Communications Quantiques : des promesses de la physique aux réalités de l'ingénieur

Philippe Gallion

Télécom ParisTech
Ecole Nationale Supérieure des Télécommunications
46, rue Barrault, 75634 Paris

Outline

- ✓ Problématique
- ✓ Contexte
- ✓ Résultats/perspectives

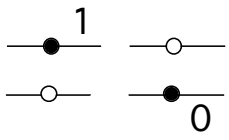
La Problématique

"...and it may well be doubted whether human ingenuity can construct an enigma of the kind which human ingenuity may not, by proper application, resolve."

Edgar Allan Poe
The Gold-Bug, Tales of Mystery and Ratiocination, 1843

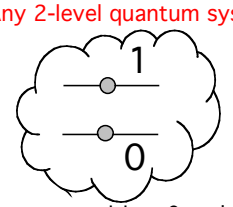
Classical Bit v.s. Quantum Bit

Classical Bit :
Any macroscopic 2-state system



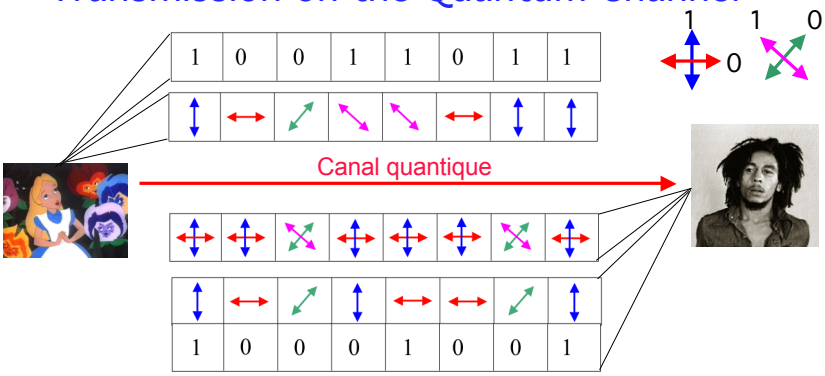
- ✓ Exclusive states : 0 or 1 at a given time
- ✓ States exist independently of measurement
- ✓ $p(1) + p(0) = 1$
- ✓ Measurement keeps the system unchanged

Quantum Bit (QB)
Any 2-level quantum system



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

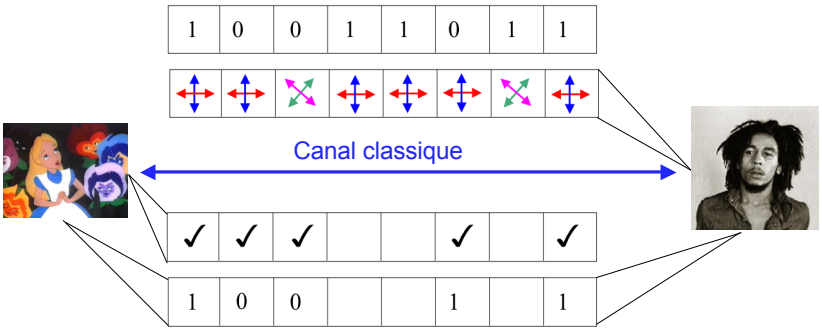
BB84/QKD : Initial Alice to Bob Transmission on the Quantum Channel



- ✓ 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/distillation 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

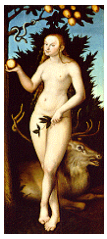
Theoretical BER is 0% but systems impairments and Eve intervention turn to BER

- ✓ 7 - Error correction
- ✓ 8 - Privacy amplification

At the expense of the key length reduction !

