Hello and welcome to this presentation of the STM32U5 symmetric crypto coprocessors. It covers the features of the AES and SAES modules, which are widely used for cryptographic applications.

STM32U5 AES feature list

- NIST FIPS197 compliant AES implementation
- 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
- AES operation modes on 128-bit data blocks , 128 or 256-bit keys
  - Encryption, Decryption (with associated key derivation mode)
- **Can load shared keys from Secure AES**
- AHB slave with suspend/resume & DMA support (IN + OUT channels)
- 32-bit data words swapping support (bit, byte or half-word)
- **Atomic key writing/loading enforcement**

Number of cycles required to process a 128-bit block
Clock frequency= AHB clock of peripheral

Key size	ECB	CBC	CTR	GCM				CCM			
				Init	Header	Payload	Tag	Init	Header	Payload	Tag
128b	51(*)		51	64	35	51	59	63	55	114	58
256b	75 (*)		75	88	35	75	75	87	79	162	82

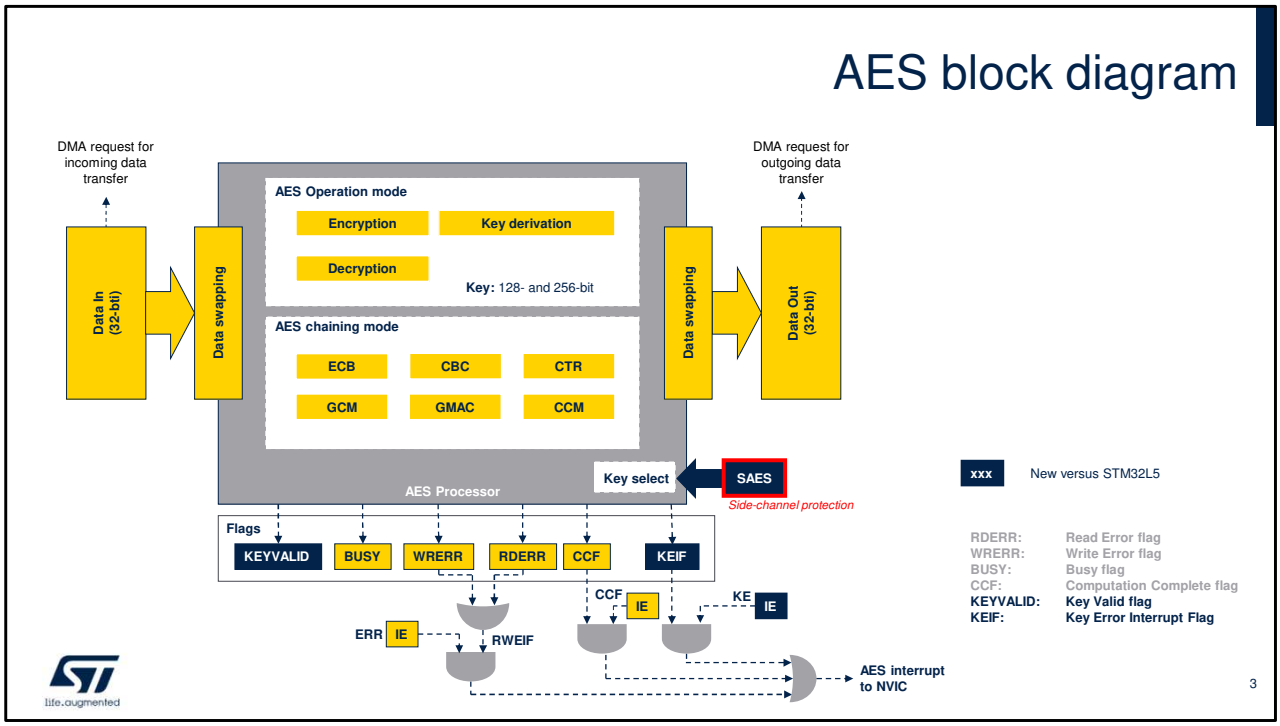
life.augmented

(*) For decryption you must add key derivation time, once

2

The AES accelerator supports three operation modes:
-Encryption
-Decryption
-Key derivation for decryption
It processes 128-bit data blocks using an encryption key that is either 128 or 256 bits long, based on the selected chaining mode.
Atomic key writing and key-loading from SAES peripheral are new features offered by the STM32U5.
Initiating the key-loading sequence sets the BUSY flag and clears the KEYVALID flag.
Once the amount of bits defined by KEYSIZE is transferred to the AES_KEYRx registers, BUSY is cleared and KEYVALID set and the EN bit becomes writable.

That ensures that the key loading operation is successfully completed.
The table indicates the number of clock cycles required to process a 128-bit block of data, according to the chaining mode and the key size.
The AES module can load shared keys from the SAES module. This procedure is controlled by SAES.



This AES block diagram highlights the new features supported by the STM32U5, compared to STM32L5.
The key valid flag and the key error interrupt flag are new.

- KEYVALID is set when a valid key is loaded in key registers.
