Briefing Note

Quantum Security

NOKIA

1 Overview

Quantum computing brings a totally new way of approaching computing. For many tasks, it is exponentially more powerful than the computers we are using today, and it can perform very complex tasks that would take normal computing millions of years. One of the tasks where quantum computing excels is in hacking encryption that is considered secure by today's standards. The concern with quantum computing is that it will be a serious threat to security, able to easily crack encryption codes and basically steal any data passing over the internet.

Is this threat credible? Yes. Can we do something about it? Absolutely.

This briefing note explains the essentials.

2 What is Quantum Computing?

Quantum computing can be a challenge to both explain and understand! But let's start on familiar territory.

In traditional computing, all data is stored as bits. Bits are binary, meaning they can be either a zero (0) or a one (1). Traditional computers use these bits to perform various tasks and produce understandable and deterministic output.

In quantum computing, information is represented differently, using qubits. Qubits can exist in a superposition of states, 0 and 1, until they are measured. Unlike classical bits, which are always in one state or the other, qubits can be in both states simultaneously. Additionally, qubits can become entangled, meaning the state of one qubit is linked to the state of another.

The unique properties of qubits – superposition and entanglement – allow quantum computers to solve highly complex problems much faster than traditional computers, while traditional computing remains more suitable for simpler problems and transactions.

An imperfect analogy is a coin toss. Imagine you have a regular coin (traditional computer) and a special quantum coin (quantum computer).

- **Regular coin:** This coin can only land on heads or tails, just like a bit in a traditional computer can only be a 0 or a 1.
- **Quantum coin:** This special coin, however, can be heads, tails, or both at the same time (superposition)! It's like the coin is spinning in the air and hasn't landed yet, but it has the potential to be either side.

This "both at the same time" trick lets quantum computers explore many possibilities simultaneously, which gives them a big advantage for certain problems.

Think of it like flipping multiple regular coins one at a time. It takes time to flip each coin and see the results. With the quantum coin, it's like flipping all the coins at once and seeing the possibilities for all of them together.

You can also have multiple quantum coins that are "linked" (entangled). If you know the state of one coin (heads), the other coin will instantly be the opposite (tails) no matter how far apart they are. This entanglement allows quantum computers to perform calculations in completely new ways.

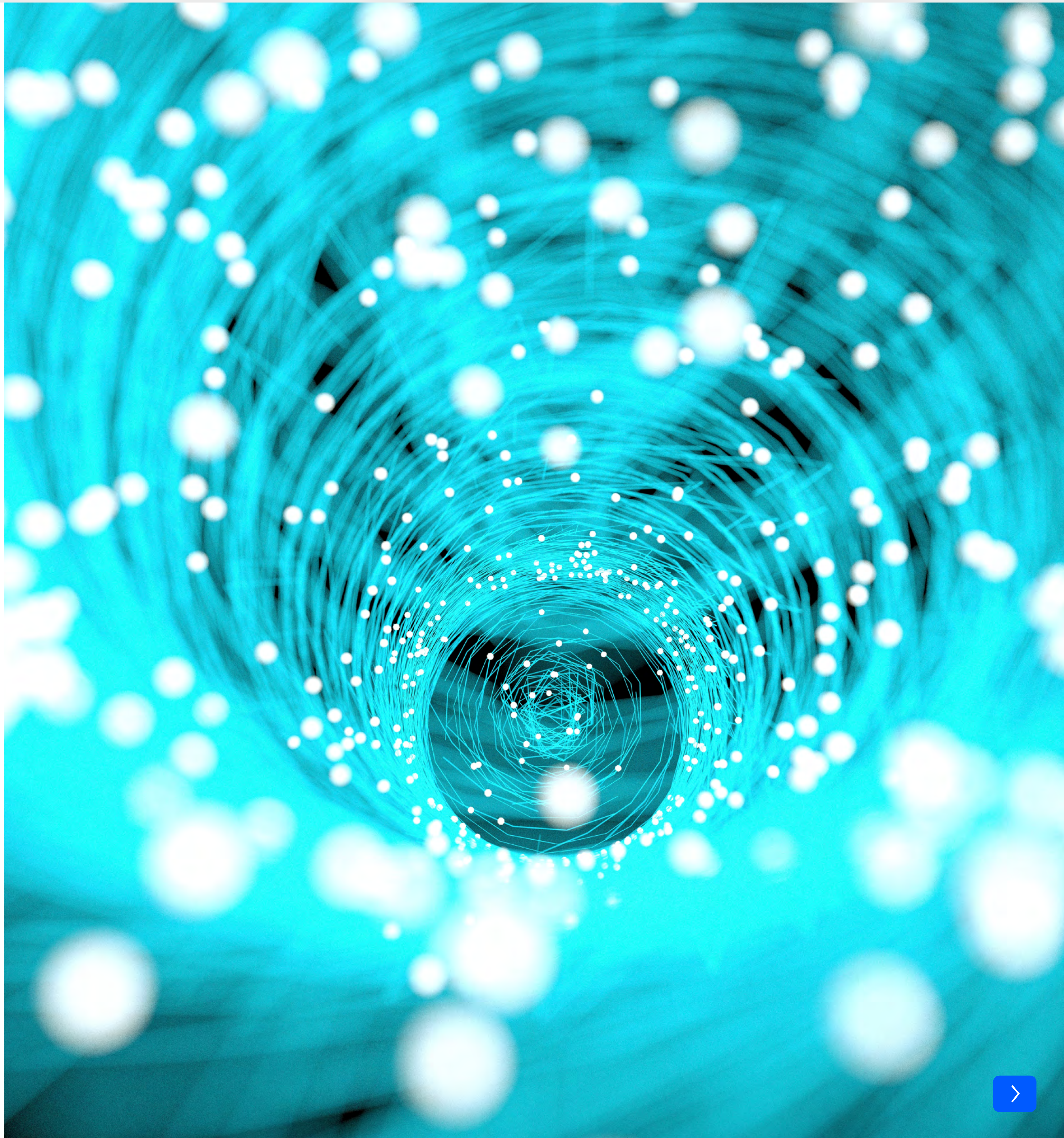
Quantum computers are ideally suited to exploring many possibilities at once, solving specific problems, searching unsorted databases, and running complex simulations. Hence the concern that they can be used to crack encrypted data.

