Fast Software Encryption 2017

Joan Daemen
Radboud University, Netherlands and STMicroelectronics, Belgium

Innovations in permutation-based encryption and/or authentication
Imagine there's no block ciphers, it's easy if you try:-)

Abstract: The SHA-3 competition has revealed that a fixed-length permutation is an excellent building block for hashing by means of the sponge. By including a key in the input this can readily be used for message authentication (MAC) and by exploiting the arbitrarily long sponge output for stream encryption. The duplex variant of sponge widens the spectrum to, among other, authenticated encryption and reseedable pseudorandom generation.
Up to a few years ago, it was widely believed that, for the same level of security, block-cipher-based modes would be more efficient than permutation-based modes. This picture has recently changed thanks to new strong generic security bounds for a keyed duplex variant that allows full-state absorbing. However, the sponge/duplex modes have the disadvantage that they are inherently serial and exploiting parallelism requires building an additional mode layer on top. We address this concern with Farfalle, a new construction that is a parallel keyed sponge variant. Its structure strongly relaxes the cryptographic requirements for the underlying permutation in comparison with keyed sponge or Even-Mansour and hence it has great potential for high-speed crypto. Farfalle builds a pseudorandom function (PRF) with arbitrary-length input and output that can readily be used for stream encryption and MAC. We realize session-based authenticated encryption, synthetic IV authentication encryption and a wide block cipher by the application of some amazingly simple PRF-based modes. In the talk, I will give an overview of these recent innovations in permutation-based crypto.

All this is joint work with Guido Bertoni, Michaël Peeters, Gilles Van Assche and Ronny Van Keer.