先進加解密標準演算法硬體電路之實現

學生:郭昌華　　指導教授:葉義雄教授
陳紹基教授
國立交通大學　電機學院　電子與光電學程碩士班

摘要

先進加解密演算法已成為全世界密碼學公認的標準。在先進加解密系統研究分為軟體及硬體電路。本論文我們著重高速度電路為主要目標並採平行架構。

在本論文中，提出一個新的方法來實現先進加解密密碼系統之架構。整個先進加解密密碼系統電路及金鑰擴展電路，利用查表法取代複雜運算電路。在硬體實現我們利用唯讀記憶體、互斥或閘及多工器來實現電路。首先，在功能驗證模擬方面，我們以 MATLAB 語言程式來模擬。其次，在 RTL 模擬驗證方面，我們利用 verilog HDL 建立系統並加以驗證。在電路合成部份，我們使用聯電 0.13um CMOS 標準元件庫來合成我們的電路。在加密部份，對於資料路徑 128 位元，工作頻率最高可達 204MHZ 左右，頻寬輸出 2.6Gbps,總閘數 273k; 在解密部份，對於資料路徑 128 位元，工作頻率最高可達 200MHZ 左右，頻寬輸出 2.56Gbps,總閘數 461k。

關鍵字: 先進加解密演算法,查表法

Table base implementation of AES hardware circuit

Student: Chang-Hwa Kuo

Advisors：Dr. Yi-Shiung Yeh

Dr. Sau-Gee Chen

Degree Program of Electrical and Computer Engineering

National Chiao Tung University

ABSTRACT

The advanced encryption standard (AES) algorithm has been standardized in cryptography all over the world. The research of AES focus on two areas: One is the software simulation and the other is the hardware implementation. In this thesis, a table-based high-speed AES ASIC design is proposed with a parallel structure.

A look-up table approach instead of complicated circuits is exploited to realize the AES algorithm, included the encryption, the decryption, and the key-expand, whose circuits are implemented by ROM table, XOR gate, and multiplexer. First, we use Matlab platform to do AES function simulation. Then, we use Verilog HDL to build and verify the AES system in RTL level. Finally, the proposed HDL code is synthesized with UMC 0.13um CMOS process. In the encryption with the 128 bits data path, it shows that the operating frequency can be over 204MHz, to provide the 2.6Gbps data throughput. The total gate counts is about 273k. Moreover, the complexity of decryption is 461k gates whose clock rate can achieve 200MHz to supports the 2.56Gbps throughput in the 128 bits data path.

Keyword: AES, look-up table

誌 謝

本論文順利完成，首先特別感謝葉義雄老師，這一年多來諄諄教誨與細心指導才會有本論文的產生。同時也謝謝陳紹基老師的寶貴意見。也謝謝黃定宇學長精神鼓勵，尤其我多次想放棄的時候，黃定宇學長總能默默鼓舞，使我能繼續完成學業。

其次，感謝我的父母，你們總是全力支持我與鼓勵我。把我當作小樹一樣灌溉，並期盼有一天我能成為大樹，如今論文完成之際，也獻給我最愛的父母與家人。

目錄

頁次

中文摘要…… i

英文摘要…… ii

誌謝…… iii

目錄…… iv

表目錄…… vi

圖目錄…… vii

一、 緒論…… 1

1.1 研究動機…… 1

1.2 研究方向…… 1

1.3 章節概要…… 2

二、 NIST AES 標準規範…… 3

2.1 AES 演算法參數…… 3

2.2 AES 加密演算法的運算函數…… 4

2.2.1 SubBytes 函數…… 4

2.2.2 ShiftRows 左旋轉位移函數…… 5

2.2.3 MixColumns 函數…… 5

2.2.4 AddRoundKeys 函數…… 6

2.3 AES 解密演算法的運算函數…… 6

2.3.1 InvSubBytes 函數……7

2.3.2 InvShiftRows 右旋轉函數…… 8

2.3.3 InvMixColumns 反混行運算……8

2.4 相關硬體研究工作…… 9

三、 AES 硬體電路架構實現……10
3.1 平行架構硬體實現方式…… 10
3.2 新架構加密電路實現…… 10
3.2.1 加密電路流程…… 10
3.2.2 平行架構整合查表法(加密電路) …… 12
3.3 新架構解密電路實現……21
3.3.1 解密電路流程……21
3.3.2 平行架構整合查表法(解密電路) ……22
3.4 加密金鑰擴展…… 32
3.5 解密金鑰擴展…… 33
四、 設計驗證…… 35
4.1 功能模擬…… 36
4.1.1 定點資料……36
4.1.2 AES 功能模擬……36
4.2 HDL 設計與驗證……37
4.3 邏輯閘合成模擬驗證……41
五、 設計結果與比較……44
5.1 實驗設計結果……44
5.2 實驗結果比較……45
六、 結論與展望……47
6.1 結論……47
6.2 未來展望……47
參考文獻……48
簡歷…… 51

表目錄

頁次

表 2.1 運算回合數N_r與N_b和N_k之關係…… 3

表 2.2 S-box 位元轉換對照表…… 5

表 2.3 InvS-box 位元轉換對照表…… 7

表 3.1 2P 轉換對照表表格……15

表 3.2 3P 轉換對照表表格……15

表 3.3 9R 轉換對照表表格……25

表 3.4 bR 轉換對照表表格……25

表 3.5 dR 轉換對照表表格……26

表 3.6 eR 轉換對照表表格……26

表 5.1 AES-128 實作結果(一般方法)…… 44

表5.2 AES-128實作結果(平行架構整合查表法改良結果)…… 44

表 5.3 實驗結果比較…… 45

圖目錄

頁次

圖 3.1 新架構 AES-128 加密電路流程圖…… 11

圖 3.2 經 AddRoundKey 函數處理所得結果…… 12

圖 3.3 經 SubBytes 函數處理所得結果…… 12

圖 3.4 經 ShiftRows 函數處理所得結果…… 13

圖 3.5 加密每回合平行架構電路圖(一)…… 16

圖 3.6 加密每回合平行架構電路圖(二)…… 17

圖 3.7 加密最後回合平行架構電路圖…… 20

圖 3.8 新架構 AES-128 解密電路流程圖……21

圖 3.9 經 AddRoundKey 函數處理所得結果…… 22

圖 3.10 經過 InvSubBytes 函數處理所得結果…… 22

圖 3.11 經過 InvShiftRows 處理所得結果…… 23

圖 3.12 解密每回合整合運算電路架構圖(一)…… 27

圖 3.13 解密每回合整合運算電路架構圖(二)…… 28

圖 3.14 解密最後回合整合運算電路架構圖…… 31

圖 3.15 AES-128 加密金鑰擴展電路流程圖…… 33

圖 3.16 AES-128 解密金鑰擴展電路流程圖…… 34

圖 4.1 設計驗證流程…… 35

圖 4.2 Matlab 程式模擬 AES-128 加密…… 36

圖 4.3 Matlab 程式模擬 AES-128 解密…… 37

圖 4.4 Modelsim 模擬驗證流程…… 38

圖 4.5 AES-128 加密模擬…… 39

圖 4.6 AES-128 解密模擬…… 39

圖 4.7 AES-128 加密擴展電路模擬…… 40

頁次

圖 4.8 AES-128 解密擴展電路模擬…… 40

圖 4.9 邏輯閘合成驗證流程……42

圖 4.10 AES 加密 Synopsys 模擬輸出…… 43

圖 4.11 AES 解密 Synopsys 模擬輸出…… 43