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

M. Neagu¹, S. Manich², R. Rodriguez², D. Arumi²
(¹) Technical University of Cluj-Napoca (²) Universitat Politècnica de Catalunya

1. Motivation
- Attacks against ICs and memories
- Confidentiality of sensitive information
- Data remanence: memory data intact for a couple of minutes, with no power supply
- Cold-boot and side-channel analysis attacks
  - DPEMA boosted cold-boot attacks
- Cache memories are targets
  - Sensitive data in plain form

2. Objectives
- Secure data in cache memories against “cold-boot boosted by DPEMA” attacks
  - Use the Interleaved Scrambling Technique and improve it
  - Conceal the stored data in the L2 cache
  - Reduce the amount of leaked information

3. Statement of the problem
- DPEMA attacks are powerful, difficult to mitigate
- Modify correlations between data and current intensity or radiated electromagnetic power to create confusion in the attacker model

4. Proposed technique
- Boost the IST with a random-masking strategy for balancing average Hamming weights the make them equal or randomly unequal
- Use a random bit generator at each CPU write in the cache
- The random bit determines which scrambling vector is used in the write process

5. Evaluation and results
- S3 - IST scrambling technique
- SSRS - IST-eDLC technique, but where the two redundant bits of the scrambling vector are generated randomly. This configuration is presented to demonstrate that not always a full random generation is beneficial.
- SSRSRC1 - IST-eDLC technique, but where one redundant bit is generated randomly.
- SSRSRC2 - IST-eDLC technique, the complete technique proposed for defense against SPEMA attacks.
- S3M - same as S3 but with random masking. A random bit generator flips the content of the scrambling vector randomly and the bit is stored in the cache together with scrambled data.
- SSRSRM - Same as SRS but with random masking.
- SSRSRCM - Same as SSRSRC1 but with random masking.
- SSRSRC2M - Same as SSRSRC2 but with random masking. This is the full RM-IST proposed in this paper for defense against DPEMA attacks which renders the minimum leakage.

6. Conclusions
- Viable solution to improve cache security
- IST is extended to attacks that analyze power consumption or electromagnetic radiation
- Random-masking strategy
- Obtained leakage reduction up to 98.2%