12112 FEVRET Eliott

PSI

Génération de nombres aléatoires grâce aux Speckles

Quand je lance une playlist en "lecture aléatoire" je me demande toujours ce qui se cache derrière ce hasard en apparence simple. Présent en cryptographie, simulation et désormais même en IA, l'aléatoire est omniprésent. J'ai donc cherché à en comprendre les mécanismes afin de concevoir un générateur de nombres aléatoires.

La génération de nombres aléatoires sécurisés représente un défi en informatique en raison de la nature déterministe des algorithmes. Mon TIPE propose alors de convertir un phénomène physique aléatoire, le speckle, en une graine aléatoire, qui sera ensuite transformée en une suite de nombres pseudo-aléatoires.

Positionnement thématique (ÉTAPE 2) :

- *PHYSIQUE (Physique Ondulatoire)*
- *INFORMATIQUE (Informatique pratique)*
- *MATHEMATIQUES (Autres)*

Mots-clés (ÉTAPE 1) :

Mots-clés (en français)	**Mots-clés (en anglais)**
Tavelure	*Speckle*
Générateur de nombres pseudo-aléatoires	*Pseudorandom number generator*
Fonction de Hachage	*Hash function*
Cryptographie	*Cryptography*
Vérification statistique	*Statistical verification*

Bibliographie commentée

Avec l'essor de l'informatique, l'aléatoire est un enjeu clé, essentiel en simulation, cryptographie et cybersécurité. Cependant, il demeure difficilement compatible avec le caractère déterministe des algorithmes. En effet, ces derniers produisent systématiquement les mêmes résultats lorsqu'ils sont appliqués avec les mêmes paramètres [1].

Pour pallier cette **incompatibilité entre aléatoire et déterminisme,** des générateurs dits "mixtes" ont été développés, alliant phénomènes physiques intrinsèquement aléatoires et

méthodes algorithmiques pour produire des suites de nombres aléatoires [1]. Une approche innovante a été proposée en 1988 par J. Taboury, qui suggérait d'utiliser les *speckles* comme source d'aléa [2], une idée que nous explorerons dans ce TIPE.

Le *speckle* est un motif d'interférences observé lors du passage de la lumière cohérente à travers un milieu diffusant. Il est composé de grains aléatoires dont la distribution d'intensité suit une loi de Rayleigh [2][3]. S'appuyant sur ce principe, Felipe Louza a proposé une méthode expérimentale permettant de réaliser des figures de *speckle* aléatoires à l'aide du mouvement *brownien*, figures qui peuvent ensuite être utilisées comme **source d'aléa** [4].

Bien que le *speckle* génère un phénomène aléatoire, il ne fournit initialement qu'une seule valeur, appelée la *graine*. Pour générer une suite de **plusieurs nombres aléatoires à partir de cette unique graine**, il est nécessaire d'utiliser des algorithmes spécifiques. La première étape consiste à partir d'un algorithme de hachage - tel que *SHA-2* - de convertir la figure aléatoire issue du *speckle* en une valeur numérique exploitable par un ordinateur [5]. Cette donnée peut ensuite être traitée par un générateur afin d'aboutir à une suite de nombres pseudo-aléatoires. Le générateur *Blum-Blum-Shub* (*BBS*) proposé dans les années 1980 et reconnu pour sa sécurité constitue un exemple pertinent que nous utiliserons [6].

Néanmoins, en raison du caractère déterministe de ces générateurs, il est crucial de **vérifier statistiquement la qualité des suites générées**. Des tests référencés par Donald Knuth, permettent de vérifier l'équiprobabilité et l'indépendance des nombres produits, garantissant ainsi la fiabilité et la sécurité du générateur, notamment dans des applications sensibles comme la cryptographie [4][6][7].

Problématique retenue

Comment concilier l'aléatoire des figures de *speckle* et le déterminisme des algorithmes afin de générer des nombres aléatoires de manière fiable et sécurisée ?

Objectifs du TIPE du candidat

- Réaliser une expérience de génération de *speckle* non stationnaire

- Associer une signature unique à une image aléatoire

- Concevoir un générateur de nombres pseudo-aléatoires à partir d'une graine

- Vérifier statistiquement la fiabilité et la performance du générateur

Références bibliographiques (ÉTAPE 1)

[1] DAMIEN VERGNAUD : L'aléatoire, clé de voûte de la sécurité informatique. *: La Recherche, Juillet-Août 2019, n°549*

[2] JEAN TABOURY : Utilisation Du 'Speckle' Comme Générateur Rapide De Tableaux Aléatoires Binaires: Optimisation Des Paramètres *: Annales Des Télécommunications, 1988*

[3] JEAN TABOURY : Transmission désordonnée et speckle *: Photoniques, 2011*

[4] FELIPE A. LOUZA : True random number generator based on laser speckle images from particles under Brownian motion *: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4622916*

[5] COMMUNAUTAIRE : Secure Hash Algorithms 2 *: https://en.wikipedia.org/wiki/SHA-2*

[6] DONALD ERVIN KNUTH : The art of computer programming *: Chapitre 3*

[7] BENJAMIN BILLET : NOMBRES PSEUDO-ALEATOIRES *: https://benjaminbillet.fr/media/prng_mathreport.pdf*

Références bibliographiques (ÉTAPE 2)

[1] PHILIPPE LALANNE : Les réseaux de neurones formels et leurs réalisations optoélectroniques. Génération optique de tableaux de nombres aléatoires, 1989. *: https://pastel.hal.science/pastel-00730634v1*

DOT

[1] *: [Février - Mars 2024] Exploration des méthodes numériques de génération de nombres aléatoires. Étude des protocoles de connexion sécurisée en ligne.*

[2] *: [Avril 2024] Choix définitif du phénomène de speckle comme source d'aléatoire. Recherche documentaire sur les principes physiques sous-jacents.*

[3] *: [Mai - Juin 2024] Prise de contact avec Mme Fabienne Besnard. Échanges autour du phénomène de speckle et clarification de points techniques. Réalisation d'une première expérience de génération de speckle en laboratoire à l'école SupOptique.*

[4] *: [Juillet - Septembre 2024] Traitement informatique des images de speckle obtenues. Vérification de la conformité avec la théorie (distribution de Rayleigh). Implémentation d'une première fonction de hachage.*

[5] *: [Octobre - Décembre 2024] Implémentation de la fonction cryptographique SHA-256 en python.*

[6] *: [Janvier 2025] Deuxième expérience visant à générer un speckle non stationnaire. Analyse des difficultés rencontrées et bilan des résultats.*

[7] *: [Février 2025] Troisième expérience, en réponse aux échecs précédents. Ajustement des paramètres expérimentaux et nouvelle collecte de données. Génération finale des clés à partir des images obtenues.*

[8] *: [Avril - Juin 2025] Finalisation du projet. Rédaction et réalisation de la présentation orale.*