Quantum Security

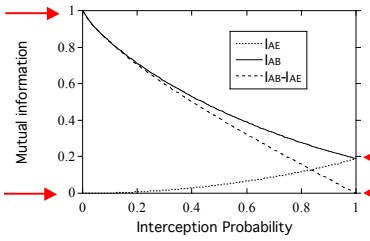
- Security rely on
  - Non cloning
  - Quantum demolition
- Information must supported by quantum system
  - Individual photon
  - Coherent state
  - Entangled photons
- Ensemble systems
  - Average the quantum behavior
  - Are (semi) classical



Eve tries to attack the QDK

Perfect security

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



$\frac{3}{4}\log_2 3 - 1$

Privacy vanishes out

Eve knows Nothing

Toward Quantum Security Engineering

- From the promises of the quantum physics and the information theory of the last century...

  ....To Quantum Cryptography system field deployment
- The state-of-the-art platforms in general are only proof of concept
  - Not fast enough : low generation key stream.
  - Not reliable enough : error correction is required
  - Not versatile enough :
    - Lack of compatibility between equipment
    - Difficulty to adapt dynamically to the hardware layers "upgrades"
    - Complexity of the synchronization procedures...
- Overall system security approach
  - Task sharing among classical and quantum securities
  - Safe electronics processing
  - Gradual transition from classical to quantum securities
  - Security on demand
- Multidisciplinary approach is mandatory
  - Quantum optics
  - Electronics
  - Computers science
  - Information theory...

Key Issues for Large Scale Field Deployment 1/2

- ✓ Optical telecommunication compatibility (1550nm wavelength)
  - ❑ Minimum loss single mode channel
  - ❑ Available integrated functional devices and circuitry
  - ❑ One way system, in a single optical fiber
  - ❑ Low performance of photon counting
  - ❑ Polarization and dispersion impairments
- ✓ Inexpensive single photon sources and detectors
- ✓ Overall system requirement
  - ❑ High speed
  - ❑ High stability
  - ❑ High versatility
- ✓ True Random Number Generators (for symbols & bases)
  - ❑ 100 to 1000 time faster than the application data rate
  - ❑ Robust against attacks
- ✓ Synchronization
  - ❑ Clock synchronization
  - ❑ Bit synchronization
  - ❑ Optical phase referencing or recovery
  - ❑ Polarization control and matching

Key Issues for Large Scale Field Deployment 2/2

- ✓ 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
- ✓ Quantum networking
  - ❑ (Untrusted) Switches
  - ❑ (Trusted) Routers
  - ❑ Coexistence of quantum level key material with WDM message
  - ❑ Security on demand
  - ❑ Security embedded from network design, both quantum and classical

Outline

- ✓ Problématique
- ✓ Contexte
- ✓ Résultats/perspectives

Groupe Communications Optiques (6 permanents, 16 thésards)

- ✓ Des activités «quantiques»
  - 1984 : Premier papier dans IEEE J. Quantum Electron
  - 1992-95 : Lasers à semi-conducteur à puits quantiques
  - 1996-99 : Etats non classiques (comprimé) de la lumière
  - 2004-2005: Lasers à semi-conducteur à ilôts quantique SCL
  - 2000- ... : Amplifications optique distribuée et bruits quantiques
  - 2001-... : Communications Quantiques (Quantum Key Distribution)
  - 2008-...Optique quantique non linéaire
- ✓ Et des activités (semi) classiques
  - Nouveaux concepts/nouveaux dispositifs
  - Nouveaux système et réseaux de communication (Back bone Métropolitain, Accès)
  - **Plateforme Haut débit**
  - Diffusion : capteurs optiques, ...

3 Groupes /2 Départements

- ✓ Le groupe Communications Optiques (Philippe Gallion)
  - ❑ Effets quantiques dans les dispositifs (1981)
  - ❑ Etats non classiques de la lumière (1995)
  - ❑ Mise en oeuvre de protocoles de distribution quantique de clef (2001)
- ✓ Le groupe Électronique (Sylvain Guilley et Jean-Luc Danger)
  - ❑ Réalisation de systèmes reconfigurables (1995)
  - ❑ Sécurité des implémentations (2000)
  - ❑ Générateur de nombres aléatoires (2004)
- ✓ Le groupe Algorithmique Quantique (Patrick Bellot)
  - ❑ Information et communications quantiques (2004)
  - ❑ Protocoles adaptés aux réseaux quantiques (2005)

