Securing Cryptography Implementations in Embedded Systems

Emmanuel Prouff[1,2]

[1] ANSSI, FRANCE
emmanuel.prouff@ssi.gouv.fr

[2] POLSYS, UMR 7606, LIP6,
Sorbonne Universities, UPMC University Paris VI

Abstract. Side Channel Analysis is a class of attacks which exploit leakages of information from a cryptographic implementation during execution. To defeat them, various techniques have been introduced during the two last decades, among which masking (aka *implementation sharing*) is a common countermeasure. The principle is to randomly split every sensitive intermediate variable occurring in the computation into several shares and the number of shares, called the order, plays the role of a security parameter. The main issue while applying masking to protect cryptographic implementations is to specify efficient schemes to secure the non-linear steps during the processing. Several solutions, applicable for arbitrary orders, have been recently published. Most of them start from the original concept of *Private Circuits* originally introduced by Ishaï, Sahai and Wagner at Crypto 2003. In parallel, and in order to formally prove the security of the proposed masking schemes, the community has also made important efforts to define leakage models that accurately capture the leakage complexity and simultaneously enable to build accurate security arguments. It is worth noting that there is a tight link between masking/sharing techniques, secure Multi Party Computation, Coding Theory and also Threshold Implementations. During a two hours tutorial, the main classes of countermeasures will be presented, together with models which have been introduced to prove their security. The link with other areas such as secure multi-party computation, error correcting codes and information theory will also be discussed.