Does Physical Security of Cryptographic Devices Need a Formal Study? (Invited Talk)

François-Xavier Standaert[1], Tal G. Malkin[2], and Moti Yung[2,3]

[1] UCL Crypto Group, Université Catholique de Louvain
[2] Dept. of Computer Science, Columbia University, [3] Google Inc.
fstandae@uclouvain.be, {tal,moti}@cs.columbia.edu

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 can be captured by the black box model. They can actually get a side-channel information, based on the device physical computational steps.

A large set of practical techniques for breaking and repairing (i.e., applying countermeasures) have been found in this area of physical security and further, the area is now an important part of "crypto-engineering." The issue that will be addressed is: Do we need more fundamental (perhaps more theoretical) study of the area?

In this talk, it will be argued that having a model and a more basic approach to formalizing the physical leakage can be useful and revealing. A model in this area relies on certain signals being communicated to the attacker, so it is (to some degree) of an Information Theory or Communication Theory nature. It will then be argued specifically that having a formal model and quantitative tools to measure the physical leakage, generalize specific instances, enables a more sound way to investigate aspects of device design and of attacks on devices, and sets up a fair ground for arguing about differences in approaches.

R. Safavi-Naini (Ed.): ICITS 2008, LNCS 5155, p. 70, 2008.