Generic Attacks on Double Block Length Sponge Hashing

César Mathéus*[1] and Gaëtan Leurent†[1]

[1]Centre Inria de Paris – Institut National de Recherche en Informatique et en Automatique – France

Résumé

The sponge construction is one of the modes of operation for hash functions.

In this talk, we study variants of the sponge construction using two permutations in parallel in order to increase the internal state size: the XOR combiner and the double sponge construction introduced by Lefèvre and Mennink.
We focus on indifferentiability security and present new distinguishers on these constructions based on a variant of the 4-sum problem, which we denote the multiple 4-sum problem.
This presentation is based on a paper accepted at the IACR Transactions on Symmetric Cryptology (ToSC) 2026 edition.

*Intervenant
†Auteur correspondant: gaetan.leurent@inria.fr