義守大學
資訊工程學系

畢業專題

AES 硬體實現效率提升

專題學生　楊立驊(11003101A)
顏孜諭(11003051A)
黃修承(11003076A)
王宥絜(11003102A)
呂采庭(11003064A)
徐瑋琪(11003110A)
指導教授　陳延華 教授

中華民國一一四年一月

目 錄

圖目錄

摘 要

本計畫旨在透過減少 AES（Advanced Encryption Standard）運算過程中的乘法次數，實現硬體效率的顯著提升。以 Quartus II 為設計平台，針對 AES 的運算模組進行優化，減少乘法操作所需的資源與時間開銷。研究成果將通過 FPGA 平台進行驗證，預期在加密性能、功耗及延遲方面均能取得明顯的改善，為嵌入式系統及物聯網設備提供更高效的加密解決方案。

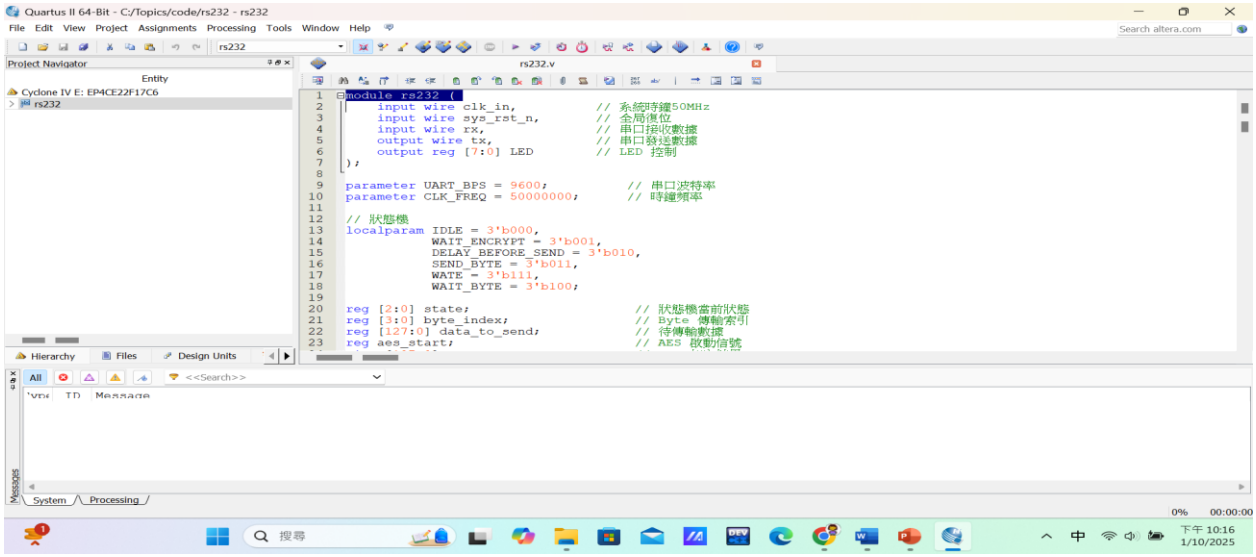
一、簡介

AES（Advanced Encryption Standard）運算中，乘法操作通常是導致性能瓶頸的主要原因，因其計算複雜度相對較高，對硬體資源需求也更大。本計畫專注於減少 AES 中乘法運算的次數，以降低硬體資源使用及加快加密過程的執行速度。通過使用 Quartus II 平台進行設計與模擬，研究將探索高效模組設計的可行性，並在 FPGA 上測試其性能表現。預期的技術成果包括優化運算模組結構、縮短數據處理延遲以及提升系統整體吞吐量，從而實現 AES 硬體實現的高效能化。

