**112061576 莊家政**

**112061603 李柏叡**

**112061621 貢暐家**

**ASoC Final Project Report**

**Introduction:**

* Aes-128 encryption:

AES-128(Advanced Encryption Standard) is a symmetric encryption algorithm that encrypts data using a fixed-length key (128 bits).

AES-128 can be used to protect the privacy of sensitive data, ensuring security during transmission and storage.

**Catapult HLS:**

* Algorithm:

一張含有 文字, 螢幕擷取畫面, 圖表, 字型 的圖片

自動產生的描述 一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述

Key expansion function:

一張含有 文字, 圖表, 螢幕擷取畫面, 方案 的圖片

自動產生的描述

Round key 1

Round key 2

Round key 10

Round key 0

Not only is the final output ciphertext verified, but the intermediate states between each round are also checked using the test value provided by NIST.

The key is generated by **GenRoundKey**. You can see that a state array is first declared to store the plaintext, and then the array is subjected to a series of operations such as **SubBytes**, **ShiftRows**, **MixColumns**,and **AddRoundKey** with keys. After repeating 10 times, the ciphertext is obtained.

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述 一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

* SubBytes:

Substitute each byte according to the lookup table.

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

* ShiftRows:

The nth column of array shifts n bytes.

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

* MixColumns:

We use the Galois Field table we provide to implement.

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

一張含有 字型, 文字, 螢幕擷取畫面, 印刷術 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述 一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

* AddRoundKey:

We use key and state to calculate the new state.

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

* GenRoundKey:

Here is key expansion. Use this function to generate the 10 keys we need.

一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

* Micro-architecture exploration:

Original:

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述 

Since there’s no need to generate all round keys before the first round, and each round key can be generated using the round key of the previous round. We decided to decompose the key expansion function into several GenRoundKey functions.

V2:

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述 

* Result:

一張含有 文字, 電子產品, 螢幕擷取畫面, 軟體 的圖片

自動產生的描述

Synthesizing the design using the Xilinx library, we get the following result.

Original:

一張含有 文字, 螢幕擷取畫面, 軟體, 陳列 的圖片

自動產生的描述

V2:

一張含有 文字, 螢幕擷取畫面, 數字, 行 的圖片

自動產生的描述

From the screenshot above, we can see that the area generated using the v2

design is much smaller than using the original design.

* Problems we’ve encountered with Catapult:

1. Catapult GUI crashed several times when I was trying out different pipeline and unroll settings.
2. Pipeline setting doesn’t work as expected.

一張含有 文字, 螢幕擷取畫面, 軟體, 行 的圖片

自動產生的描述

一張含有 文字, 軟體, 數字, 行 的圖片

自動產生的描述

* Scverify:

一張含有 文字, 螢幕擷取畫面, 陳列, 軟體 的圖片

自動產生的描述

**Integrate into FSIC:**

* Block diagram:

一張含有 文字, 圖表, 方案, 工程製圖 的圖片

自動產生的描述

The input and output of our aes128\_en is 128-bit, but the width of axi-stream in

FSIC is only 32-bit. Therefore, a control logic is added to deal with the problem.

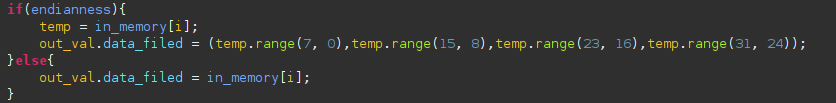
* Control register map:

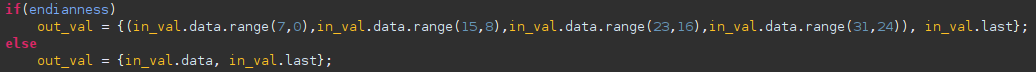
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Register | WordOffset | ResetVal | Access | Description |
| Reg\_rst | 0 | 0 | R/W | 1:reset (this won’t reset data length and keys) |
| Done | 1 | 0 | R-O | 1:done |
| Data\_length | 2 | 0 | R/W | Data length in unit of blocks (16bytes) |
| Key0 | 4 | 0 | R/W | Key\_in{[0],[1],[2],[3]} |
| Key1 | 5 | 0 | R/W | Key\_in{[4],[5],[6],[7]} |
| Key2 | 6 | 0 | R/W | Key\_in{[8],[9],[10],[11]} |
| Key3 | 7 | 0 | R/W | Key\_in{[12],[13],[14],[15]} |
| clk\_cnt\_low | 8 | 0 | R-O | (only for fpga validation)  Count how many clock cycles elapsed from receiving the first plaintext to sending the last ciphertext |
| Clk\_cnt\_high | 9 | 0 | R-O |

**Caravel-FSIC FPGA simulation:**

* USER DMA:

Our application accelerator is big endian, but the rest of the system is little endian. We added a register in user dma to control the conversion.



 一張含有 文字, 軟體, 多媒體軟體, 螢幕擷取畫面 的圖片

自動產生的描述

* Result:

一張含有 文字, 螢幕擷取畫面, 軟體, 多媒體軟體 的圖片

自動產生的描述

**Caravel-FSIC FPGA validation:**

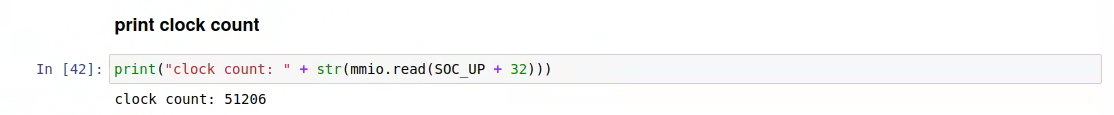
* Using:



* Result:

一張含有 文字, 螢幕擷取畫面, 字型, 數字 的圖片

自動產生的描述



It took 51206 clock cycles to encrypt 1024 blocks (16384 bytes) of data, which means 50 cycles per block.

It seems like using throughput cycles=45 is not fast enough. Also, we can add a FIFO at the output port so that it doesn’t have to wait until all the ciphertext is streamed out before it can start encrypting next block.

**Synopsys flow:**

* Synthesis:

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述 一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 功能表 的圖片

自動產生的描述

* Floorplan:

一張含有 文字, 螢幕擷取畫面 的圖片

自動產生的描述

一張含有 文字, 螢幕擷取畫面, 字型 的圖片

自動產生的描述

An error occurred when executing the power plan. From the previous i2c\_master\_top.v of lab3, we learned that the input of this file includes vdd and gnd. And our own design does not have vdd, gnd.

It is speculated that i2c\_master\_top is a small circuit and may not need a power ring, so it directly provides vdd and gnd to the circuit.

**Github link:**

<https://github.com/ruei7916/ASoC-Final-Project>

**Reference:**

1.NIST FIPS 197 Advanced Encryption Standard (AES)

<https://csrc.nist.gov/pubs/fips/197/final>

2.Cryptographic Standards and Guidelines - AES Development

<https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines/archived-crypto-projects/aes-development>