Cryptographie Quantique
Principes, Implementation, Perspectives

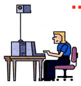
Séminaire du
Département Communications et Electronique
3 juillet 2012

Philippe Gallion
Télécom ParisTech
Ecole Nationale Supérieure des Télécommunications
Centre National de la Recherche Scientifique, CNRS LTCI
46, rue Barrault 75634 Paris CEDEX 13, France

Quantum Cryptography
Principle, Implementation, Perspectives

Traditional Cryptography Starring

Alice is the message sender

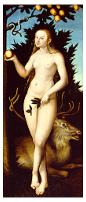


Eve is the eavesdropper

Bob is the receiver

Bob Marley the Reagee Music Star

Alice in wonderland (Lewis Caroll)

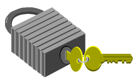


Cranach' the Elder (Germain Painting)

Cryptosystem (or Ciphers)

Message + Key —Encryption→ Cryptogram

Cryptogram + Key —Decryption→ Message



- ✓ Decryption without the key is:
  - ❑ «Impossible» (nothing is)
    - «Impossible n'est pas français» (Bonaparte)
    - «Inviolable n'est pas russe» (Georges Armand Masson)
  - ❑ Difficult (growing exponentially with the key length)
  - ❑ «Easy» (growing polynomially with the key length)
- ✓ Key is a secret shared by Alice & Bob

...il est vraiment douteux que l'ingéniosité humaine puisse créer une énigme de ce genre dont l'ingéniosité humaine ne vienne à bout par une application suffisante

Edgar Allan Poe
The Gold-Bug, Tales of Mystery and Ratiocination, 1843,
Traduction de Charles Baudelaire

Secret Key (Symmetrical) Cipher

- ✓ Exclusive OR
  - ❑ XOR,
  - ❑ Addition modulo 2

	0	1
0	0	1
1	1	0

- ✓ Two consecutive additions return to the initial message

TEXT	Q	C
ASCII	1 0 0 0 1 0 1	1 1 0 0 0 0 1
+ KEY	0 1 1 0 0 1 1	0 1 1 0 0 1 1
ENCODED MESSAGE	1 1 1 0 1 1 0	1 0 1 0 0 1 0
+KEY	0 1 1 0 0 1 1	0 1 1 0 0 1 1
ASCII	1 0 0 0 1 0 1	1 1 0 0 0 0 1
TEXT	Q	C

“One Time Pad” Necessity (Vernan Code)

- ✓ Eve’s recording of scrambled message allows to start a picture of the message
- ✓ The addition 2 messages scrambled with the same key is only the sum of the 2 messages
- ✓ Perfectly secure for “One Time Pad” (OTP)
  - ❑ Key of the same length than the message
- ✓ Quantum Key Distribution (QKD) is the Key issue !

Quantum Cryptography
Principle, Implementation, Perspectives

Quantum Physics Principles

- ✓ Principle of indetermination (Heisenberg)
  - ❑ Indeterminism inherent to the nature
- ✓ The wave nature (de Broglie, Schrödinger)
  - ❑ Describing probabilities
- ✓ Principle of complementary (Bohr)
  - ❑ Wave and (quantum) corpuscular nature are two perspectives of the same reality
  - ❑ Its is a duality
  - ❑ It is NOT dualism
- ✓ Principle of correspondence (Ehrenfest)
  - ❑ Quantum mechanics and classical one agree as the quantum nature disappears
  - ❑ Classical mechanics is only a limit

Quantum States

- ✓ A QS is the superposition of eigenstates

$$|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle \quad \text{with} \quad \alpha_i = \langle \psi_i | \psi \rangle$$

- ✓ A measurement converts a QS into one of its eigenstates

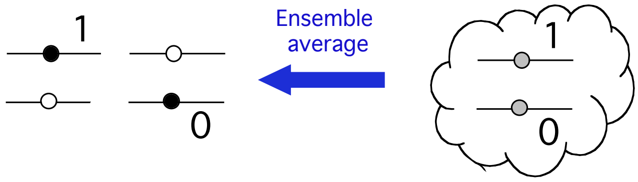
$$|\psi\rangle \longrightarrow |\psi_i\rangle$$

- ✓ The measurement result is the corresponding eigenvalue
  - ❑ The probability of this result is $|\alpha_i|^2$
- ✓ Consequences
  - ❑ Except for eigenstates, measurement destroy the system
    Quantum demolition
  - ❑ Simultaneous and precise measurements are impossible
  - ❑ Duplication of unknown quantum state is impossible
    Non clonning

} Sources Of Security

Classical Bit v.s. Quantum Bit

Classical Bit : Any macroscopic 2-state system	Quantum Bit (QB) Any 2-level quantum system

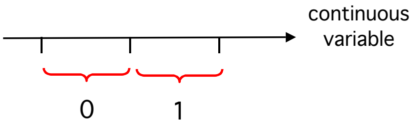


- ✓ Exclusive states : 0 or 1 at a given time
- ✓ States exist independently of measurement
- ✓ $p(1) + p(0) = 1$
- ✓ Measurement keeps the system unchanged

