|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **[5:0]enableSignals** | | | | | |
| **State** | **cypherTextOn** | **subByteOn** | **shiftRowsOn** | **mixColumnsOn** | **keyExpansionOn** | **addRoundKeyOn** |
| round1 | 1 | 0 | 0 | 0 | 0 | 1 |
| round2 | 0 | 1 | 1 | 1 | 1 | 1 |
| round3 | 0 | 1 | 1 | 1 | 1 | 1 |
| round4 | 0 | 1 | 1 | 1 | 1 | 1 |
| round5 | 0 | 1 | 1 | 1 | 1 | 1 |
| round6 | 0 | 1 | 1 | 1 | 1 | 1 |
| round7 | 0 | 1 | 1 | 1 | 1 | 1 |
| round8 | 0 | 1 | 1 | 1 | 1 | 1 |
| round9 | 0 | 1 | 1 | 1 | 1 | 1 |
| round10 | 0 | 1 | 1 | 1 | 1 | 1 |
| round11 | 0 | 1 | 1 | 0 | 1 | 1 |
| round12 | 0 | 0 | 0 | 0 | 0 | 0 |
| default | 0 | 0 | 0 | 0 | 0 | 0 |

Controller FSM Enable Signals

Rcon and Round #

|  |  |
| --- | --- |
| **State** | **[31:0]Rcon** |
| round1 | 0x01000000 |
| round2 | 0x02000000 |
| round3 | 0x04000000 |
| round4 | 0x08000000 |
| round5 | 0x10000000 |
| round6 | 0x20000000 |
| round7 | 0x40000000 |
| round8 | 0x80000000 |
| round9 | 0x1B000000 |
| round10 | 0x36000000 |
| default | 0x00000000 |