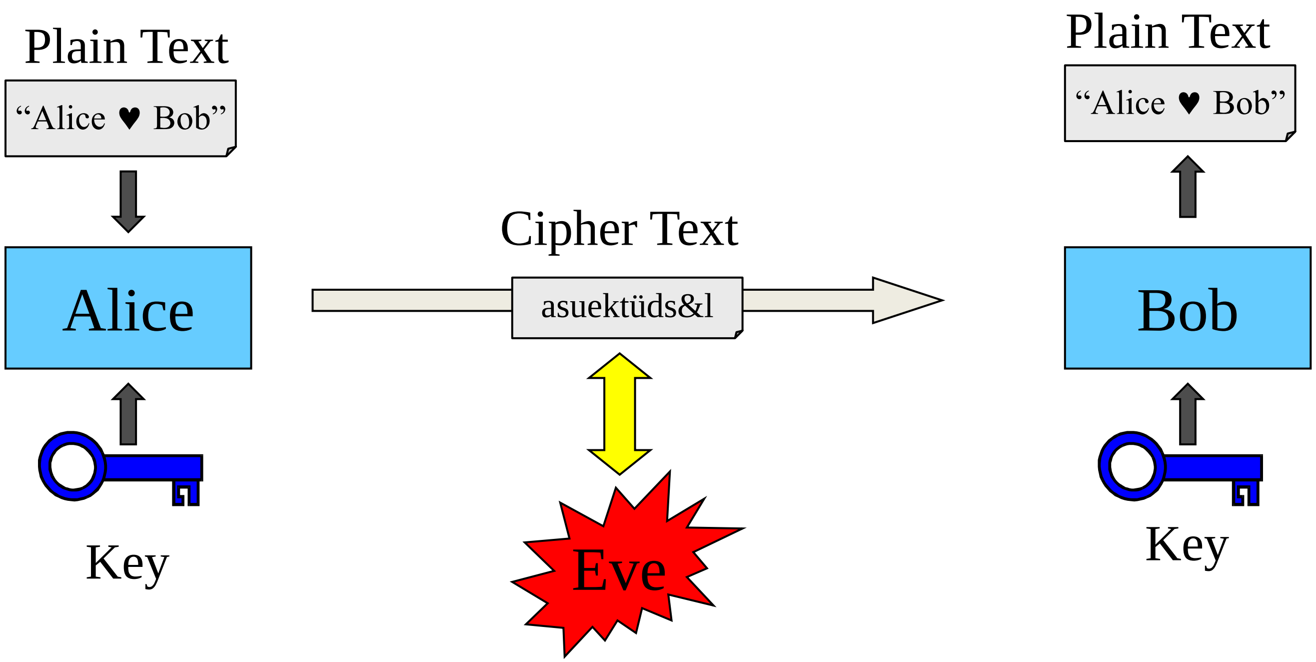
QKD: from the concept to a commercial application

Hugo Zbinden
Groupe de Physique Appliquée
"Quantum Technologies"
Université de Genève

QKD concept
QKD state of the art (academic)
QKD academic and commercial challenges
QRNG concept to application
Steganography

UNIVERSITÉ DE GENÈVE

What's Cryptography?



- Secure communication between Alice and Bob
- The spy, Eve, tries to read the encoded message

Classical Cryptography

- Based on Complexity
  DES, AES (secret key)
  RSA (public key)

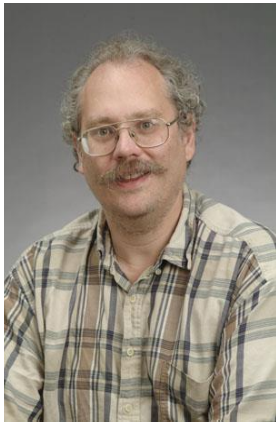
Security unproven

One-way functions

Integer factorisation

$107 \times 53 = x$

$5671 = y \times z$



Classical Cryptography

- based on Information Theory
  one time pad (Vernam)

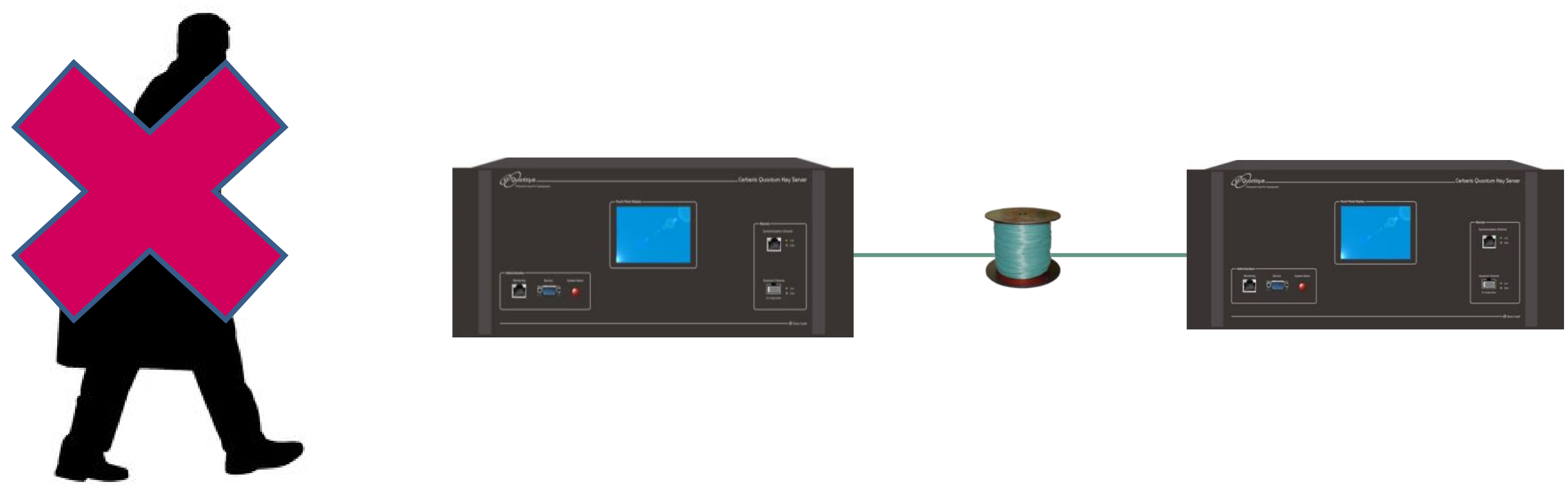
  plaintext : 00101001001001110101000110100 1
  key: +10101101101100101010011101010 1
  cyphertext: 10000100100101011111011011100

  security proven

  problem: key distribution

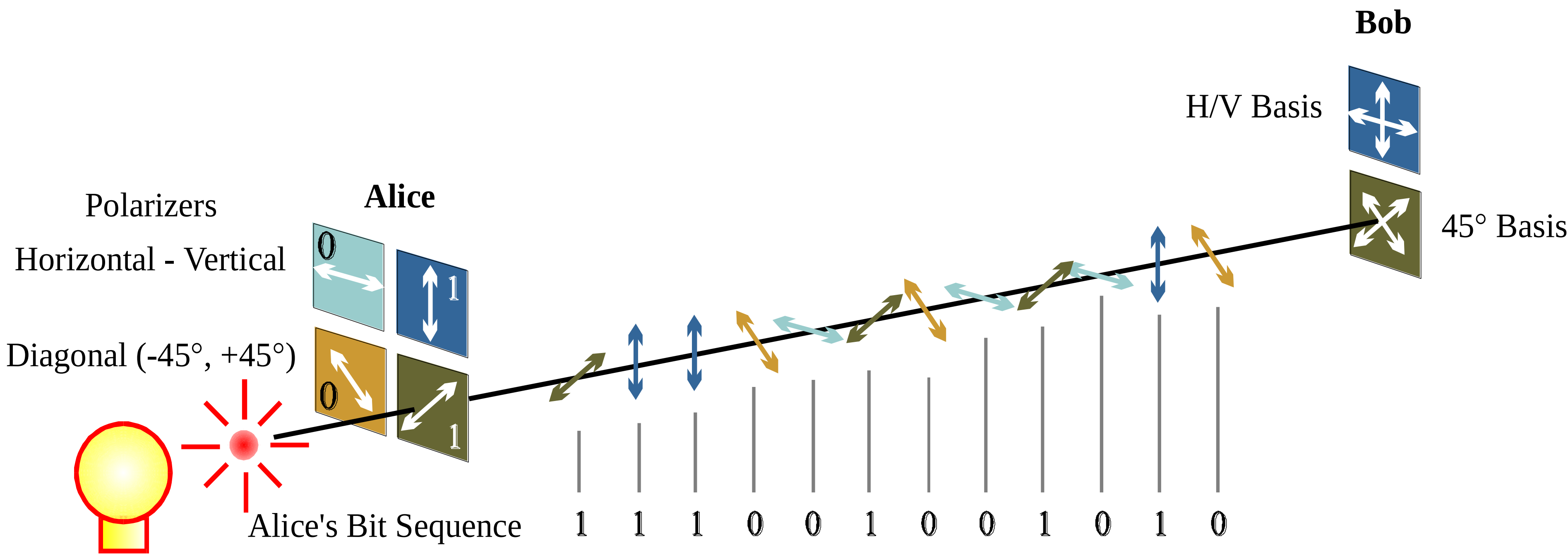
Quantum Key Distribution

- Quantum Crpytography is not a new coding method
- Send key with individual photons (quantum states)
- The eavesdropper may not measure without perturbation (Heisenbergs uncertainty principle)
- Eavesdropping can be detected by Alice and Bob!



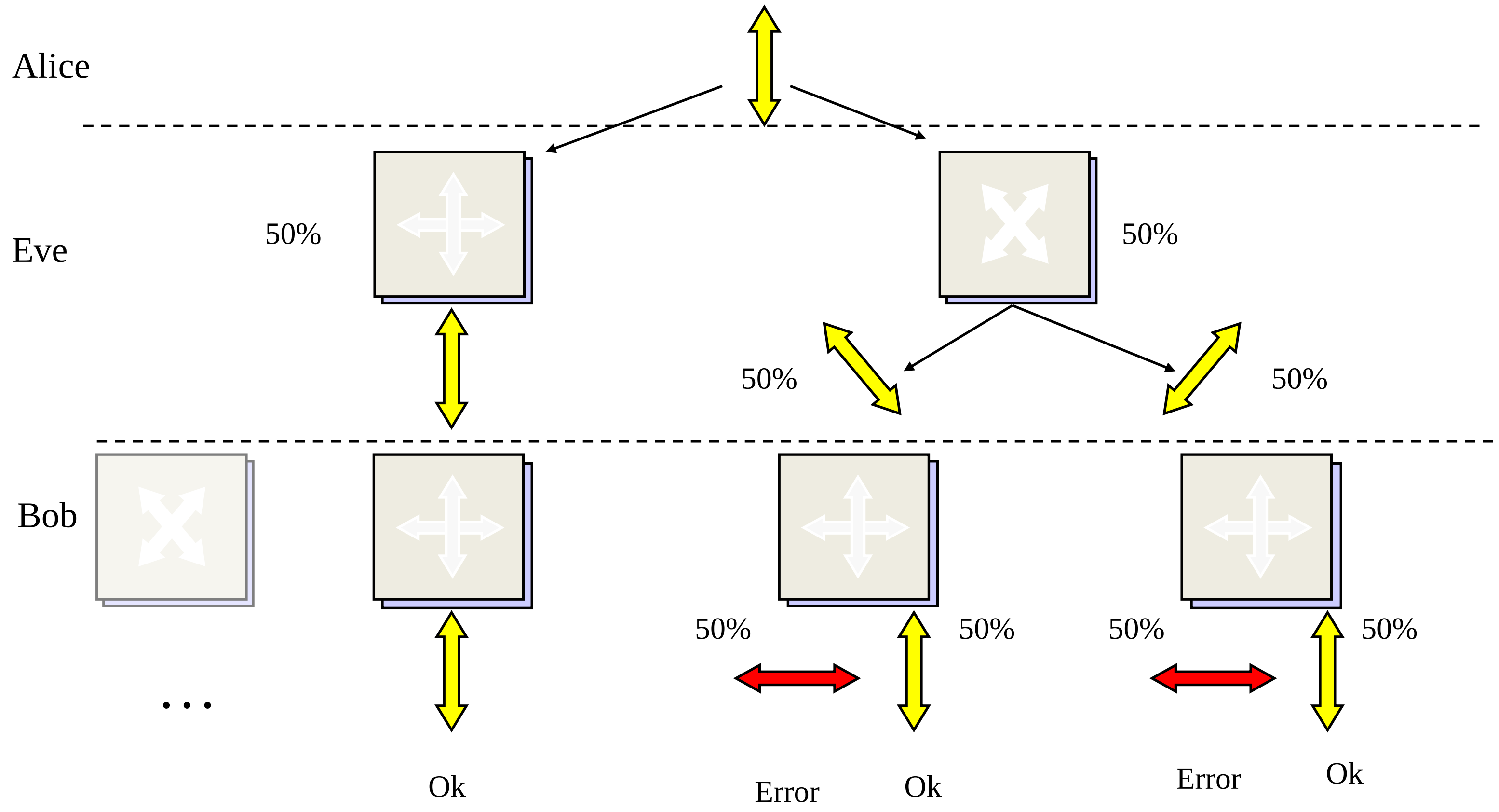
QKD is proven information theoretically secure!

