Proposition de recherche doctorale

Logic Level Countermeasures to Secure FPGA based Designs

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)

Modern field programmable gate arrays (FPGA) are capable of implementing complex system on chip (SoC) and providing high performance. Therefore, FPGAs are finding wide application. A complex SoC generally contains embedded cryptographic cores to encrypt/decrypt data to ensure security. These cryptographic cores are mathematically secure but their physical implementations can be compromised using side channel attacks (SCA) or fault attacks (FA). This thesis focuses on countermeasure for securing cryptographic cores on FPGAs. Firstly, a register-transfer level countermeasure called "Unrolling" is proposed. This hiding countermeasure executes multiple rounds of a cryptographic algorithm per clock which allows deeper diffusion of data. Results show excellent resistance against SCA. This is followed by dual-rail precharge logic (DPL) based countermeasures, which form a major part of this work. Wave dynamic differential logic (WDDL), a commonly used DPL countermeasure well suited for FPGAs is studied. Analysis of WDDL (DPL in general) against FA revealed that it is resistant against majority of faults. Therefore, if flaws in DPL namely early propagation effect (EPE) and technological imbalance are fixed, DPL can evolve as a common countermeasure against SCA and FA. Continuing on this line of research we propose two new countermeasures: DPL without EPE and Balanced-Cell based DPL (BCDL). Finally advanced evaluation tools like stochastic model, mutual information and combined attacks are discussed which are useful when analyzing countermeasures.