In-Memory implementation of SBoxes using Ferroelectric transistors

Cédric Marchand, Ian O'Connor
Univ Lyon, Ecole Centrale de Lyon, CNRS,
INSA Lyon, Université Claude Bernard Lyon 1,
CPE Lyon,
INL, UMR5270, 69130 Ecully, France
cedric.marchand@ec-lyon.fr

Stefan Slesazeck†, Thomas Mikolajick†‡
†NaMLab gGmbH
Dresden, Germany
‡Chair of Nanoelectronics, IHM,
TU Dresden, Germany
stefan.slesazeck@namlab.com

Among promising non-volatile emerging technologies capable of tackling the Von Neumann bottleneck of computing architectures, CMOS compatible ferroelectric transistors (FeFET) offer a large design space exploration for new computing paradigms such as logic-in-memory or in-memory-computing. A first use case is to store one value as a non-volatile constant inside a dedicated logic gate. The other operand(s) can then be presented at the gate of the logic gate to perform a computation. A second use case is to configure a FeFET-based circuit to compute a specific function as in a non-volatile FPGA. Recently, novel memory oriented circuits have been demonstrated, such as 2-FeFET ternary content addressable memory (TCAM) for embedded artificial intelligence application.

In this work, we present a new circuit called TC-MEM as well as its different features. This hybrid circuit can be accessed by address (as with conventional memory) but also by content search (as with a TCAM). In addition to the classical in memory operation, the TC-MEM enables the in-memory computation of bit-wise XOR operations, which remains a difficult task for in-memory-computing architectures. As well as presenting the TC-MEM cell and its different features, we also use the principal reversible property of this circuit to demonstrate how the TC-MEM can be used to implement cryptographic SBoxes using a single address space for encryption and decryption. We also discuss advantages and drawbacks of the various possible implementations in terms of control logic complexity and attack countermeasures.