二、研究環境與設備

2-1 研究環境

使用 Quartus II 平台進行設計與模擬，選用的晶片為 EP4CE22F17C6，並將要燒入程式的硬體連接電腦，電腦透過此軟體燒入程式。



圖一、程式開發

使用 IDLE(Python 3.12 64-bit)進行介面的開發

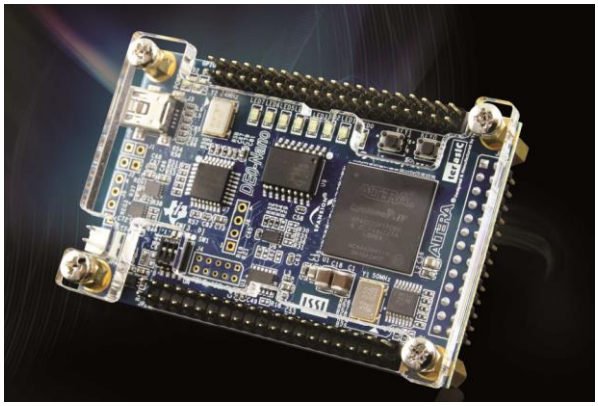
圖二、介面開發

2-1 研究設備

USB TO UART RS232: 此線有四個接腳，分別是 RX、TX、VCC、GND，這是四線連接到影體上，USB 頭連接電腦。

圖三、USB TO UART RS232

DE0: 一個緊湊型的 FPGA 開發平台，非常適合用於原型電路設計。此開發板專為 Cyclone IV 裝置設計，最多支援 22,320 個邏輯單元（LEs），以最簡單的方式實現應用。DE0-Nano 板的優勢在於其小巧的體積和重量，並能在不攜帶多餘硬體的情況下重新配置，這使其有別於其他通用型開發板。



圖四、DE0-Nano

三、研究方法與過程

3-1 平方部分

從原本是直接使用一個乘法器做平方，到變成是先乘完，透過係數的位移完成平方的結果，以 GF(2^3)來舉例，算式如下

$f(x)=x^3+x+1$

$(a_2x^2+ a_1x^1 +a_0)^2$

$=a_2^2x^4+ a_1^2x^2+ a_0^2+ a_2a_1x^3+ a_2a_1x^3+ a_2a_0x^2+ a_2a_0x^2+ a_1a_0x+ a_1a_0x$

$=a_2^2x^4+ a_1^2x^2+ a_1^2$

$=a_2x^4+ a_1x^2+ a_0$

$=a_2x^2+ a_2x+ a_1x^2+ a_0$

$=(a_2+ a_1)x^2+ a_2x+ a_0$

在有限體數學中，相同的數相加會抵消，有顏色的部分會抵消，且係數只有 0 跟 1，所以 a_2^2 a_1^2 a_1^2有沒有平方都一樣，最後 a_2x^4超過 f(x)的最高次方，因此要取餘數，取完後變成 $a_2x^2+ a_2x$，利用這種方法，可以在不使用乘法器的情況下，透過位移係數，來達到平方器的效果。

