Utilisation d'un automate cellulaire en cryptographie

Pour s'assurer de l'authenticité, l'intégrité ou la confidentialité d'une information, l'étude de procédés cryptographiques est nécessaire. Leurs applications s'étendent aujourd'hui à l'internet des objets. L'étude en cryptographie des automates cellulaires fournit une approche différente de celle de la théorie des nombres.

Une règle d'évolution est nécessaire pour définir un automate cellulaire. Cette règle considère le voisinage d'une cellule, d'où une notion d'interaction entre les cellules. De plus, un cryptosystème peut être vu comme une interface, échangeant des données avec un utilisateur.

Positionnement thématique (phase 2)

INFORMATIQUE (*Informatique Théorique*), MATHÉMATIQUES (*Autres*).

Mots-clés (phase 2)

Mots-Clés (en français)	Mots-Clés (en anglais)
<i>Automate cellulaire</i>	<i>Cellular automaton</i>
<i>Cryptographie</i>	<i>Cryptography</i>
<i>Chiffrement de Vernam</i>	<i>Vernam cipher</i>
<i>Générateur de nombres pseudo-aléatoires</i>	<i>Pseudorandom number generator</i>
<i>Fourmi de Langton</i>	<i>Langton's ant</i>

Bibliographie commentée

La théorie du chiffrement permet en cryptographie de s'assurer de la confidentialité d'une information. Cette théorie est essentielle pour communiquer ou préserver une information « *secrète* ». Le chiffrement symétrique utilise une « *clé secrète* » pour chiffrer et déchiffrer une information, contrairement au chiffrement asymétrique qui nécessite une « *clé publique* » et une « *clé privée* » [1]. L'utilisation du chiffrement symétrique peut sembler inappropriée dans le cadre d'une communication en ligne, mais une méthode « *hybride* » est en réalité souvent utilisée, par exemple pour le protocole HTTPS par un « *échange de clés* ». La théorie du chiffrement symétrique est donc toujours d'actualité.

Dans les années 1940, *Ulam* et *von Neumann* construisent une machine abstraite : le premier automate cellulaire, capable de s'autorépliquer [2]. Un automate cellulaire est une machine formelle consistant en une grille d'états, qui évoluent selon un nombre discret d'étapes en respectant une règle établie, basée sur les états des cellules d'un voisinage [2]. Le « *Jeu de la vie* » (*Game of Life*) de *Conway* en est un célèbre exemple. Dans son ouvrage principal, *Stephen Wolfram* propose d'étudier ces automates en cryptographie [3]. Les automates cellulaires sont caractérisés par des comportements complexes, chaotiques et émergents, malgré la simplicité de certaines règles de transition [4], ce qui engendre un aspect de « *hasard* ». Un automate cellulaire est chaotique parce que déterministe mais non prévisible : son comportement change radicalement pour une petite variation des conditions initiales - à la manière d'un pendule double. La notion d'émergence, est le

phénomène qui rend reconnaissable l'évolution d'un système à l'échelle macroscopique uniquement. Ainsi, la génération de nombres pseudo-aléatoires par un automate à partir d'une clé permet par la méthode de Vernam de chiffrer une information [5].

L'automate « *fourmi de Langton* » [6] inventé par *Christopher Langton* est défini par une règle simple et symétrique, mais produit une structure chaotique puis émergente. Si l'on s'affranchit de la structure émergente, l'automate semble à priori idéal pour servir de générateur de nombres pseudo-aléatoires. Pour le vérifier, des tests statistiques existent [7, 8]. Pour commencer, la fréquence d'apparition de 0 et 1 se doit d'être égale à 0,5. Le test du χ^2 permet de déterminer si le générateur suit une certaine loi de probabilité, ici une loi uniforme de 0 et 1. D'autres tests plus avancés se concentrent sur la fréquence d'apparitions successives d'un chiffre et même sur la répétition périodique d'un bloc de chiffres en utilisant une transformée de Fourier discrète.

L'article exposant la méthode du chiffrement de Vernam [5] s'intéresse uniquement au cas d'un automate cellulaire de dimension 1.

Problématique retenue

La « *fourmi de Langton* » étant un automate de dimension 2, est-il possible de généraliser la méthode décrite à cet automate ? Le résultat obtenu est-il satisfaisant ?