BB84 protocol (Bennett, Brassard, 1984)



Alice's Bit Sequence	1	1	1	0	0	1	0	0	1	0	1	0
Bob's Bases	+	+	×	×	+	×	+	×	×	+	+	×
Bob's Results	0	1	0	-	0	1	1	1	1	-	1	0
Key	-	1	-	-	0	1	-	-	1	-	1	0

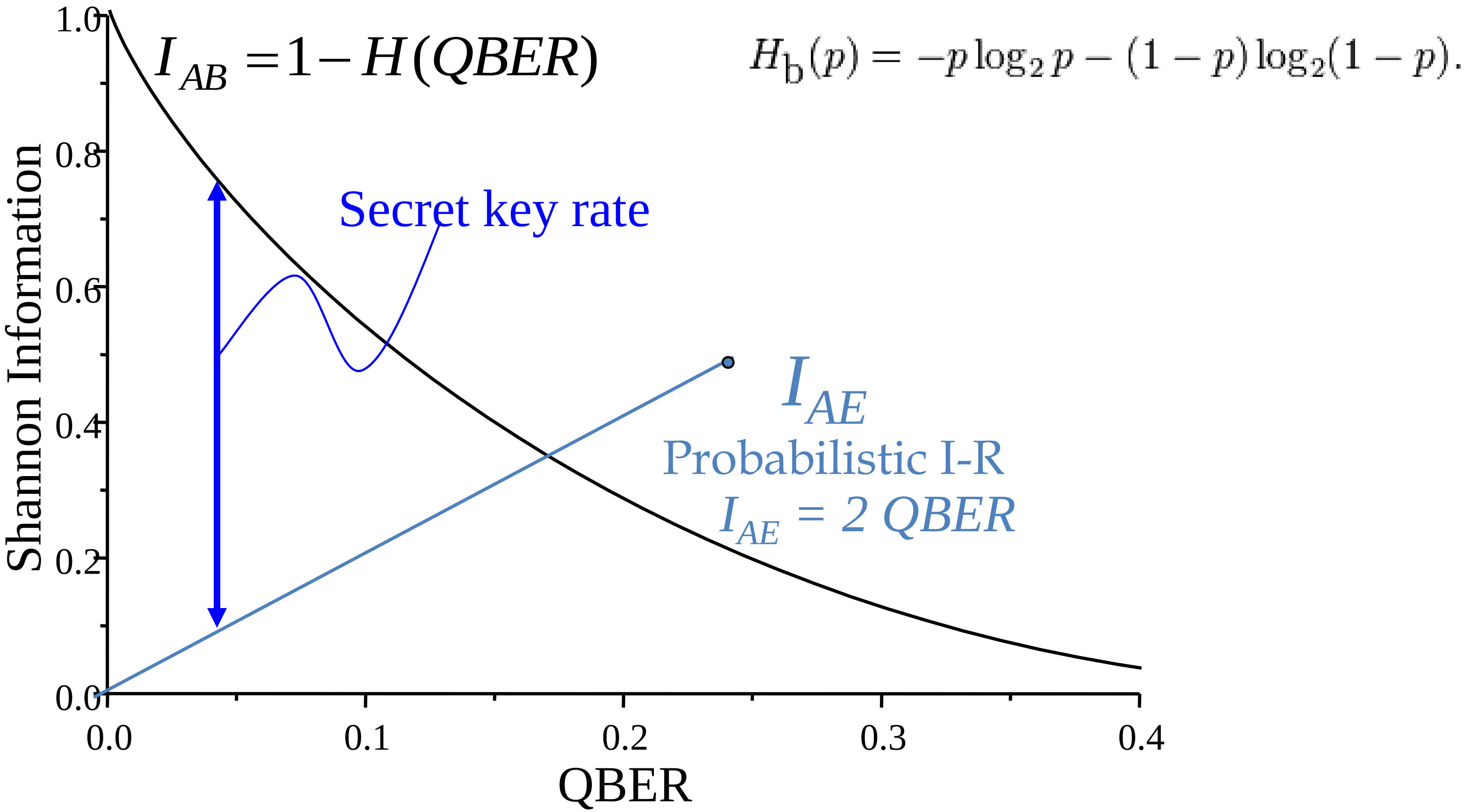
Eavesdropping (intercept-resend)



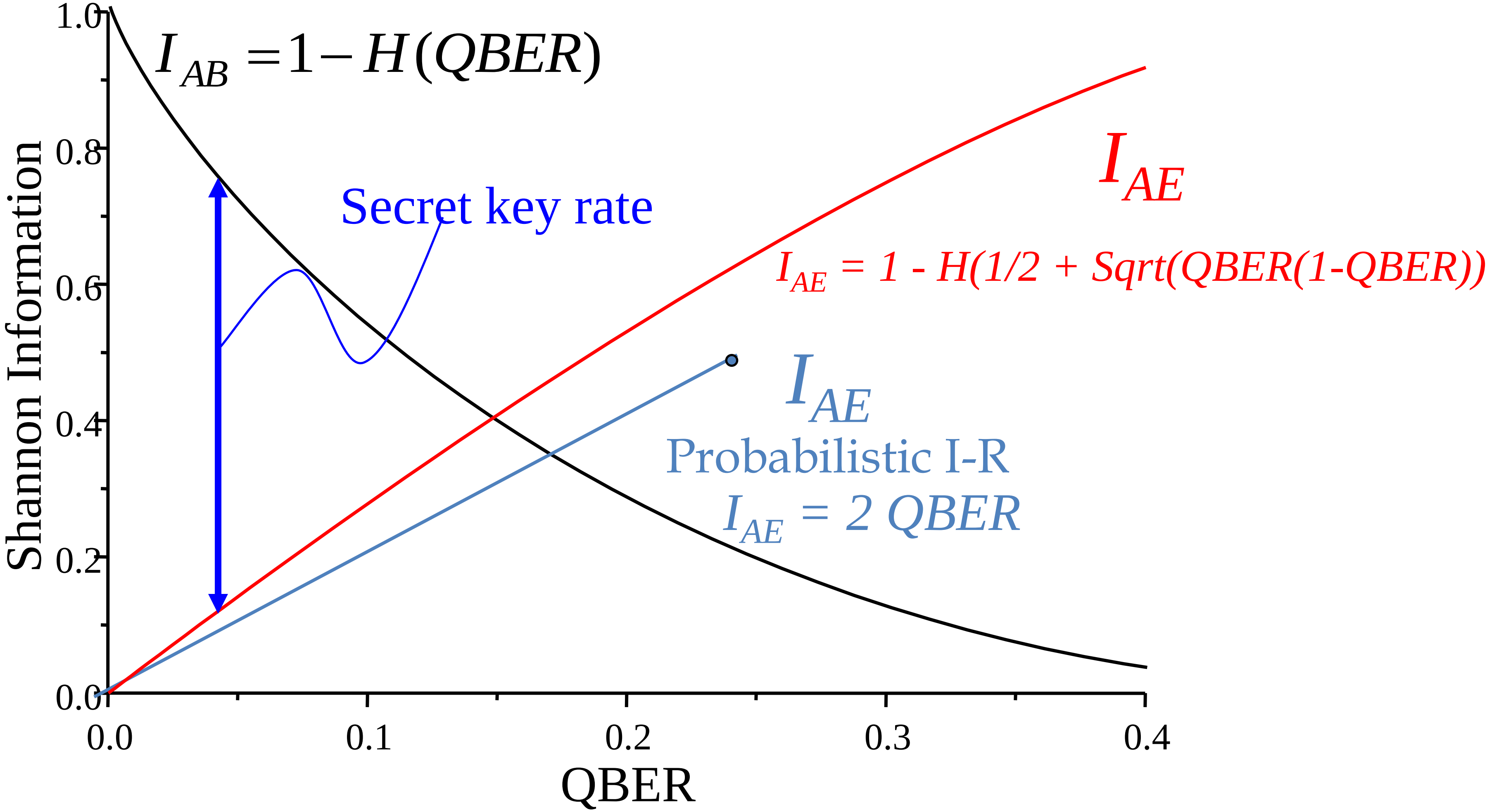
Error with 25 % probability

I_{AE} = 2 QBER (quantum bit error rate)

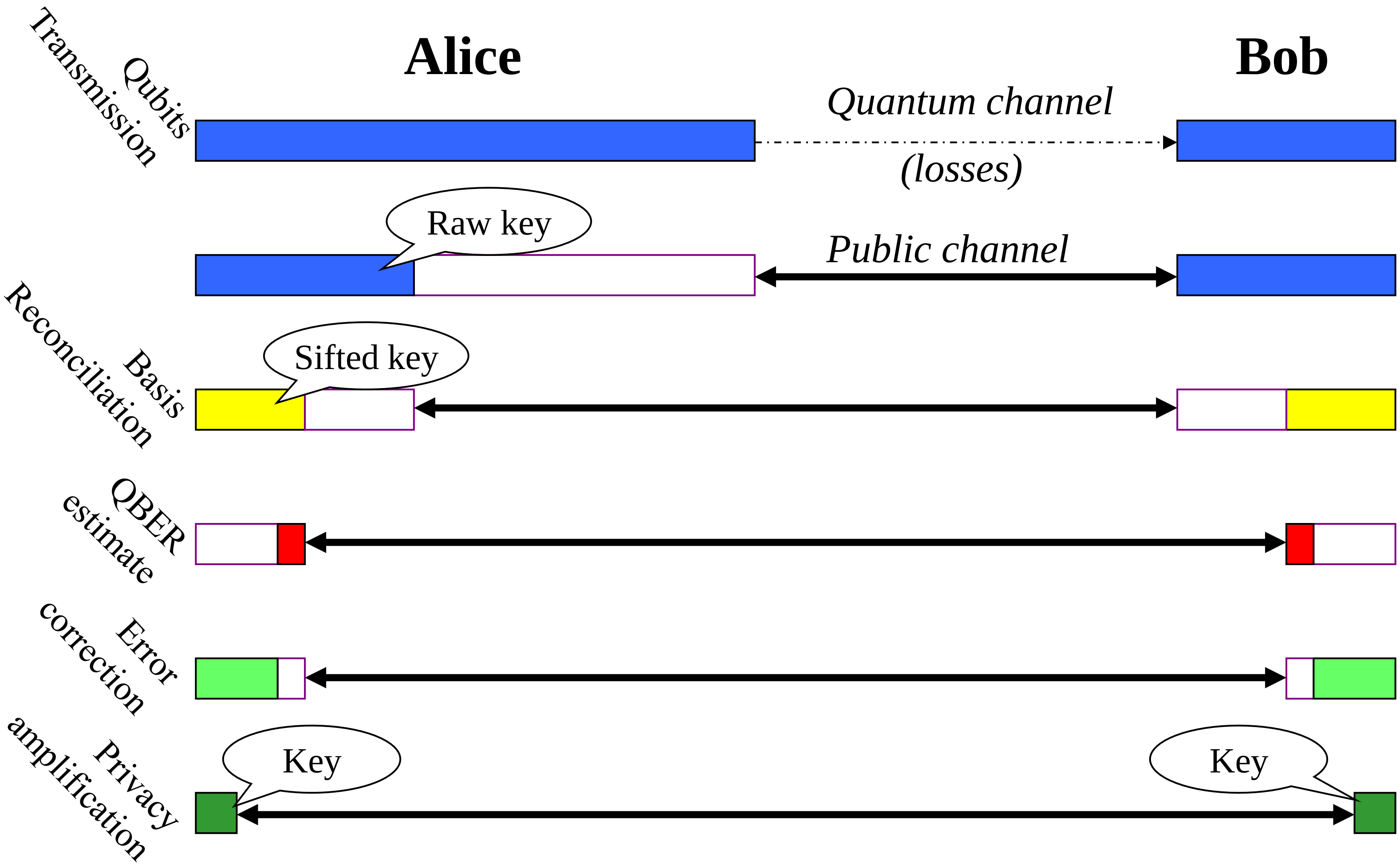
Eve attacks: information curves



Incoherent attacks: information curves

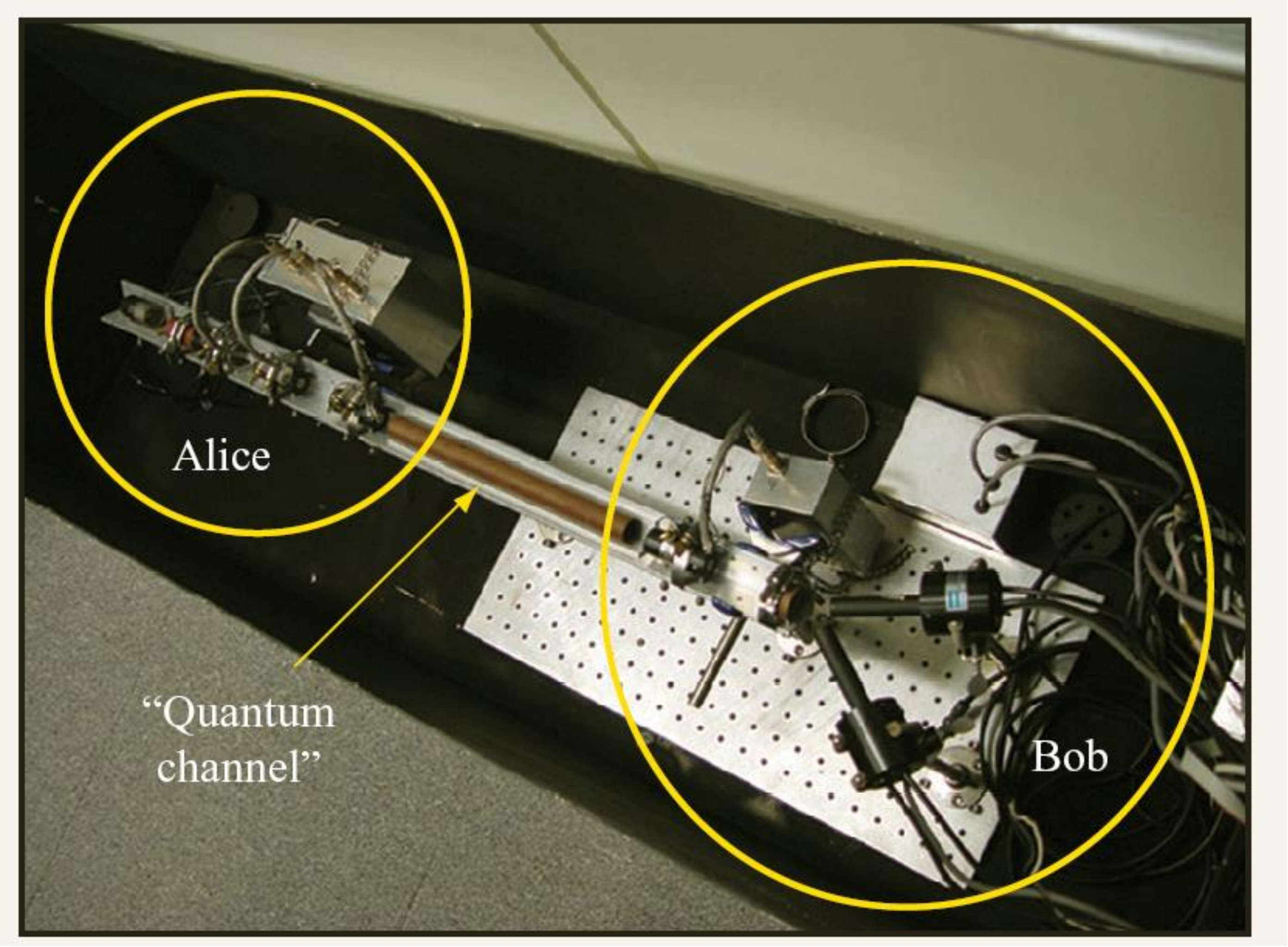


The steps to a secret key



+ Authentication!!!

