mitrani Waldimar Amaya

Carlos Abellán



Morgan Mitchell

external:

David Domenech
Pascual Muñoz
Jose Capmany
Stefano Longhi
Marcos Curty

erc

MINISTERIO DE CIENCIA E INNOVACIÓN

icrea
Institució Catalana de Recerca i Estudis Avançats

ICFO
The Institute of Photonic Sciences

Generalitat de Catalunya

Fundació Privada CELLEX