MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE DJILLALI LIABES SIDI BEL ABBES

FACULTE DE TECHNOLOGIE

RESUME DE MEMOIRE DE MAGISTER

Nom & Prénom(s)	BENTOUILA Sara
E-mail (obligatoire)	bentouila.sara@yahoo.fr
Spécialité	Informatique
Titre	Cryptographie symétrique des images numériques par les automates cellulaires
Date de soutenance	17/12/2013
Nom, prénom(s) et grade de l'encadreur	Kamel Mohamed FERAOUN

Résumé :
Dans ce mémoire, nous introduisons un nouvel algorithme de chiffrement basé sur les automates cellulaires (AC). Leur comportement complexe et leur nature parallèle les rend intéressants dans le domaine de la cryptographie. Les algorithmes proposés appartient à la classe des systèmes à clés symétriques basés sur le chiffrement par flot.
Un générateur de séquence de nombre pseudo aléatoire (PRNG) de haute qualité peut être construit en utilisant les automates cellulaires. Nous proposons un crypto-système basé sur un AC unidimensionnel, qui peut résister aux différentes attaques de la cryptanalyse.
Enfin, nous fournissons des résultats expérimentaux pour vérifier la qualité du SNPA en utilisant des suites de tests statistiques comme ENT, DIEHARD et NIST.
Les résultats des expérimentations montrent que les crypto-systèmes proposés sont capables de produire des SNPAs de très haute qualité et même de qualité supérieure aux systèmes cryptographiques connus, et elles sont aussi beaucoup plus résistantes aux tentatives de cassage des clés des systèmes connus.

Mots clés :
Cryptographie, Automate cellulaire, Chiffrement par flot, Générateur de nombres pseudo-aléatoire (PRNG), Séquence de nombres pseudo-aléatoire (SNPA), Règle, Test statistique.

Abstract
We introduce a new encryption algorithm based on cellular automata (CA). Complexity of the behavior achieved by CA and its parallel nature makes them interesting from point of view of cryptography. The proposed algorithms belongs to the class of symmetric key systems based on stream cipher.
High-quality PRNG can be constructed by employing cellular automata.We propose a cryptosystem based on a one-dimensional CA, which can resist the more significant cryptanalytic attacks.
Finally, we provide experimental results to verify the randomness quality using ENT, DIEHARD and NIST test suites.
Results of experiments shown that the proposed cryptosystems are able to produce PNSs of a very high quality outperforming the quality of known secret key cryptosystems, which also are much more resistant for breaking cryptography keys that known systems.

Keywords :
Cryptography, Cellular automata, Stream ciphers, pseudorandom number generator (PRNG), pseudo-random number sequence (PNS), Rule, Statistical test.