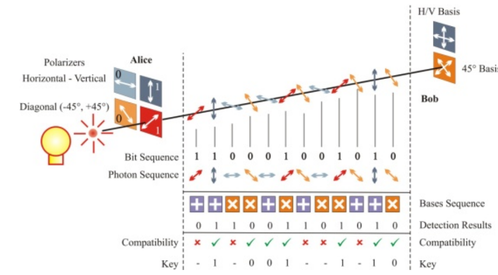
Hints for QKD Industrialization

J. Dávila, D. Lancho, J. Martínez & V. Martín
Research group on Quantum Information and Computation
Facultad de Informática, Universidad Politécnica de Madrid, Spain
http://gcc.ls.fi.upm.es/

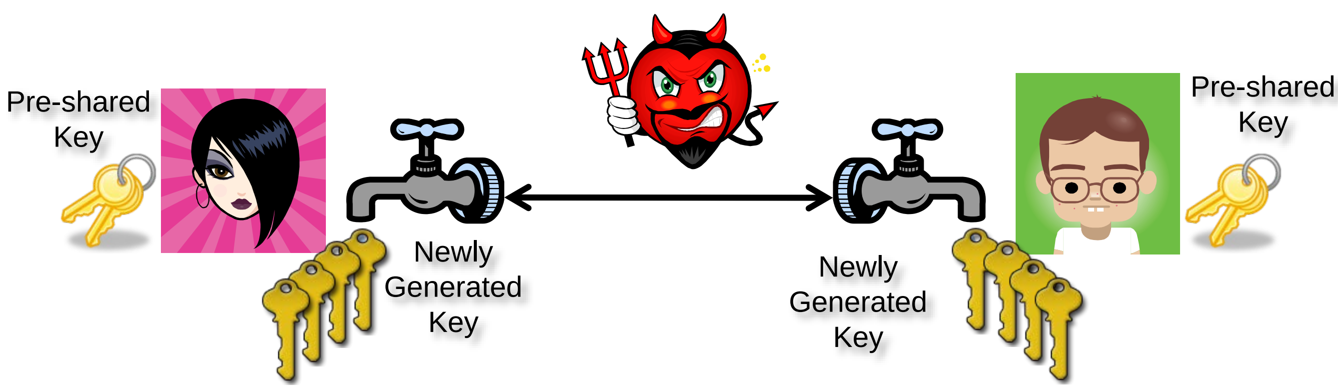
QKD Essentials

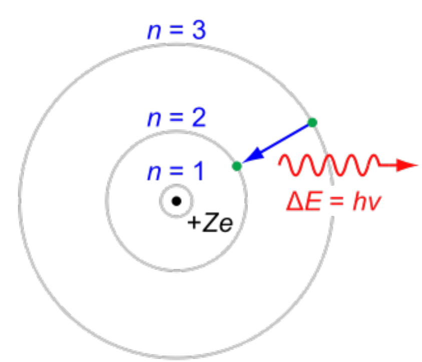
- Quantum Cryptography was born in 1984 with the BB84 protocol.
- **Quantum Cryptography** and **Quantum Key Distribution** (**QKD**) as synonymous.
- From CC, QKD is a **Symmetric Key Agreement Protocol** that requires previous **authentication**.
- QKD grows a pre-shared secret among two parties, QKD is referred as **Quantum Key Growing**.



In QKD, quantum properties of nature guarantee the privacy of the generated key.

