Quantum Technologies Cyber Threat over Encryption Protocols & Mitigation Options

FRnOG 38 – 06/10/2023
AGENDA

- Introduction to Quantum Technologies
- Understand the Quantum Cyber Threat
- Quantum-based Mitigation Options
- Quantum-proof Mitigation Options
- Timeline(s) & Regulations
- PQC Migration Roadmap
Introduction to Quantum Technologies
What are Quantum Technologies?

When we harness Quantum Mechanics properties... ...to enhance today’s Technologies...

Quantum Superposition

Quantum Interference

Quantum Entanglement

...we get Quantum Technologies:

Computational Calculation

Secured Communications

Sensors and detectors

Quantum Computing

Quantum Communication

Quantum Sensing
Insight on Quantum Computing

Source: MITxPRO
Understand the Quantum Cyber Threat
Quantum Computing Threat on Cyber-Cryptography

**Symmetric Cryptography**

- AES
- SHA-2

Impacted by quantum computing, but we can mitigate by increasing key sizes (Grover's Algorithm 1996)

**Asymmetric Cryptography**

- RSA signatures
- Elliptic curve Diffie-Hellman key exchange

Can be solved efficiently by a large-scale quantum computer (Shor's Algorithm 1994)
How to break RSA encryption?

Classical computers have been able to break RSA protocols up to RSA-250 (829 bits keys equaling 250 decimal digits)

Key Generation
- 2 large prime numbers \( p \) and \( q \)
  - \( n = p \times q \)
- \( z = (p - 1)(q - 1) \)
- Choose \( e \) where \( 1 < e < z \)
  - \( d = e^{-1} \mod (p - 1)(q - 1) \)
- Bundle Private key pair \((n, d)\)
- Bundle Public key pair \((n, e)\)

Encryption
- \( \text{cipher} = m^e \mod n \)

Decryption
- \( \text{plaintext} = \text{cipher}^d \mod n \)

*Each logical Qubit (stable Qubit) equals 100 to 1000 physical Qubits (unstable Qubits)
Shor's Algorithm at work

1. Select a prime number $N$ to factorize. (ex. $N=15$)
2. Choose a random number $k$ between 1 and $N$ (ex. $K=7$)
3. Find $\text{GCD}(N, k)$
4. Find the smallest integer $r$ such as: $f(x) = k^x \mod N$, then $f(a) = f(a+r)$
5. Define a new variable $q=1$
6. Step 6 is performed by a Quantum Computer
Quantum Key Distribution (QKD):
- secure communication method for exchanging encryption keys only known between shared parties;
- based on properties found in quantum physics;
- uses a quantum system to protect the data, rather than relying on mathematics.

**Advantage**: The no-cloning theorem states that it is impossible to create identical copies of an unknown quantum state, which prevents attackers from simply copying the data in the same manner that they can copy network traffic today. Additionally, if an attacker disturbs or looks at the system, the system will change in such a way that the intended parties involved will know.
Challenges & Promises of Quantum Communication

**CHALLENGES**

- Integration of QKD systems into current infrastructure
- Distance in which photons can travel
- Difficulties in implementing infrastructure for QKD

**PROMISES**

Quantum Internet

Bob can store his entanglement with Alice in his lab while the other end establishes entanglement with Charlie.

A photon is transmitted through optical fibre and delivered to another device to establish an entanglement.
Quantum-proof Mitigation Options

(Post-Quantum Cryptography)
NIST Post-Quantum Cryptography Initiative

Evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms

- 5 years ago NIST initiated a project seeking “to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.”
- Currently in fourth round
- Even if one of NIST ‘finalist’ solutions is fully developed, tested and proven effective, it can never be fool-proof.

“We have no absolute guarantee of security for any cryptosystem. The best we can say is that after a lot of study by a lot of smart people, nobody has found any cracks.”
—Dustin Moody, NIST

<table>
<thead>
<tr>
<th>Public-Key Encryption/KEMs</th>
<th>Digital Signatures</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRYSALS-KYBER</td>
<td>CRYSALS-Dilithium</td>
</tr>
<tr>
<td></td>
<td>FALCON</td>
</tr>
<tr>
<td></td>
<td>SPHINCS+</td>
</tr>
</tbody>
</table>
Challenges of PQC Migration

- PQC protocols efficiency toward Quantum Computers
- Hardware implementation security issues
- PQC protocols adequacy to applications
Timeline(s) & Regulations
Forecast & Migration Timelines

Exhibit 1 - The Time Window for Upgrading Cryptographic Infrastructure Is Closing Rapidly

Sources: NIST Post-Quantum Cryptography timeline, BCG analysis.
Note: PQC: Post-Quantum Cryptography. NIST: National Institute of Standards and Technology USA.
1Based on NIST PQC timeline.
2Public Key Cryptography (up to RSA-2048).
Acknowledging the immaturity of PQC is important: ANSSI will not endorse any direct drop-in replacement of currently used algorithms in the short/medium term. However, this immaturity should not serve as an argument for postponing the deployments. ANSSI encourages all industries to initiate in the next months a gradual overlap transition in order to progressively increase trust on the post-quantum algorithms and their implementations while ensuring no security regression as far as classical (pre-quantum) security is concerned.

**What is the recommended post-quantum transition roadmap?**
To support a gradual transition, ANSSI encourages the following 3-phase roadmap (see below for a detailed description):

- Phase 1 (today): hybridation to provide some additional post-quantum *defense-in-depth* to the pre-quantum security assurance.
- Phase 2 (not earlier than 2025): hybridation to provide *post-quantum security assurance* while avoiding any pre-quantum security regression.
- Phase 3 (probably not earlier than 2030): optional standalone post-quantum cryptography.

ANSSI, January 4, 2022
This document is an update of ANSSI’s position on the post quantum cryptography transition in view of the recent advances in the topic. It should be read as an addendum to 2022’s publication [1]. We will detail our recommendations in terms of post-quantum algorithms and hybridization techniques.

ANSSI also decided to speed-up the original agenda. First French security visas for products implementing hybrid post-quantum cryptography are expected to be delivered around 2024-2025.

1. It is important to avoid modifying the parameters of the standardized instance.
2. The parameters are defined for several minimum security levels. We recommend to use the highest NIST security level as possible, preferably level-5 (i.e. equivalent to AES-256) or level-3 (i.e. equivalent to AES-192).
3. We recommend to use ephemeral keys as much as possible. The systematic use of ephemeral private keys allows to prevent many attacks like decryption failures ones.
4. We also recommend to use the actively secure version (IND-CCA) that will be standardized by NIST. There are some cases, like in provable authenticated protocols, where the passively secure (IND-CPA) version in static or ephemeral mode may still be secure. But an extra care must then be paid to make sure that no decryption oracle is available under any circumstance even in the case of side-channel attacks.

ANSSI, August 29, 2023
PQC Migration
Roadmap
Roadmap to Quantum-Resistant Cryptography

OUR FRAMEWORK TO ENHANCE YOUR QUANTUM RESILIENCE

Quantum Vulnerable
Uninformed or vaguely informed about Quantum basics and cybersecurity threats

Quantum Aware
Well informed about Quantum cybersecurity threats and possible mitigation solutions

Quantum Planner
Quantum cybersecurity plan defined, and Quantum resistant solutions selected to be adopted

Quantum Safe
Quantum resistant solutions successfully adopted and implemented in production

Quantum Cyber Risk Assessment

Quantum Cyber Inventoring

Quantum Cyber POC Migration

Quantum Cyber Strategy Planning

Quantum Cyber Awareness

Quantum Awareness

Quantum Safe

Maturity level