- ✓ State superposition: 0 and 1 at the same time : $QB> = \alpha\ |0> + \beta\ |1>$
- ✓ One of the 2 eigenstates is obtained after a measurement
- ✓ $|\alpha|^2$ is the probability to obtain $|0>$
  $|\alpha|^2 + |\beta|^2 = 1$
- ✓ Measurement destroys the superposition

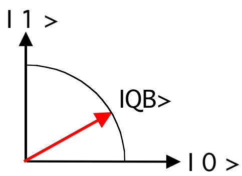
Classical Bit v.s. Quantum Bit - 2/2

Classical Bit (CB)



- ✓ 1 dimension
- ✓ Areas selected for bit value representation
- ✓ 2 possibilities
- ✓ n bits belongs to an n dimension space

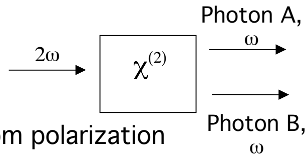
Quantum Bit (QB)



- ✓ 2 dimensions
- ✓ n qubits belongs to a 2^n dimension space
- ✓ Schrödinger' s cat paradox
- ✓ Breton's soluble fish paradox

Entangled States

- ✓ Quantum « super correlation » ≠ classical correlation
  - ❑ Verschränkung (i.e.“Bras dessus bras dessous”)
  - ❑ Entanglement
  - ❑ Intrication (Fr)
- ✓ 2 photon parametric generation



- ✓ The individual photon have a random polarization

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\rangle + |\rightarrow\rangle \right]$$

- ✓ When both measured they have always orthogonal polarization

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}\left[|\uparrow\rangle_A |\rightarrow\rangle_B + |\rightarrow\rangle_A |\uparrow\rangle_B \right]$$

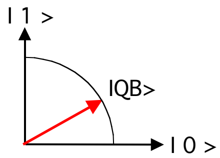
- ✓ Entangled states constitute a single quantum object
  - ❑ They have interacted in the past,
  - ❑ They have some locally inaccessible information in common
  - ❑ This information cannot be accessed in any experiment performed on either of them alone

Quantum Cryptography
Principle, Implementation, Perspectives

- ✓ 1. Introduction
- ✓ 2. Basics Concepts of Quantum Physics
- ✓ 3. Quantum Cryptography Protocols and Attacks
- ✓ 5. Homodyne QPSK Implementation
- ✓ 6. Perspectives

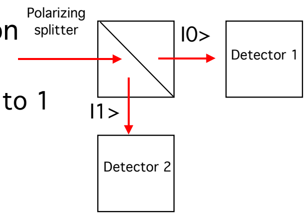
Qbit Communication System
using Simple Eigenstate Encoding - 1

- ✓ Polarization (i.e. spin) is an example
- ✓ Any 2-level system acts in the same way
- ✓ Q bit are used : IQB > $=\alpha$ I0> + β I1>



- ✓ Simple eigenstate information encoding
  - ❑ $\alpha=1$ for bit 0 and $\beta=0$ $\quad |\rightarrow\rangle = |0\rangle$
  - ❑ $\alpha=0$ for bit 1 and $\beta=1$ $\quad |\uparrow\rangle = |1\rangle$

- ✓ Simple polarization splitting discrimination
  - ❑ A 2 detector arrangement is mandatory
  - ❑ Correct detection probabilities are equal to 1
  - ❑ Error free transmission



Qbit Communication System
using Simple Eigenstate Encoding - 2

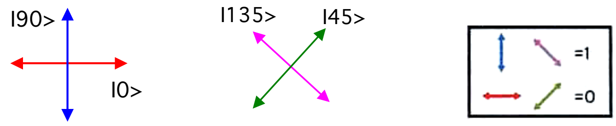
Where is the Rub ?

- ✓ Eve can
  - ❑ Intercept,
  - ❑ Detect the same way....and get the key
  - ❑ Resend to Bob ...who get it too
- ✓ The goal is
  - ❑ Not only an error free communication
  - ❑ ....but a secret communication too!

- ✓ Simple eigenstate encoding is not relevant
- ✓ Protocol required for QKD

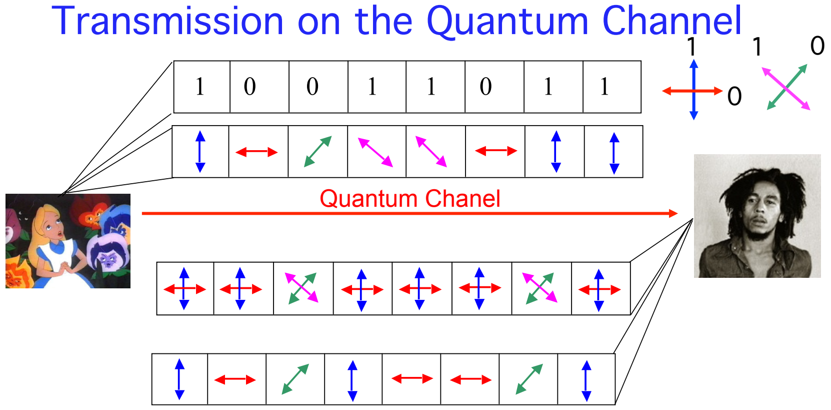
Bennett-Brassard Protocol 1984 (BB84)