Smolin and Bennett
IBM 1989



UNIVERSITÉ DE GENÈVE

Swiss QCRYPT project (2013)

nature photonics

LETTERS

PUBLISHED ONLINE: XX XX 2015 | DOI: 10.1038/NPHOTON.2014.327

Provably secure and practical quantum key distribution over 307 km of optical fibre

Boris Korzh[1]*, Charles Ci Wen Lim[1]*, Raphael Houlmann[1], Nicolas Gisin[1], Ming Jun Li[2], Daniel Nolan[2], Bruno Sanguinetti[1], Rob Thew[1] and Hugo Zbinden[1]

Proposed in 1984, quantum key distribution (QKD) allows two users to exchange provably secure keys via a potentially insecure quantum channel[1]. Since then, QKD has attracted much attention and significant progress has been made both in

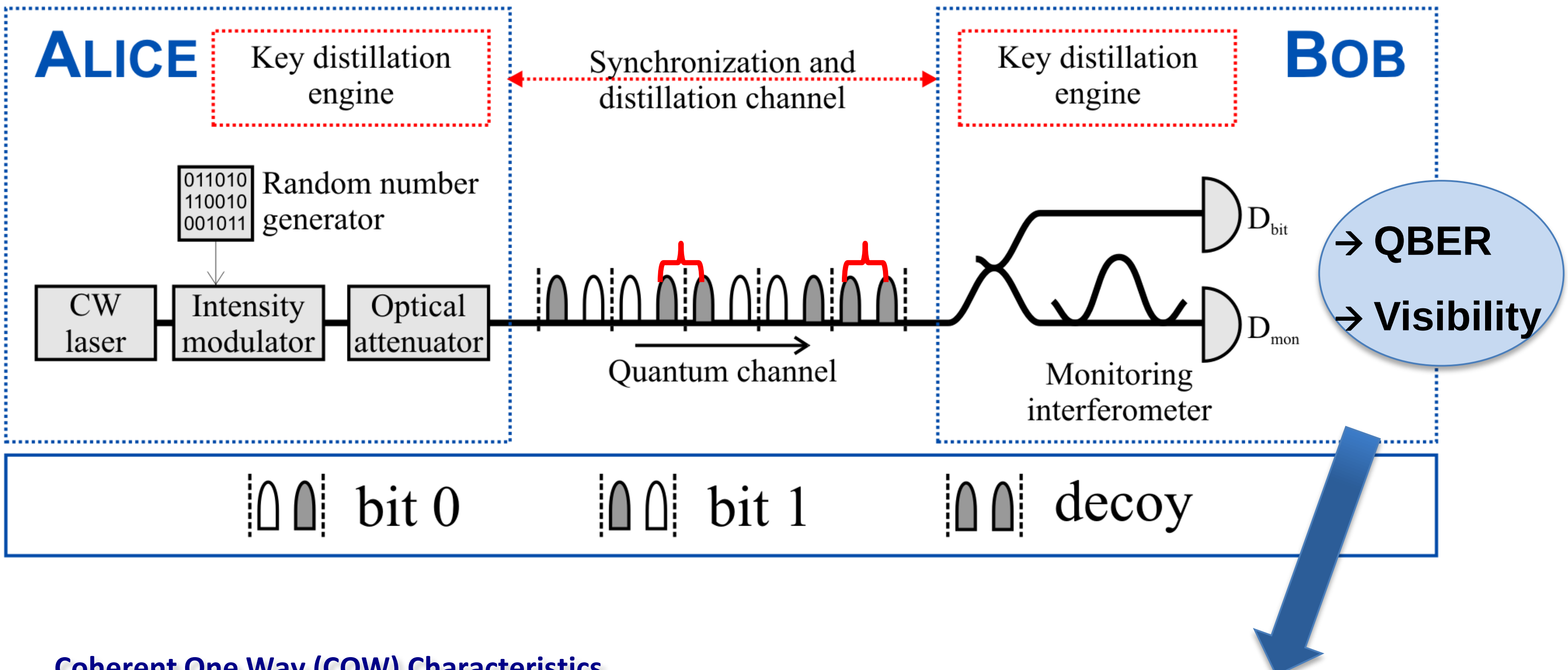
sends an additional test state, $|\alpha_t\rangle := |\alpha\rangle|\alpha\rangle$, to check for phase coherence between any two successive laser pulses. Therefore, phase coherence can be checked in any of these sequences, $|\alpha_0\rangle|\alpha_1\rangle$, $|\alpha_0\rangle|\alpha_t\rangle$, $|\alpha_t\rangle|\alpha_1\rangle$, $|\alpha_t\rangle$, $|\alpha_t\rangle|\alpha_t\rangle$, by using an imbalanced

- ❑ Efficient protocol
- ❑ Finite key analysis
- ❑ Low noise detectors
- ❑ Low loss fibres

Nature Photonics 9, 163–168 (2015)

UNIVERSITÉ DE GENÈVE

Ingredient 1: efficient and simple QKD scheme



Coherent One Way (COW) Characteristics

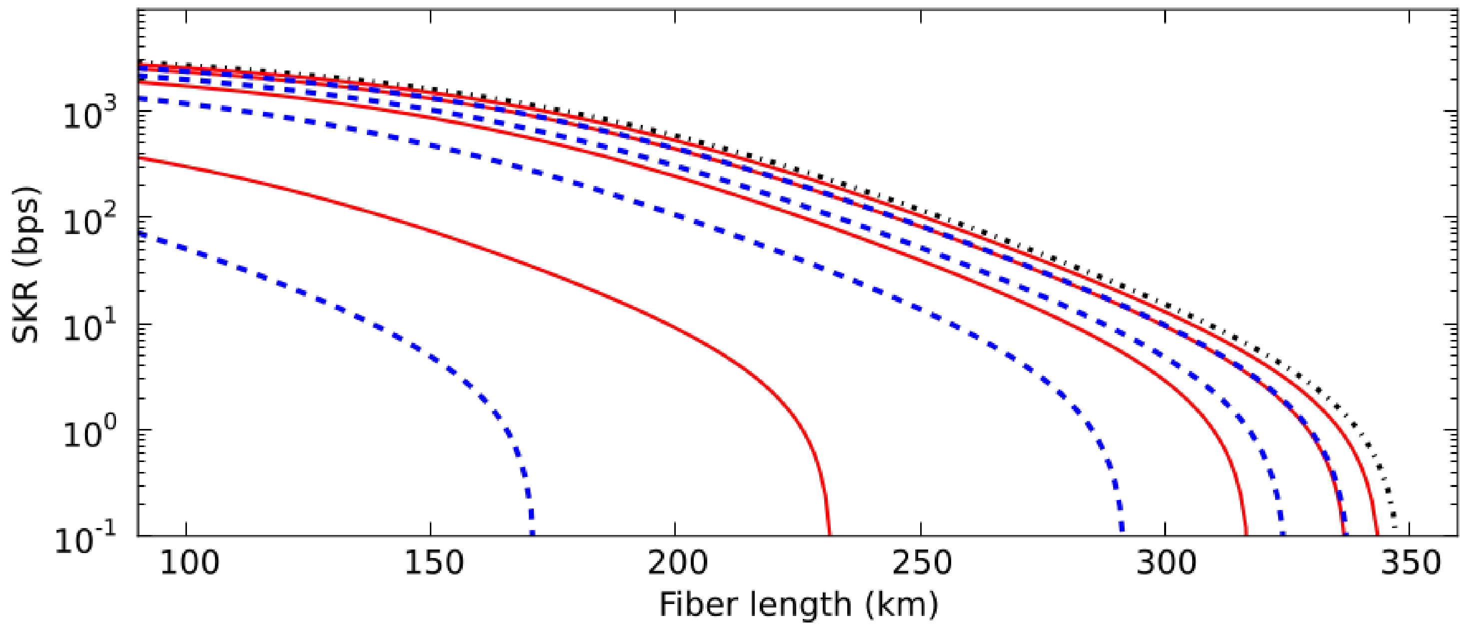
- 1.25 GHz clock (625 MHz bit generation rate)
- No active elements at Bob, robust bit measurement basis
- **Robust against photon number splitting PNS attacks**
- Security proof for collective attacks

check of coherence between qbits

Reveals action of eavesdropper
Input for key distillation

Ingredient 2: tight finite key analysis

Allows around an order of magnitude reduction of post-processing block size

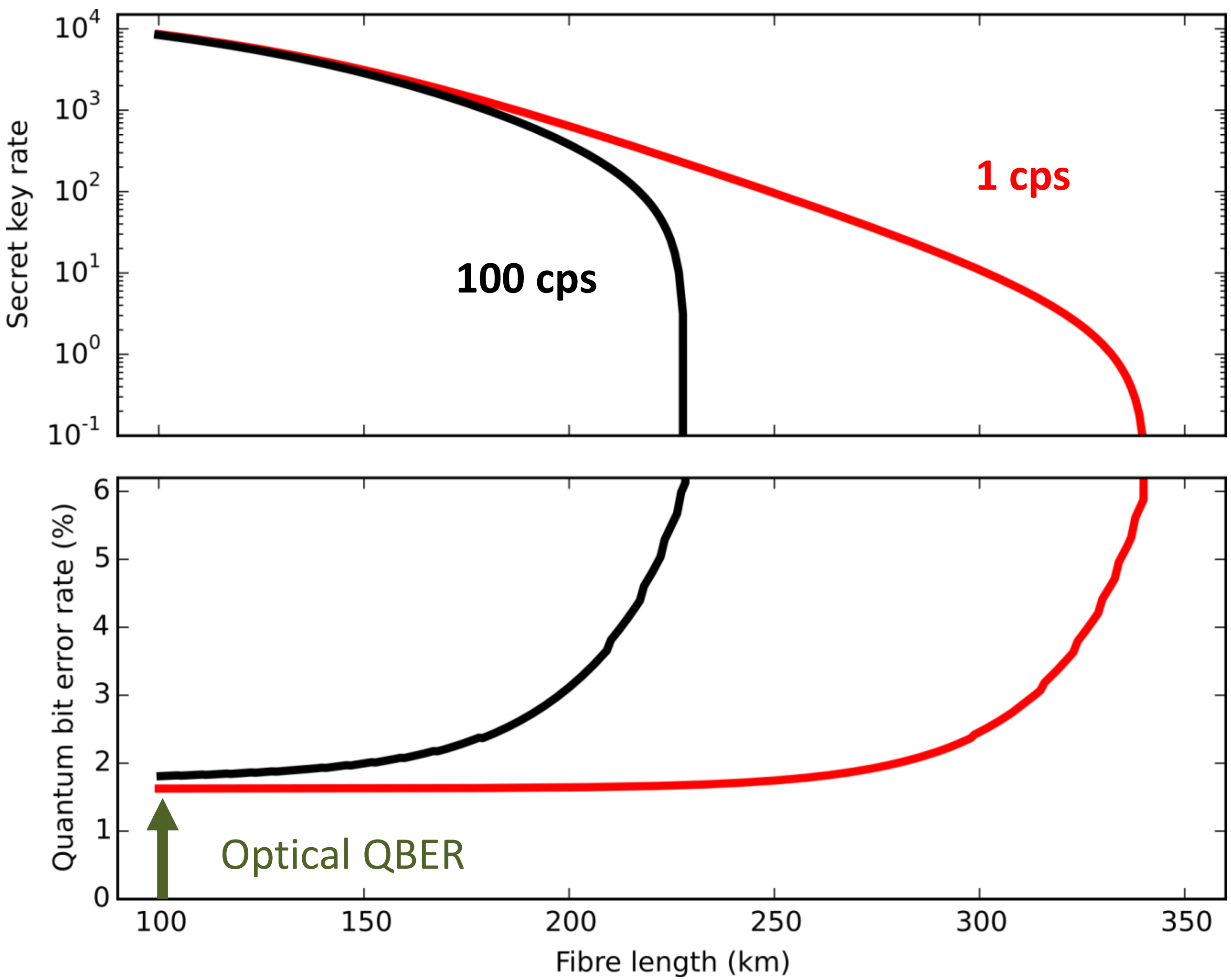


Comparison of secret key rate using different postprocessing blocksizes (10^4, 10^5, 10^6, 10^7 left to right)

Solid red: New tail inequality

Dashed blue: Previous tail inequality

Ingredient 3: low noise single photon detectors



System requirements:

- Low **dark count rate** of SPD
- Compact (no SNSPD)

Ingredient 4: Low Loss Optical Fibres

Total attenuation of an optical fiber:

CORNING

Not major contributors

Eliminated by CVD

Reduced by Cl dry

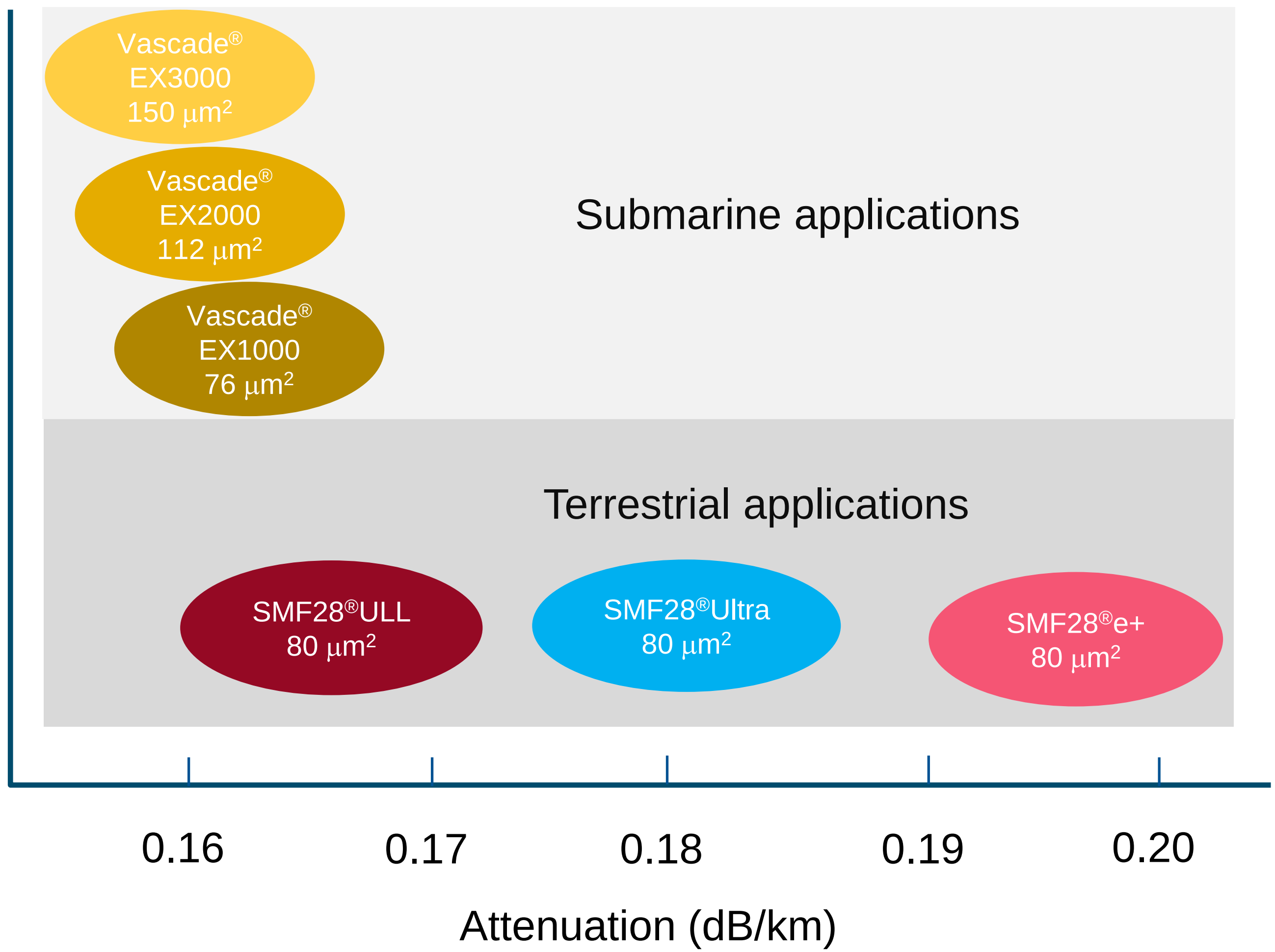
Reduced stresses

Fiber design Coating materials

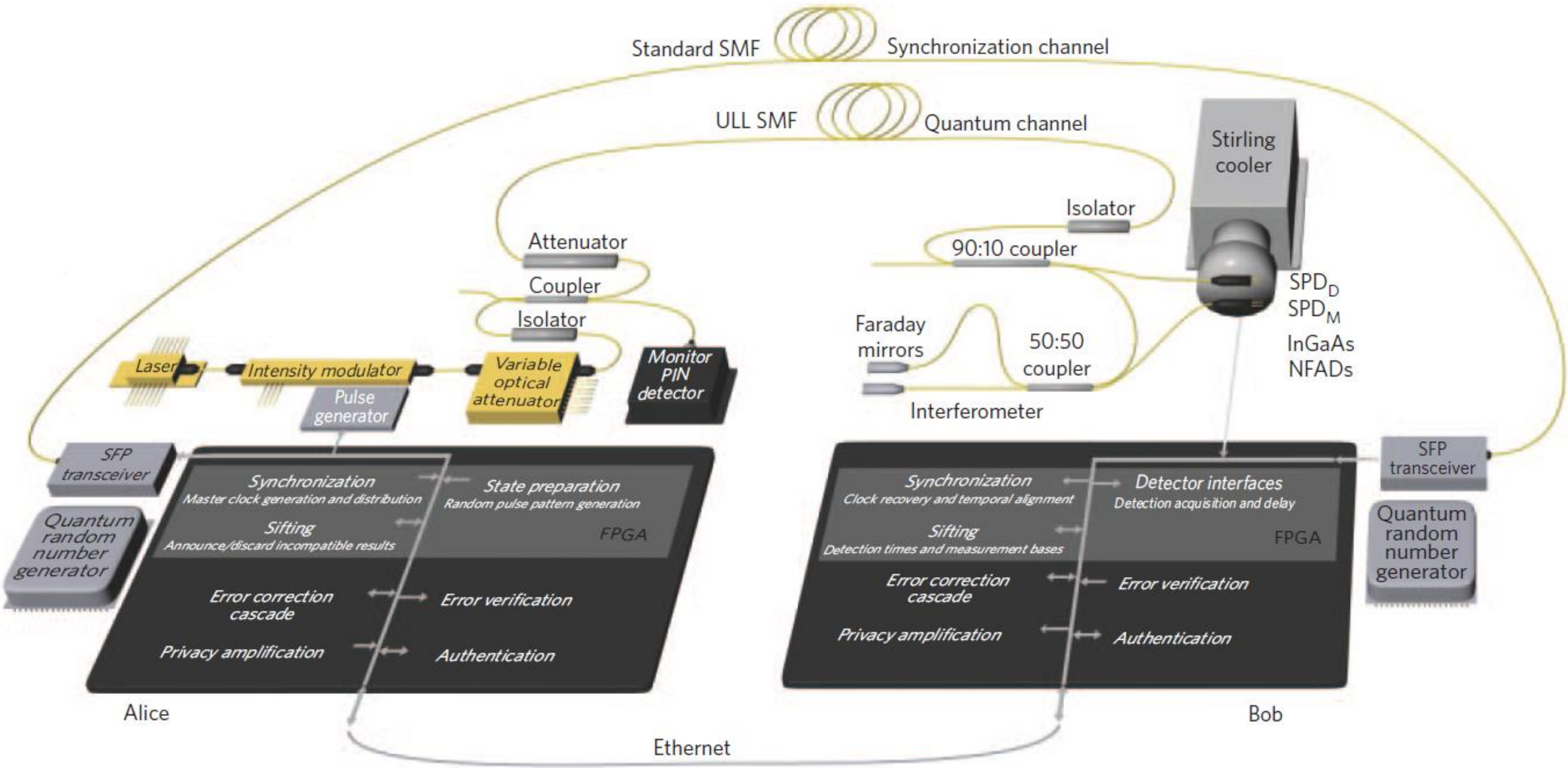
$$\alpha = \underbrace{\alpha_{RS} + \alpha_{IR} + \alpha_{UV}}_{\text{Intrinsic}} + \underbrace{\alpha_{TM} + \alpha_{OH} + \alpha_{IM} + \alpha_{BL}}_{\text{Extrinsic}}$$

Rayleigh scattering is dominant: density and dopant fluctuations minimized by choosing optimum (small) dopant concentration.

Ultra low loss fibers

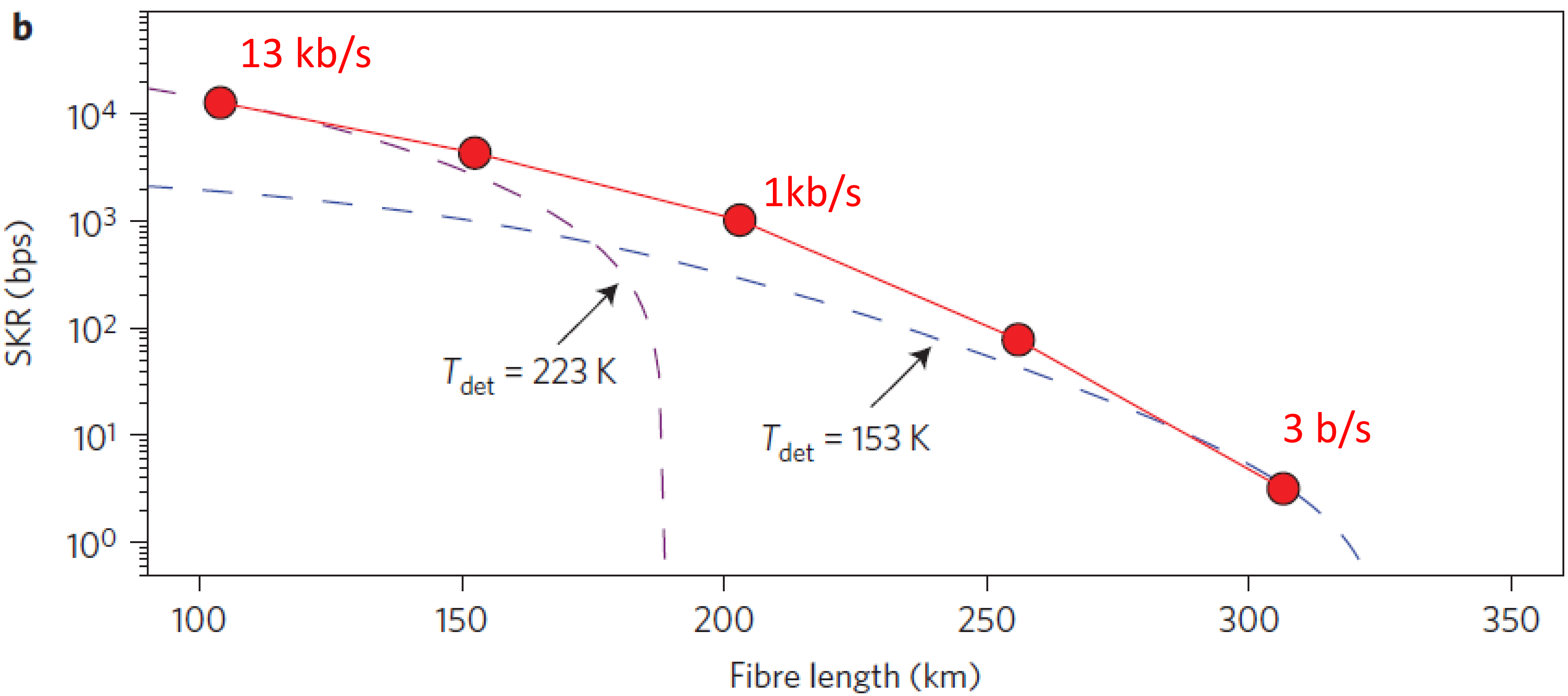


....putting all together:



FPGA is essential!

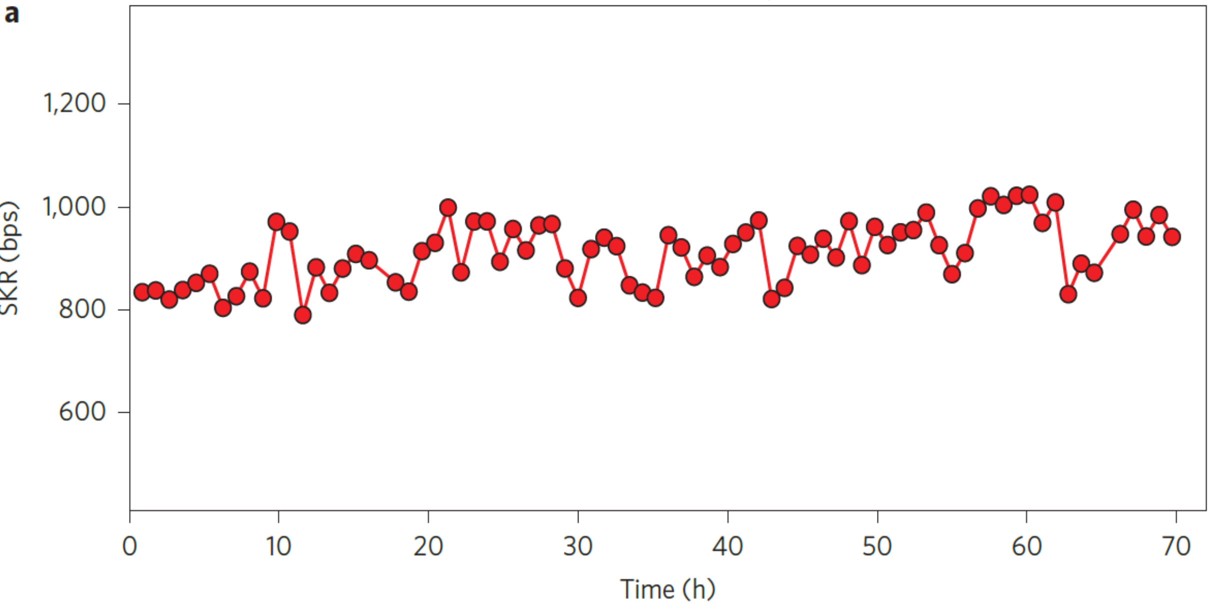
Results: Secret (finite key) rates vs distance



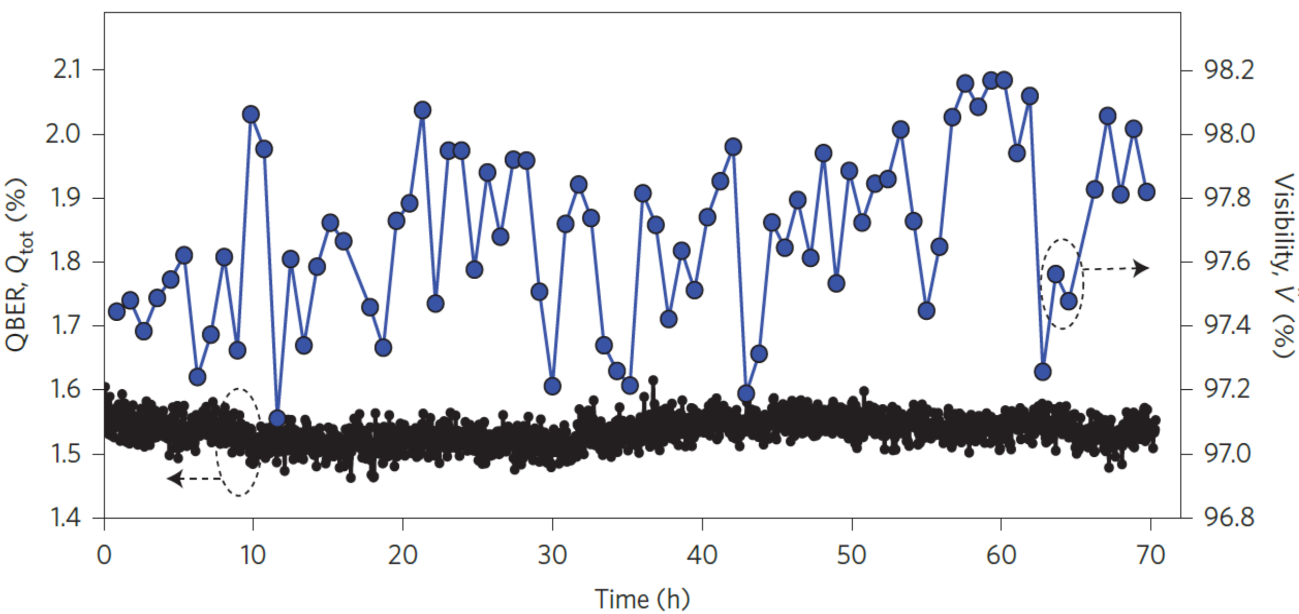
ε_{QKD}= $4x10^{-9}$

Stability over 70h (200km)

a



b



Automatic tracking:

QBER

- Temporal alignment:
  Quantum signal clock recovery with 10 ps resolution
- Extinction ratio:
  Modulator bias voltage

Visibility

- *Adjust Laser current (wavelength)*

UNIVERSITÉ DE GENÈVE

Current developments

- ❑ Make it smaller (ATCA Telecom standard),
- ❑ Make it cheaper (integrated optics)
- ❑ Make it faster
- ❑ longer distances (quantum repeater, satellite)

UNIVERSITÉ DE GENÈVE

Practical Security

MIT Technology Review

NEWS & ANALYSIS FEATURES VIEWS MULTIMEDIA DISCUSSIONS TOPICS POPULAR: SMARTPHONE BREAKTHRO

VIEW

5 COMMENTS

The Physics arXiv Blog
May 17, 2010

Commercial Quantum Cryptography System Hacked

Physicists have mounted the first successful attack of its kind on a commercial quantum cryptography system.

