注意: この日本語版文書は参考資料としてご利用ください。
最新情報は必ずオリジナルの英語版をご参照願います。

MICROCHIP

AN3923

SAM E54向けのMPLAB Harmony v3を使ったAES暗号モード

はじめに

AES(共通鍵暗号化規格)は、Rijndael(ラインダール) アルゴリズムとしても知られている対称ブロック暗号化アルゴリズムで、NISTの仕様(FIPS PUB. 197)に準拠し、128ビット、192ビット、256ビットの鍵長を使って128ビットのデータブロックを処理できます。対称キーアルゴリズムは暗号化と復号に同じ鍵を必要とします。AESはNIST Special Publication 800-38A/B/C/Dで推奨されているブロック暗号アルゴリズム向けに特別に設計された各種動作モードで使えます。

SAM D5x/E5xファミリのデバイスはAES暗号化ハードウェアをサポートしています。本書では、SAME54のMPLAB® Harmony v3フレームワークにおける以下の4つの機密保持動作モードのAESの実装について説明します。

- ECB(Electronic Code Book)
- CBC(暗号ブロックチェーン接続)
- CTR(カウンタ)
- GCM(ガロアカウンタ モード)

MPLAB Harmony v3は、サードパーティのwolfSSLライブラリ上に構築された暗号化ライブラリを使います。wolfSSLライブラリのwolfCrypt部分は、デバイスのAESブロックの設定と管理のためのインターフェイスを提供します。

目次

はじめに 1

1. 用語集 3

2. AESの概要 4
   - 2.1 AES暗号化 4
   - 2.2 AES復号 5

3. MPLAB Harmony v3におけるAES暗号モード 6
   - 3.1 暗号化ライブラリ 6
   - 3.2 AESの動作モード 6

4. AESモードの暗号化/復号の例: アプリケーションの実装 9
   - 4.1 前提条件 9
   - 4.2 アプリケーションの概要 9
   - 4.3 デモ アプリケーションの実行 10
   - 4.4 アプリケーションの作成 12

5. 補遺 16
   - 5.1 補遺A: AES暗号モードのベクタの例 16
   - 5.2 補遺B: 確認事項 17

6. 参考情報 21

Microchip社ウェブサイト 22

製品変更通知サービス 22

お客様サポート 22

Microchip社のデバイスコード保護機能 22

法律上の注意点 22

商標 23

品質管理システム 24

各国の営業所とサービス 25

1. 用語集

本書では以下の用語を使います。

AES	Advanced Encryption Standard(共通鍵暗号化規格)の略。
ブロック暗号	一定のサイズのデータを処理する暗号アルゴリズム。AESは16バイトのブロック単位で転送します。
CBC	Cipher Block Chaining(暗号ブロックチェーン接続)の略。
CT(暗号文)	暗号化されたデータ。
CTR	カウンタ。
ECB	Electronic Code Bookの略。
GCM	Galois Counter Mode(ガロアカウンタ モード)の略。
復号	機密保持モードのプロセスのうち、暗号化されたデータを元の使用可能なデータに変換するプロセス。
暗号化	機密保持モードのプロセスのうち、使用可能なデータを読み取り不可能な形式に変換するプロセス。
FIPS	Federal information Processing Standard(連邦情報処理標準)の略。
Forward Cipher Function(正暗号関数)	ブロック暗号アルゴリズムの2つの関数のうち、暗号化キーによって選択される関数。
初期化ベクタ(IV)	一部の動作モードにおいて、初期入力として追加で必要となるデータブロック。
Inverse Cipher Function(逆転暗号関数)	同じ暗号鍵が使われる時、Forward Cipher Functionを逆転変換させる関数。
出力ブロック	ブロック暗号アルゴリズムのForward Cipher FunctionまたはInverse Cipher Functionからの出力データブロック。
入力ブロック	ブロック暗号アルゴリズムのForward Cipher FunctionまたはInverse Cipher Functionへの入力データブロック。
PT(平文)	モードへの入力としてフォーマットされた使用可能なデータ。
S-box	複数バイト置換変換とキー拡張ルーチンで使われる非線形置換テーブルで、1対1のバイト値の置換を実行します。

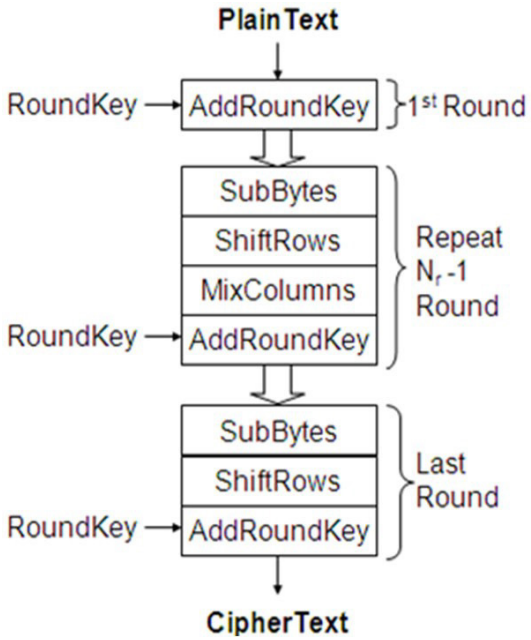
2. AESの概要

AES(共通鍵暗号化規格)は、電子データ保護のために利用できるFIPS承認(FIPS Pub.197)の暗号アルゴリズムを実装します。AESは、入力データの128ビットブロックに対して指定された回数だけ動作する対称キーアルゴリズムです。対称キーとは暗号化と復号化の両方に同じキーを使うという意味です。暗号化プロセスはデータを理解不可能な形態(暗号文と呼ぶ)に変換します。復号プロセスは暗号文から元の平文にデータを変換します。暗号文の長さは平文の長さと同じです。AESの暗号化と復号に使う鍵の長さは128ビットの固定入力ブロックサイズに対して128ビット、192ビット、または256ビットにする事ができます。鍵の長さによって実行されるラウンド数とE54ハードウェアがブロック演算を実行するのにかかる時間が決まります。鍵長が長いほど、ハードウェアがブロック演算を実行するのにかかる時間は長くなります。

2.1 AES暗号化

AES-128暗号化プロセスには、128ビットのデータ暗号化のための初期ラウンドと10ラウンドの暗号化が含まれます。まず、キー拡張ルーチンを使って128ビットキーが11個の128ビット ラウンドキーのセットに拡張されます。これらの各キーがラウンドに使われ、その結果として最終的に暗号文が出力されます。AES暗号化に関わる全体的なプロセスを以下の図に示します。

図2-1. AES暗号化



AES暗号化アルゴリズムには以下のステップが含まれています。

1. キーの拡張 - AESキー拡張ルーチンは、ユーザから対称キーを取得し、ラウンドキーのセット (キースケジュールと呼ぶ)を生成します。これらの各キーがそれぞれのラウンドに使われ、その結果として最終的に暗号文が出力されます。
2. 初期ラウンド - AES暗号化の初期ラウンドには、平文が暗号文とXOR演算されるAddRoundKeyステップが含まれます。このプロセスでは、状態の各バイトがビット単位のXORを使ってラウンドキーと結合されます。
3. ラウンド - 以降のラウンドでは、各種のバイト指向変換を実行します。一般的に、1ラウンドは以下のサブプロセスで構成されます。
   - SubBytes - S-boxを使ったバイト置換。
   - ShiftRows - 状態の配列の行を各種オフセットでシフトさせます。

