

MEMOIRE

présenté à l'Université de BATNA

*la faculté des sciences de l'ingénieur
département d'informatique*

**Pour l'obtention du diplôme
Magister en informatique**

**OPTION
INFORMATIQUE INDUSTRIELLE**

Par
KADRI Ouahab

Thème

**ANALYSE ET CONCEPTION D'UN MODELE DE
PROGRAMMATION PARALLELE POUR LE PROBLEME
DE LA CRYPTOGRAPHIE**

Soutenu le : .. / .. /2003 Devant le jury composé de

A. ZIDANI	<i>Maître de conférences, Université de Batna</i>	Président
M. BENMOHAMED	<i>Maître de conférences, Université de Constantine</i>	Rapporteur
B. BELATTAR	<i>Chargé de cours, Université de Batna</i>	Examineur
M. BATOUCHE	<i>Maître de conférences, Université de Constantine</i>	Examineur

Résumé

La cryptologie, on l'appelle aussi la science du secret, est une discipline mathématique. Elle regroupe la cryptographie et la cryptanalyse. Alors que le rôle des cryptographes est de construire et prouver, entre autres, des systèmes de chiffrement ou de signature, l'objectif des cryptanalystes est de casser ces systèmes.

C'est dans ce contexte que s'inscrit notre travail. L'augmentation de la taille de clé dans le nouveau standard AES a beaucoup influé sur la vitesse de chiffrement. Pour remédier à ce problème, nous essayons dans ce mémoire d'accélérer la vitesse de chiffrement et déchiffrement de l'algorithme qui est le but de ce mémoire. L'existence de la propriété de parallélisme dans Rijndael nous a permis de proposer une implémentation parallèle. Pour la réalisation, nous avons utilisé un réseau de stations de travail (RS) comme une machine parallèle puisqu'il présente un rapport coût/performance nettement favorable quand on le compare à celui des architectures parallèles classiques.

Mots clés :

Cryptologie, Cryptanalyse, Cryptographie, AES Rijndael, Architectures Parallèles, Parallélisme, Réseau de Stations de travail (RS), Chiffrement, Déchiffrement.

Abstract

The cryptology, we also call it the science of the secret, is a mathematical discipline. It regroups the cryptography and the cryptanalysis. Whereas the role of the cryptographers is to construct and to prove, among others, systems of ciphering or signature, the objective of the cryptanalysts is to break these systems.

It is in this context that appears our work. The increase of the key size in the new AES standard influenced a lot on the speed of ciphering. For remedy to this problem, we try in this thesis to accelerate the speed of ciphering and decoding of the algorithm which is the goal of this thesis. The existence of the parallelism property in Rijndael permitted us to propose a parallel implementation. For the realization, we used a network of Workstations (NOW) as a parallel machine since it presents a ratio cost/performance distinctly favorable when it compared to the one of the classic parallel architectures.

Keywords :

Cryptology, cryptanalysis, cryptography, AES Rijndael, parallel architectures, parallelism, Network of Workstations (NOW), Ciphering, Decoding.

Sommaire

LISTE DES FIGURES.....	6
LISTE DES TABLEAUX.....	8
LISTE DES ACRONYMES	9
Introduction Générale	
INTRODUCTION	10
PLAN DU MEMOIRE.....	12
Chapitre 1 Introduction A La Cryptographie	
1 INTRODUCTION	14
1.1 HISTORIQUE.....	14
1.2 DEFINITION	14
2 CRYPTOGRAPHIE.....	14
3 CRYPTANALYSE	15
4 LES METHODES DE CHIFFREMENT.....	16
4.1 LES METHODES CLASSIQUES	16
4.1.1 <i>Substitution</i>	16
4.1.2 <i>Transposition</i>	16
4.2 LES METHODES MODERNES	17
4.2.1 <i>Chiffrement symétrique</i>	17
4.2.2 <i>Chiffrement asymétrique</i>	21
4.2.3 <i>Comparaison entre la cryptographie Symétrique et Asymétrique</i>	22
4.2.4 <i>Chiffrement mixte</i>	24
4.2.5 <i>Les mécanismes cryptographiques associés</i>	25
4.3 LES METHODES FUTURES.....	27
5 LES PROTOCOLES CRYPTOGRAPHIQUES	28
5.1 LE PROTOCOLE SSL.....	28
5.2 LE PROTOCOLE HTTPS.....	28
5.3 LE PROTOCOLE IPSEC	28
6 CONCLUSION	29
Chapitre 2 Les Algorithmes Symétriques	
1 INTRODUCTION	30
2 ALGORITHME DES.....	30
2.1 HISTORIQUE	30
2.2 DESCRIPTION	30

