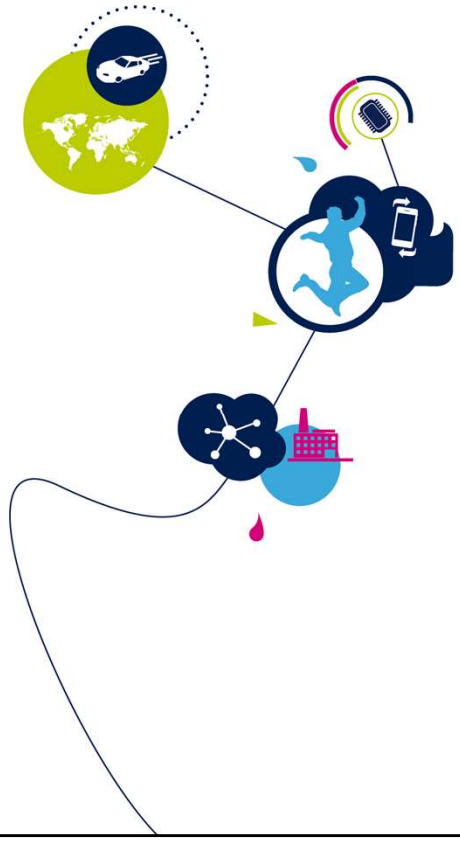
STM32WB – PKA

公開鍵アクセラレータ

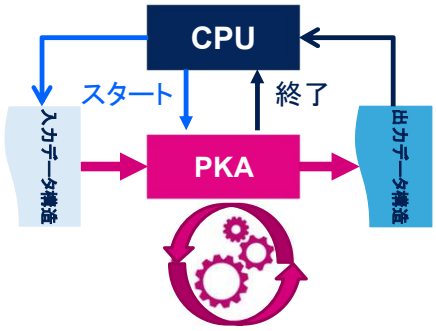
1.0 版



life.augmented

STM32WB マイクロコントローラに組み込まれている STM32 公開鍵アクセラレータのプレゼンテーションにようこそ。
ここでは、暗号アプリケーションに広く要求されている非対称鍵暗号の実行に用いられる機能の説明を行います。

概要



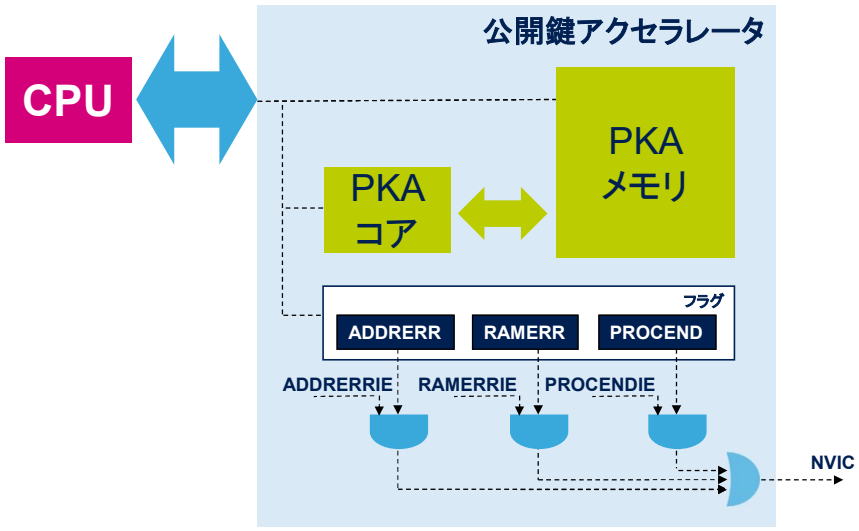
- PKA を使用すると、CPU によって実行される公開鍵暗号が大幅に高速化。
- PKA は世界で広く使用されている多くのセキュリティ規格（NIST、IEEE、ANSIなど）に対応。

アプリケーション側の利点

- インターネットのようなオープンネットワークを通じたセキュア通信チャネルの確立や、電子署名を介した完全性と認証の提供
- 対称暗号（AES）よりも 1 桁長い CPU 処理時間を大幅に削減

公開鍵暗号は、数多くのセキュリティ規格の一部であり、インターネットのような非セキュアなオープンネットワークにセキュアな通信チャネルを確立するためや、電子署名を介して認証を行うために、広く用いられています。
ソフトウェアのみのソリューションはリアルタイムアプリケーションには遅すぎて、システムの全体性能に影響を及ぼします。
PKA ペリフェラルは、CPU によって実行される公開鍵暗号操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。

