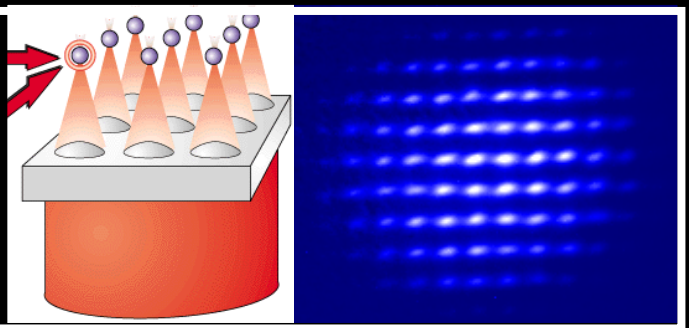
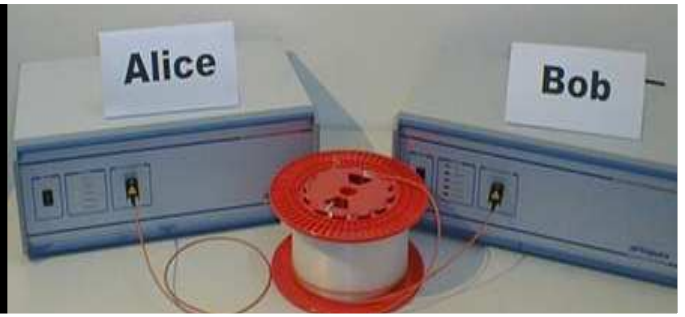
COMPUTACIÓ QUÀNTICA
PRADA DE CONFLENT, 22 I 24 D'AGOST DE 2010

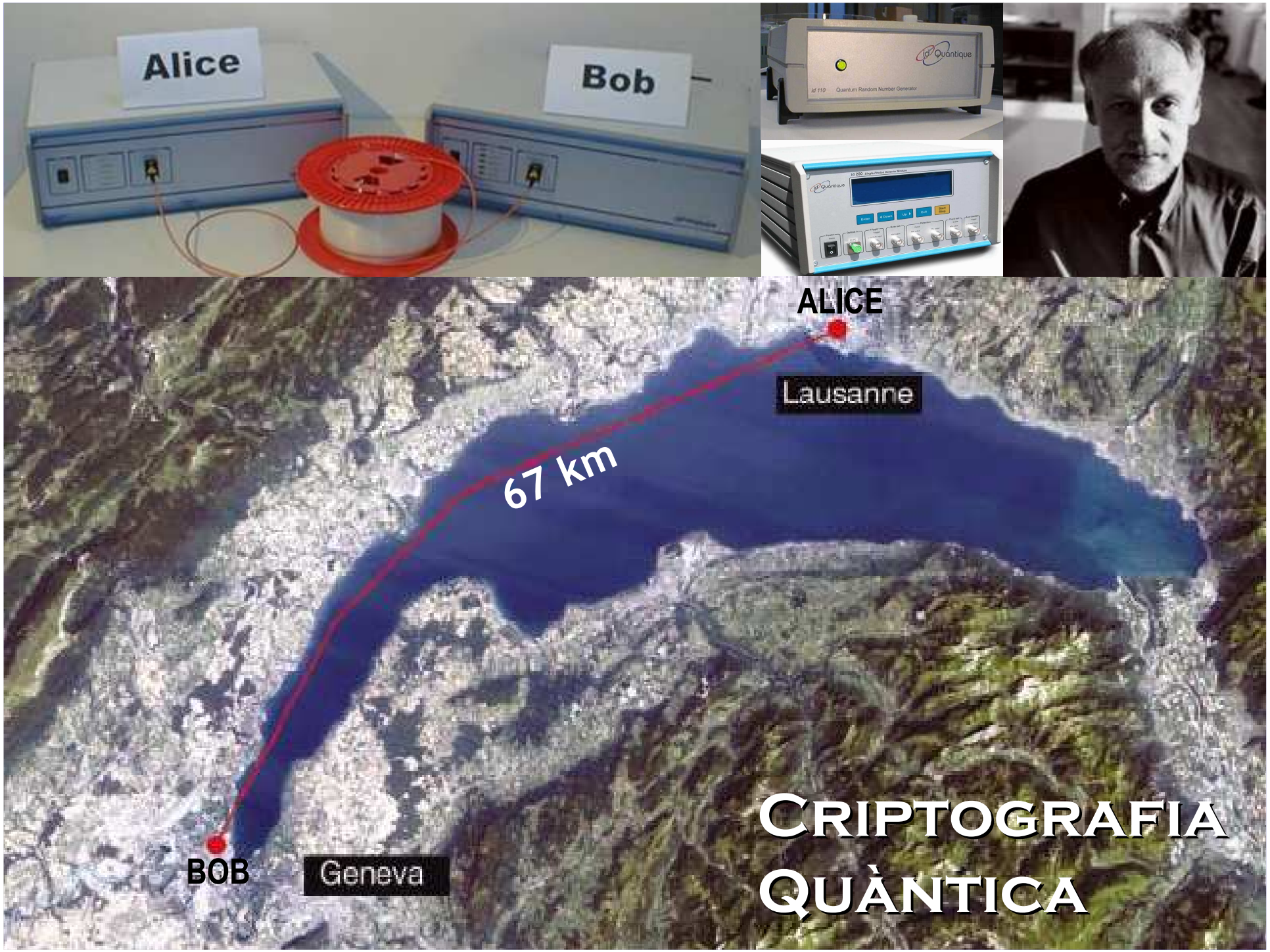
1 MOTIVACIÓ

2 COMPUTACIÓ QUÀNTICA



3 CRIPTOGRAFIA QUÀNTICA




Alice
Bob
id Quantique
Quantum Random Number Generator
ALICE
Lausanne
67 km
BOB
Geneva
Criptografia
Quàntica

INDEX

3.1 Introducció i Motivació

Informació Quàntica

Comunicació: enviar informació entre dues persones/màquines distants (ALICE és l'emissor i BOB és el receptor)

Computació: processat de la informació (simulacions, portes lògiques, algorismes,...)

Quàntic/clàssic: les regles del joc canvien (amplituds de probabilitat, col·lapse de la funció d'ona, superposició, interferències, estats entortolligats,...)

- Informació Quàntica
  - Comunicació Quàntica → Fotons ("flying qubits")
  - Computació Quàntica
    - Partícules atrapades:
      - àtoms,
      - ions,
      - electrons,
      - molècules,
      - quantum dots...

Fotons ("flying qubits")
- viatjen a c = 300 000 km/s en el buit
- no interaccionen entre sí directament
- la polarització és el qubit "ideal"

Comunicació Quàntica
- Criptografia Quàntica
- Teleportació
- Codificació densa

CRIPTOGRAFIA

Criptografia és l'art consistent en codificar missatges de tal forma que només la persona a qui s'adreça el missatge es capaç de llegir-lo.

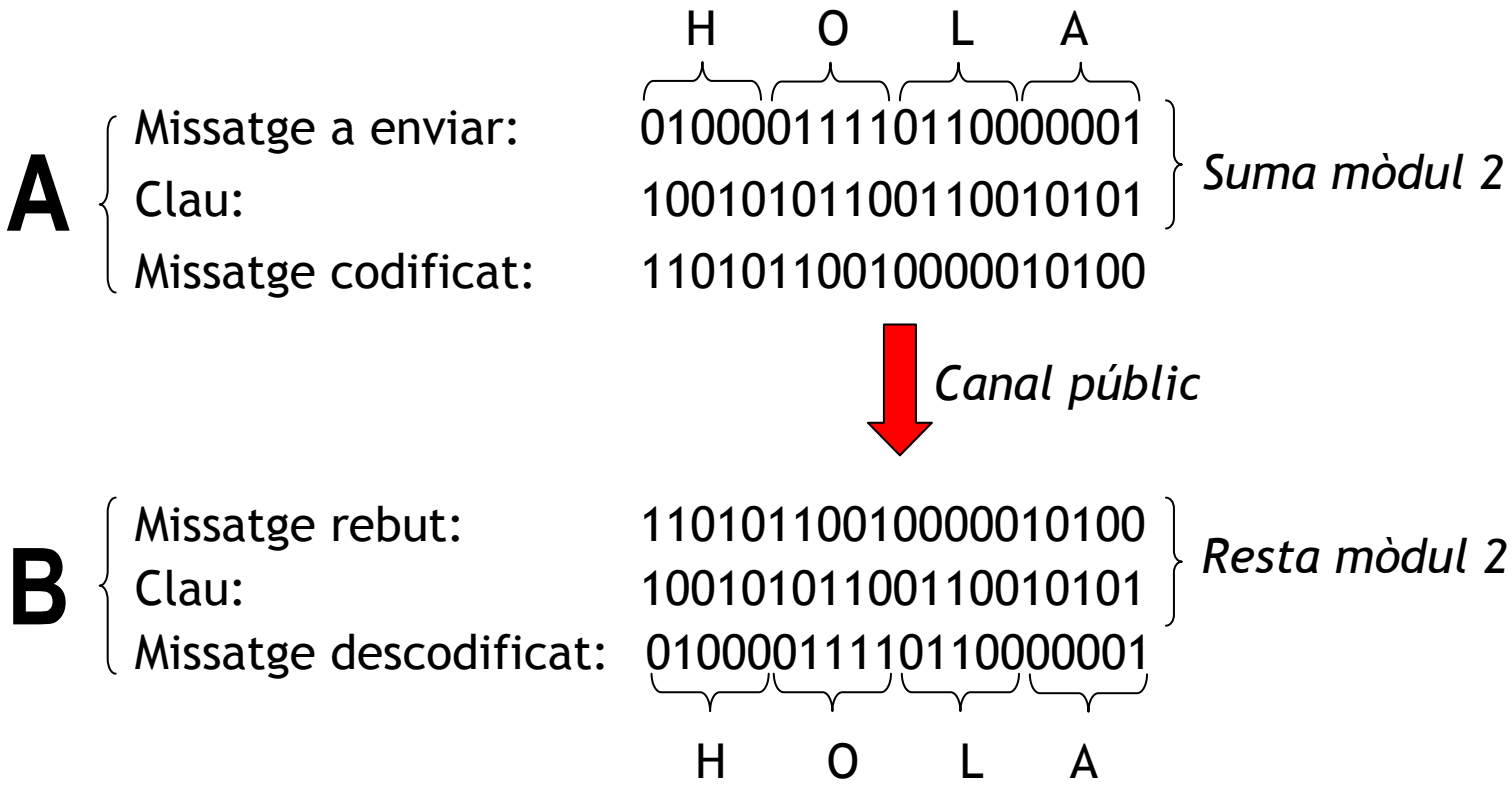
- *Criptografia de clau privada*
  Només l'emissor i el receptor coneixen la clau que permet encriptar la informació. El missatge es públic.