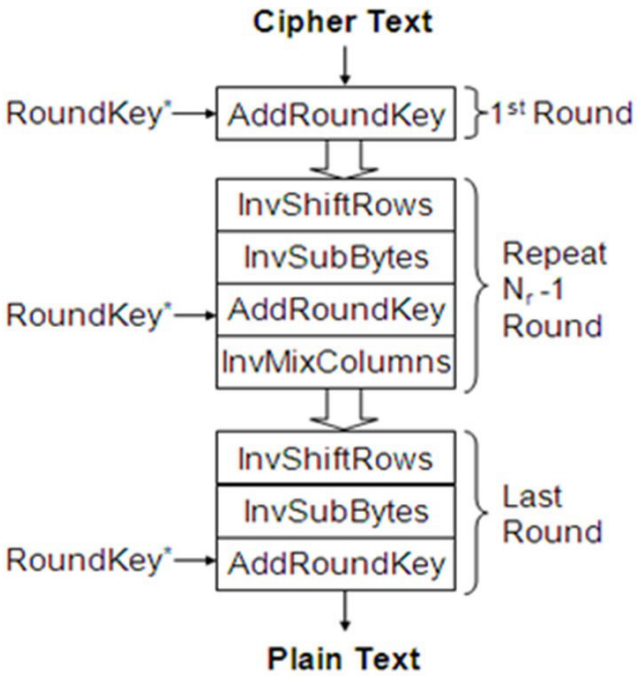
- MixColumns - 各列内のデータをミックスします。
- AddRoundKey - ラウンドキーを状態に追加します。

4. FinalRound - 最終ラウンド(n番目のラウンド)は同じサブプロセスを含みますが、MixColumnsプロセスは使いません。

2.2 AES復号

AES暗号文の復号プロセスでは、暗号化プロセスを逆順に行います。
AES-128復号プロセスにはAES-128暗号化プロセスと同様のラウンド数が含まれ、対応する逆変換を行います。

図2-2. AES復号



AES復号アルゴリズムのステップを以下に説明します。

1. 初期ラウンド - AES復号の初期ラウンドには、AES暗号化プロセスと同じAddRoundKeyステップが含まれます。
2. ラウンド - 以降のラウンドでは逆変換を行います。以降のラウンドの逆変換を以下に示します。
   - InverseShiftRows - ShiftRows変換の逆変換です。
   - InverseSubBytes - 逆S-Boxを使ったSubBytes変換の逆変換です。
   - AddRoundKey - 入力ブロックと出力ブロック間でのXOR演算のみを行うため、暗号化ステップと同じです。
   - InverseMixColumn - MixColumns変換の逆変換です。
3. FinalRound - 最終ラウンドでは、MixColumnsステップを除く上記のステップが必要です。

Note: AESの暗号化と復号のステップは、SAME54デバイス内のハードウェアAESエンジンによって処理されます。このプロセスにユーザがソフトウェアを使う必要はありません。AES規格の詳細は「FIPS PUB. 197」を参照してください。

3. MPLAB Harmony v3におけるAES暗号モード

3.1 暗号化ライブラリ

MPLAB Harmony v3の暗号ライブラリは便利なC言語インターフェイスを持つ暗号化ライブラリを提供します。この暗号ライブラリは、組み込みアプリケーション内で暗号化、復号、ハッシング、認証、圧縮等を実行するための多くの関数を提供します。対称ブロック暗号であるAESは、ECB、CBC、CTR、GCM等の様々な暗号モードに対応した暗号ライブラリの暗号化APIと復号APIを提供します。

この暗号ライブラリはwolfSSLのwolfCryptライブラリ上に構築されています。wolfCrypt暗号化エンジンはANSI「C」で記述された軽量暗号ライブラリです。主にそのサイズの小ささ、高速性、機能セットにより、組み込み、RTOS、リソース制約のある環境をターゲットとしています。Microchip社はWolfSSL社とWolfSSLをロイヤリティフリーで利用する契約を結んでいます。Microchip社製品を使う場合、wolfSSLライブラリを追加ライセンス料金なしで利用できます。ライセンスの詳細はこちらを参照してください。

Cryptoリポジトリには、MPLAB Harmony v3フレームワーク向けの暗号モジュールが含まれています。暗号モジュールには、暗号化用のMPLAB Harmony v3 API、ハードウェア暗号アクセラレーションのためのSAM E54ドライバ(その他のデバイスもサポート)、ハードウェア アクセラレータを使うためのwolfCryptまたはwolfSSLライブラリのデルタ/パッチが含まれています。以下のファイルがAESの暗号処理に関連しています。

configuration.h	暗号化ライブラリの設定

表3-1. 暗号化ライブラリのファイル

crypto.h	暗号ライブラリへのインターフェイス
crypto.c	全ての暗号ライブラリ関数の定義

表3-2. wolfCryptライブラリのファイル

aes.h	Wolfcryptライブラリ関数へのインターフェイス
crypt_aes_u2238.h	ハードウェアAES用の暗号フレームワーク ライブラリ インターフェイス ファイル
crypt_aes_u2238.c	暗号化関数用の暗号フレームワーク ライブラリのソース

Note:

1. SAM E54はハードウェアAES暗号エンジンを備えています。wolfCryptライブラリはハードウェアによる暗号化とアクセラレーションをサポートしています。crypt_aes_u2238.h/cファイルには、AESハードウェアアクセラレーション用のインターフェイスとソース関数が含まれています。
2. AES用の暗号ライブラリとwolfSSLまたはwolfCryptライブラリはCrypto Library HelpとwolfCrypt Library Helpにあります。

3.2 AESの動作モード

NISTでは、基礎とする対称キーブロック暗号アルゴリズムと組み合わせて使う各種機密保持動作モードを推奨しています。動作モードとは、暗号の1ブロック演算を繰り返し適用して1ブロックを超えるデータを暗号化する方法を記述したアルゴリズムの事です。本書では以下のモードについて述べます。

- ECB(Electronic Code Book) モード
- CBC(暗号ブロックチェーン接続)モード
- CTR(カウンタ) モード
- GCM(ガロアカウンタ モード)

3.2.1 ECB(Electronic Code Book)

全モードの中で最もシンプルなモードです。このモードでは、入力は128ビットの別々のブロックに分割されます。

各ブロックは独立して暗号化または復号されます。ECB暗号化では、暗号化関数は各入力ブロックに直接適用され、暗号文が生成されます。ECB復号では、Inverse Cipher Function(逆転暗号関数)が各ブロックに適用され、平文に戻します。ECBモードを使う事は推奨されません。ECBモードは常に同じ平文を同じ暗号文に暗号化し、容易に侵入可能な攻撃ベクトルを提供するためです。

表3-3. ECB用のHarmony API

暗号化ライブラリAPI	CRYPT_AES_ECB_Encrypt
	CRYPT_AES_ECB_Decrypt
wolfcryptライブラリAPI	wc_AesEcbEncrypt
	wc_AesEcbDecrypt

Note: 暗号化関数CRYPT_AES_ECBと復号関数CRYPT_AES_ECBはこのプロジェクトのcrypto.h/cファイル内で自動的に生成されません。詳細は「確認事項」を参照してください。

3.2.2 CBC(暗号ブロックチェーン接続)モード

CBCモードでは、各平文ブロックは前の暗号文ブロックとXOR演算された上で暗号化されます。これにより、各暗号文ブロックはそれまでに処理された全ての平文ブロックに依存します。各メッセージを一意にするため、最初のブロックに初期化ベクタ(IV)を使う必要があります。IVは秘密ではありませんが、予測不可能である必要があります。復号の際は、入力された暗号文に逆暗号化を適用し、出力ブロックをIVとXOR演算する事で平文の最初のブロックを取得します。CBCモードと初期化ベクタの各種生成方法は「FIPS Pub 800-38A」に説明されています。

