42024 Digital IC Design Homework 5

|  |  |  |  |
| --- | --- | --- | --- |
| NAME | 陳映臻 | | |
| Student ID | P76111783 | | |
| Score = area\*timing (ps) | 45448\*982750 | | |
| Cycle time (ns) | 8.5 | | |
| **Simulation Result** | | | |
| Functional simulation | Completed | Gate-level simulation | Completed |
| (your functional sim result) | | | |
| (your gate-level sim result) | | | |
| **Description of your design** | | | |
| AES.v: 包含所有AES Encryption path的主要程式，cycle變數確認pipeline的register是否應該輸出，register\_S[0:9]和register\_K[0:9]是pipeline每個round的register，分別存取當個round的state\_array和key，也就是下一個round的輸入。  AddRoundKey.v: 執行作業說明AddRoundKey步驟的XOR模組。  KeyExpansion.v: 執行作業說明KeyExpansion步驟的模組。  RoundTwoFive.v: 將執行作業說明步驟2~5功能回合總和的模組。  RoundTwoFour.v: 將執行作業說明步驟2~4功能回合總和的模組。  SubBytes.v: 將state array每個SubByte轉換成State的substitution table (S-box)模組。  ShiftRows.v: 執行作業說明ShiftRows步驟的模組。  MixColumns.v: 執行作業說明MixColumns步驟的模組。  Sbox.v: S-box的LUT查表模組。 | | | |

The scoring standard: (The smaller, the better)

*Scoring =*

*Area cost \* Timing cost*

*Area cost =*

*Total logic elements + total memory bits + 9\*embedded multiplier 9-bit elements*

*Timing cost =*

*Simulation time*

*A screenshot of a computer program

Description automatically generated*