IEEE France Section

TELECOM ParisTech

IEEE photonics SOCIETY

Célébration du 125ème anniversaire d'IEEE
et de l'attribution du Prix Nobel de physique à
W.S. Boyle, G.E. Smith et C.K. Kao (fellows IEEE)
Abbaye de Royaumont (Val d'Oise)
les 6 et 7 novembre 2009

La Cryptographie Quantique : des promesses de la physique aux réalités de l'ingénieur

Philippe Gallion

IEEE Photonics Society French Chapter
Télécom ParisTech
Ecole Nationale Supérieure des Télécommunications
46, rue Barrault, 75634 Paris

Goals

- ✓ Making communications interaction as safe as perfectly secret personal meeting
- ✓ Confidentiality
- ✓ Identification
- ✓ Authentication
- ✓ Non-repudiation

"...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

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)

Secret Key (Symmetrical) Cipher

✓ Exclusive OR or XOR, or addition modulo 2

	0	1
0	0	1
1	1	0

✓ Two consecutive additions return to the initial message

				Q							C				
TEXT															
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	1	1	1	0	1	1	0	1	0	1	0	0	1	0	
MESSAGE															
+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 :

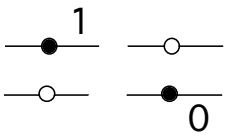
  The addition of to messages scrambled with the same key is the sum of the 2 messages

- ✓ Perfectly secure for "One Time Pad" (OTP)
- ✓ Key of the same length than the message itself

Quantum Key Distribution (QKD) is the Key issue

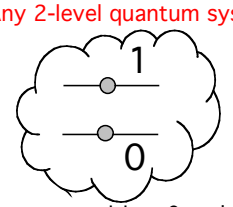
Classical Bit v.s. Quantum Bit

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

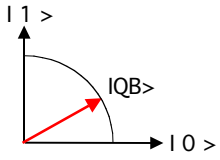


- ✓ State superposition: 0 and 1 at the same time : $QB > = \alpha\ |0> + \beta\ |1>$
- ✓ One of the 2 eigenstates is obtained after a measurement
- ✓ $|\alpha|^2$ is the probability to obtain $|0>$

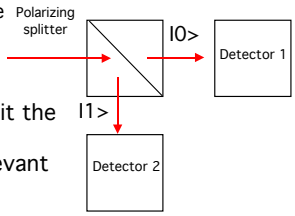
  $|\alpha|^2 + |\beta|^2 = 1$
- ✓ Measurement destroys the superposition

Eigenstate Qbit Communication System

- ✓ 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 with
  - ❑ α =1 for bit 0 and β =0 $\quad |\rightarrow\rangle = |0\rangle$
  - ❑ α =0 for bit 1 and β =1 $\quad |\uparrow\rangle = |1\rangle$



- ✓ Bit discrimination by simple polarization splitting
  - ❑ A 2 detector arrangement is mandatory
  - ❑ Correct detection probabilities are equal to one
  - ❑ Error free transmission

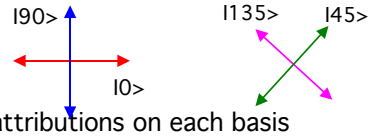


But

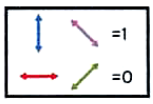
- ✓ Eve can intercept, do the same and retransmit the same eigenstate to Bob
- ✓ Simple transmission of eigenstates is not relevant
- ✓ Protocol required for QC

Bennett-Brassard Protocol 1984 (BB84)

- ✓ 4 quantum states , forming 2 basis are used

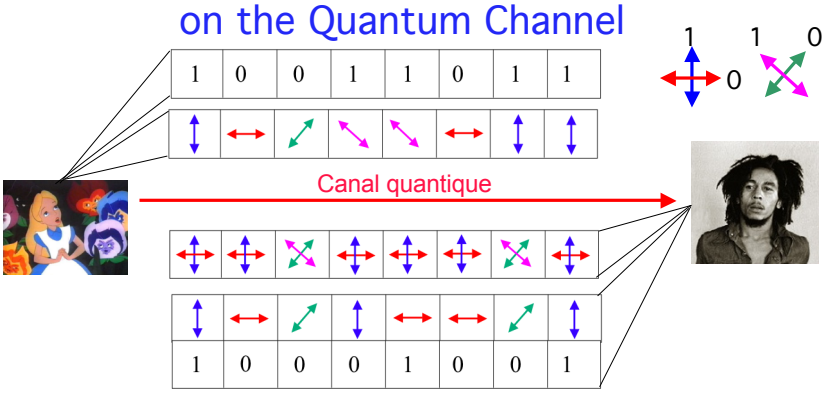


- ✓ Binary value attributions on each basis
- ✓ Simultaneous observations using the 2 basis are im
- ✓ Alice and Bob can select any basis
- ✓ Basis coincidence allows correct bit detection
- ✓ Basis anti-coincidence



