Problématiques modernes de la génération d'aléa véritable: étude approfondie d'un TRNG basé sur les PLLs

Florent Bernard*[1] and Nathalie Bochard*[1]

[1]Laboratoire Hubert Curien, Saint-Étienne – Centre National de la Recherche Scientifique - CNRS – France

Résumé

Au cours de cette présentation et due à l'importance des nombres aléatoires en cryptographie, nous discuterons des problématiques liées à la génération d'aléa dans des circuits logiques. En effet, malgré la présence de normes de certification modernes imposant une compréhension et caractérisation de la source d'aléa utilisée, de nombreux générateurs d'aléa s'intéressent encore seulement au débit ou au fait que les séquences produites par ces dispositifs passent des batteries de tests statistiques. A travers l'exemple du générateur d'aléa basé sur les PLLs (Boucle à verrouillage de phase), nous présenterons la démarche suivie permettant d'évaluer la qualité du générateur. Cette démarche repose sur la proposition d'un modèle stochastique amélioré que nous détaillerons ainsi que la validation expérimentale des hypothèses sur lesquelles reposent ce modèle. Grâce à ce modèle, nous proposons deux tests en ligne dédiés (online test et total failure test) permettant dévaluer la qualité de l'aléa généré en cours de fonctionnement. Enfin nous présenterons une méthodologie permettant en pratique de paramétrer le générateur pour garantir que le modèle stochastique le décrivant s'applique et permet de garantir un niveau de sécurité demandé par les normes de certification les plus exigeantes (AIS31 par exemple).

*Intervenant