Title: Fast symmetric cryptography using ARM specialized instructions

Abstract: Recently, ARM™ added special instructions to their ARMv8-A instruction set that aim at accelerating standard cryptographic algorithms. Among these, a small set of instructions targets the acceleration of the Keccak-f permutation inside SHA-3, and it turns out that these instructions are actually fairly general and offer potential use beyond Keccak/SHA-3. In particular, we believe that these instructions could also accelerate authenticated encryption schemes like Xoofff, although using a non-trivial representation. The goal of this master’s thesis would be first to evaluate the suitability of the these instruction for Xoofff, for other Farfalle-based schemes and for any other state-of-the-art scheme. Then, the student would implement and benchmark selected schemes on an ARMv8-A platform. Finally, the student would be analyze how to take best advantage of these instructions in the design of new primitives and in particular of new Farfalle-based schemes.

Promoter: Gilles Van Assche