A True Random Number Generator Based on quantum-optical noise

André de Almeida Ruegger
Gilberto Medeiros
Roberto Nogueira
Wagner Rodrigues
Fernando Soares
Jeroen van de Graaf
Julio Cezar de Melo

UFMG

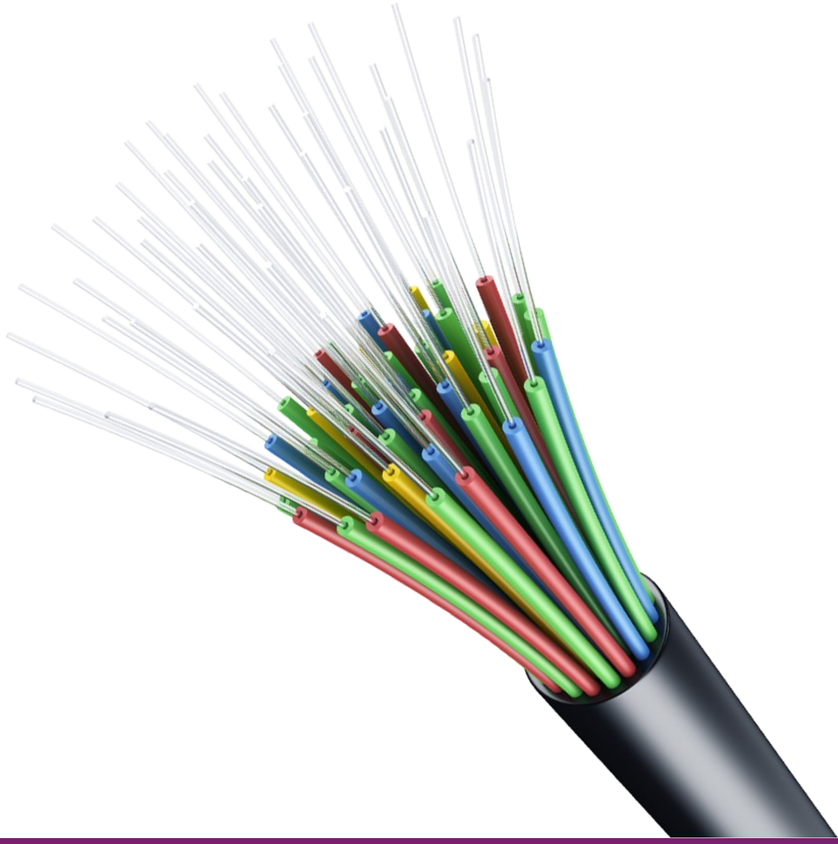
Geraldo A. Barbosa

QuantaSec Ltd.

