RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Why Post-Quantum cryptography is the future of secure communications

Sébastien KUNZ-JACQUES

Deputy director, Expertise division, ANSSI, France

A BIT OF HISTORY

Secure Networks with symmetric cryptography

The only solution ≈ 1990 for “high security” networks, at least in France

Centralized, cumbersome key management…

…but possible if mostly fixed set of endpoints.

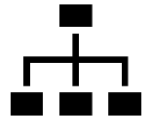
Quantum-safe! (mostly)

Some networks with purely symmetric cryptography still exist today.

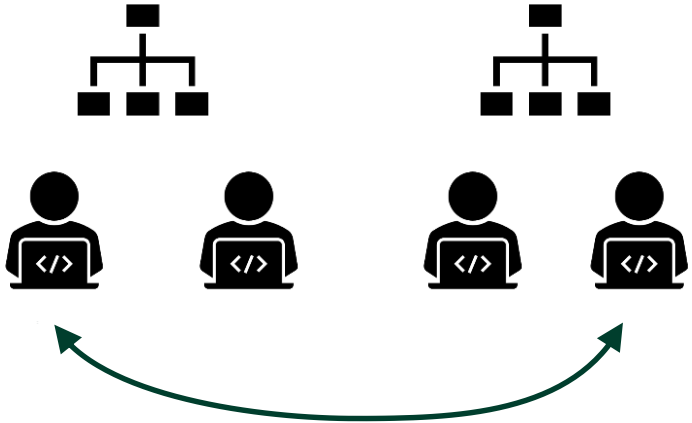
Public-key cryptography: enables decentralized trust

Public / private Key pairs

- do not directly protect data
- authenticate endpoints (machines, users, arbitrary entities)



Endpoint authentication can be delegated to intermediate certification authorities.



PKC is the only manageable way to provide end-to-end encryption in loosely coordinated networks

WWW : millions of endpoints

Large company with branches / multi-state network

THE QUANTUM COMPUTING PROBLEM AND CANDIDATE SOLUTIONS

Public Key Cryptography and Quantum Computing

Currently used PKC algorithms overwhelmingly based on problems broken by the Shor algorithm on a quantum computer.

Does not mean that QC breaks all PKC.

NIST standardization results due soon for post-quantum (i.e. QC resistant) key-exchange algorithms.

Hybrid use (pre + post Q) possible.

Quantum Key Distribution

Functionally equivalent to public key exchange.

Immune to purely computational attacks, classical or quantum :
Relies on physical effects to detect and quantify eavesdropping.

May be vulnerable to side-channel attacks,

but

ex post facto cryptanalysis is generally not possible, which is a good thing.

QKD: FOR WHICH APPLICATIONS?

Limitations of a hardware solution

Inherently hardware-based : endpoints are QKD devices

Range, routing, infrastructure

Range limitation; can be overcome by chaining links

- With no intermediate security (“trusted nodes”)
- Or in the future, with quantum relays

Physical security and cybersecurity of trusted nodes is a grave concern

Quantum relays may alleviate the end-to-end range limitation but

- Still routing-incompatible
- Intermediate nodes need to be managed and to be compatible with endpoints

Needs dedicated links or a carefully controlled “signal neighborhood”

Tradeoffs for classical cryptography choices

QKD relies on classical cryptography for

- Data encryption and authentication
- QKD signaling authentication

Two sensible choices:

- Unconditionally secure primitives for everything:
  the smallest attack surface, but extremely slow data exchange

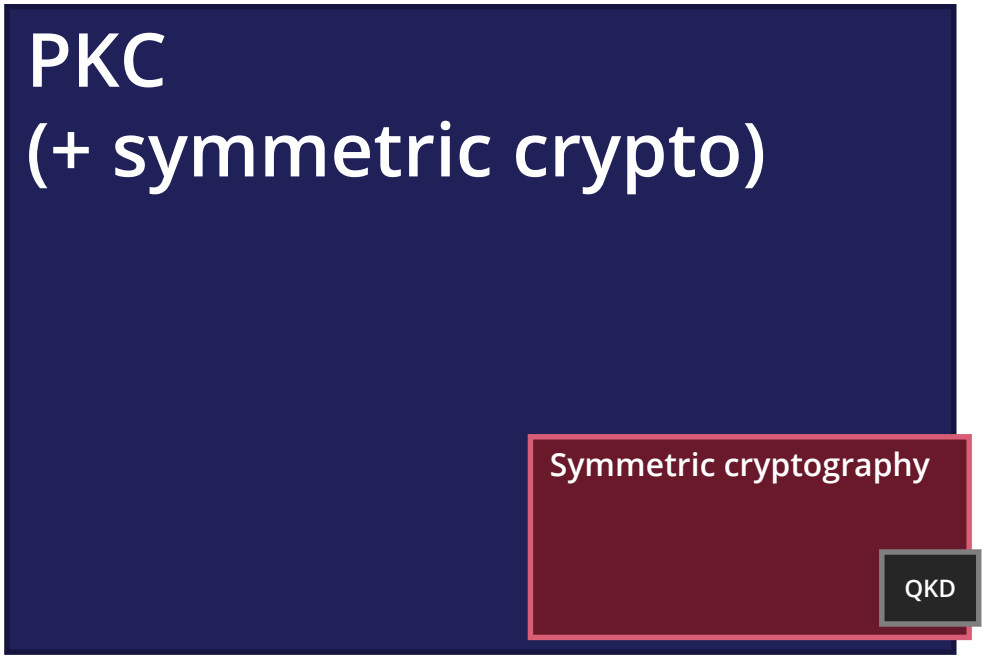
- Primitives based on symmetric cryptography:
  no performance limit, but assumptions not different from classical crypto devices

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

In short

	PKI-based cryptography	Purely symmetric cryptography	QKD with PKI-based signaling	Unconditionally secure QKD
Building blocks	Message encryption and authentication with symmetric cryptography. Keys provided by asymmetric key establishment algorithms authenticated with signatures using a Public Key Infrastructure (PKI).	Message encryption and authentication with symmetric cryptography. Keys initialized offline and possibly managed remotely.	QKD + symmetric cryptography for message encryption and authentication, with QKD keys; QKD signaling authenticated with hash-based signatures using a PKI.	QKD paired with unconditionally secure message encryption (i.e. One-Time Pad) and authentication, with QKD keys; QKD signaling authenticated unconditionally, with keys initialized offline and renewed by QKD.
Can be deployed over the Internet or private networks	Yes	Yes	No	No
Resists to quantum computers / to cryptanalysis advances	++	+++	+++	++++ No purely algorithmic attack is possible.
Resists to device/software hacking and side-channel attacks	Not in general. Implementation-dependent.			
Can easily scale; endpoints can evolve easily	Yes	No	No	No
Can provide end-to-end security	Yes	Yes	No	No
Can achieve high performance (e.g. 100Gb/s encryption)	Yes	Yes	Yes	No

Even shorter : use cases



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Thank you for your attention

https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/