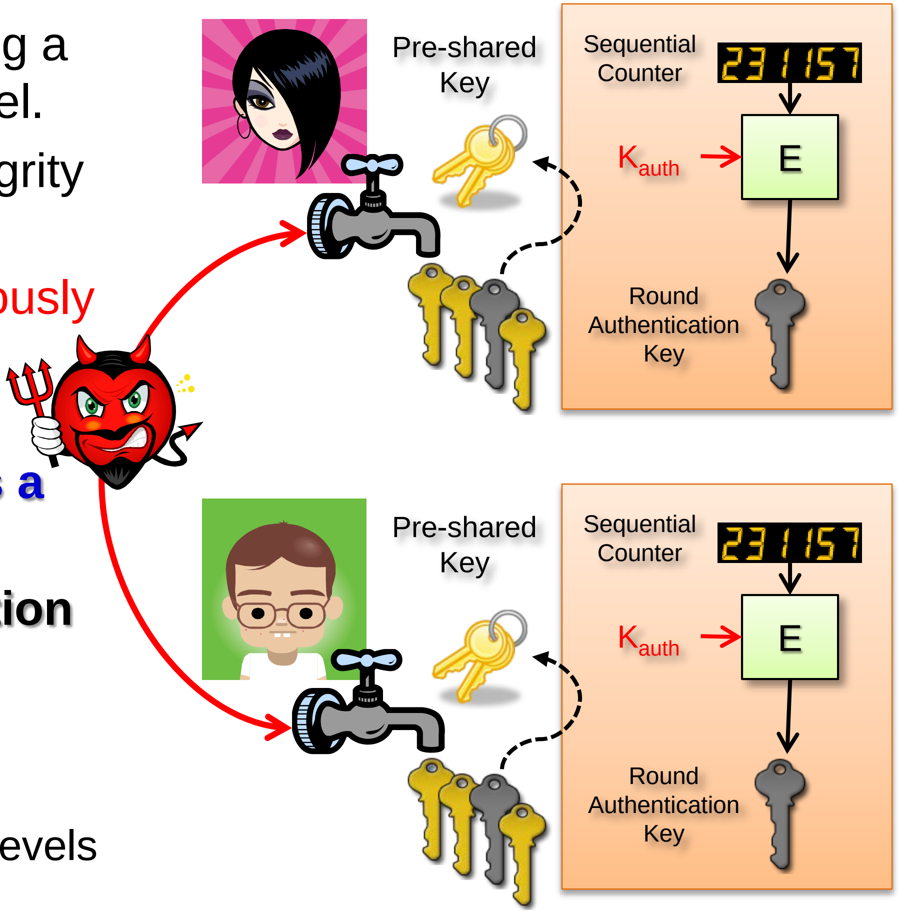
$$\Delta p \Delta q \geq \hbar/2^{*}$$





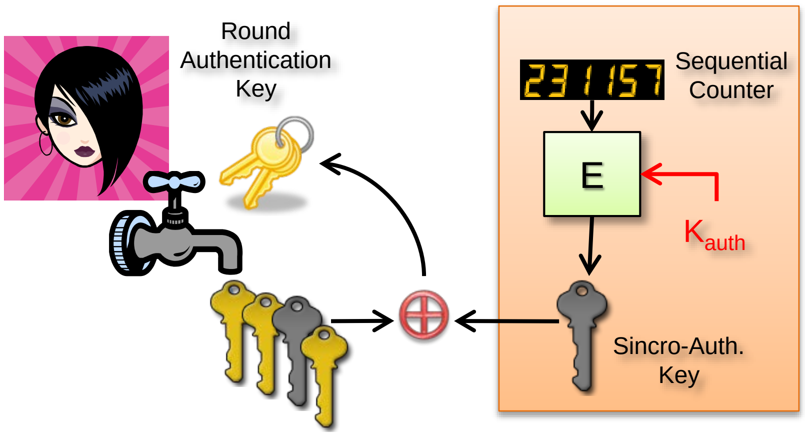
Separation of Duties

- Authentication is only required during a round execution in the public channel.
- This authentication assures the integrity of the protocol.
- In current proposals, part of a previously shared key is used to **assure the integrity** of the next protocol round.
- ***Isolation of different processes is a well-known practice in CC.***
- **Integrity Control** and **Key Generation** are two fundamentally different processes that should be kept separated.
  - As in MILS (Multiple Independent Levels of Security/Safety).



The Authentication Chain

- Authentication can be done using conventional solutions (**synchro-key generation**).
- Simple conventional integrity control techniques well regarded in practice, like seeding a **Pseudo Random Number Generator** (**PRNG**) with an initially shared secret.
  - Robust and demand only a small secret to run for a long time.



A simple **XOR** among the strings obtained by PRNG and the Quantum Key used for the same purpose would provide the best of both worlds.

Key Management

- Key management is **essential** for any security infrastructure.
- Key material is needed for **confidentiality**, **authentication**, **identification**, **initial values** & **nonces**, **transfer protocols**, …

- Proven theoretically secure under **simple assumptions** cannot be backed by an implementation under any known **industrial process**.
- Unfortunately, any error in any step will compromise the key security / secrecy.