- 4 quantum states, forming 2 basis are used



- Conventional binary value attributions on each basis
- Alice and Bob can randomly select any basis
- Basis coincidence allows correct bit detection
- Basis anti-coincidence
  - $|\nearrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\rightarrow\rangle\right)$ and $|\nwarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\rightarrow\rangle\right)$
  - *p(0) = p(1)= 1/2* whatever is the transmitted bit
  - Measurement result without any relation with the transmitted bit
- A second detection is impossible (quantum demolition)

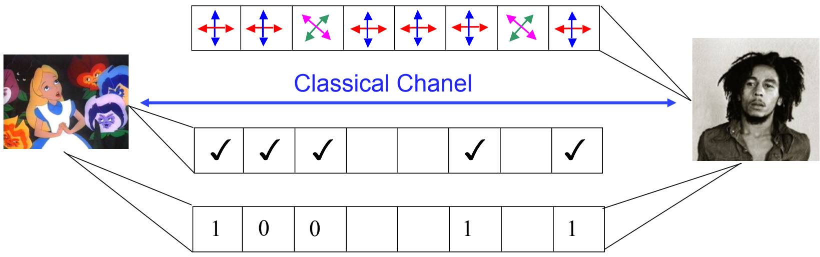
BB84/QKD : Initial Alice to Bob Transmission on the Quantum Channel



- 1 - Alice chooses a random series of bits
- 2 - Alice sends each bit with a random bases choice
- 3 - Bob detects each bit using another random choice of the bases

Resulting BER is 25%:

BB84/QKD : Reconciliation on the Public Classical Channel



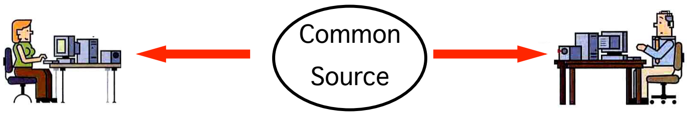
- ✓ 4 - Bob publicly announces his series of bases choices (not the measurement result!)
- ✓ 5 - Alice publicly announces the bases coincidences i.e. the bits correctly detected by Bob
- ✓ 6 - Bob & Alice use this bit sequence as the key: Reconciliation

Theoretical BER is 0%

Using QC

- ✓ Neither Alice and Bob decide of the key
- ✓ Key is a result of random basis choice coincidences in a random series of bits
- ✓ Eve intervention
  - ❑ Only 50% of her base coincidence with the base use by Alice and Bob
  - ❑ QBER =25%
  - ❑ Easily detected by Bob and Alice by an afterward checking the error rate
- ✓ Retrospect security
  - ❑ Unusefull for the message itself
  - ❑ Solves the key distribution problem because intercepted key may be discarded
- ✓ Key may be used on classical channel with OTP (Vernan code)

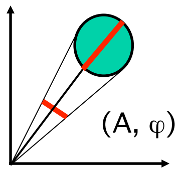
2 Qubit Ekert (EPR) Protocol

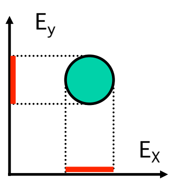


- The 2 qubits are in the same state chosen randomly among the 4 states of the BB84 protocol
  - The source announces the base
  - Alice & Bob only consider compatible basis measurements
  - Equivalent to BB84 protocol
  - But the source may be controlled by Eve!
- The 2 qubits are emitted as an entangled state
  - Reduction of basis coincidence probability

Continuous Variable Protocol

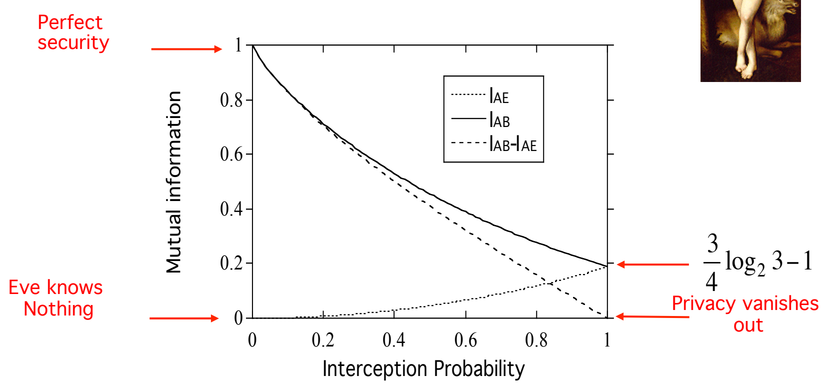
- Information is encoded as CW modulation of two optical field quadrature (E_X, E_Y) or (A, φ)
- Security relies on
  - Non simultaneous precision measurements
  - Non cloning
- Conversion into digital signal for
  - Privacy amplification
  - Error Correction
- Squeezing or EPR correlation are not required
- Chaos cryptography is an other way





Unconditional Quantum Security

A Simple Attack Strategy:
Random interception with probability ω and resend



Some Other Attack Strategies

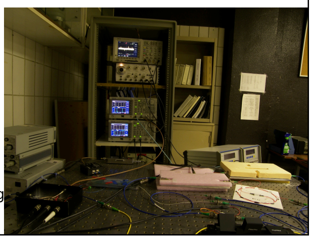
- ✓ Wide range of attacks
  - ❑ Selection of an other base
  - ❑ Using teleportation
  - ❑ Photon number splitting (PNS)
  - ❑ Collective Attack
  - ❑ Fred may help Eve....
- ✓ Performances limited by
  - ❑ The channel imperfection
  - ❑ The available time for a key sharing
  - ❑ Eve resources

