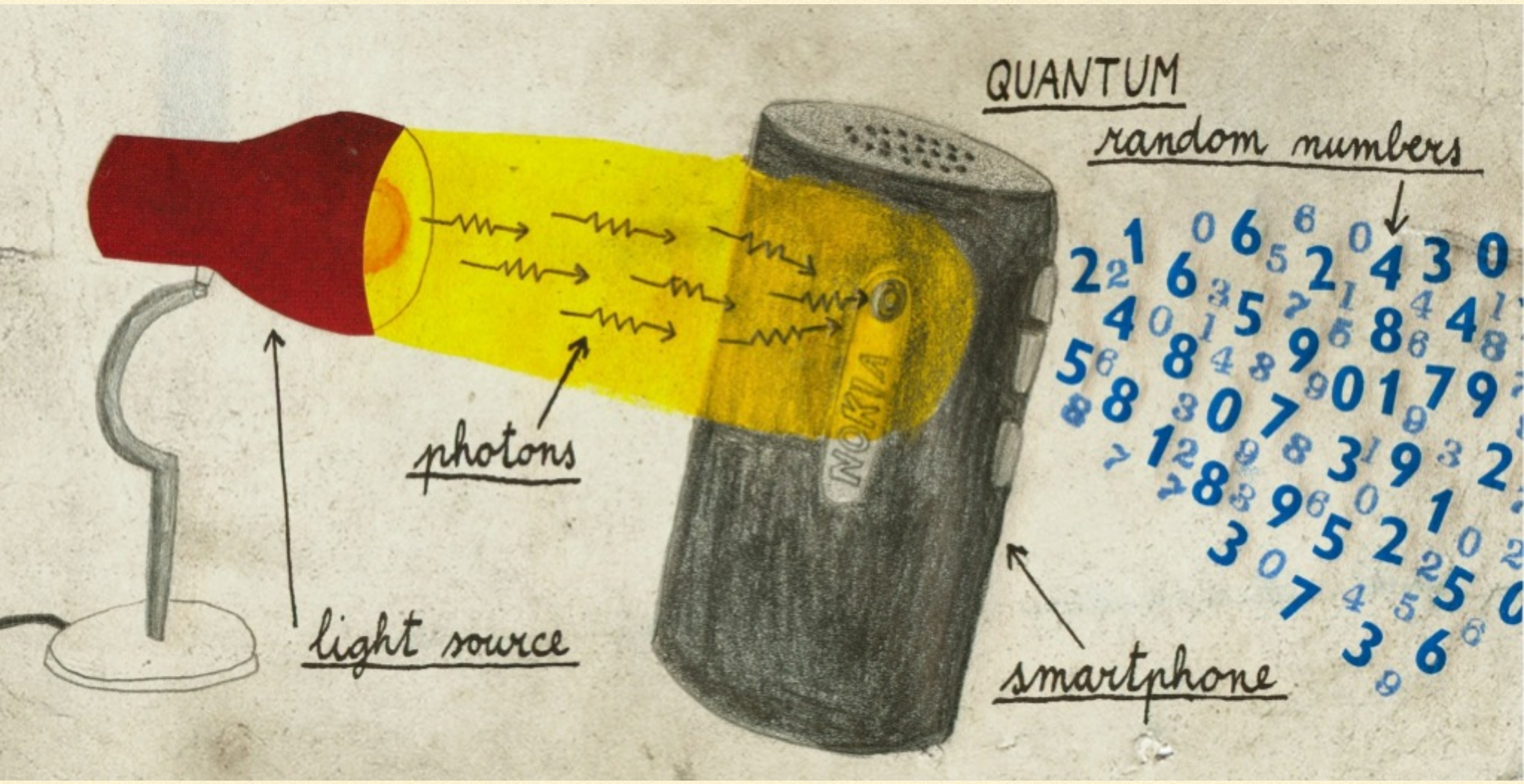
QUANTUM RANDOM NUMBER GENERATOR ON A MOBILE PHONE

Bruno Sanguinetti, Anthony Martin, Hugo Zbinden and Nicolas Gisin

UNIVERSITÉ DE GENÈVE

FACULTÉ DES SCIENCES



“The security of a cypher must reside entirely in the key”

auguste Kerckhoffs [1]

[1] A. Kerckhoffs. *Journal des sciences militaires*, vol. IX:38, 1883.

Compromising the security of the key compromises the system

[1] L. Bello. openssl – predictable random number generator. *Debian security advisory 1571-1*, 2008.

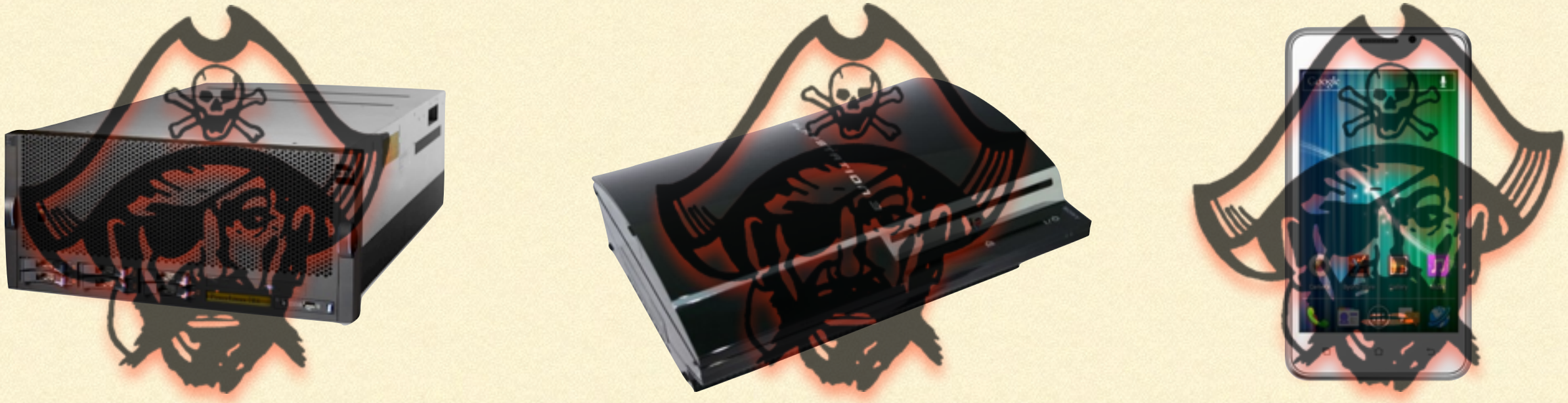
[2] Bushing, Marcan, Segher, and Sven. PS3 epic fail. 27th Chaos Communication Congress, 2010.

[3] R. Chirgwin. Android bug batters bitcoin wallets. The Register, 2013.

[4] L. Dorrendorf, Z. Gutterman, and B. Pinkas. Cryptanalysis of the random number generator of the windows operating system. *ACM Trans. Inf. Syst. Secur.*, 13(1):1–32, 2009.

[5] A. K. Lenstra, H. J. P., M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Ron was wrong, Whit is right. *Cryptology ePrint Archive*, 2012.

Compromising the security of the key compromises the system



[1] L. Bello. openssl – predictable random number generator. *Debian security advisory 1571-1*, 2008.

[2] Bushing, Marcan, Segher, and Sven. PS3 epic fail. 27th Chaos Communication Congress, 2010.

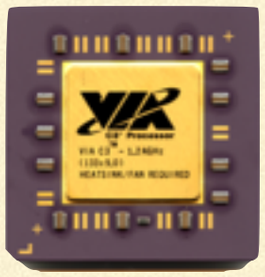
[3] R. Chirgwin. Android bug batters bitcoin wallets. The Register, 2013.

[4] L. Dorrendorf, Z. Gutterman, and B. Pinkas. Cryptanalysis of the random number generator of the windows operating system. *ACM Trans. Inf. Syst. Secur.*, 13(1):1–32, 2009.

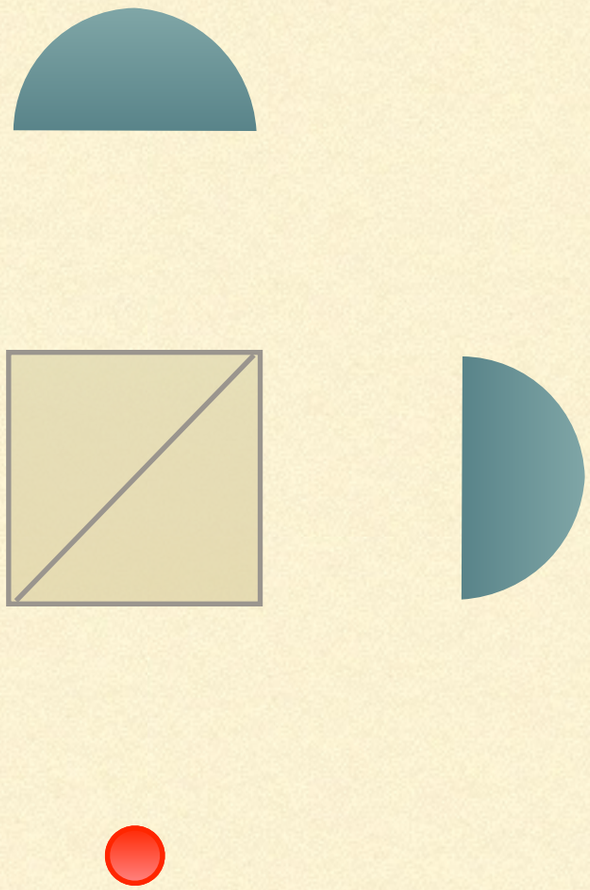
[5] A. K. Lenstra, H. J. P., M. Augier, J. W. Bos, T. Kleinjung, and C. Wachter. Ron was wrong, Whit is right. *Cryptology ePrint Archive*, 2012.