"When the chariot starts moving, then the pumpkins accommodate them selves" Mexican proverb

Projets Successifs et Moyens

Obtenus/Demandés

- ✓ 2001 : T_0
- ✓ 2002 Début de la première thèse
- ✓ 2004-05 : KANTIC - 50 k€ / 130 k€, CNRS LTCI
  - ❑ Achat des Compteurs de Photons
- ✓ 2005-06 : Voix sur IP Quantique VISQ VISQ - 45 k€ /126 k€, Projet incitatif GET
  - ❑ + 1 stagiaire CNRS LTCI + 2 stagiaires INFRES
  - ❑ 12 mois de Post-Doc CNRS
- ✓ 2007-09 : HQNET 242 k€ /300 k€, ANR exploratoire
  - ❑ 12 mois de financement de thèse «Institut»

Le Consortium HQNET :

High bit-rate and versatile Quantum-secured NETworks

des PME	des labos CNRS	des institutions académiques
Photline Technologies	femto-st sciences & technologies	UFC Université de Franche-Comté
SmartQuantum	cnrs LTCI	TELECOM ParisTech
	GT CNRS Georgia Tech-CNRS	GeorgiaTechLorraine The European Campus of the Georgia Institute of Technology

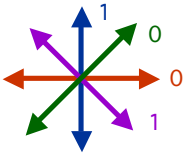
Outline

- ✓ Problématique
- ✓ Contexte
- ✓ Résultats/perspectives

Encoding Quantum Level Optical Pulses

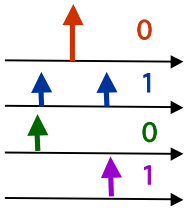
2 representations of the 2 binary symbols on 2 conjugated bases

Polarization Encoding



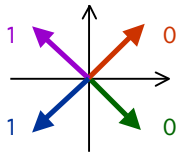
Orthogonal states of polarization (2 modes)
Discrimination by polarizer

Frequency Encoding



Modulation bandwidth FSK
Discrimination by filters

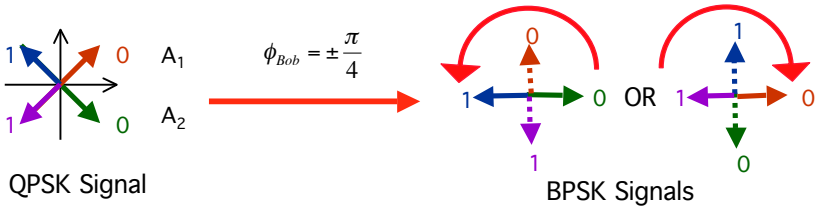
Phase Encoding (QPSK)



Antipodal state of Phase
Discrimination by interference or Homodyne arrangement

QPSK to BPSK Conversion at Bob's End

- ✓ Bob uses identical dual-electrode Mach-Zehnder modulator.
- ✓ Bob introduces his own bases choice
- ✓ Base choice produces clockwise or counter clockwise constellation rotation



QPSK Signal

BPSK Signals

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

Coherent States vs Number States

- ✓ Single photon source (photon gun) not available so far
- ✓ Fainted coherent state pulses easy to be produced
- ✓ 0.1 to 0,5 or (little more) photons average pulse energy
  - ❑ Trade-off between empty pulses and multi photon pulses
- ✓ Non orthogonal coherent states may expand 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

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

  - ❑ Error free distinction is impossible
- ✓ BPSK signal overlap

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

- ✓ Photon Number Splitting (PNS) attacks are possible

Photons Counters

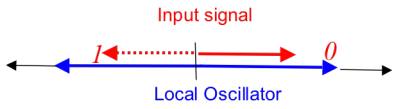
- ✓ Avalanche Photodiodes (APD)
  - ❑ Biased above breakdown
  - ❑ Single photon trigger 1000 electron avalanche
  - ❑ Quenching required and recovery time
- ✓ Telecom wavelength (1550nm) with SMF pig tail
- ✓ Quantum efficiency 10 to 25% (tradeoff with dark count)
- ✓ Noise
  - ❑ Dark counts proportional 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€

