QKD: from the concept to a commercial application

Hugo Zbinden
Groupe de Physique Appliquée
“Quantum Technologies”
Université de Genève

QKD concept
QKD state of the art (academic)
QKD academic and commercial challenges
QRNG concept to application
Steganography
What's Cryptography?

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

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

Security unproven

One-way functions
Integer factorisation

\[ 107 \times 53 = x \]
\[ 5671 = y \times z \]
Classical Cryptography

- based on Information Theory
  one time pad (Vernam)

plaintext : 001010010010011101010001101001
key: +101011011011001010100111010101
cyphertext: 100001001001010111110110111100

security proven

problem: key distribution
Quantum Key Distribution

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

QKD is proven information theoretically secure!
BB84 protocol (Bennett, Brassard, 1984)

Alice's Bit Sequence
0     1     0     -     0     1     1     1     1     -      1     0
-      1     -     -      0    1      -      -     1     -      1     0

Bob's Bases

Key

Bob's Results

Alice

Polarizers
Horizontal - Vertical

Diagonal (-45°, +45°)

Bob

H/V Basis

45° Basis

Bob
Eavesdropping (intercept-resend)

Error with 25% probability

\[ I_{AE} = 2 \text{ QBER} \text{ (quantum bit error rate)} \]
Eve attacks: information curves

\[ I_{AB} = 1 - H(QBER) \]

\[ H_b(p) = -p \log_2 p - (1 - p) \log_2(1 - p). \]
Incoherent attacks: information curves

\[ I_{AB} = 1 - H(QBER) \]

\[ I_{AE} = 1 - H\left(\frac{1}{2} + \sqrt{QBER(1 - QBER)}\right) \]

\[ I_{AE} = 2 \times QBER \]

Shannon Information

QBER
The steps to a secret key

- **Transmission of Qubits**
  - Alice sends quantum bits to Bob through a quantum channel.
  - **Quantum channel (losses)**

- **Reconciliation**
  - Basis reconciliation: Alice and Bob compare their basis to discard the sifted key.
  - **Sifted key**

- **QBER estimate**
  - Error correction involves estimating the QBER (Quantum Bit Error Rate).
  - **Error correction**

- **Privacy amplification**
  - Key generation: Alice and Bob use error correction to amplify the sifted key.
  - **Key**

- **Public channel**
  - Authentication: Alice and Bob use a public channel to authenticate the key.
  - **+ Authentication!!!**
Smolin and Bennett
IBM 1989
Swiss QCRIPT project (2013)
Efficient protocol
Finite key analysis
Low noise detectors
Low loss fibres

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

 sends an additional test state, \(|\alpha_1\rangle := |\alpha\rangle|\alpha\rangle\rangle\), to check for phase coherence between any two successive laser pulses. Therefore, phase coherence can be checked in any of these sequences, \(|\alpha_0\rangle|\alpha_1\rangle, |\alpha_0\rangle|\alpha_1\rangle, |\alpha_1\rangle|\alpha_1\rangle, |\alpha_1\rangle, |\alpha_1\rangle|\alpha_1\rangle\), by using an imbalanced
Ingredient 1: efficient and simple QKD scheme

**Coherent One Way (COW) Characteristics**

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

**ALICE**

- Key distillation engine
- Random number generator
- CW laser
- Intensity modulator
- Optical attenuator

**Bob**

- QBER
- Visibility
- Monitoring interferometer
- Key distillation engine

Reveals action of eavesdropper
Input for key distillation

check of coherence between qbits
Ingredient 2: tight finite key analysis

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

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

Solid red: New tail inequality
Dashed blue: Previous tail inequality
Ingredient 3: low noise single photon detectors

System requirements:
- Low dark count rate of SPD
- Compact (no SNSPD)
Ingredient 4: Low Loss Optical Fibres

Total attenuation of an optical fiber:

\[ \alpha = \alpha_{RS} + \alpha_{IR} + \alpha_{UV} + \alpha_{TM} + \alpha_{OH} + \alpha_{IM} + \alpha_{BL} \]

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

Submarine applications

- Vascade® EX3000 150 μm²
- Vascade® EX2000 112 μm²
- Vascade® EX1000 76 μm²

Terrestrial applications

- SMF28®ull 80 μm²
- SMF28®Ultra 80 μm²
- SMF28®e+ 80 μm²

© 2015 Corning Incorporated
….putting all together:

**FPGA is essential!**
Results: Secret (finite key) rates vs distance

$\varepsilon_{QKD} = 4 \times 10^{-9}$
Stability over 70h (200km)

Automatic tracking:

QBER

Temporal alignment: *Quantum signal clock recovery with 10 ps resolution*

Extinction ratio: *Modulator bias voltage*

Visibility

*Adjust Laser current (wavelength)*
Current developments

- Make it smaller (ATCA Telecom standard),
- Make it cheaper (integrated optics)
- Make it faster
- longer distances (quantum repeater, satellite)
Commercial Quantum Cryptography System Hacked

Physicists have mounted the first successful attack of its kind on a commercial quantum cryptography system.
Researchers crack the world’s toughest encryption by listening to the tiny sounds made by your computer’s CPU

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

4096-bit RSA

Pillars of Cryptography

Public Key Cryptography
- Security
  - Assumptions on difficulty of mathematical problems
  - Universality of classical computer model
  - Correct Implementation

Quantum Key Distribution
- Quantum Physics
  - Correct Implementation

QKD cannot be broken, but a specific implementation can!
Quantum Correlations for Device Independent Quantum Key Distribution

Bell violation guarantees entanglement independently of the device!

It is crucial to close the detection loophole!

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

Bell test without detection loophole, conditioned on the heralding signal

PRL 105, 070501 (2010)
Without a Single Photon Sources on demand, DI-QKD is completely unrealistic.

P(1) = 95%, Repetition rate 10 GHz
Measurement Device Independent (MDI) QKD

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

Lo et. al., PRL 2011
Where are the limits?
What’s the device? What’s the secure office?

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

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

What are the concerns of a QKD company?
ID Quantique

Swiss company, founded 2001, based in Geneva.

World leaders in Quantum-Safe Crypto.

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

Photon Counting

Quantum-Safe Security

Random Number Generation

Services

Technology
Quantum-Enabled Network Encryption: Today

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

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

![Quantum Channel - Dark Fiber or multiplexed](image)

![Local Area Network](image)

![Quantum key server](image)
QKD Dual Key Agreement

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

- All digital assets of bank pass over over DCI link.

Supports AES 256 bit key exchange every hour, with additional quantum key buffer.

Quantum channel:

- Both on dedicated dark fibre (up to 100km).
- Or multiplexed with data over single fibre (up to ~30 kms).
QKD in Data Centers for Financial Companies

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

- Why RNG?
  Game/Simulation/Classical Cryptography (RSA, DSA ...)/Quantum Key Distribution

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

- Why Quantum RNG?
  Random classical noise could be predictable
  Possibility to estimate/certify the entropy
Realisations of QRNGs

- using single photons

Rate: 4 Mbit/s per module
Evaluation and Certification

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

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

- **National Security Government Agencies**
  - Focus: Physical Principle, Implementation
  - Products covered: Component
• Exploiting photon statistics (shot noise)

\[ \langle n \rangle = N \times P_{\text{det/pixel}} + \text{Noise} \]

\[ \sigma_n = \sqrt{N \times P_{\text{det/pixel}} + \sigma^2_{\text{Noise}}} \]

If \[ N \times P_{\text{det/pixel}} \gg \sigma^2_{\text{Noise}} \]

Possibility to extract quantum randomness

Example with a Nokia N10

Application of shot noise: Quantum Secure Steganography

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

Bruno Sanguinetti, Giulia Traverso, Jonathan Lavoie, Anthony Martin, and Hugo Zbinden

1 Group of Applied Physics, University of Geneva, Switzerland
2 Fachbereich Informatik, Technische Universität Darmstadt, Germany

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

Disclaimer: We are physicists....
What is Steganography?

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

Alice

Cover-image C → stego-image S

Cleartext T

Bob

stego-image S → Cleartext T
• Steganography exploiting shot noise

Example with a Nokia N10

Naive idea

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

Simulated Histogram of the pixel values of a homogeneous area
Better idea

- Take photographs of a static object in rapid succession

Assumptions:
1. State of object and camera unchanged between consecutive pictures $K$ and $C$
2. Each pixel is statistical independent (no crosstalk).

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

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

$S$ cannot be distinguished from any real photograph
Private key steganography

Step 1: key exchange
- Alice
  - A
  - B
- Key-image over private channel
- Bob
  - A

Step 2: message exchange
- Cleartext
- Stego-image published
- Cleartext
Experimental realisation

- Tests with scientific mono-chrome and consumer colour cameras with raw image files
- 8 Mpix 16 bit tiff files
- error-correction applied (Reed-Solomon code)
Results

- It works!
- No cross-pixel correlations
- Stability depends on experimental situation
- Colour camera needs more investigations
- Works also for jpeg files (less bits can be hidden)
PhD positions available!