3-2 反元部分

$$A^{-1}=A^{2^8-2}$$

在 GF(2^8)中，

而通過費馬小定理 $2^8-2=2^7+2^6+2^5+2^4+2^3+2^2+2^1$

我們可以得出以下算式，並開始製作電路

$$2^8-2$$

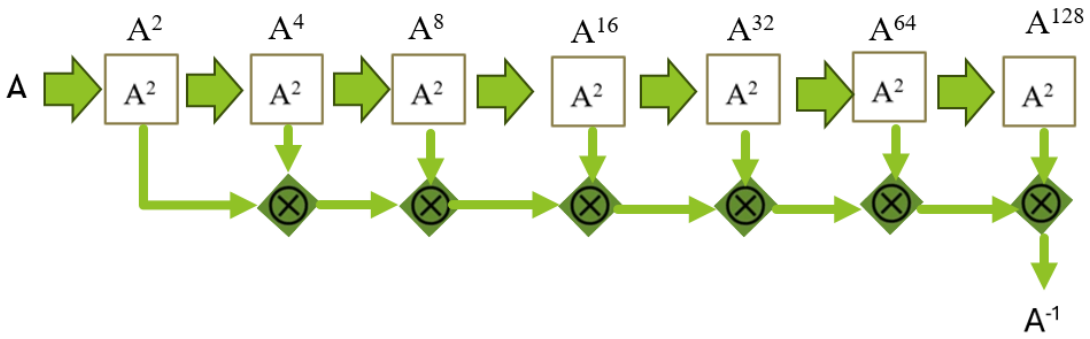
$$=2^7+2^6+2^5+2^4+2^3+2^2+2^1$$

$$=(2^7+2^6+2^5)+(2^4+2^3+2^2)+2^1$$

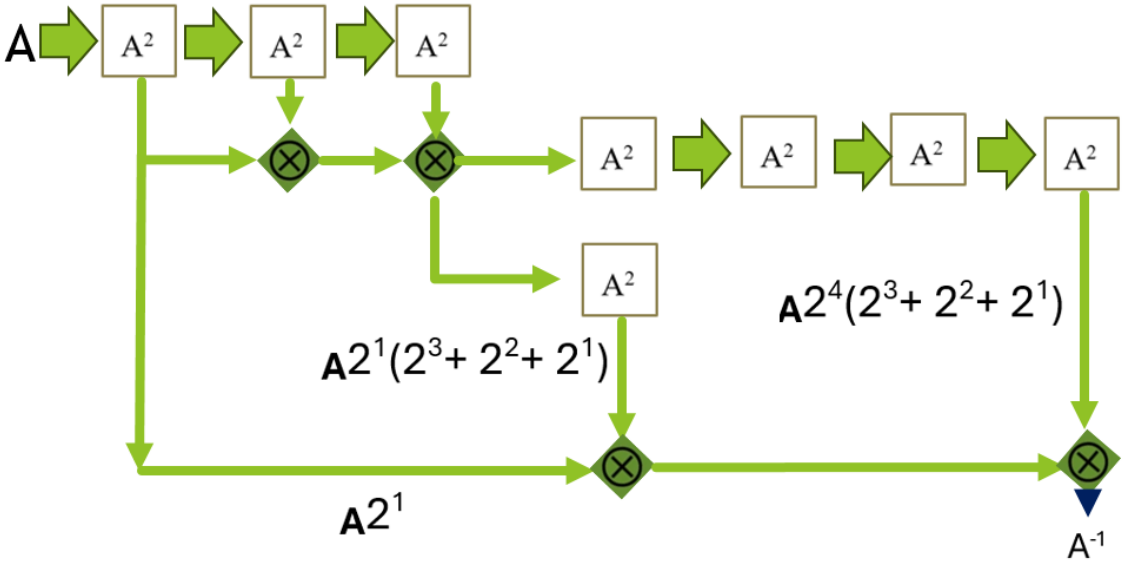
$$=2^4(2^3+2^2+2^1)+2^1(2^3+2^2+2^1)+2^1$$

$$=A^{2^4}(2^3+2^2+2^1)\times A^{2^1}(2^3+2^2+2^1)\times A^{2^1}$$

圖五、反元計算化簡



圖六、反元電路改良前

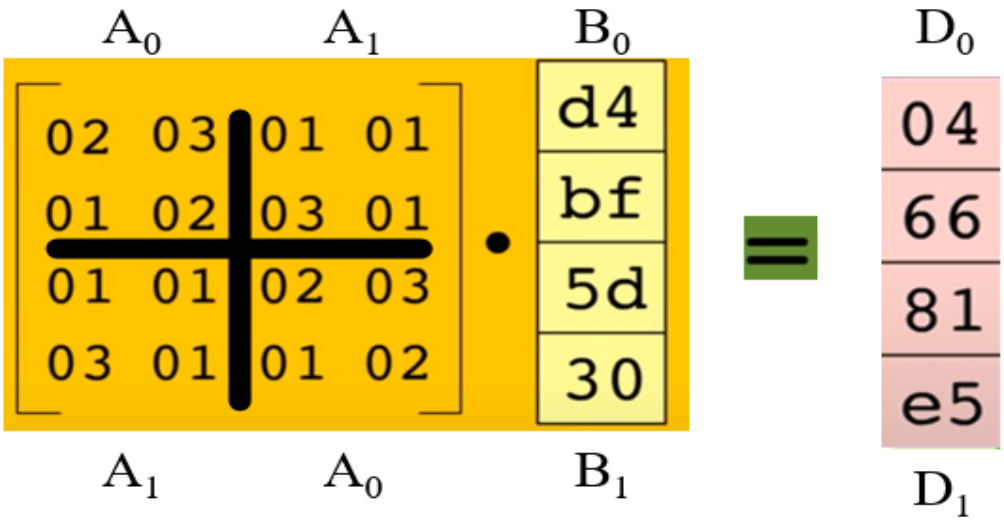


圖七、反元電路改良後

從使用 6 個乘法下降到只使用 4 個乘法。

3-1MixColumns 部分

透過以下方式切割矩陣



$D_0 = A_0 B_0 + A_1 B_1$
$D_1 = A_0 B_1 + A_1 B_0$

4個乘2個加

圖八、MixColumns 矩陣運算

- $A_0 B_0 + A_1 B_1 = A_0 B_0 + A_0 B_1 + A_0 B_1 + A_1 B_1 =$
- $A_0(B_0 + B_1) + (A_0 + A_1) B_1$

$A_0(B_0 + B_1) = T$
$(A_0 + A_1) B_1 = F$
$(A_0 + A_1) B_0 = G$

- $A_0 B_1 + A_1 B_0 = A_0 B_0 + A_0 B_1 + A_0 B_0 + A_1 B_0 =$
- $A_0(B_0 + B_1) + (A_0 + A_1) B_0$

$T + F = D_0$
$T + G = D_1$

圖九、MixColumns 運算化簡

由於在有限體數學中，相同的數相加會抵消，紅字的部分會抵消，而藍字跟黃底的部分因為重複了，所以算過就不用再算了，因此從4個乘2個加變成3個乘4個加，雖然加法的數量增加了，但乘法減少，乘法的運算量，比加法多很多，所以是賺的，可以加快效率。