Current Commercial RNG implementations

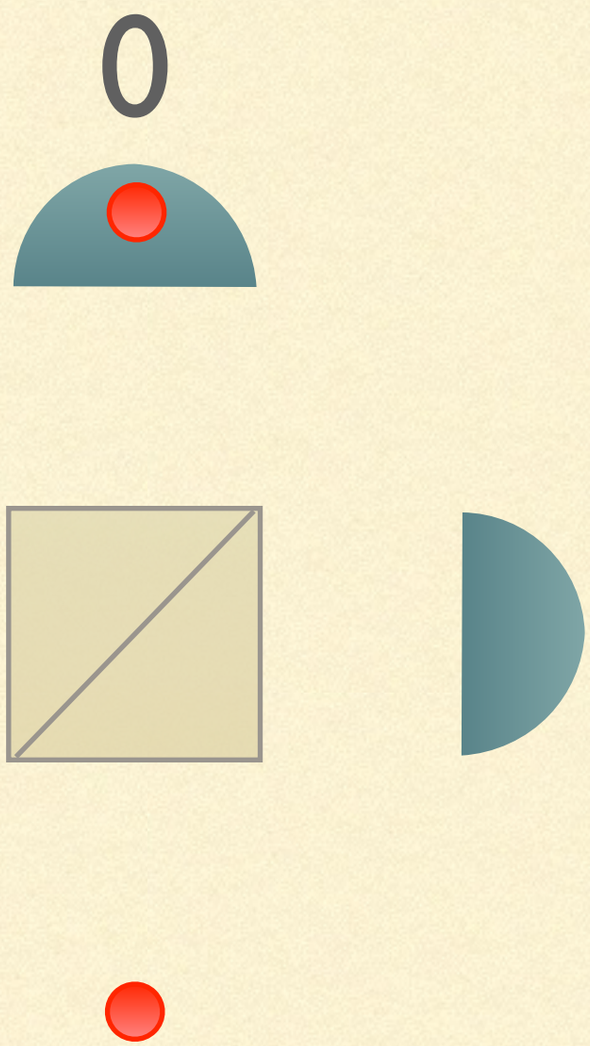
- Software (not random)
- Microphone (can be controlled)
- PLL (no one knows…)
- Shot noise in diode (slow)
- Quantis (“large” and “expensive”)