Tradução:
Leandro Fabian Junior

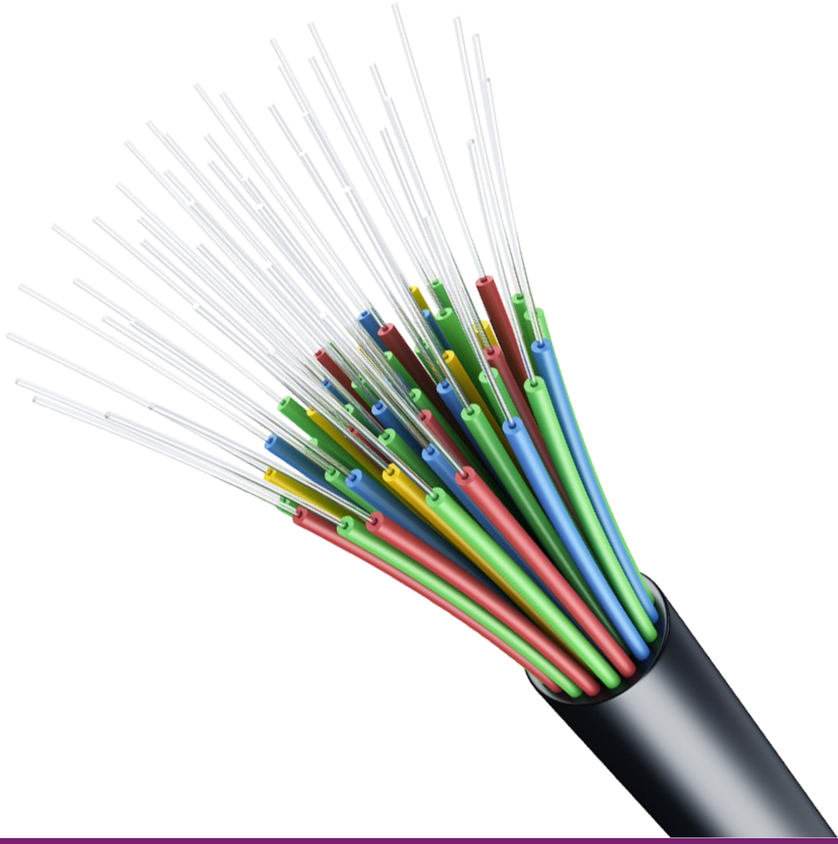
Universidade Tecnológica Federal do Paraná

