Applied cryptography with quantum, post-quantum and traditional insights. A popularisation talk

UCA–Singapore Workshop

Bruno Martin

I3S Laboratory (CS), Université Côte d'Azur

June 19–22, 2023

Quizz

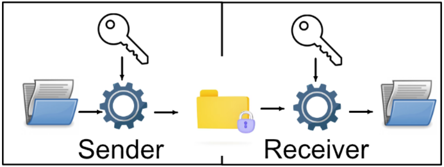
In current Internet secured protocols (`https`, `gpg`, `S/MIME`), do you think the data is encrypted with:

- ☐ Secret Key
- ☐ Public Key
- ☐ Other

Correct answer:

Hybrid Encryption (Other)

Secret Key Cryptography



- Stream cipher (Vernam) ensures perfect security (Information theoretic)
- Blocks chaining encryption (AES-256-CTR) ensures semantic security (complexity theoretic)

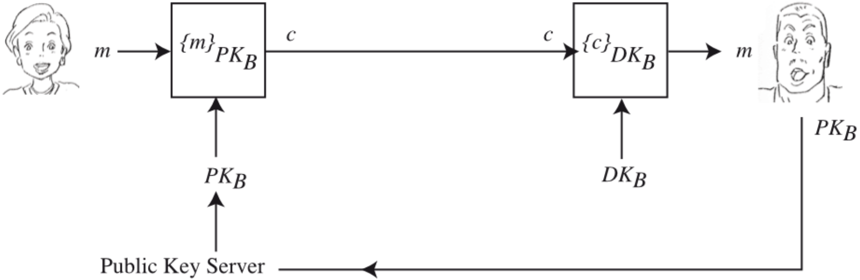
Pros:

Cleartext and Ciphertext are about the sime size ; quick computation

Cons:

Secret Key transmission

Public Key Cryptography



Basically RSA encryption (with padding schemes) or ciphers based on number theory problems (factoring, discrete log.)

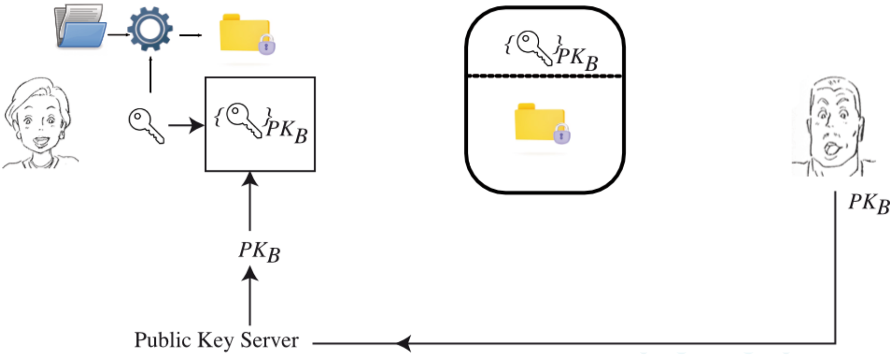
Pros:

Public key transmission

Cons:

Slow computation (factor 4k); Ciphertext's size larger than cleartext

Hybrid Encryption



Pros:

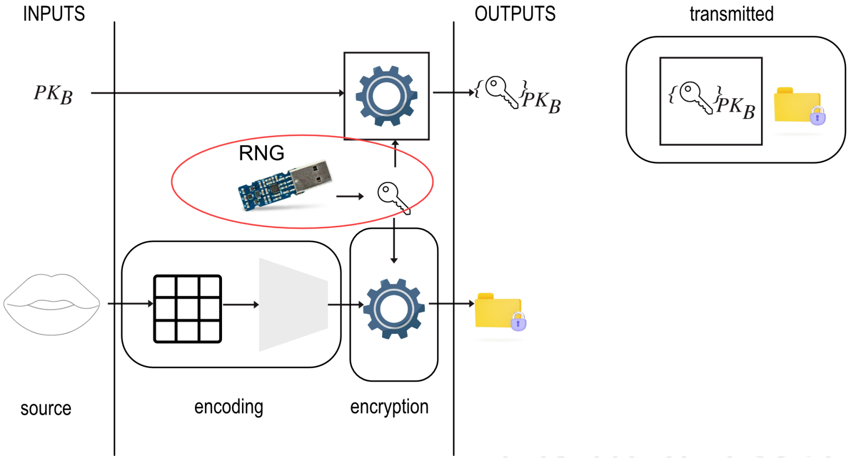
Public key transmission; Cleartext and ciphertext the same size; quick computation