Idealistic Single Detector Quantum Receivers

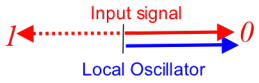
- ✓ Helstrom limit
  - Information theory
  - Maximum likehood

$$BErrorR = \frac{1}{2}\left(1 - \sqrt{1 - \exp(-4N_S)}\right) \approx \frac{1}{4}\exp(-4N_S)$$

- ✓ Dolinar receiver
  - Single photon counter
  - Nearly unit transmission coupler
  - Conditionnal nulling
  - Phase switching and amplitude tuning of LO



- ✓ Kennedy (Super Homodyne) receiver
  - Single photon counter
  - Nearly unit transmission coupler
  - Unconditionnal nulling
  - Error if no photon occurs when $4N_s$ are expected
  - Super quantum limit



$$BErrorR = \frac{1}{2}\exp(-4N_S)$$

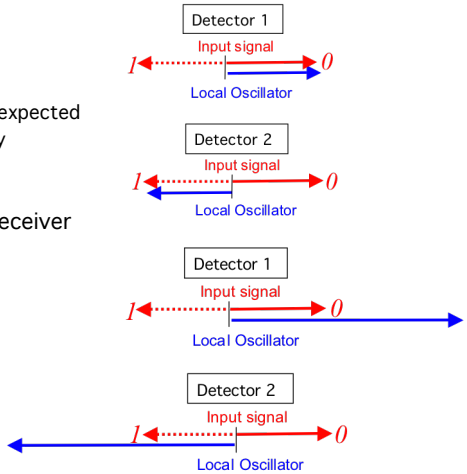
2 Realistic Quantum Receivers

- ✓ Super homodyne receiver
  - 50%-50% coupler
  - 2 photon counters
  - Same amplitude local field
  - Unconditional nulling on one detector
  - Error if no photon occurs when $2N_s$ are expected
  - Kennedy receiver with 1/2 signal energy

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

- ✓ Balanced strong reference homodyne receiver
  - 50%-50% coupler/π phase shift
  - 2 PIN photodiodes/out-put subtraction
  - Strong reference
  - Local field mixing gain
  - Single quadrature measurement
  - Standard quantum limit (SQL)

$$BErrorR = \frac{1}{2}\operatorname{erfc}\left(\sqrt{2N_S}\right) \approx \frac{1}{2}\exp(-2N_S)$$

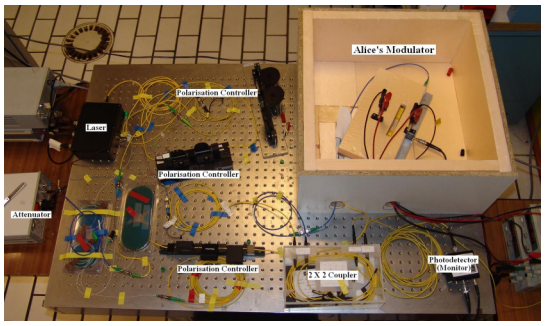


Our 2 Experimental Set-ups

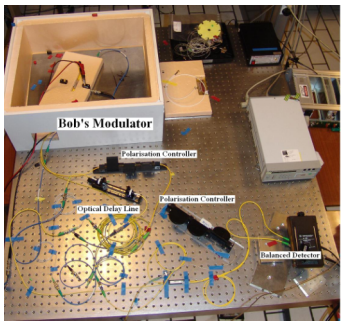
- ✓ Fainted pulse coherent states
  - ❑ Telecommunication wavelength 1550nm
  - ❑ Integrated laser and modulator(ILM) 30dB extinction ratio
  - ❑ 5 ns pulse width
  - ❑ 4 Mhz repetition rate (limited by photon counters)
  - ❑ Calibrated variable attenuation control for operation in the 0.1 to 2 average photon number range