  - ❑ $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$ and $|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle)$
  - ❑ *p(0) = p(1)= 1/2* whatever is the transmitted bit
- ✓ A second detection is impossible (quantum demolition)

BB84: Initial Alice to Bob Transmission on the Quantum Channel



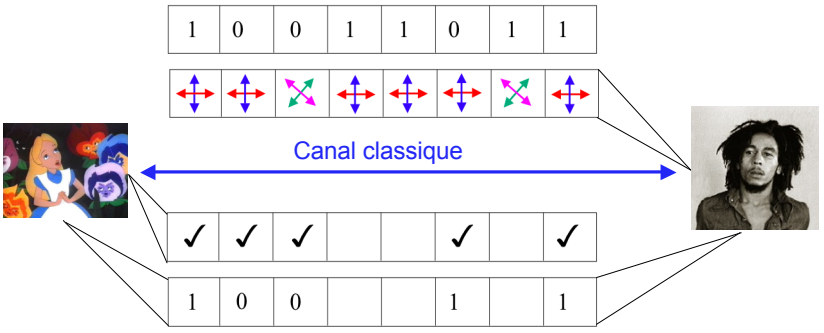
- ✓ 1 - Alice chooses a random series of bits
- ✓ 2 - Alice sends each bit with a random bases choice
- ✓ 3 - Bob detects each bit using another random choice of the bases

Resulting BER is 25%:

50% of good results from bases coincidence

25% of good result from bases anti coincidence

BB84: Reconciliation on the Public Classical Channel

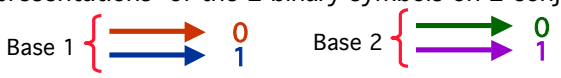


- ✓ 4 - Bob publicly announces his series of bases choices (not the measurement result!)
- ✓ 5 - Alice publicly announces the bases coincidences i.e.the bits correctly detected by Bob
- ✓ 6 - Bob & Alice use this bit sequence as the key: Reconciliation

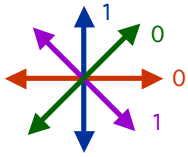
Theoretical BER is 0%:

Encoding information on a Single Photon

- ✓ Classical systems average out the quantum character
- ✓ Quantum system must be used
- ✓ 2 representations of the 2 binary symbols on 2 conjugated bases

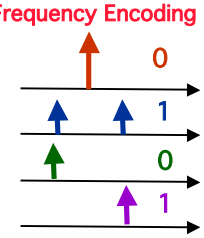


Polarization Encoding



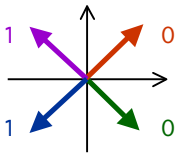
Orthogonal states of polarization
(Discrimination by polarizer)

Frequency Encoding



Modulation bandwidth FSK
(Discrimination by filters)

Phase Encoding (QPSK)



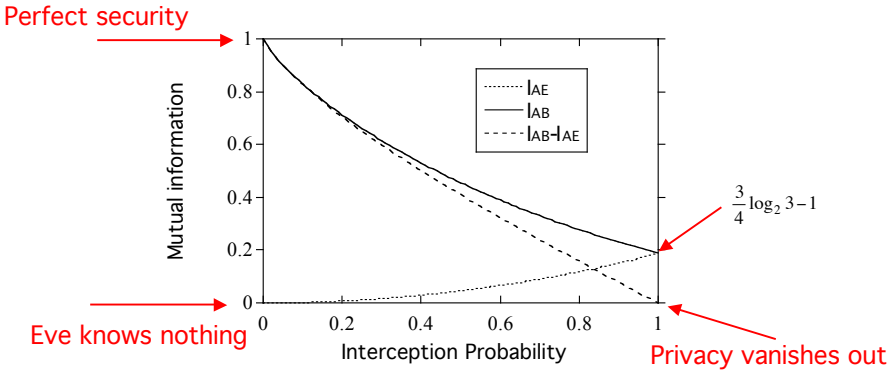
Antipodal state of Phase
(Discrimination by interference)

