Advanced techniques for Side Channel Analysis

Mots clés :
- Directeur de thèse : JEAN-LUC DANGER
- Co-encadrant(s) :
- Unité de recherche : Laboratoire Traitement et Communication de l'Information
- Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
- Domaine scientifique principal: Divers

Résumé du projet de recherche (Langue 1)

With the proliferation of the small embedded electronic devices, such as smart cards, their security becomes an important issue since they are used to more and more manipulate sensitive information such as banking information or user identity... It has been shown that the side channel attack [1] is a powerful technique to reveal the secret key stored in smartcard. Side channel analysis is an attack based on information (for example execution time [2], power consumption [3], electromagnetic [4]) gained from the physical implementation of a cryptosystem to reveal secret data. The achievement of a side-channel analysis depends on four factors: a good attack algorithm, a high signal acquisition quality, appropriate signal processing techniques and an intelligent key selection strategy. If attack algorithms have been well studied with the most famous attacks DPA [3], CPA[5] and MIA [6], the three other factors can still be improved. The first objective of the thesis is to enhance the efficiency of side channel attacks by proposing advanced techniques in these three steps. In the acquisition step, one can imagine to combine different kinds of signals at different instants and positions. In the processing step, signal processing and statistical analysis techniques will be studied to extract the maximum useful information from acquired signals. Last but not least, a new multi-criteria decision making will be examined in the key selection strategy. The second objective of the thesis aims at building a high level simulator for cryptographic modules implemented in embedded systems. In fact, this subject is very relevant from the point of view of smartcard manufacturers who do not have much information about the architecture of the chips in which they program their applications. The simulator will be used to evaluate not only the efficiency the proposed attack techniques but also the impacts of software counter-measures.

Résumé du projet de recherche (Langue 2)

* new side channel analysis proposals and the development of a simulator which is based on a platform with a known layout (first version). The side channel analysis proposals will be evaluated on the first version of the simulator. * Simulator validation with real-word legacy smartcards (second version). In this step, the device’s layout is unknown (or limited). Therefore, some adaptations will be envisaged. The side channel analysis proposals are improved and evaluated on the second version of the simulator. * evaluation of software counter-measures which are implemented in real smartcards and in the simulator. The efficiency and the impacts of software countermeasures will be evaluated with real signals and simulation signals.