- *Criptografia de clau pública (RSA, PGP, FNMT,...)*
  Tant la clau com el missatge són públics.
  La clau es inutilitzable per aquells que no l'han generada.

Mètode d'encriptació ONE-TIME-PAD (cifrat de Vernam)

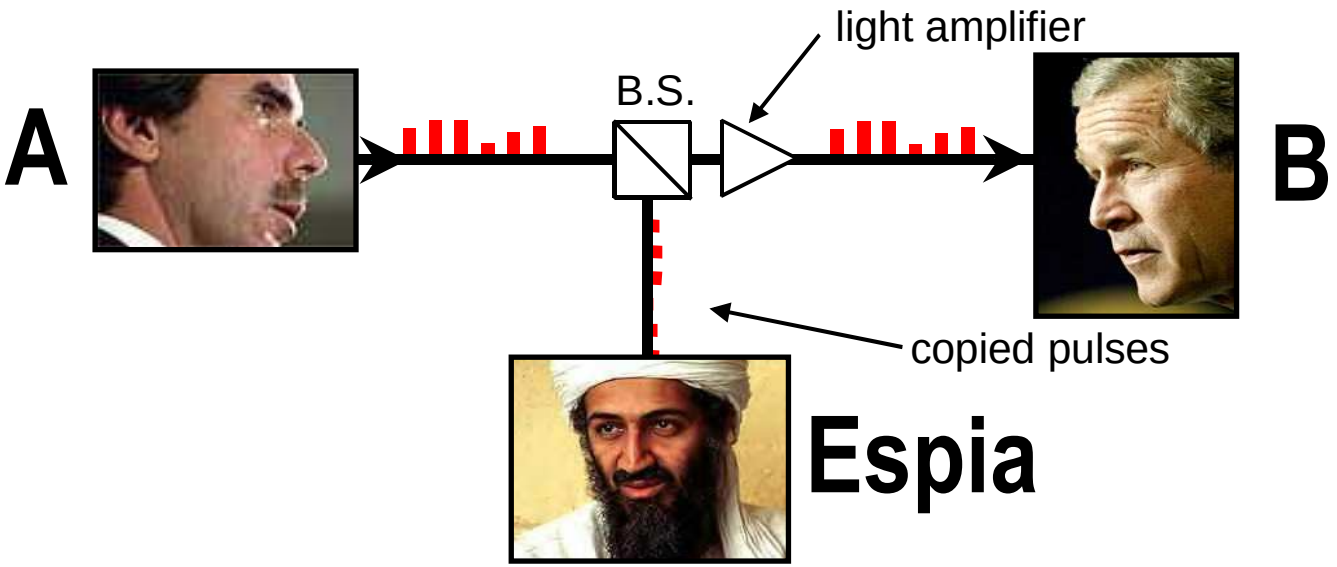
El missatge es codifica mitjançant una clau que només coneixen l'emissor A i el receptor B. La clau es un conjunt de números aleatoris.

EXEMPLE: Lletres = 5 digits binaris entre 1 i 26
[A=00001; B=00010; C=00011; ...; Z=11010]



El mètode ONE-TIME-PAD és, en principi, segur:
No hi ha estructures en el missatge encriptat que un criptoanalista pugui reconèixer ja que la clau es RANDOM i ÚNICA per a cada missatge.

Problema: l'emissor i el receptor han d'intercanviar-se una clau privada cada vegada sense que l'espia la detecti



- *Per a que el mètode sigui segur cal saber si l'ESPIA està actuant.*
- *Si sabem que l'ESPIA ha obtingut una certa clau, aquesta la descartem, en generem una altra, i ens la intercanviem.*
- *La MECÀNICA QUÀNTICA ens facilita eines per saber amb total seguretat si l'ESPIA ha obtingut la clau privada.*

Lectura complementària: EL CIFRAT DE VERNAM

(de http://www.pro-technix.com/information/crypto/pages/vernam_base.html)

There is only one perfectly secure cryptosystem known

Of all the methods of encryption ever devised, only one has been mathematically proved to be completely secure. It is called the Vernam cipher or one-time pad. The worth of all other ciphers is based on computational security. If a cipher is computationally secure this means the probability of cracking the encryption key using current computational technology and algorithms within a reasonable time is supposedly extremely small, yet not impossible. In theory, every cryptographic algorithm except for the Vernam cipher can be broken given enough ciphertext and time.
For example the public key cryptosystems such as PGP and RSA are based on the following :
Calculate an integer N such that it has only two prime number factors f1 and f2. This triad of integers forms the basis of the encryption and decryption keys used in PK cryptosystems. The security of these systems is simply based on the computational difficulty of calculating f2 and f1 from N if N is a very large integer. To break this cipher N must be factored, and at the time these systems were devised the best publicly available factoring algorithms would take millions of years to factor a 200 digit number. This does not logically exclude the possibility of a new factoring algorithm being discovered, or the existence of a secret factoring algorithm, or the invention of technology capable of running current factoring algorithms at high speed.

The Vernam cipher or one-time pad.

Cryptology is such a complex specialist subject that there seems no choice but to place your trust in a few individuals with sufficient knowledge to grasp the underlying principles of supposedly secure cryptosystems. However understanding the operation of the Vernam cipher is not demanding. Its perfect security is intuitively obvious.

Using the Vernam cipher

In 1917 during the First World War the American scientist Gilbert Vernam was given the task of inventing an encryption method the Germans could not break by AT&T. What was devised was the only provably unbreakable encryption scheme known to this day. Compared with most cryptosystems it is a very simple. To use a one-time pad, you need 2 copies of the "pad" (also known as the key) which is a block of truly random data at least as long as the message you wish to encode. If the data on the pad is not truly random, the security of the pad is compromised.One-time pads are used in pairs. The more copies of a given pad, the greater the likelihood is that one may be captured, in which case the system is completely broken. One copy of the pad is kept by each user, and pads must be exchanged via a secure channel (e.g. face to face on floppy disks). Pads must only be used once. The fastest method of encrypting a message with a one-time pad is with a computer. If you do choose this method keep the pad on a floppy disk and destroy it completely once used. 'Deleted' data can be easily reconstructed from disks, so never store pads on your hard drive or keep the floppy. The message recipient should apply the same precautions. Never use a networked computer for implementing the encryption because of possible eavesdropping.

Why 'one-time' pad?

A pad should never be reused. As long as the pads are unique and never reused no statistical analysis or pattern matching techniques can be applied by cryptanalysts. The fact that the pad can be used only once is the "one time" point of this cipher.
Soviet intelligence once reused one-time pads years after they had originally been distributed to field agents in Britain. The British intelligence service noticed some patterns in coded messages and began searching for comparisons through a complete archive of all encrypted communications intercepts. Over a period of years, various secret communications were compromised. This operation took place under the code word VERONA. The NSA has recently declassified parts of the story and put information about VENONA on the Web

3.2 CRIPTOGRAFIA QUÀNTICA

- Criptografia quàntica
  - Protocol [BB84] (En el procés quàntic de la mesura)
    C. H. Bennet and G. Brassard,
    Proc. Internat. Conf. Computer Systems and Signal Processing,
    Bangalore pp. 175 (1984)
  - Protocol [Ekert91] (En fotons entrellaçats)
    A. Ekert, Phys. Rev. Lett., ***67****, 661 (1991)*
  - Protocol [SARG04] (En el procés quàntic de la mesura)
    Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin
    Phys. Rev. Lett. ***92****, 057901 (2004)*

- Protocol [BB84]

  Volem intercanviar una clau privada (PKD) sense que ningú la intercepti

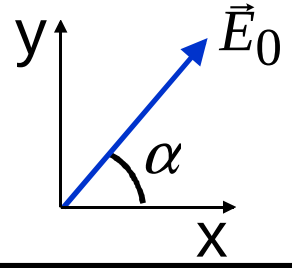
  El protocol BB84 no impedeix que un ESPIA intercepti la clau privada però si permet a ALICE i BOB saber si l' ESPIA l' ha interceptada

