Data protection and privacy in a quantum world

Sébastien Canard*[1]

[1]Télécom Paris – Télécom Paris, Télécom-Paris – France

Résumé

Cryptography is used daily to secure our data and our privacy. For this purpose, it relies on standards and mechanisms that have been known and mastered for many years. But today, it has to face an unprecedented threat: quantum computers. Under the initiative of the NIST, the cryptographic community has passed the last five years to propose and improve the so-called post-quantum cryptography. What is the situation today? Where do we stand?
We will see in this talk that if for basic mechanisms such as encryption and digital signature, everything is now on track, the case of advanced cryptography, especially to protect our privacy, is still very far from reaching the maturity of traditional cryptography.

*Intervenant