3 What is the implication for PON networks?

PON networks are secure today, equipped with strong features that separate, encrypt, and protect data.

But in the post-Quantum era, current security methods could be at risk. While practical Quantum computers may still be years away, the “harvest now, decrypt later” threat is real, because hackers could capture encrypted data today and decrypt it once Quantum technology matures.

As PON networks increasingly support enterprises and other mission-critical services, it’s essential to begin preparing for Quantum-safe security features.



4 What is the mitigation?

The combined approach of secure locks and keys enables Quantum-resistant PON networks.

Secure locks are provided through encryption. PON networks use the well-known Advanced Encryption Standard (AES) algorithms, based on AES-128 and AES-256. Both are recognized by NIST (U.S. National Institute of Standards and Technology) as resistant to Quantum attacks. In addition, encryption keys are refreshed every hour, and control messages are carried separately within the PON encapsulation frame, ensuring they are also encrypted.

To ensure secure keys, PON technologies must guarantee sufficient entropy for generating true, random, and unpredictable keys. These keys must also be exchanged securely using methods such as out-of-band key exchange or pre-shared keys.

Combined, these techniques significantly strengthen PON security today and lay the foundation for future Quantum-resilient networks.

[1] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

5 How far away is the threat?

Predictions vary significantly as quantum computing faces two major challenges en route to widespread availability: accuracy and scalability. Errors stem from qubit instability and interference, restricting the qubit's superposition lifespan to milliseconds or microseconds. To manage this instability, precise cooling systems are necessary, often using cryogenic temperatures near absolute zero (-273.15°C or 0 Kelvin). However, achieving and maintaining such low temperatures poses significant engineering challenges and adds complexity to the overall system design. Consequently, scaling quantum computers is proving difficult due to the specific environment quantum computers require for operation.

6 Conclusion

PON networks already provide military-grade security, thanks to the security features mentioned: AES encryption for user traffic, which changes every hour; encrypted control messages in the PON encapsulation frame, and; message integrity checks. Today, they provide maximum protection against data being intercepted as well as maximum protection of the data itself.

With NIST having already defined a number of standard cryptography algorithms that are quantum resistant, we can be reassured that security of internet traffic is a step ahead of quantum computing.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID:214054

nokia.com

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.