New Results on Quantum Symmetric Cryptanalysis

Maria Naya Plasencia*[1]

[1]INRIA – - – France

Résumé

The security of symmetric cryptography is completely based on cryptanalysis: we only gain confidence in the security of a symmetric primitive through extensive and continuous scrutiny. It is therefore not possible to determine whether a symmetric primitive might be secure or not in a post-quantum world without first understanding how a quantum adversary could attack it.

In this talk we will provide an overview of the subject and present some recent results on symmetric quantum cryptanalysis: some attacks exploiting Simon's algorithm, quantization of some classical attacks, a new efficient quantum collision search algorithm and an analysis of the use of modular additions on symmetric primitives.

We will discuss some implications of these results in quantum-safe symmetric cryptography.

*Intervenant