  Es fonamenta en el procés quàntic de la mesura en partícules individuals

- La mesura quàntica

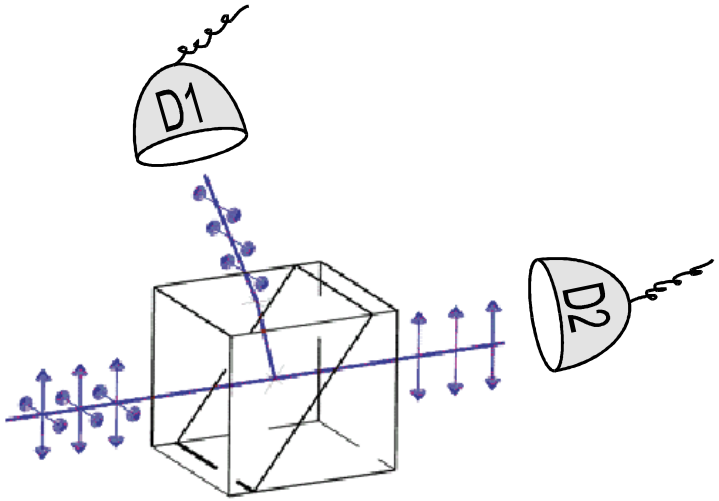
  Estat quàntic: la polarització d'un fotó

$$\vec{E} = E_0(\cos\alpha\,\vec{i} + \sin\alpha\,\vec{j})e^{i(\omega t - kz + \varphi)}$$



3.3 El Protocol BB84

Aparell de mesura: Polarization Beam Splitter (e.g. cristall de calcita)



Probabilitats de detecció

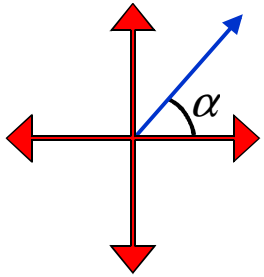
en D1: $P_x = \cos^2 \alpha$

en D2: $P_y = \sin^2 \alpha$

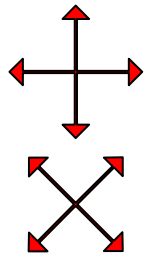
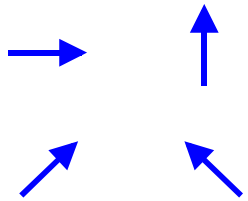
Estat després del PBS

Les mesures perturben l'estat quàntic de les partícules

Procés de mesura

Base	Probabilitats	Estat després de la mesura
	$P_x = \cos^2 \alpha$ $P_y = \sin^2 \alpha$	

Codificació binària

Base	0	1
		

Conjunt de passos del protocol BB84 (sense imperfeccions experimentals)

1. ALICE prepara una cadena aleatòria de bits i els codifica en l'estat de polarització dels fotons escollint de manera aleatòria entre les dues bases  i  . A continuació envia els fotons a BOB.

2. BOB rep els fotons i analitza la seva polarització utilitzant de manera aleatòria, les bases  i  .

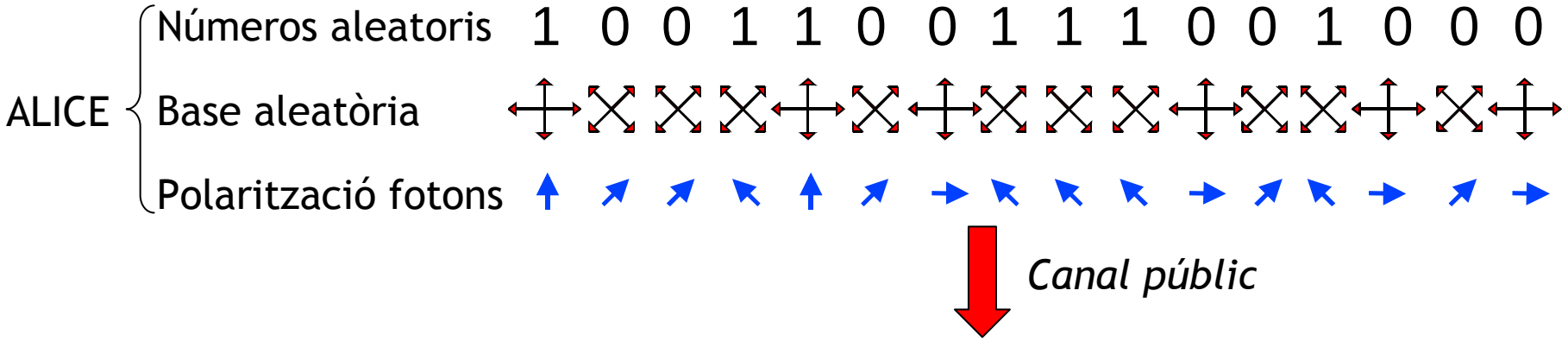
3. BOB comunica les bases que ha utilitzat a ALICE per un canal públic. ALICE identifica el subconjunt de bits en que tots dos han utilitzat la mateixa base i li ho comunica públicament a BOB. ALICE i BOB eliminen el subconjunt de dades en que no utilitzaven les mateixes bases (*basis reconcilliation*). El conjunt de dades que resten constitueix la clau esporgada (*sifted key*)

4. BOB envia, mitjançant un canal públic, una fracció de les dades de la clau esporgada a ALICE per a que comprovi la correlació entre les seves dades i les de BOB.

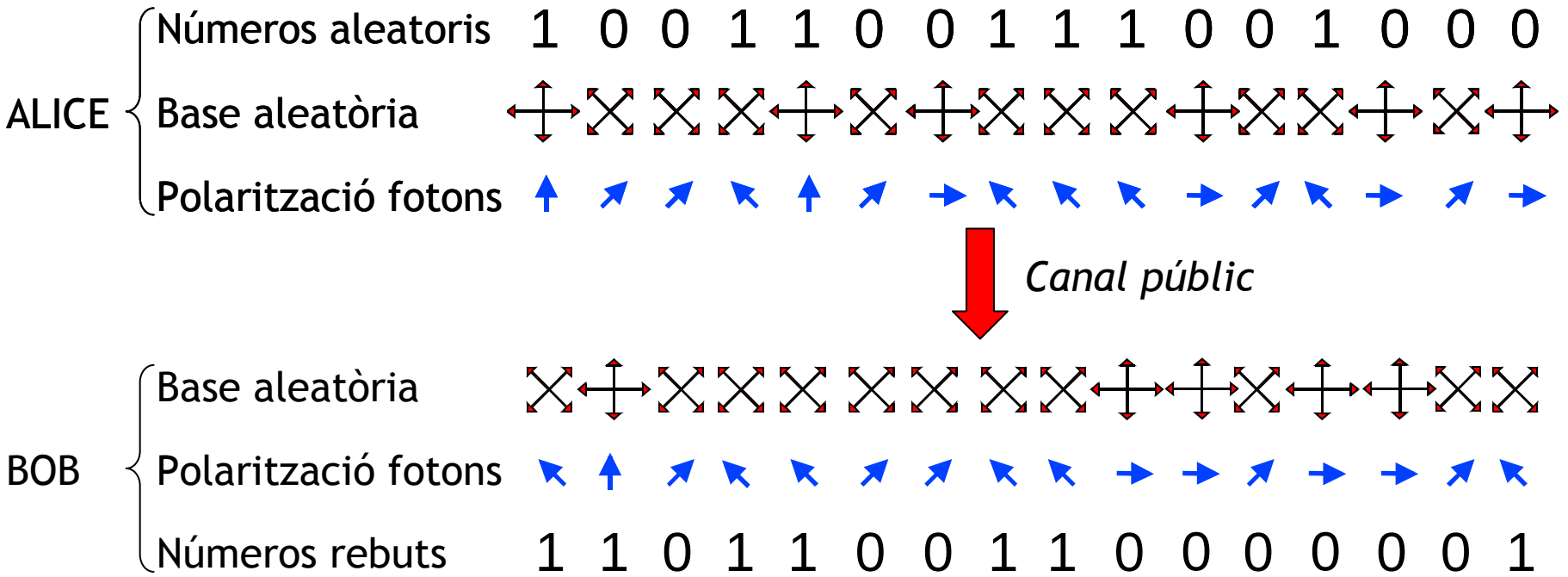
5. ALICE analitza la taxa d'error (QBER), és a dir, els errors en la correlació de resultats entre ALICE i BOB per deduir si l'EVE ha estat actuant.