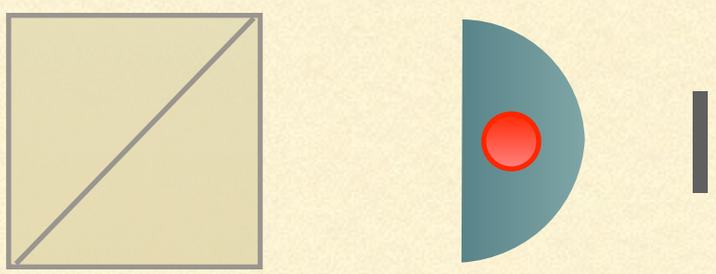
Simplified principle of operation



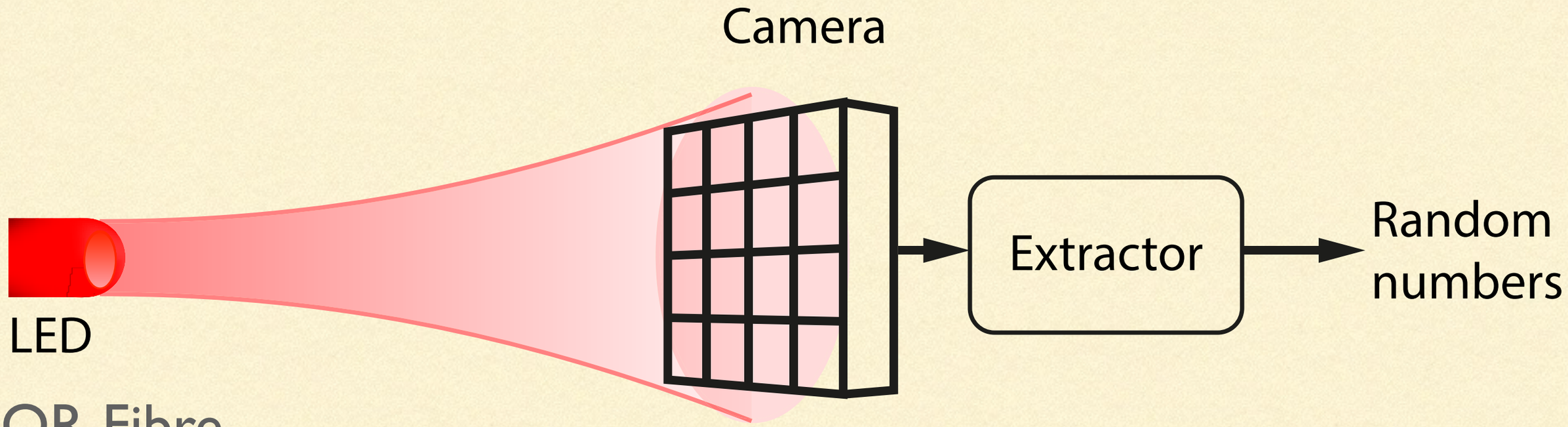
Simplified principle of operation



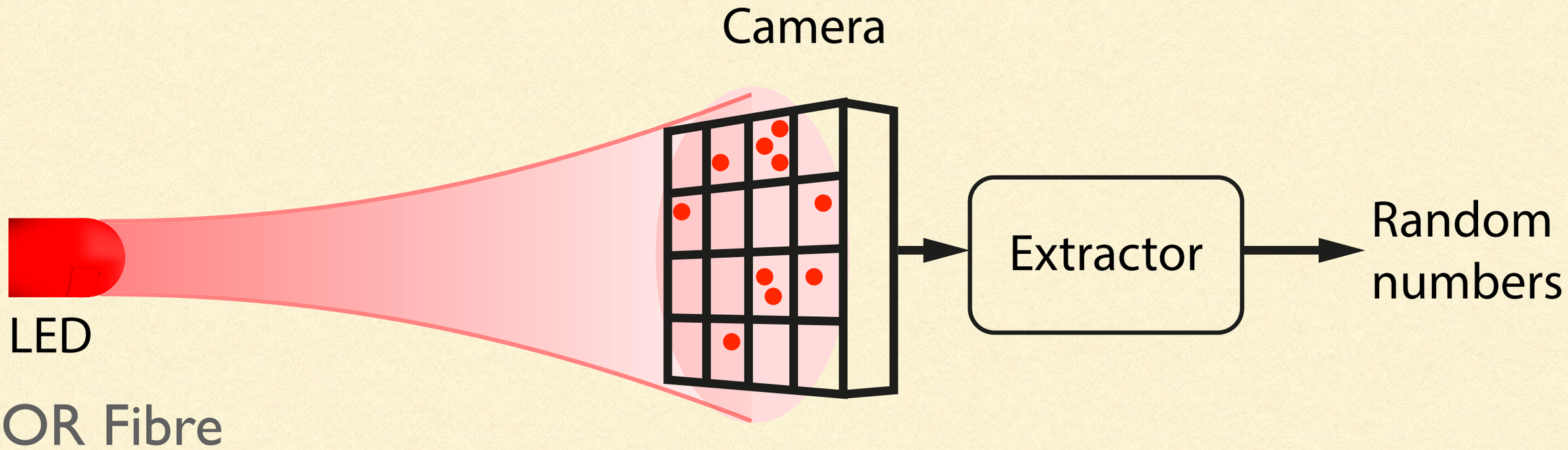
Simplified principle of operation



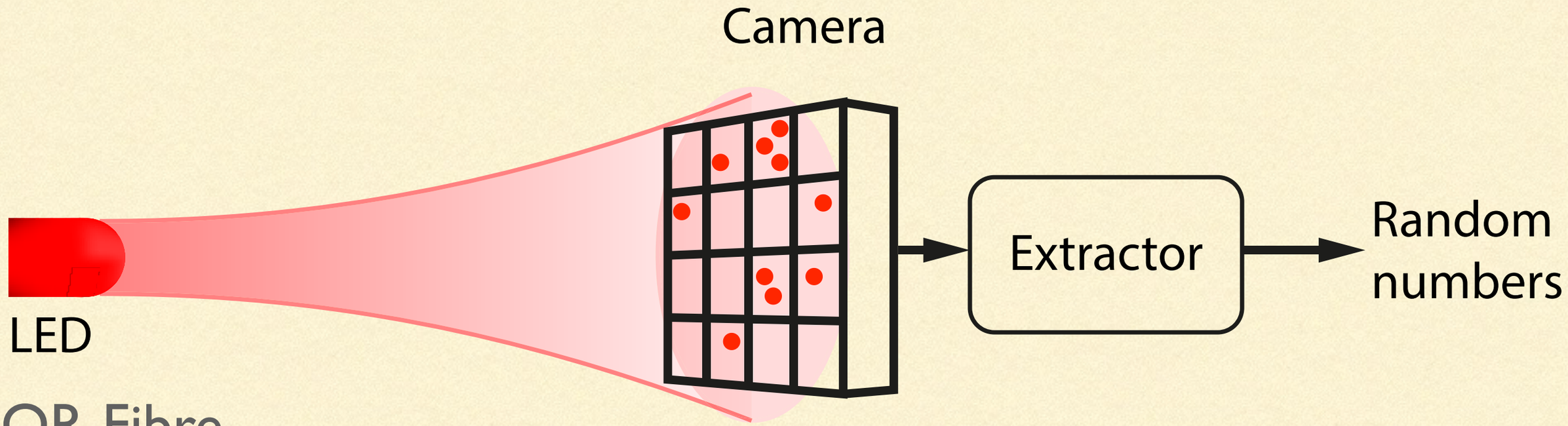
Concept

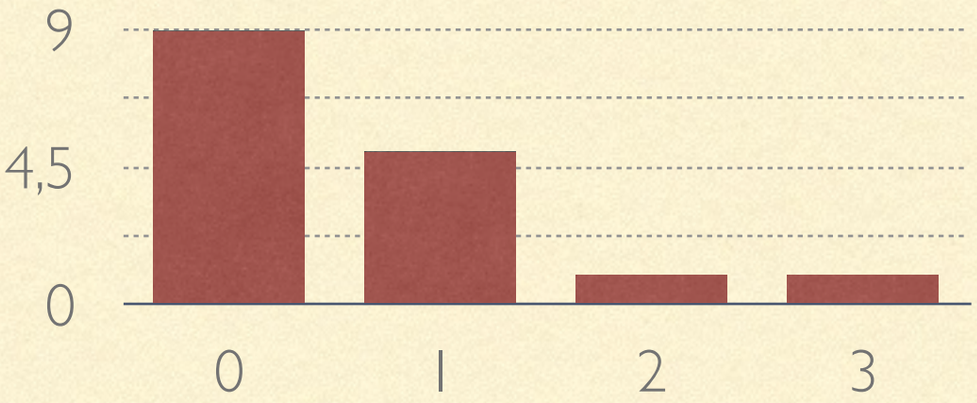


Concept

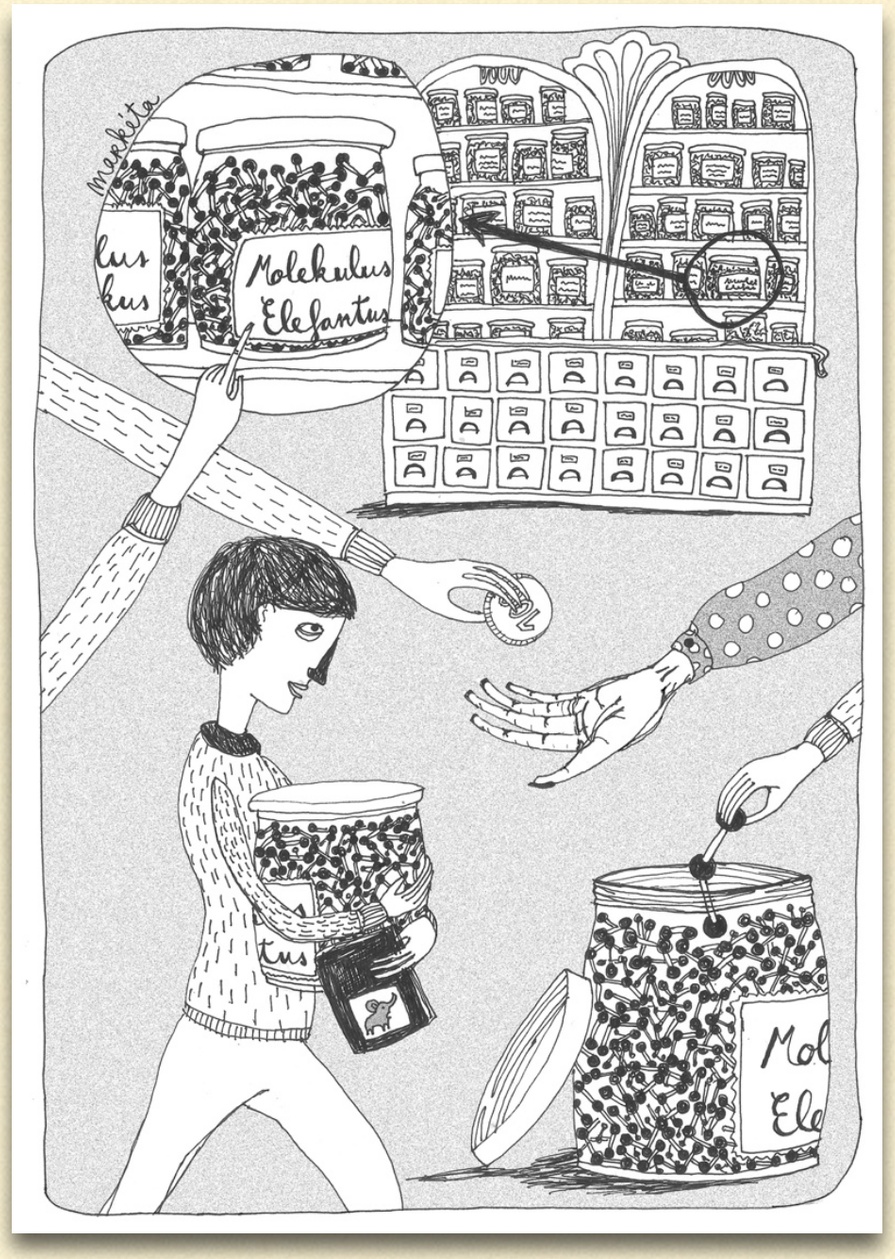


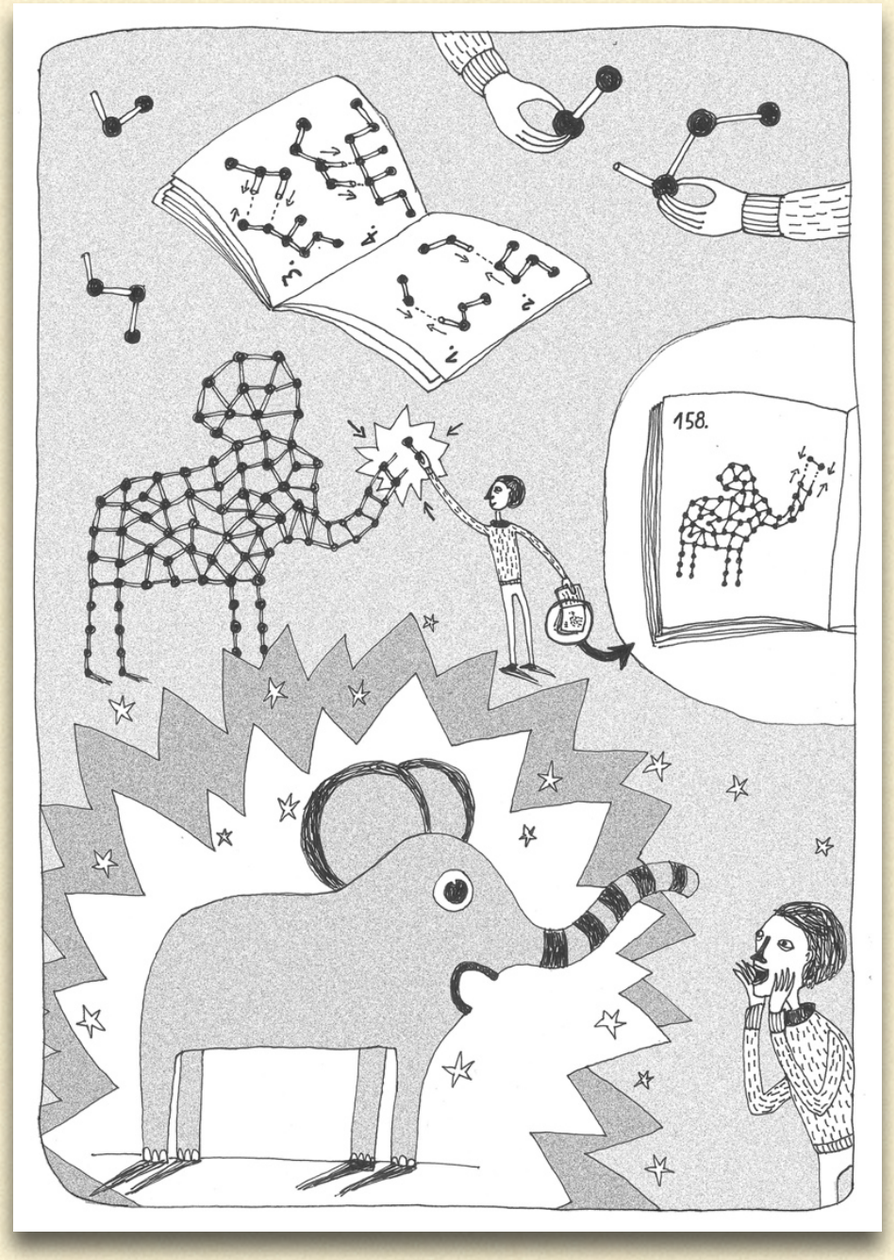
Concept





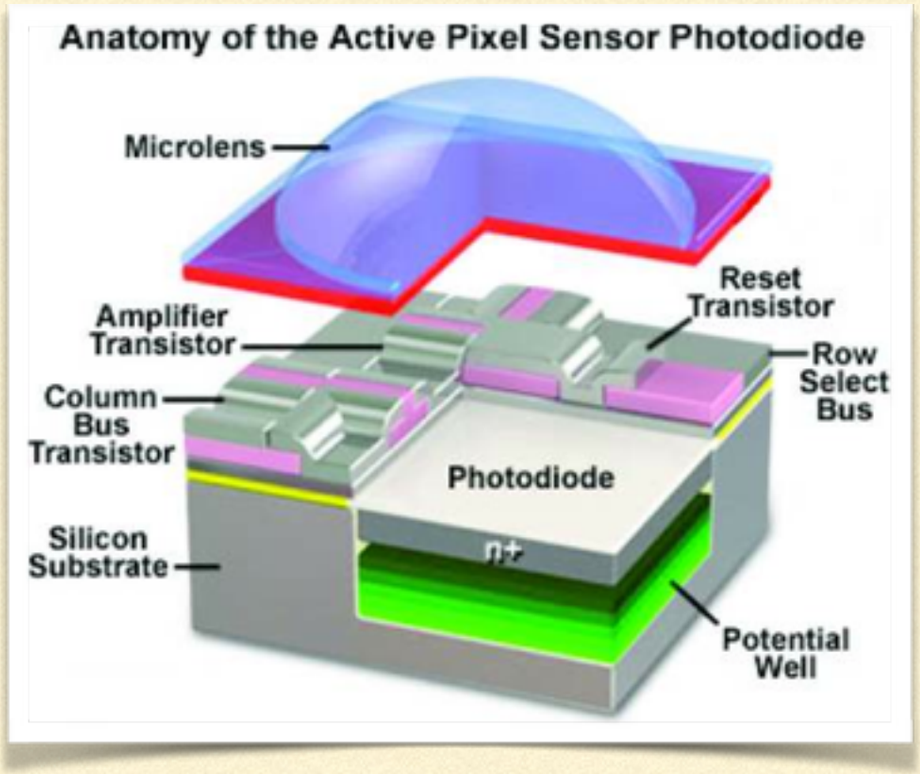
Fundamental research
→ cool applications

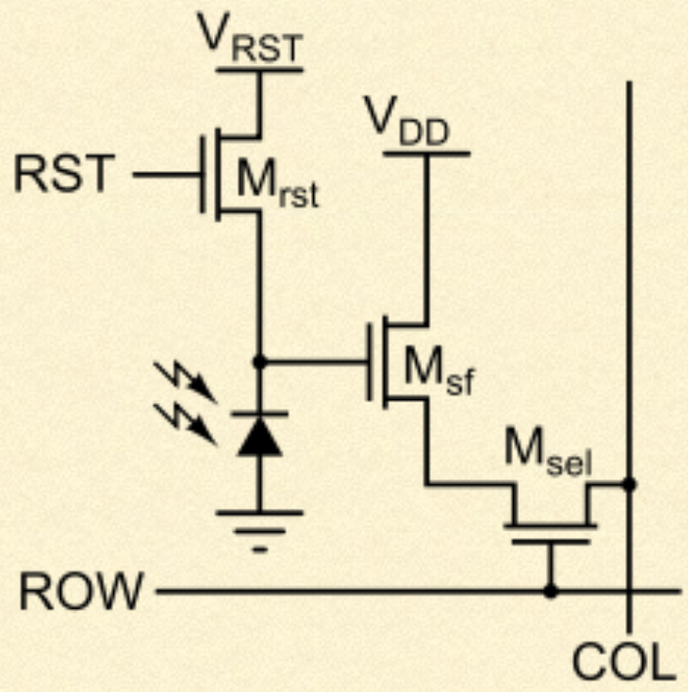




Mobile phone sensors are excellent!