Researchers crack the world's toughest encryption by listening to the tiny sounds made by your computer's CPU

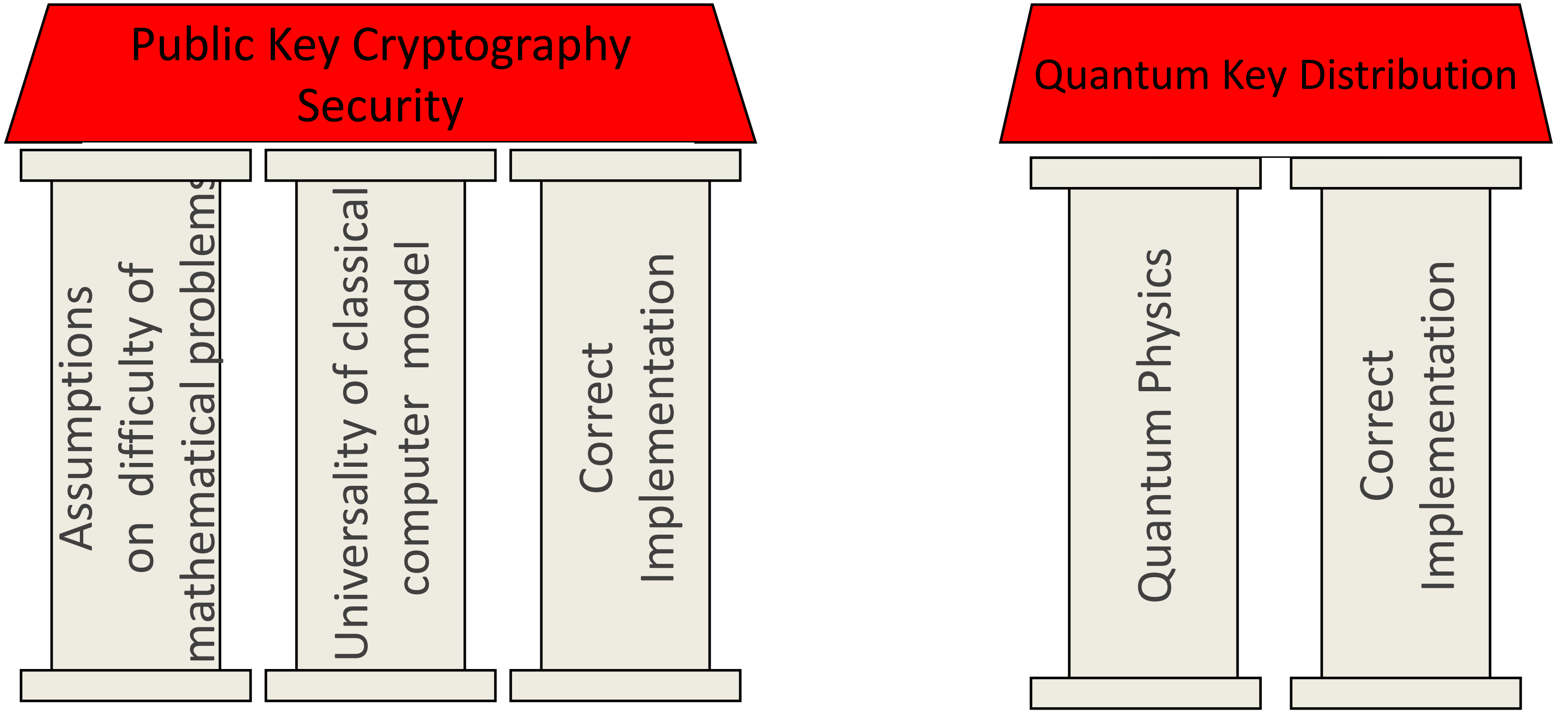
By Sebastian Anthony on December 18, 2013 at 2:27 pm | 55 Comments

4096-bit RSA

http://www.tau.ac.il/~tromer/papers/acoustic-20131218.pdf

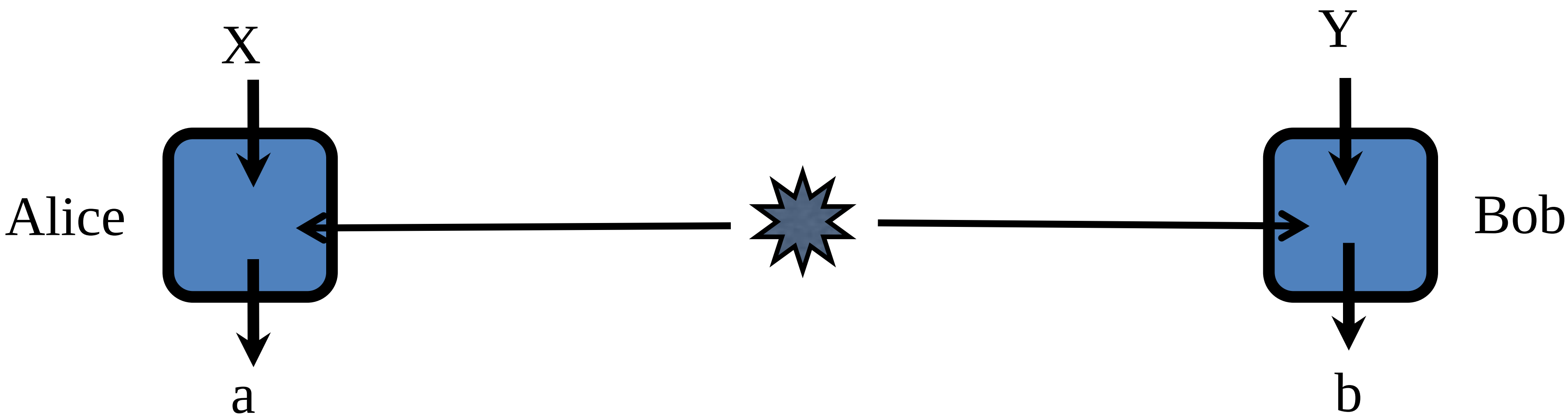
UNIVERSITÉ DE GENÈVE

Pillars of Cryptography



QKD cannot be broken, but a specific implementation can!

Quantum Correlations
for Device Independent Quantum Key Distribution

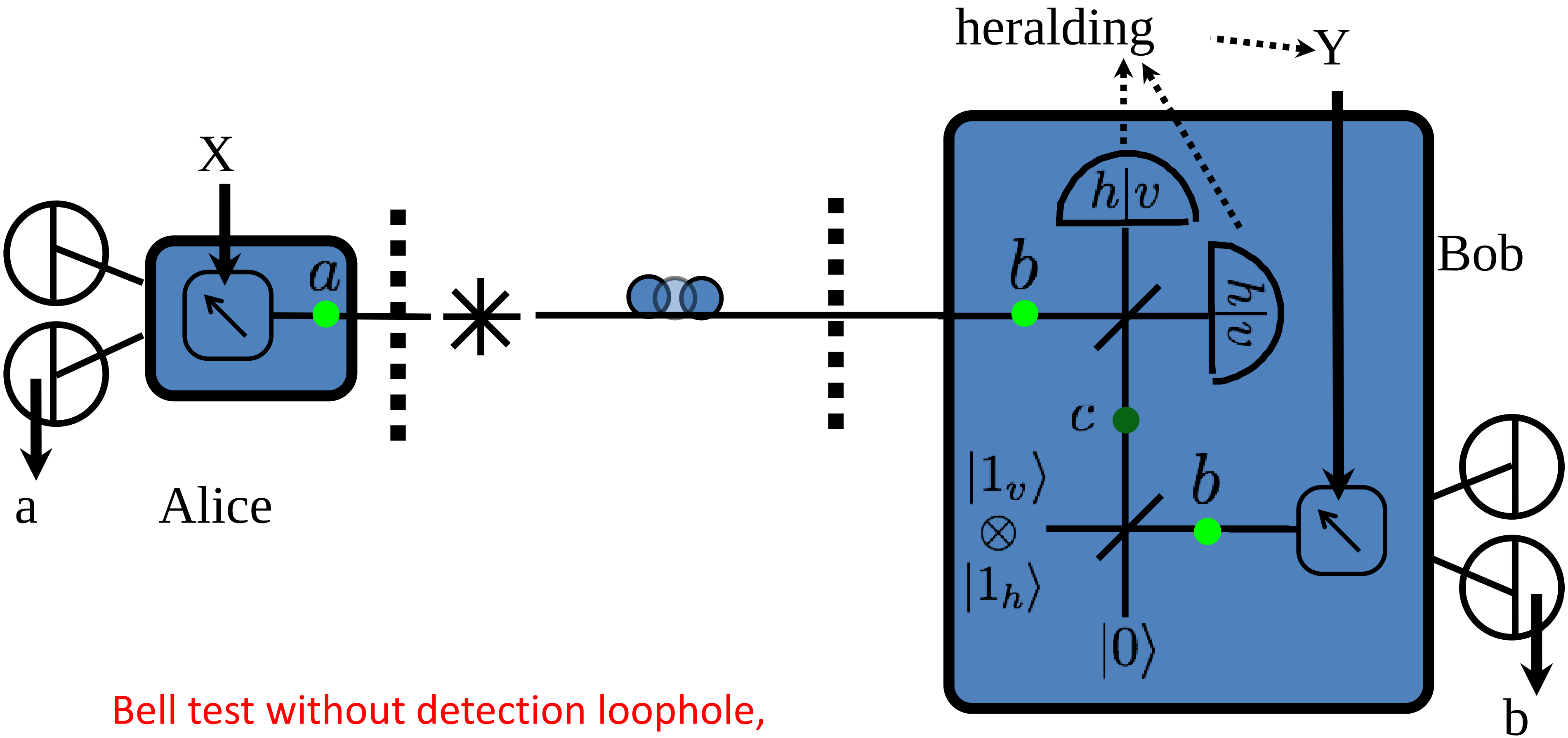


Bell violation guarantees entanglement
independently of the device!

It is crucial to close the detection loophole!

Required efficiency 82.8%
Transmission efficiency of 10 km of telecom fiber is roughly 60% !

Qubit amplifier

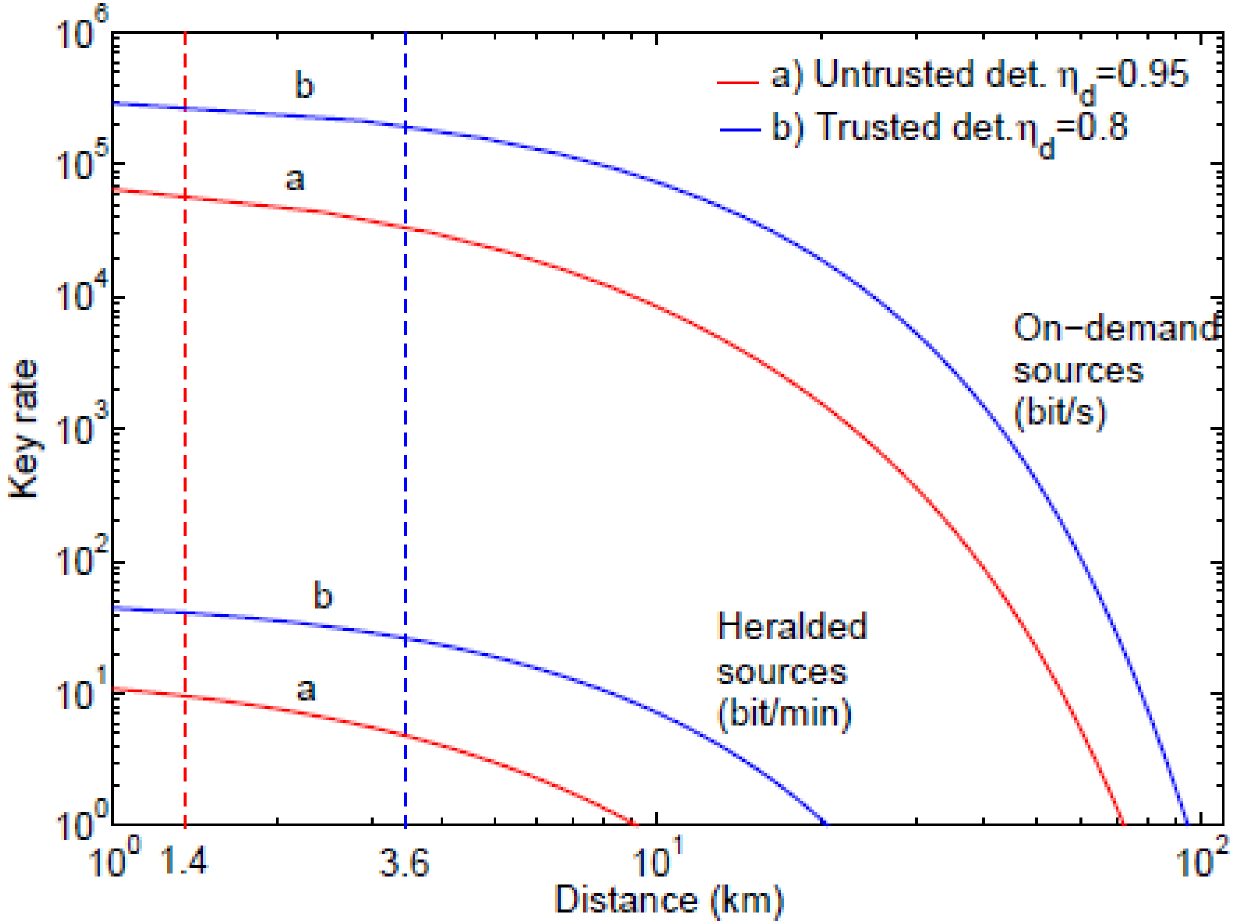


Bell test without detection loophole,
conditioned on the heralding signal

PRL 105, 070501 (2010)

UNIVERSITÉ DE GENÈVE

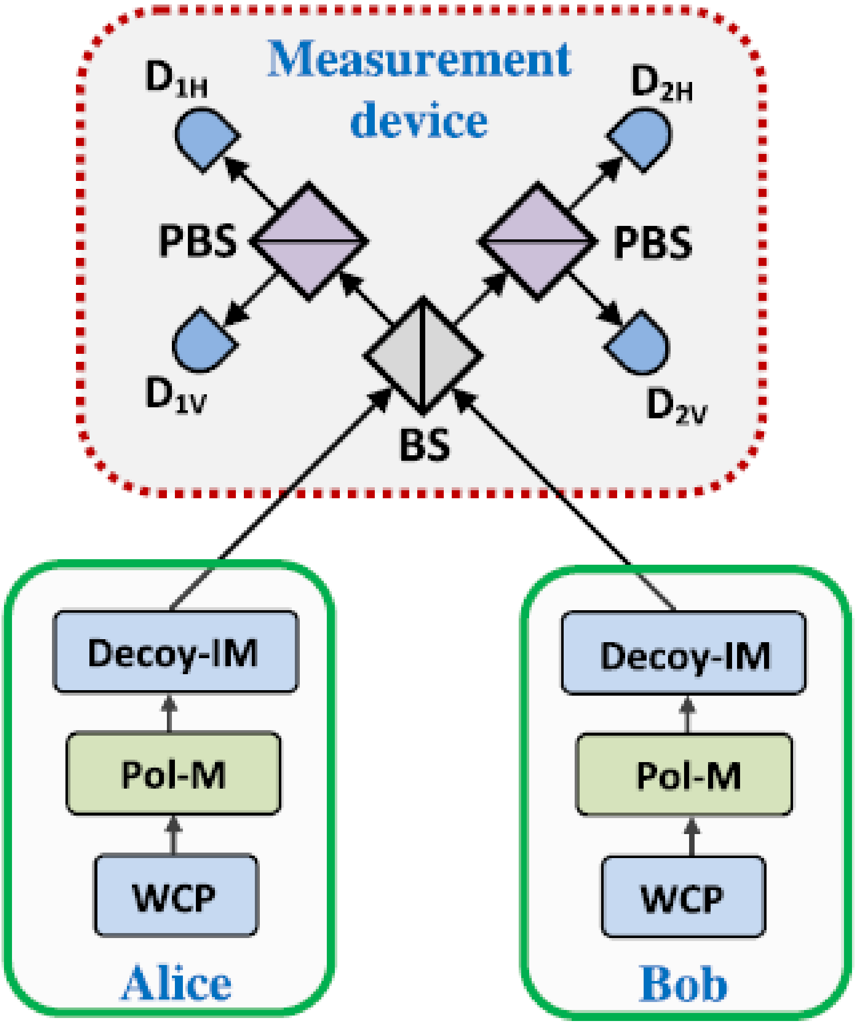
Without a Single Photon Sources on demand, DI-QKD is completely unrealistic



