非対称暗号化アプリケーションに広く使用されている STM32U5 公開鍵アクセラレータのプレゼンテーションへようこそ。

新バージョン V.S. STM32L5

PKA の機能

- 非対称暗号化の高速化：RSA/DH では最大 4160 ビット、楕円曲線では 640 ビット
  - NIST FIPS186-4、RSA PKCS#1、ANSI X9.62、IETF RFC5639（Brainpool）、Chinese SM2、および SEC2 曲線で使用
- 秘密を操作するサイドチャネル攻撃に対する保護
  - RSA / DSA 専用のべき剰余
  - ECC スカラー乗算、署名生成
- 秘密を操作しないオペレーションにも対応
  - RSA/DSA 公開べき剰余およびその高速な CRT（Chinese Remainder Theorem：中国剰余定理）バージョン
  - ECDSA 署名の検証
  - ECC 曲線上の点の確認、完全な加算、ダブルベースラダー & 座標変換（プロジェクティブからアファイン）
  - 加算、減算、乗算、比較、訳文などの算術および剰余演算

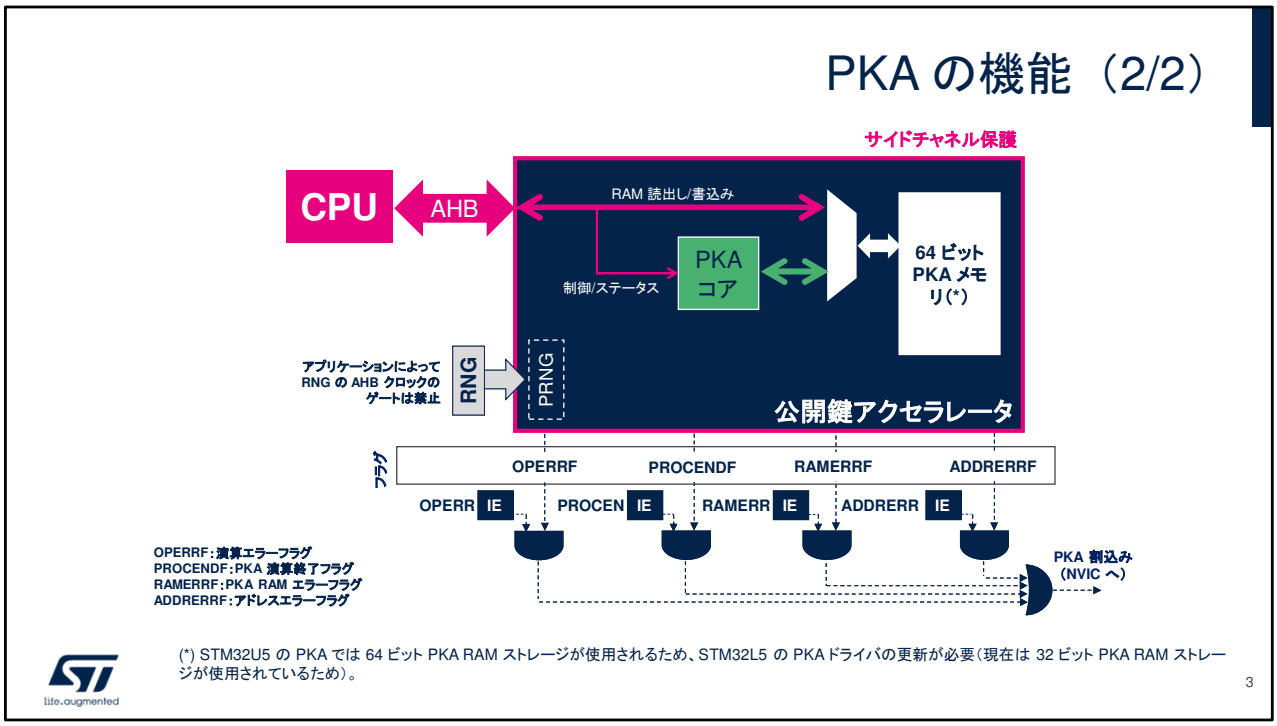
life.augmented

注：これらの操作を行うには、STM32L5 の PKA ドライバの更新が必要（次を参照）

公開鍵暗号化は、多くのセキュリティ標準の一部であり、インターネットのような安全でないオープンネットワークで安全な通信チャネルを確立したり、電子署名による認証を提供したりするために広く使用されています。
ソフトウェアのみのソリューションでは、リアルタイムアプリケーションには時間がかかりすぎ、システム全体の性能に影響する可能性があります。

PKA モジュールは、CPU によって実行される公開鍵暗号化動作を高速化する効率的なハードウェアアクセラレータです。リベスト、シャミア、エーデルマン（RSA）、ディフィー – ヘルマン（DH）、素体上の楕円曲線暗号（ECC）の演算を高速化することができます。サポートされるオペランドサイズは、RSA および DH では最大 4160 ビット、ECC では最大 640 ビットです。2 値曲線、エドワーズ曲線、および Curve25519 は、PKA ではサポートされません。

