Quantum symmetric cryptanalysis beyond Grover's algorithm

André Schrottenloher*[1]

[1]Centre Inria de l'Université de Rennes – Institut National de Recherche en Informatique et en Automatique – France

Résumé

Quantum computing devices, despite being still under development, have profoundly impacted the landscape of public-key cryptography. In fact, factoring and solving discrete logarithms (via Shor's algorithm) are one of the best targets to demonstrate the advantage of large-scale quantum computers.

The same cannot be said about secret-key cryptography. Indeed, attacks in this setting are most often based on Grover's algorithm. While Grover's speedup remains non negligible - from T to sqrt(T), it rather illustrates the inadequacy of quantum computers to tackle the "unstructured" problems that arise in symmetric cryptanalysis.

However, classical cryptanalysis exploits particular properties of Boolean functions (like correlations), meaning that the problems we solve do have some "structure". Does this mean that we could also, in some scenarios, reach a stronger speedup than Grover's algorithm? In this talk, I will focus on such families of quantum attacks, based on Simon's algorithm and discrete convolutions. While these algorithms are not as versatile as classical cryptanalysis tools, their complexity distinguishes them in the broader scope of quantum algorithms.

*Intervenant