AES Cipher/Inverse Cipher Block Diagram

Alex Pearson
Daniel Collins
Scott Lawson

ECE 571 Final Project
SP2016

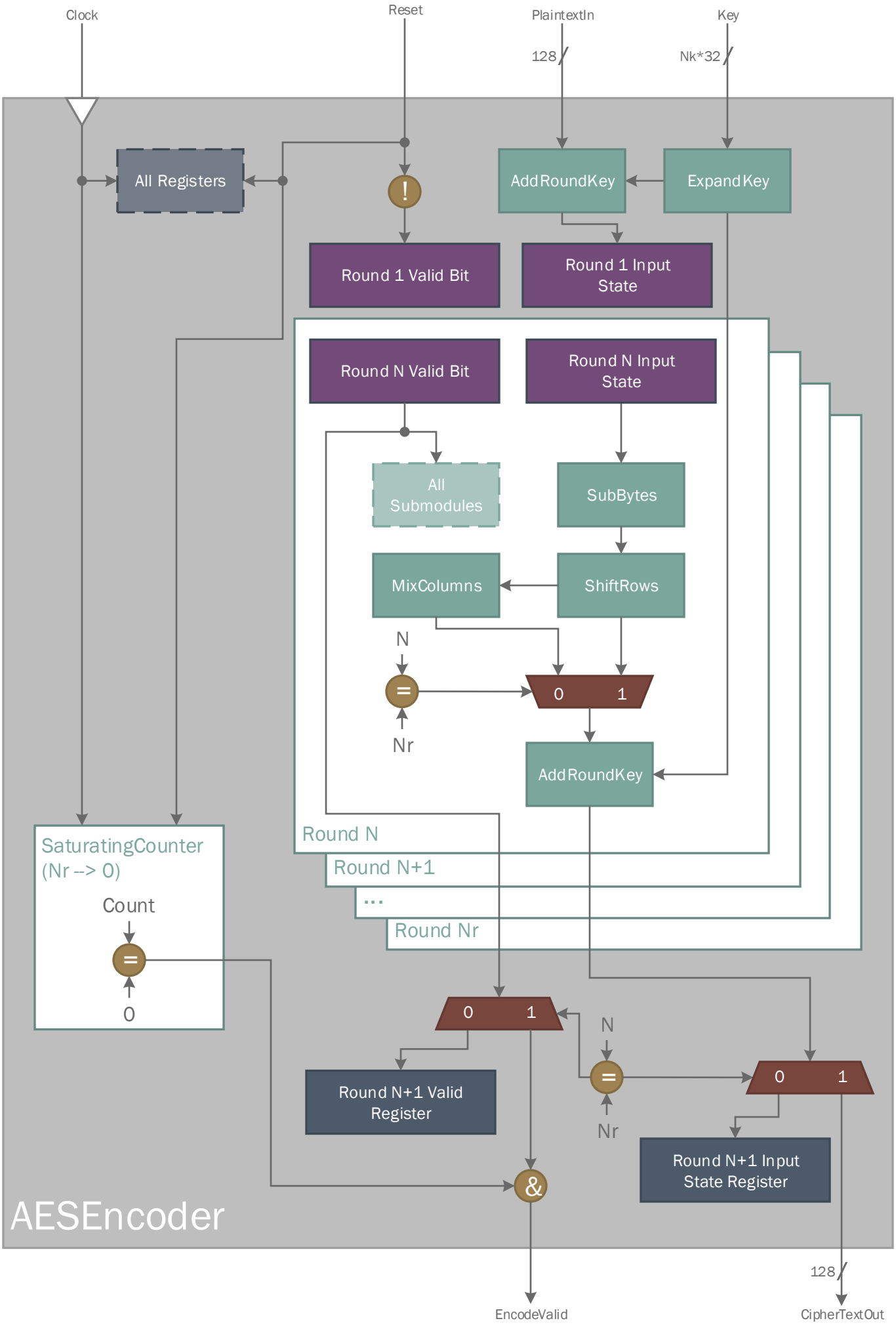
Derived from the AES Standard, Nov 26 2001, issued by NIST
Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