Segurança na fibra ótica



Segurança na fibra ótica

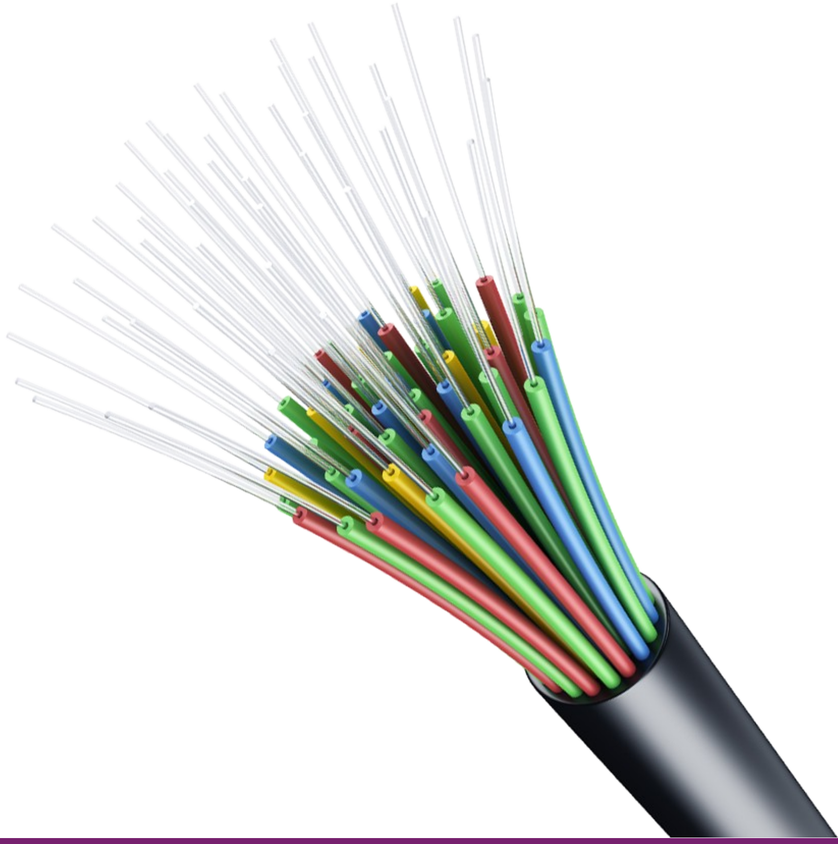
Segurança física insuficiente



Segurança na fibra ótica

Segurança física insuficiente

Criptografia quântica

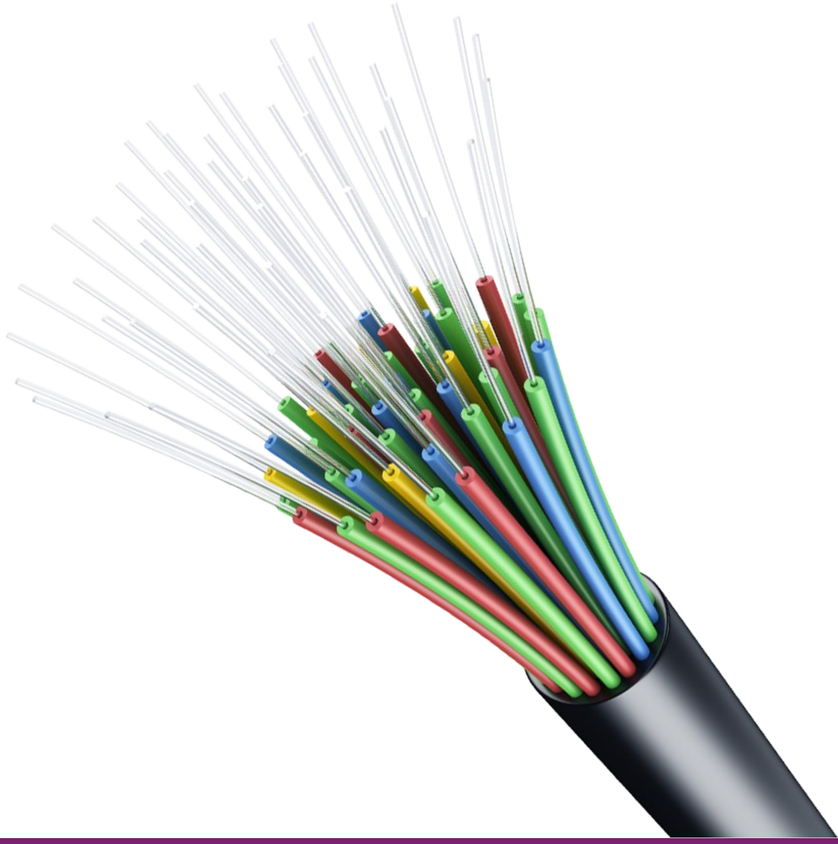


Segurança na fibra ótica

Segurança física insuficiente

Criptografia quântica

BB84 (Bennett e Brassard, 1984)



Criptografia quântica

Princípio da Incerteza (Heisenberg)