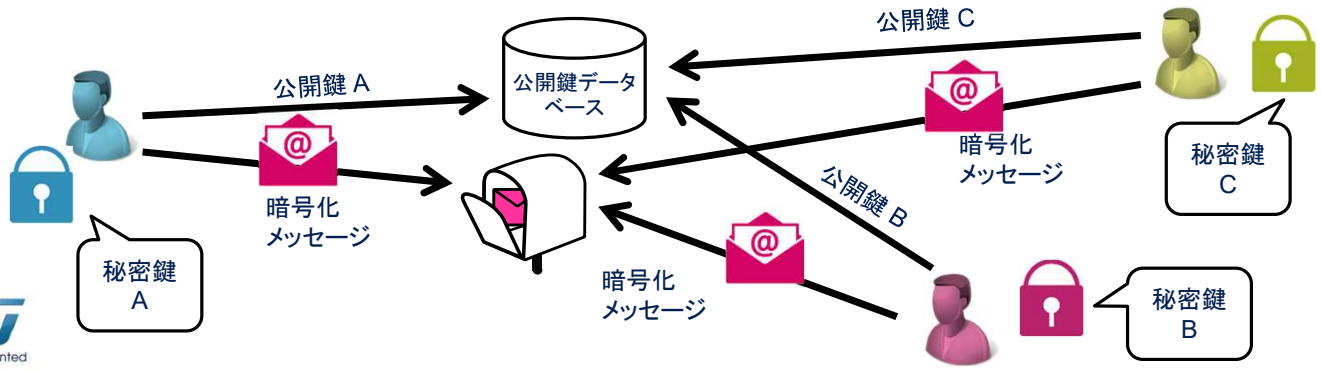
PKA のブロック図



公開鍵暗号の実行には、すべてをソフトウェアで行うと大きな負荷となる集中的な演算が必要となります。公開鍵アクセラレータによって、PKA コアの中で専用 PKA メモリを使用したキー操作が行われ、STM32WB CPU の負荷が軽減されます。
CPUは、アドレスオフセット 0x400 にある PKA 内部 RAM に初期データをロードします。次に、CPU は PKA 制御レジスタの中で実行すべき操作を指定し、最後に START ビットをアサートします。PKA が操作の終了（PROCENDF）を報告すると、CPU は結果データを PKA RAM から読み出してから PROCENDF フラグをクリアします。
ソフトウェアは、PKA_CR レジスタの EN ビットをクリアすることで、PKA 操作をいつでもアボートできます。この場合、PKA メモリの内容は保証されません。
PKA には、アドレスエラーフラグ（ADDRERRF）と RAM エラーフラグ（RAMERRF）の 2 種類のエラーフラグがあります。すべてのフラグは、対応する割込みイネーブルビット（PROCENDIE、ADDRERRIE、またはRAMERRIE）がセットされている場合、割込みを生成可能です。

アプリケーション例：キー配信

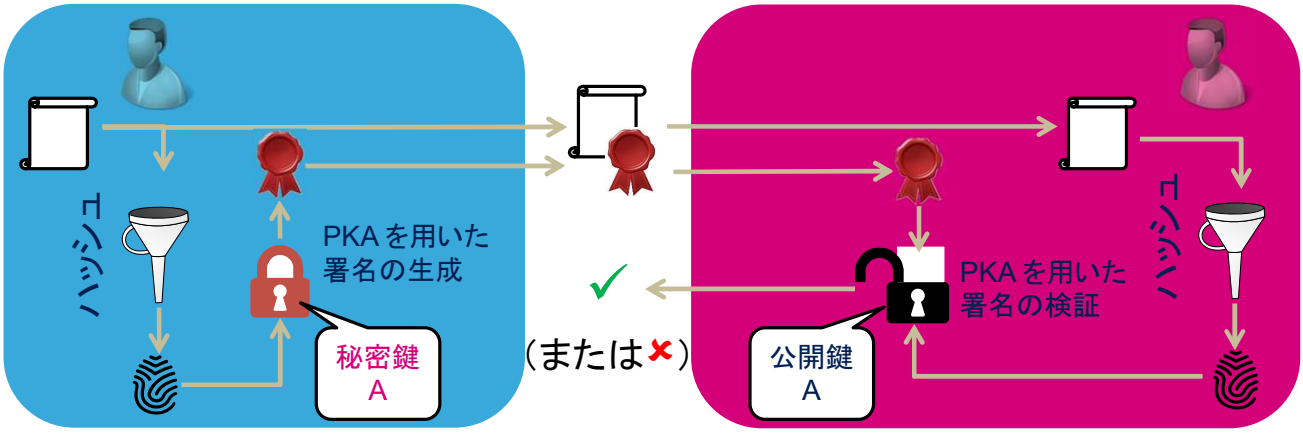
- 複数の人が秘密の方法で情報を交換したいと思った場合、異なるキーを 2 個使用することが非常に効率的。
  - 1 個のキーは平文メッセージを暗号化、もう 1 個のキーは暗号文メッセージを復号化。
- 暗号化キーは公開されており、復号化キー（秘密鍵）の唯一の所有者に暗号化されたメッセージを送信するのは誰にでも可能。