- KEYEIF is set when key information failed to load into key registers.

The other flags are also present in the STM32L5:

- The Read Error flag (RDERR) is set in the AES Status register when an unexpected read operation is detected during the computation phase or during the input phase.
- The Write Error flag (WRERR) is set in the AES Status register when an unexpected write operation is

detected during the output phase or during the computation phase.

An interrupt can be generated when one of these two error flags is set if the read or write error interrupt enable (RWEIE) bit in the AES interrupt enable register was previously set.

Two extra flags are available for the AES accelerator to indicate the status of current operation:

-The Computation Complete flag (CCF) is set by hardware when the computation is complete. An interrupt is generated if the CCF Interrupt Enable bit was previously set.

-The Busy flag (BUSY), used only with GCM mode, indicates that a higher priority message can interrupt the current message during the GCM payload phase in encryption mode.

The AES module supports hardware key sharing with side-channel resistant SAES peripherals (Shared-key mode), controlled by SAES.

SAES feature list (STM32U5 only)

- NIST FIPS197 compliant AES implementation
- AES chaining modes
  - Electronic codebook (ECB)
  - Cipher block chaining (CBC)
- **Enhanced secure key storage**
  - **Hardware keys (DHUK, BHK)**
    - **Device-dependent, with DHUK**
    - **Application dependent, with BHK**
  - **Hardware secret key decryption (key unwrap)**
  - **Atomic key writing/loading enforcement**
- AES operation modes on 128-bit data blocks, 128 or 256-bit keys
  - Encryption, Decryption (with associated key derivation mode)
- Key modes: normal, **wrapped and shared key (loaded by faster AES engine)**
- AHB slave with suspend/resume & DMA support (IN + OUT channels)
- **Resistant to side channel attacks**

Number of cycles required to process a 128-bit block
➢ Clock frequency = 48MHz unobservable clock (SHSI)

Key size	Encryption		Decryption	
	ECB	CBC	ECB	CBC
128b	528		528 [+200] (*)	
256b	743		743 [+324] (*)	