Cons:

Not quantum safe. . . (Wait a bit)

Complete processing chain

Focus on RNG



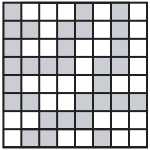
See [Krasnowski, 2021]'s PhD co-advised with J. Lebrun (Signal processing) for a complete processing chain

Random Number Generation

- TRNG: uses a nondeterministic source to make randomness. Random numbers come from measuring unpredictable natural processes (pulse detectors of ionizing radiation activities, gas discharge tubes, and leaky capacitors,...).
- QRNG: exploit elementary quantum optic processes that are intrinsically probablilistic to generate true randomness. Random numbers are a result of measurement on a quantum system.
- PRNG: runs an algorithm that uses mathematical formulas or algorithms to produce random numbers.

Random Generator (rule 30) – Example of RNG

t=0



[Wolfram, 1986]: given i, $\{x_i^t\}_{t \geq 0}$ is pseudo-random.
Used in Mathematica™.
Justified by Knuth's statistical tests.
Not suitable for cryptography; can be improved [Martin et al., 2014]

What is a binary random sequence?

A random sequence

- is unpredictable
- is uncompressible (there is no shorter program than the program which prints out the random sequence)
- passes all (effective) statistical tests

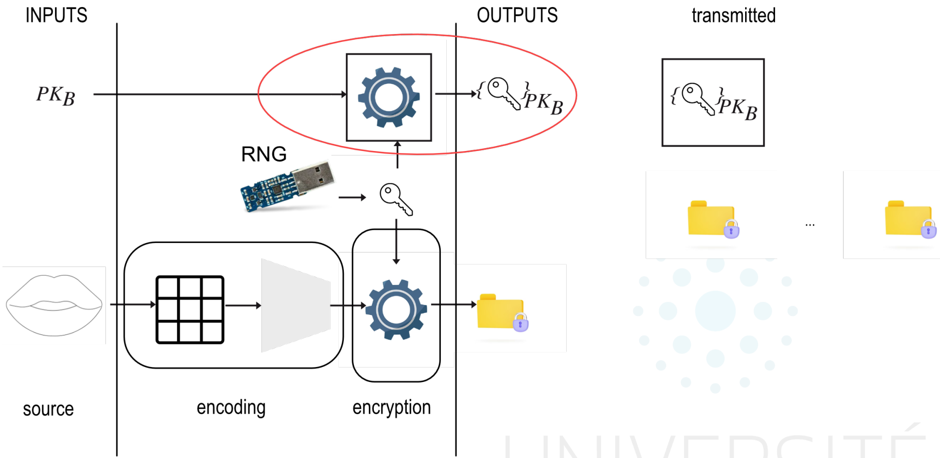
No program can generate a true random sequence, only pseudo-random. Random sequences are obtained by observing natural phenomenon.

Randomness definitions

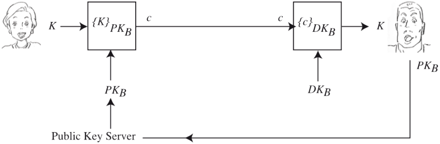
- TRS: a sequence that is unpredictable
- PRS: a sequence that cannot be distinguished from a TRS by any PPT algorithm.

Complete processing chain

Focus on Key Transportation

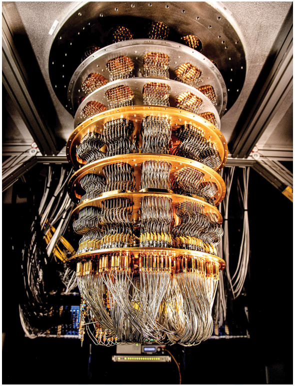


Key Transportation



- Today's PKC: RSA, DH, ECDH
- Based on number theoretic problems
- Increased importance of ECC

(co-advisor with A. Hirschowitz of a PhD on ECC [Virat, 2009])



- Shor's algorithm in QP
- Simon's Algo in QP
- 2300 qubits to break RSA-1024
- IBM Osprey: 433 qubits

HSP, Simon, Shor

Definition

Given G a group, $H \leq G$ a subgroup, X a finite set, $f : G \to X$ hides H if, $\forall g_1, g_2 \in G$, $f(g_1) = f(g_2)$ iff $g_1 H = g_2 H$.