- Low noise (< 1e-), linear, *small pixels, low capacitance before amp*
- Fast (1Gpixel/s ~10 GBits/s) *for video*
- Cheap (~1$); market for *billions* of sensors (I have 30 at home)
- CMOS technology: source, detector and processing on a single chip.





pentaxforum.com

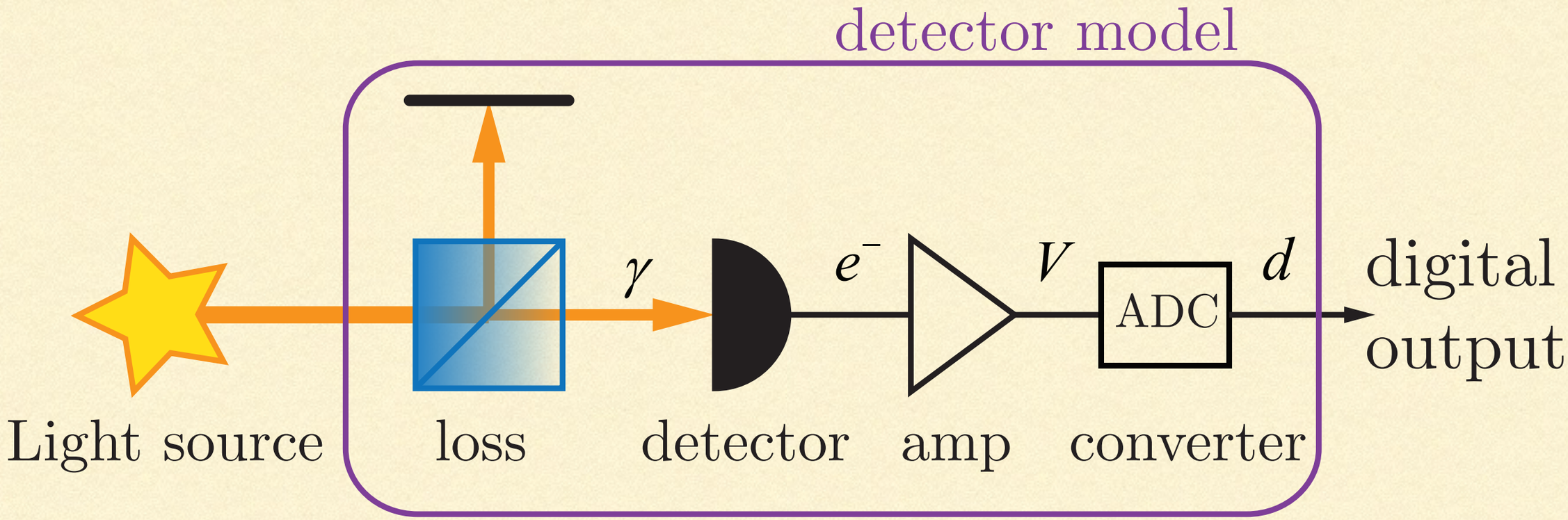
Tested with two cameras

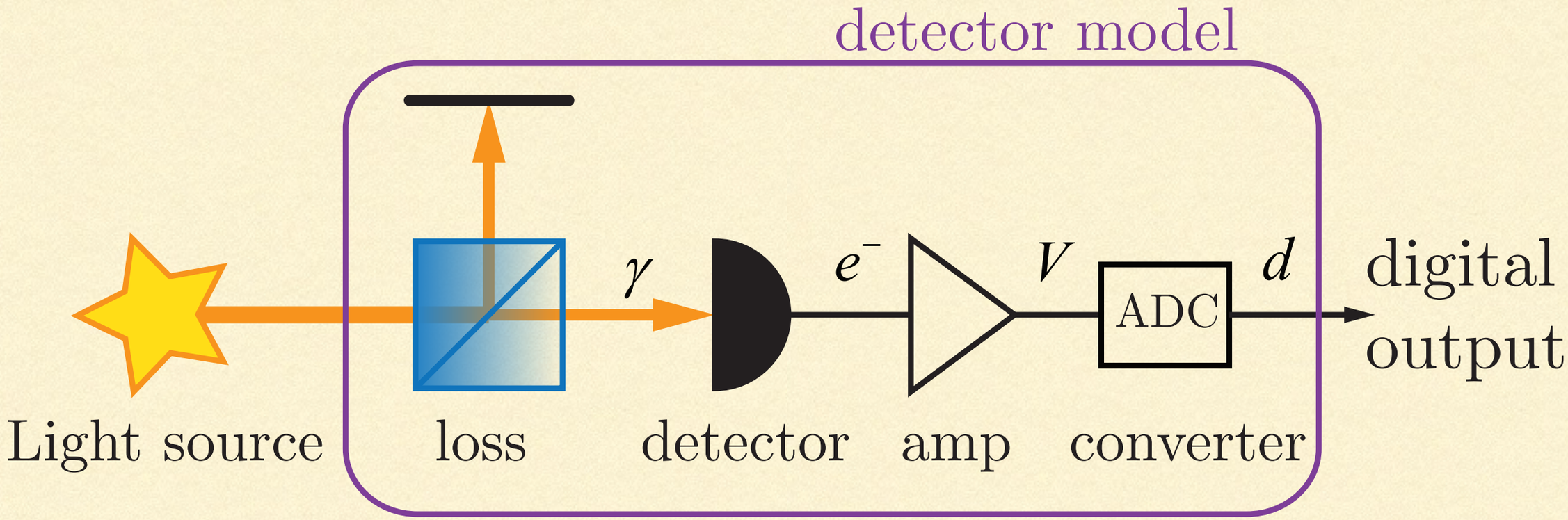
Astronomy CCD
(ATIK 383L+)