表3-4. CBC用のHarmony API

暗号化ライブラリAPI	CRYPT_AES_CBC_Encrypt
	CRYPT_AES_CBC_Decrypt
wolfcryptライブラリAPI	wc_AesCbcEncrypt
	wc_AesCbcDecrypt

3.2.3 CTR(カウンタ) モード

CTR(カウンタ) モードは、一連の入力ブロック (カウンタと呼ぶ)に対してForward Cipher Function(正暗号関数)を適用し、平文とXOR演算を行った一連の出力ブロックを生成して暗号文を生成する(またはその逆を実行する)機密保持モードです。カウンタモードはブロック暗号をストリーム暗号に変換します。シーケンス内の各ブロックはカウンタ シーケンス内の他のいずれのブロックとも異なります。全てのカウンタは一意でなければなりません。CTRモードでは、ユーザが初期カウンタを選択し、カウンタがオーバーフローするまで後続の全ての中間結果でインクリメントされます。CTR暗号化とCTR復号では、Forward Cipher Function(正暗号関数)を並列に実行できます。各種のカウンタ生成方法が「FIPS Pub 800-38A」のAppendix Bに説明されています。

表3-5. CTR用のHarmony API

暗号化ライブラリAPI	CRYPT_AES_CTR_Encrypt
wolfcryptライブラリAPI	wc_AesCtrEncrypt

3.2.4 GCM(ガロアカウンタ モード)

GCMはCTRモードのAESエンジンと、メッセージ認証タグを生成するためにバイナリガロア体で定義されたユニバーサル ハッシュ関数(GHASHエンジン)で構成されています。この処理はデータに真正性(整合性)と機密性を提供するために設計された認証暗号化アルゴリズムです。GHASHエンジンはAES演算後にデータパケットを処理します。GCMは暗号化のためのAESカウンタ動作モードにより、データの機密性を保証します。機密データの真正性はGHASHエンジンによって保証されます。

AES-GCMはストリーム状の暗号モードで、暗号文とメッセージ認証コード(認証タグとも呼ぶ)の2つの出力を生成します。暗号化と復号には、CTRモードのForward Cipher Function(正暗号関数)が使われます。プロトコルのバージョン、受信者情報等の機密でないデータを送信するためにAAD(追加認証データ)が使われます。AADは認証されますが、暗号化はされません。そのため、AADはAES-GCMの出力には含まれません。平文パケットヘッダの認証

に使えます。GCMには12バイトの初期化ベクタを使う事を推奨します。それ以上の大きさの初期化ベクタを使うと処理に時間がかかり、動作が遅くなるためです。GCMのセキュリティは認証タグのサイズに大きく依存します。タグのサイズが大きいほどセキュリティは向上します。セキュリティを確保するため、タグの長さは最大の16バイトにする事を推奨します。GCMモードの詳細は「NIST SP 800-38D」を参照してください。

表3-6. GCM用のHarmony API

アプリケーションAPI	`int aesgcm_default_test(void);`
	`static int aesgcm_default_test_helper(const uint8_t*, int, const uint8_t*, int, const uint8_t*, int, const uint8_t*, int ,const uint8_t*, int, const uint8_t*, int);`
暗号化ライブラリAPI	CRYPT_AES_GCM_SetKey
	CRYPT_AES_GCM_Encrypt
	CRYPT_AES_GCM_Decrypt
wolfcryptライブラリAPI	wc_AesGcmSetKey
	wc_AesGcmEncrypt
	wc_AesGcmDecrypt

ECB、CBC、CTRモードでの使用がサポートされているその他のAPI

表3-7. キーとIV用のAPI

アプリケーションAPI	`void aes_test(void)`
暗号化ライブラリAPI	CRYPT_AES_KeySet
	CRYPT_AES_IvSet

4. AESモードの暗号化/復号の例: アプリケーションの実装

4.1 前提条件

ハードウェアとソフトウェアに関する以下の前提条件を考慮する必要があります。

ハードウェア

- 1 x SAM E54 Xplained Pro評価用キット
- 1 x Micro USBケーブル

ソフトウェア

- MPLAB X IDE v5.30以上(最新版のMPLABXをダウンロード)
- MPLAB XC32/32++コンパイラv2.30以上(最新のXC32コンパイラをダウンロード)
- MPLAB Harmony v3 Configurator (v3.6.2)(MHCをインストール)
- MPLAB Harmony v3パッケージ:
  - MPLAB Harmony v3 bspリポジトリ、v3.7.0 (Github bsp)
  - MPLAB Harmony v3 cspリポジトリ、v3.7.0 (Github csp)
  - MPLAB Harmony v3 coreリポジトリ、v3.7.0 (Github core)
  - MPLAB Harmony v3 dev-packsリポジトリ、v3.8.0 (Github dev-packs)
  - MPLAB Harmony v3 Cryptoリポジトリ、v3.6.0 (Github Crypto Repo)
  - MPLAB Harmony v3 wolfSSLリポジトリ、v4.5.0 (Github wolfSSL)
- ターミナル アプリケーション(Tera Term)

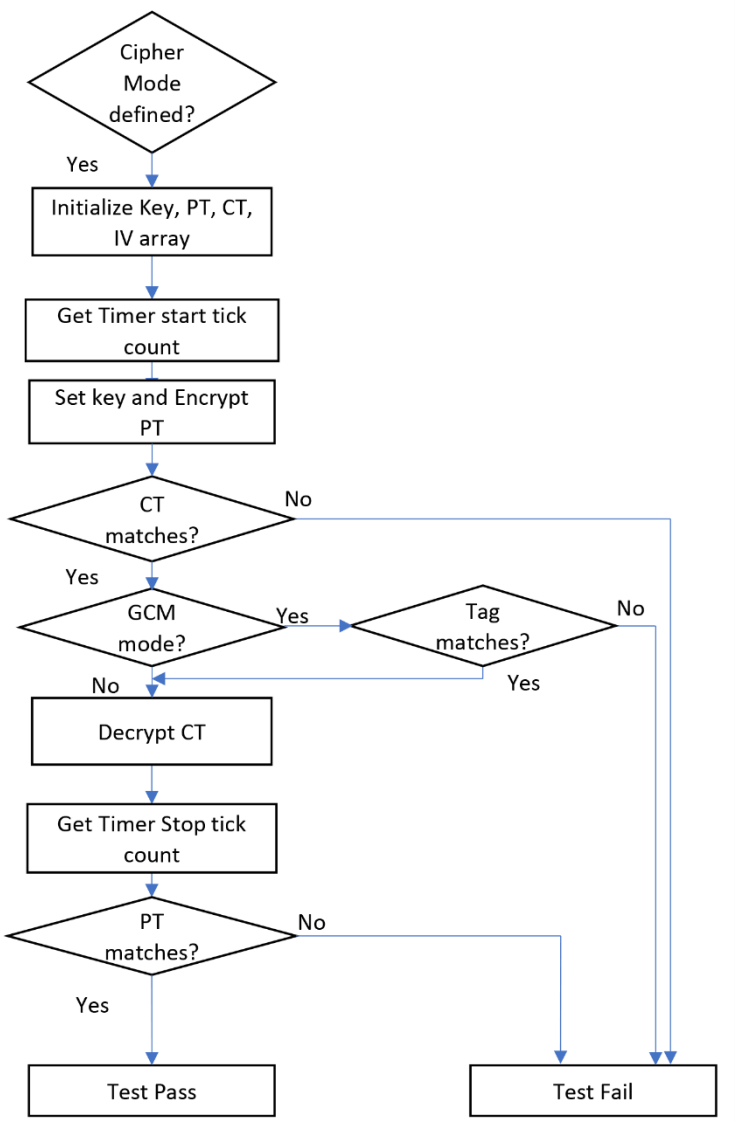
4.2 アプリケーションの概要

このアプリケーション例では、ECB、CBC、CTR、GCM等の様々なブロック暗号動作モードの基礎となる対称ブロック暗号関数としてAESを使います。AESは128ビット、192ビット、256ビットの3つの鍵長をサポートしています。このアプリケーションは全モードで128ビットの鍵長を使います。全てのモードにおいて、暗号化されたPT(平文)はCT(暗号文)と商号され、復号されたCT(暗号文)はPT(平文)と照合されます。チェックで成功が返されるとテストは合格です。

