REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE D'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

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

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

A. ZIDANI	*Maître de conférences,* Université de Batna	***Président***
M. BENMOHAMED	*Maître de conférences*, Université de Constantine	***Rapporteur***
B. BELATTAR	*Chargé de cours,* Université de Batna	***Examinateur***
M. BATOUCHE	*Maître de conférences,* Université de Constantine	***Examinateur***

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 cryptanalys. Whereas the role of the cryptographers is to construct and to prove, among others, systems of ciphering or signature, the objectif of the cryptanalystes 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 witch is the goal of this thesis. The existence of the parallelism property in Rijndael permitted us to propose a parallel implémentation. 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

Chapitre 4 Les Algorithmes Parallèles

Chapitre 5 Spécification De L'algorithme Rijndael

Chapitre 6 Implémentation Parallèle De L'algorithme Rijndael