Republic of Iraq
Ministry of Higher Education
& Scientific Research
University of Technology
Department of Computer Science

# Accelerating High Performance Symmetric Ciphers Multicore CPU

A THESIS
SUBMITTED
TO THE DEPARTMENT OF COMPUTER SIENCE
UNIVERSITY OF TECHNOLOGY
IN A PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN
COMPUTER SIENCE

By
**Aseel Ali Hussein Abood**

Supervised by
**Prof. Dr. Abdul Monem S. Rahma**

2015 1437

# الخلاصة

ان استخدام الحواسيب متعددة النوى كان مقتصرا على نظام التشغيل و البرامج العامة التابعة له. و لغرض الاستغلال الكلي لهذه الفائدة في انظمة الحواسيب الحديثة وجب توجيه البرمجة الموازية لتطبيقها على البرامج المستقلة المصممة مبدئيا للبرمجة المتسلسلة، و هذا هو الهدف الرئيسي لهذه الاطروحة.

تقنيات المعالجة الحديثة تقدم تطويرا مهما يتمثل بوصول الحواسيب ذات المعالجة المتوازية الى غالبية المبرمجين و المستخدمين. لكن المشكلة الاساسية تكمن في عدم مقابلة هذا التطوير بتطوير يقابله في مجال البرمجة الموازية. و برغم ان غالبية الاجهزة الحالية متعددة النوى و مهيأة للبرمجة المتوازية الا ان غالبية البرامج الحالية لا تزال تعالج بطريقة متسلسلة.

الانظمة الامنية في يومنا هذا تمتلك متطلب مهم يتمثل في ضرورة كونها عالية السرعة لان المعلومات السرية يتم نقلها في شبكات عالية السرعة. لذا فمن الضروري معالجتها في اقل مدة ممكن توفيرها في هذا العصر المتطلب للسرعة. و من طرق زيادة هذه السرعة هو تطبيق المعالجة المتوازية.

اساس الفكرة يكمن في استخدام البرامج المستقلة و تحديدا طريقة تشفير كمثال لحالة معالجة متوازية. طريقة التشفير الكتلية هذه لا تزال تطبق بشكل متسلسل برغم تعقيدها و الحجم الهائل من البيانات التي تستخدم لتشفيرها و كذلك العدد الكبير من خطواتها المتكررة التي تستغرق وقتا ملحوظا لتنفيذها. الطريقة المقترحة تتضمن اعادة كتابة البرنامج ليماشي في عمله توفر وحدات المعالجة المتعددة المذكورة انفا من اجل الاستغلال الكامل للخوارزمية المذكورة اعلاه.

هذه الطرق توفر سرعة تنفيذ اعلى لغالبية خوارزميات معالجة البيانات التي تستطيع اختصار للنصف و في بعض الاحيان اكثر من ذلك في المستقبل القريب. و هذا السبب من الاسباب الرئيسية لدمج خوارزمية التشفير مع المعالجة المتوازية. حيث ان امن البيانات يقدر في بعض الاحيان كعبء على المستخدم مما يدفعه في بعض الاحيان الى تلافيها او حتى اهمالها من اجل اختصار وقت التنفيذ. لذلك فان ادخال البرمجة المتوازية كحل سوف ينفي الحاجة الى التخلي عن امنية البيانات في صالح اختصار الوقت اذ انها لن تتعارض تقريبا. و هذا الطتبيق قد قاد الى زيادة ملحوظة في السرعة وصلت الى 58%. ما يعتبر نسبة عالية مقارنة بسرعة التنفيذ بالطريقة التسلسلية التقليدية ما قد يقود المبرمجين في المستقبل الى التركيز على هذه الطريقة البرمجية في تصميم برامجهم في المستقبل القريب.

جمهورية العراق

وزارة التعليم العالي والبحث العلمي

الجامعة التكنولوجية

قسم علوم الحاسوب

# تسريع التشفير المتناظر عالي الجودة في المعالجات متعددة النوى

اطروحة مقدمة الى قسم علوم الحاسوب

الجامعة التكنولوجية

وهي جزء من متطلبات نيل درجة ماجستير

في علوم الحاسبات

من قبل

**أسيل علي حسين عبود**

بإشراف

**أ.د. عبد المنعم صالح رحمة**

1437هـ 2015م