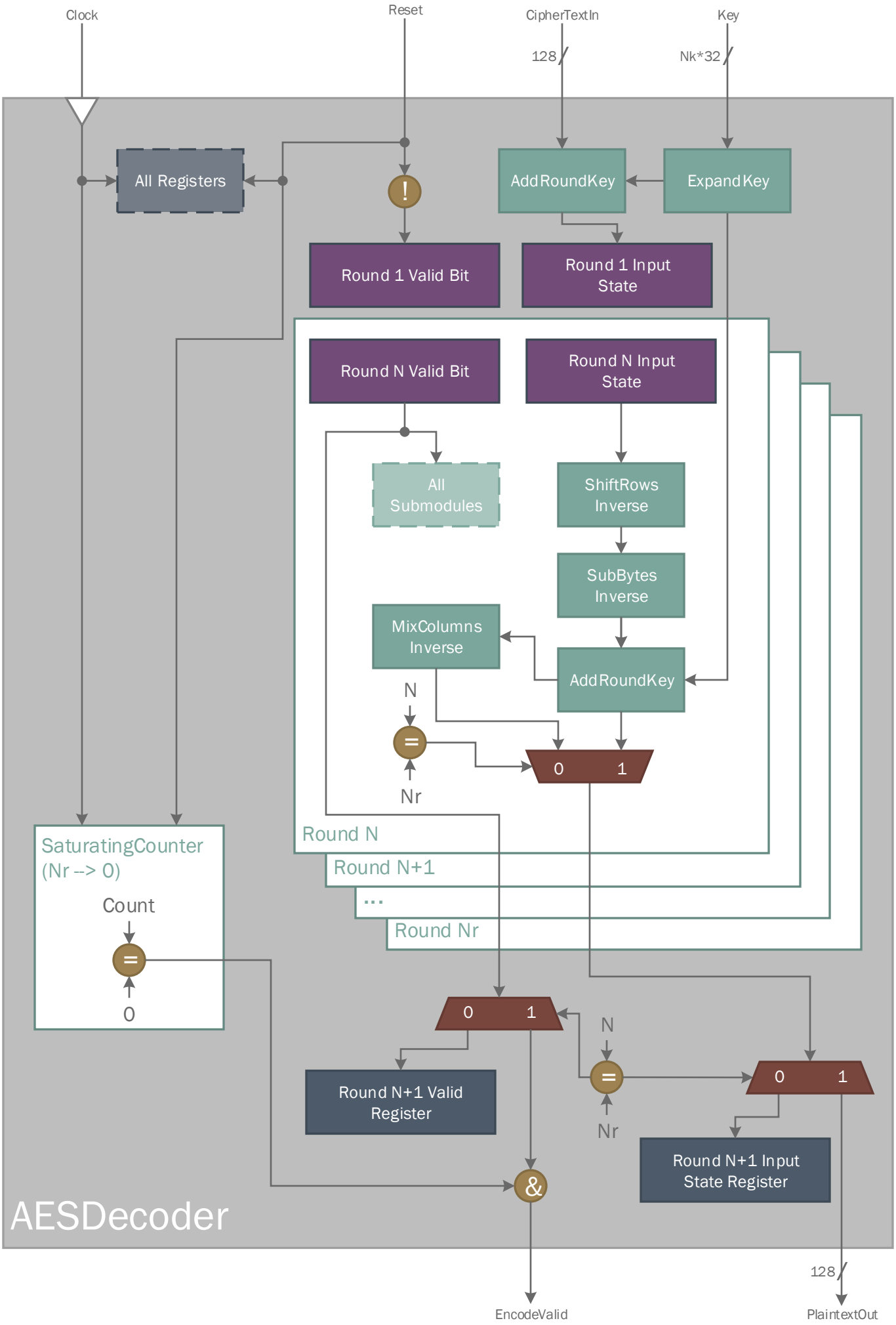
Key:

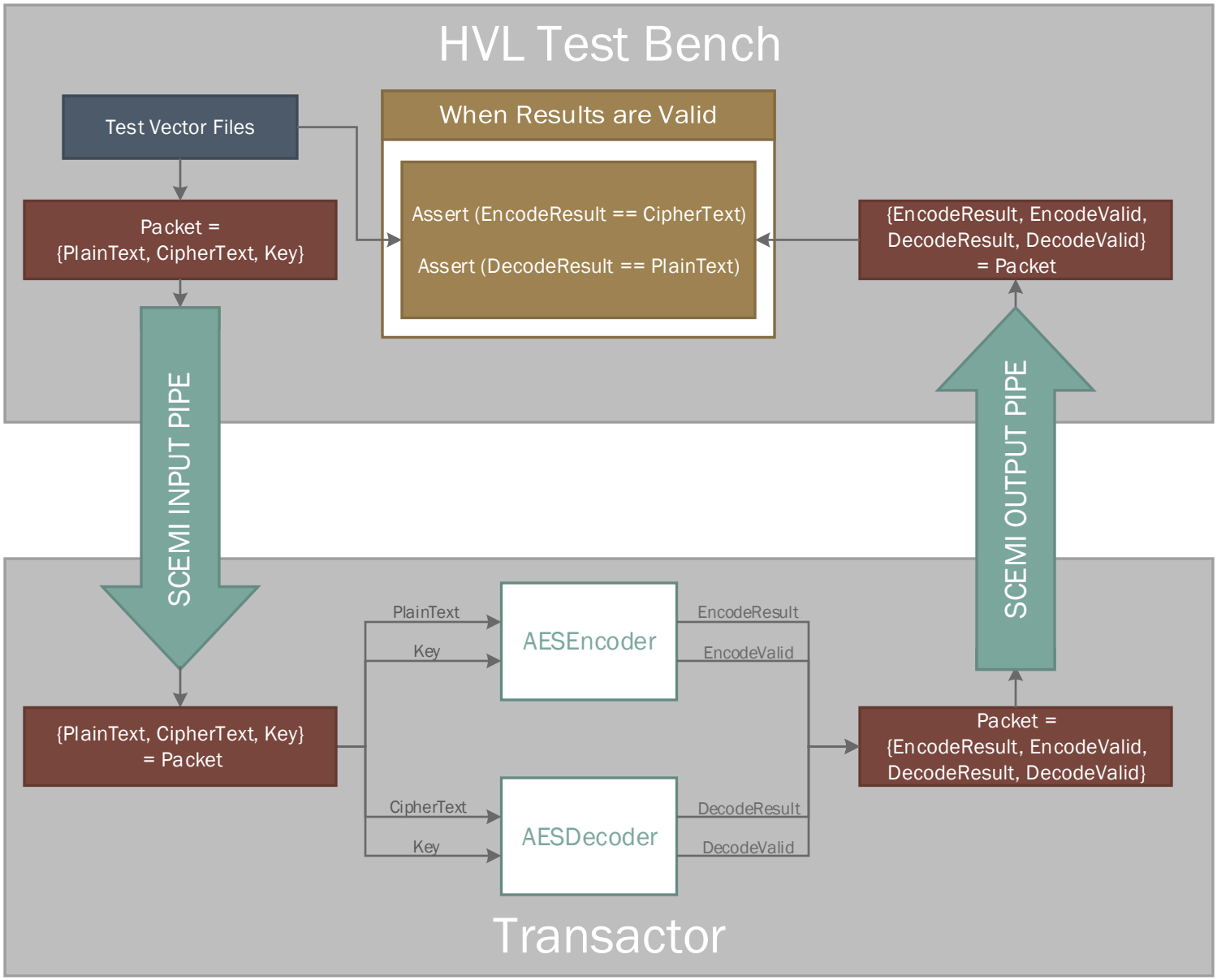
- Nb — Number of 32-bit words comprising the State, input, and output widths
  - This value always 4 according to the current version of the standard, so these vectors are always 128 bits wide
- Nk — Number of 32-bit words comprising the Cipher Key
  - Allowed values are 4, 6, or 8 (128-, 196-, and 256-bit wide keys, respectively)
- Nr — Number of rounds
  - Is 10 when Nk=4, 12 when Nk=6, and 14 when Nk=8


Clock
Reset
Key
Nk*32
Plaintext
128
AESEncoder
Valid
Ciphertext
128


Clock
Reset
Key
Nk*32
Ciphertext
128
AESDecoder
Valid
Plaintext
128


Clock
Reset
PlaintextIn
128
Key
Nk*32
All Registers
!
AddRoundKey
ExpandKey
Round 1 Valid Bit
Round 1 Input State
Round N Valid Bit
Round N Input State
All Submodules
SubBytes
MixColumns
ShiftRows
N
=
Nr
0
1
AddRoundKey
Round N
Round N+1
...
Round Nr
SaturatingCounter (Nr --> 0)
Count
=
0
0
1
N
=
Nr
0
1
Round N+1 Valid Register
Round N+1 Input State Register
&
AESEncoder
EncodeValid
128
CipherTextOut


Clock
Reset
CipherTextIn
128
Key
Nk*32
All Registers
!
AddRoundKey
ExpandKey
Round 1 Valid Bit
Round 1 Input State
Round N Valid Bit
Round N Input State
All Submodules
ShiftRows Inverse
SubBytes Inverse
MixColumns Inverse
AddRoundKey
N
=
Nr
0
1
Round N
Round N+1
...
Round Nr
SaturatingCounter (Nr --> 0)
Count
=
0
0
1
N
=
Nr
0
1
Round N+1 Valid Register
Round N+1 Input State Register
&
AESDecoder
EncodeValid
128
PlaintextOut


HVL Test Bench
Test Vector Files
When Results are Valid
Assert (EncodeResult == CipherText)
Assert (DecodeResult == PlainText)
Packet =
{PlainText, CipherText, Key}
{EncodeResult, EncodeValid,
DecodeResult, DecodeValid}
= Packet
SCEMI INPUT PIPE
SCEMI OUTPUT PIPE
PlainText
Key
AESEncoder
EncodeResult
EncodeValid
{PlainText, CipherText, Key}
= Packet
Packet =
{EncodeResult, EncodeValid,
DecodeResult, DecodeValid}
CipherText
Key
AESDecoder
DecodeResult
DecodeValid
Transactor