P(1) = 95%, Repetition rate 10 GHz

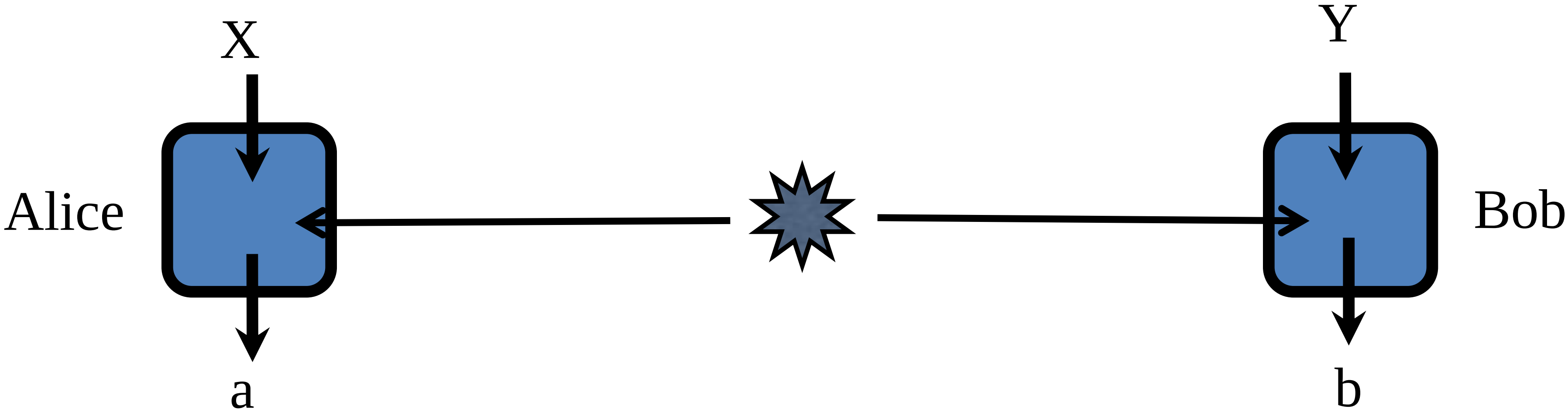
Measurement Device Independent (MDI) QKD

(basic idea: «BSM measurement by central untrusted agent)



Lo et. al., PRL 2011

Where are the limits?
What's the device? What's the secure office?

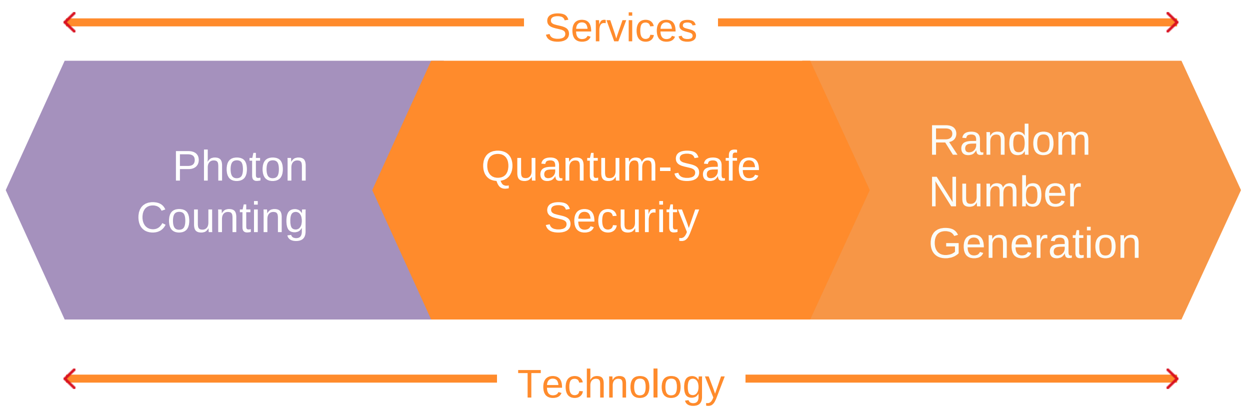


What is the main concern?
Imperfect device? Manufacturer not trustworthy?

- Standardization (ETSI)
- Open hardware / open software solution

What are the concerns of a QKD company?

ID Quantique



Swiss company, founded 2001, based in Geneva.

World leaders in Quantum-Safe Crypto.

Spin-off of University of Geneva, Group of Applied Physics.

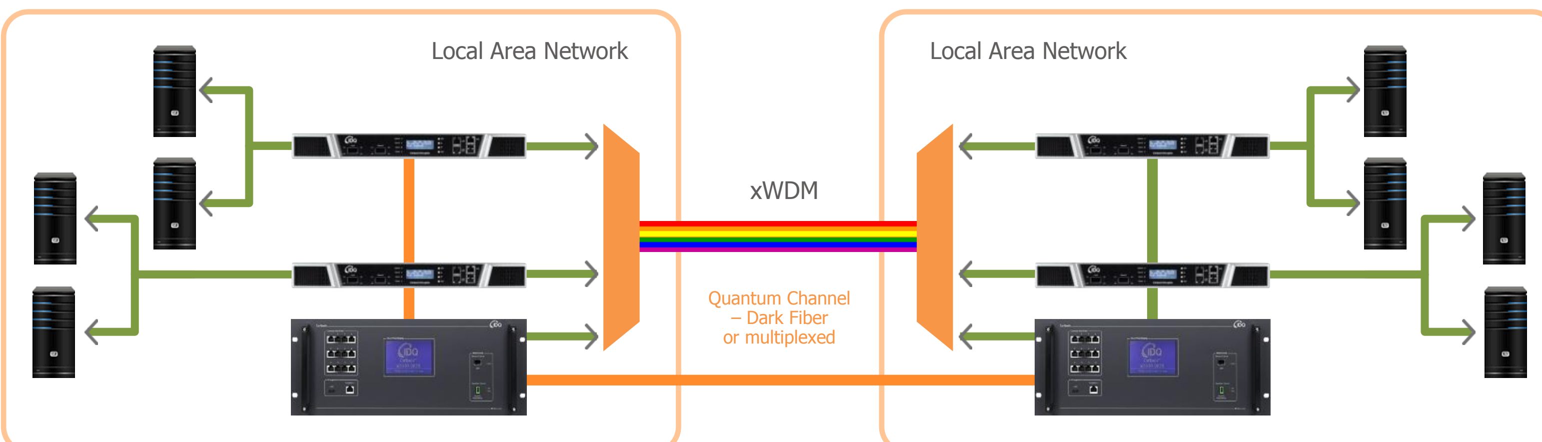
Quantum-Enabled Network Encryption: Today

- Transparent Layer 2 Encryption
  - AES-256 up to 100Gbps
  - Multiprotocol (Ethernet, Fibre Channel)

- Provably secure key distribution
  - Distilled key distribution rate: 1000 bps over 25km/6dB
  - Range: 100km

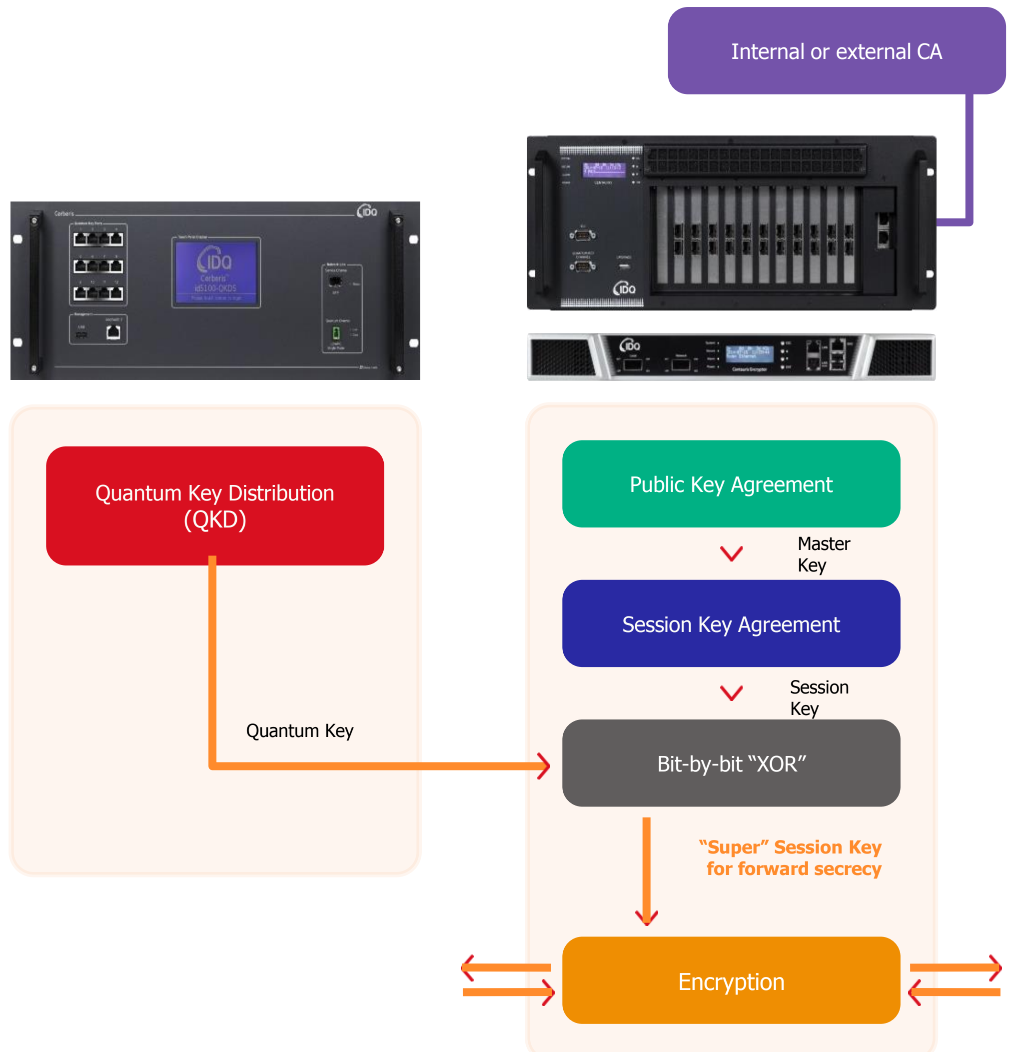
+

Quantum key server



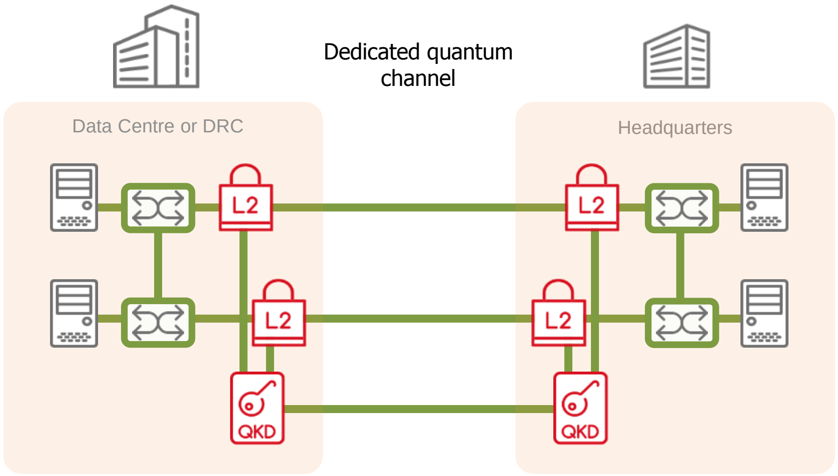
QKD Dual Key Agreement

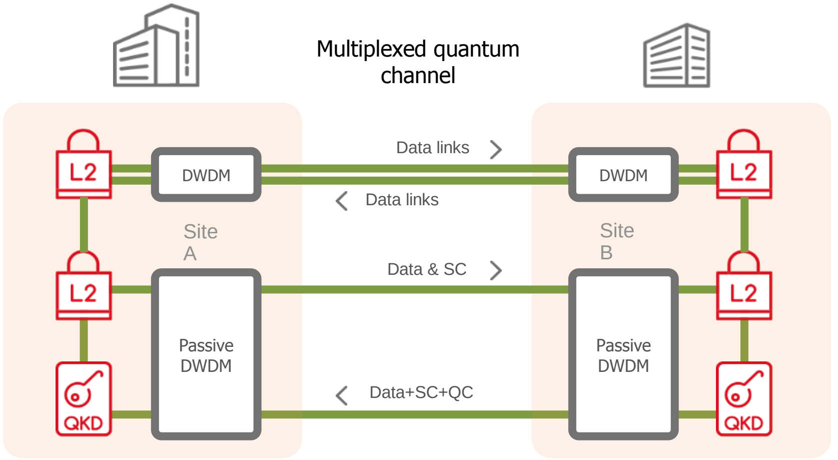
- Quantum keys are based on high quality entropy (encryption key) from provably random QRNG.
- Quantum Key is mixed with the standard AES session key.
- Advantages:
  - Maintains existing encryptor certifications (eg. FIPS, CC).
  - Generates "super session“ key which guarantees forward secrecy.
  - Eavesdropping protection.
  - No single point of vulnerability back to public-key exchange or manual key exchange (where the initial keys remain static for a long period of time). In contrast each quantum key is independent & uncorrelated, and automatically updated every minute.



European Banks: QKD in Data Center Interconnect

- European banks secure critical links between bank headquarters and data recovery centers, and inside MAN.
  - All digital assets of bank pass over over DCI link.
- Supports AES 256 bit key exchange every hour, with additional quantum key buffer.
- Quantum channel:
  - Both on dedicated dark fibre (up to 100km).
  - Or multiplexed with data over single fibre (up to ~30 kms).