- ✓ Phase modulation
  - ❑ QPSK constellation, turning to BPSK after Bob base selection
  - ❑ Mach Zendher interferometer phase modulation
- ✓ 2 Receiver structures compared
  - ❑ Balanced super homodyne receiver with ID Quantic photon counters (4 Mhz)
  - ❑ Strong reference balanced homodyne receiver with PIN photodiodes (150Mhz)
- ✓ Phase referencing
  - ❑ Time multiplexed phase reference pulse transmission after 20 ns time delay
  - ❑ Single fiber operation
  - ❑ Differential phase and polarization stabilizations only
  - ❑ Strong pulsed clock synchronization
  - ❑ Orthogonal polarizations for signal and local (30dB extinction ratio improvement)

Photon Counting and Homodyne Detection 2



Alice's end

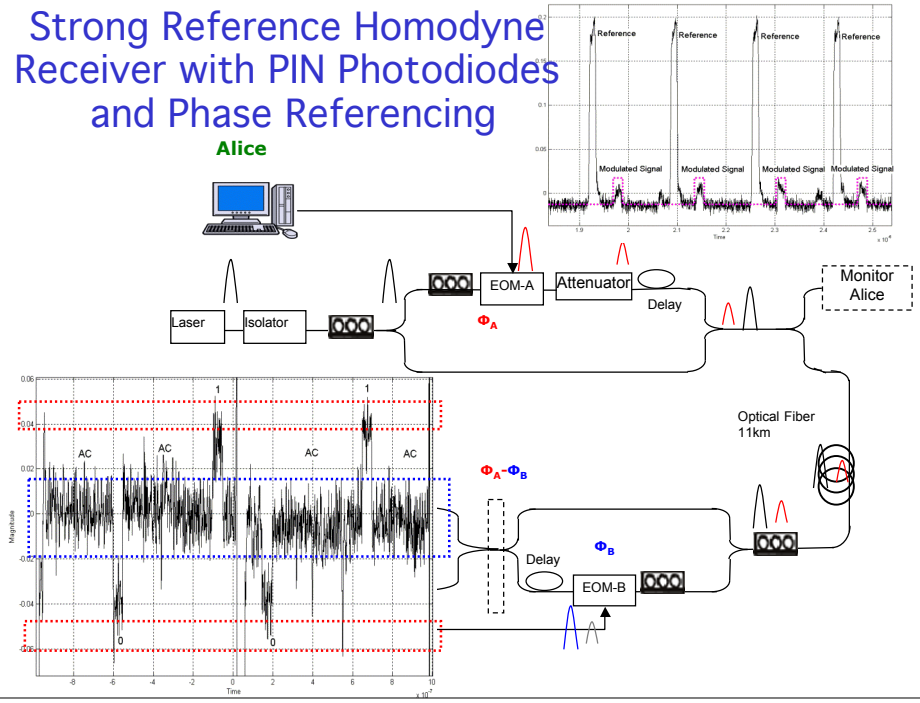


Bob's end

4 Mbits/s Clock rate (limited by photon counters)

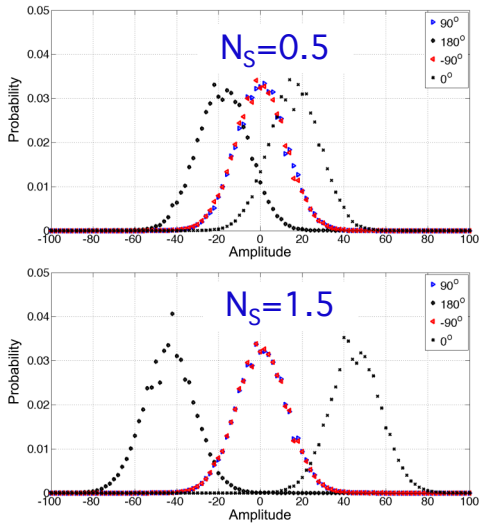
2.5 ns photon counter gate

Strong Reference Homodyne Receiver with PIN Photodiodes and Phase Referencing



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

Receiver comparison @1550nm

Super Homodyne Receiver with Photon Counters

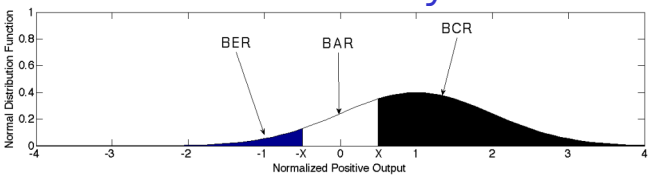
- ☹ Photon counter (gated Geiger APD)
  - ✓Low speed (MHz)
  - ✓Low quantum efficiency (10%)
  - ✓Dark count limit (QBER)
  - ✓Cooling required
  - ✓Quenching required
- ☺ No strong reference
- ☹ Decision threshold
