Differential clustering for Skinny

Thomas Sagot*[1]

[1]Laboratoire Lorrain de Recherche en Informatique et ses Applications – Institut National de Recherche en Informatique et en Automatique, Université de Lorraine, Centre National de la Recherche Scientifique, Centre National de la Recherche Scientifique : UMR7503 – France

Résumé

Differential cryptanalysis of SPN ciphers is usually composed of two steps : the first one, where we search for an activity pattern minimizing the number of active Sboxes, the second where we try to instantiate one or multiple differential trails. Finding multiple trails (i.e. searching for a differential cluster) is usually more computationally expensive, but gives better probabilities.
The Skinny cipher is a lightweight SPN cipher. It has a very aggressive construction, which allows cryptanalysts to use new strategies to attack this cipher. In particular, Skinny's Sboxes are very simple (4 nor and 4 xor for Skinny64, two times more for Skinny128). We managed to leverage this property to bypass the first step for the research of a differential, and we are able to found a differential trail with only one model, using a bitwise model. We can furthermore modify this model to find a differential cluster, introducing a state where we allow differences to be 0 or 1. One other strategy lay on the simple Mixcolumns operation, which induces trivial constraints that a differential trail must satisfy to be an instance of an activity pattern. This model gives probabilities very close to what we get experimentally, whilst having a low computing time.

Collaboration avec Xavier Bonnetain, Virginie Lallemand

*Intervenant