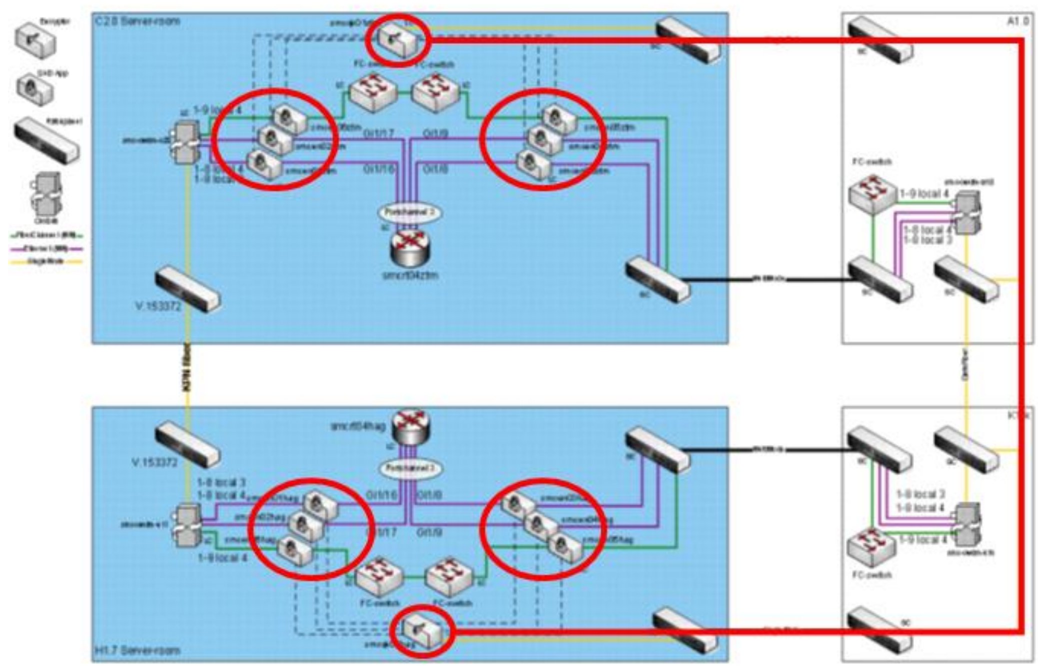




QKD in Data Centers for Financial Companies

Atos SIEMENS

- QKD-secured data center link large financial institution in the Netherlands.
- Installed in 2010.
  - High-speed encryption
  - 4 x Ethernet 1G links
  - 2 x FC-4 links



Quantum Random Number Generator

- ## Why RNG?

  Game/Simulation/Classical Cryptography (RSA, DSA …)/
  Quantum Key Distribution

- ## Why Physical RNG?

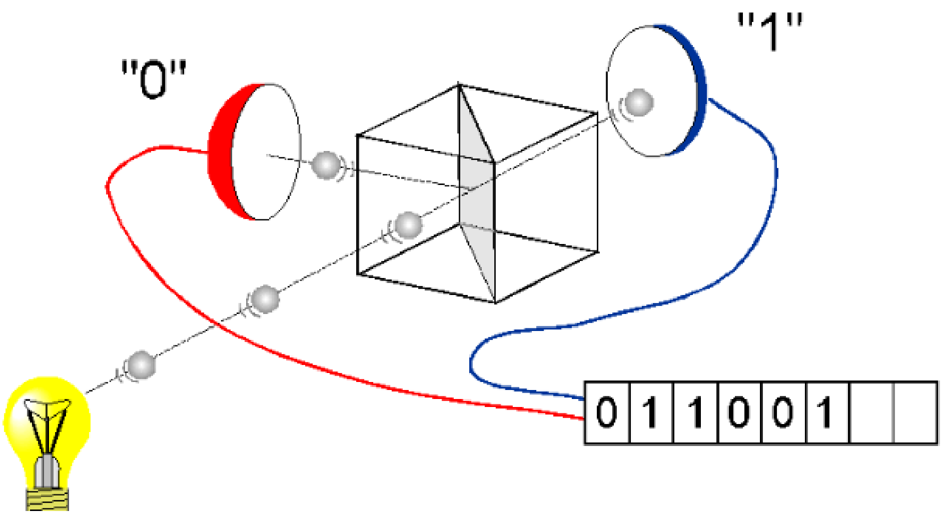
  "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." John von Neumann (1951)

- ## Why Quantum RNG?

  Random classical noise could be predictable
  Possibility to estimate/certify the entropy

Realisations of QRNGs

- using single photons



Rate: 4 Mbit/s per module

Evaluation and Certification

- National Metrology Laboratory
  - Focus: Physical Principle, Statistical Properties
  - Products covered: PCI, PCIe, USB (+ component)

- Gaming Test Houses
  - Focus: Statistical Properties, Software, Scaling
  - Products covered: PCI, PCIe, USB (+ component)

- National Security Government Agencies
  - Focus: Physical Principle, Implementation
  - Products covered: Component


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Justice and Police FDJP
Federal Office of Metrology METAS

Certificate of Conformity No 151-04255

Object	**Quantum Random Number Generator** Quantis-USB S/N 070222A410 Quantis-PCI-1 S/N 08338A310
Applicant	**id Quantique SA** Ch. De la Marbrerie 3 1227 Carouge/Geneva Switzerland


CTL

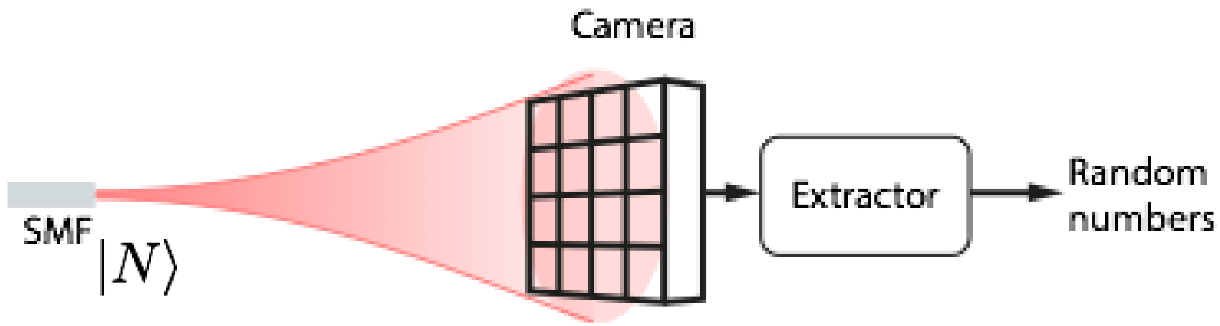
Certificate of Compliance

This is to certify that the Random Number Generator
Quantis-v10.10.08
by
ID Quantique SA
has been tested by
CTL, Compliance Testing Laboratory
and has been found to be *suitably unpredictable and fit for purpose*

Issue Date: 30.03.2011

Technical Compliance Manager, CAST Limited

- Exploiting photon statistics (shot noise)



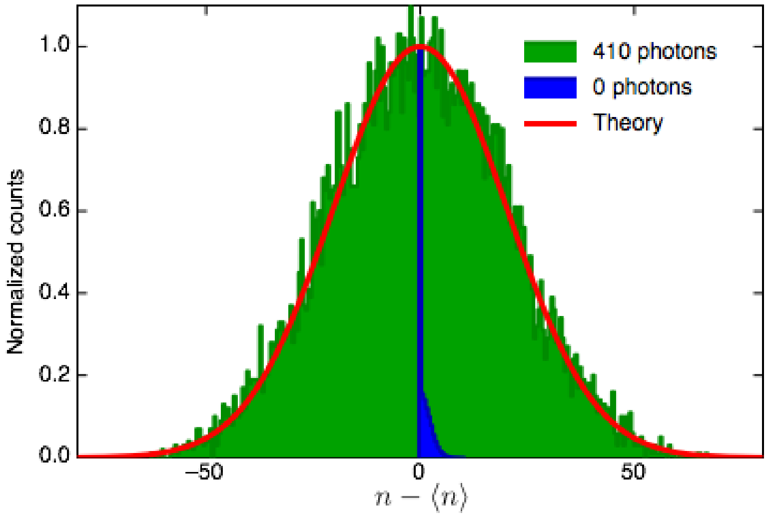
$$\langle n \rangle = N \times P_{\mathrm{det/pixel}} + \mathrm{Noise}$$

$$\sigma_n = \sqrt{N \times P_{\mathrm{det/pixel}} + \sigma^2_{\mathrm{Noise}}}$$

If $N \times P_{\mathrm{det/pixel}} \gg \sigma^2_{\mathrm{Noise}}$

Possibility to
extract quantum randomness

Example with a Nokia N10



Sanguinetti B., *et al.* 2004 Phys. Rev. X 4 031056

Application of shot noise: Quantum Secure Steganography

PHYSICAL REVIEW A **93**, 012336 (2016)

Perfectly secure steganography: Hiding information in the quantum noise of a photograph

Bruno Sanguinetti,[1,*] Giulia Traverso,[2] Jonathan Lavoie,[1] Anthony Martin,[1,†] and Hugo Zbinden[1]

[1] *Group of Applied Physics, University of Geneva, Switzerland*

[2] *Fachbereich Informatik, Technische Universität Darmstadt, Germany*

(Received 28 April 2015; revised manuscript received 19 November 2015; published 21 January 2016)

Disclaimer: We are physicists....

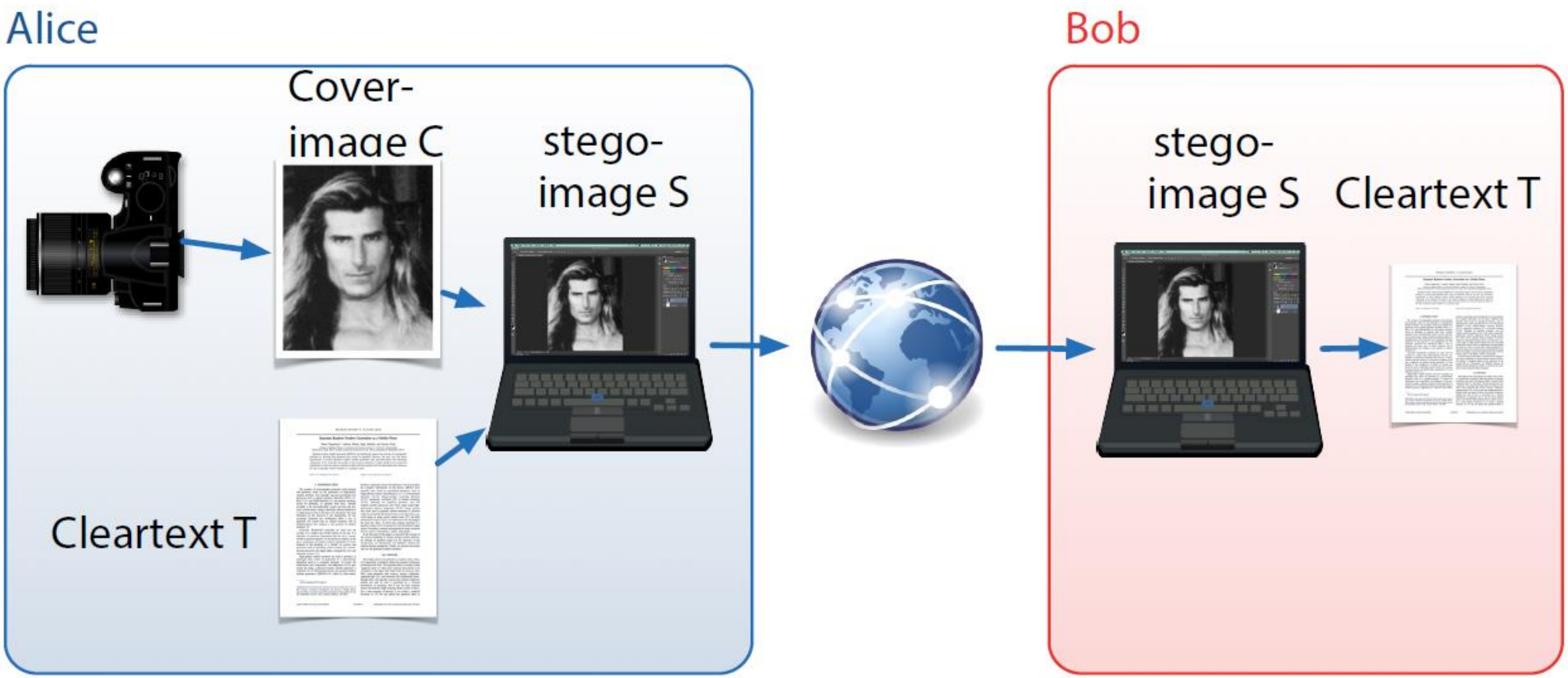
UNIVERSITÉ DE GENÈVE

What is Steganography?

- from Greek *steganos*, or "covered," and *graphie*, or "writing"): hiding of a secret message within an ordinary message
- Cryptography guarantees secrecy, but not privacy.
- Steganography important in countries with untrustworthy, totalitarian regimes
- Universal Declaration of Human Rights: Art. 19