Generation

Exchange

Storage

Safeguarding

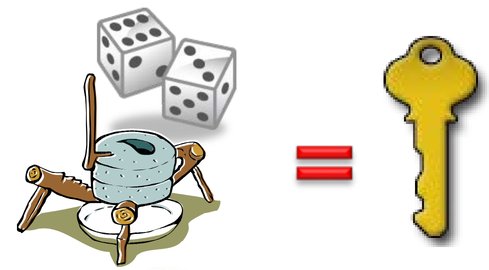
Use

Strengthening

Vetting

Replacement

Destruction

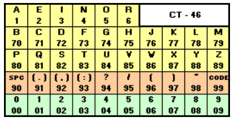


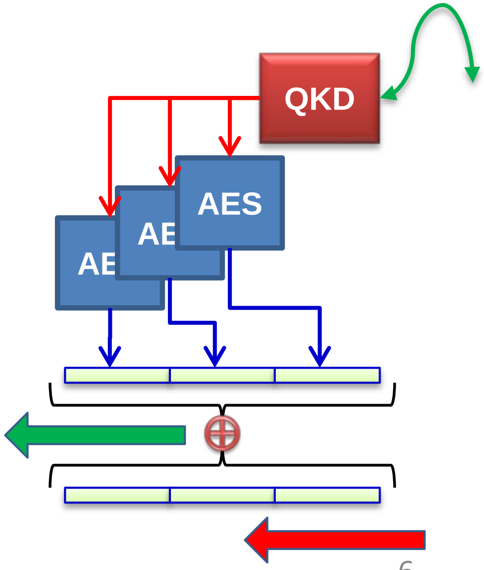
KYK-13

OTP Cipher

- The most commonly cited potential use for QKD keys is the **Vernam-Mauborgne cipher**, but probably **it would be one of the least used**.
- It allows the encryption of a message with informational-assurance of the confidentiality.

- Surely, in order to encrypt large amounts of data through a shared link, AES would be much more likely.
  Even for a high speed channel, **changing the key a few times per hour** may be enough to obtain a much higher security than the attained nowadays.





The Unfeasible Perfection

- The **widely spread illusion** that QKD could achieve **perfect secrecy** in **real applications** is flawed.
- QKD marketing has two major mistakes:
  1. **Excessively triumphant** views.
  2. QKD solves only one part of the information protection process: secret sharing. QKD covers only a **small part** of the whole security market.
- Wrong marketing could lead to the **early dismissal** of QKD by most security practitioners.
  – QKD is relegated to an immature technology status.
- QKD devices require to be **marketed and tested in competition** with other conventional technologies.
- This competition includes: security level, reliability, usability, interoperability, cost/benefit, etc.

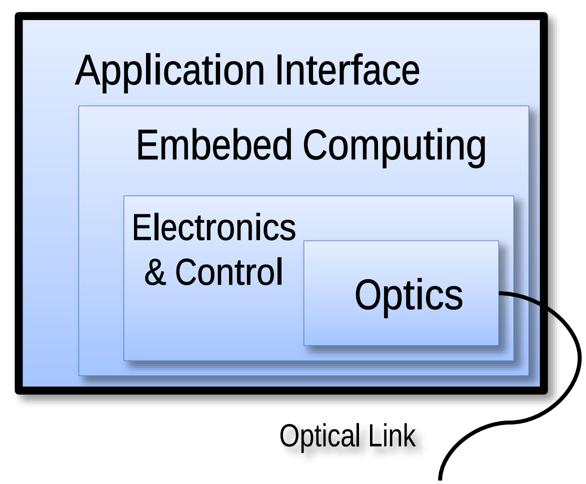
Security Market is not Empty

- A lot of technologies try to fulfill the needs of Security Market.
- **Absolute Security** is not really an interesting goal to pursue in itself.
  - Security is a general quality of the system that is built up over many components.
  - Strengthening one of them not necessarily makes the full system more secure.
- Application needs dictates the security level.
- Often, **usability**, **reliability**, **interoperability** and **costs** are as relevant as security needs.
- It is necessary to **build trust on the final user**:
  1. Intensive and detailed independent evaluation.
  2. Strict quality control, and certification.
  3. Good acceptance by the insurance companies.
  4. Adequate information campaigns to market this (new) security product.

"98% of the useful information is collected before it gets encrypted"
NSA

Security Certification

- Security certification of real systems is expensive and challenging, but **absolutely necessary**.
- **ETSI** is working on an standard oriented to the **QKD certification**.
- These works are based on a well-known security standards: **FIPS 140-3** and **Common Criteria**.
- Certifications is routinely applied to all kinds of electronic devices.
- Security Certification concerning the QKD Optical subsystems is an unexplored field to be addressed.

