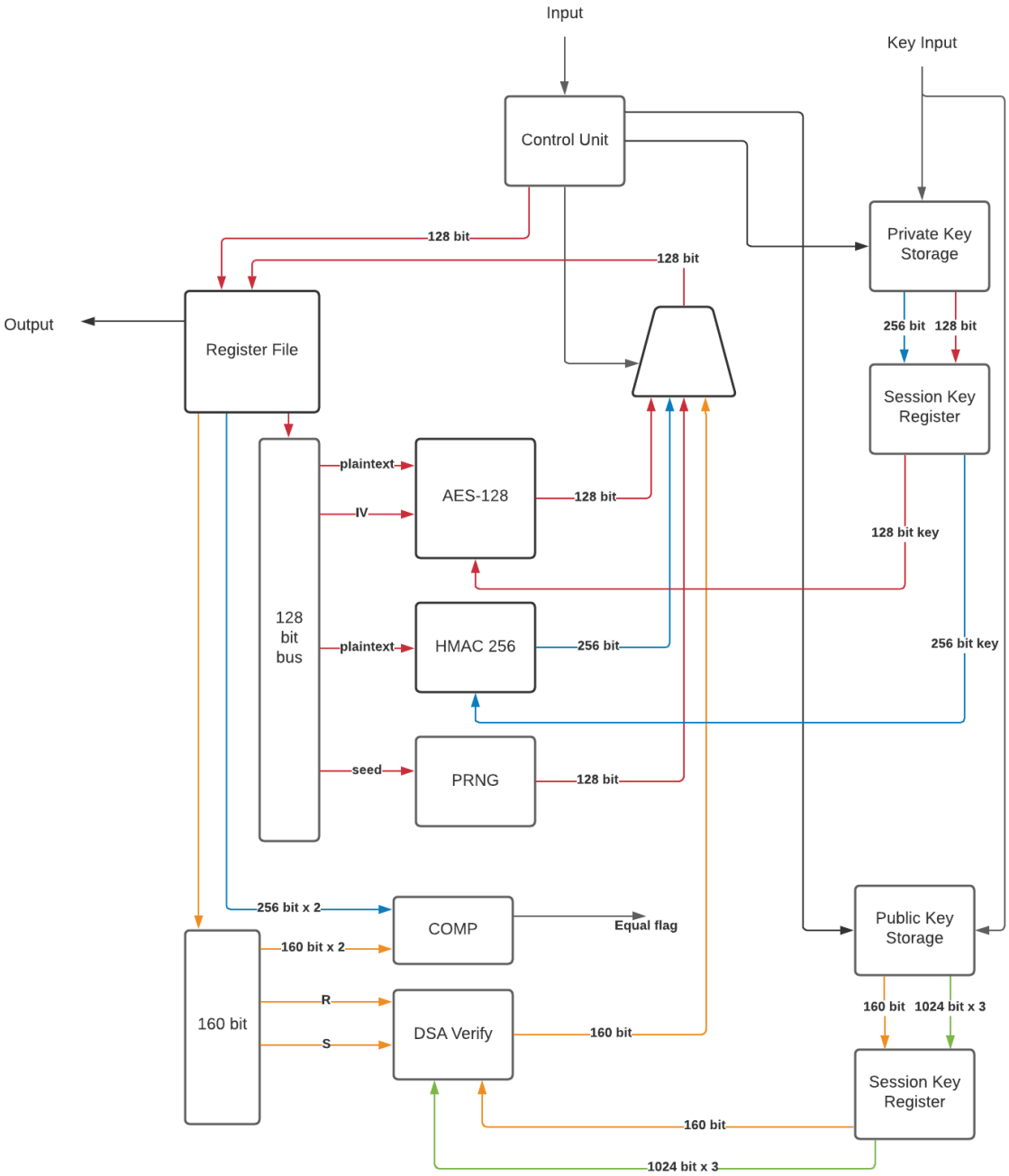
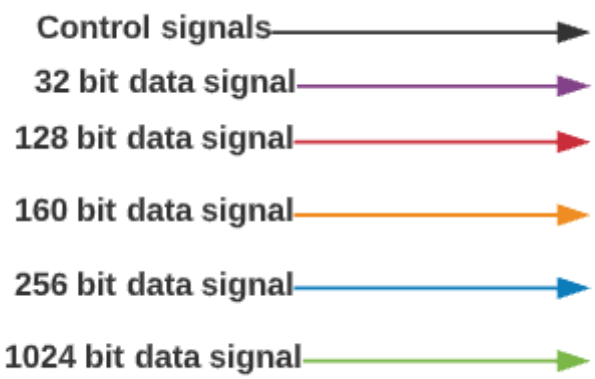
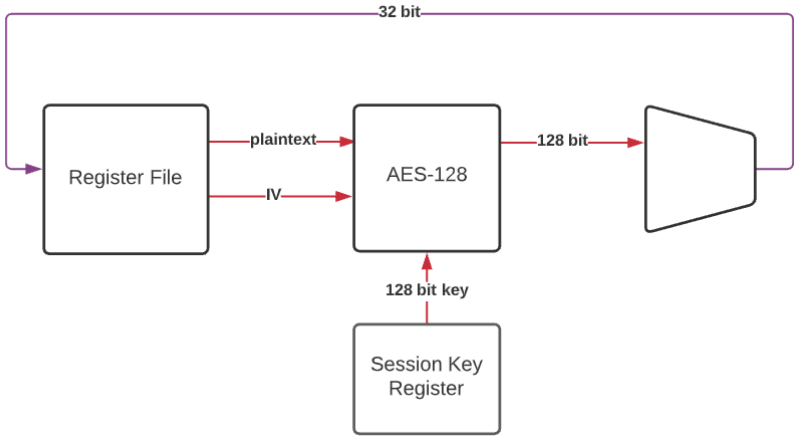