四、研究結果

Flow Summary	
Flow Status	Successful - Thu Jan 02 19:36:35 2025
Quartus II 64-Bit Version	13.0.1 Build 232 06/12/2013 SP 1 SJ Web Edition
Revision Name	a2_function
Top-level Entity Name	a2_function
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	54 / 22,320 (< 1 %)
Total combinational functions	54 / 22,320 (< 1 %)
Dedicated logic registers	0 / 22,320 (0 %)
Total registers	0
Total pins	24 / 154 (16 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

圖十、平方改良前

Flow Summary	
Flow Status	Successful - Thu Jan 02 19:34:23 2025
Quartus II 64-Bit Version	13.0.1 Build 232 06/12/2013 SP 1 SJ Web Edition
Revision Name	a2_function
Top-level Entity Name	a2_function
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	8 / 22,320 (< 1 %)
Total combinational functions	8 / 22,320 (< 1 %)
Dedicated logic registers	0 / 22,320 (0 %)
Total registers	0
Total pins	16 / 154 (10 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

圖十一、平方改良後

Total logic elements 從 54 減少至 8，54/8 等於 6.75 ，也就是提升 6.75 倍。

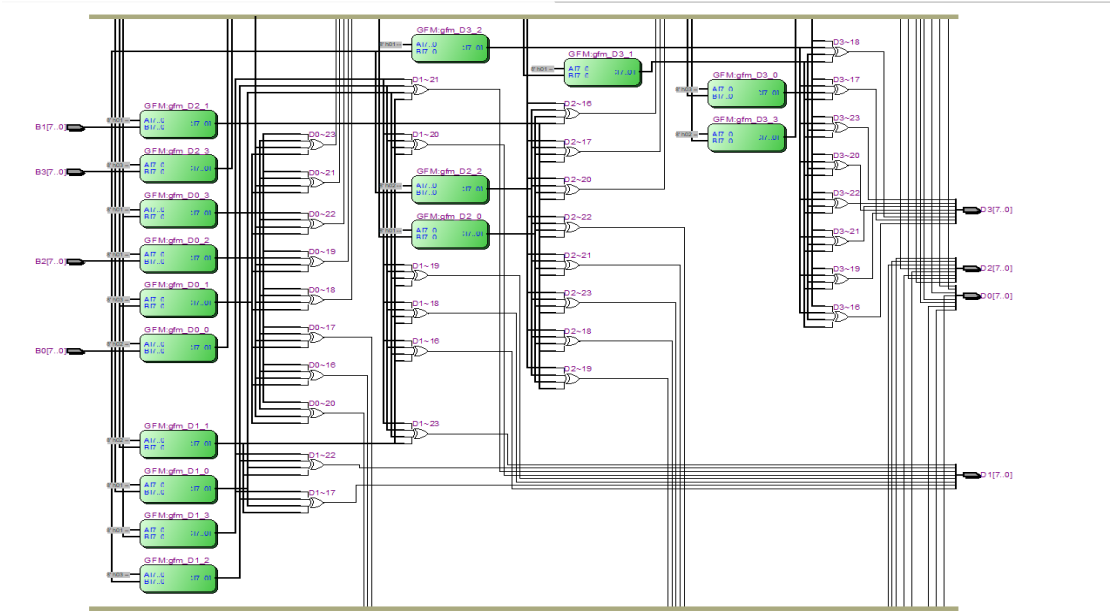
Flow Summary	
Flow Status	Successful - Tue Dec 31 13:20:52 2024
Quartus II 64-Bit Version	13.0.1 Build 232 06/12/2013 SP 1 SJ Web Edition
Revision Name	inv
Top-level Entity Name	inv
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	377 / 22,320 (2 %)
Total combinational functions	377 / 22,320 (2 %)
Dedicated logic registers	0 / 22,320 (0 %)
Total registers	0
Total pins	16 / 154 (10 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

