AES Cipher/Inverse Cipher Block Diagram

Alex Pearson
Daniel Collins
Scott Lawson

ECE 571 Final Project
SP2016

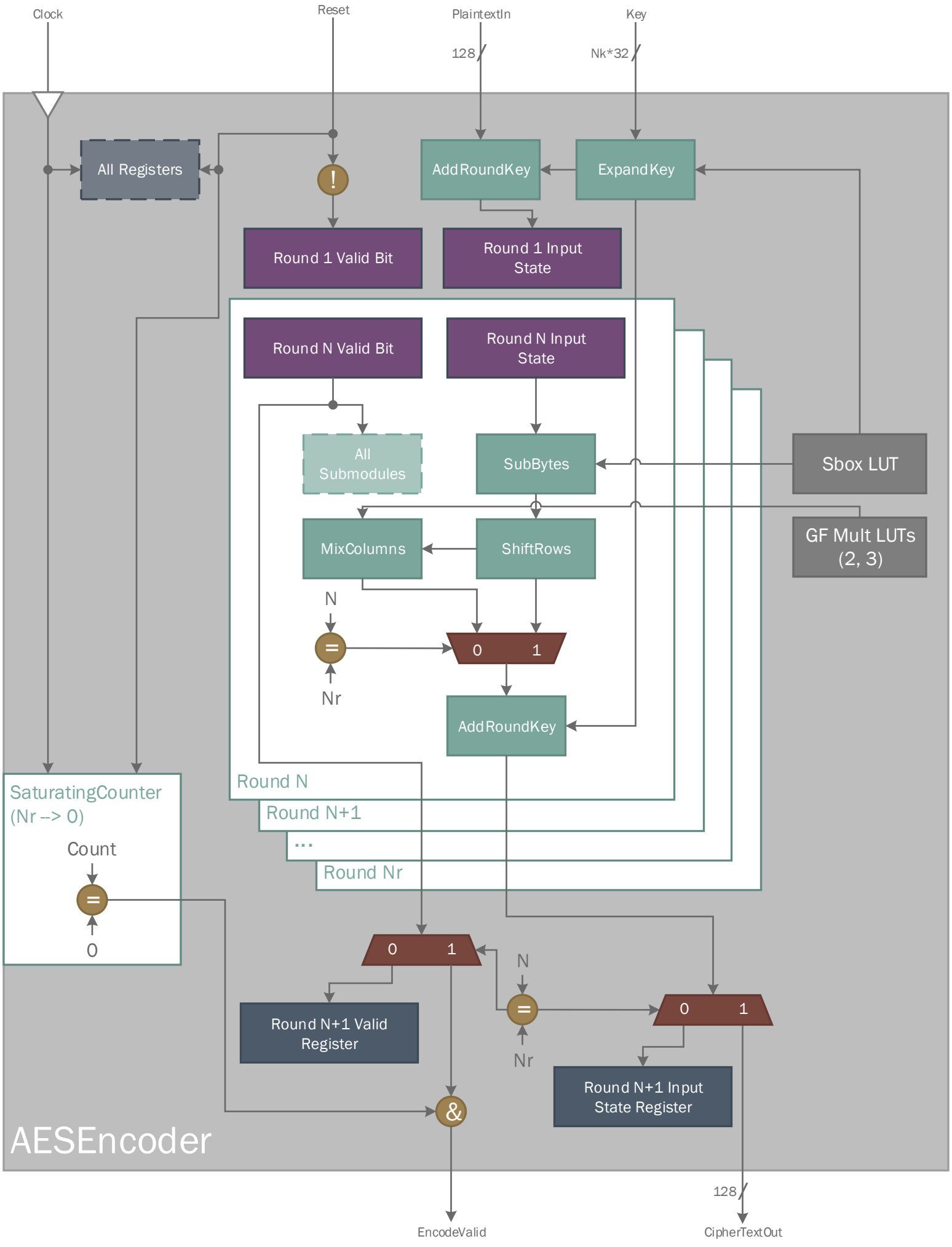
Derived from the AES Standard, Nov 26 2001, issued by NIST
Available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

