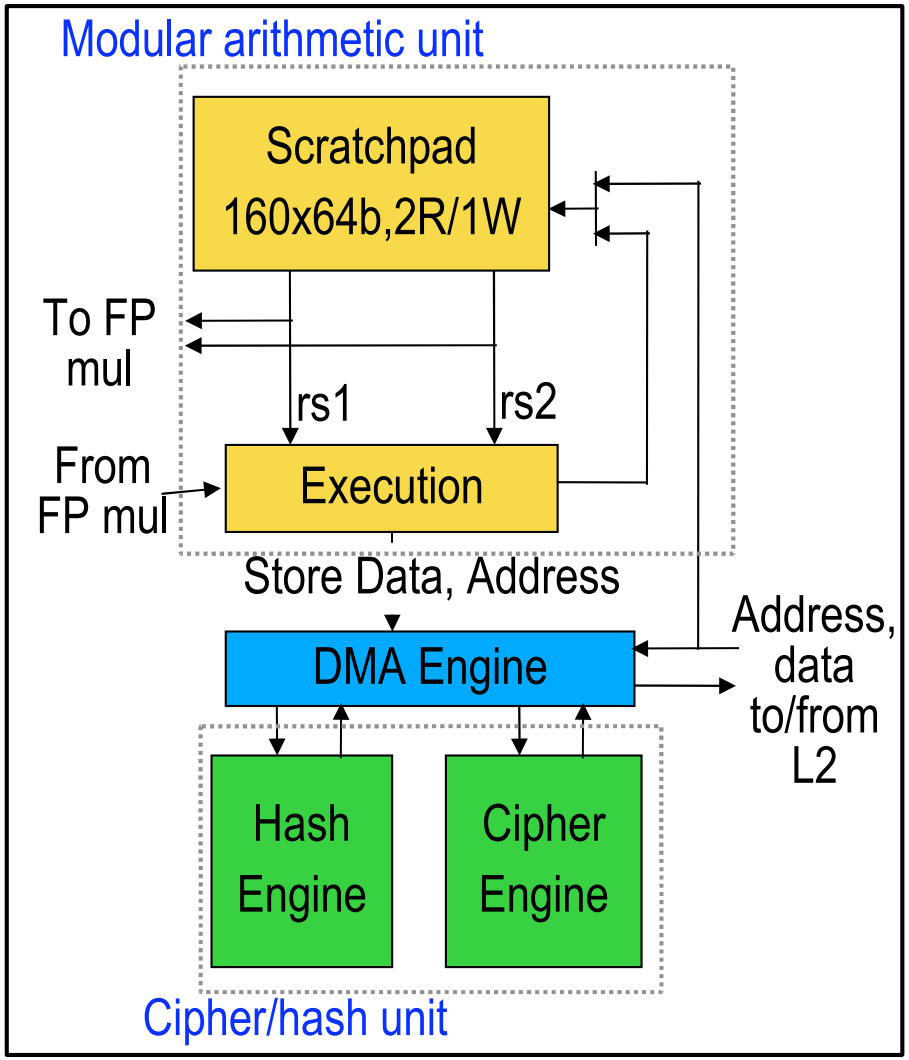
RF UltraSPARC crypto accelerator

- Accelerators are per core
  - 2 basic sub-units (can operate in parallel)
  - Operate in parallel with threads
- Accelerator is shared by all the core's strands
  - 8 strands per core on UltraSPARC RF
- Accelerators are Hyerprivileged
  - Each strand could be under the control of a different OS
- Accelerators expose a light-weight interface to SW
  - Communication via a memory-based control word queue (CWQ)
  - Requests are fully self-contained
  - Both sync and async operation supported

RF accelerator overview



Rainbow Falls (RF) peak performance

Bulk cipher

Algorithm
DES
3DES
AES-128
AES-192
AES-256
Kasumi

Secure hash

Algorithm
MD5
SHA-1
SHA-256
SHA-512

Public key

Algorithm
RSA-1024
RSA-2048
ECC

- RF provides up to 16 accelerators per processor
- Common ciphers supported (helps SSL, IPsec etc)
- HW peak performance is dependent on object size
  - ~90% of peak for 1KB objects when L2$ sourced
  - ~70% of peak for 1KB objects when DRAM sourced
- Accelerators support common modes of operation for block ciphers (EBC, CBC, CTR, & CFB)
- Hashed Message Authentication Code (HMAC) support
- HW gather support
- HW support for IP checksum and CRC32c acceleration and data movement