Exemple

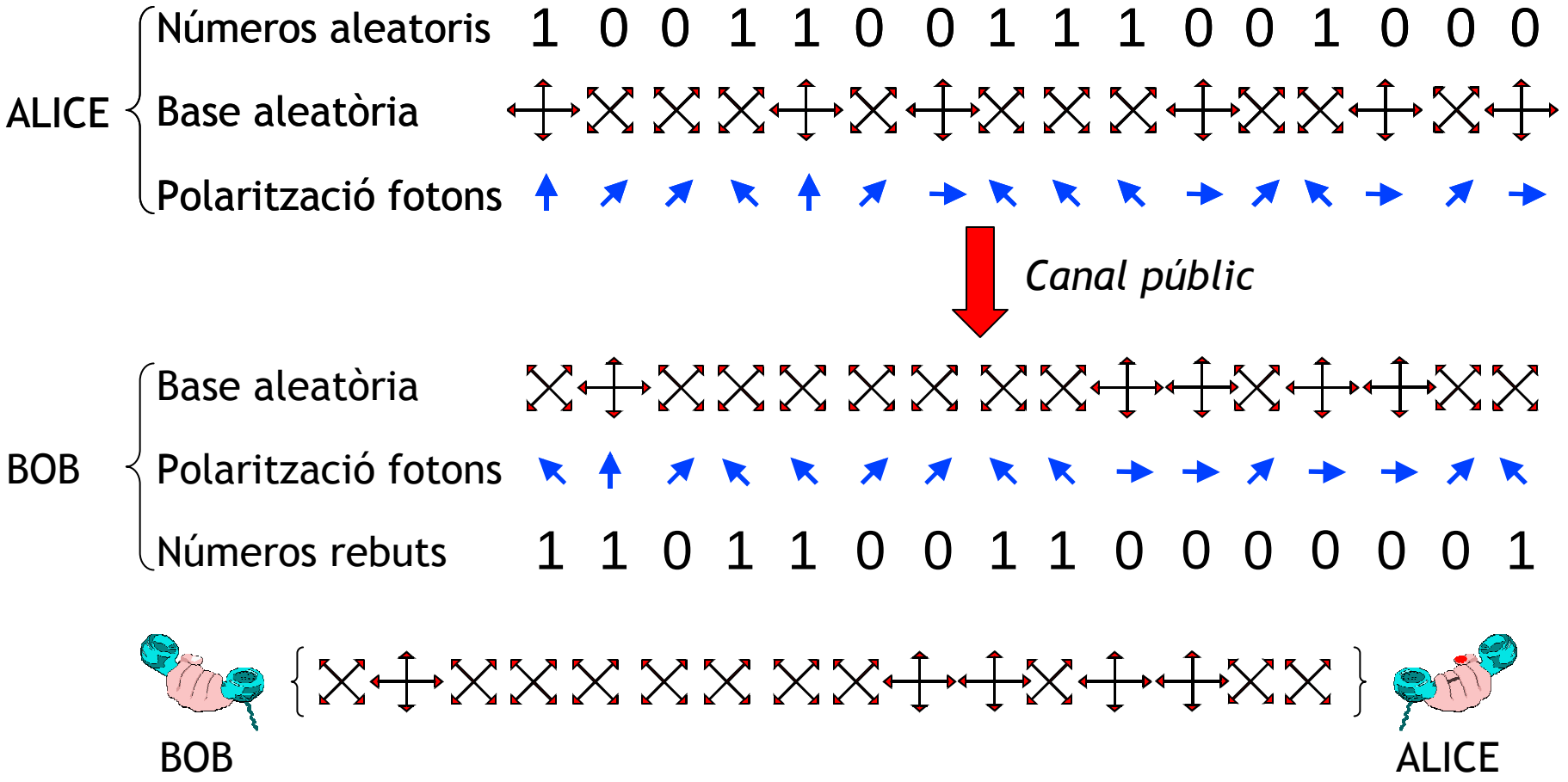
1 ALICE prepara una cadena aleatòria de bits i els codifica en l'estat de polarització dels fotons escollint de manera aleatòria entre les dues bases + i × . A continuació envia els fotons a BOB.



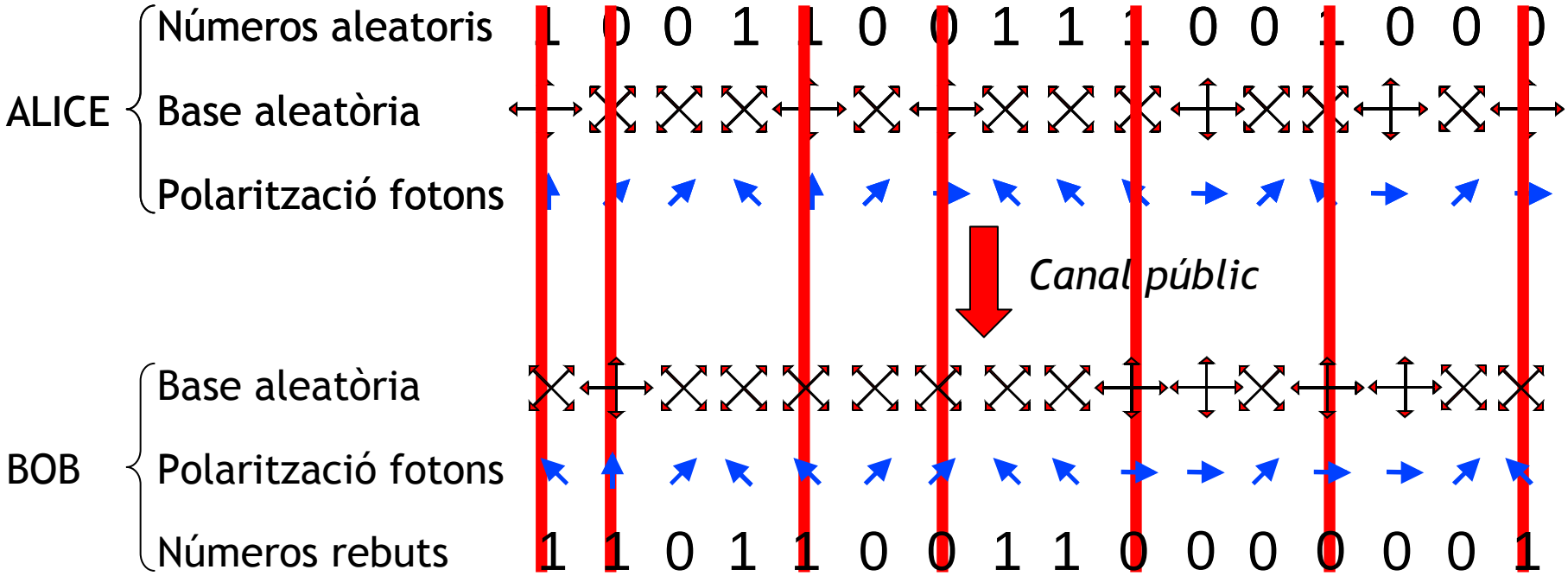
2 BOB rep els fotons i analitza la seva polarització utilitzant de manera aleatòria, les bases + i × .



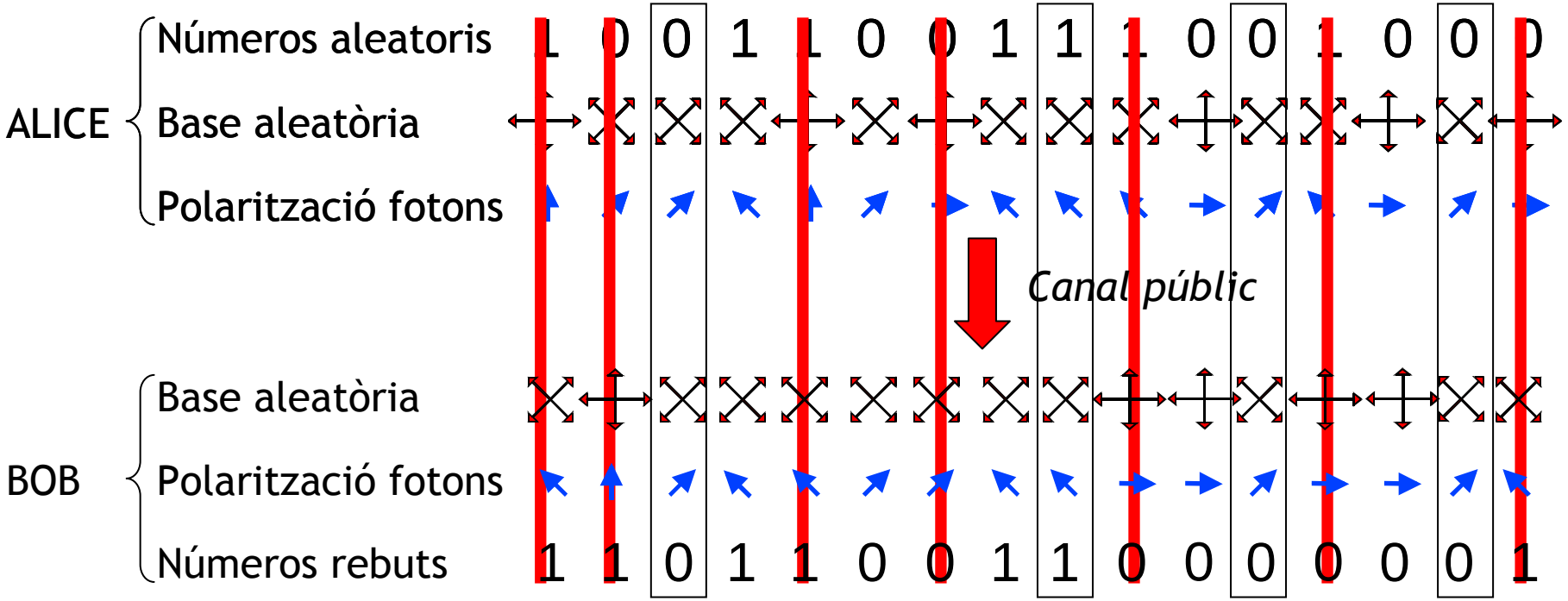
3 BOB comunica les bases que ha utilitzat a ALICE per un canal públic. ALICE identifica el subconjunt de bits en que tots dos han utilitzat la mateixa base i li ho comunica públicament a BOB...