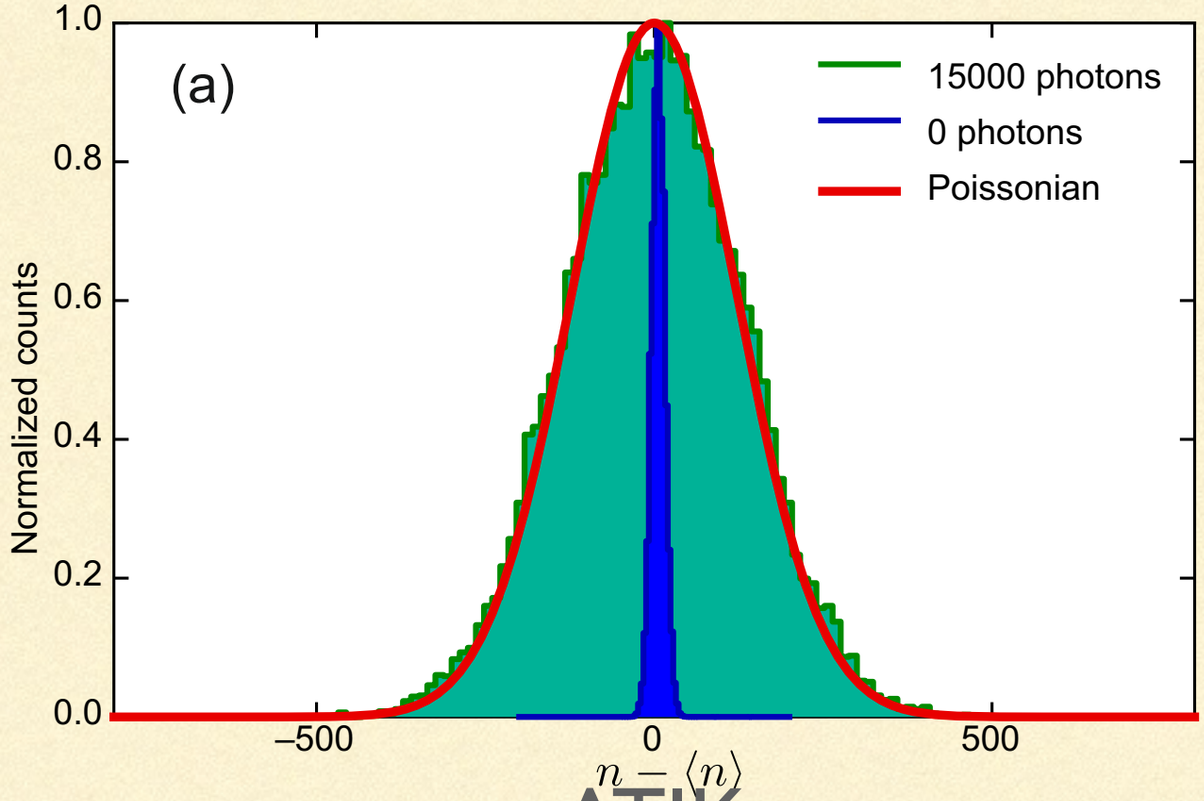
Noise: 10 e^-

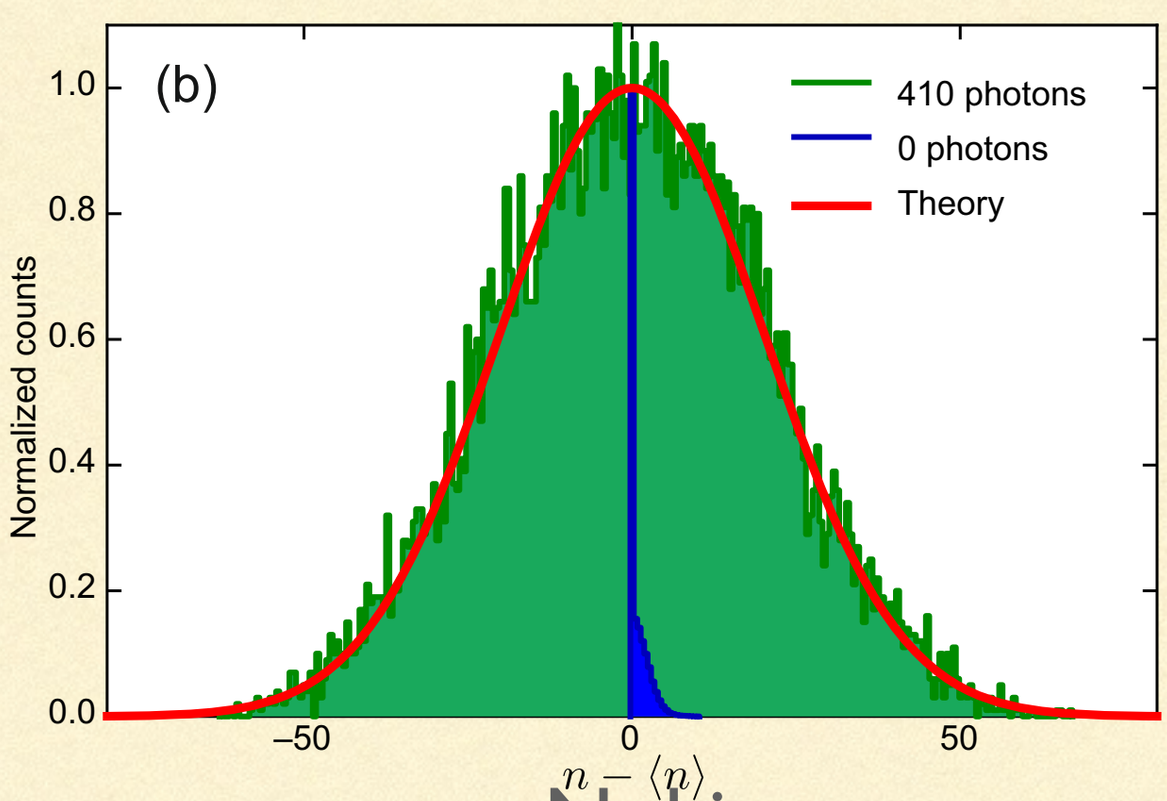
Phone CMOS
(Nokia N9)

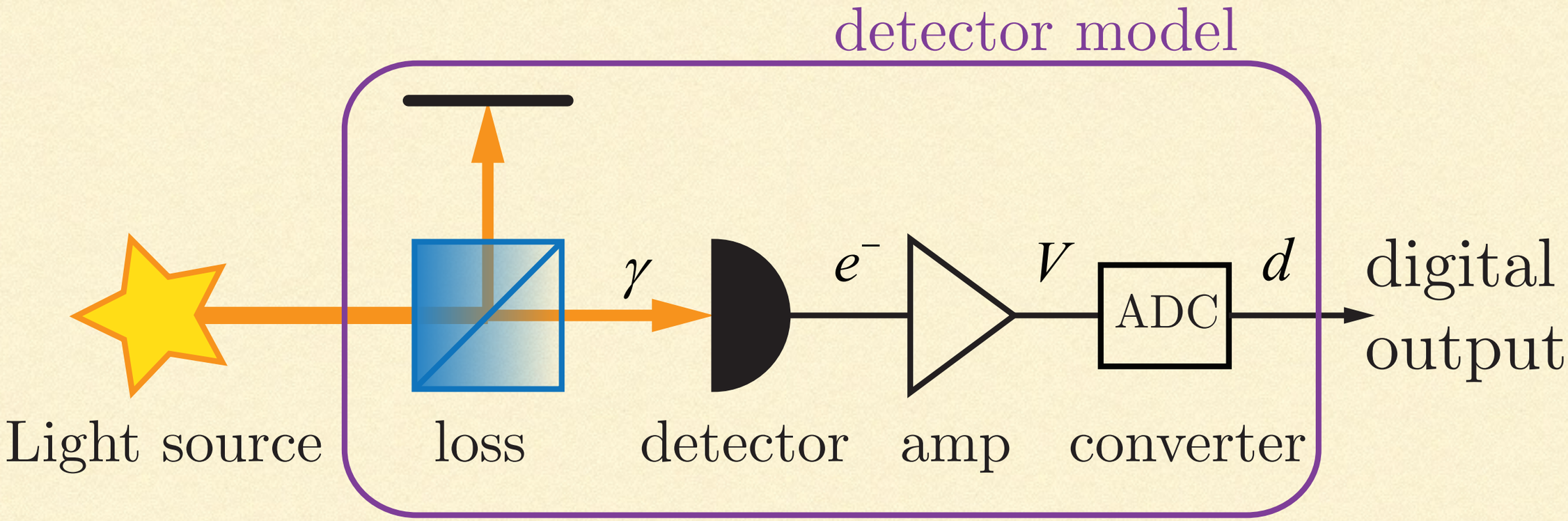
Noise: 3 e^-


detector model
γ
e^-
V
d
ADC
digital output
Light source
loss
detector
amp
converter


detector model
Light source
loss
detector
amp
converter
ADC
γ
e^-
V
d
digital output

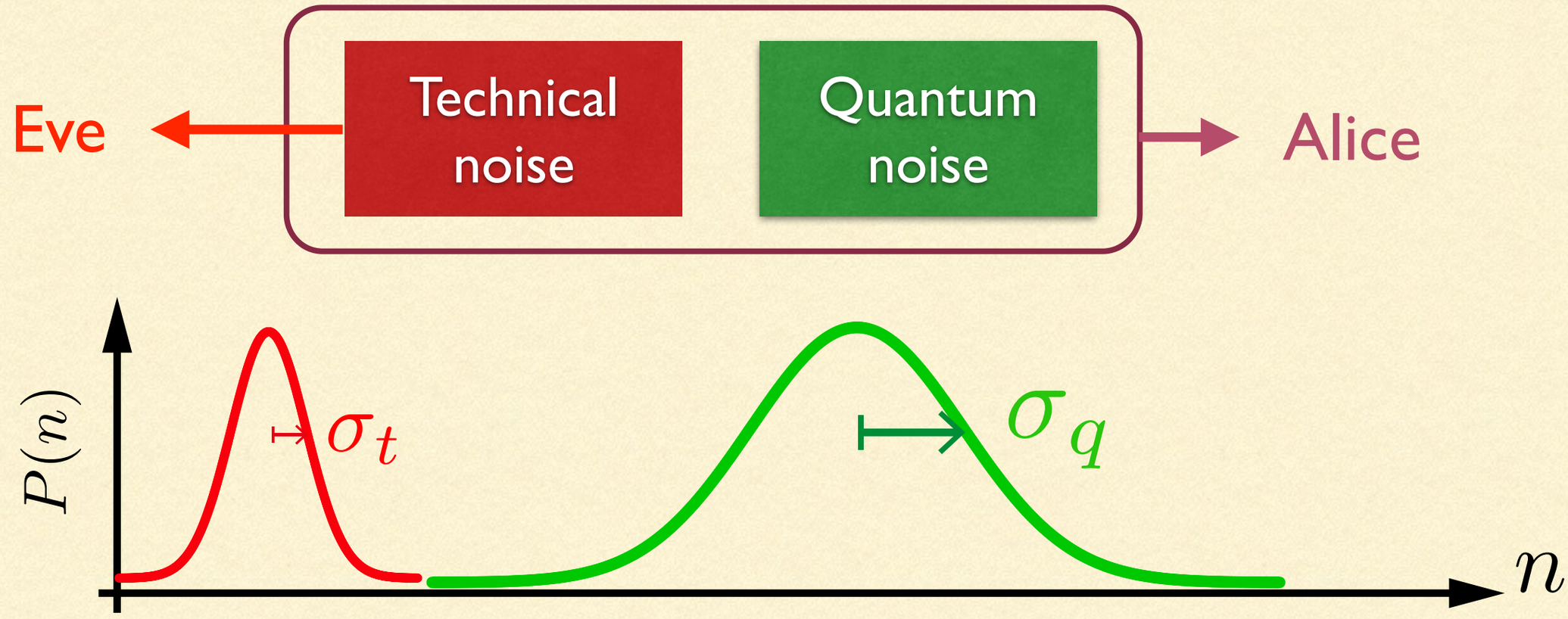

(a)
15000 photons
0 photons
Poissonian
Normalized counts
$n - \langle n \rangle$
ATIK


(b)
410 photons
0 photons
Theory
Normalized counts
$n - \langle n \rangle$
Nokia



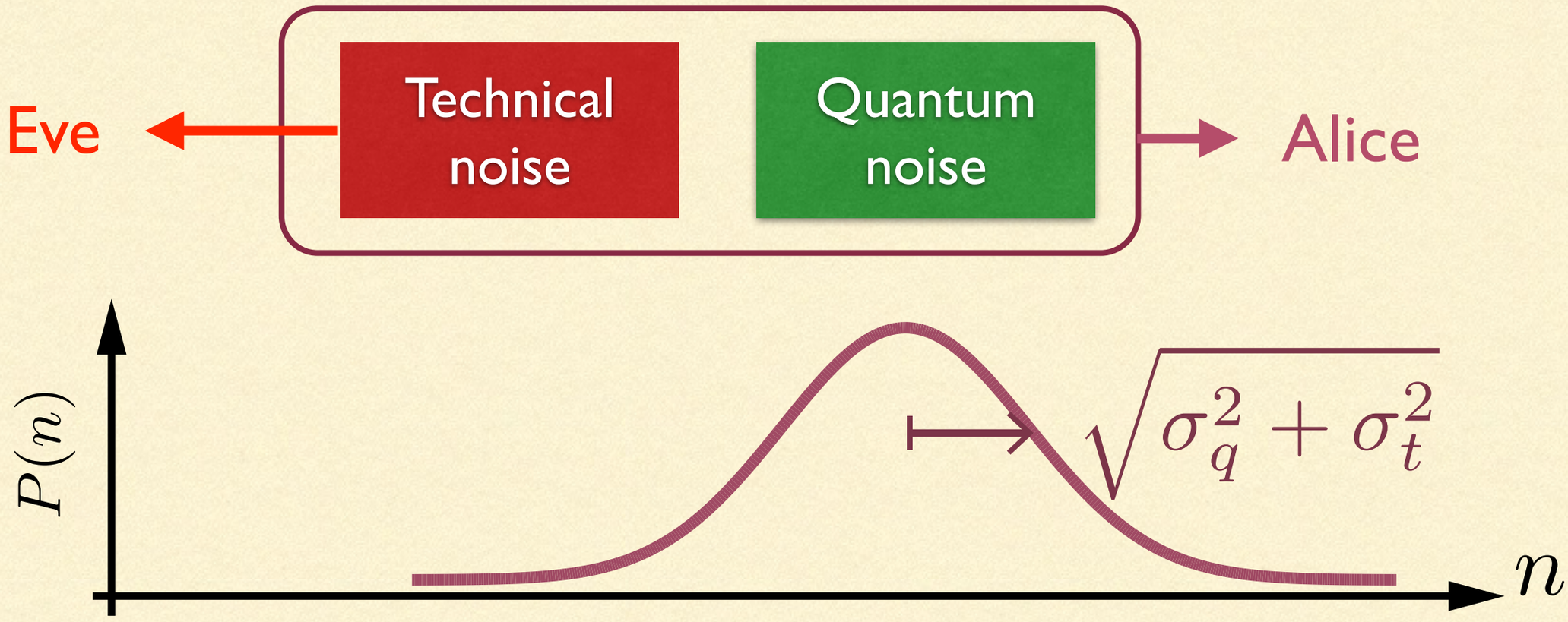
	ATIK 383L	Nokia N9
Noise, σ_t (e^-)	10	3.3
Saturation (e^-)	2×10^4	500
Illumination (e^-)	1.5×10^4	410
Quantum uncertainty, σ_q (e^-)	122	20
Offset (e^-)	144	-6
Output bits per pixel	16	10
Quantum entropy per pixel	8.3 bits	5.7 bits
Quantum entropy per raw bit	0.52	0.57

