Quantum Truncated Differential Attacks using Convolutions

Pichollet–Mugnier Aurel*[1]

[1]Univ Rennes, Inria, CNRS, IRISA, Rennes, France – Centre Inria de l'Université de Rennes – France

Résumé

Quantum computing is good for some problems, however it provides only a limited acceleration for problems arising in symmetric cryptanalysis.
Indeed, Grover's algorithm has been proven to be optimal for black-box searching and "only" provides a quadratic speedup over (classical) exhaustive search, i.e., offering a complexity of O(2ˆ{n/2}) instead of O(2ˆn).
However, a dedicated analysis is still needed in order to have an accurate measure of the security of symmetric ciphers.

{ }
In this presentation, we will introduce a new quantum attack that can, in theory attain a super-quadratic speedup (although not on practical ciphers so far) over classical attacks.
This attack is inspired by works previously done on {linear cryptanalysis} and is adapted to the case of differential cryptanalysis.
Differential cryptanalysis leverages the fact that some differences between plaintexts can lead to target differences in the resulting ciphertexts with non-negligible probability.
By using this property, one can design key-recovery attacks, which is the topic of our work.
The idea of our attack is to use the quantum convolution algorithm in order to write the probability of the differential as a convolution of functions.
Such convolutions can be computed using Quantum Fourier Transform which can be very efficiently be computed in the quantum setting.
We then construct a quantum state whose amplitudes encode the probability of the differential for different key guesses, and use this as the starting point of a quantum search, yielding a key-recovery attack.

*Intervenant