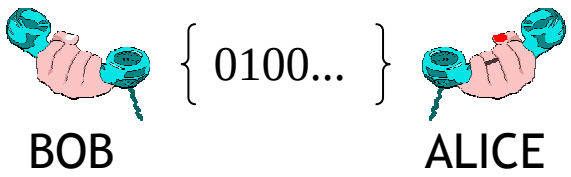


3 ... ALICE i BOB eliminen el subconjunt de dades en que no utilitzaven les mateixes bases (*basis reconcilliation*). El conjunt de dades que resten constitueix la clau esporgada (*sifted key*)



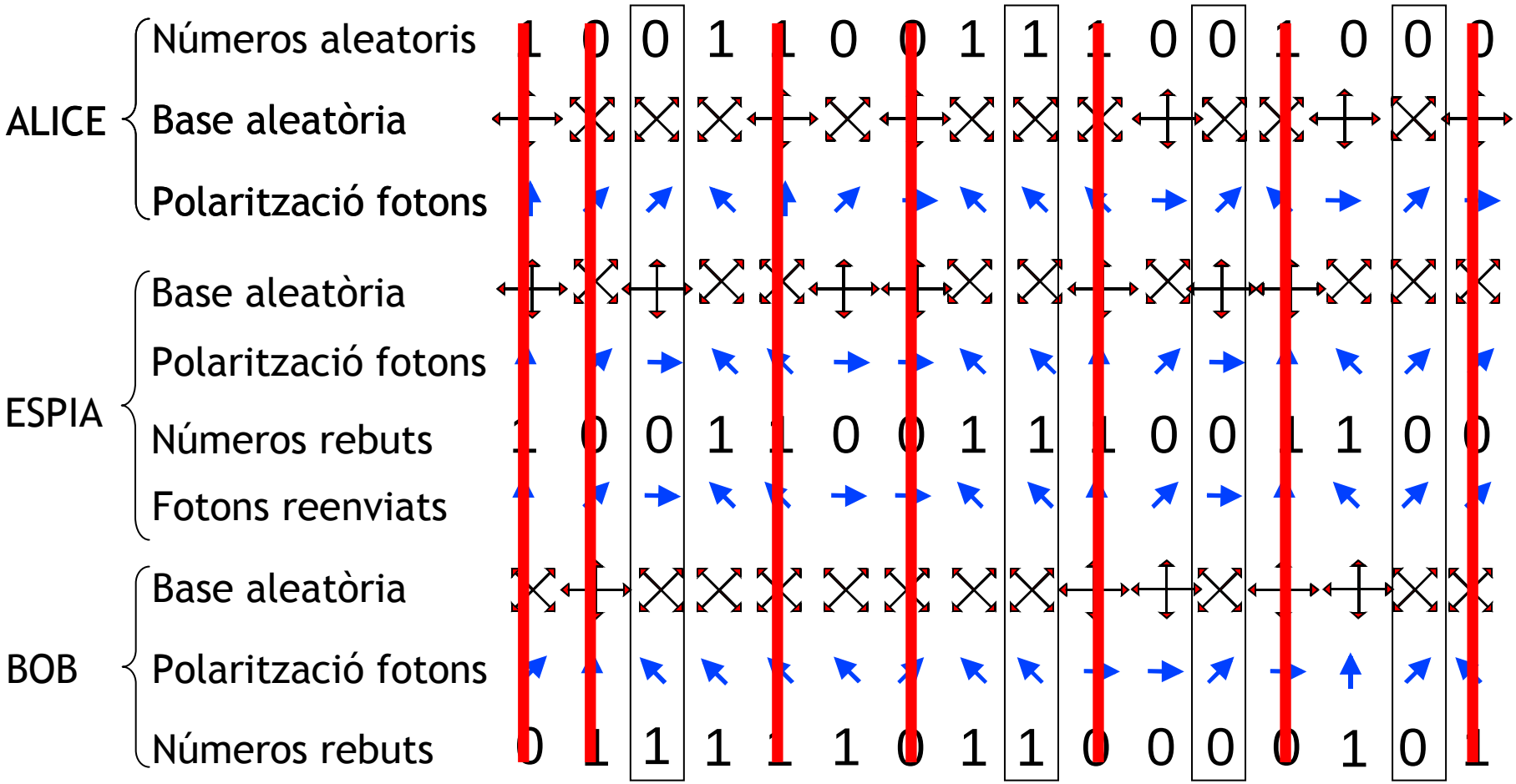
4 BOB envia, mitjançant un canal públic, una fracció de les dades de la clau esporgada a ALICE per a que comprovi la correlació entre les seves dades i les de BOB.





ESPIA ABSENT = CORRELACIO PERFECTA

5 ALICE analitza la taxa d'error (QBER), és a dir, els errors en la correlació de resultats entre ALICE i BOB per deduir si l'EVE ha estat actuant.



EVE (L'ESPIA)

La informació que EVE té la pot haver aconseguit mitjançant diverses estratègies.
En destaquem dues:

Interceptar i reenviar un fotó

EVE intercepta un fotó, mesura el seu estat de polarització, i reenvia un fotó amb l'estat de polarització que ha obtingut en la mesura. Aquesta estratègia s'anomena intercept-and-resend i, tal com ha estat discutit anteriorment, en un 25% dels casos produeix un error en la correlació.

Extracció de fotons

Si els polsos de llum contenen més d'un fotó, EVE pot extreure'n una part del pols (*photon number splitting*, PNS) sense pertorbar la resta del pols. Analitzant l'estat de polarització dels fotons que extreu pot obtenir informació de la clau sense introduir errors de correlació. Es tractarà doncs d'utilitzar fonts de fotons individuals, o de minimitzar la possibilitat que un pols de llum contingui dos o més fotons. Tot i que aquesta estratègia no afecta al QBER si que donarà lloc a una major atenuació dels polsos.

QUÈ CAL FER ABANS D'UTILITZAR LA CLAU

- Avaluar el QBER (Quantum Bit Error Rate):

  Típicament QBER $\leq$ 11%

- Aplicar un protocol clàssic de correcció d'errors:

  EXEMPLE:

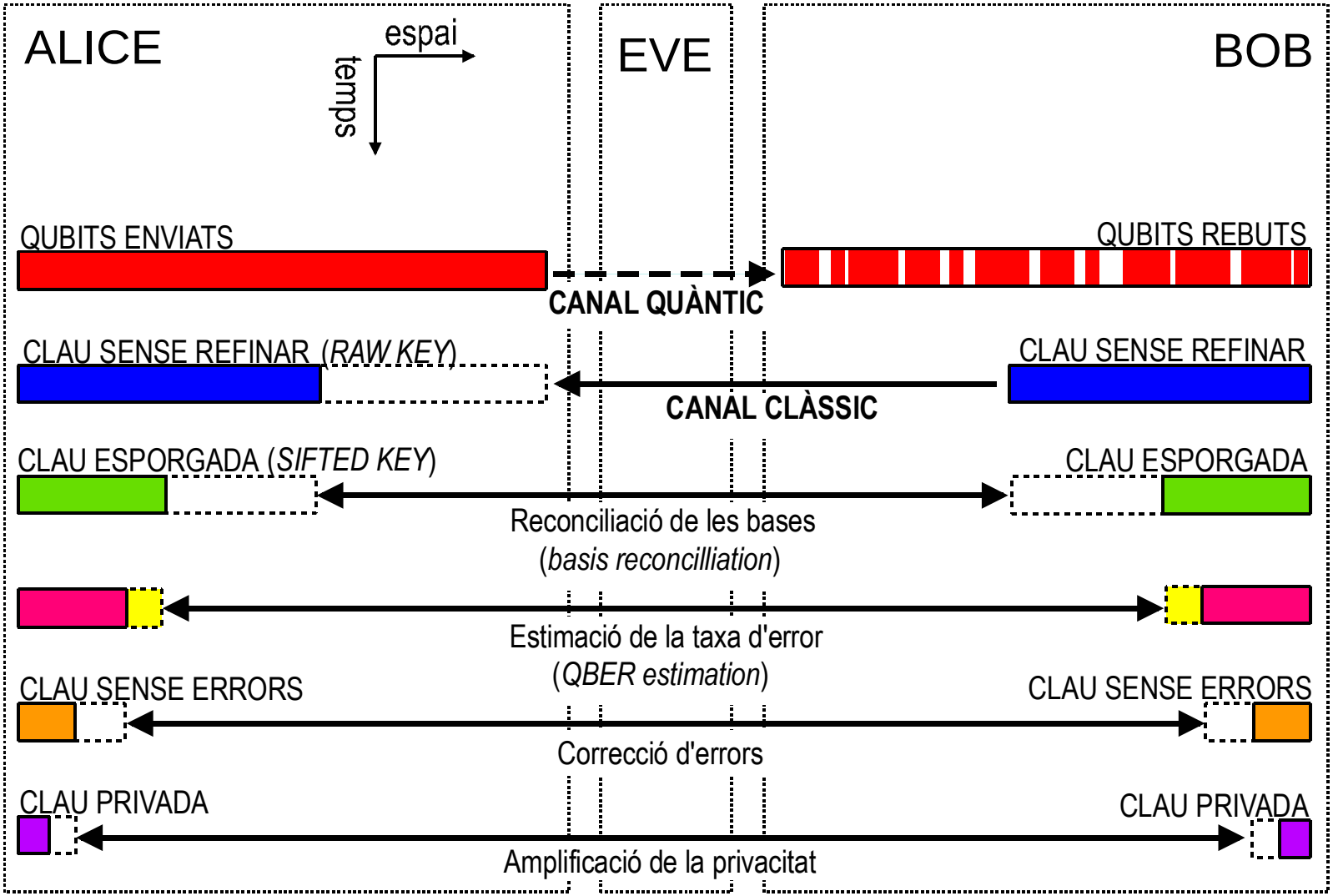
  - ALICE i BOB comparen la suma de dos bits: $b_k + b_m$
  - Si obtenen el mateix resultat, aleshores eliminen b_k i es queden amb b_m
  - Si obtenen resultats diferents eliminen tots dos bits

- Aplicar un protocol d'amplificació de la privacitat:

  EXEMPLE:

  - ALICE i BOB fan la següent substitució: $b_k + b_m \rightarrow b_k$

DESTIL·LACIÓ DE LA CLAU



3.4 Implementació del Protocol BB84

Quin és l' "State of the Art"?

http://www.idquantique.com

http://www.magiqtech.com

Quantum key distribution over 67 km with a plug&play system
D Stucki, N Gisin, O Guinnard, G Ribordy, and H Zbinden
New Journal of Physics ***4****, 41.1-41.8 (2002)*

Figure 3. Satellite view of Lake Geneva with the bnɑ Lausanne.