Objectifs du TIPE

- Dans un premier temps, une étude de l'automate présenté est nécessaire. En particulier, seule la phase chaotique est intéressante et il est nécessaire de conserver uniquement un comportement imprévisible pour l'automate.
- Ensuite, une implémentation algorithmique du procédé décrit est à effectuer, en généralisant le concept de dimension 1 en dimension 2.
- Enfin, une sélection des différents tests existants s'impose pour évaluer la qualité de la méthode - ou comprendre ses limites le cas échéant.

Abstract

Thanks to cryptography, confidentiality of data can be guaranteed. Key exchange algorithms enable symmetric ciphers to be used for online applications. *Cellular automata* are abstract machines defined on a lattice of cells, which evolves according to a rule applied on the neighborhood of each cells. Chaotic behaviours of cellular automata can be used in cryptography to generate random numbers and encrypt data thanks to a *Vernam-Shannon cipher*. To verify the quality of *random numbers generators*, a few statistical test suites exist. Langton's ant is a chaotic but emergent cellular automaton that passes this test suites on a bounded lattice.

Références bibliographiques (phase 2)

- [1] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL) : Comprendre les grands principes de la cryptologie et du chiffrement : 2016. url : www.cnil.fr/fr/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement (visité le 06/01/2018).
- [2] WIKIPÉDIA : Automate cellulaire : 2018. url : fr.wikipedia.org/wiki/Automate_cellulaire (visité le 15/08/2017).

- [3] STEPHEN WOLFRAM : A New Kind of Science : *Wolfram Media, 2002. Chap. 10, p. 598-605. isbn : 978-15795500880. url : www.wolframscience.com/nks (visité le 15/08/2017).*
- [4] STEPHEN WOLFRAM : Universality and complexity in cellular automata : *Physica D : Nonlinear Phenomena 10 (1984), p. 1-35. url : www.stephenwolfram.com/publications/academic/universality-complexity-cellular-automata.pdf (visité le 14/01/2018).*
- [5] KAR BIJAYALAXMI, RAO CHANDRASEKHRA ET RATH AMIYA KUMAR : Generating PNS for Secret Key Cryptography Using Cellular Automaton : *International Journal of Advanced Computer Science and Applications 2.5 (2011).*
- [6] CHRISTOPHER LANGTON : Studying artificial life with cellular automata : *Physica D : Nonlinear Phenomena 22 (1986).*
- [7] DAN BIEBIGHAUSER : Testing Random Number Generators : 2000. url : www-users.math.umn.edu/~garrett/students/reu/pRNGs.pdf (visité le 28/01/2018).
- [8] RUKHIN, SOTO, NECHVATAL, SMID, BARKER, LEIGH, LEVENSON, VANGEL, BANKS, HECKERT, DRAY ET VO : A statistical test suite for random and pseudorandom number generators for cryptographic applications : 2001. url : www.dtic.mil/dtic/tr/fulltext/u2/a393366.pdf (visité le 28/01/2018).

DOT

- [1] *Recherche de résultats sur les automates cellulaires et leurs rapports au chiffrement. Malgré le peu d'articles scientifiques sur le sujet, des extraits d'articles et de thèses m'ont permis d'appréhender le sujet.*
- [2] *Implémentation en Python de l'automate cellulaire : Fourmi de Langton.*
- [3] *Mise en place de la méthode du chiffrement de Vernam pour l'automate Fourmi de Langton. Le nombre d'itérations à effectuer était alors déterminé par la clé de chiffrement, ce qui posait plusieurs problèmes lors du chiffrement.*
- [4] *Contact avec le physicien Graham Medland en juin 2017 sur les propriétés chaotiques de l'automate Fourmi de Langton. Ce contact m'a permis de fixer le nombre d'itérations à effectuer, supprimant le problème précédent.*
- [5] *Recherche de résultats mathématiques sur les générateurs de nombres pseudo-aléatoires.*
- [6] *Implémentation en Python de tests statistiques vérifiant l'aspect aléatoire d'un générateur. La bibliothèque Numpy ne permettant pas de calculer le rang d'une matrice binaire de dimension supérieure à 20, j'ai dû me renseigner sur une autre bibliothèque : BinaryMatrix.*
- [7] *Implémentation en Python de la méthode de chiffrement finale, permettant de chiffrer une image, un entier ou une chaîne de caractères.*