GCMモードでは、真正性と機密性の検証が必要です。そのため、機密データと非機密のAAD(追加認証データ)を復号する前に、暗号化後に生成された認証タグが検証されます。

各暗号モードでキーの設定、暗号化、復号の処理にかかるシステムクロック サイクル数を計算するために、MPLAB Harmony v3 Time system serviceが有効化されます。

図4-1. アプリケーションのフローチャート



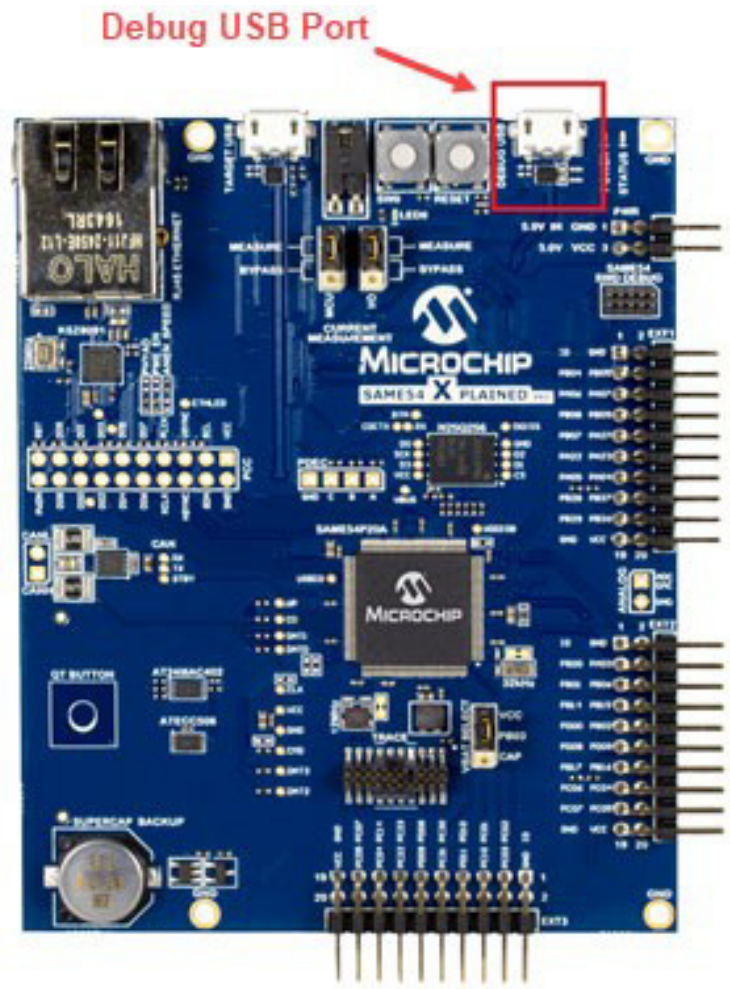
4.3 デモ アプリケーションの実行

SAM E54用のデモ アプリケーションはH3 Cryptoリポジトリの /crypto_apps_encrypt_decrypt/apps/encrypt_decrypt/firmware/sam_e54_xplained_pro.Xにあります。

以下の手順に従ってデモ アプリケーションをプログラムします。

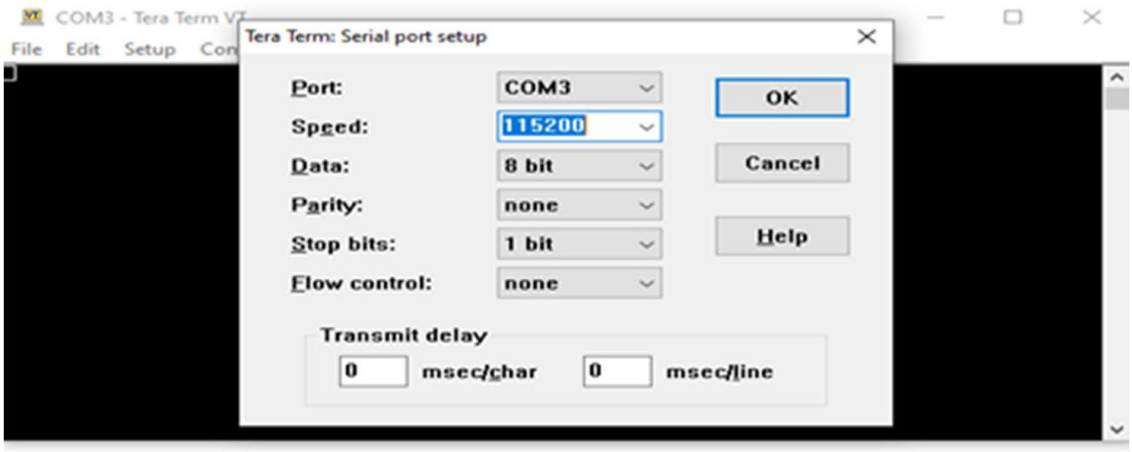
1. micro-USBケーブルをSAM E54 Xplained ProボードのDEBUG USBコネクタに接続し、ボードの電源を入れます。

図4-2. SAM E54 XproのDEBUG USBとの接続



2. ターミナル アプリケーション(Tera Term)を起動し、baudレートを115200に設定します。

図4-3. TeraTermでbaudレートを設定

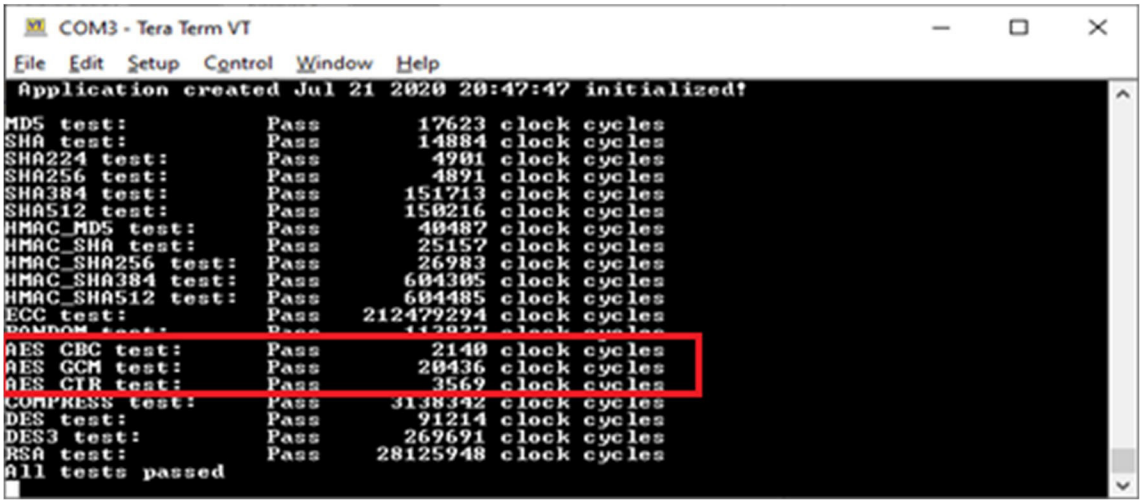


3. MPLAB X IDEでプロジェクトを開きます。

4. [File] > [Open Project]を選択し、H3 Cryptoリポジトリから以下の場所を選択します。`(\crypto_apps_encrypt_decrypt\apps\encrypt_decrypt\firmware\sam_e54_xplained_pro.X)`.