Hidden Subgroup Problem

For a group G, X a finite set, $f : G \to X$ hides $H \leq G$.
Given f by an oracle using $O(\log |G| + \log |X|)$ bits and using evaluations of f via its oracle, determine a generating set for H

- [Simon, 1997] exhibited a quantum algorithm that solves Simon's problem (a special case of HSP)
- [Shor, 1999]'s quantum algorithm for factoring and discrete logarithm computing relies on the ability of quantum computers to solve the HSP for finite Abelian groups.

Going Post-Quantum

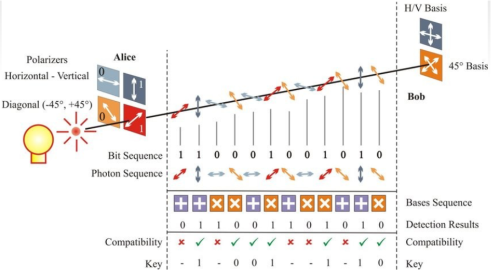
Replace traditional PKC

- Shor's and Simon's algorithms solve in quantum-polynomial time:
  - Integer factorization. RSA is dead.
  - The discrete-logarithm problem in finite fields[1]. DSA is dead
  - The discrete-logarithm problem on elliptic curves. ECDH is dead
- **Post-quantum crypto** must resist attacks by quantum computers
- Replace RSA, DSA, ECDH by new standards
- Current standards (2022) rely on the problem **Learning With Errors** over arithmetic lattices.
  - CRYSTALS-Kyber for encryption (keysizes: pk=1184, dk=2400, block=1088)
  - CRYSTALS-Dilithium for signatures
- In use: OpenSSH, Cloudflare, AWS, IBM backup device

[1] DLOG computation requires half the number of qubits required to factor an integer of the same size

Going Quantum

Remove PKC



Key transportation with [Bennett and Brassard, 1984] or [Ekert, 1991]. Nice survey [Pirandola et al., 2020] (approx. 200p)

Pros:

Highly secure

Cons:

Slow throughput; relatively small distance; requires two channels

Goal achieved

Key transportation

Different ways to transport a secret key.
Either with

- PQC
- QKD

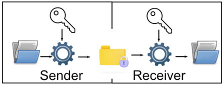
First step

Alice and Bob share a key !

They can use it to encipher a message

Secret Key Cryptography

Stream cipher (Vernam)



A and B share a random sequence of n bits: the secret key K.
A enciphers M of n bits in $C = M \oplus K$. B deciphers C in $M = K \oplus C$.

Example

$M = 0011, K = 0101$
$C = 0011 \oplus 0101 = 0110$
$M = K \oplus C$.

Pros:

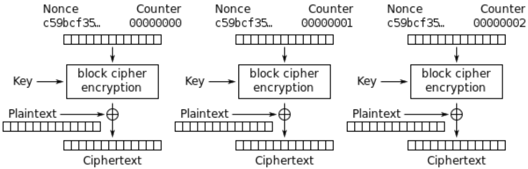
Quick ; high throughput ; perfectly secure

Cons:

Long and perfectly random key ; not reusable

Secret Key Cryptography

Blocks chaining encryption (AES-256-CTR)



Counter (CTR) mode encryption

Pros:

Quick ; high throughput ; short key ; semantic security ; quantum safe

Cons:

not perfectly secure

Quantum attacks against SKC

Searching the key uses [Simon, 1997]'s or [Grover, 1996]'s algorithms.

Grover's algorithm

Search an element among n items requires time $n/2$ on the average or time n in the worst case with a classical computer. It can be done in $\sqrt{n}$ steps on a quantum computer.