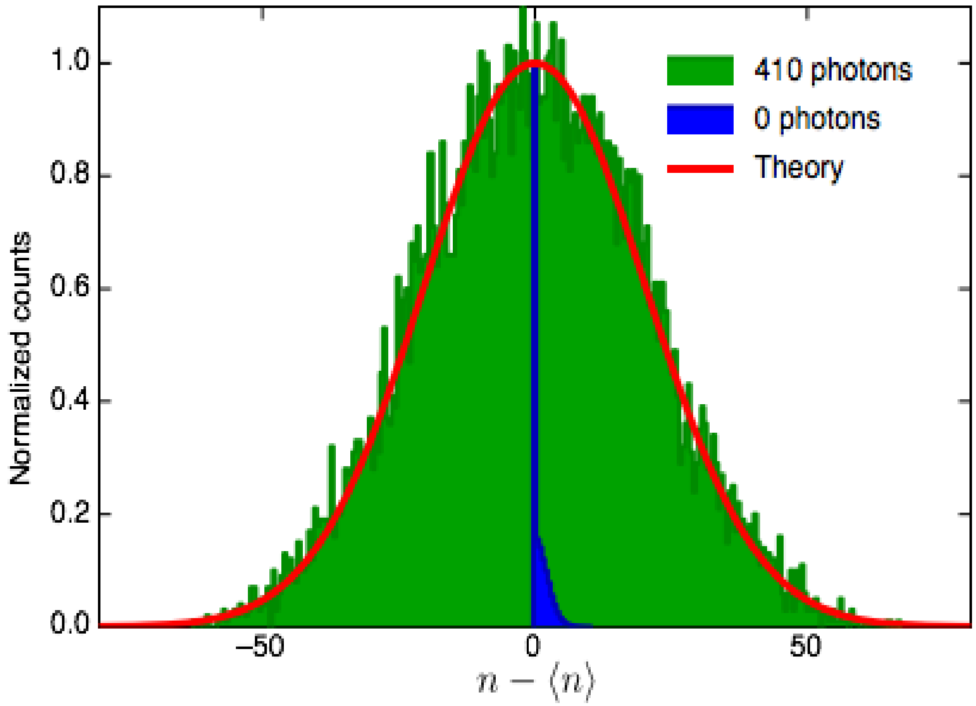
UNIVERSITÉ DE GENÈVE

Hiding secret information in a picture

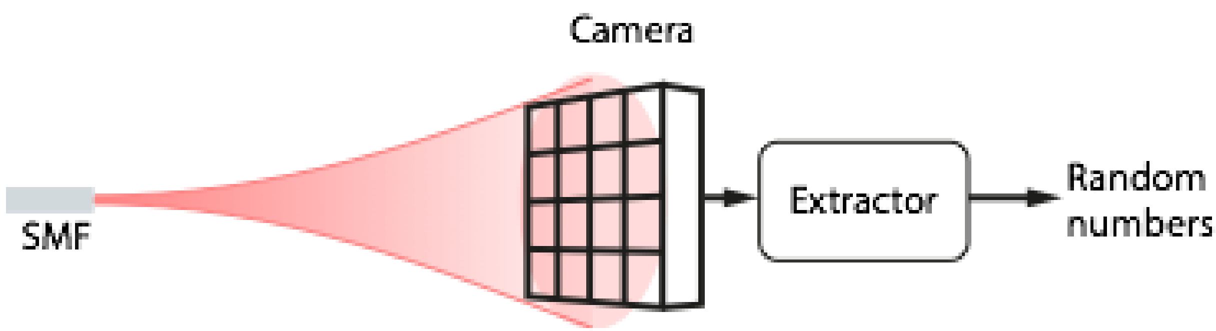


UNIVERSITÉ DE GENÈVE

- Steganography exploiting shot noise



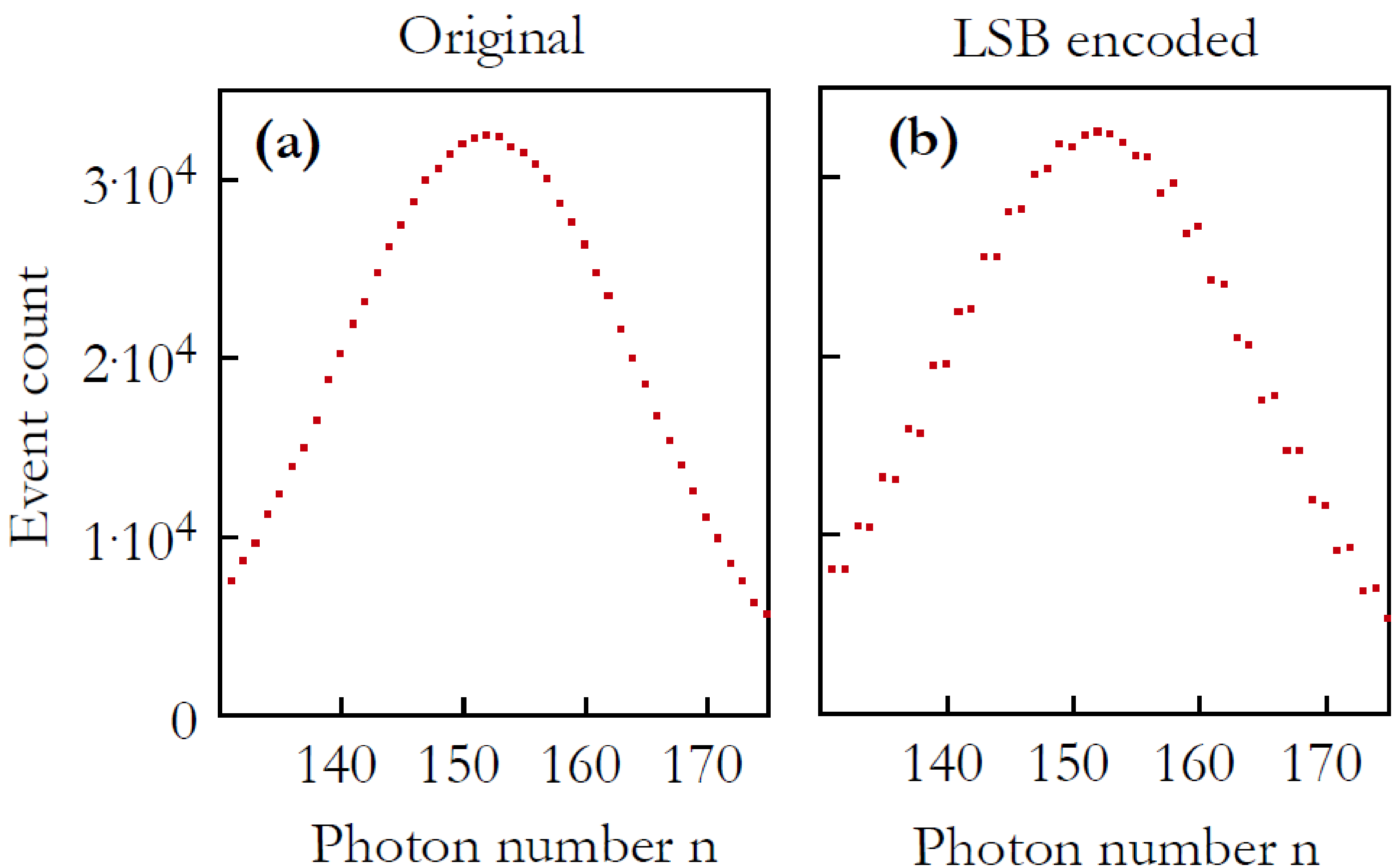
Example with a Nokia N10



Sanguinetti B., *et al.* 2004 Phys. Rev. X 4 031056

Naive idea

- Use least significant bit to transmit (OTP) encoded data



Simulated Histogram of the pixel values of a homogeneous area

Better idea

- Take photographs of a static object in rapid succession
- Assumptions:
  1. state of object and camera unchanged between to consecutive pictures K and C
  2. Each pixel is statistical independent (no crosstalk).

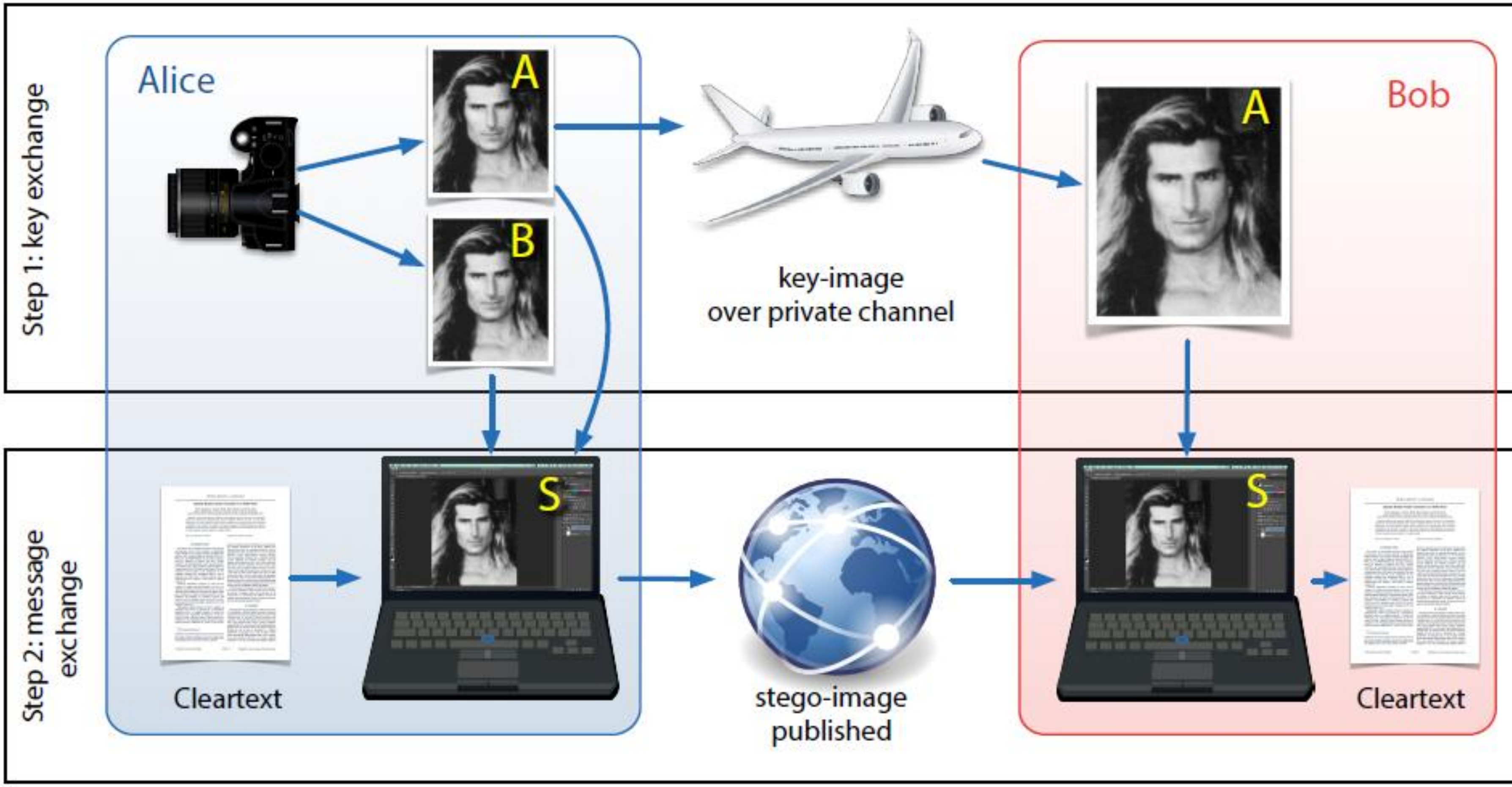
- Protocol: *given* Text T, create a new picture S as follows:

$$S_i := \begin{cases} K_i, & \text{if} \quad T_i = 0 \\ C_i, & \text{if} \quad T_i = 1 \end{cases} \qquad T_i := \begin{cases} 0, & \text{if} \quad S_i = K_i \\ 1, & \text{if} \quad S_i \neq K_i. \end{cases}$$

- S cannot be distinguished from any real photograph

UNIVERSITÉ DE GENÈVE

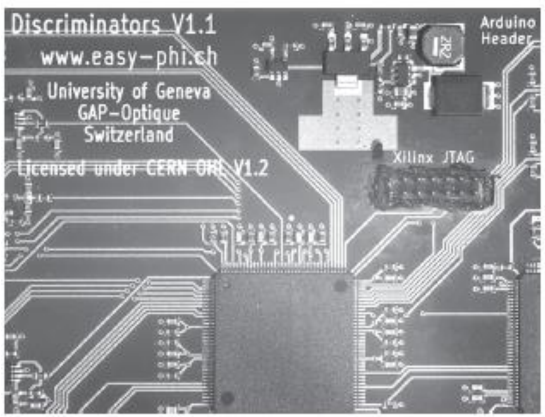
Private key steganography



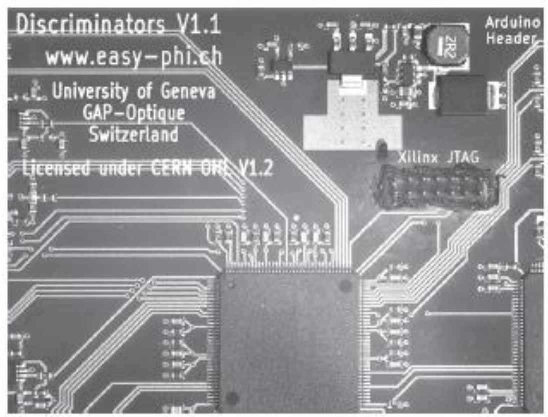
Experimental realisation

- Tests with scientific mono-chrome and consumer colour cameras with raw image files
- 8 Mpix 16 bit tiff files

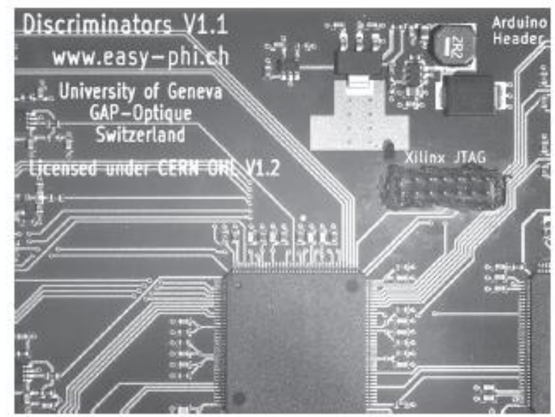
Key-image $\mathcal{A}$



Auxiliary image B



Stego-image $\mathcal{S}$

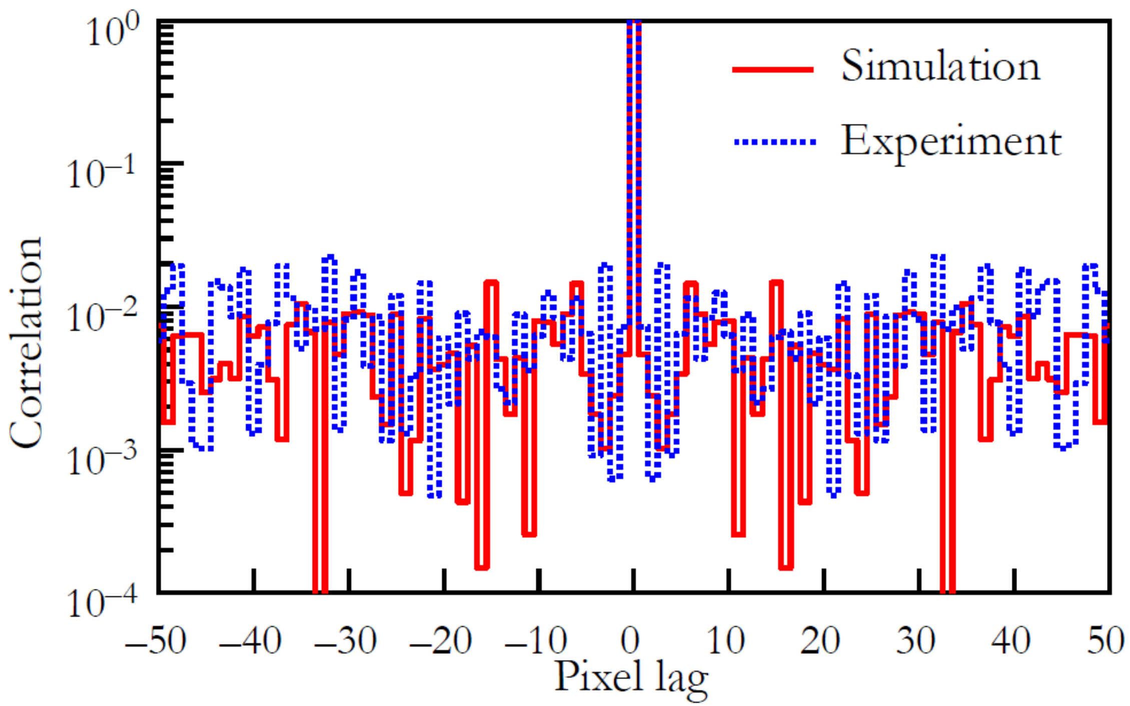


- error-correction applied (Reed-Solomon code)

UNIVERSITÉ DE GENÈVE

Results

- It works!
  - no cross-pixel correlations
  - stability depends on experimental situation
  - …stigations
  - …bits can be



Merci!

- PhD positions available!

UNIVERSITÉ DE GENÈVE