こちらのプレゼンテーションへようこそ。ここでは、STM32L5 との比較により、STM32U5 の暗号化モジュールで提供される新機能を説明します。

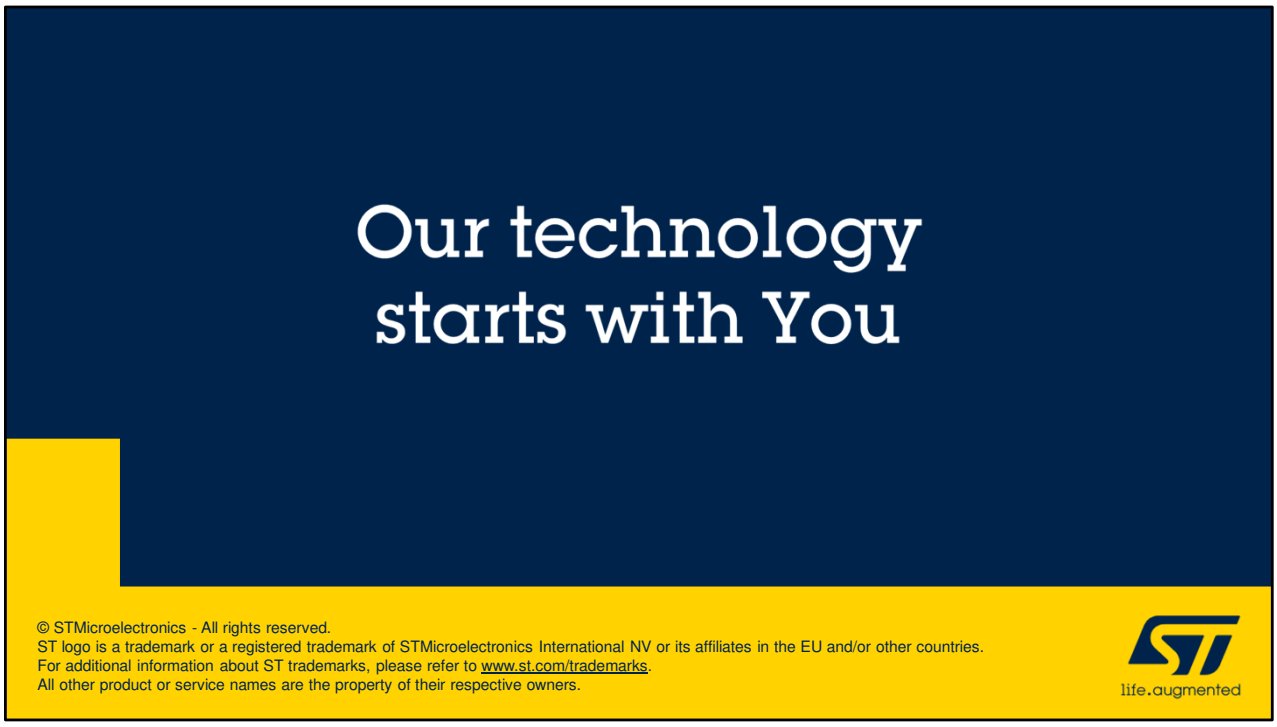
STM32U5 と L5：暗号機能

暗号機能		STM32L5	STM32U5
対称暗号	AES-128 または 256 ECB、CBC、CTR、GCM、CCM	AES ペリフェラル（同じ）	
	AES-128 または 256 モード ECB、CBC サイドチャネル攻撃保護 ハードウェア保護鍵	利用不可	**（SAES ペリフェラル）** **AES ペリフェラルと鍵を共有するための専用バス**
非対称暗号	GF(p) 上の RSA、DH および ECC の公開鍵プリミティブ	PKA ペリフェラル 32 ビットメモリ	（PKA ペリフェラル） **高速コア、DPA 耐性、64 ビットメモリ**
ハッシュ関数（+HMAC）	ダイジェスト：MD5, SHA-1	HASH ペリフェラル（同じ）	
	暗号ハッシュ：SHA-256, SHA-224		
乱数	FIPS 140-2 NDRNG （NIST SP800-90B 認証可能）	（TRNG ペリフェラル）	（TRNG ペリフェラル） **PKA、SAES ペリフェラルのサイドチャネル保護に透過的に使用**
メモリ暗号化	オンザフライ復号	OTFDEC ペリフェラル（同じ）	

life.augmented

2

この表には、STM32L5 と STM32U5 の暗号化ペリフェラルの違いをまとめます。
対称暗号に関して、STM32U5 は、レギュラ AES モジュールに加え、セキュア AES（SAES）と呼ばれる新しいモジュールに対応しています。
差動電力解析（DPA）など、サイドチャネル攻撃（SCA）に対する保護が組み込まれています。
SAES では、秘密鍵（ブートハードウェア鍵 BHK および派生ハードウェア・ユニーク・キー DHUK）をハードウェアによってロードすることができます。これは、アプリケーションから使用はできますが、読出しはできないものです。
この転送は、専用バスを介して、鍵が存在する Flash オプションバイトと、耐タンパ性のセキュアバックアップレジスタを接続することにより実行されます。
SAES では、レギュラ AES モジュールと鍵を共有することができます。
非対称暗号に関して、公開鍵アクセラレータ（PKA）では、より高速なコアである DPA 耐性メモリを使用しています。PKA RAM へのアクセスは、より幅の広いデータバスを介して行われます。STM32L5 では 32 ビット、STM32U5 では 64 ビットです。
RAM サイズも、STM32L5 では 3576 バイトでしたが、STM32U5 では 5336 バイトに拡大されています。タンパ検出によって、この RAM をリセットできます。
ハッシュ関数は、STM32L5 と STM32U5 で同様に実装されます。
真の乱数発生器（RNG）に関して、STM32U5 は新機能に対応しています。RNG はサイドチャネル保護に透過的に使用され、PKA および SAES モジュールが有効になるとこれらにランダムシードを供給します。
最後に、命令の復号化および外部メモリからのデータの読出しに使用されるオンザフライ復号化モジュールが、STM32L5 と STM32U5 に同様に実装されています。



このプレゼンテーションにご参加いただき、ありがとうございました。
STM32U5 の暗号モジュールの動作を詳しく説明したプレゼンテーションを参照してください。

- 対称暗号
- 非対称暗号

強化された耐タンパに関するプレゼンテーションも有用です。