Improving the Sifted Keys

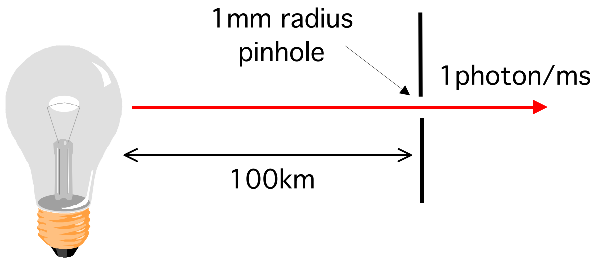
- ✓ The shared key contains error thanks to
  - ❑ Technical imperfection
  - ❑ Eve's intervention
- ✓ QBER differs from BER usually in the 10^{-9} range
  - ❑ Corrected a priori using FEC and over heading of the signal
- ✓ QBER is usually in the few percent range
  - ❑ Corrected with a posteriori classical error correction
  - ❑ Public channel is used to distill key without error
  - ❑ At the expense of the key length reduction !
- ✓ Eve have catch some information about the key
  - ❑ Privacy amplification
  - ❑ Public channel is used
  - ❑ At the expense of the key length reduction !

Quantum Cryptography
Principle, Implementation, Perspectives

- ✓ 1. Introduction
- ✓ 2. Basics Concepts of Quantum Physics
- ✓ 3. Quantum Cryptography Protocols and Attacks
- ✓ 5. Homodyne QPSK Implementation
- ✓ 6. Perspectives



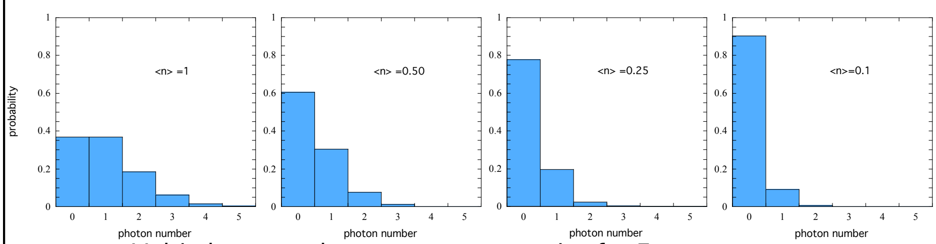
Single Photon Source



- ✓ Power P =100W Standard ligth bulb
- ✓ Efficiency η = 10%
- ✓ Wavelength λ =650nm
- ✓ Distance r =100km
- ✓ Pinhole radius r_0 =1mm
- ✓ Integration time t =1ms

Single Photon Sources

- ✓ Single photon sources
  - ❑ Emitting one and only one photon on request and only on request
  - ❑ Not yet available !
- ✓ Fainted coherent state optical pulses
  - ❑ Simply produced by standard laser
  - ❑ Poisonnian photon number



  - ❑ Multi photon pulses are an opportunity for Eve
  - ❑ Fainting the pulses leads to empty pulse occurrences
  - ❑ Trade-off 0.2 to 0.6 photon /pulse

Coherent States vs Number States

- ✓ Number states $|n\rangle$ are orthogonal $|\langle n|m\rangle|^2 = \delta_{nm}$
- ✓ Coherent states $|\alpha\rangle$ are not
  - ❑ may expanded as a sum of number states

$$|\alpha\rangle = \exp(-\frac{1}{2}|\alpha|^2)\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle$$

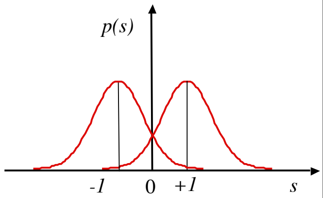
  - ❑ Two coherent states overlap

$$|\langle\alpha_1|\alpha_2\rangle|^2 = \exp(-|\alpha_1 - \alpha_2|^2)$$

  - ❑ BPSK signal overlap

$$\langle\alpha|-\alpha\rangle = \exp(-4N_S) \quad \text{with } N_S = \alpha^2$$

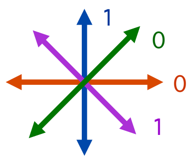
  - ❑ Error free distinction is impossible
- ✓ Photon Number Splitting (PNS) attacks are possible



Encoding Optical Pulses at Quantum Level

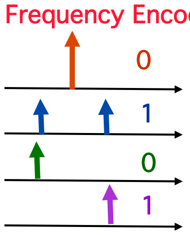
2 representations of the 2 binary symbols on 2 conjugated bases

Polarization Encoding



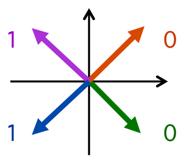
Orthogonal states of polarization (2 modes)
Discrimination by polarizer

Frequency Encoding



Modulation bandwidth FSK
Discrimination by filters

Phase Encoding (QPSK)



