Hello, and welcome to this presentation that highlights the new features offered by the cryptographic modules of the STM32H5.

STM32H5 hardware crypto features

Crypto features		STM32H5
Symmetric crypto	AES-128 or 256 Modes ECB, CBC, CTR, GCM, CCM HW protected keys (from SAES)	**AES peripheral**
	AES-128 or 256 Modes ECB, CBC, CTR, GCM, CCM Side channel attack protection, HW protected keys including derived hardware unique key (DHUK)	**SAES peripheral** **Dedicated bus to share keys with CRYP peripheral**
Asymmetric crypto	Public key primitives for RSA, DH and ECC over GF(p) Side channel attack protection	**PKA peripheral**
Hash functions (+HMAC)	Digest: SHA-1	**HASH peripheral**
	Crypto hash: SHA2-224/ 256/ 384/ 512 Truncated hash: SHA2-512/224, SHA2-512/256	
Random numbers	FIPS 140-3 NDRNG (NIST SP800-90B certifiable)	**RNG peripheral** **Transparently used for side channel protections in PKA and SAES peripherals**
Memory encryption	On-the-fly decryption (AES-CTR, 128-bit)	**OTFDEC peripheral**

See also dedicated modules

life.augmented

2

This table sums up the available hardware cryptographic acceleration in the STM32H5.

Thank you

life.augmented

Thank you for having attended this presentation!
You can now refer to the presentations that detail the operation of the STM32H5's cryptographic modules:

- Symmetric crypto
- Asymmetric crypto
- HASH and True Random Generator
- One-The-Fly decryption engine

A reference to the presentation on enhanced anti-tampers can also be useful.