NON-IDEAL CAMERA: STILL OK



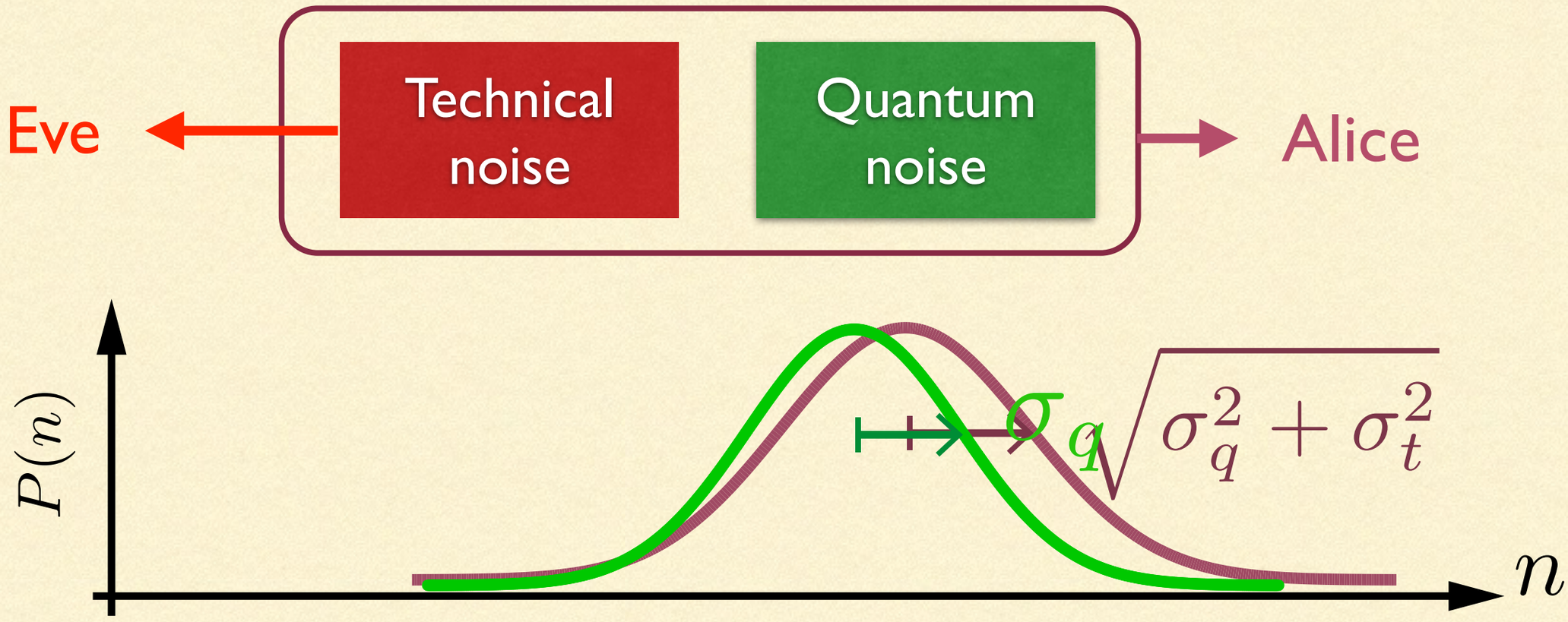
Even if Eve has full knowledge of the technical noise, the best she can do is recover the quantum noise.

NON-IDEAL CAMERA: STILL OK



Even if Eve has full knowledge of the technical noise, the best she can do is recover the quantum noise.

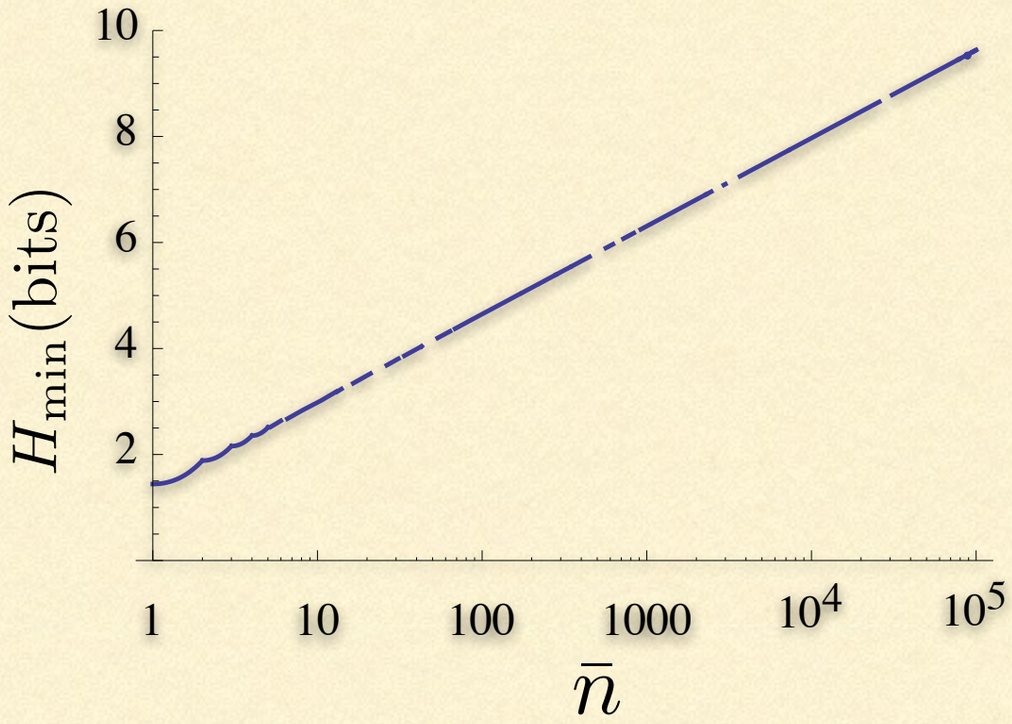
NON-IDEAL CAMERA: STILL OK



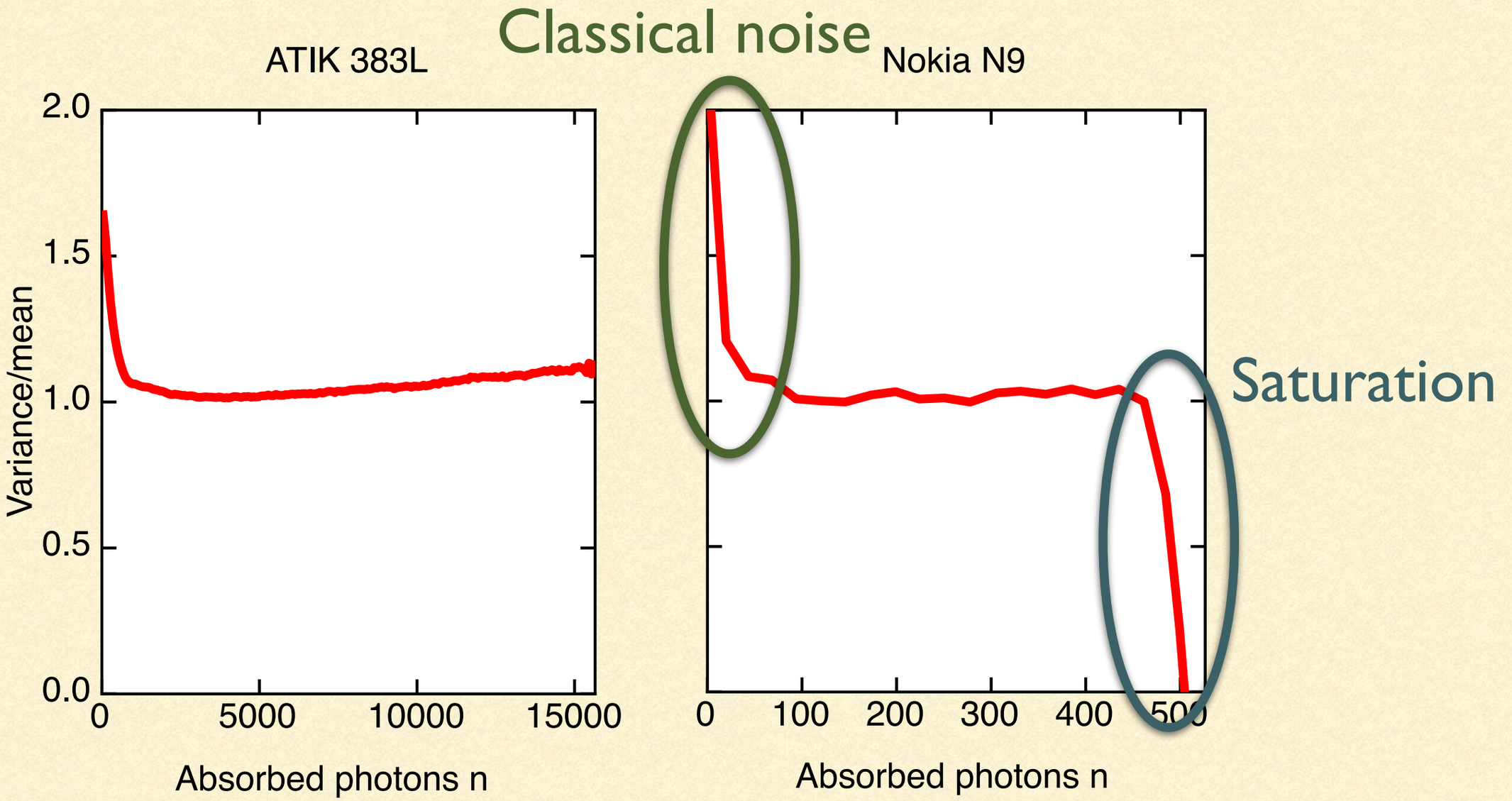
Even if Eve has full knowledge of the technical noise, the best she can do is recover the quantum noise.

