**Générateur de nombres aléatoires**

**(GNA)**

**Préambule : (65 mots)**

**Dans le cadre de la MCOT, la problématique que j'ai souhaité aborder était : Les générateurs de nombres aléatoires de haute qualité sont indispensables aujourd’hui dans tous les domaines pour des raisons de sécurité. Il s’agit de choisir le phénomène physique adéquat pour avoir un bon générateur qui passe les test statistiques et qui soit bien protégé pour optimiser au maximum les résultats obtenus.**

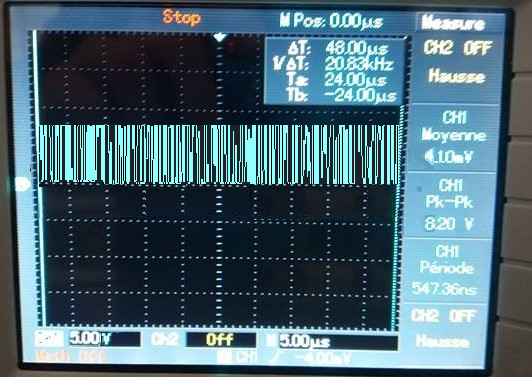
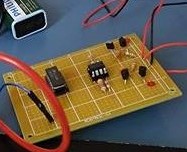
**Introduction : (90 mots)**

**Le besoin des générateurs de nombres aléatoires augmente toujours, surtout dans le domaine de la sécurité électronique. Dans ce cadre, je me suis proposé de mettre en place un GNA de haute qualité, ainsi, mes objectifs s’articulent en :**

1. **Conception et fabrication du circuit électrique responsable de la génération des nombres aléatoires.**
2. **Test du caractère aléatoire des données générées par le système à travers les outils convenables tels que la série des tests statistiques de NIST…**
3. **Protection du système contre les attaques possibles venant du milieu extérieur.**

**Corps principal : (545 mots)**

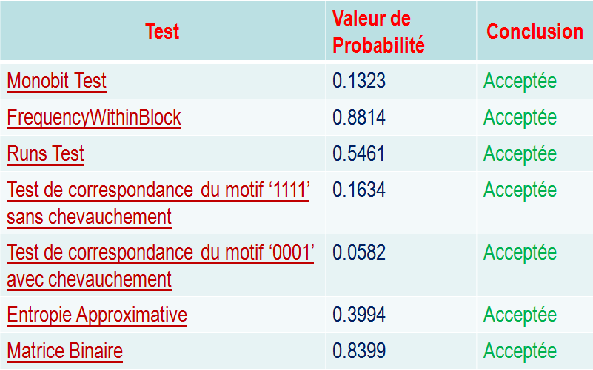
**Dans une première partie, un choix de source d’entropie doit être fait et pour cela, on choisit le bruit électronique et plus précisément le bruit d’Avalanche qui se produit dans une jonction PN polarisée en inverse car ce bruit généré se caractérise par une forte amplitude (de l’ordre de 70 mV) par rapport aux autres types de bruit électronique tel que le bruit thermique. Une première idée du circuit électrique se présente qui est la suivante : Amplifier une seule source de bruit puis comparer le signal généré à sa moyenne. Mais, le problème majeur de cette méthode est la difficulté au niveau de la détermination rapide et précise de la valeur moyenne. Ainsi, on optimalise cette idée en faisant intervenir une deuxième source de bruit amplifié à laquelle on compare le 1er signal. Concernant la phase d’amplification, on va utiliser un Amplificateur Opérationnel (TL082) dans un circuit non inverseur avec un gain réel de 20. Quant à la phase de comparaison, on va utiliser un circuit intégré qui est le comparateur LM139j dédié pour la comparaison de signaux variables chaotiques. Après l’acquisition du signal provenant de la sortie du comparateur, il nous reste une dernière phase d’échantillonnage qui va être réalisée à l’aide de la carte ArduinoUno pour pouvoir produire la séquence aléatoire de bits.**

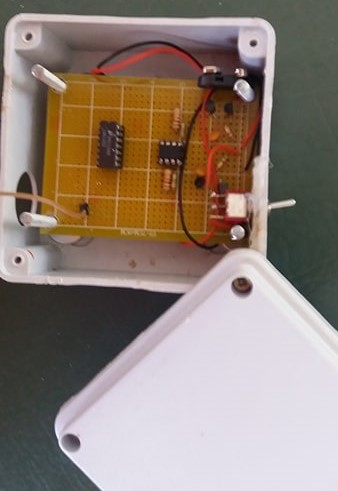
**** ****

**Après la génération de la séquence, une phase de test est inévitable pour pouvoir conclure quant à son caractère aléatoire, parce qu’un bon GNA est celui qui génère des séquences de haute qualité, ainsi, on aura recours aux tests statistiques développés par les chercheurs de NIST (National Institute of Standards and Technology). Ces tests servent à la détection de toutes formes de déviation de la séquence testée du modèle mathématique élaboré par le NIST qui est le modèle d’une séquence aléatoire caractérisée par :**

1. **La fréquence des zéros est égale à celle des uns que ce soit globalement o localement (dans des sous-séquences de la séquence « mère »).**
2. **L’oscillation entre les zéros et les uns dans la séquence testée est ni rapide ni lente.**
3. **L’absence de tout motif que ce soit périodique ou apériodique.**
4. **L’indépendance entre les bits consécutifs et entre les sous-séquences de longueur M (M est fixé par NIST) de la séquence testée.**
5. **Une entropie maximale puisque l’entropie est proportionnelle au désordre.**

**Les résultats obtenus à partir de ces tests (après leurs implémentations sur Python) vont permettre de déterminer si la séquence testée est à rejeter ou à garder surtout lorsqu’il s’agit des domaines cruciaux tels que les jeux d’argent et la cryptographie.**

****

**La phase de test n’est pas suffisante pour garantir le bon fonctionnement du système puisque les générateurs de nombres aléatoires sont toujours en danger à cause des différentes attaques extérieures qui puissent se produire, alors, une phase de protection serait nécessaire pour empêcher tout acte de piratage, et parmi ces attaques on trouve la méthode d’injection d’une tension ou d’une fréquence dont le but est de saturer le GNA mais cette méthode est inefficace grâce à la comparaison différentielle implémentée dans le circuit. Une autre méthode est de varier la température pour diminuer l’amplitude de bruit généré mais cette méthode peut être facilement évitée grâce à une isolation thermique du boîtier où on va garder notre système.**

**Conclusion générale : (51 mots)**

**En conclusion, on remarque que la mise en place d’un générateur de nombres aléatoires de haute qualité demande une étude scientifique très approfondie qui couvre plusieurs domaines tels que l’électronique, la probabilité et la programmation mais ça le mérite puisque un tel système aura de la valeur ajoutée dans notre monde.**