aes

sck

sdi

load

aes_spi

sck — sdo

sdi

plaintext — 128

key — 128

cyphertext

HSOSC — int_osc

aes_core

plaintext — a — y

key — key

roundCount

0
1

addRoundKey

a — y — **subByte** — clk

a — y — **shiftRows**

a — y — **mixcolumns**

roundCount

0
1

a — y

addRoundKeys

key

V
en

roundCount

0
1

clk

generateNextWords

nextWords — 128

currentWords — 128

rconn — 32

rconn

cyphertext — 128

sdo

done

Legend

———▶ = 128 Bit Text Mid Cypher Routine