  - ✓At the counter level
  - ✓Trade-off between efficiency and dark count
- ☺ Erasure rate at twice the SQL BER

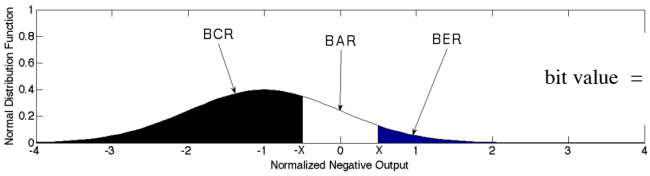
Strong Reference Balanced Homodyne Receiver with PIN Photodiodes

- ☺ 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!

Dual-Thresholds Balanced Homodyne Detection QKD





- ❑ Bit Error Rate
- ❑ Bit Abandon Rate
- ❑ Bit Correct Rat

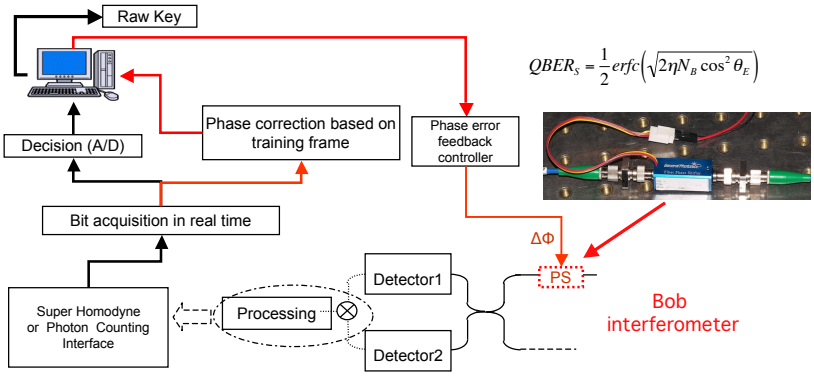
$$\text{bit value} = \begin{cases} 1 \text{ if } N > XN_S \\ 0 \text{ if } N < -XN_S \\ \textit{inconclusive} \text{ otherwise,} \end{cases}$$

- ✓ 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

$$\begin{cases} BER_i = 1/2\, erfc\left[(2N_S)^{1/2}(X+1)\right] \\ BCR_i = 1/2\, erfc\left[(2N_S)^{1/2}(X-1)\right] \\ BAR_i = 1 - BER_i - BCR_i \end{cases}$$

Versatile Phase Compensation System

(Operating both for super homodyne and Photon counting receiver)



- ✓ Feedback from a deterministic training frame
- ✓ Training Frame including the 4 equiprobable states of the constellation
- ✓ Each received bit compared to the expected one
- ✓ Multiplication of 2 quadrature averaged results allows phase mismatch extraction
- ✓ Control feedback signal applied on a piezoelectric fiber spool (PS)
- ✓ Forcing phase error down to 0

Publications Internationales 2005-2009
15/70

(hors CR de contrats, soumissions et rédactions en cours...)