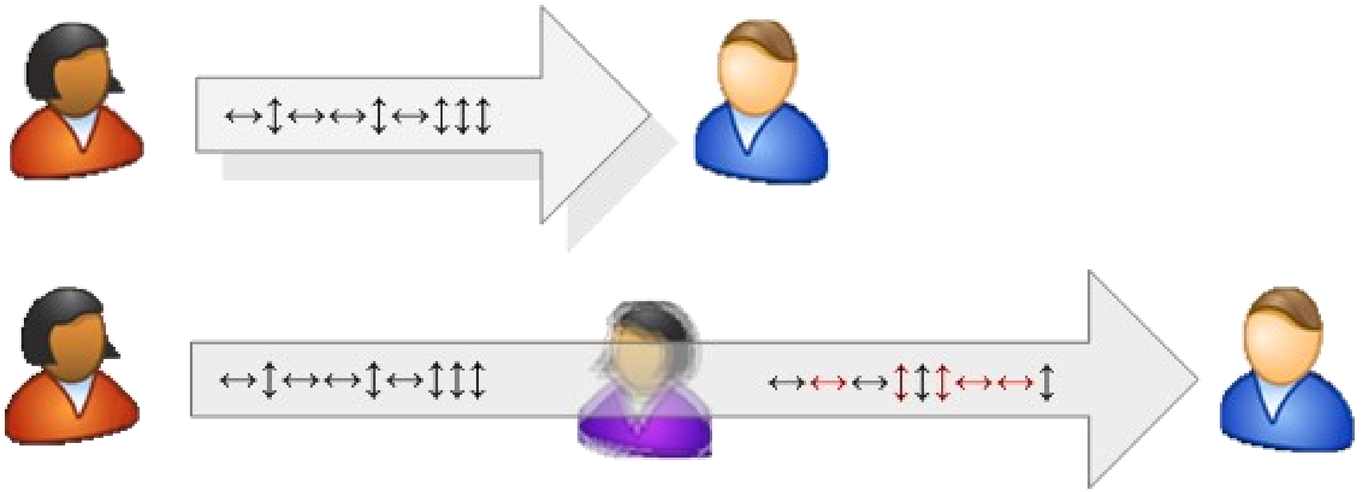
Criptografia quântica

Princípio da Incerteza (Heisenberg)

Não é possível determinar
em simultâneo todos os estados
físicos de uma partícula sem
interferir na mesma, alterando-a
de forma inegável