2.3 DECHIFFREMENT DU DES	32
2.4 LA SECURITE	33
2.4.1 <i>La recherche exhaustive de la clé</i>	33
2.4.2 <i>La cryptanalyse différentielle</i>	33
2.4.3 <i>Cryptanalyse linéaire</i>	33
2.5 LE TRIPLE-DES	34
2.6 LA VITESSE	34
3 ALGORITHME IDEA.....	35
3.1 HISTORIQUE	35
3.2 DESCRIPTION	35
3.3 LA SECURITE	37
3.4 LA VITESSE	37
4 RIJNDAEL ET L' AES	37
4.1 HISTORIQUE	37
4.2 DESCRIPTION	38
4.3 LA SECURITE	40
4.4 LA VITESSE	40
5 POURQUOI RIJNDAEL.....	40
5.1 LA SECURITE	40
5.2 LA VITESSE	41
5.3 L'UTILISATION	41
6 CONCLUSION	42
Chapitre 3 Les Architectures Parallèles	
1 INTRODUCTION	43
1.1 HISTORIQUE	43
2 ARCHITECTURES DES MACHINES PARALLELES	43
2.1 DEFINITIONS	43
2.2 CLASSIFICATION DE FLYNN	44
3 LES ARCHITECTURES SIMD.....	45
4 LES ARCHITECTURES MIMD	46
4.1 MACHINE PARALLELE MIMD A MEMOIRE CENTRALISEE.....	46
4.1.1 <i>Multiprocesseurs à bus</i>	46
4.1.2 <i>Multiprocesseurs vectoriels et accès mémoire uniforme</i>	47
4.2 MACHINE PARALLELE MIMD A MEMOIRE DISTRIBUEE.....	47
4.2.1 <i>Machine parallèle à passage de message</i>	48
4.2.2 <i>Machine MIMD à espace d'adressage unique</i>	50
5 RESEAUX D'INTERCONNEXION	51
6 MODES DE COMMUNICATION	53
7 CONCLUSION	54

Chapitre 4 Les Algorithmes Parallèles

1 INTRODUCTION	55
2 PARALLELISME.....	55
2.1 DEFINITIONS	55
2.2 MOTIVATIONS POUR LE PARALLELISME	55
2.2.1 <i>Besoins des applications</i>	55
2.2.2 <i>Limites de l'approche microprocesseur</i>	56
2.3 CONTRAINTES SUR LE PARALLELISME.....	56
2.3.1 <i>Dépendance de données</i>	56
2.3.2 <i>Dépendance de contrôle</i>	57
2.3.3 <i>Dépendance de ressource</i>	57
3 LES TYPES DE PARALLELISME.....	58
3.1 PARALLELISME DE DONNEES.....	58
3.2 PARALLELISME DE CONTROLE.....	59
3.3 PARALLELISME DE FLUX	60
4 ENVIRONNEMENT DE PROGRAMMATION.....	60
4.1 LES BLAS.....	61
4.2 LAPACK.....	61
4.3 ARPACK	61
4.4 OPEN MP	61
4.5 PVM.....	62
4.6 MPI.....	62
4.7 HPF	62
5 LE GRAIN ET LE DEGRE DU PARALLELISME	62
5.1 GRANULARITE FINE.....	63
5.2 GRANULARITE MOYENNE.....	63
5.3 GRANULARITE FORTE.....	64
6 EVALUATION DU PARALLELISME.....	64
7 CONCLUSION	67

