

Titre : Caractérisation et modélisation de source d'aléa et de générateurs de suites binaires aléatoires dans les circuits intégrés analogiques et logiques

Directeur de thèse : Viktor FISCHER - professeur (LaHC)

Co-directeurs de thèse : Florent BERNARD – maître de conférences (LaHC)
Benjamin DUVAL (Société INVIA)

Laboratoire : Laboratoire Hubert Curien UMR n° 5516, Université Jean Monnet Saint Etienne

Collaboration : en collaboration avec la société INVIA 13590 Meyreuil

Mode de financement : CIFRE

RESUME

La thèse aura pour objectif central d'étudier les différentes sources d'aléas potentiellement utilisables pour l'implantation de générateurs de suites binaires aléatoires dans des circuits analogiques et logiques. Il s'agit d'une recherche amont permettant de caractériser finement ces sources d'aléas, de proposer des outils de modélisation de leur fonctionnement physique et d'apporter la preuve de la qualité statistique des séquences binaires aléatoires extraites. Ces travaux feront appel à un vaste spectre de compétences intégrant une connaissance approfondie de la technologie de circuits logiques et analogiques, une maîtrise des principes physiques et des outils mathématiques de modélisation des composants de l'électronique numérique et analogique ainsi qu'une capacité d'utilisation des tests statistiques de référence dans le domaine de la cryptologie.

Présentation du sujet et objectifs

Les générateurs de suites binaires aléatoires constituent la partie primordiale d'un système cryptographique. Ils sont utilisés surtout pour générer les clés confidentielles ou les vecteurs d'initialisation, mais également dans différents protocoles pour le stockage et la transmission sécurisés de l'information. La vitesse (le débit), la qualité des suites générées (le biais, la corrélation), la sécurité (résistance contre les attaques et les défauts de fonctionnement) et la consommation (statique et dynamique par bit généré) jouent un rôle essentiel dans le choix d'un générateur. La sécurité du système cryptographique augmente si un tel système peut être réalisé dans un seul circuit.

La génération de nombres aléatoires dans des circuits intégrés analogiques et logiques représente un problème scientifique ouvert pour plusieurs raisons : les sources de phénomènes aléatoires ne sont pas encore suffisamment maîtrisées, les sources d'aléa exploitées ne sont pas caractérisées d'une manière suffisante, les méthodes d'extraction d'aléa utilisées présentent parfois des failles de fonctionnement ou ne sont pas suffisamment robustes contre les manipulations et les attaques et enfin, les contraintes de faible consommation ne sont pas encore suffisamment exploitées.

Cette problématique de la qualité des sources d'aléas peut apparaître comme dans un premier temps comme un sujet à dimension uniquement technologique. Les communications scientifiques dans ce domaine ont d'ailleurs longtemps négligé les aspects amont de modélisation et de caractérisation des sources d'aléas en se concentrant principalement sur des dimensions architecturales et technologiques des générateurs. Les publications récentes montrent clairement que seuls des travaux plus fondamentaux sur la source physique de l'aléa et de sa modélisation peuvent garantir une validation scientifique de la qualité des générateurs. C'est cette orientation qui est clairement proposée dans le cadre de ce sujet de thèse.

Ces travaux se heurtent aujourd'hui à une connaissance insuffisante des principes du mécanisme de base de la génération d'aléas ce qui limite ensuite les possibilités d'une connaissance approfondie du fonctionnement et du comportement des générateurs, éléments indispensables pour permettre une véritable validation de leur qualité intrinsèque. La maîtrise totale du phénomène physique exploité comme la source d'aléas par rapport aux changements d'environnement et des conditions de travail (et notamment de l'alimentation) et la validation de sa robustesse par rapport aux attaques constituent un critère prioritaire de sélection d'une source d'aléas.

Dans ce contexte le sujet de thèse proposé comportera les parties suivantes :

1. Etude des méthodes existantes de caractérisation et de mesure de sources d'aléas disponibles dans des circuits intégrés analogiques et logiques
2. Adaptation de méthodes existantes et proposition de nouvelles méthodes de mesure adaptées pour le contexte d'utilisation d'aléas générés dans des circuits logiques et analogiques
3. Recherche et proposition de modèles stochastiques permettant d'estimer l'entropie de sources d'aléas exploitées
4. Validation de modèles proposés par des simulations et par des mesures dans des circuits

Le travail de recherche se fera en étroite collaboration avec un doctorant de l'Institut Matériaux Microélectronique Nanosciences de Provence (IM2NP), UMR 6242 CNRS Universités Paul Cézanne Provence et Sud Toulon-Var, dont le sujet abordera la sélection de la source aléa implantable dans des circuits intégrés analogiques et la conception du générateur de suites binaires aléatoires à faible consommation basé sur la source d'aléa sélectionnée.

Contexte scientifique

Entreprise / Laboratoire

Le doctorant sera recruté dans le cadre d'un dispositif CIFRE par la société INVIA qui développe et commercialise des fonctions microélectroniques destinées aux circuits intégrés de plates formes sécurisées. Le doctorant sera également intégré au sein l'équipe SES (Systèmes Embarqués Sécurisés) du Département Informatique-Telecom -Image du Laboratoire Hubert Curien.

Directeurs de thèse

Viktor FISCHER, professeur des universités, est responsable de l'équipe SES sera le directeur de cette thèse. La thèse sera co-encadrée par Florent BERNARD, maître de conférences, également membre de l'équipe SES et par Benjamin DUVAL ingénieur de la société INVIA.

Profil du candidat

Le candidat devra être issu d'un master relevant de l'une des deux communautés cryptologie (informatique) ou électronique. Compte tenu de l'aspect pluridisciplinaire, il devra disposer d'une ouverture suffisante pour acquérir les compétences complémentaires en cryptologie (informatique) ou en électronique dont il aura besoin.