Évaluation d'un générateur de nombres aléatoires par la caractérisation d'anomalies statistiques dans les séquences générées.

Antoine Levotre, doctorant 2ème année
Université Grenoble Alpes, Insitut Fourier, CEA

Les générateurs de nombres aléatoires sont une brique essentielle des mécanismes cryptographiques actuels, ceux-ci servant notamment à la génération de données secrètes telles que les clés ou les nonces dans les calculs de signature ECDSA. La sécurité de ces protocoles repose donc sur la qualité de l'aléa fourni par le générateur.
Pour évaluer cette qualité, deux approches sont envisageables. Si la source d'aléa du générateur est un phénomène physique, on va chercher à obtenir une expression analytique de l'entropie (au sens de la théorie de l'information) du système à partir de la modélisation mathématique de ce phénomène (Cf. [FL14][1] par exemple).
Toutefois, si ce modèle n'est pas disponible, ou si la source d'aléa du générateur n'est pas un phénomène physique, il est nécessaire d'évaluer le générateur en "boîte noire", par le biais de tests d'hypothèse sur des séquences générées. L'hypothèse nulle de ces tests est alors "la séquence étudiée peut être issue d'un générateur idéal". L'un des inconvénients de cette méthode est que, au-delà des potentiels acceptations ou refus erronés de l'hypothèse nulle, un simple échec des tests ne permet pas de distinguer la caractéristique de la séquence qui fait défaut, ce qui pourrait pourtant intéresser un concepteur (ou un attaquant).

L'objectif de cet exposé est alors de proposer une troisième approche à l'évaluation des générateurs de nombres aléatoires, forme hybride des deux méthodologies précédentes. À défaut de pouvoir modéliser mathématiquement le générateur lui-même, on cherche à obtenir une modélisation des déviations au modèle uniforme idéal pouvant l'affecter (telles qu'une disproportion dans la génération des bits 0 et 1, ou encore des dépendances entre bits successifs). Cette modélisation se présente sous la forme d'une fonction d'un certain nombre de paramètres, chacun caractérisant un type de déviation au modèle idéal. L'étude de la qualité du générateur s'effectue ensuite par l'estimation des différents paramètres et donc de l'écart aux valeurs attendues par rapport au cas d'un générateur idéal. Les caractéristiques faisant défaut dans la séquence étudiée seront alors clairement mises en évidence par les valeurs des paramètres qui leur sont associées. Cela reste donc une méthodologie en boîte noire, qui ne tire parti d'aucune information préalable sur le générateur, mais qui présente l'avantage de pouvoir caractériser précisément les défauts potentiels de celui-ci.

[1] [FL14] Viktor Fischer et David Lubicz, Embedded evaluation of randomness in oscillator based elementary TRNG. *Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2014.*