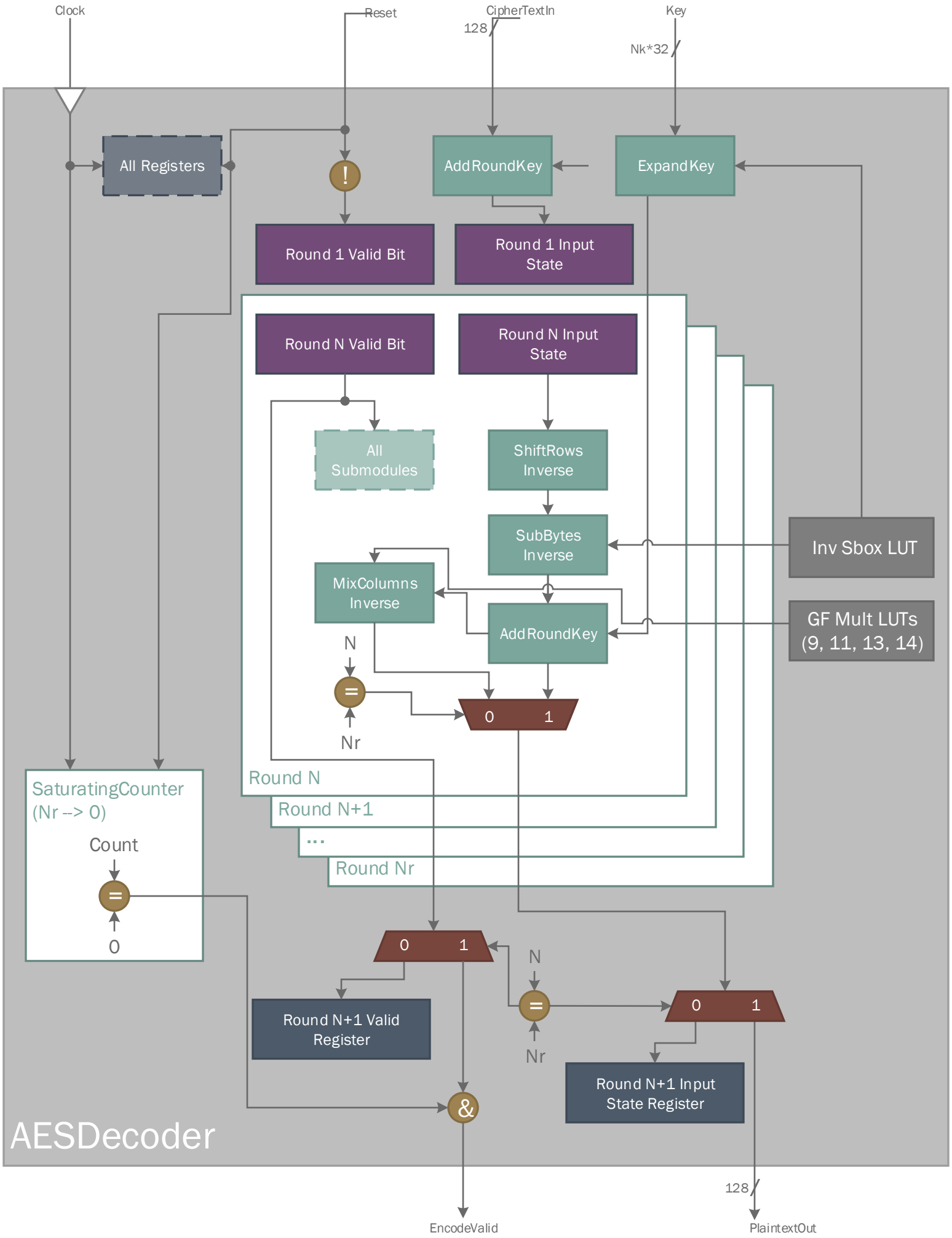
Key:

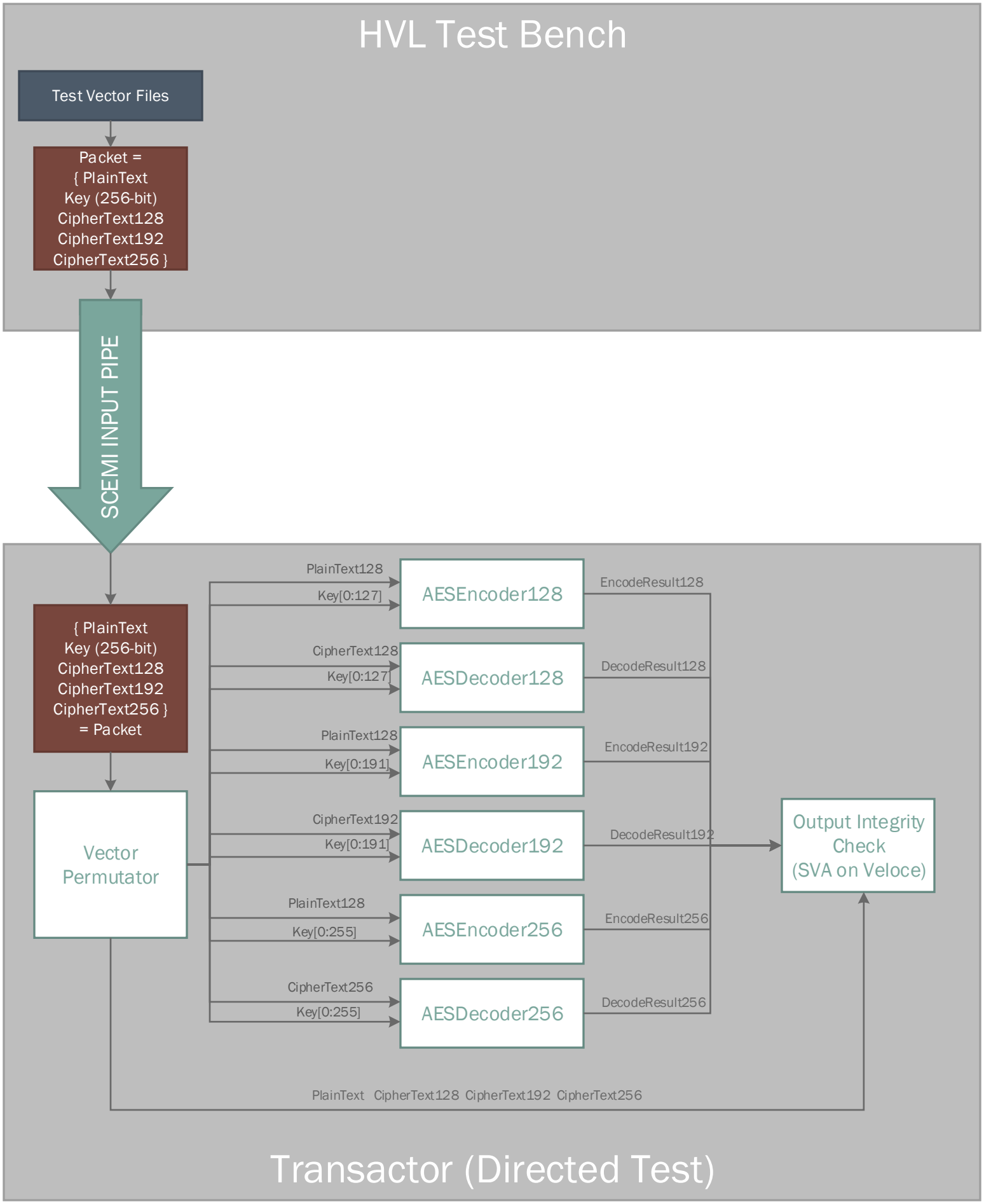
- Nb — Number of 32-bit words comprising the State, input, and output widths
  - This value always 4 according to the current version of the standard, so these vectors are always 128 bits wide
- Nk — Number of 32-bit words comprising the Cipher Key
  - Allowed values are 4, 6, or 8 (128-, 196-, and 256-bit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