Up to 10 random bits per pixel

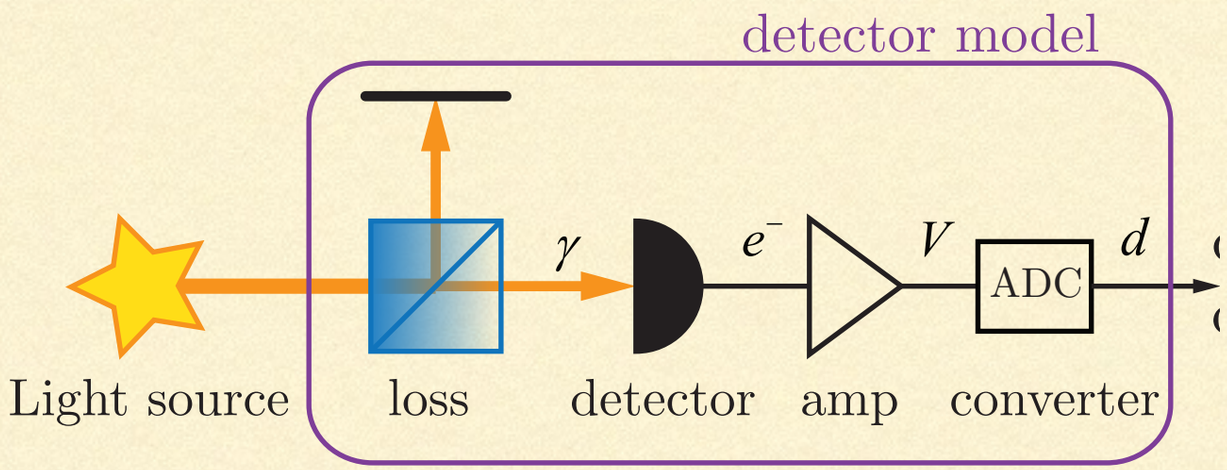
$$
\begin{aligned}
H_{\min}(X_q) &= -\log_2 \left[\max\left(P_q(n)\right)\right] \\
&= -\log_2 \left[\max\left(\frac{e^{-\bar{n}}\,\bar{n}^n}{n!}\right)\right] \\
&= -\log_2 \left[\frac{e^{-\bar{n}}\,\bar{n}^{\lfloor \bar{n} \rfloor}}{\lfloor \bar{n} \rfloor!}\right]
\end{aligned}
$$



Detector linearity is important



Randomness extractor



Raw data in

$$\begin{pmatrix} 0\\0\\1\\1\\1\\1\\0\\0\\0\\0\\0\\1\\0\\0\\1\\0 \end{pmatrix} \times \begin{pmatrix} 0&0&0&0\\0&0&0&1\\0&0&1&1\\1&1&1&1\\1&0&0&0\\1&1&1&1\\1&1&0&1\\0&0&1&0\\0&1&1&1\\1&1&0&1\\0&0&0&1\\0&1&0&0\\0&0&0&0\\1&1&1&1\\1&0&0&0\\0&0&0&0 \end{pmatrix}$$

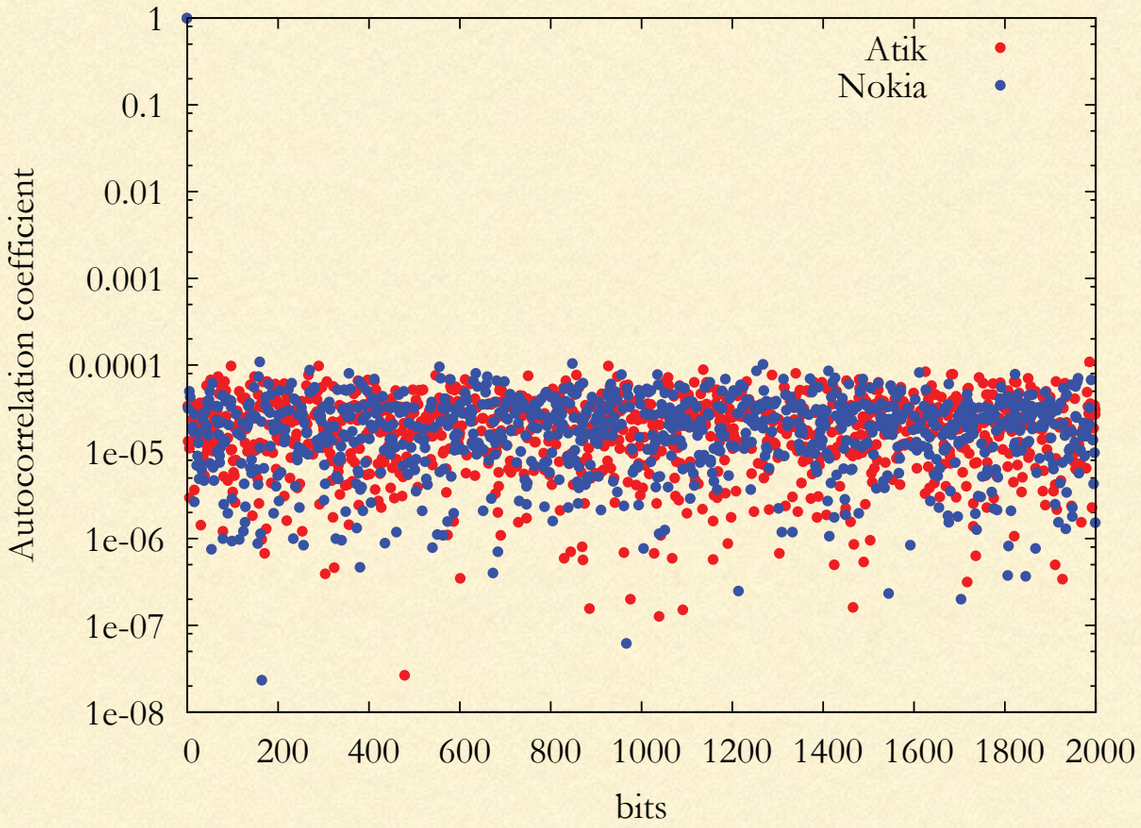
Extractor matrix (actually 2000x500)

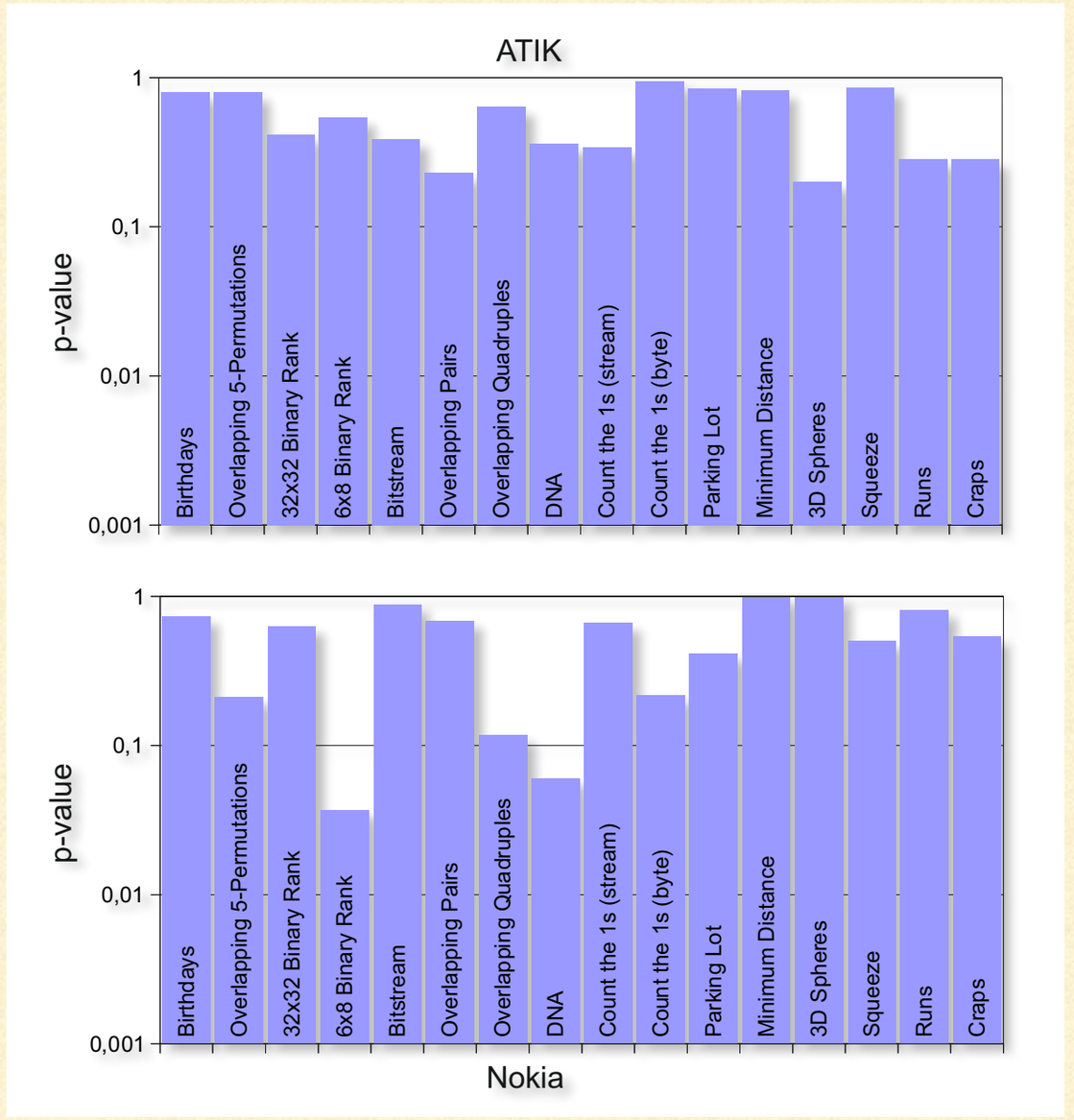
$$(1\ 1\ 1\ 0)$$ Random bits out

[1] D. Frauchiger, R. Renner, and M. Troyer. True randomness from realistic quantum devices. arXiv preprint arXiv:1311.4547, 2013.
[2] M. Troyer and R. Renner. A randomness extractor for the quantis device. Id Quantique technical report, 2012.