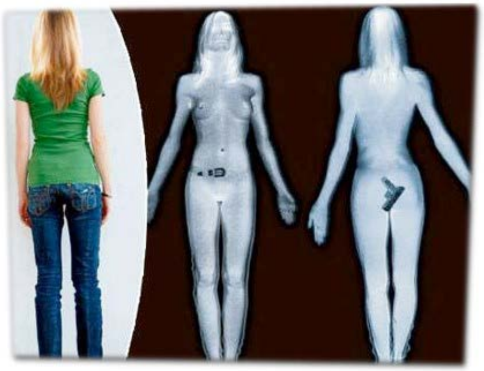


QKD Standardization (I): Scope

- What is needed?
  1. A complete enclosure of **physical protection** around the QKD module.
  2. **Sensors** to detect any intrusion.
  3. Mechanisms to respond in time, to all unauthorized attempts of physical access, resulting in the **immediate zeroization**.

QKD Standardization (II): Basics

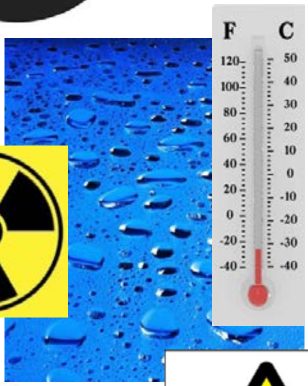
- **Enclosures** must be **opaque** to all visual and non-visual radiation examination, even when the module is inactive.
- **Tamper detection** and **zeroization** circuitry is protected against disablement.
- Authentication must require at least **two-factor authentication** for operator authentication (secret password, physical key or token, biometric, etc.).
- Access and module operation must require **identity-based authentication** mechanisms that enhance a role-based organization.



QKD Standardization (III): HW

- Modules must be **protected against environmental conditions** or fluctuations outside of the module's normal operating ranges
  - Deviations can be an attack, and it will increase the module failure probability compromising the module security and its operation.
  - Some magnitudes to control: darkness, temperature, voltage, pressure, humidity, atmospheric chemical composition, mechanical vibrations and the presence of nuclear and any other ionizing radiation.

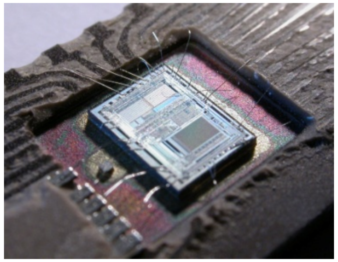


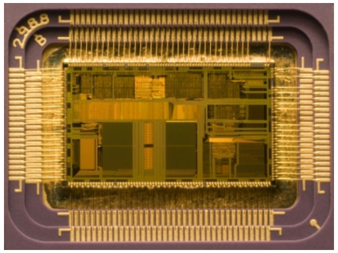



- All QKD modules require the protection of Critical Security Parameters against **Timing Analysis attacks**, Simple **Power Analysis**, Differential Power Analysis attacks and **Electromagnetic Emanation Attacks**, etc.
- The module must have a clear indication that the module is **operating in an Approved Mode**.

QKD Standardization (IV): HW

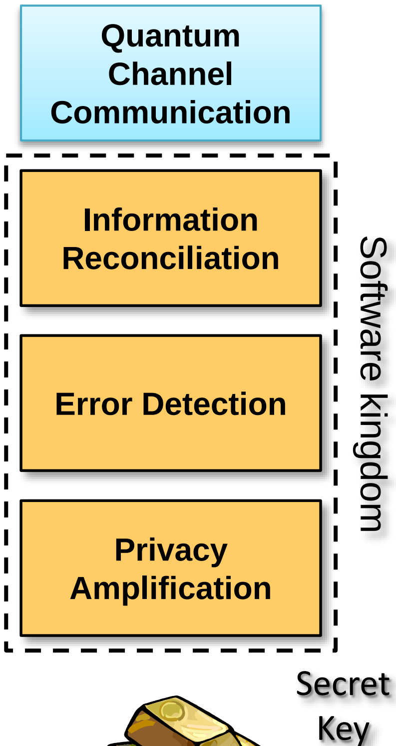
- QKD modules include microcontrollers, memories, buses and many other elements common to the **general microelectronics market**.
- **QKD modules cannot be safer than the software that runs inside them** and controls all their functionalities.
- **Every software module that can be reprogrammed**, updated or maintained inside a QKD module has to be specially protected because its **integrity must be guaranteed** all along the module service.
- Using **general purpose hardware** and software components the final cost is lowered and maintenance is easier, but it can also introduce **security breaches** in the system.