ここでは、サポートされる演算のリストを説明します。RSA 復号化のための STM32L5 のべき剰余とは異なり、ECC のスカラー乗算と署名はサイドチャネル攻撃から保護されます。これらの演算は、秘密鍵を操作するときに使用されます。



PKA では CPU の負荷を軽減するため、専用の PKA メモリを使用して PKA コアで主要な演算を行います。
最初に 初期データが CPU により、アドレスオフセット 0x400 にある PKA 内部 RAM にロードされます。次に、PKA 制御レジスタで CPU により、実行する演算が指定され、最後に START ビットがアサートされます。PKA により演算終了（PROCENDF）が報告されると、CPU により結果のデータが PKA RAM から読み出され、PROCENDF フラグがクリアされます。
ソフトウェアでは、PKA_CR レジスタの EN ビットをクリアすることによって、いつでも PKA 演算をアボートできます。この場合、PKA メモリの内容は保証されません。

PKA にはエラーフラグとして、演算エラーフラグ（OPERRF）、アドレスエラーフラグ（ADDRERRF）、RAM エラーフラグ（RAMERRF）の 3 つがあります。対応する割込み有効ビット（OPERRIE、PROCENDIE、ADDRERRIE、または RAMERRIE）がセットされている場合、すべてのフラグで割込みを生成できます。
PKA ペリフェラルリセット信号が解放されると、PKA RAM は自動的にクリアされます。これには 667 クロックサイクル必要です。この間、PKA_CR の EN ビットの設定は無視されます。

PKA サイドチャネル保護操作（RSA 復号化のべき剰余、ECC のスカラー乗算および署名）では、演算終了時に自動的に PKA RAM から消去される秘密を管理します。

PKA 処理時間（STM32L5@110MHz）

- べき剰余演算（ミリ秒）

	指数の長さ（ビット単位）	オペランドの長さ(ビット単位)		
		1024	2048	3072
パブリック	3	2.8	7.4	15.8
プライベート	1024	103 または 32（CRT）	-	-
	2048	-	750 または 213（CRT）	-
	3072	-	-	2500 または 667（CRT）

- その他の演算（ミリ秒）

注：CRT は「中国の剰余定理」最適化です。

	係数の長さ（ビット単位）			
	256	384	512	521
ECC スカラー乗算	44	124	262	301
ECDSA 署名	48	133	278	323
ECDSA 検証	95	265	558	651

life.augmented

4

ここに、指数とオペランドサイズごとのべき剰余演算の処理時間を示します。ECC スカラー乗算などの重要な演算や、ECDSA 署名/検証についても説明します。
値は STM32L5 において、110MHz の PKA クロックについて計算しています。

新バージョン V.S. STM32L5
（同じ周波数）

PKA 処理時間（STM32U5@110MHz）

- べき剰余演算（ミリ秒単位）（DPA 耐性）

	指数の長さ（ビット単位）	オペランドの長さ（ビット単位）		
		1024	2048	3072
パブリック	3	1.1	4.5	6.2
プライベート	1024	90、52、または 16（CRT）	-	-
	2048	-	580、380、または 106（CRT）	-
	3072	-	-	1800、1240、または 335（CRT）

2 倍の高速化（非 DPA）

DPA が 20% 高速化

- その他の演算（ms単位）（DPA 耐性）

注：CRT は「中国の剰余定理」最適化です。

	係数の長さ（ビット単位）			
	256	384	512	521
ECC スカラー乗算	28	77	162	191
ECDSA 署名	25	65	131	152
ECDSA 検証	27	72	153	175