Input
Key Input
Control Unit
128 bit
128 bit
Private Key Storage
Output
Register File
256 bit
128 bit
Session Key Register
plaintext
IV
AES-128
128 bit
128 bit key
128 bit bus
plaintext
HMAC 256
256 bit
256 bit key
seed
PRNG
128 bit
256 bit x 2
COMP
Equal flag
Public Key Storage
160 bit x 2
160 bit
R
S
DSA Verify
160 bit
160 bit
1024 bit x 3
Session Key Register
160 bit
1024 bit x 3

Legend


Control signals
32 bit data signal
128 bit data signal
160 bit data signal
256 bit data signal
1024 bit data signal

Security scenario (AES Block)



AES modes:

- Electronic Codebook (ECB) mode.
- Cipher Block Chaining (CBC) mode.
- Cipher Feedback (CFB) mode.
- Output Feedback (OFB) mode.
- Counter (CTR) mode.

Supported plain text, key, and cipher text length: 128 bits

Round counts of encryption/decryption: 17 rounds

Registers:

Plaintext (128 bit) (wr)

IV (128 bit) (wr)

Ciphertext (128 bit) (ro)

AES flags:

Encryption/decryption flag (rw): encryption (0) or decryption(1).

Start flag (wo): pause(0) or start (1). It is set zero after encryption/decryption automatically.

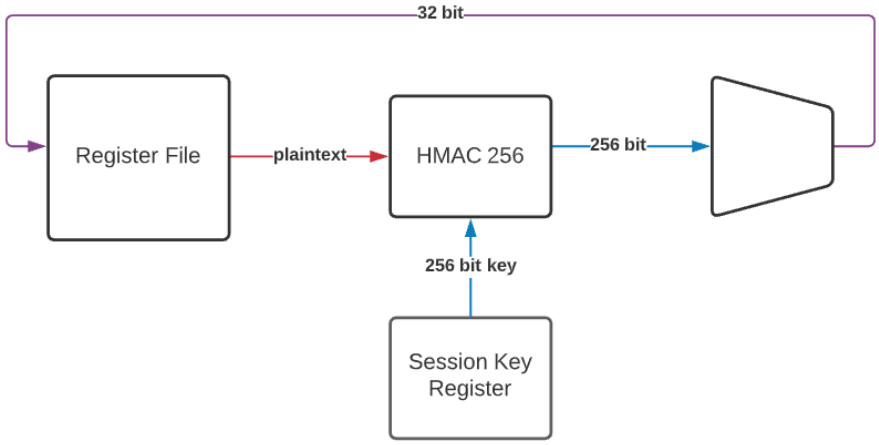
Busy flag(ro) : idle (0) or busy (1).

IV source flag (rw) : from outside (0) or from PRNG (1).

Reset (wo): to reset count number (1). It must be set zero before the operation.

Done (ro): Operation is done (1) or not (0). It is set one (1) after encryption/decryption automatically and set zero while the operation is starting.

Message authentication scenario (HMAC block):



Key length: 256-bit

Round counts of hashing: 92 rounds

Registers:

Plaintext (128-bit) (wr)

Digest0 (256-bit) (ro)

Digest1 (256-bit) (wr)

Key length (8-bit) (ro)

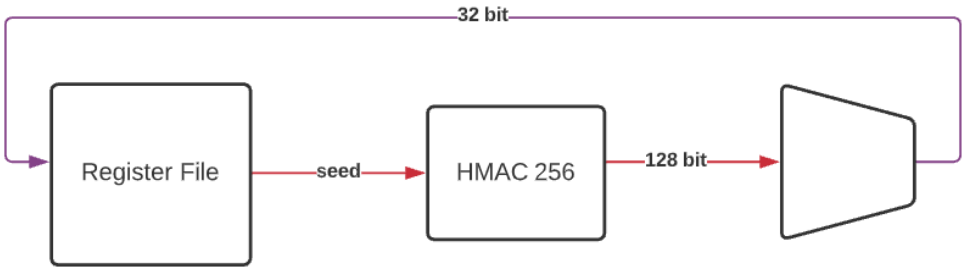
HMAC flags:

Start hashing flag (wo): pause(0) or start (1). It is set zero after encryption/decryption automatically.

