Title:

Random masking interleaved scrambling technique as a countermeasure for DPA/DEMA attacks in cache memories

Authors:

- **Mădălin Neagu**, Technical University of Cluj-Napoca, Romania, email: neagumada@yahoo.com, Madalin.Neagu@cs.utcluj.ro
- **R. Rodríguez, D. Arumí, S. Manich**, U. Politecnica de Catalunya, Barcelona, Spain, email: Salvador.Manich@upc.edu

ABSTRACT:

Memory remanence in SRAMs and DRAMs is usually exploited through cold-boot attacks and the targets are the main memory and the L2 cache memory. Hence, a sudden power shutdown may give an attacker the opportunity to download the contents of the memory and extract critical data.

Side-channel attacks such as differential power or differential electromagnetic analysis have proven to be very effective against memory security. Furthermore, blending cold-boot attacks with DPA or DEMA can overpower even a high-level of security in cache or main memories. In this scope, data scrambling techniques have been explored and employed to improve the security, with a minor penalty in performance. Enforcing security techniques and methods in cache memories is risky because any substantial reduction in the cache memory speed might be devastating to the CPU, which is why the performance penalty must be minimal.

In this paper, we introduce an improved scrambling technique which uses random masking of the scrambling vector and it is designed to protect cache memories against cold-boot and differential power or electromagnetic attacks.

The technique is analyzed in terms of area, power and speed, while the level of security is evaluated through adversary models and simulated attacks.

Keywords: data scrambling, cache memories, differential power analysis, side-channel attack, error correction.

Acknowledgment: This work has been partially financed by Spanish TEC2013-J41209-P government project.