Post-Taitement de Générateurs de nombres aléatoires

Les génrateurs de nombres aléatoires sont des composants essentiels dans la sécurité des systèmes d'informations (génération de clés, algorithmes de chiffrements, contremesures, …). Pour construire une suite de nombres aléatoires on utilise une source physique d'entropie qui est numérisée, évaluée et retraitée. Le retraitement algorithmique de la séquence numérisée doit à la fois garantir une « bonne » qualité statistique de la séquece de sortie et impacter le plus faiblement possible les performances du générateur. Dans un cadre de certification, ces retraitements doivent respécter les standards comme AIS31, de l'authorité allemande BSI (Bundesamt für Sicherheit in der Informationstechnik).
L'objectif du travail proposé est d'étudier les différents retraitements possible dans le cadre de la certification AIS31, de mettre en exergue les solutions les plus performantes et de fournir, si possible, des garanties sur les propriétés statistiques en sorite du retraitement.