Centre d'Etudes Doctorales : Sciences et Techniques et Sciences Médicales

Avis de Soutenance

THESE DE DOCTORAT

Présentée par

Monsieur IMAD EL HANOUTI

Discipline : Sciences et Techniques d'Information et de Communication
Spécialité : Informatique

Sujet de la thèse

Contributions to the Design and Cryptanalysis of Symmetric-Key Cryptographic Constructions Based on Discrete Dynamical Systems: Applications to Multimedia Data

Formation Doctorale " Sciences de l'Ingénieur, Sciences Physiques, Mathématiques et Informatique "

Thèse présentée et soutenue **le samedi 21 décembre 2024 à 10h** à l'Ecole Nationale des Sciences Appliquées de Fès, devant le jury composé de :

Nom et Prénom	Titre	Etablissement	
Saad BENNANI DOSSE	PES	Ecole Nationale des Sciences Appliquées de Fès	Président
Nour El Houda CHAOUI	PES	Ecole Supérieure de Technologie de Kenitra	Rapporteur
Brahim AKSASSE	PES	Faculté des Sciences de Meknès	Rapporteur
Abdelali BOUSHABA	MCH	Faculté des Sciences et Techniques de Fès	Rapporteur
Khalid ZENKOUAR	PES	Faculté des Sciences et Techniques de Fès	Examinateur
Hakim EL FADILI	PES	Ecole Nationale des Sciences Appliquées de Fès	Directeur de Thèse

Laboratoire de recherche : Laboratoire d'Informatique et de physique Interdisciplinaire
Etablissement : Ecole Nationale des Sciences Appliquées de Fès

Résumé de la thèse

L'avènement des réseaux de télécommunication modernes a considérablement élargi le champ de la communication et de l'échange d'informations. Ce progrès technologique rapide a par conséquent accentué le besoin de méthodes cryptographiques avancées, entraînant des recherches approfondies et intensives dans les domaines de la cryptographie et de la théorie de la communication.

Au début des années 1950, Claude Shannon, un ingénieur en électronique considéré par beaucoup comme le père de la cryptographie moderne, a articulé les principes fondamentaux des systèmes de secret. Shannon a utilisé la métaphore suivante pour illustrer la construction de transformations de mélange efficaces pour le chiffrement : « Les bonnes transformations de mélange sont souvent formées par des produits répétés de deux opérations simples non commutatives. Hopf a montré, par exemple, que la pâte à pâtisserie peut être mélangée par une telle séquence d'opérations. La pâte est d'abord étalée en une fine couche, puis repliée, puis roulée, et ensuite repliée à nouveau, etc. »

En termes géométriques, il est connu que l'étirement et le pliage dans l'espace de phase d'un système dynamique conduisent fréquemment à un comportement chaotique. Il est évident que Shannon a discuté d'un chemin commun vers le « chaos » à travers l'étirement et le pliage, un concept bien établi dans la théorie des systèmes dynamiques. Bien que le terme « chaos » n'ait été inventé qu'au cours des années 1970, Shannon se référait implicitement à ce concept dans ses perspectives théoriques.

Le domaine des systèmes dynamiques, en particulier l'étude des systèmes chaotiques, a été reconnu comme l'une des découvertes scientifiques majeures du siècle dernier. Bien que relativement jeune, il gagne indéniablement en importance dans une large gamme de disciplines scientifiques. Les connaissances acquises dans ce domaine sont de plus en plus essentielles pour faire progresser notre compréhension des phénomènes imprévisibles dans la nature et dans diverses sciences appliquées.

En cryptographie, nous recherchons des systèmes imprévisibles. Cette imprévisibilité est inhérente aux systèmes dynamiques chaotiques. Par exemple, l'exposant de Lyapunov positif dans les systèmes chaotiques indique quantitativement la dépendance aux conditions initiales, ce qui est le principal facteur menant à l'imprévisibilité. En cryptographie, la dépendance déterministe de la séquence cryptographique sur la graine caractérise la « sensibilité » aux paramètres et aux clés du système.

Historiquement, le défi était de développer des générateurs de nombres pseudo-aléatoires qui pouvaient fournir des nombres uniformément distribués sur l'intervalle réel [0, 1] pour les simulations informatiques impliquant des processus aléatoires. Cela impliquait d'identifier un « système dynamique chaotique » approprié, selon la terminologie actuelle, qui mappait l'intervalle [0,1] en lui-même. Une sélection courante impliquait souvent un composant de décalage unilatéral, une « carte chaotique » bien établie.

Cette relation intrigante entre le chaos dans les systèmes dynamiques et la cryptographie semble prometteuse pour explorer de nouveaux chemins dans la conception cryptographique. Cependant, de nombreux chercheurs ont étudié l'intégration de systèmes dynamiques bien connus dans la conception cryptographique depuis la fin des années 1980.

Cependant, il a été découvert que l'intégration n'est pas simple et directe. La communauté de la cryptanalyse a joué un rôle majeur en montrant que bien qu'il existe une relation très étroite entre le chaos et la cryptographie, il n'est pas simple de développer un système digne de ce nom ou de réaliser une percée majeure à ce jour.

Dans cette thèse, nos objectifs sont doubles : premièrement, nous concevrons une fonction pseudo-aléatoire et une fonction de hachage résistante aux collisions basées sur deux systèmes dynamiques mathématiques connus : la carte Tent à une dimension et la carte Hénon à deux dimensions. À partir de ces primitives, plusieurs constructions cryptographiques émergeront, y compris des codes d'authentification de message (MAC) et des chiffrements par flux et par blocs. Le deuxième objectif concerne la cryptanalyse. Positivement formulé, nous visons à identifier les faiblesses et les défauts de conception courants dans les cryptosystèmes chaotiques à travers des études de cas tirées de la littérature récente. Ce faisant, nous mettrons en lumière les pratiques à éviter lors de la conception de ces cryptosystèmes, contribuant ainsi à faire avancer le domaine de manière plus rigoureuse.

Bien que nos conclusions de conception et de cryptanalyse soient largement (et naturellement) applicables à tout type de données, nous nous concentrons spécifiquement sur les données multimédia. Ce choix est motivé par la prévalence du contenu multimédia dans le monde moderne et les exigences uniques pour le chiffrement multimédia, telles que la tolérance à la perte de données (dans les systèmes lossy), l'efficacité et la sélectivité (traitant des régions d'intérêt).

Mots clés : Cryptographie • Cryptanalyse • Constructions à clé symétrique • Chaos • Système dynamique discret • Fonction pseudo-aléatoire • Générateur pseudo-aléatoire • Système MAC • Fonction de hachage • Multimédia • Carte Hénon • Carte Tent