Pros:

Up to 4 qubits required (for Grover)

Cons:

Exponential algorithm (square root speedup compared with brute-force.)

Security Notions

- **Perfect security** is about confidentiality against arbitrary adversaries. It is based on information theory. It can be achieved with Vernam Cipher with a TRNG or QRNG
- **Semantic security** is about confidentiality against computationally bounded adversaries. It is based on complexity theory and the adversary is a PPT algorithm. It can be achieved with PRNG
- **Quantum safe** is about confidentiality against computationally bounded adversaries. It is based on complexity theory and the adversary is a quantum algorithm

Goal achieved

Encryption

Different encryptions to secure a message

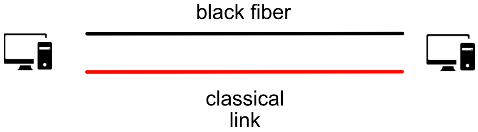
- Vernam cipher to achieve perfect security
- Traditionnal ciphers to achieve quantum safety (with a key large enough at least 256 bits)

Second step

Alice and Bob can communicate securely !

Going further

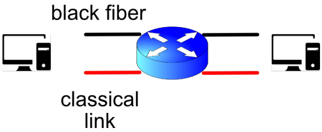
Direct connection



- When both quantum and classical links are available (150km).
- QKD can be achieved and the key used to encipher data (with perfect security or quantum safety)

Going further

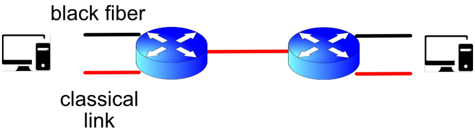
Indirect connection – 1 hop



- When both quantum and classical links are available between end systems interconnected with a single router
- QKD can be achieved between end systems and the router
- A protocol has to be designed to generate and transport a key
- Quantum safe encryption can be achieved (or better ?)

Going further

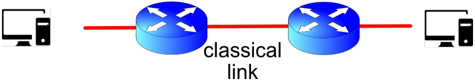
Indirect connection – many hops



- When both quantum and classical links are available between end systems and routers interconnected with a classical link
- QKD can be achieved between end systems and routers but not inbetween.
- A protocol has to be designed to generate and transport a key
- Quantum safe encryption can be achieved

Going further

Classical link



- When no quantum links are available
- Key transportation has to be done with post-quantum cryptography
- Quantum safe encryption can be achieved

Integration

We intend to integrate the previous cases in standard librairies to secure

- IP layer with IPSec
- TCP layer with TLS, which ensures security of classical Internet protocols (`http`, `smtp`, `imap`,...)

with different levels of security.

Thanks for your attention

References I

Bennett, C. and Brassard, G. (1984).
Quantum cryptography: Public key distribution and coin tossing.
Theoretical Computer Science, 560:7–11.

Ekert, A. (1991).
Quantum cryptography based on Bell's theorem.
Physical Review Letters, 67(6):661–663.

Grover, L. K. (1996).
A fast quantum mechanical algorithm for database search.
In ACM, editor, *STOC'96*, pages 212–219.

Krasnowski, P. (2021).
Joint source-cryptographic-channel coding for real-time secure voice communications on voice channels.
PhD thesis, Université Côte d'Azur.

Martin, B., Formenti, E., Imai, K., and Yunès, J.-B. (2014).
Advances on random number generation by uniform cellular automata.
In Calude, C., Freivalds, R., and Kazuo, I., editors, *Computing with New Resources*, volume 8808 of *LNCS*, pages 56–70. Springer Verlag.

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., and Wallden, P. (2020).
Advances in quantum cryptography.
Adv. Opt. Photon., 12(4):1012–1236.

Shor, P. W. (1999).
Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
SIAM review, 41(2):303–332.

References II

Simon, D. R. (1997).
On the power of quantum computation.
SIAM J. on Computing, 26(5):1474–1483.

Virat, M. (2009).
Courbes elliptiques sur un anneau et applications cryptographiques.
PhD thesis, Université Nice Sophia-Antipolis.

Wolfram, S. (1986).
Random sequence generation by cellular automata.
Advances in applied mathematics, 7:123–169.

UNIVERSITÉ CÔTE D'AZUR