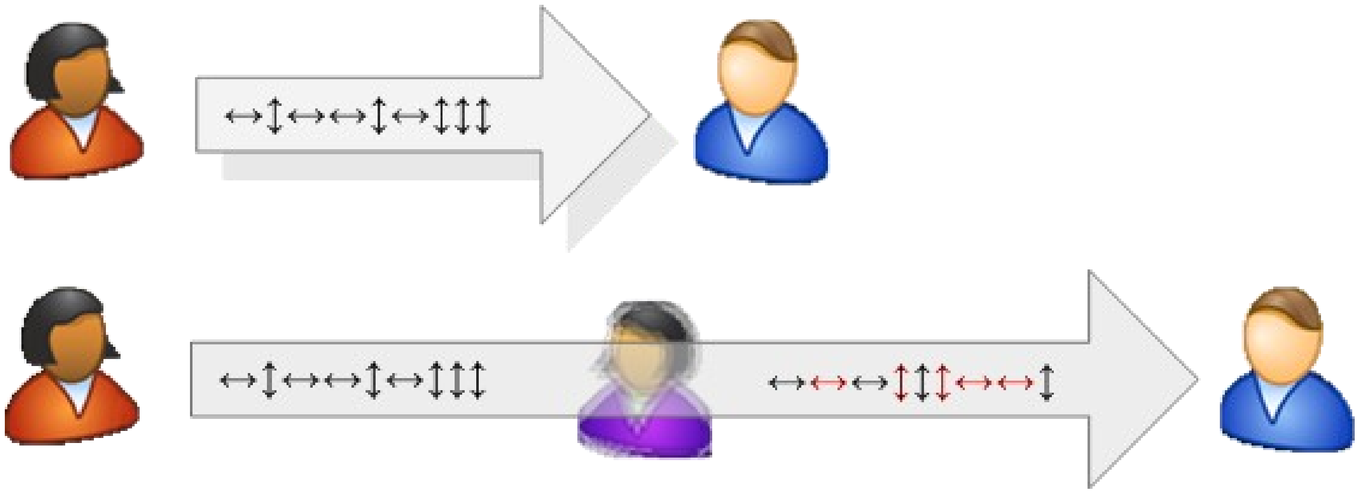
Criptografia quântica

Detecção de intrusos



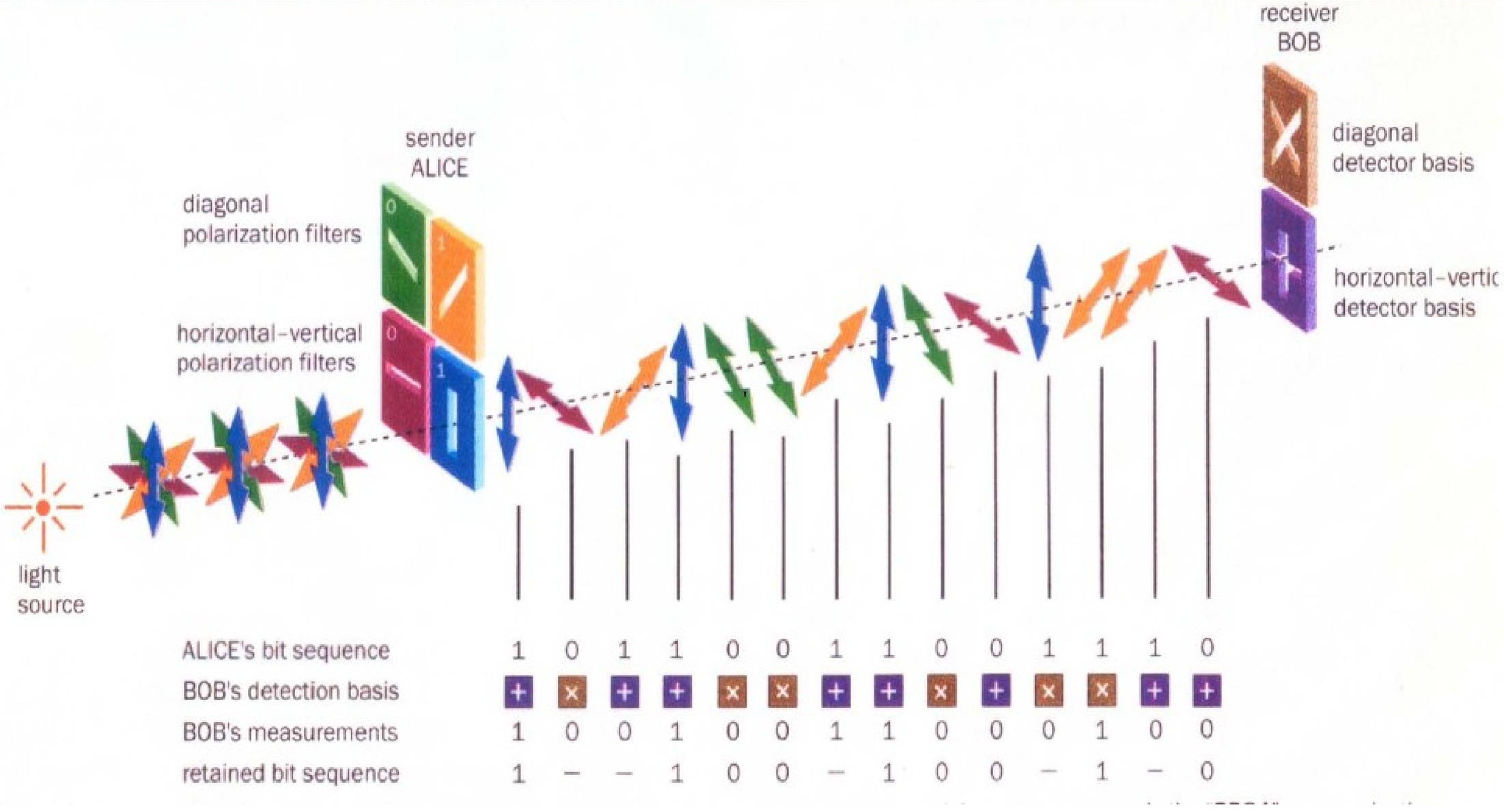
Criptografia quântica

Detecção de intrusos



Segurança mesmo com poder computacional ilimitado

BB84


receiver
BOB
sender
ALICE
diagonal
detector basis
diagonal
polarization filters
horizontal–vertic
detector basis
horizontal–vertical
polarization filters
light
source
ALICE's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1 1 0
BOB's detection basis + × + + × × + + × + × × + +
BOB's measurements 1 0 0 1 0 0 1 1 0 0 0 1 0 0
retained bit sequence 1 – – 1 0 0 – 1 0 0 – 1 – 0

Problema e Alternativa

Pulsos de fótons unitários (equipamento caro)

