Treball de Final de Grau “Enginyeria Informàtica”

Curs 2017-2018

Rendiment dels algorismes de xifratge en Embedded Systems mitjançant un HSM (Hardware Security Module)

Alumne: Joan Canals Mascorda  
Tutor: David Gómez Alari  
Universitat Rovira i Virgili  
ETSEI  
[joancanals95@gmail.com](mailto:joancanals95@gmail.com)

Índex del Treball

[1. Abstract 3](#_Toc519013987)

[2. Preàmbul 4](#_Toc519013988)

[I. Introducció 4](#_Toc519013989)

[II. Motivació personal 4](#_Toc519013990)

[3. Especificació tècnica dels dispositius 4](#_Toc519013991)

[I. Raspberry Pi 3B Plus 4](#_Toc519013992)

[II. HSM 4](#_Toc519013993)

[III. Dispositiu Android 4](#_Toc519013994)

[4. Llenguatges, funcionament i fragments de codi 4](#_Toc519013995)

[I. Raspberry 4](#_Toc519013996)

[II. HSM 4](#_Toc519013997)

[III. Android APP 4](#_Toc519013998)

[5. Característiques dels criptosistemes 4](#_Toc519013999)

[I. AES 4](#_Toc519014000)

[II. 3DES 4](#_Toc519014001)

[III. Camellia 4](#_Toc519014002)

[6. Estudi 4](#_Toc519014003)

[7. Conclusions 4](#_Toc519014004)

[8. Bibliografia i Webgrafia 4](#_Toc519014005)

[9. Paraules clau 4](#_Toc519014006)

[10. Annex 5](#_Toc519014007)

[I. Especificació tècnica dels dispositius 5](#_Toc519014008)

[i. Raspberry Pi 3B Plus 5](#_Toc519014009)

1. Abstract
   1. *words, in Engish.*
2. Preàmbul
   1. Introducció

La intenció d’aquest treball de final de grau és veure i estudiar el rendiment d’un sistema encastat alhora d’encriptar i desencriptar fitxers de diferents dimensions i extensions, utilitzant els recursos primaris del mateix sistema, comparant-ne els resultats obtinguts amb les dades de les operacions d’un xip **HSM**[[1]](#footnote-1) dedicat especialment a dur aquest tipus de tasques.

Ambdós tests realitzen el mateix càlcul amb el mateix fitxer. La qüestió és veure i poder analitzar quant és realment necessari disposar d’un xip dedicat per a realitzar depenent de quines encriptacions, i el nivell d’estrès que pot arribar a suportar un sistema encastat quan se li demana encriptar depenent de quin fitxer.

Aquests tipus de sistemes encastats utilitzen sistemes d’encriptació lleugers, o *‘****Lightweight cryptography****’*, últimament en més ús i en ple desenvolupament gràcies al **IoT**.

* 1. Motivació personal

La motivació personal que m’ha fet escollir aquest treball de fi de grau ve marcada pel fet que durant la realització de la carrera em van cridar molt l’atenció dos assignatures que mostraven dos camps diferenciats dins del món de la informàtica: el camp de la seguretat informàtica; i el camp dels sistemes encastats.

Així doncs, i gràcies a un encaminament adient del meu tutor del treball, vaig decidir fer un estudi que engloba els dos camps, podent així interpretar-los i gaudir-los en més detall.

1. Especificació tècnica dels dispositius

A continuació hi ha una breu descripció dels dispositius emprats durant la realització de l’estudi, per a poder justificar les dades obtingudes.

Abans de continuar, a l’apartat d’Annex hi ha un seguit de fotografies dels dispositius i les especificacions físiques dels mateixos.

* 1. Raspberry Pi 3B Plus

Sistema encastat que ha estat utilitzat per a realitzar l’estudi, aquí una molt breu descripció tècnica del dispositiu:

* Processador: Broadcom BCM2837B0, Cortex-A53 64-bit SoC.
* Freqüència del processador: 1.4 GHz
* Memòria: 1GB LPDDR2 SDRAM
  1. HSM
  2. Dispositiu Android

1. Llenguatges, funcionament i fragments de codi
   1. Raspberry
   2. HSM
   3. Android APP
2. Característiques dels criptosistemes
   1. AES
   2. 3DES
   3. Camellia
3. Estudi
4. Conclusions
5. Bibliografia i Webgrafia

* Web oficial de Zymbit, per a la compra del mateix i les especificacions tècniques i de la utilització de la API:  
  <https://www.zymbit.com/keys-to-security-raspberry-pi/>
* Fòrum oficial de Raspberry Pi, per a la consulta d’informació tècnica i resolució de bugs:  
  <https://www.raspberrypi.org/forums/>
* Fòrum d’Stack Overflow, per a la consulta de comandes Android i algunes comandes de Python:  
  <https://stackoverflow.com>

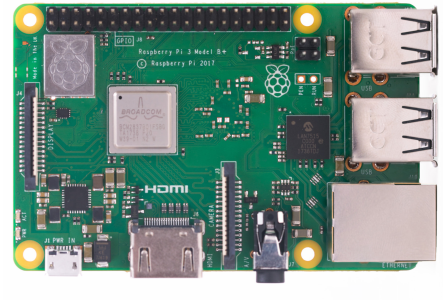
1. Paraules clau

**HSM:** Hardware Security Module, o mòdul de seguretat dedicat, és el Hardware que desenvolupa les tasques dedicades d’encriptació i desencriptació.

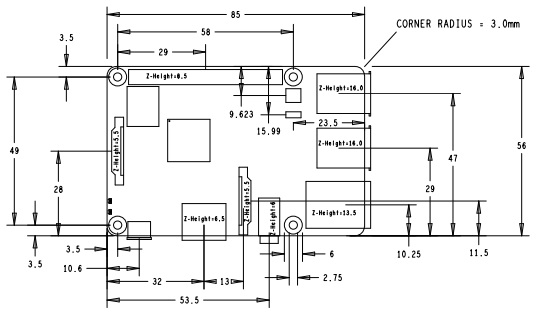
**IoT:** Internet of Things o Internet de les Coses.

**Lightweight cryptography:** Criptosistemes lleugers, són els criptosistemes que pretenen actuar com un sistema d’encriptació i desencriptació normal, utilitzant menys recursos i sent igual o millor d’eficaços i eficients.

1. Annex
   1. Especificació tècnica dels dispositius
      1. Raspberry Pi 3B Plus



* **Resum**
  + Processador: Broadcom BCM2837B0, Cortex-A53 64-bit SoC @ 1.4 GHz
  + Memòria: 1GB LPDDR2 SDRAM
  + Connectivitat Bluetooth: 2.4 GHz i 5 GHz IEEE 802.11 .b/g/n/ac wireless LAN, Bluetooth 4.2, BLE
  + Accés: Extended 40-pin GPIO header
* **Especificacions físiques**



1. Tota paraula en negreta té la seva explicació i/o traducció en l’apartat *‘9. Paraules Clau’*. [↑](#footnote-ref-1)