Hello, and welcome to this presentation that highlights the new features offered by the cryptographic modules of the STM32U5 with respect to STM32L5.

STM32U5 vs. L5: crypto features

Crypto features		STM32L5	STM32U5
Symmetric crypto	AES-128 or 256 ECB, CBC, CTR, GCM, CCM	AES peripheral (same)	
	AES-128 or 256 modes ECB, CBC Side channel attack protection HW protected keys	Not available	**SAES peripheral** **Dedicated bus to share keys with AES peripheral**
Asymmetric crypto	Public key primitives for RSA, DH and ECC over GF(p)	PKA peripheral 32-bit memory	PKA peripheral **Faster core, DPA resistant, 64-bit memory**
Hash functions (+HMAC)	Digests: MD5, SHA-1	HASH peripheral (same)	
	Crypto hash: SHA-256, SHA-224		
Random numbers	FIPS 140-2 NDRNG (NIST SP800-90B certifiable)	TRNG peripheral	TRNG peripheral **Transparently used for side channel protections in PKA, SAES peripherals**
Memory encryption	On-the-fly decryption	OTFDEC peripheral (same)	

life.augmented

2

This table sums up the differences between STM32L5 and STM32U5 cryptographic peripherals.
Regarding symmetric crypto, the STM32U5 supports a new module called Secure AES or SAES, in addition to the regular AES module.
It incorporates a protection against side-channel attacks (SCA), including differential power analysis (DPA).
SAES has the possibility to load secret keys (boot hardware key BHK and derived hardware unique key DHUK) by hardware, usable but not readable by the application.
This transfer is done through a dedicated bus connecting the flash option bytes, in which the key resides, and tamper-resistant secure backup registers.

SAES has the possibility to share keys with the regular AES module.
Regarding asymmetric crypto, the Public Key Accelerator or PKA is based on a faster core, DPA resistant memory.
The PKA RAM is accessed through a wider data bus: 32 bits in the STM32L5, 64 bits in the STM32U5.
The RAM size has also been increased, from 3576 bytes in the STM32L5 to 5336 bytes in the STM32U5.
A tamper detection can reset this RAM.
Hash functions are implemented similarly in STM32L5 and STM32U5.
Regarding the True Random Number Generator, the STM32U5 supports a new feature. The RNG is transparently used for side-channel protection, feeding random seeds to the PKA and SAES modules when they are enabled.
At finally the On-The-Fly decryption module, used to decrypt instructions and read data from external memories, is implemented similarly in STM32L5 and STM32U5.

Thank you

life.augmented

Thank you for attending this presentation!
You can now refer to the presentations that detail the operation of the STM32U5's cryptographic modules:

- Symmetric crypto
- Asymmetric crypto.

The presentation on enhanced anti-tampers can also be useful.