公開鍵暗号は、インターネットのような非セキュアなネットワークを通じて秘密の方法でメッセージを交換する際の問題に対して、非常にエレガントなソリューションを提供します。メッセージを交換する各人は、自分の公開鍵を用いて暗号化された後に自分に送信されてきたメッセージを復号化するために使用する秘密鍵を保有しています。
この技術が機能するには、一般大衆の公開鍵の信頼できる中央リポジトリが推奨されます。

アプリケーション例：デジタル署名

- 所有者だけがアクセス可能な秘密鍵は、所有者の公開鍵情報を用いて誰でも検証可能であるデジタル署名の生成に使用可能。
  - デジタル署名 が所定の公開鍵で機能しない場合、その唯一の所有者 がそのメッセージ の作成者であることはあり得ない。



デジタル署名は、会計トランザクショントークンなどのデジタル資産の完全性、認証、否認防止を保証する強力な技術です。
人「A」は、最初にメッセージにセキュアなハッシュ関数を適用し、自分の秘密鍵を用いて結果として得られたダイジェストを暗号化することで、署名されたメッセージを作成できます。結果として得られた署名は、メッセージとともに人「B」に送信されます。
人「B」は、同じハッシュ関数を適用してから、Aの署名付きのメッセージを検証します、その後にメッセージをAのパブリックキーと署名の検証機能を実行した時の結果で検証できます。検証機能の結果によって、メッセージが本物であるか否かが判定されます。

PKA 機能（1/2）

- 非対称暗号（FIPS 186-4、RSA PKCS#1、ANSI X9.62、Brainpool など）の高速化
  - べき剰余とその高速 CRT バージョン（中国の剰余定理）
  - ECC スカラー乗算
  - 曲線上の点からの計算、公開鍵の検証は重要（他者から）
  - ECDSA 署名の生成および検証
- 加算、減算、乗算、比較、リダクションなどの非対称演算と剰余演算

これは、PKA が実行できる演算のリストです。
非対称暗号の高速化：
- べき剰余および RSA 中国剰余定理（CRT）べき乗
- ECC スカラー乗算および曲線上の点からの計算
- ECDSA 署名の生成および検証

算術演算と剰余操作：
- 算術加算、減算、乗算、比較
- 剰余加算、減算、リダクション & 逆数
- モンゴメリ乗算

これらの演算により、PKA は多くの標準公開鍵アルゴリズムに対応しています：べき剰余、CRT べき乗、RSA 暗号、楕円曲線暗号（ECC）、デジタル署名アルゴリズム（DSA）、楕円曲線 DSA（ECDSA）

PKA 機能(2/2)

- RSA/DH では最大 3136bit、楕円曲線では最大 640bit のオペランドを処理可能
  - 暗号鍵長推奨ウェブサイト https://www.keylength.com によると、これらのキー値は現在のコンピュータ・アーキテクチャを用いて長期間使用可能です。
- モンゴメリ定義域内外への変換
- AMBA AHB スレーブペリフェラル

公開鍵アクセラレータ(PKA)は、Rivest, Shamir and Adleman(RSA)、Diffie-Hellman(DH)、楕円曲線暗号(Elliptic Curve Cryptography: ECC)の素数演算を高速化するために使用されます。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 3136bit、ECC では最大 640bit です。
PKA は、Arm® アドバンストマイクロコントローラバスアーキテクチャ(AMBA)の AHB スレーブペリフェラルであり、32bit ワードのシングルアクセスでのみアクセス可能です(それ以外は、書込みの場合に AHB バスエラーが発生し、書込みアクセスは無視されます)。

PKA 処理時間

- べき剰余演算(ミリ秒)

指数の長さ(bit)	オペランドの長さ(bit)		
	1024	2048	3072
$2^{16}+1$	3 または 1(高速)	9 または 4(高速)	20 または 9(高速)
1024	91 または 88(高速) または 27(CRT)	-	-
2048	-	654 または 640(高速)または 183(CRT)	-
3072	-	-	2140 または 573(CRT)