圖十二、反元改良前

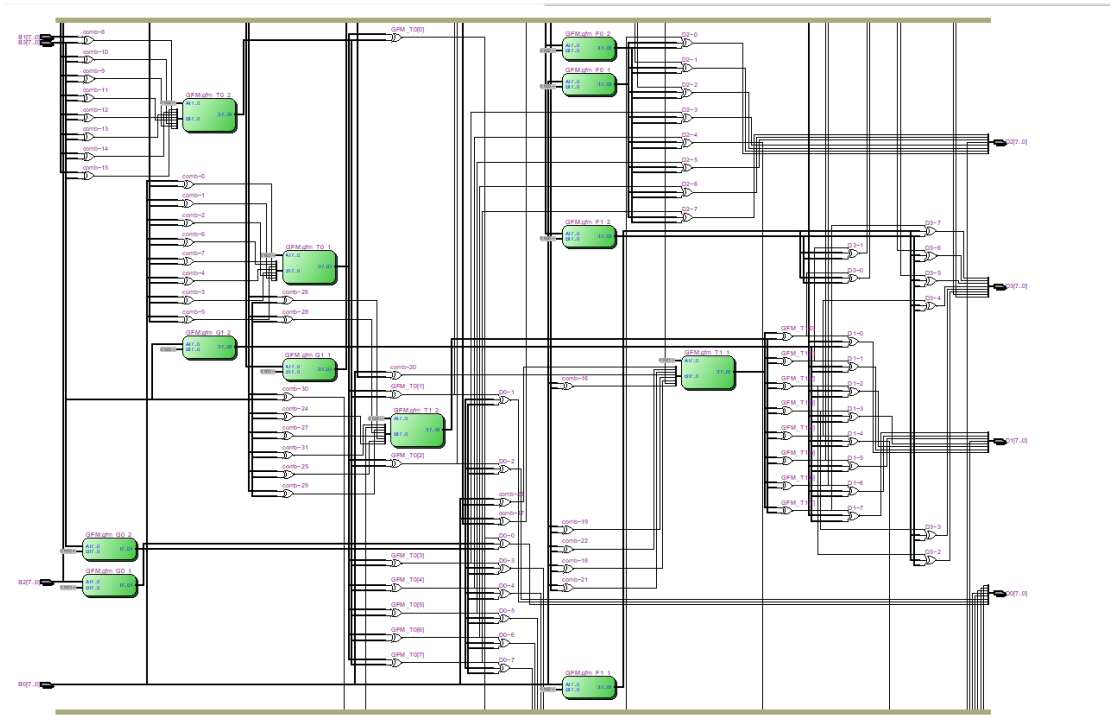
Flow Summary	
Flow Status	Successful - Tue Dec 31 13:22:06 2024
Quartus II 64-Bit Version	13.0.1 Build 232 06/12/2013 SP 1 SJ Web Edition
Revision Name	ninv
Top-level Entity Name	ninv
Family	Cyclone IV E
Device	EP4CE22F17C6
Timing Models	Final
Total logic elements	270 / 22,320 (1 %)
Total combinational functions	270 / 22,320 (1 %)
Dedicated logic registers	0 / 22,320 (0 %)
Total registers	0
Total pins	16 / 154 (10 %)
Total virtual pins	0
Total memory bits	0 / 608,256 (0 %)
Embedded Multiplier 9-bit elements	0 / 132 (0 %)
Total PLLs	0 / 4 (0 %)

圖十三、反元改良後

Total logic elements 從 377 減少至 270，377/270 約等於 1.39 ，也就是提升 1.39 倍。



圖十四、MixColumns 改良前



圖十五、MixColumns 改良後

乘法器的數量從 16 減少至 12，16/12 約等於 1.33 ，也就是提升 1.33 倍。

五、結論與未來研究方向

5-1 結論

本研究成功透過減少 AES（Advanced Encryption Standard）運算過程中的乘法次數，顯著提升了硬體實現的運算速度。實驗結果表明，改良後的設計在加密過程中有效降低了計算延遲，同時維持了系統的正確性與穩定性。基於 FPGA 的實驗驗證進一步支持了該設計在嵌入式系統與物聯網應用中的潛在價值。

5-2 未來研究方向

未來的研究將聚焦於以下幾個方向：

解密功能的實現與優化:新增 AES 解密過程的實現，並應用類似減少乘法的設計方法，以提升解密運算的效率。

全面性能評估與安全性測試:進一步量化分析設計在不同應用場景下的性能表現，確保優化後設計在密碼學安全性上的完整性。

應用擴展:將優化設計應用於更廣泛的密碼學協議或其他運算密集型應用，例如區塊鏈、資料傳輸加密，以及物聯網安全通信。

硬體架構進一步優化:探索進一步的硬體架構改進，包括記憶體訪問的優化與流水線並行度的提升，以應對更高效能需求。

參考文獻

[1] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[2] https://en.wikipedia.org/wiki/Fermat%27s_little_theorem

[3] https://doc.embedfire.com/fpga/altera/ep4ce10_mini/zh/latest/fpga/RS232.html