# Recent results on side-channel attacks and countermeasures

F.-X. Standaert

U.C.Louvain

Traditionally, cryptographic algorithms provide security against an adversary who has only black box access to cryptographic devices. That is, the only thing the adversary can do is to query the cryptographic algorithm on inputs of its choice and analyze the responses, which are always computed according to the correct original secret information. However, such a model does not always correspond to the realities of physical implementations. During the last decade, significant attention has been paid to the physical security evaluation of cryptographic devices. In particular, it has been demonstrated that actual attackers may be much more powerful than what is captured by the black box model. For example, they can actually get a side-channel information, based on the device's physical computational steps. As a consequence, some kind of obfuscation is required to protect integrated circuits from these physical attacks. This is especially important for small embedded devices (e.g. smart card, RFIDs, sensor networks, ...) that can typically be under an adversary's control for a short period of time. This implies new theoretical concerns (how to exactly model and evaluate these physical threats) and practical ones (how to prevent them). In this talk, I will discuss different results in the area of side-channel attacks, with a particular focus on formal tools that can be used to evaluate physical security on a fair basis.