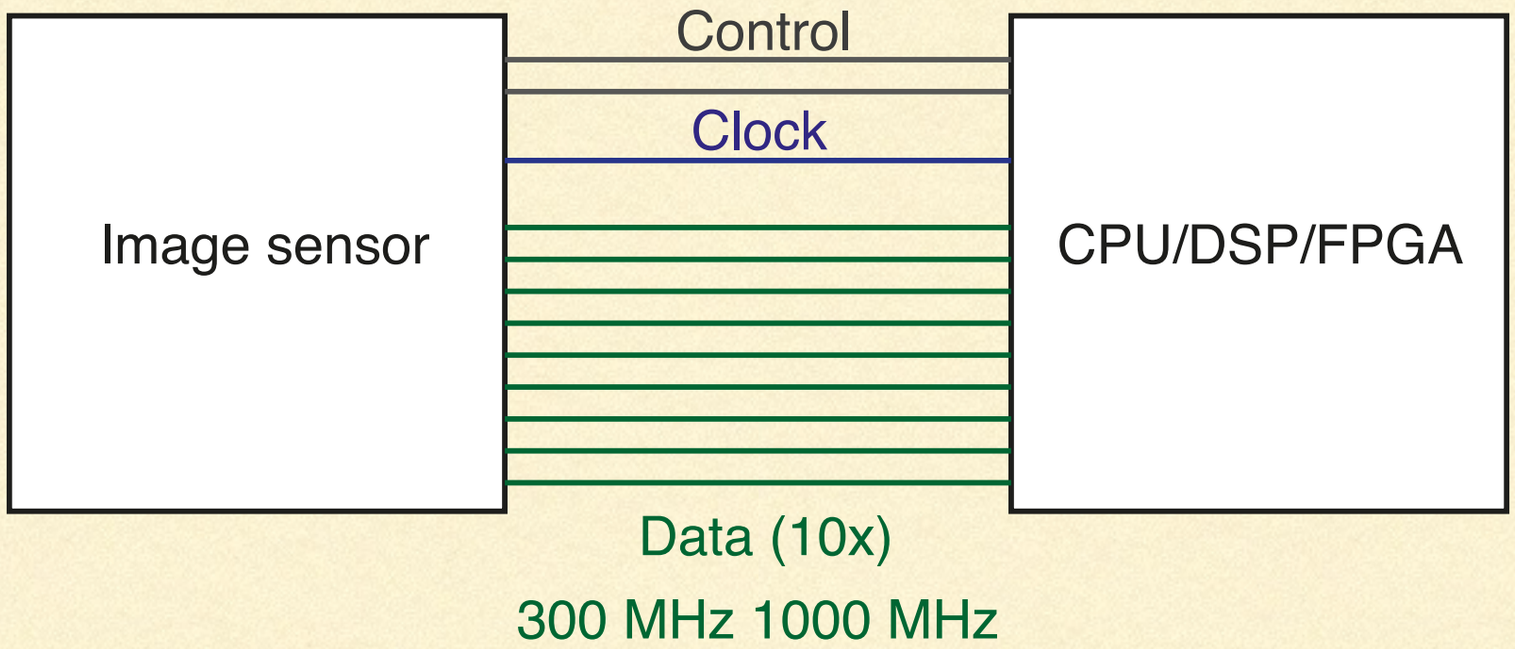
$\sim 2 \times 10^{96}$ trials before a deviation is found

Tests, "DieHarder"



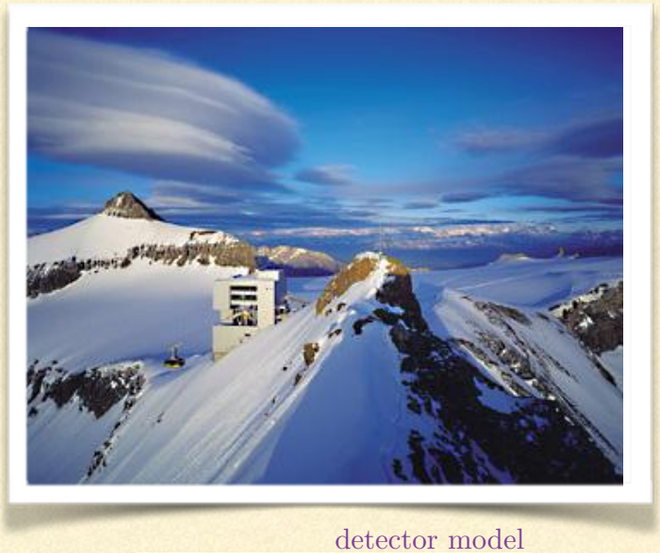


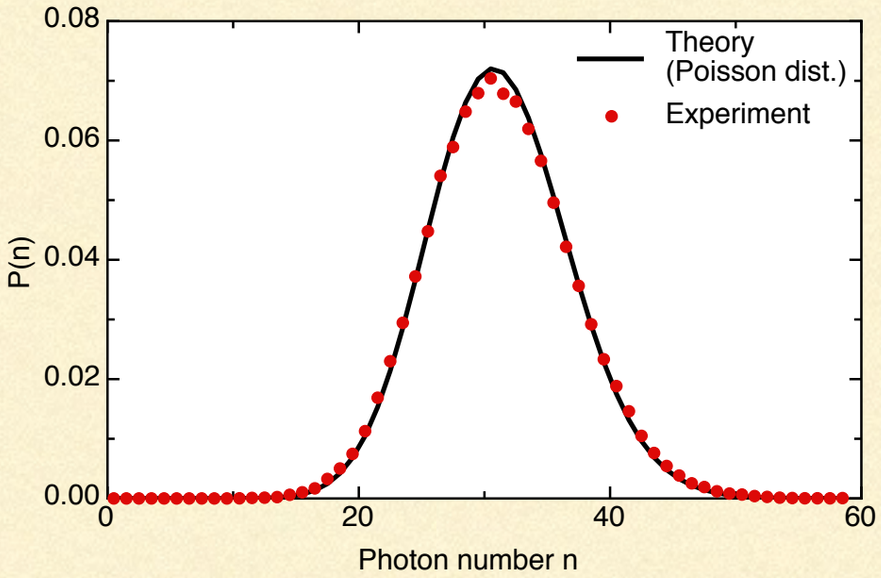
Speed



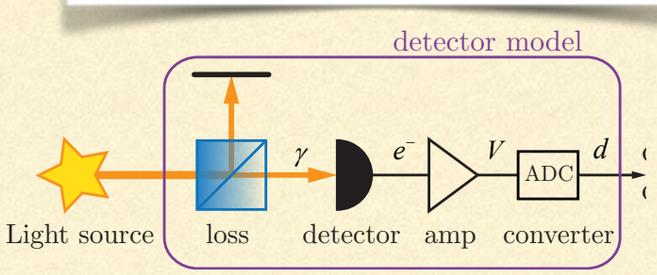
Sensor: 8 Megapixels x 30 frames/s x 3 bits = 720 Mbit/s
Extractor: software ~10 Mbps; PFGA ~ 1.25 Gbps
Mobile phone: limited memory

Most "calibrated" sources are usable, with certain assumptions.

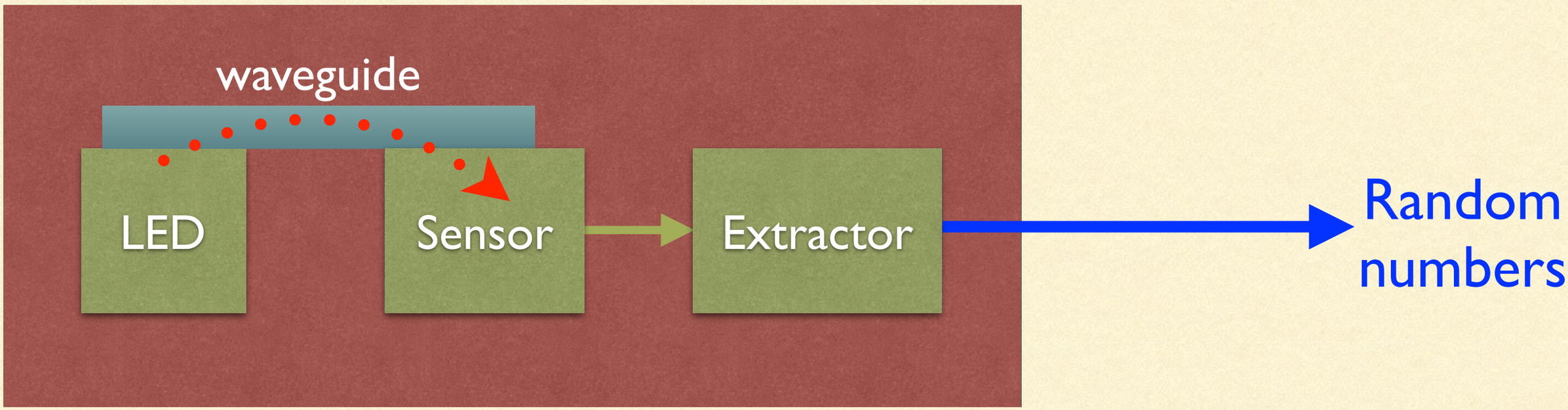




Test of LED photon number distribution with single photon detector



Can be completely integrated on chip



Conclusion

- Cheap image sensors really work at the quantum level
- QRNG can be made cheaply and integrated, using existing technology
- Still some work on the theory required

Thanks for your attention

Hugo Zbinden

Anthony Martin

Nicolas Gisin

7th ID Quantique Winter school 18 Jan -22 Jan 2015

Tutorial by:

- Whitfried Diffie
- Colin Williams (D-Wave)
- Nicolas Gisin
- Eleni Diamanti
- Tracy Northup
- Sandu Popescu
- Mikael Afzelius
- Renner Renato