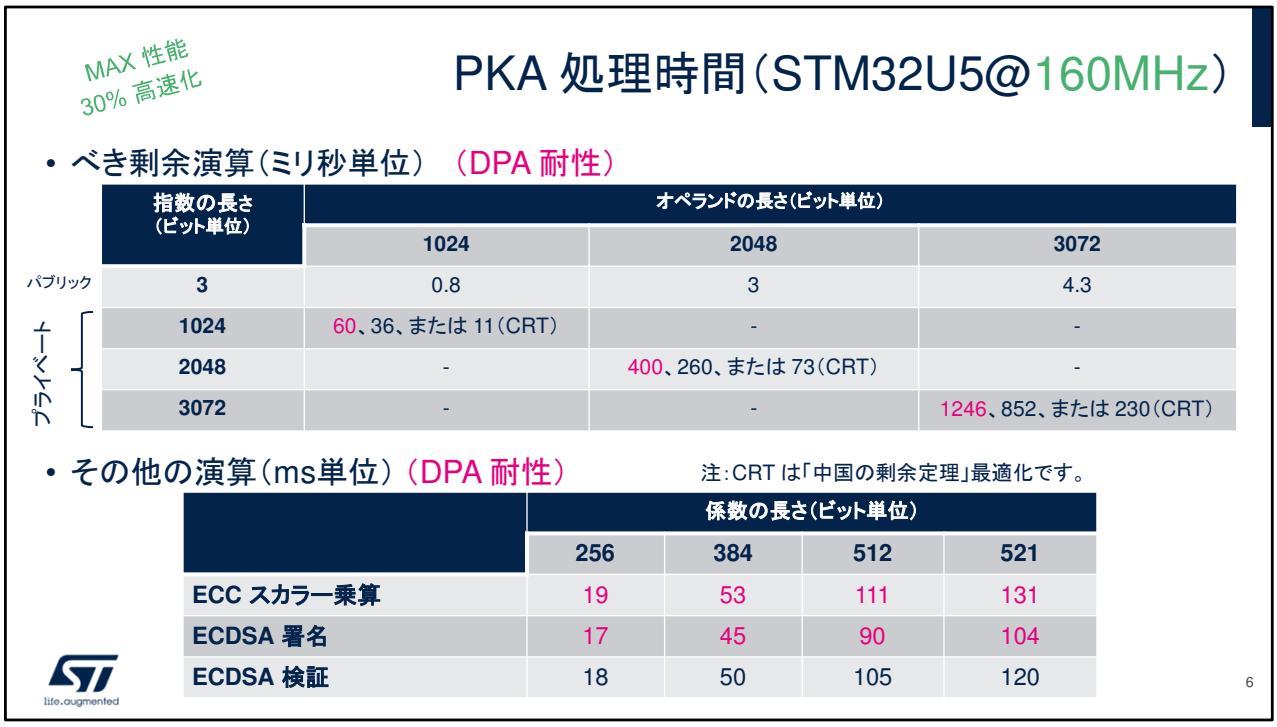
2 倍の高速化

70% 高速化

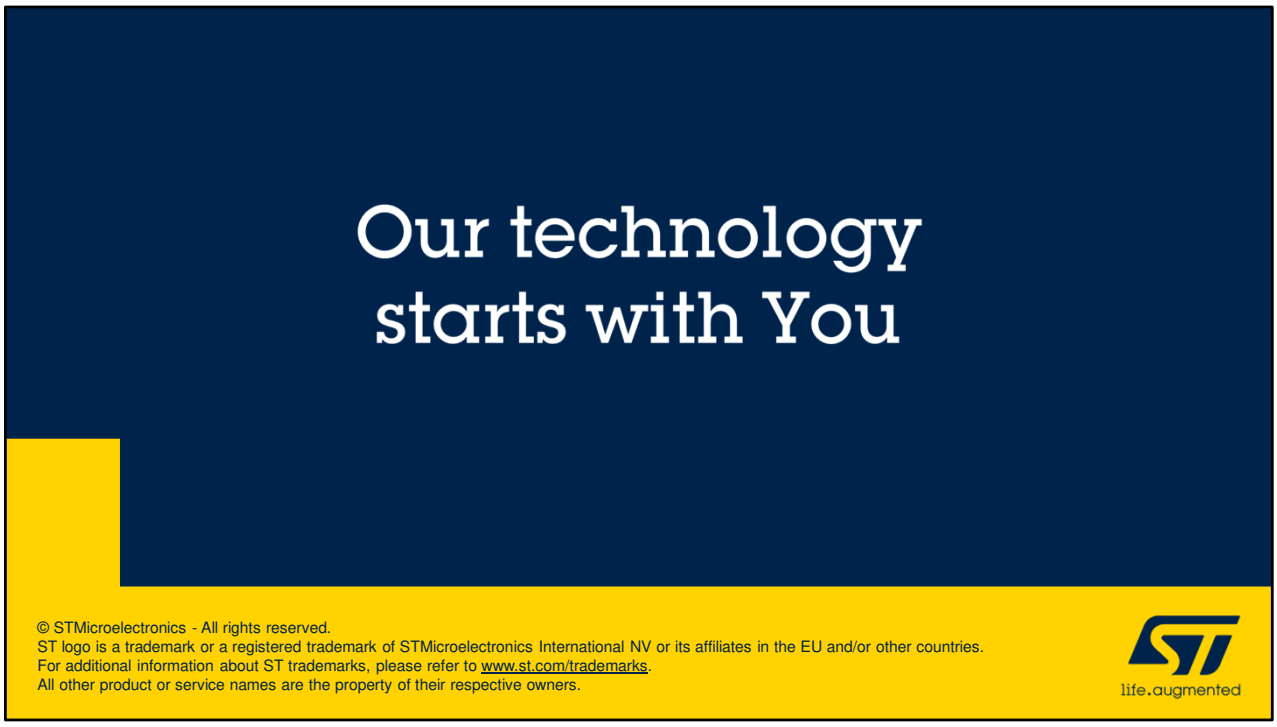
life.augmented

5

ここに、指数とオペランドサイズごとのべき剰余演算の処理時間を示します。ECC スカラー乗算などの重要な演算や、ECDSA 署名/検証についても説明します。
値は STM32U5 において、110MHz の PKA クロックについて計算しています。同じクロックで動作している STM32L5 PKA との違いをハイライトして示しています。



ここに、指数とオペランドサイズごとのべき剰余演算の処理時間を示します。ECC スカラー乗算などの重要な演算や、ECDSA 署名/検証についても説明します。
値は、160MHz のクロックで計算されています。



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。