Antipodal state of Phase
Discrimination by interference or Homodyne arrangement

Nos activités depuis 2001

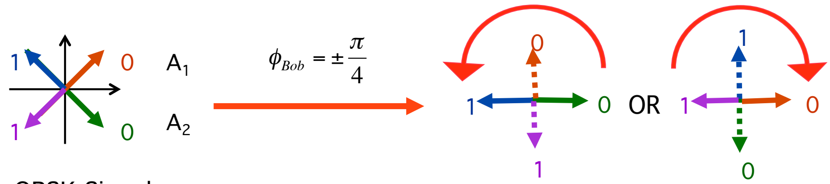
- ✓ Distribution quantique de clef
  - ❑ 155à nm (Longueur d' onde Télécom)
    - Système à Fibre
    - Dispositif télécom
  - ❑ Impulsions atténuées
  - ❑ Modulation de phase QPSK
  - ❑ Compteur de photons
  - ❑ Détection cohérente
- ✓ Sécurité globale
  - ❑ Sylvain Guilley et Jean-Luc Danger
    - Sécurité des implémentations
    - Canaux cachés
    - Générateur de nombres aléatoires
  - ❑ Patrick Bellot
    - Gestion des Flux Interfaçage
    - Affinage et gestion de clef
    - Authentification
- ✓ Partenaires
  - ❑ Georgia Tech Atlanta
  - ❑ Georgia Tech Lorraine
  - ❑ Cisese Mexique
  - ❑ Aexa
  - ❑ Smart Quantum/Auréa
  - ❑ Photline
  - ❑ Université de Besançon

Our 2 Experimental Set-ups

- ✓ Fainted pulse coherent states
  - ❑ Integrated laser and modulator(ILM) 30dB extinction ratio
  - ❑ 5 ns pulse width
  - ❑ Calibrated attenuation control
- ✓ Phase modulation
  - ❑ QPSK constellation
  - ❑ Mach Zendher interferometer phase modulation
- ✓ 2 Receiver structures compared
  - ❑ Balanced super homodyne receiver with photon counters (4 Mhz)
  - ❑ Strong reference homodyne receiver with PIN photodiodes (150Mhz)
- ✓ Phase referencing
  - ❑ Time multiplexed phase reference pulse transmission after 20 ns time delay
  - ❑ Differential phase and polarization stabilizations
  - ❑ Strong pulsed also used clock synchronization
  - ❑ Orthogonal polarizations for signal and local
    - 30dB extinction ratio improvement

Phase Encoding

- ✓ Required for fiber systems
- ✓ Bob introduces his own bases choice by clockwise or counter clockwise constellation rotation
- ✓ Quadrature Phase Shift Keying (QPSK) turns to Binary Phase Shift Keyed (BPSK)

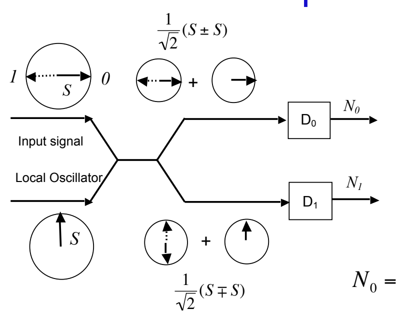


QPSK Signal

BPSK Signal

$$\hat{\rho} = \frac{1}{4}\left(|\alpha_S\rangle\langle\alpha_S| + |-\alpha_S\rangle\langle-\alpha_S| + |j\alpha_S\rangle\langle j\alpha_S| + |-j\alpha_S\rangle\langle -j\alpha_S|\right) \longrightarrow \hat{\rho} = \frac{1}{4}\left(|\alpha_S\rangle\langle\alpha_S| + |-\alpha_S\rangle\langle-\alpha_S|\right)$$

Balanced super homodyne receiver with photon counters



- ✓ 50%/50% coupler
- ✓ Same local and signal amplitudes $L=S$
- ✓ Nulling receiver
- ✓ Half of the signal is wasted

$$N_0 = \frac{1}{2}(S \pm S)^2 = \begin{cases} 2S^2 = 2N_S & \text{when 0 is transmitted} \\ 0 & \text{when 0 is transmitted} \end{cases}$$

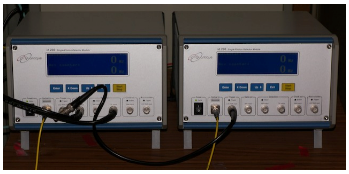
$$N_1 = \frac{1}{2}(S \mp S)^2 = \begin{cases} 0 & \text{when 0 is transmitted} \\ 2S^2 = 2N_S & \text{when 0 is transmitted} \end{cases}$$