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
- ✓ Security relies on
  - ❑ Quantum demolition measurement
  - ❑ Non cloning
- ✓ 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

A Simple Attack Strategy and Unconditional Security

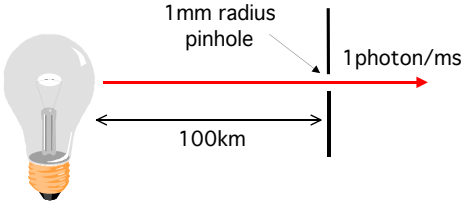
Interception with probability ω and random reemission



Single Photon Source 1/2

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

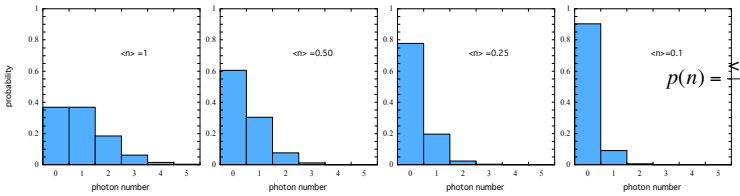
$$n = \frac{\eta P \tau}{h\nu} \cdot \frac{\pi r_0^2}{4\pi r^2} \approx 1 \text{ photon}$$



"When in the darkness, it is good to believe in the light" Edmond Rostand

Single Photon Source 2/2

- ✓ Reliable single photon sources not yet available
  - ❑ Emitting one and only one photon on request
- ✓ Fainted Poisonnian coherent optical pulses are widely used



$$p(n) = \frac{< n >^n}{n!} \exp - < n >$$

- ✓ Pulses with several photon are an opportunity for Eve
  - ❑ Photon Number Splitting Attack)
- ✓ Fainting the pulses leads to empty pulses
- ✓ 0.2 photon /pulse
  - ❑ Trade-off between empty pulses and pulses containing more of one photon
  - ❑ Optimal number depends on transmission loss

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€

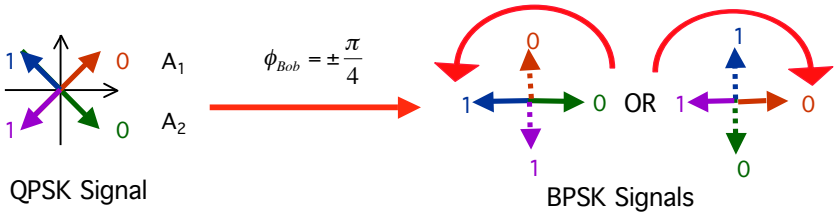
Key Issues for Large Scale Field Deployment 1/2

- ✓ Optical telecommunication compatibility
  - ❑ Standard optical fiber: Loss, polarization and dispersion impairments
  - ❑ 1550nm wavelength: Low performance of photon counting
  - ❑ One way system, in a single optical fiber
- ✓ 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

Using Phase Encoding: QPSK-QKD



- ✓ QPSK turn to BPSK
- ✓ Antipodal signal
- ✓ Coherent states are not orthogonal