- ✓ Physique
  - ❑ Phys Rev Letters
  - ❑ JOSA
  - ❑ Opt Xpress
- ✓ IEEE
  - ❑ Journal of Quantum Electronics
  - ❑ Journal of Selected Topics in Quantum Electronics
  - ❑ Journal of Lighwave Technology
  - ❑ Photonics Technology Letters
- ✓ Chapitre de Livre : "Signal and quantum noise in optical communications and in cryptography". Elsevier 2008, Progress in Optics, Volume 52, Jan 2009, 112 pages

Communications Internationales (2005-2009) 20/100

(Hors Workshops, Séminaires....)

- ✓ Conférences majeures
  - Optical FC
  - European Conference on Optical Communication
  - Conference on Lasers and Electro optics
- ✓ IEEE Regional meetings
- ✓ OSA/IEEE Topical meetings

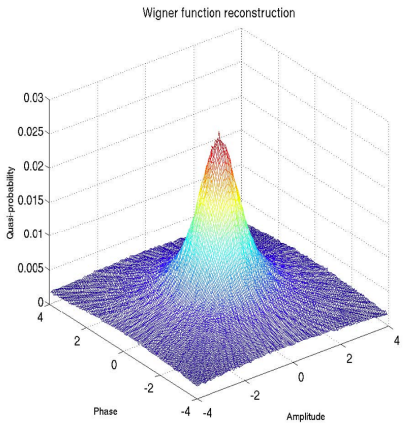
Thèses Soutenues (2005-2009) : 6/38

- ✓ Préparées à l'Ecole
  - SABBAN Manuel - «Détection Optique Homodyne : Application à la Cryptographie Quantique » Thèse TELECOM ParisTech, ENST, soutenue le 29 avril 2009.
  - XU Qing - « Détection Optique Homodyne : Application à la Cryptographie Quantique » Thèse TELECOM ParisTech, ENST, soutenue le 28 avril 2009
  - JIANG Shifeng. - «Contributions à l'étude théorique des bruits quantiques et classiques dans les amplificateurs Raman distribuées». Thèse ENST, Soutenue le 15 février, 2008.
  - AGNOLINI Sebastien - «Contribution à l'étude et à la réalisation d'un système de distribution quantuique de clef par codage en phase». Thèse ENST, soutenue le 23 avril 2007.
  - BRISTIEL Bristiel - «Contritution à l'Etude du Bruit dans les Amplificateurs Raman». Thèse ENST, soutenue le 27 mars 2006
- ✓ En cotutelle (Shanghai Jiao Tong University)
  - ZHOU JunHe - « Raman fiber laser, application of Neural network in amplifier design, and the performance of the hybrid amplifier ». TELECOM ParisTech, ENST/Jiao Tong Soutenue le October, 31, 2008,

Forces/Faiblesses

- ✓ Formel et expérimental
- ✓ Environnement «Communications et Electronique»
  - ❑ Optique
  - ❑ Quantique
  - ❑ Communications Numériques
  - ❑ Electronique
    - Sécurité
    - Circuits interface
    - TRNG
- ✓ Interdisciplinarité
  - ❑ Différents Groupes
  - ❑ Différents Départements
- ✓ Réussite collective
- ✓ Manip difficiles
  - ❑ Moyens financiers
  - ❑ Pas de technicien de Labo
- ✓ Déficit relatif de visibilité interne

Perspectives



- ✓ Communications quantiques
  - ❑ Compatibilité avec canaux classiques
  - ❑ Canaux cachés de la couche physique
  - ❑ Intégration verticale
    - Traitement Matériel sûr (SEM)
    - Traitement logiciel (INF)
  - ❑ Sécurité holistique
    - End-on-End
    - Sécurité distribuée
    - Entrisme dans la sécurité classique
    - Sécurité à la demande
- ✓ Tomographie
  - ❑ Fonction Wigner
  - ❑ Analyse de constellations I/Q
- ✓ Limites fondamentales des systèmes cohérents
- ✓ Nouveau concepts et effets quantiques dans les dispositifs

Merci pour la qualité de votre écoute