- ✓ Erasure rate
  - ❑ No photon is received when N_S is expected (Poisson)
  - ❑ May occurs for any of the 2 symbols

$$BErasureR = \exp(-2N_S)$$

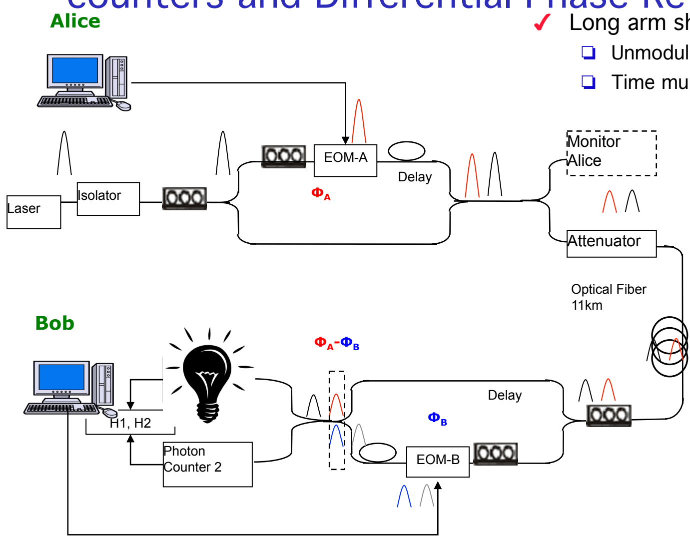
Photons Counters

- ✓ Avalanche Photodiodes (APD)
  - ❑ Biased above breakdown
  - ❑ Single photon trigger 1000 electron avalanche
  - ❑ Quenching required and recovery time
- ✓ Quantum efficiency 10 to 25% (tradeoff with dark count)
- ✓ Noise
  - ❑ Dark counts proportional to the gated opening time : 10^{-4} to 10^{-5} /ns
  - ❑ After pulse counts : reduced by a dead time
- ✓ Speed
  - ❑ Gate width 2.5 to 100ns required photon arrival time control
    - Time synchronization,
    - Heralded photon
  - ❑ Gate trigger up to 8Mhz
- ✓ Feature
  - ❑ Cooling requires :-50°C
  - ❑ Several Kg
  - ❑ Several 10K€



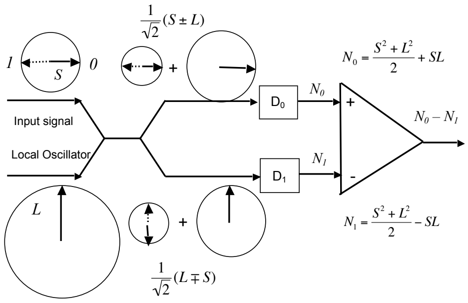
Balanced super homodyne receiver with photon counters and Differential Phase Referencing

- ✓ Long arm short arms
  - ❑ Unmodulated reference pulses
  - ❑ Time multiplexed



- ✓ (Short+short) and (Long+Long) photon paths are disregarded
- ✓ High erasures channel thank to empty pulses

Strong reference homodyne receiver

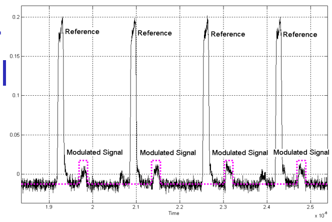


- ✓ 50%/50% coupler
- ✓ Strong local field L >>S
- ✓ Mixing gain
- ✓ PIN photodiodes
- ✓ 2 detector output subtraction

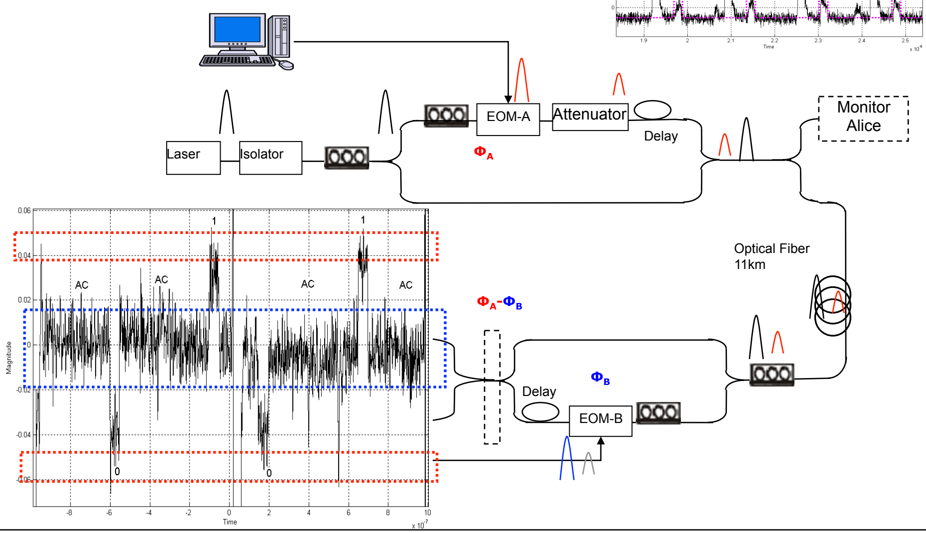
$$N = N_1 - N_1 = 2SL = \pm 2\sqrt{N_S N_L}$$

- ✓ Signal to noise ratio $\frac{S}{N} = \frac{4N_S N_L}{N_L} = 4N_S$
- ✓ Bit Error rate (Gaussian) $BER = \frac{1}{2}\text{erfc}\left(\sqrt{2N_S}\right) \approx \frac{1}{2}\exp(-2N_S)$

Strong reference homodyne receiver with PIN photodiodes and differential phase referencing