Phase Referencing

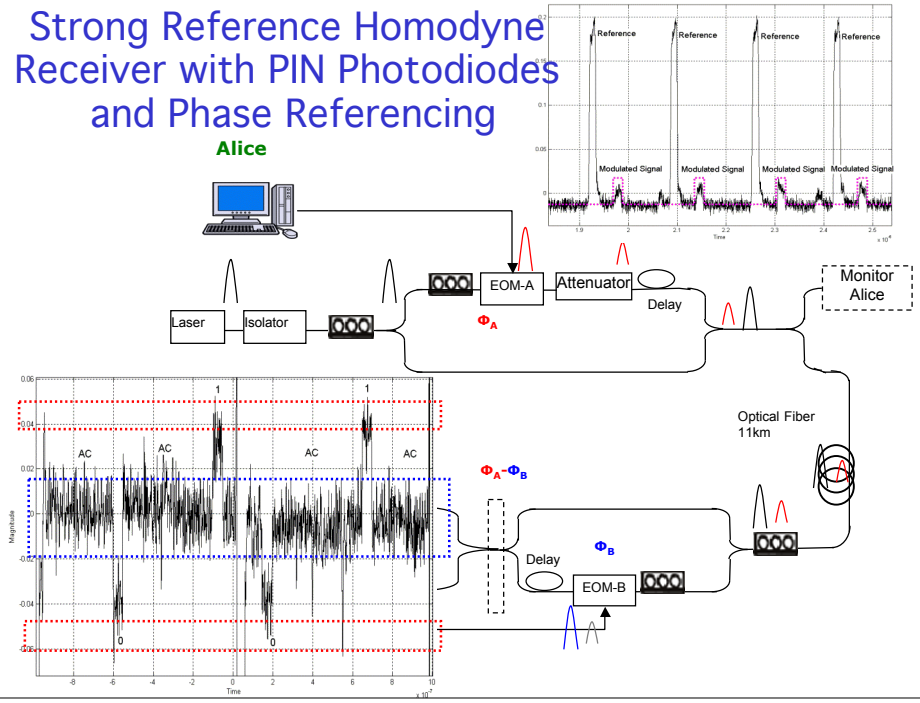
- ✓ 2 arm interferometer
  - ❑ 2 fibers required
  - ❑ Phase and polarization control required
  - ❑ Strict thermal and mechanical isolation
  - ❑ Periodic switching to bright light for phase tracking

  Two fibers
- ✓ "Plug and Play" configuration
  - ❑ Self compensation by round trip
  - ❑ Faraday
  - ❑ Phase conjugated mirror

  Single fiber two ways
- ✓ Phase locked local oscillator
  - ❑ Super homodyne
  - ❑ Injection locking of an independent local laser
- ✓ Differential interferometer arrangement
  - ❑ Relaxes absolute to relative phase and polarization control
- ✓ Time Shared (strong) phase referencing
  - ❑ Relaxes absolute to relative phase and polarization control
  - ❑ Mixing gain
  - ❑ Low cost and fast PIN photodiode may be used
  - ❑ Clock synchronization

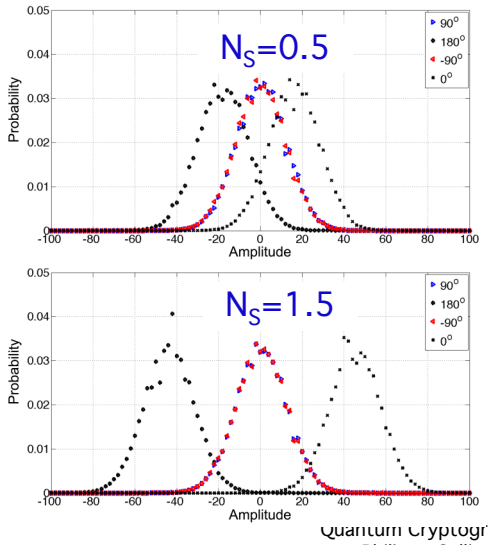
  Single fiber One way

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

Toward Quantum Security Engineering

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

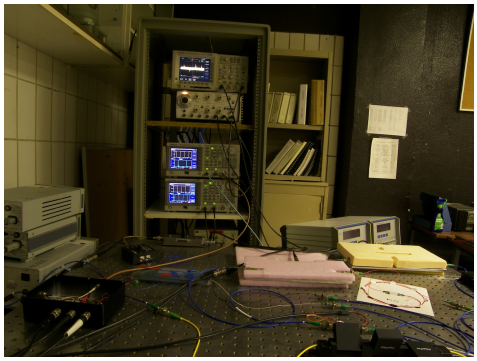
  ....To Quantum Cryptography system field deployment
- The state-of-the-art platforms in general are only proof of concept
  - Not fast enough : low generation key stream.
  - Not reliable enough : error correction is required
  - Not versatile enough :
    - Lack of compatibility between equipment
    - 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...

Future

- Infinite security means infinite cost and no interest
- Vulnerability & Price have a given product
- The worst case is never a certainty (Spinoza)
- Companies involved
  - SmartQuantum
  - ID Quantique
  - MagicQ....

- 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
- Now, what about the Edgar Allan Poe sentence ?



Thank you for the quality of your attention