YANG – Chunxiao

Fractional chaotic pseudo-random number generator design and application to image cryptosystem

Résumé : Des systèmes chaotiques ont été utilisés pour concevoir des générateurs de nombres pseudo-aléatoires (PRNG) et appliqués aux cryptosystèmes en raison de leurs caractéristiques prometteuses, telles que le caractère aléatoire et la sensibilité aux conditions initiales. Les systèmes chaotiques fractionnaires, bien que beaucoup moins discutés que les cartes et systèmes chaotiques classiques d'ordre entier, possèdent une complexité intrigante qui peut fournir de la nouveauté, de la complexité et des clés secrètes supplémentaires à la conception Chaotic PRNG (CPRNG), qui à son tour améliore la sécurité du cryptosystème.
Cette thèse a étudié différentes approches de calcul numérique pour les systèmes chaotiques fractionnaires. Une méthode de calcul de grille non uniforme avec deux compositions de grille différentes a été proposée pour résoudre numériquement les systèmes chaotiques fractionnaires 3D. Les CPRNG fractionnaires (FCPRNG), qui répondent aux exigences aléatoires et statistiques, ont été conçus pour la première fois en utilisant trois systèmes chaotiques fractionnaires différents. De plus, un chiffrement par flux et un chiffrement par blocs basés sur des méthodes de codage et de décodage de l'ADN ont été proposés et étudiés à l'aide des FCPRNG conçus. Les deux chiffrements ont été verifies pour être sûrs et fiables.

Mots-clés : Système chaotiques fractionnaires, crypto-système basé sur le chaos, chiffrement de flux, chiffrement par bloc, générateur de nombres pseudo-aléatoires