5. プロジェクトをターゲットボードにビルドしプログラムするには、  アイコン([Make and Program Device]アイコン)をクリックします。COM3 - Tera Termウィンドウに暗号化方式と圧縮テストの結果が表示されます。

図4-4. 出力ウィンドウ



Note:

1. 出力ウィンドウには、全ての暗号化方式と圧縮テストの結果が表示されます。AES CBC、AES GCM、AES CTRは、CBC、GCM、CTRモードのブロック暗号演算の結果を示しています。
2. デモにECBモードを含めるには、「確認事項」を参照してください。

4.4 アプリケーションの作成

32ビットデバイスの周辺モジュールとコアの設定はGUIを使う事で大幅に簡素化できるため、本アプリケーションはMPLAB Harmony v3 Configurator (MHC)で作成されています。MHCは使い勝手の良いツールで、特定の周辺モジュール ドライバを設定できるため、アプリケーションの開発が容易になります。MHCの詳細は「GitHub wikiページ」を参照してください。

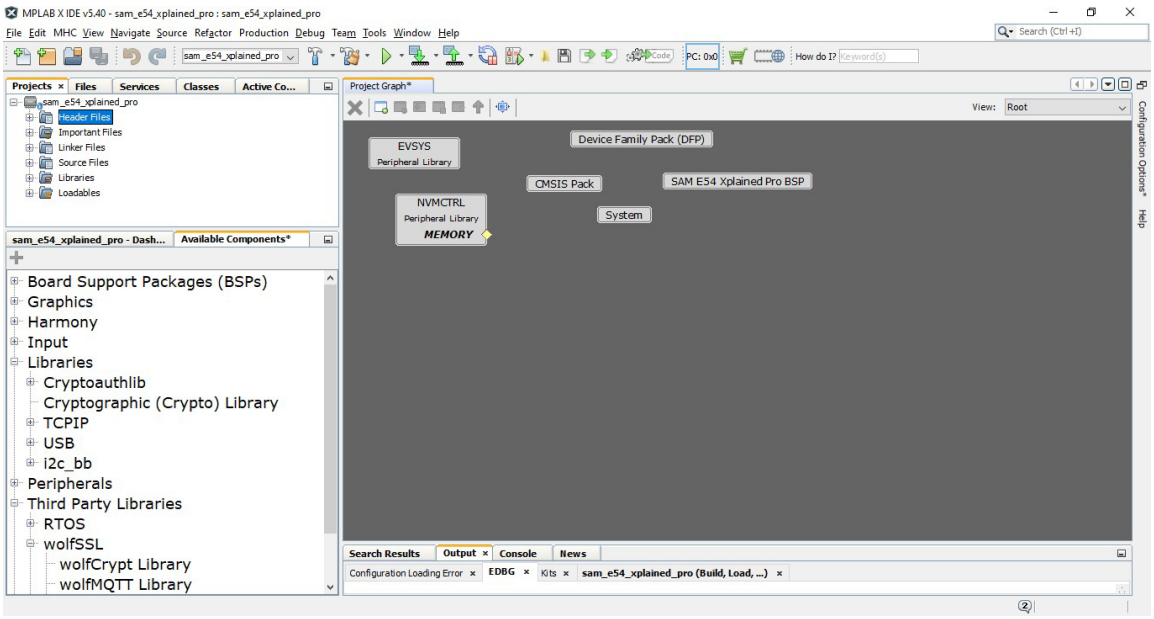
ユーザは、以下のセクションに記載されている手順に従ってAESアプリケーションを作成できます。ここでは、これまでのセクションで説明したMPLAB Harmony v3 AESデモ アプリケーションを参考として使います。

MPLAB Harmony v3の設定

以下の手順を行う前に、最新バージョンのMPLABX IDEとMPLAB Harmony v3プラグインがインストールされている事を確認してください。

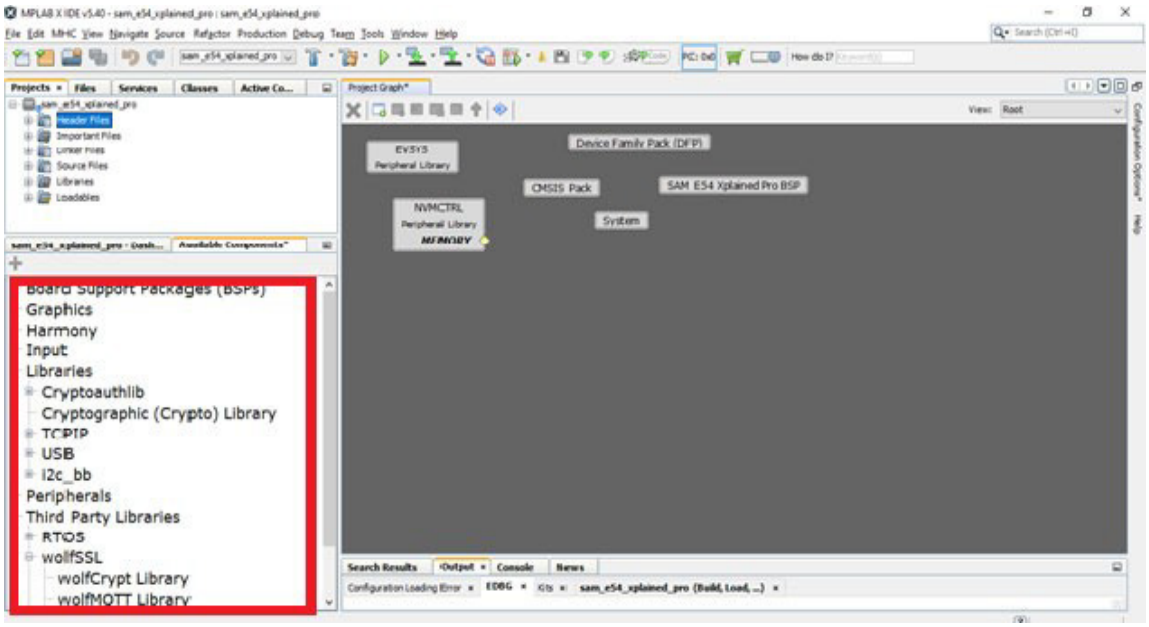
1. MPLAB X IDEを使ってSAME54P20A向けのMPLAB Harmony v3プロジェクトを作成するには、「Create Harmony v3 project」を参照してください。
2. コンフィグレータの起動時、既定ではDFP(デバイスファミリ パック)、システム、CMSISパック、SAM E54 Xpro BSPが存在しています。

図4-5. MHCの既定値モジュール



3. このデモ アプリケーションのプロジェクト グラフに暗号化ライブラリ、wolfCryptライブラリ、USART周辺モジュール ドライバ、タイムシステム サービスを追加します。関連するライブラリと周辺モジュールを追加するには、MPLAB X IDEの左下にある**[Available Components]**タブをクリックします。

図4-6. Available Components



4. 暗号ライブラリはwolfCryptライブラリに依存しています。
[Libraries] > [Cryptographic (Crypto) Library]

[Third Party Libraries] > [wolfSSL - wolfCrypt Library]

