Effets des différents bruits sur la variance d'Allan du jitter dans des RO: Expérimentation et émulation

Licinius Benea*[1]

[1]Direction de Recherche Technologique (CEA) – Univ. Grenoble Alpes, CEA, LETI, F38054 Grenoble – France

Résumé

La caractérisation de la source d'entropie physique devient une exigence incontournable pour toute certification de TRNG. Dans le cas des oscillateurs en anneau, la variance d'Allan du jitter est un outil fiable qui permet de faire la distinction entre le jitter provenant du bruit flicker (autocorrélé) et du bruit thermique (blanc). Nos données, obtenues par des mesures directes, ainsi que des preuves de la littérature, indiquent la présence d'une troisième source de bruit : le bruit de quantification. Les résultats montrent qu'un échantillonnage insuffisant (c'est-à-dire un bruit de quantification plus élevé) peut conduire à une surestimation du jitter provenant du bruit thermique et donc à une surestimation de l'entropie calculée selon les modèles existants. En complément de ces résultats expérimentaux, nous présenterons des premiers résultats basés sur notre émulateur de jitter intégrant les bruits thermiques et flicker. Les mesures expérimentales permettent de consolider la fiabilité de l'émulateur à simuler un jitter réel. Ceci ouvre la porte à des simulations avancées, notamment sur une quantification concrète de l'effet du flicker sur l'entropie du TRNG.

*Intervenant