Hello and welcome to this presentation of the STM32MP13's CRYP

CRYP feature list

- AES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
  - Counter (CTR) mode
  - Galois counter mode (GCM)
  - Galois message authentication code (GMAC)
  - Counter with CBC-MAC (CCM) mode
- DES/TDES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
- Compliant AES and DES/TDES implementation
  - AES operations on 128, 192 or 256-bit keys
- Atomic key writing/loading enforcement
- Can load shared AES key from SAES
- AHB slave with suspend/resume & DMA support (IN + OUT channels with FIFOs)
- 32-bit data words swapping support (bit, byte or half-word)

Number of cycles required to process a block(**) (Clock frequency= AHB clock of peripheral)

Algo-rithm	ECB/ CBC	AES (Key size)	ECB	CBC	CTR	GCM				CCM			
						Init	Header	Payload	Tag	Init	Header	Payload	Tag
DES	16	**128b**	51(*)		51	64	35	51	59	63	55	114	58
TDES	48	**256b**	75 (*)		75	88	35	75	75	87	79	162	82

(*) For decryption you must add key derivation time, once (**) Block size= 128-bit for AES, 64-bit for DES/TDES

life.augmented

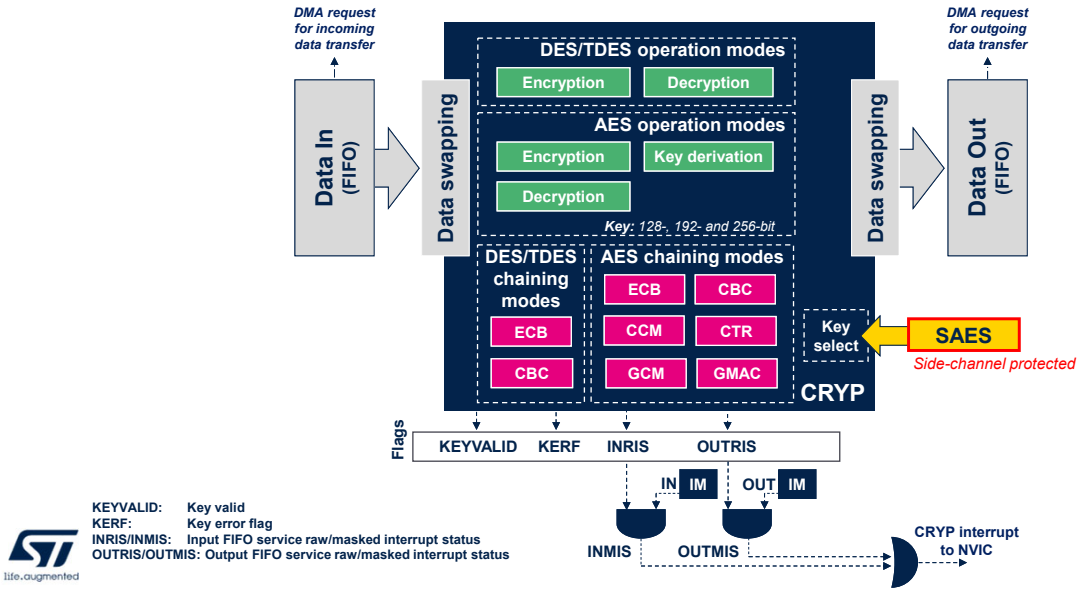
2

The CRYP module supports the Data Encryption Standard (DES), the Triple-DES and the Advanced Encryption System (AES) in several operating modes described in the slide.
In AES mode, the peripheral processes 128-bit data blocks using an encryption key with a length of 128, 192 or 256 bits, based on the selected chaining mode.
In DES/TDES mode, CRYP processes 64-bit data blocks using a standard-length encryption key.
The table indicates the number of clock cycles required to process a block of data, according to the algorithm, the chaining mode and the key size.

A full data flow can be automated with the help of the

Direct memory access controller (DMA).
The CRYP module in AES mode can load shared keys from the side-channel resistant SAES module. This procedure is controlled by SAES.

CRYP peripheral block diagram



This simplified block diagram of the CRYP module shows the data path from Data In on the left to Data Out on the right.
In AES mode, the peripheral processes 128-bit data blocks using an encryption key with a length of 128, 192 or 256 bits, with or without a data swapping option.
In DES/TDES mode, CRYP processes 64-bit data blocks using a standard-length encryption key, with or without a data swapping option.

There are two functional interrupts defined for the peripheral: one set when the input FIFO is ready to receive data and one set when output data are ready to be flushed by the CPU or the DMA.

A special set of encrypted keys managed in the side-channel resistant SAES module can be shared with the CRYP module when the SAES application activates the sharing function.

Thank you

life.augmented

For more details on the new enhanced secure key storage feature and wrap/share key modes, please refer to the Enhanced secure key storage training module.