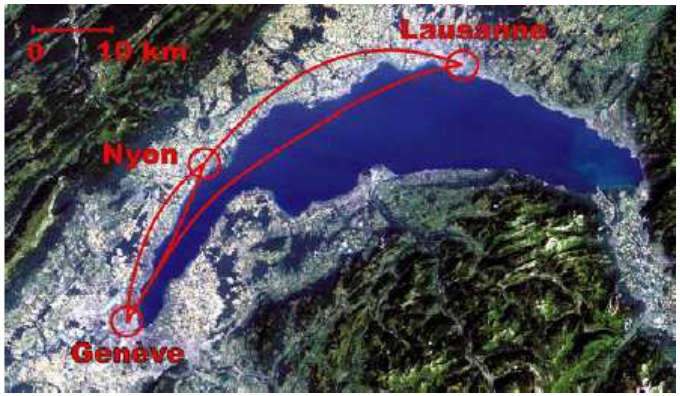


Table 2. Overview of exchanged keys over different fibres ($\mu = 0.2$).

Fibre	Length (km)	Key (kbit)	*QBER* (%)
Geneva–Nyon (under lake)	22.0	27.9	2.0 ± 0.1
Geneva–Nyon (terrestrial)	22.6	27.5	2.1 ± 0.1
Nyon–Lausanne (terrestrial)	37.8	25.1	3.9 ± 0.2
Geneva–Lausanne (under lake) A	67.1	12.9	6.1 ± 0.4
Geneva–Lausanne (under lake) B	67.1	12.9	5.6 ± 0.3
Ste Croix (aerial) A	8.7	63.8	3.0 ± 0.1
Ste Croix (aerial) B	23.7	117.6	3.0 ± 0.1

Quin és l' "State of the Art" (a principis de 2010)?

http://en.wikipedia.org/wiki/Quantum_cryptography

The highest bit rate system currently demonstrated exchanges secure keys at 1 Mbit/s (over 20 km of optical fibre) and 10 kbit/s (over 100 km of fibre), achieved by a collaboration between the University of Cambridge and Toshiba using the BB84 protocol with decoy pulses[4].

As of March 2007 the longest distance over which quantum key distribution has been demonstrated using optic fibre is 148.7 km, achieved by Los Alamos/NIST using the BB84 protocol[5]. Significantly, this distance is long enough for almost all the spans found in today's fibre networks. The distance record for free space QKD is 144 km between two of the Canary Islands, achieved by a European collaboration using entangled photons (the Ekert scheme) in 2006[6], and using BB84 enhanced with decoy states[7] in 2007 [8]. The experiments suggest transmission to satellites is possible, due to the lower atmospheric density at higher altitudes. For example although the minimum distance from the International Space Station to the ESA Space Debris Telescope is about 400 km, the atmospheric thickness is about an order of magnitude less than in the European experiment, thus yielding less attenuation compared to this experiment.

The DARPA Quantum Network[9], a 10-node quantum cryptography network, has been running since 2004 in Massachusetts, USA. It is being developed by BBN Technologies, Harvard University, Boston University and QinetiQ.

Quantum encryption technology provided by the Swiss company Id Quantique was used in the Swiss canton (state) of Geneva to transmit ballot results to the capitol in the national election occurring on Oct. 21, 2007.[10]

In 2004, the world's first bank transfer using quantum cryptography was carried in Vienna, Austria. An important cheque, which needed absolute security, was transmitted from the Mayor of the city to an Austrian bank.[11]

The world's first computer network protected by quantum cryptography was implemented in October 2008, at a scientific conference in Vienna. The network used 200 km of standard fibre optic cable to interconnect six locations across Vienna and the town of St Poelten located 69 km to the west. The event was witnessed by Gilles Brassard and Anton Zeilinger. [10]

Qué es Necessita?

Què es necessita?

- Generació:
  - Generador de la clau aleatòria
  - Fonts de fotons individuals
- Propagació:
  - Fibres òptiques
  - Espai lliure
- Detecció:
  - Photomultiplier tubes
  - Single photon avalanche diodes (SPAD)

GENERADOR DE NÚMEROS ALEATORIS

Randomness and the Vernam cipher

True Randomness

The most critical feature of the Vernam cipher is the randomness of the pad sequence. An event sequence can be said to be truly random if it is impossible to predict the next event in the sequence even if the entire state of the generating process up to that point is known. Any deterministic process, such as running software on a computer, can never produce truly random numbers. The next event in a computer is completely predictable given the current machine/network/IO state. (This ignores the slight probability of a high energy subatomic particle passing through your CPU or RAM chips and altering the state unpredictably)

Random data for the pad should never be generated purely by software. It must be gathered by hardware accessing processes of a truly non-deterministic nature. Radioactive decay and electron tunneling in electronic components are both non-deterministic phenomena produced by events occurring at the quantum subatomic level. By gathering and processing the output from Geiger counters or Zener diodes it is possible to obtain truly random data for the pad.

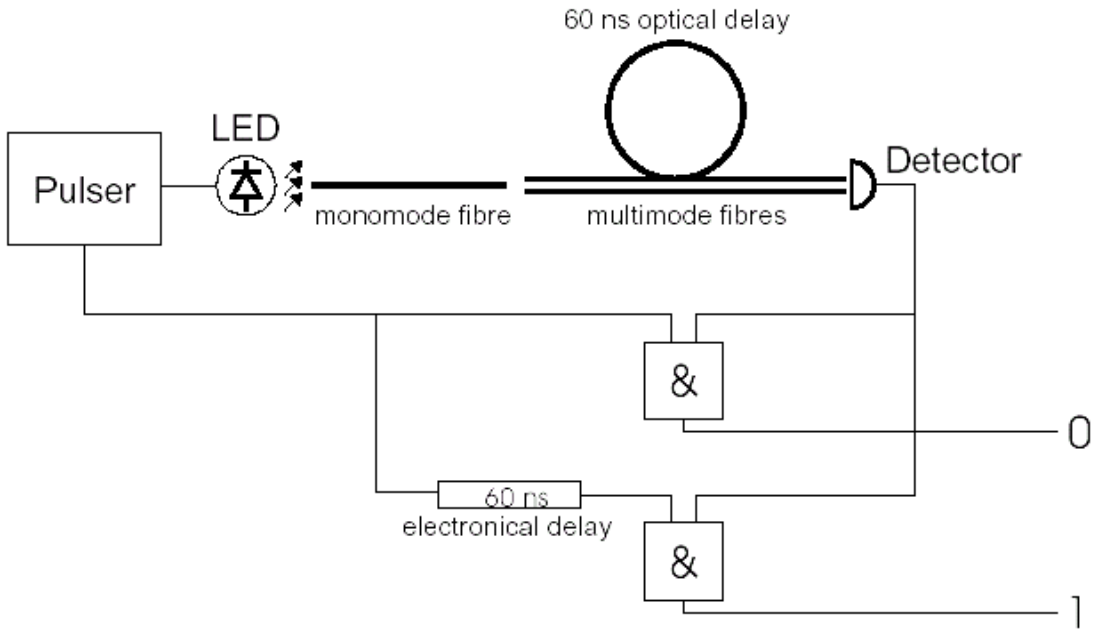
(de http://www.pro-technix.com/information/crypto/pages/vernam_base.html)

La mecànica quàntica és intrinsecament alateoria a través del procés de mesura i, en conseqüència, es pot utilizar per generar cadenes de números aleatoris

EXEMPLE:

El LED emet polsos dèbils (0.1 fotons) a 830 nm

El "generation rate" es, aproximadament, de 100kHz, corresponent a polsos de 0.1 fotons d'un LED que es (elèctricament) polsat al ritme de 1MHz.



http://www.idquantique.com/qrng.html

Fonts de fotons individuals: llum clàssica

Atenuació d'un feix làser (WCP: weak coherent pulse)

Per a que no hi hagi més d'un fotó en cada pols de llum es pren $\langle N \rangle = 0.1$
El 90% de les vegades no s'envia cap fotó.

El fet que, en certs moments, es puguin emetre, per exemple, dos fotons, està relacionat amb el fet que en les fonts de llum clàssiques hi ha molts possibles emissors.