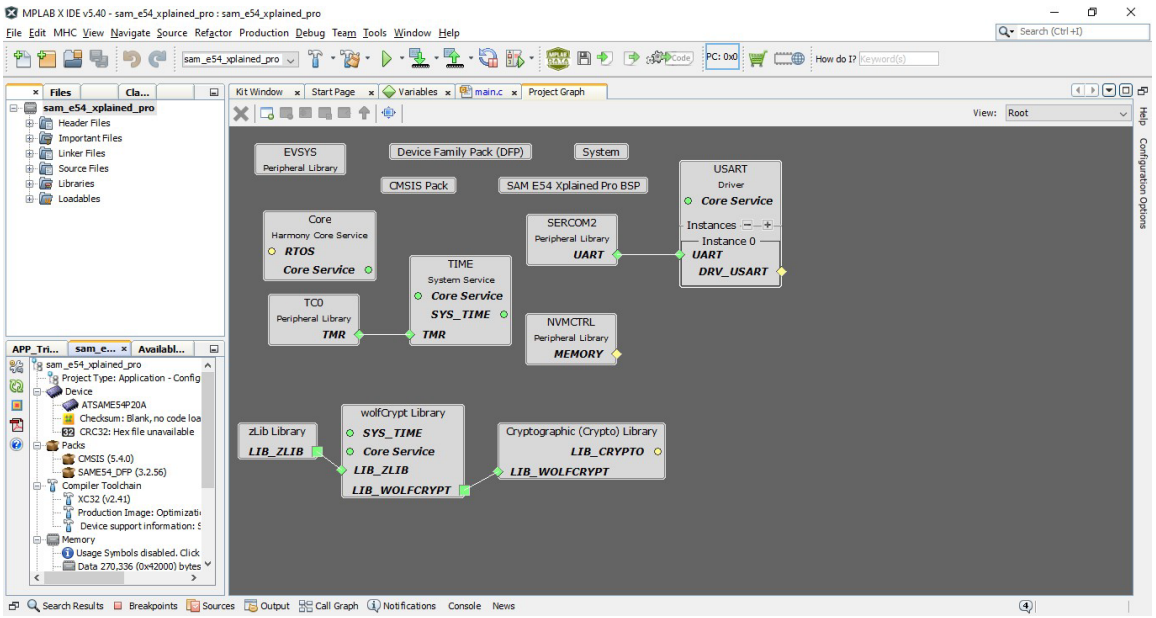
図4-7. Harmony v3とwolfCryptライブラリ

5. USART Harmonyドライバは SERCOM2インスタンスに依存しています。
   [Harmony] > [Drivers] > [USART]

   [Peripherals] > [SERCOM] > [SERCOM2]
6. TC0インスタンスはタイムシステム サービスで使われます。
   [Harmony] > [System services] > [Time]

   [Peripherals] > [Timer] > [TC0]
7. これらのコンポーネントを設定済みのHarmony設定ファイル(`.xml`)がH3 Cryptoリポジトリの以下のパスにあります。
   `\crypto_apps_encrypt_decrypt\apps\encrypt_decrypt\firmware\src\config\sam_e54_xpl ained_pro`.
   このファイルを読み込むには、MPLAB Harmony v3 Configuratorから[MHC] > [File] > [Load State]を選択します。
8. このデモ アプリケーションのプロジェクト グラフを以下の図に示します。

   図4-8. アプリケーションのプロジェクト グラフ

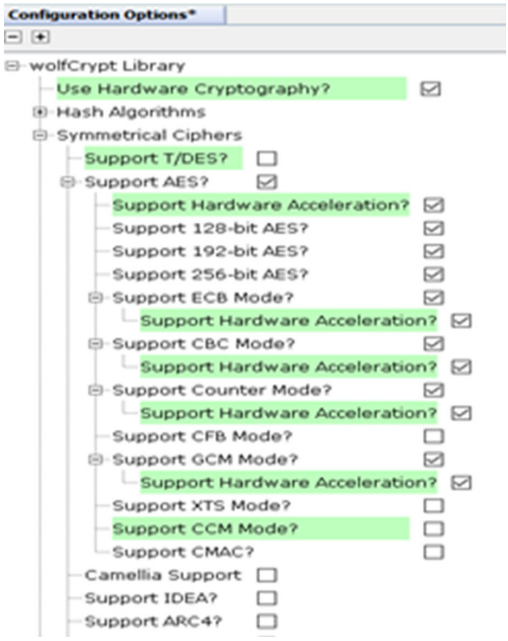


9. 本書は暗号化機能を中心に説明しているため、以下の図を参照してAES用wolfCryptライブラリを設定できます。

Note:

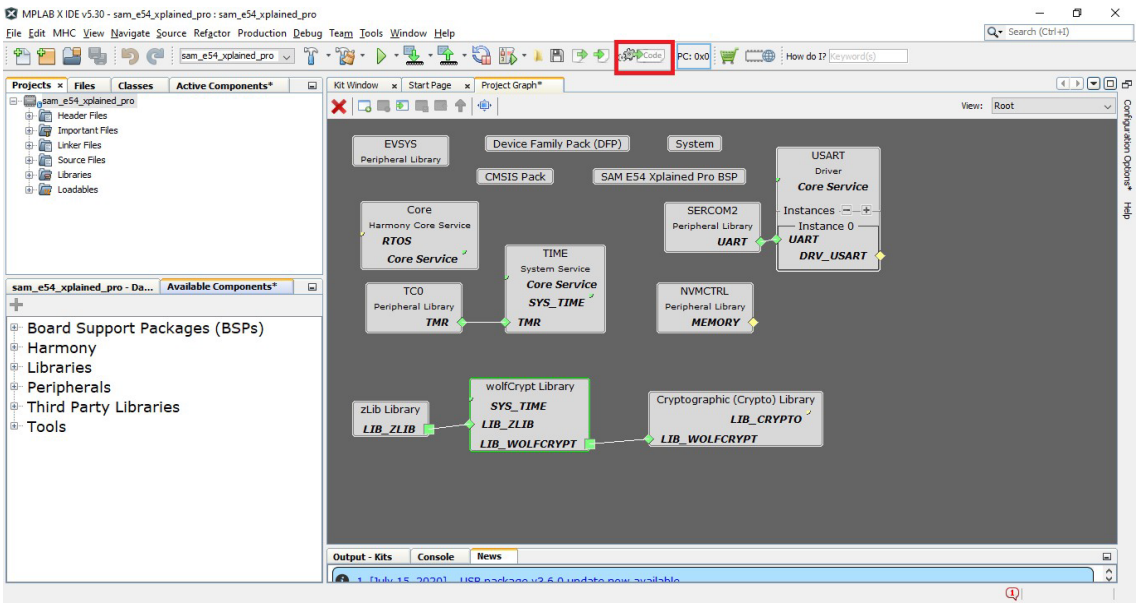
1. デモ アプリケーション(`encrypt_decrypt`)はハッシング、非対称暗号、乱数生成等、多くの暗号機能を備えており、圧縮が有効になっています。本書はAESのみを対象とするため、他の機能については説明しません。
2. zLibライブラリには、例の他のアルゴリズムで使われるデータエンコード、デコード、圧縮をサポートするAPIが含まれています。ただし、zLibライブラリはAESの動作に必須ではないため、本書では説明しません。

図4-9. wolfCryptライブラリの設定オプション



10. 設定を変更した場合、  [Generate Code]ボタン) をクリックする事で対応するコードを生成できます。

図4-10. Generate Code



5. 補遺

5.1 補遺A: AES暗号モードのベクタの例

本書で説明した各種モードで使ったテストベクタの例を以下に示します。その他のベクタはNIST Publicationにあります。NISTのテストベクタはNIST Block VectorsとNIST GCM Vectorsからダウンロードできます。

