Special Session on Secure Compute-in-Memory Architectures

A Case Study: Secure Reconfigurable FET-Based SRAM Architecture for In-Memory Computing

Farah Naz Syed (RU Bochum), Peng Chong, Juan Martinez, Stefan Slesazeck, Jens Trommer, Thomas Mikolajick (NamLab gGmbH), Akash Kumar (RU Bochum)

Abstract: The article presents the study of a reconfigurable field effect transistor (RFET) based in-memory computing (IMC) architecture that combines logic and memory primitive circuit blocks within a unified device-circuit model. This architecture is based on a fundamental set of RFET-based primitive circuit blocks, such as NOT, NAND gates, an SRAM cell, and a sense amplifier, which facilitate binary computations within the memory array. By leveraging the inherent polarity reconfigurability of RFET devices, this IMC architecture eliminates the need for peripheral logic to switch between memory and computing modes. Unlike CMOS circuits that show asymmetrical I-V characteristics for p- and n-type transistors, RFET devices show symmetrical characteristics, which reduces power variation and improves security against power side-channel attacks. This RFET-based secure SRAM architecture demonstrates a higher read noise margin compared to a traditional CMOS-based SRAM approach, as verified through simulation results, which is a result of enhanced control of channel conduction with reduced bit-line voltage contention, thus reducing charge-sharing effects under process variations. In addition, this secure SRAM architecture demonstrates a lower leakage power consumption, which is a result of suppressed sub-threshold and junction leakages using electrostatically created source/drain junctions in the non-conducting state of RFET devices.