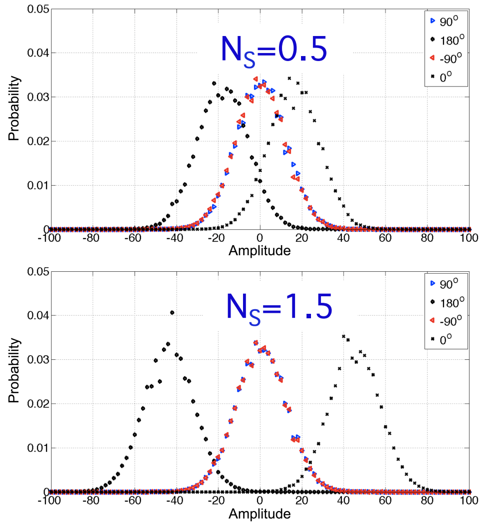


Alice



Strong reference homodyne receiver with PIN photodiodes and differential phase referencing

Experimental and Theoretical Histograms for Different Average Signal Energies



N_S from 0.02 to 3 photons

N_L = 2.8 10^5 photons

Pulse durations = 5ns

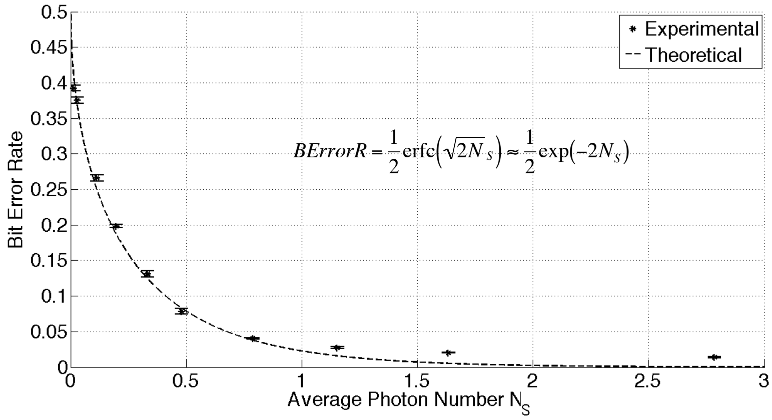
Overlap control below 0.2ns (10cm of fiber)

Only 0 and π may be distinguished

$+\pi/2$ and $+\pi/2$ are undistinguishable

PIN Photodiode and Strong LO Homodyne Detection with differential Phase Referencing

Bit Error Rate as a Function of the Average Photon Number



Phase Mismatch Influence on Super Homodyne with Photon Counters

When 1 is transmitted

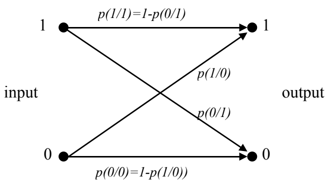
Phase Mismatch

D_1	=1	$=\cos\phi/2$
D_2	= 0	$=\sin\phi/2$

Optical contrast: C =1

Optical contrast : C =cos ϕ

$$|QB\rangle = \cos(\phi/2)|1\rangle + \sin(\phi/2)|0\rangle$$

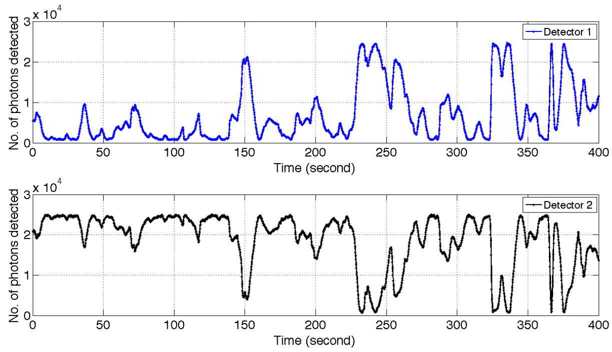


$$p(1/0) = p(0/1) = \sin^2(\phi/2)$$

$$(QBER)_{OPT} = \sin^2(\phi/2) = \frac{1-C}{2}$$

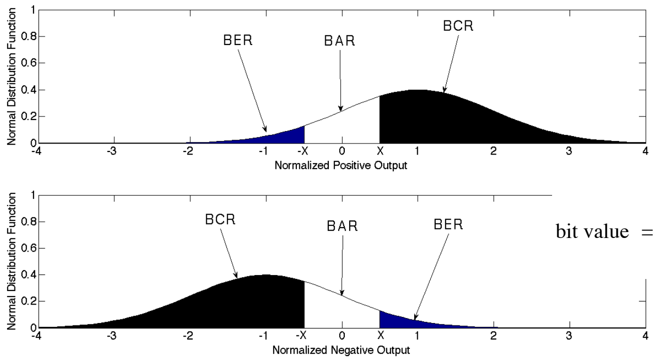
Other system impairments and Eve intervention contribute to QBER

Free running phase drift of the balanced super homodyne receiver (photon counters)



- ✓ Free-running photon counts of the two detectors
  - ❑ CW signal is used
  - ❑ Random but strong negative correlated photon counter out-puts
- ✓ Versatile Phase Compensation System
  - ❑ Phase control with <1s time response required
  - ❑ Differential operation relaxes the difficulty

