- ChaChaPoly
- SHA3, SHAKE128, and SHAKE256
- SM4

- Public Key cryptographic engine (PKE) and Isolated Key Generator (IKG)
  - Modular exponentiation – RSA with and without CRT; 4096-bit maximum operand size
  - Elliptic Curve Cryptography (ECC) with 640-bit maximum operand size
  - Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA, EC-KCDSA, and EdDSA), with 4096-bit maximum operand size
  - Diffie-Hellman (D-H and ECDH) key exchange
- Random Number Generator (RNG)

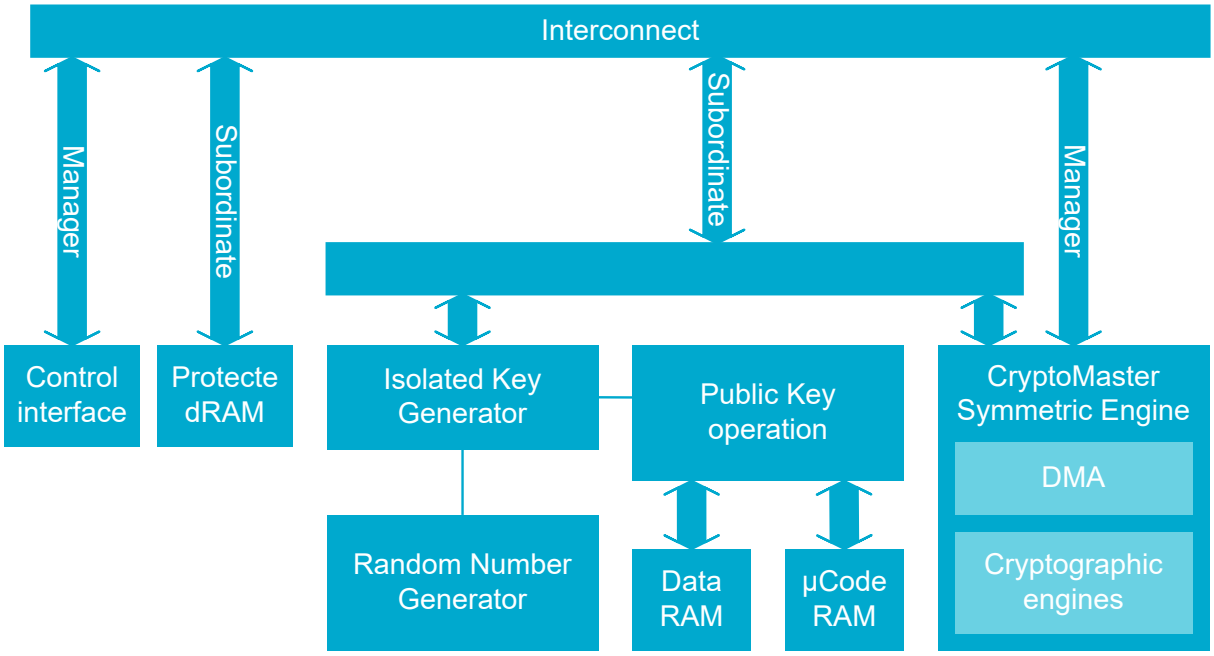

Figure 31: Cryptographic accelerator engine block diagram

7.8.1.1 Initialization

Before the CRACEN peripheral can be used, it must be configured.

At reset, each hardware crypto operation category is disabled and must be individually enabled using the ENABLE register. To use CRACEN, the desired module must first be enabled. Ongoing crypto operations will complete even if the module is disabled during the operation.

Before transferring data to CRACENCORE, CRACEN must be enabled using ENABLE on page 140.

When CRACEN is enabled, it will erase the PKE data RAM by starting a zeroization process. When the PKBUSY field of the PK.STATUS is cleared, the zeroization operation is complete. The PKE engine is not available until the zeroization process has finished.

7.8.1.2 Protected RAM

Protected RAM regions can be retained and locked for storing symmetric keys. The CPU cannot access these regions.

After KMU has pushed keys into the protected RAM, PROTECTEDRAMLOCK must be set to `Enabled` before CRACEN can access and use the keys.

Register PROTECTEDRAMLOCK is a write-once register, and cannot be changed until the next device reset.

The following areas are defined for the protected RAM.