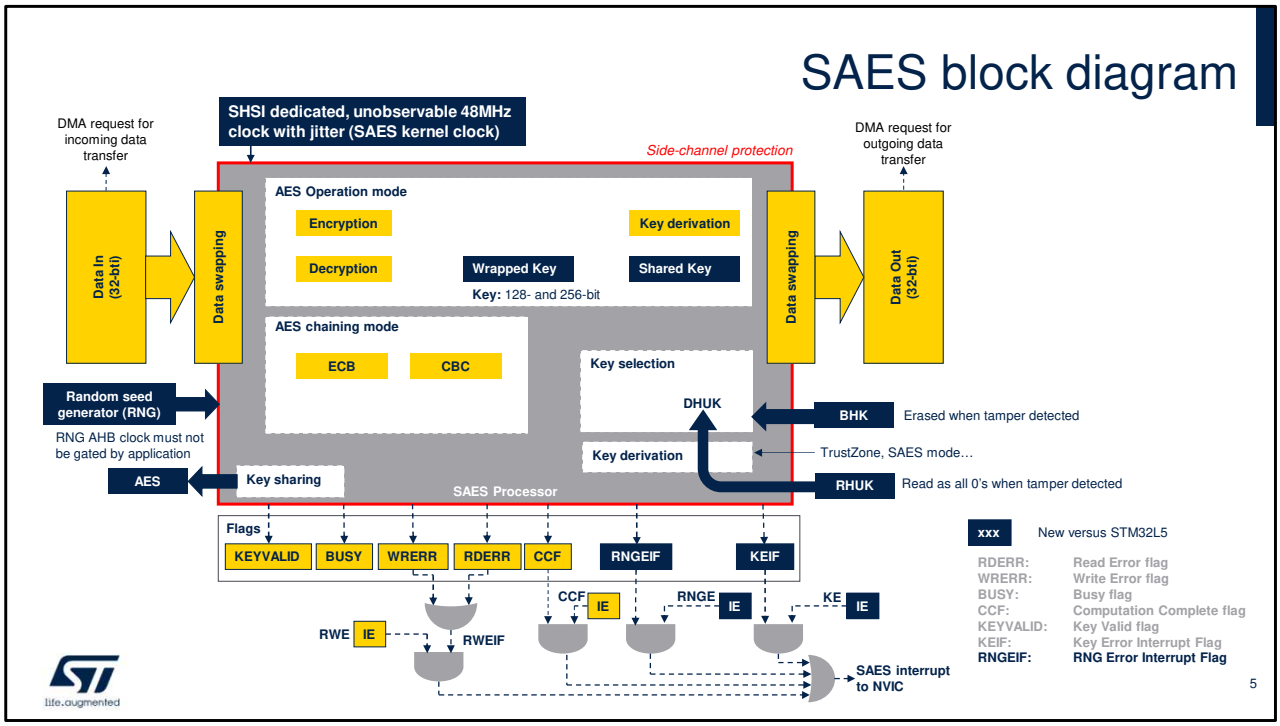
(*) For decryption you must add key derivation time, once

life.augmented

4

The SAES implements features, which are similar to the AES module, they are written in grey.
The new features are written in blue.
Only ECB, and CBC chaining modes are supported.
SAES has the possibility to load secret keys by hardware (boot hardware key BHK and derived hardware unique key DHUK), usable but not readable by the application.
The SAES peripheral can wrap (encrypt) and unwrap (decrypt) application keys using these hardware-secret keys DHUK, XOR-ed or not with the application key BHK.
With this feature, AES keys can be made usable by application software without being exposed in clear-text (unencrypted).
The SAES module incorporates a protection against side-

channel attacks (SCA), including differential power analysis (DPA).
The table indicates the number of clock cycles required to process a 128-bit block of data, according to the chaining mode and key size.
Note that performance is lower than AES.
The SHSI clock provided by the RCC has a 48 MHz frequency with +/-15% jitter.



This SAES block diagram highlights the new features supported by the SAES, compared to AES.
First the 48 MHz kernel clock is unobservable. It is not visible externally.
Then SAES fetches random numbers from the RNG peripheral automatically after a module reset triggered in the RCC.
SAES cannot be used when RNGEIF is set. This flag is set when an error is detected while fetching a random number from RNG peripheral, due to, for example, bad entropy.
SAES has the possibility to load the secret keys DHUK and BHK by hardware.
These keys can be cleared / erased when a tamper is detected, making all secrets undecipherable by the

attacker.
Note that any key managed by SAES, excluding DHUK and BHK, can be shared with the AES module when the SAES key sharing function is activated.

Thank you

life.augmented

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