Busy flag(ro) : idle (0) or busy (1).

Done (ro): Operation is done (1) or not (0). It is set one (1) after encryption/decryption automatically and set zero while the operation is starting.

PRNG:



Produces 128-bit pseudorandom number with seed.

Registers:

Seed (128-bit) (wr)

Random number (128-bit) (ro)

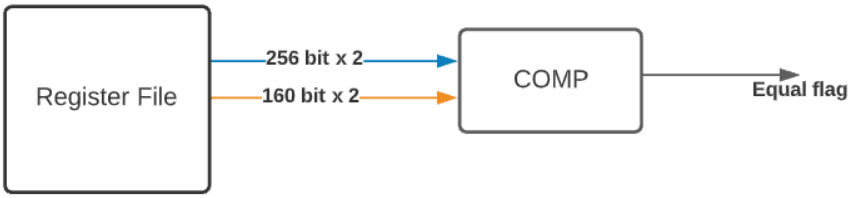
Flags:

Start flag (wo): pause(0) or start (1). It is set zero after encryption/decryption automatically.

Busy flag(ro) : idle (0) or busy (1).

Done (ro): Operation is done (1) or not (0). It is set one (1) after encryption/decryption automatically and set zero while the operation is starting.

Comparator:



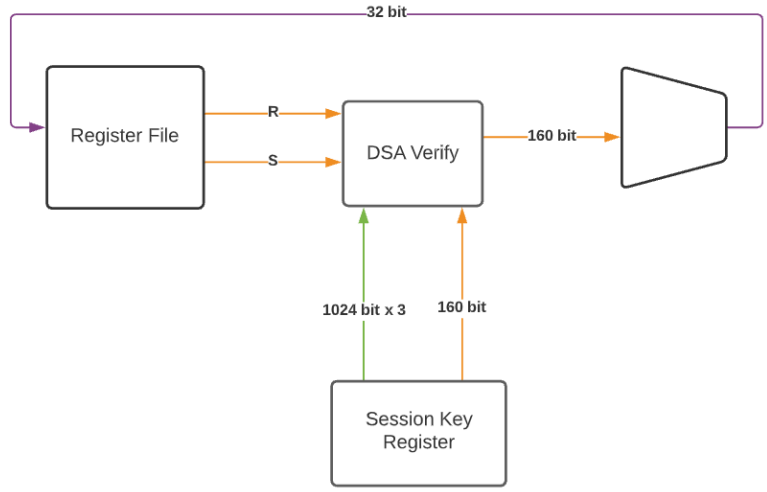
Compares two registers.

Flags:

Compare modes (wr): Compare 256-bit (0) or compare 160-bit (1).

Equal (ro): Two registers are equal (1) or not equal (0).

Signature authentication scenario (DSA Verify Block):



Registers:

R register (160-bit) (wr)

S register (160-bit) (wr)

V register (160-bit) (ro)

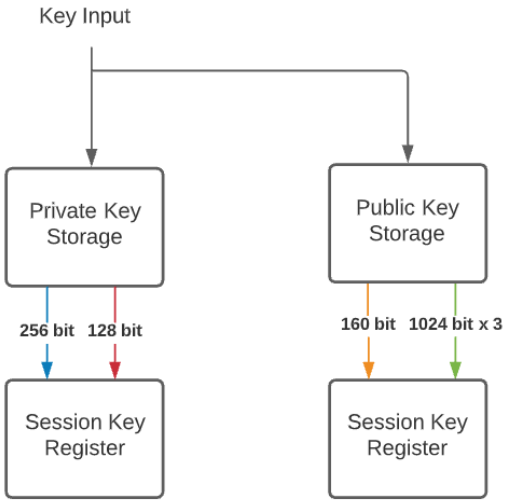
Flags:

Start verifying (wo) : Start (1) or pause (0). It is set zero after encryption/decryption automatically.

Busy (ro) : Busy (1) or idle (0).

Verification result (ro): Verified (1) or not (0).

Key Storage



Public key storage:

P register (1024-bit) (wr)

Q register (160-bit) (wr)

G register (1024-bit) (wr)

Y register (1024-bit) (wr)

Private key storage (AES and HMAC)

256-bit, 4 key storing capability.

Flags:

Key bit size selection: 128-bit (0) or 256-bit (1).