Proposition de recherche doctorale

Caractérisation et modélisation de générateurs d'aléas basés sur la métastabilité

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)

Les générateurs d'aléa vrai(TRNG)~\cite{TRNG-ICTER-2009,DBLP:conf/ches/KillmannS08} sont des éléments essentiels de certains protocoles cryptographiques, mais aussi de contre-mesures. Un TRNG prédictible est simplement contradictoire avec sa vocation. Ainsi le concepteur doit être en mesure de caractériser le TRNG notamment en terme d'entropie et en fonction de l'environnement. Une catégorie de TRNGs délivrant le maximum de débit repose sur le phénomène de métastabilité ~\cite{JLD:ELSEVIER-09,srinivasan-09} dans les éléments mémoire. Ils sont particulièrement attrayants pour la protection des implémentations cryptographiques. En revanche l'hypothèse de générateur idéal d'aléa dans un système cryptographique ne peut véritablement être vérifié qu'avec la génération d'un modèle mathématique décrivant le comportement~\cite{suresh-2010,DBLP:conf/ches/KillmannS08}. Ce modèle permet de certifier le bon fonctionnement et la résistance face aux attaques physiques dans un environnement. Le modèle est basé sur des paramètres obtenus grâce à des evaluations au laboratoire ou à l'aide de simulateur électrique. Les TRNG nécessitent un étage de post-traitement permettant d'éliminer des biais ou augmenter leur fiabilité ou résistance aux attaques. Ces étages doivent également être évalués et modélisés pour considérer le comportement global du TRNG.

Résumé du projet de recherche (Langue 2)

L'objectif de cette thèse est de caractériser et modéliser des structures TRNG et PUF qui soient, en fonction d'un \textbf{modèle physique}, susceptibles de remplir leurs propriétés a priori antinomiques. Ces structures seront implémentées dans des cartes de développement FPGA. Une \textbf{méthodologie de caractérisation} sera définie, et appliquée. Cette méthodologie se décline en deux volets : quantité à mesurer (relatives notamment à des entropies) et méthode de mesure (protocole expérimental pour accéder à la valeur). Cette caractérisation sera ensuite mesurée \textbf{en fonction de l'environnement} du composant, notamment sa température, sa tension d'alimentation, son exposition à un rayonnement. Cette étude a pour but de quantifier la qualité du TRNG et le pouvoir d'un attaquant, que l'on considérera comme adaptatif, contre les structures TRNGs. Une retombée est, entre autres, une indication sur la résilience inhérentes des structures TRNG et PUF. Cette information guidera le concepteur dans son choix des contre-mesures extrinsèques additionnelles (typiquement des détecteurs). Un modèle comportemental et statistique sera élaboré et permettra de valider les protections tirant parti des TRNG dans les implémentations cryptographiques. Cette thèse s'inscrit dans une convention CIFRE dans la société Secure-IC . Les travaux de recherche sont donc directement liés aux activités et outils de secure-IC au même titre que le laboratoire d'accueil de Telecom ParisTech. La liste des tâches de l'étude peut se décliner ainsi : * Etude bibliographique des principaux TRNG et en particulier ceux étudiés à Telecom ParisTech (Open-Loop TRNG). * Méthodes pour analyser les TRNG. Dans cette phase. Le SmartSIC Analyzer de Secure-IC pourra servir de base pour mettre au point une méthode d'analyse. * Caractérisations des TRNG dans différents environnements. La plate-forme SmartSIC+ pourra servir comme support à cette étape. * Etude de modélisation. Lien avec les processus de certification des systèmes cryptographiques comme par exemple AIS 31, Critères Communs (processus de normalisation de la sécurité à l'échelle internationale)

Informations complémentaires (Langue 1)

Colaboration avec le laboratoire BSI (Bonn) sur l'utilisation de la norme AIS31