注 1:高速モードにはモンゴメリパラメータ計算が必要です。
注 2:CRTは中国剰余定理最適化のことです。

- 他の演算(ミリ秒)

	係数の長さ(bit)			
	256	384	512	521
ECC スカラー乗算	38	106	225	259
ECDSA 署名	41	114	239	277
ECDSA 検証	82	227	479	559

life.augmented

これらの表には、各種の指数サイズとオペランドサイズを用いた、べき剰余の処理時間が示されています。
数字に「高速」という表記があるものについては、高速演算の実行にはこの情報が必要であるため、アプリケーションがモンゴメリパラメータ計算を実行する必要があります。モンゴメリパラメータは連続した数回の計算で再利用可能であり、多くの回数を繰り返した場合に演算全体がより効率的となります。
モンゴメリ乗算オーバヘッド:1024bit(+0ms)、2048bit(+3ms)、3072bit(+8ms)

割込みと DMA

割込みイベント	説明
PKA 演算終了	計算が完了したときにセットされます。
PKA RAM アクセスエラー	PKA 演算の進行中に PKA RAM アクセスが検出された場合にセットされます。
マップされていないアドレスへのアクセスエラー	PKA RAM アクセスが範囲外（マップされていないアドレス）であると検出された場合にセットされます。

- PKA は DMA の使用に非対応。

life.augmented

ここでは、ネスト化されたベクタ割込みコントローラで割り込みをトリガ可能な PKA イベントである、PKA 計算終了、PKA RAM アクセスエラー、マップされていないアドレスへのアクセスエラーの概要を示します。
ダイレクトメモリアクセス（DMA）コントローラは、PKA とともに使用できません。

低電力モード

モード	説明
RUN	アクティブ
SLEEP	デフォルトでアクティブ（ディセーブル可能）
STOP 0 / STOP 1 / STOP 2	無効
STANDBY	パワーダウン
SHUTDOWN	パワーダウン

life.augmented

ここでは、各低電力モードにおける PKA ペリフェラルのステータスの概要を示します。
デバイスが STOP モードのときには、PKA の動作はできません。

関連ペリフェラル

- このペリフェラルに関連した以下のペリフェラルトレーニングを参照してください。
  - RCC（PKA クロック有効、PKA リセット）
  - 割込み（NVIC）

これは、PKAに関連したペリフェラルのリストです。詳細については、必要に応じてこれらのペリフェラルトレーニングを参照してください。

参照(1)

- 詳細と追加情報については、以下を参照してください。
  - RSA
    - PKCS#1：RSA Cryptography Standard（v1.5、2.1 および v2.2）[RSA ラボ]
  - DH
    - ANSI X9.42：Implementation of Diffie-Hellman [ANSI]
    - PKCS#3：Diffie-Hellman Key Agreement Standard [RSA ラボ]
  - 楕円曲線
    - ANSI X9.63：Key Agreement and Key Transport Using Elliptic Curve Cryptography [ANSI]
    - IEEE 1363：Standard Specifications For Public Key Cryptography [ANSI]
  - 楕円曲線（続き）
    - ANSI X9.62：The Elliptic Curve Digital Signature Algorithm [ANSI]
    - FIPS 186-4：Digital Signature Standard（DSS）[NIST]
    - SP 800-56A and SP 800-56B [NIST]
    - Curve25519：Key establishment based on ECC [Daniel J. Bernstein]

life.augmented

これらのリンクと参考資料では不十分な場合には、次のスライドに記載されている STM32CubeMX リポジトリの中の PKA ドライバを参照してください。

参照(2)

- 詳細と追加情報については、以下の STMicroelectronics ソフトウェアリファレンスを参照してください。
  - STM32WB 上で PKA を用いてアプリケーションを開発するユーザを支援するために、2 つの C ソフトウェアライブラリが提供されています。
    - ローレイヤ(LL)ライブラリは、直接レジスタアクセスによって PKA のプログラミングを行っている経験を積んだユーザのためのものです。
    - ハードウェア抽象化レイヤ(HAL)ライブラリは、使いやすい機能を提供します。
  - これらのライブラリは、www.st.com から直接入手可能な STM32CubeMx(STM32 用グラフィカル構成ツール)に付属しています。
    - stm32cubemx(www.st.com)
  - これらのライブラリは、STM32CubeWB ページから .zip ファイルとして直接ダウンロード可能です。

life.augmented

詳細と追加情報については、以下の有用ソフトウェアリファレンスを参照してください。