ECB AES 128

キー 2b7e151628aed2a6abf7158809cf4f3c

ブロック#1

平文 6bc1bee22e409f96e93d7e117393172a

暗号文 3ad77bb40d7a3660a89ecaf32466ef97

ブロック#2

平文 ae2d8a571e03ac9c9eb76fac45af8e51

暗号文 f5d3d58503b9699de785895a96fdbaaf

ブロック#3

平文 30c81c46a35ce411e5fbc1191a0a52ef

暗号文 43b1cd7f598ece23881b00e3ed030688

ブロック#4

平文 f69f2445df4f9b17ad2b417be66c3710

暗号文 7b0c785e27e8ad3f8223207104725dd4

CBC AES 128

ブロック#1

キー 2b7e151628aed2a6abf7158809cf4f3c

IV 000102030405060708090a0b0c0d0e0f

平文 6bc1bee22e409f96e93d7e117393172a

暗号文 7649abac8119b246cee98e9b12e9197d

ブロック#2

キー 00000000000000000000000000000000

IV 00000000000000000000000000000000

平文 f34481ec3cc627bacd5dc3fb08f273e6

暗号文 0336763e966d92595a567cc9ce537f5e

CTR 128 AES

キー 2b7e151628aed2a6abf7158809cf4f3c

初期化カウンタ f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff

ブロック#1

平文 6bc1bee22e409f96e93d7e117393172a

暗号文 874d6191b620e3261bef6864990db6ce

ブロック#2

平文 ae2d8a571e03ac9c9eb76fac45af8e51

暗号文 9806f66b7970fdff8617187bb9fffdff

ブロック#3

平文 30c81c46a35ce411e5fbc1191a0a52ef

暗号文 5ae4df3edbd5d35e5b4f09020db03eab

ブロック#4

平文 f69f2445df4f9b17ad2b417be66c3710

暗号文 1e031dda2fbe03d1792170a0f3009cee

GCM 128

ブロック#1

キー 298efa1ccf29cf62ae6824bfc19557fc

IV 6f58a93fe1d207fae4ed2f6d

PT cc38bccd6bc536ad919b1395f5d63801f99f8068d65ca5ac63872daf16b93901

AAD 021fafd238463973ffe80256e5b1c6b1

CT dfce4e9cd291103d7fe4e63351d9e79d3dfd391e3267104658212da96521b7db

タグ 542465ef599316f73a7a560509a2d9f2

ブロック#2

[AAD = 0]

キー 016dbb38daa76dfe7da384ebf1240364

IV 0793ef3ada782f78c98affe3

PT 4b34a9ec5763524b191d5616c547f6b7

CT 609aa3f4541bc0fe9931daad2ee15d0c

タグ 33afec59c45baf689a5e1b13ae423619

ブロック#3

[平文、AAD長 = 0]

キー b01e45cc3088aaba9fa43d81d481823f

IV 5a2c4a66468713456a4bd5e1

タグ 014280f944f53c681164b2ff

5.2 補遺B: 確認事項

暗号ライブラリ バージョン3.6.0とwolfCryptライブラリ4.5.0を使う場合、AESアプリケーションで作業する前に以下の確認が必要です。

- (encrypt_decrypt\firmware\src\config\default\peripheral\clock\plib_clock.c) の `CLOCK_Initialize()` 関数に、AES用のAPBCブリッジ マスキングが設定されている事を確認します。設定されていない場合、以下の行を末尾に追加します。

  ```
  /* Configure the APBC Bridge Clocks */
   MCLK_REGS->MCLK_APBCMASK = 0x2e00;
  ```

  AES用APBクロックのマスクを解除しないと、AESレジスタに書き込んでクロックが利用可能かどうかを確認する事ができません。
- H3の例にはECB機能は実装されていません。ECBテストを含めるには、プロジェクトに以下の追加の修正を行う必要があります。

1. ECBハードウェア アクセラレーションが有効化されている事を確認します。確認したら、コードを生成します。
2. app.hファイルのAPP_DATA構造内で以下の変数を宣言します。
   - \crypto_apps_encrypt_decrypt\apps\encrypt_decrypt\firmware\src\app.h

```
int aes_ecb_test_result;
uint32_t aes_ecb_timing;
```

3. ECB APIのCRYPT_AES_ECB_EncryptとCRYPT_AES_ECB_Decryptは、暗号ライブラリ バージョン3.6.0で生成されるcrypto.h/cに宣言も定義もされていません。ユーザが対応するファイルに含める必要があります。wolfCryptライブラリのファイルに変更を加える必要はありません。
   crypto.cファイルに以下のコードを追加します。

```
../src/config/sam_e54_xpalined_pro/crypto/src/crypto.c

#ifdef HAVE_AES_ECB
int CRYPT_AES_ECB_Encrypt(CRYPT_AES_CTX* aes, unsigned char* out,
                          const unsigned char* in, unsigned int inSz)
{
    if (aes == NULL || out == NULL || in == NULL)
        return BAD_FUNC_ARG;

    return wc_AesEcbEncrypt((Aes*)aes, out, in, inSz);
}



/* AES ECB Decrypt */
int CRYPT_AES_ECB_Decrypt(CRYPT_AES_CTX* aes, unsigned char* out,
                          const unsigned char* in, unsigned int inSz)
{
    if (aes == NULL || out == NULL || in == NULL)
        return BAD_FUNC_ARG;

    return wc_AesEcbDecrypt((Aes*)aes, out, in, inSz);
}
#endif /* HAVE_AES_ECB */
```

4. 以下で**太字**で示すコードをapp.cファイルの関数aes_test(void)内に追加します。

```
void aes_test(void)
{
    CRYPT_AES_CTX enc;
    CRYPT_AES_CTX dec;

    int AES_KEYSIZE = 0;
    #ifdef HAVE_AES_ECB


/* Input Message of 128 bit length*/
      const uint8_t msgecb[] = {
      0x6b, 0xc1, 0xbe, 0xe2, 0x2e, 0x40, 0x9f, 0x96,
      0xe9, 0x3d, 0x7e, 0x11, 0x73, 0x93, 0x17, 0x2a
    };
    /*Ciphertext of 128 bit length*/
    const uint8_t verifyecb[] =
    {
      0x3a, 0xd7, 0x7b, 0xb4, 0x0d, 0x7a, 0x36, 0x60,
      0xa8, 0x9e, 0xca, 0xf3, 0x24, 0x66, 0xef, 0x97
    };
    /* AES - ECB 128 bit key*/
    uint8_t keyecb[] = {0x2b, 0x7e, 0x15, 0x16, 0x28, 0xae, 0xd2, 0xa6,
                        0xab, 0xf7,0x15, 0x88, 0x09, 0xcf, 0x4f, 0x3c};
    /* I.V is not required in ECB mode*/
    uint8_t ivecb[] = {0}; /* align */
    /* arrays to store encryption and decryption results respectively*/
    uint8_t cipherecb[AES_BLOCK_SIZE * 4] = {0};
```