Chapitre 5 Spécification De L'algorithme Rijndael

1 INTRODUCTION	68
2 LES ETATS DE RIJNDAEL.....	68
3 LE CHIFFREMENT	68
3.1 LA TRANSFORMATION SUBBYTES.....	69
3.2 LA TRANSFORMATION SHIFTRAWS	71
3.3 LA TRANSFORMATION MIXCOLUMNS	72
3.4 LA TRANSFORMATION XORROUNDKEY.....	73
4 GENERATION DES CLES (<i>KEY SCHEDULE</i>).....	74
5 LE DECHIFFREMENT.....	75
5.1 LA TRANSFORMATION INVERSE DE SHIFTRAWS.....	76

5.2 LA TRANSFORMATION INVERSE DE SUBBYTES	76
5.3 LA TRANSFORMATION INVERSE DE XORROUNDKEY.....	77
5.4 LA TRANSFORMATION INVERSE DE MIXCOLUMNS.....	77
6 COMPLEXITE DE RIJNDAEL.....	78
7 CONCLUSION.....	79
Chapitre 6 Implémentation Parallèle De L'algorithmme Rijndael	
1 INTRODUCTION	80
2 ARCHITECTURE MATERIELLE.....	80
2.1 ETHERNET.....	80
2.1.1 Principes de base.....	81
2.1.2 Evolution de réseau Ethernet.....	81
2.2 CONFIGURATION DU RESEAU.....	82
2.3 OUTILS LOGICIELS.....	83
2.3.1 Le <i>pacquage FastNet</i>	83
3 DESCRIPTION GENERALE DU LOGICIEL R-SPMD	84
3.1 SYSTEME DE CRYPTAGE	84
3.2 L'INTERFACE DU LOGICIEL.....	84
3.3 PRINCIPE DE FONCTIONNEMENT	84
3.4 CARACTERISTIQUES DU MODELE.....	85
3.4.1 <i>Architecture client/serveur</i>	85
3.4.2 <i>Multithreads</i>	86
4 BIBLIOTHEQUE DE COMMUNICATION	87
4.1 PROPRIETES DES COMMUNICATIONS	87
4.2 DEROULEMENT D'UNE COMMUNICATION.....	87
4.2.1 <i>Les méthodes d'envoi</i>	87
4.2.2 <i>Les méthodes de réception</i>	88
5 BIBLIOTHEQUE DE CRYPTAGE.....	89
5.1 STRUCTURES DE DONNEES	89
5.1.1 <i>Les états</i>	89
5.1.2 <i>Les clés</i>	89
5.1.3 <i>Les tables de substitution</i>	89
5.2 LES METHODES DE CRYPTAGE.....	90
6 LES COMMUNICATIONS	90
7 EXPERIMENTATION ET DISCUSSION	93
7.1 CONDITIONS D'EXPERIMENTATION	93
7.2 L'EXPERIMENTATION.....	93
7.2.1 <i>Calcul de la vitesse</i>	93
7.2.2 <i>Calcul de l'accélération</i>	94
8 CONCLUSION.....	95

Conclusion Générale

CONCLUSION.....97

BIBLIOGRAPHIE.....99

Annexes**Annexe A**1 LE CHAMP $GF(2^8)$ 103

2 LES OPERATIONS.....103

2.1 L'ADDITION103

2.2 LA MULTIPLICATION103

2.3 MULTIPLICATION PAR X.....104

3 POLYNOMES AVEC COEFFICIENTS DANS $GF(2^8)$ 104

4 MULTIPLICATION PAR X.....105

Annexe B

1. INSTALLATION.....106

2. CRYPTER UN FICHIER.....106