→ Ótica mesoscópica

→ Intensidade média da luz

Problema e Alternativa

Pulsos de fótons unitários (equipamento caro)

→ Ótica mesoscópica

→ Intensidade média da luz

Plataforma KeyBITS (QuantaSEC)

Gerador de números aleatórios

Geradores de números pseudo- aleatórios

TRNG Intel

→ Semente aleatória

→ AES (Advanced Encryption Standard)

Gerador de números aleatórios

Geradores de números pseudo- aleatórios

TRNG Intel

→ Semente aleatória

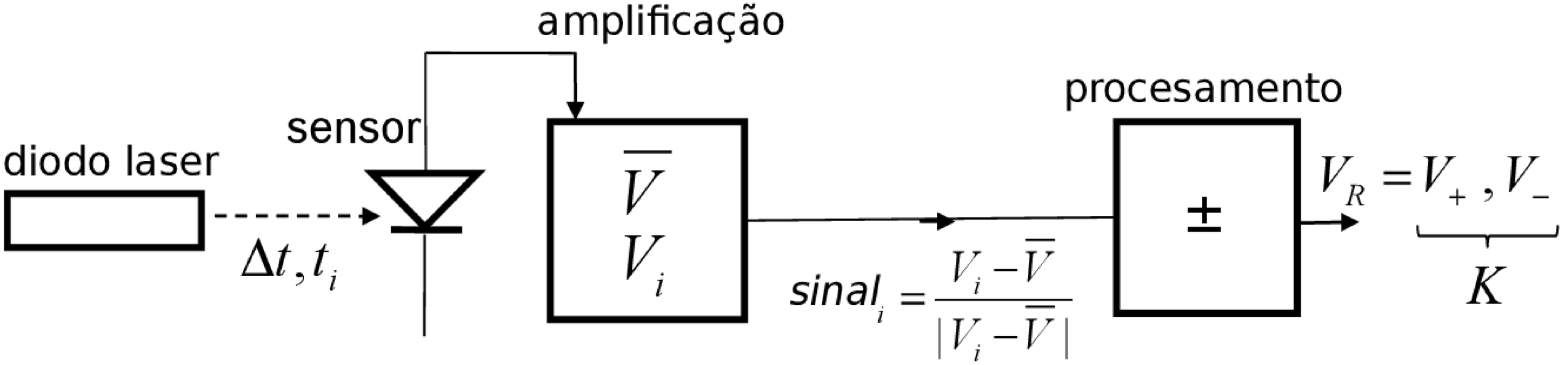
→ AES (Advanced Encryption Standard)

KeyBITS

→ Velocidade de geração de bits

→ Números realmente aleatórios

Esquemático do TRNG



Distribuição dos fótons

Distribuição de Poisson:

$$p(n) = \frac{e^{\langle n \rangle} \langle n \rangle^{n}}{n!}$$

Distribuição dos fótons

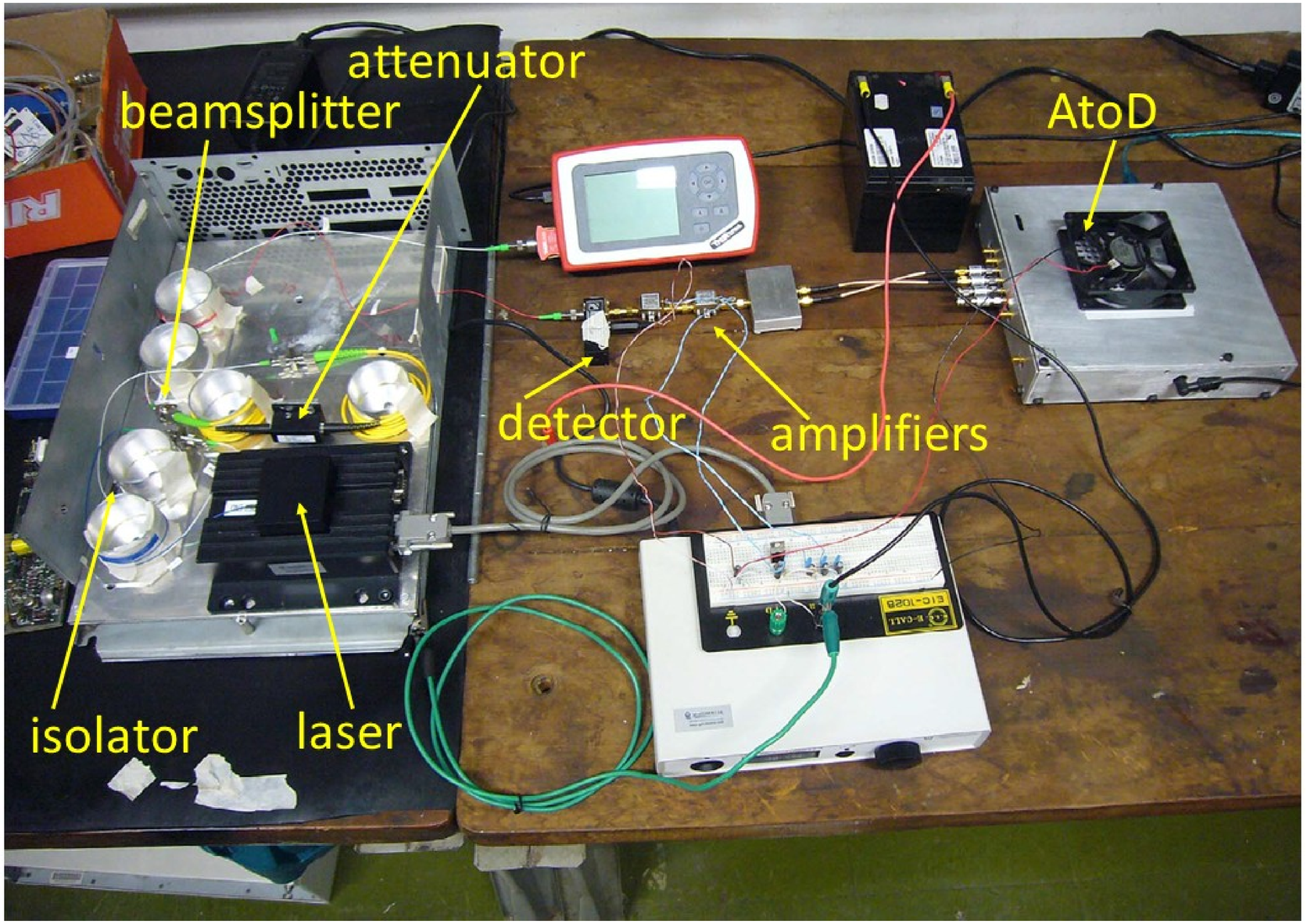
Distribuição de Poisson:

