# SYMMETRIC CRYPTOGRAPHY 2.0

**Joan Daemen**

Radboud University and STMicroelectronics,
the Netherlands

The goal of cryptography is to protect secrecy and integrity of data, but also digital services and transactions. Due to the electronic media its importance has strongly increased during the last decades. It is usually subdivided into two kinds: asymmetric cryptography that is versatile and based on advanced mathematics but slow and symmetric cryptography that is limited and rather ad-hoc but fast. Both make use of building blocks, called primitives, and ways to use these, called modes. Ironically, there is more symmetry in asymmetric primitives than in the so-called symmetric ones. Moreover, there is a tendency for ever increasing complexity in modes and primitives.

In his presentation, Joan Daemen will speak about a counter-movement to clean up symmetric cryptography. In particular the so-called sponge-based modes make use of the simplest possible primitive, a fixed-length permutation, and currently causing a small revolution that deserves to be called symmetric crypto 2.0.