Decision Abandon: Dual-Thresholds QKD

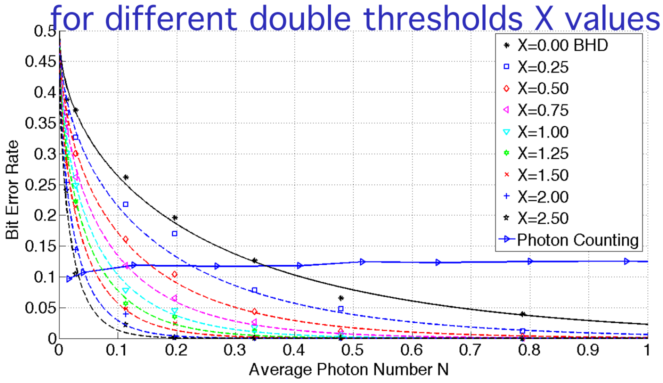


BER: Bit Error Rate
BAR: Bit Abandon Rate
BCR: Bit Correct Rate

$$\text{bit value} = \begin{cases} 1 \ \text{ if } \ N > XN_S \\ 0 \ \text{ if } \ N < -XN_S \\ \textit{inconclusive} \ \text{ otherwise,} \end{cases}$$

- ✓ Bob abandons decision for low level signal
- ✓ Abandoned bits are discarded during reconciliation
- ✓ Abandons not permitted for Eve
- ✓ Bits attenuated by attack are more probably discarded
- ✓ Trade-off between error rate and efficiency

Measured and Theoretical Quantum Bit Error Rate for different double thresholds X values



- ✓ QBER is improved at the expense of the efficiency reduction
- ✓ Better performance than photon counting easily achieved

Receiver comparison @1550nm

Super Homodyne Receiver with Photon Counters

☹ Photon counter (gated Geiger APD)
- ✓Low speed (MHz)
- ✓Low quantum efficiency (10%)
- ✓Dark count limit (QBER)
- ✓Cooling required
- ✓Quenching required

☺ No strong reference

☹ Decision threshold
- ✓At the counter level
- ✓Trade-off between efficiency and dark count

☺ Erasure rate at twice the SQL BER

Strong Reference Balanced Homodyne Receiver with PIN Photodiodes

☺ Standard PIN photodiode
- ✓High speed (GHz)
- ✓High quantum efficiency(90%)
- ✓Room Temperature
- ✓Low cost

☹ Strong reference

☺ Noise free mixing gain

☺ Clock provided by reference pulses

☺ Decision threshold(s)
- ✓Post detection at high signal level
- ✓Multi level decision possible

☺ Standard Quantum Limit (SQL)

In any case: Challenging polarization and phase controls required!

Quantum Cryptography
Principle, Implementation, Perspectives

✓ 1. Introduction
✓ 2. Basics Concepts of Quantum Physics
✓ 3. Quantum Cryptography Protocols and Attacks
✓ 5. Homodyne QPSK Implementation
✓ 6. Perspectives

From the promises of physics of the last century...toward quantum security engineering

- ✓ Implementation of the physical layer is demonstrated
  - ❑ 1550nm wavelength operation without photon counter
  - ❑ Standard optical fiber and devices
  - ❑ One way system, in single optical fiber
  - ❑ Off-the shelf and low cost optoelectronics components
  - ❑ Phase referencing and stabilization
- ✓ End to end approach started
  - ❑ True Random Number Generators (for symbols & bases)
    - 100 to 1000 time faster than the application data rate
    - Robust against attacks
  - ❑ Raw key processing
    - Electronics interface
    - Buffering for key material management
    - Secured electronics processing
  - ❑ Application interface
    - Key distillation using public channel
    - Key management
    - Upper layer interface

About Unconditional Security

- ✓ QKD provides the only protocol which may provide unconditional security
- ✓ About time independent unconditional security
  - ❑ Finite coast not proven
  - ❑ Quantum layer approach is not sufficient to achieve an end-to-end security up to the application layer
    - Attack on the quantum layer is an heavy strategy mistake for Eve
    - Conventional integrated electronics circuits are very vulnerable to the so-called side-channel attacks,
  - ❑ Needs very limited v.s. security on demand
- ✓ Unconditional security limitation discussion
  - ❑ Traditionally considered as limited only by the principles of physics
  - ❑ Not in terms of resources that could realistically have Eve on a given time scale
  - ❑ Confining into academics or thought experiments,
  - ❑ Where is the better emergence probability
    - For the technologies usually evoked in unconditional security discussion ?
    - For technology that would collapse the traditional security systems ?

Looking ahead for a credible role in the «Security Theater »

- The security world is also sometime «Security theater »

  (Bruce Schneier in his book "Beyond Fear")
  - More intended to provide the feeling of improved security
  - Less than some time doing something efficient to actually improve it
- Security is a conservative world
  - Up to now the monopole of classical software based security
  - It cannot afford any technical risk
  - Afraid by disruptive technology
- A credible for quantum security requires
  - Infiltration (Trojan horse' s) in classically secured system technology and culture
    - Classical and quantum securities osmosis
    - Quantum seeded classical key
  - End-to-end security approach
  - Clarification of compatibility with WDM systems

Conclusion

As the vine was too high for him to reach the grapes the fox said,
"They're sour, I can see it,
these grapes are good just for loirs and squirrels!"

"THE FOX AND THE GRAPES » Jean de La Fontaine's fable

- What about the Edgar Allan Poe sentence ?

id Quantique MagiQ AUREA TECHNOLOGY

Merci pour la qualité de votre écoute