AES Registers

AES plaintext register (128 bit)

IV register (128 bit)

Ciphertext register (128 bit)

AES Control and Status Register (CSR) (Used 7 bits):

- Encryption/decryption flag (1 bit) (rw)
- Mode selection (3-bit) (rw)
- Start flag (1 bit) (rw)
- Busy flag (1 bit) (ro)
- Done (1 bit) (ro)

SHA-256 Registers

SHA2 plaintext register (447-bit) (rw)

Digest0 register (256-bit) (ro)

Digest1 register (256-bit) (rw)

SHA2 CSR (Used 67 bits):

- Key length (64-bit) (rw)
- Start flag (1 bit) (rw)
- Busy flag (1 bit) (ro)
- Done (1 bit) (ro)

PRNG Registers

Seed (128-bit)

Generated random number (128-bit)

PRNG CSR (Used 4 bits):

- Seed used or not (1 bit) (rw)
- Start flag (1 bit) (rw)
- Busy flag (1 bit) (ro)
- Done (1 bit) (ro)

Comparator Registers

COMP CSR:

- 160 or 256 bit comparing (1 bit) (wr)
- Equal (1 bit) (ro)

DSA Verify Registers

R register (160-bit)

S register (160-bit)

V register (160-bit)

CSR (used 2 bits):

- Start flag (rw)
- Busy (ro)
- Verification finished (ro)

0	AES_plaintext (128)
1	IV register (128)
2	AES_ciphertext (128)
3	AES_CSR (7)
4	SHA2_plaintext (447)
5	Hash0 (256)
6	Hash1 (256)
7	SHA2_CSR (67)
8	PRNG_Seed (128)
9	PRNG_Generated (128)
10	PRNG_CSR (4)
11	COMP_CSR (1)
12	DSA_R (160)
13	DSA_S (160)
14	DSA_V (160)
15	DSA_CSR (3)