Es per això que el número de fotons en la llum clàssica segueix una distribució de Poisson que permet que hi hagi "bunching" de fotons.

Fonts de fotons individuals: llum no clàssica

Cal tenir només un emissor.

Quan l'emissor ha emés un fotó, necessita un temps per a poder tornar a emetre un fotó. En conseqüència, no es poden generar dos fotons simultàniament. És a dir, tenim l'"antibunching" característic de la llum no clàssica.

EXEMPLES: { "quantum dots" individuals; centres de color; àtoms en "Cavity" QED } → "Photon guns"

FIBRES ÒPTIQUES

SUMITOMO ELECTRIC

http://www.sei.co.jp/sn/2002/06/06p4t.html

Z-PLUS Fiber™

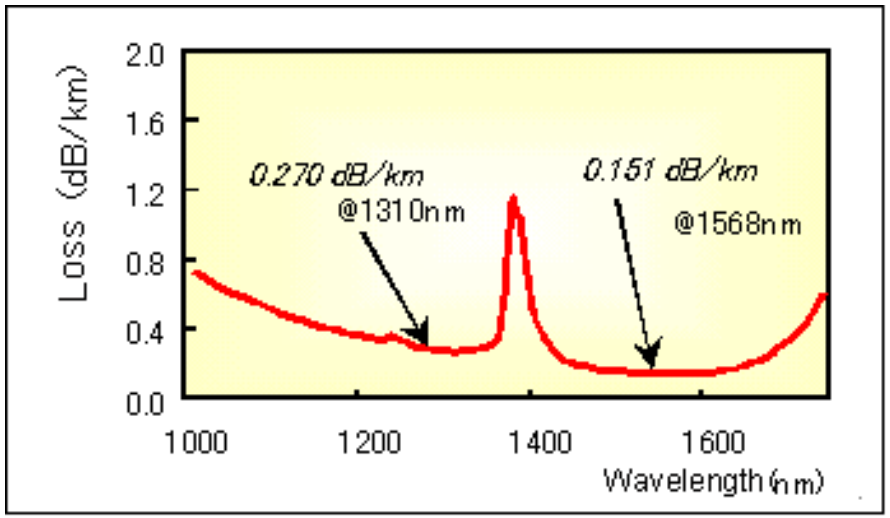


Figure 1. New world record for low optical fiber loss

Hi ha dues finestres de transmissió en les fibres òptiques: a 1310 nm i a 1568 nm

Les mínimes pèrdues valen 0.151 db/km

$$Loss\ (en\ dB) = 10\log_{10}\frac{I_{in} - I_{out}}{I_{in}} \Rightarrow 0.151\,db/km = 4\%/km$$

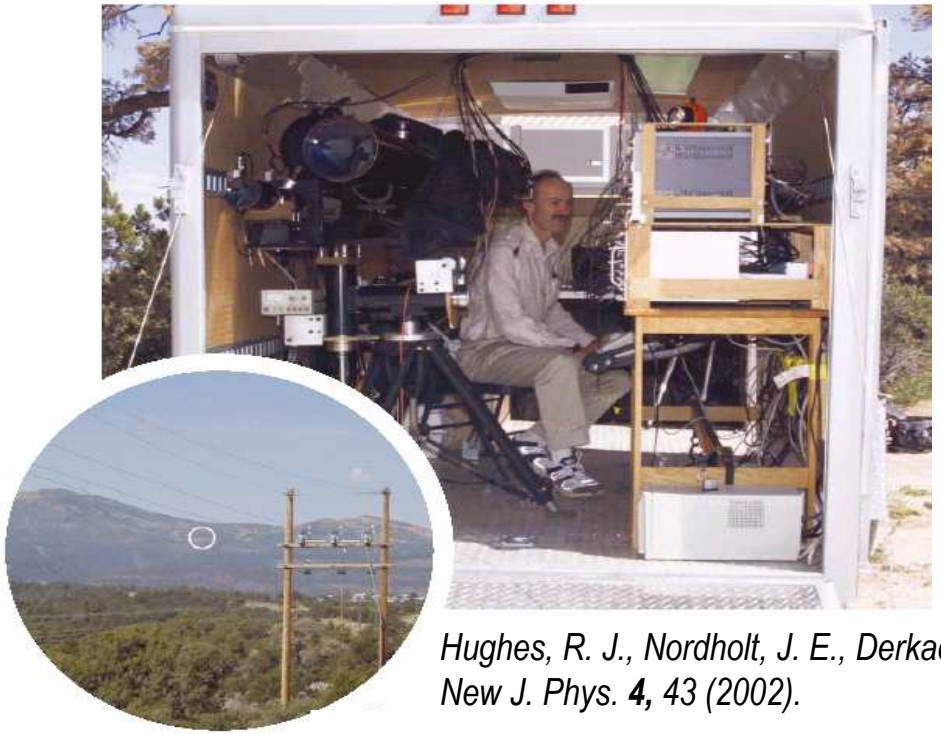
PROPAGACIÓ EN L'ESPAI LLIURE

⇒ Primera demostració de la criptografia quàntica
Bennettt, C.H. et al., Experimental quantum cryptography. J. Cryptol, ***5****, 3 (1992)*

- LED's a 550 nm
- 0.32 m

⇒ Actualment, s'assoleixen distàncies de 10 km (amb fotons amb freq. òptiques)

S'utilitzen telescopis per enviar i rebre els fotons.
Es necessiten per combatre el fenòmen de la difracció que es produeix a tant llargues distàncies



Hughes, R. J., Nordholt, J. E., Derkacs, D. & Peterson, C. G.
New J. Phys. ***4,*** *43 (2002).*

Problemes:

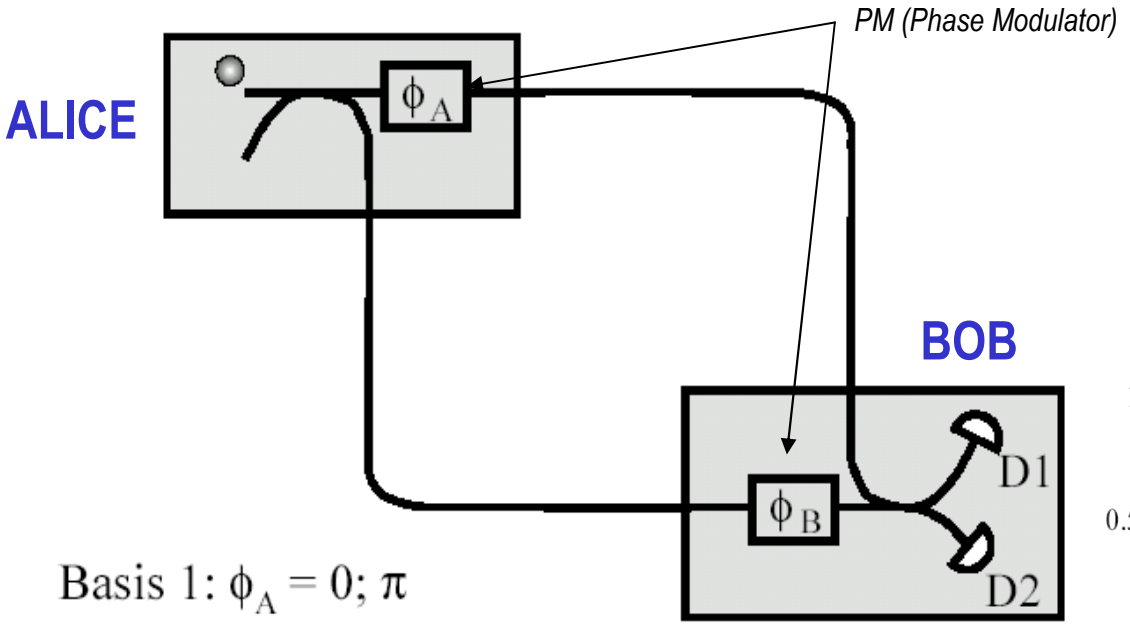
Turbulència atmosfèrica: produeix desviació i endarreriment o avançament del fotó. Aquest efecte es pot minimitzar enviant un pols de llum molt brillant per davant del fotó. Cal indicar però, que la turbulència es produeix majoritàriament al llarg dels dos primers km de l'atmosfera.

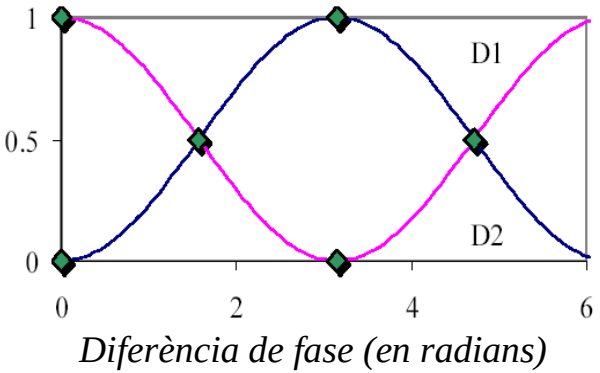
"Stray light": del Sol o de la Lluna. Es pot reduir mitjançant filtres i encenent els detectors només quan l'emissor envia el fotó.

