Hello and welcome to this presentation of the STM32MP13's DDR MCE.

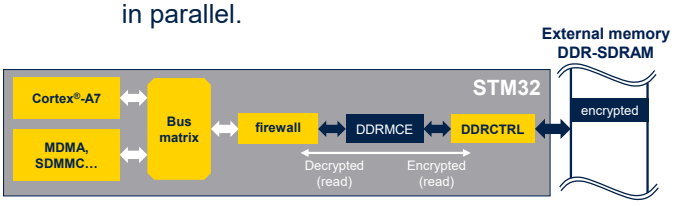
DDR Memory cipher engine (DDRMCE) features

- Encrypt and decrypts on-the-fly selected information that is stored in external DDR-SDRAM memory
  - One region can be defined
- Uses standard AES-128 in ECB mode, with an associated key derivation function based on well-known Keccak-400 algorithm

Number of cycles required to process a 16-byte block		
Read	Write	Key computation(*)
11	22	15
11	22	15

(*) Computed for two consecutive 16-bytes blocks

- Global security mechanisms
  - Privileged-only accesses when PRIV bit is set in MCE_PRIVCFGR
  - Write protection until next reset (GLOCK)
  - Write-only key registers
- Firewall to encrypted region managed by TrustZone® address space controller (TZC)
- Read boost: when no write is ongoing the two cipher cores are allocated to decrypt two reads in parallel.



life.augmented

2

The DDRMCE module automatically decrypts reads and encrypts writes toward a single region defined in external DDR-SDRAM memory.
AES 128-bit cipher in ECB mode is used with an associated key derivation function based on the well-documented Keccak-400 algorithm. The key derivation function is leakage-resilient, as defense against side channel attacks (SCA).
When no write is ongoing in DDRMCE, the two AES cores are allocated to decrypt two reads in parallel, increasing performances.
When the PRIV bit is set in DDRMCE, only privileged accesses are granted. The GLOCK bit can be used to freeze the module configuration until the next reset.

All traffic going through DDRMCE is filtered by the TrustZone® address space controller for DDR (TZC).

Thank you

life.augmented

Thank you for having attended this presentation!
You can now refer to the presentations that detail the operation of the STM32MP's security modules:

- Symmetric cryptography.
- Asymmetric cryptography.
- Hash and random number generation.
- Enhanced anti-tamper.
- Enhanced key storage.