Abstract

Cryptography process is considered to be the main basis for preserving the data security and integrity, via transmission through the modern communication media between people.

The power of cryptography system is mainly based on the possibility generation of sequence numbers to be real randomness, that is to say an attempt to construct and design a system to generate random numbers of high quality, which represent the cryptosystem key.

In this thesis we present a new technique to generate a high-quality Pseudorandom numbers (PRNs) by applying three-dimensional cellular automata (3-D CA), whereas the updating process for CA is based upon the neighbor cells and the selected rules for application in the calculating of the next state for CA. There is a huge search space of the rules, that can be applied in the process of calculating the next state of CA and for choosing the rules that will be applied to updating the values of the cells of 3-D CA.

Thus the cellular programming (CP) technique were applied, which gives us a group of rules, whereas the 5-neighbor or more was selected to be used in updating the 3-D CA cells values, in order to acquire high-quality random number generation.

A group of statistical tests was applied to examining the high-quality random number generation by applying the chosen rules. Thereby we found out that we have acquired random numbers of high-quality CA random number generators (RNGs).

Accordingly, and as a consequence of that a symmetric block cryptosystem was designed and built by applying nonuniform 3-D CA, as well as a nonuniform one was designed and built by using a reversible 3-D CA.

PDF created with pdfFactory trial version www.pdffactory.com

الخـــــــلاصة

إن عملية التجفير (Cryptography) هي القاعدة الأساسية للحفاظ على أمنية وتكاملية البيانات اثناء عملية نقلها عبر وسائل الاتصالات الحديثة بين الأشخاص . كما ان قوة نظام التجفير تعتمد بشكل اساسي على أمكانية توليد سلسلة من الأرقام تكون عشوائيتها قريبة جدا من الـ real randomness. أي انه يتم محاولة بناء وتصميم نظام يولد أرقام عشوائية ذات نوعية عالية (high-quality random number generator) والتي تمثل المفتاح لنظام التجفير .

في هذه الأطروحة سوف نقدم تقنية جديدة لبناء وتصميم مولد أرقام عشوائية ذات نوعية عالية (high-quality PRNGs) باستخدام الـ three-dimensional CA. وحيث ان عملية تحديث الـ CA تعتمد على الخلايا المجاورة (Neighbor cells) والـ rules المختارة لتطبيقها في عملية احتساب الحالة التالية (Next state) للـ CA . للعلم هناك مجال بحث هائل من الـ Rules التي يمكن استخدامها في عملية احتساب الحالة التالية للـ CA . ولاختيار الـ Rules التي سوف يتم استخدامها في تحديث قيم خلايا (Cells) الـ 3-D CA ، تم استخدام تقنية Cellular programming (CP) والتي تعطينا مجموعة من الـ Rules ، حيث يتم اختيار five Rules أو أكثر من هذه المجموعة لتطبيقها في تحديث قيم خلايا ال 3-D CA للحصول على سلسلة أرقام عشوائية ذات نوعية عالية .

تم تطبيق مجموعة من الاختيارات الإحصائية (Statistical tests) لاختبار مدى عشوائية سلسلة الأرقام التي تم توليدها باستخدام الـ Rules المختارة ووجدنا ان السلسلة الناتجة تجتاز هذه الـ Tests، وهذا يعني إننا حصلنا على أرقام عشوائية من الـ 3-D CA ذات نوعية عالية (high-quality CA RNGs)

نتيجة لذلك تم بناء وتصميم نظام تجفير كتلي متماثل (Symmetric Block Cryptosystem) باستخدام ال Nonuniform 3-D CA ، كذلك أيضا تم بناء وتصميم نظام تجفير كتلي متماثل باستخدام ال 3-D CA القابلة للانعكاس.

إن النظامين اللذين تم تقديهما في هذه الأطروحة تمتلك مستوى أمنية عالية (high security-level) وذلك بسبب مجال البحث الهائل جدا الذي سوف يحتاجه المعترض (Intruder) من حيث عدد الحالات ، عدد الـ Rules، الـ time steps ، والـ Initial boundary

PDF created with pdfFactory trial version www.pdffactory.com