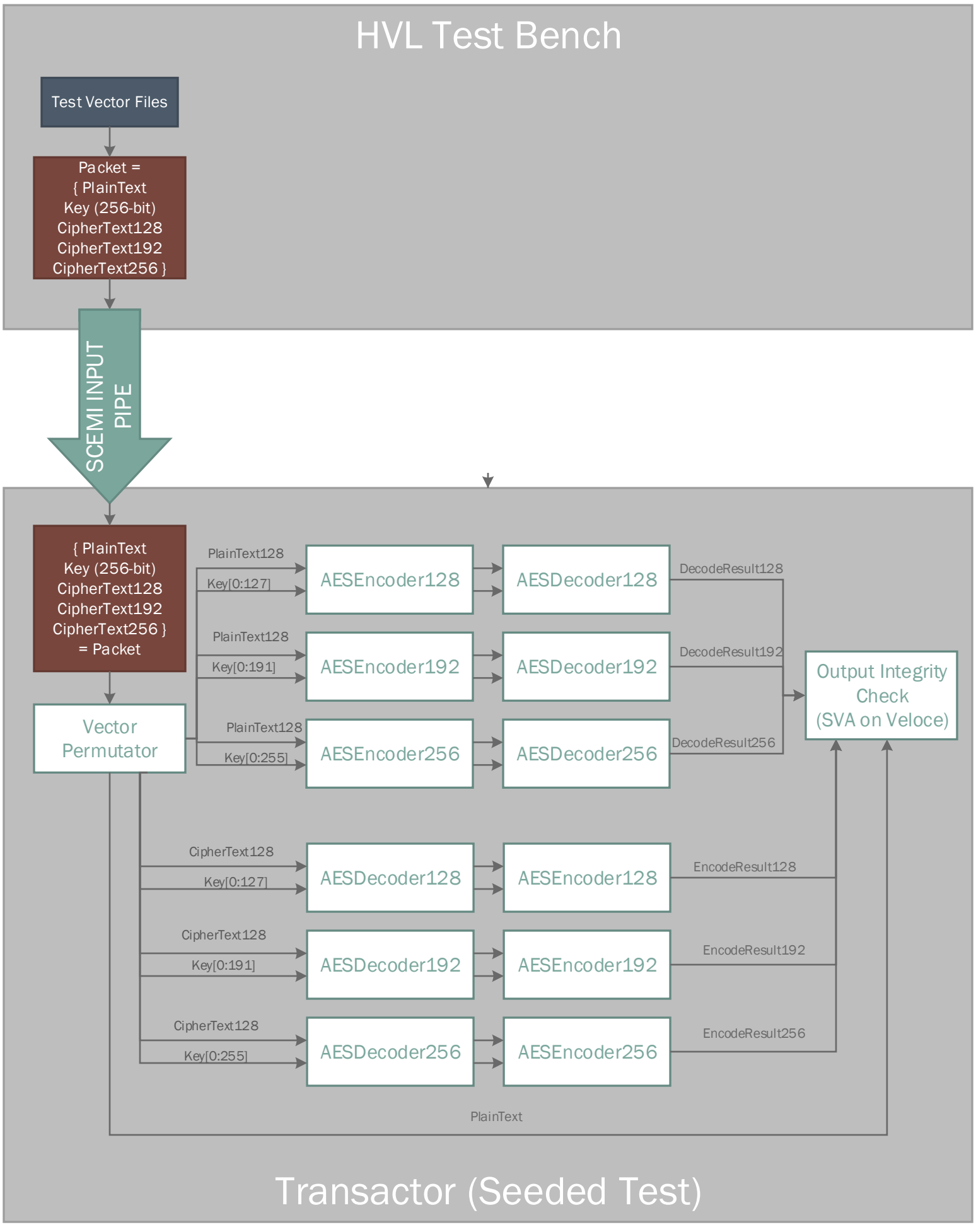

Clock
Reset
Key
Nk*32
Plaintext
128
AESEncoder
Valid
Ciphertext
128


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
Sbox LUT
MixColumns
ShiftRows
GF Mult LUTs (2, 3)
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
AESDecoder
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
Inv Sbox LUT
MixColumns Inverse
AddRoundKey
GF Mult LUTs (9, 11, 13, 14)
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
&
128
EncodeValid
PlaintextOut


HVL Test Bench
Test Vector Files
Packet =
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
SCEMI INPUT PIPE
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
= Packet
Vector
Permutator
PlainText128
Key[0:127]
AESEncoder128
EncodeResult128
CipherText128
Key[0:127]
AESDecoder128
DecodeResult128
PlainText128
Key[0:191]
AESEncoder192
EncodeResult192
CipherText192
Key[0:191]
AESDecoder192
DecodeResult192
PlainText128
Key[0:255]
AESEncoder256
EncodeResult256
CipherText256
Key[0:255]
AESDecoder256
DecodeResult256
Output Integrity
Check
(SVA on Veloce)
PlainText CipherText128 CipherText192 CipherText256
Transactor (Directed Test)


HVL Test Bench
Test Vector Files
Packet =
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
SCEMI INPUT PIPE
{ PlainText
Key (256-bit)
CipherText128
CipherText192
CipherText256 }
= Packet
Vector Permutator
PlainText128
Key[0:127]
AESEncoder128
AESDecoder128
DecodeResult128
PlainText128
Key[0:191]
AESEncoder192
AESDecoder192
DecodeResult192
PlainText128
Key[0:255]
AESEncoder256
AESDecoder256
DecodeResult256
Output Integrity Check
(SVA on Veloce)
CipherText128
Key[0:127]
AESDecoder128
AESEncoder128
EncodeResult128
CipherText128
Key[0:191]
AESDecoder192
AESEncoder192
EncodeResult192
CipherText128
Key[0:255]
AESDecoder256
AESEncoder256
EncodeResult256
PlainText
Transactor (Seeded Test)