QKD Standardization (V): Software

- Software is responsible of almost everything, QKD modules require **specific purpose software** to:
  1. Implement the Quantum Protocols.
  2. Control the optoelectronic hardware.
  3. To be responsible of the administrative and operational interfaces.
  4. Checks that everything is working properly.
  5. Verifies in real time the integrity of the security perimeter.
- Software security is a **security upper bound** in a QKD system.
- Software is the most important part of a QKD system, and the most difficult to certify.



QKD Standardization (VI): Software

- Software must be **secure by design**, has to be **evaluated**, **inspected** and **certified** at a high level of security.
- The design of every QKD module has to be:
  - Verified by a **formal model** and by
  - **Informal proof of correspondence** between the formal model and the functional specification.

- This is of particular importance, not only with the software part of the system, also with **the correctness of particular the quantum protocols implemented**.

Security Levels

- Security and risk always go together.
- Security has to be as **multi-valuated** as the risk is in real scenarios.
- Is it worth to see if QKD technology can provide **different security levels** with **different costs** using **different technologies** or settings**?**
- Flexibility is **desirable** to meet the different demands of the various potential markets.





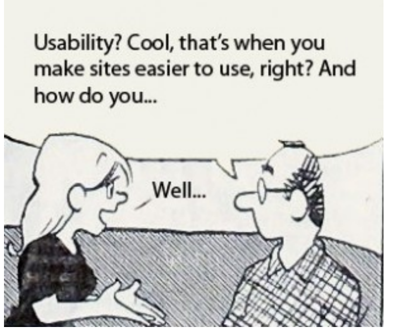
QKD Security Certification

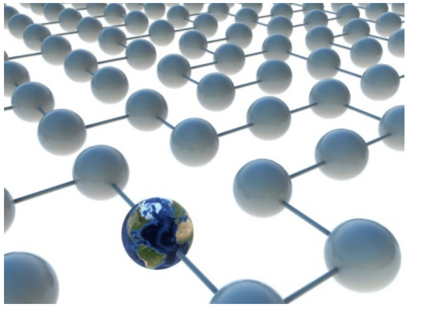
- **Security certification is not the holy grail**.
- Common Criteria higher levels do not necessarily equate with higher security, but claims have been more thoroughly evaluated.
  - For instance, Windows XP is EAL4+ certified, despite the continuous patches needed due security failures.

- **The set of claims for QKD must be carefully crafted to be meaningful for the intended market.**
- Certification translates QKD jargon and claims to the language used by its potential customers.

Usability & Interoperability

- **Usability** and **interoperability** are essential requirements for the QKD success.
  1. QKD systems will be probably introduced in **an already deployed platform**.
  2. Usability and Interoperability are as essential as the perceived security increase.
  3. QKD devices generate keys to be used outside the QKD device itself, into an **Electronic Key Management System** (EKMS) or **fill device** that will distribute it for its final use.
  4. QKD equipment has to be fully compatible with all key management systems it wants to connect to and to operate with.
- QKD systems have to be interoperable with all the systems they will work with.





Interoperability as a concept would imply moving directly from one world to another

Conclusions

- **Separation of duties**: **integrity control** and **key generation** are two fundamentally different processes.
- Some **QKD claims to be revised**: the use of **OTP cipher** or **absolute security** among others.
- **Security market is not empty**.
- **Security certification is absolutely necessary**, but it does not imply high security.
- Software security is probably a **security upper bound** in a QKDS.
- **Usability** and **interoperability** are essential requirements for the **QKD success**.

- QKD still has a **long way** to its industrialization.

Thank you for your attention ;-)

Bibliography

1. J. Davila, D. Lancho, J. Martinez, V. Martin (2009), "*On QKD Industrialization*", in **First International Conference on Quantum Communication and Quantum Networking** (QuantumComm 2009), Workshop: Quantum and Classical Information Security, October 26-30, Naples, Italy, LNICST, vol. 36, pp. 297-302.