CODIFICACIÓ EN LA FASE

- L'estat de polarització es manté en l'espai lliure.
  Malauradament, les fibres presenten: (i) depolarització; i (ii) birefringència
- En fibres òptiques es comú que s'utilitzi la codificació en la fase enlloc de fer-ho en la polarització

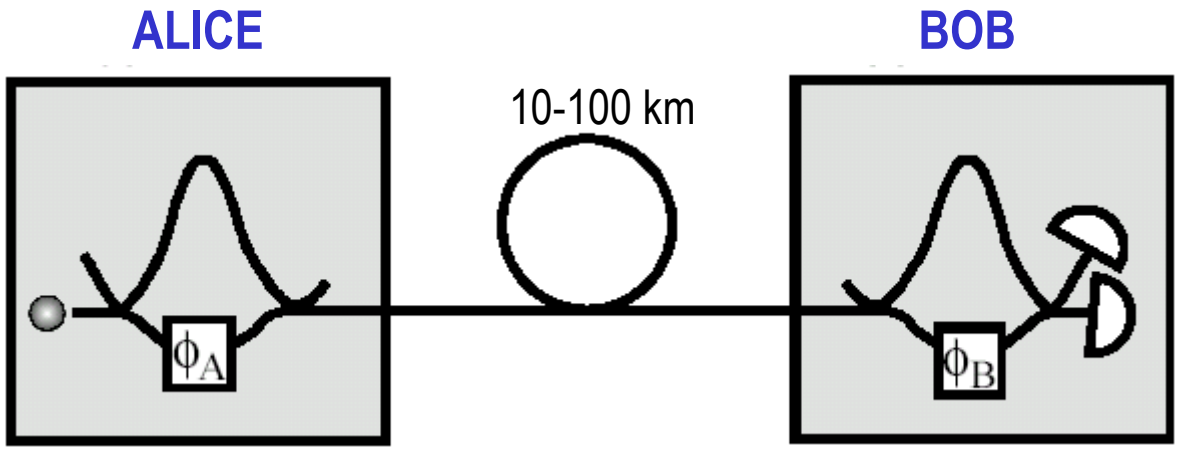
Interferòmetre Mach-Zehnder





⟹ Mantenir la diferència de fase distàncies de 10 km o més és molt difícil.

⟹ En realitat el que es fa es comprimir els interferometres

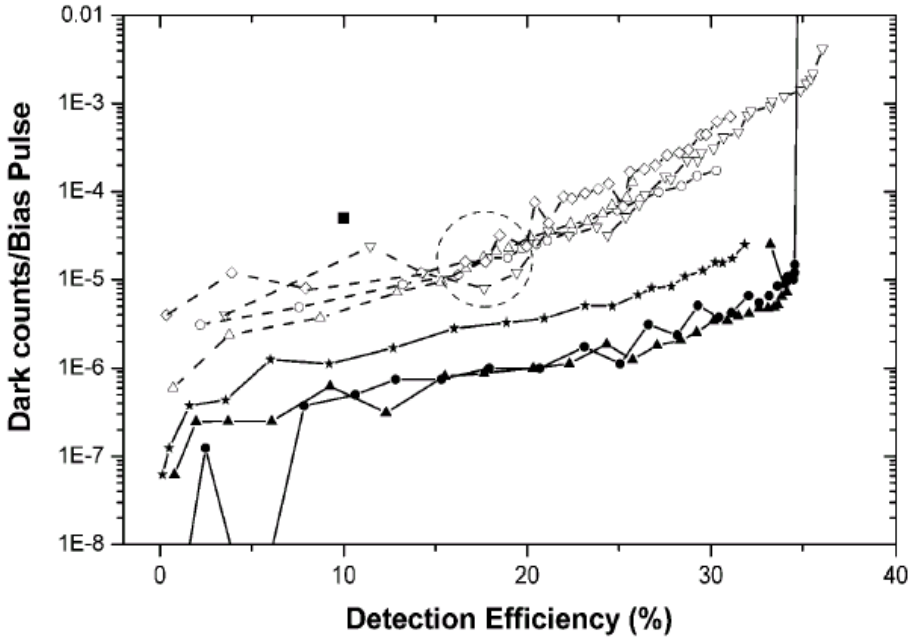


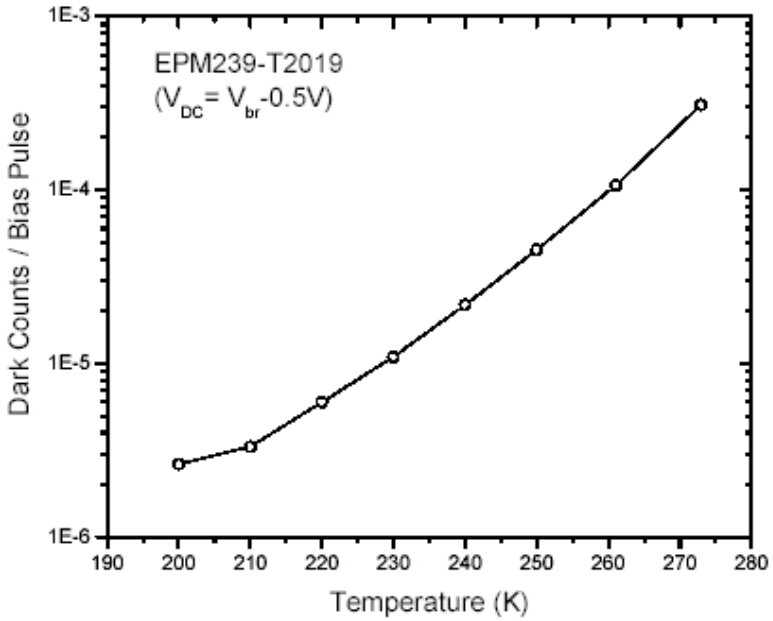
- Alice utilitza un MZ per generar dos pulsos de llum
- Els dos polsos de llum viatjen un darrera de l'altre al llarg de la fibra
- En els detectors de BOB hi arriben el seguents polsos:
  SS (short-short); LL (Long-Long); SL (Short-Long); i LS (Long-Short).
  Nomes interfereixen SL amb LS
- Alice i Bob utilizen els "Phase Modulators" per codificar la informació.
- Aquest métode es molt més estable però es perd la meitat del senyal en SS i LL.

SPD (SINGLE PHOTON DETECTORS)

SPD per a les longituds d'ona de telecomunicacions (1310 i 1568 nm)

APD (Avalanche Photo Diodes):
Un fotó excita un electró de la banda de valència a la banda de conducció.
El corrent generat es amplificat fins a tenir uns 10^5-10^6 electrons.

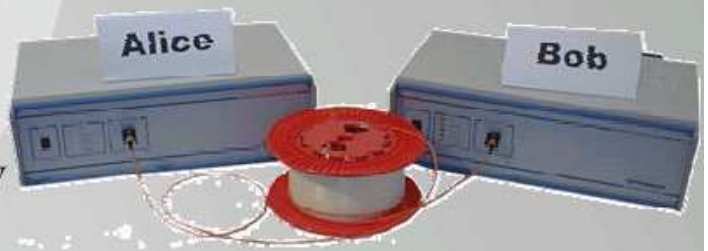




id-Quantique

http://www.idquantique.com

- Company established in 2001
  - Spin-off from the University of Geneva



- Products
  - Quantum Cryptography (optical fiber system)
  - Quantum Random Number Generator
  - Single-photon detector module (1.3 µm and 1.55 µm)

- Contact information

email: info@idquantique.com

web: http://www.idquantique.com

MagiQ

MagiQ **NAVAJO SECURITY GATEWAY™**
Uncompromising VPN Security™

http://www.magiqtech.com

Enterprise Class Network Security

- Absolutely secure Quantum Key Distribution
- Key refresh rate up to 100 keys a second
- Key management uses last validated key
- Automatic "intrusion detection"
- Always-on base VPN
- Data protection with best of breed encryption technologies
- In-transit data security
- Network compatibility
- Streamlined VPN IPSec policy definition
- Compliant with industry standards BB-84, 3DES, AES

OVERVIEW

Technology companies have responded to heightened requirements for information security with an avalanche of new cryptography products, software, and protocols. As sophisticated as these solutions are, they share three things in common:

- They're all built with digital technology.
- They all rely on computational difficulty as the source of their protection.
- And none can escape the fact that information security that relies on digital technology and computational difficulty is ultimately vulnerable.

Breaking through to information security that's NOT VULNERABLE means breaking new ground. Breaking with the tradition of refining current solutions. Finding new directions. Pioneering completely new technologies that can't be threatened by the next new chip or the next new software algorithm. That's been the mission of MagiQ Technologies since 1999. And today MagiQ is proud to report "mission accomplished."

Presenting Navajo Security Gateway™ Quantum Key Distribution (QKD) System.

3.5 Conclusions

Per finalitzar, què és el que s'ha fet fins ara?

- Bennett (IBM, 1989): 30cm
- Hughes et al. (Los Alamos, 2000): 48 km (fibra) 1.6 km -> 10 km (espai lliure)
- Gisin et al. (Switzerland, 2002): 67 km, 1 kbps (fibra)
- Mitsubishi (Japan, 2002): 87 km, 1kbps (fibra); Tokyo-Fuji Mt.
- Los Alamos/NIST (2007); 148.7 km (fibra); protocol BB84.
- Col·laboració Europea (Illes Canàries, 2007); 144km (espai lliure) protocol Ekert91

Reptes experimentals:

- Veritables fonts de fotons individuals
- Fibres òptiques amb menys pèrdues, amb menys efectes nocius per a la polarització
- Detectors amb millor eficiència quàntica
- Progrés en la generació de fotons entrellaçats