$$p(n)=\frac{e^{\langle n\rangle}\langle n\rangle^{n}}{n!}$$

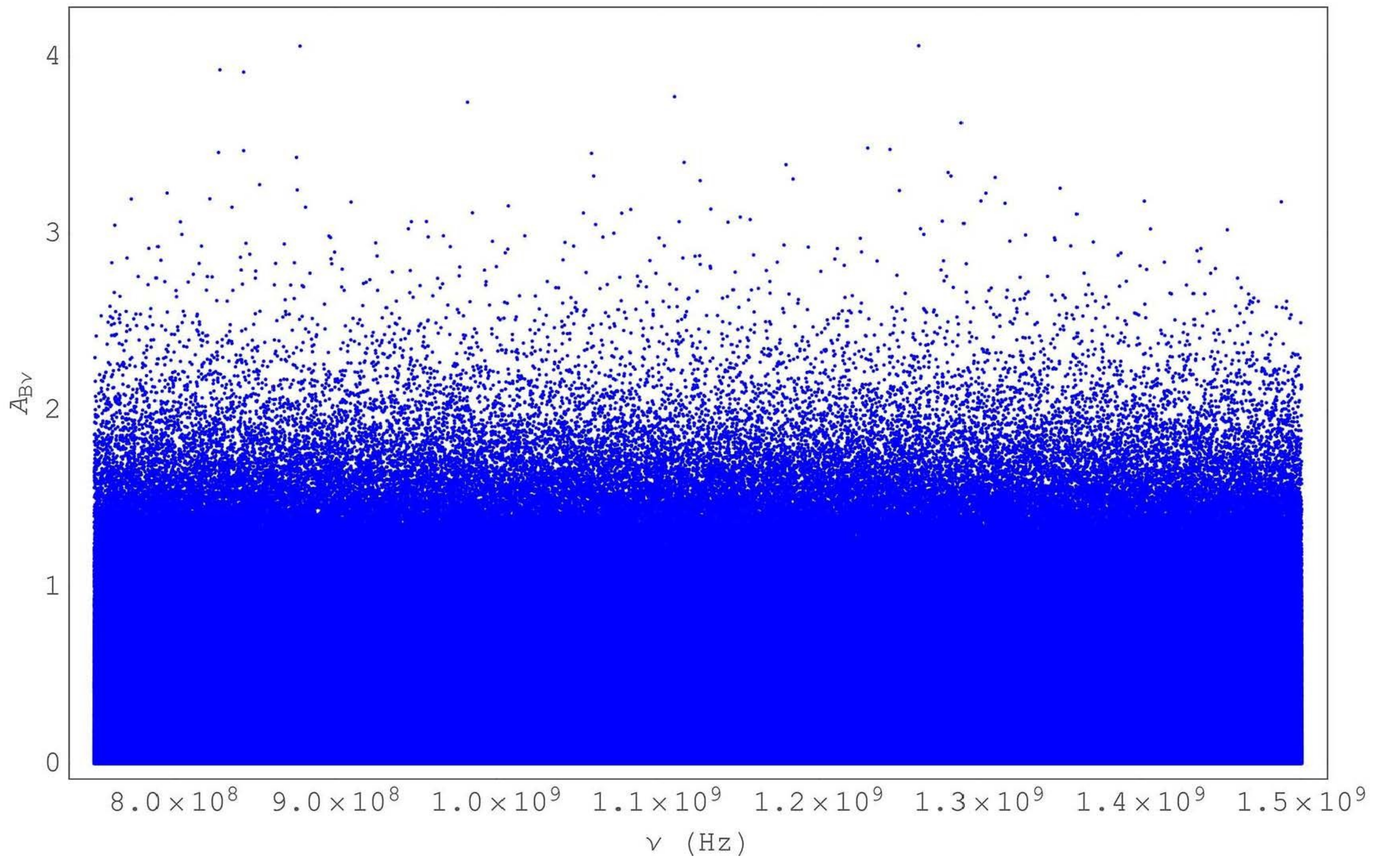
Grupo de fótons medidos entre um intervalo curto $\Delta t \ll \tau$ (tempo de coerência do laser) são independentes

$$\langle n_1 n_2\rangle = \langle n_1\rangle\langle n_2\rangle$$

Protótipo


attenuator
beamsplitter
AtoD
detector
amplifiers
isolator
laser

Amostra de 19.660.800 bits



Espectro de Fourier

Teste	P-Value
ApproximateEntropy	0.812035
BlockFrequency	0.751001
CumulativeSums	0.784649
CumulativeSums(reverse)	0.842644
FFT	0.669945
Frequency	0.607710
LinearComplexity	0.709032
LongestRun	0.948537
NonOverlappingTemplate	146/148
OverlappingTemplate	0.672652
RandomExcursions	8/8
RandomExcursionVariant	18/18
Rank	0.695808
Runs	0.511987
Serial	2/2
Universal	0.953639

Teste NIST para geradores aleatórios

Fim!