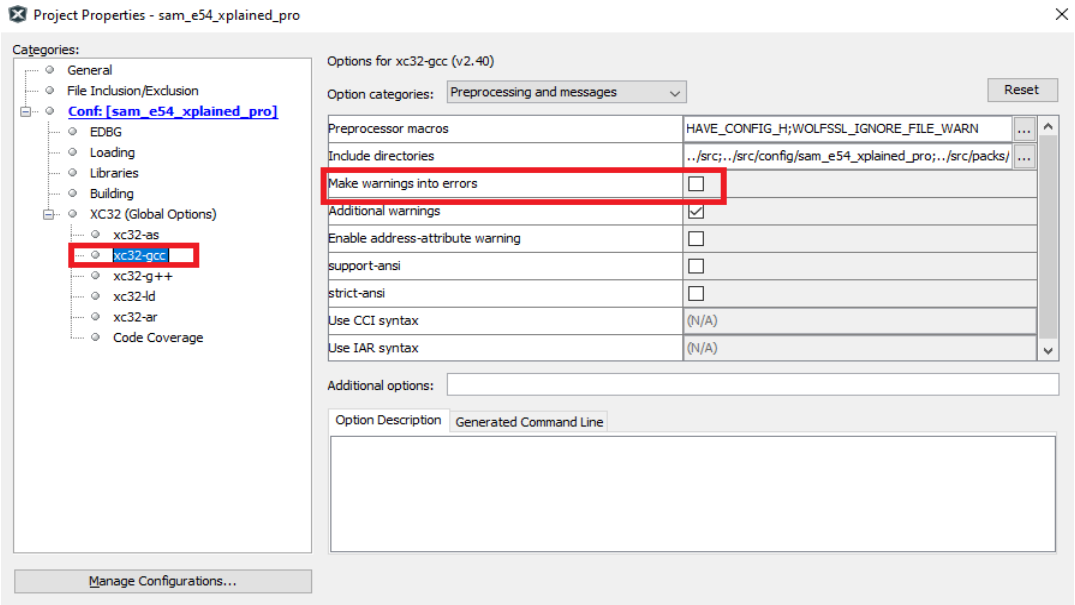
```
    uint8_t plainecb [AES_BLOCK_SIZE * 4] = {0};
    /* Test Pass count*/
    int numEcbSubTests = 2;
    uint32_t hashEcbStart;
    uint32_t hashEcbStop;
    AES_KEYSIZE = sizeof(keyecb);
    hashEcbStart = APP_getTicks();
    /* The above const allocates in RAM, but does not flush out of cache.
Copy
       it back out so it is in physical memory. */
   #if defined(HW_CRYPTO)
    SYS_DEVCON_DataCacheFlush();
#endif
    CRYPT_AES_KeySet(&enc, keyecb, AES_KEYSIZE, ivecb, AES_ENCRYPTION);
    CRYPT_AES_KeySet(&dec, keyecb, AES_KEYSIZE, ivecb, AES_DECRYPTION);
    CRYPT_AES_ECB_Encrypt(&enc, cipherecb, msgecb,   AES_BLOCK_SIZE);
    CRYPT_AES_ECB_Decrypt(&dec, plainecb, verifyecb, AES_BLOCK_SIZE);

    appData.aes_ecb_test_result = numEcbSubTests;

    if (!(memcmp(plainecb, msgecb, AES_BLOCK_SIZE)))
        appData.aes_ecb_test_result--;
    if (!(memcmp(cipherecb, verifyecb, AES_BLOCK_SIZE)))
        appData.aes_ecb_test_result--;
    hashEcbStop = APP_getTicks();
    appData.aes_ecb_timing = hashEcbStop - hashEcbStart;
#endif /* HAVE_AES_ECB */
```

5. ECBテスト結果を出力するには、以下のコードを`app.c`ファイルに含めます。

```
#ifdef HAVE_AES_ECB
sprintf(printBuffer, "%s\n\rAES ECB test:
%s",printBuffer,
(appData.aes_ecb_test_result==expectedResult?"Pass":"FAIL"));
sprintf(printBuffer, "%s\t
%10d clock cycles", printBuffer, (int) appData.aes_ecb_timing);
#endif
```

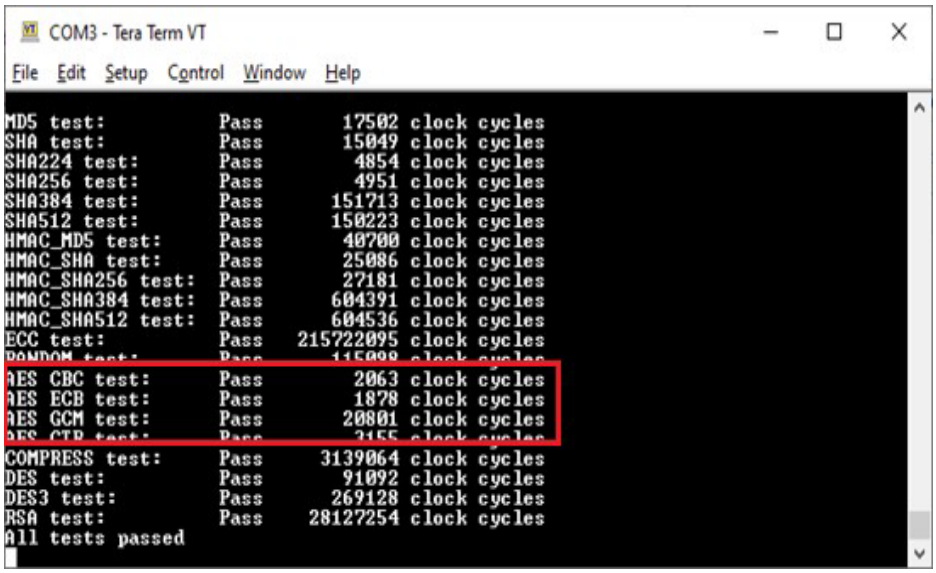
6. プロジェクトに対してこれらの変更を行った後、[Project Properties]ウィンドウの[Categories]セクションで[xc32-gcc]を選択します。
7. [Preprocessing and messages]カテゴリの**[Make warnings into error]**チェックボックスをクリアします。

図5-1. [Project Properties]ウィンドウ



8. 「4.3 デモ」に示す手順に従います。出力ウィンドウに、下図のようにECBテストの詳細が表示されます。

図5-2. ECB結果を示す出力ウィンドウ



6. 参考情報

1. NIST Special Publication 800-38A 2001 Edition - Recommendation for Block Cipher Modes of Operation: nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
2. NIST Special Publication 800-38D November, 2007 - Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC: nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf
3. How to Build an Application by Adding a New PLIB, Driver, or Middleware to an Existing MPLAB Harmony v3 Project: ww1.microchip.com/downloads/en/DeviceDoc/How_to_Build_Application_Adding_PLIB_%20Driver_or_Middleware%20_to_MPLAB_Harmony_v3Project_DS90003253A.pdf
4. MPLAB Harmony v3 Installation and Usage: github.com/Microchip-MPLAB-Harmony/mhc/wiki
5. MPLAB Harmony v3 Crypto Library: github.com/Microchip-MPLAB-Harmony/crypto/wiki
6. SAM E54 Xplained Pro: www.microchip.com/developmenttools/ProductDetails/atsame54-xpro
7. MPLAB® Harmony v3でSAME54のプロジェクトを作成する方法: www.youtube.com/watch?v=KTEajJQ4ukcmicrochip.wikidot.com/harmony3:same54-getting-started-training-module
8. MPLAB Harmony v3のホームページ: www.microchip.com/en-us/development-tools-tools-and-software/embedded-software-center/mplab-harmony-v3

Microchip社ウェブサイト

Microchip社はウェブサイト(www.microchip.com)を通してオンライン サポートを提供しています。当ウェブサイトでは、お客様に役立つ情報やファイルを提供しています。以下を含む各種の情報をご覧になれます。

- **製品サポート** - データシートとエラッタ、アプリケーション ノートとサンプル プログラム、設計リソース、ユーザガイドとハードウェア サポート文書、最新のソフトウェアと過去のソフトウェア
- **技術サポート** - FAQ(よく寄せられる質問)、技術サポートのご依頼、オンライン ディスカッション グループ、Microchip社のデザイン パートナー プログラムおよびメンバーリスト
- **ご注文とお問い合わせ** - 製品セレクタと注文ガイド、最新プレスリリース、セミナー/イベントの一覧、お問い合わせ先(営業所/正規代理店)の一覧

製品変更通知サービス

Microchip社の製品変更通知サービスは、お客様にMicrochip社製品の最新情報をお届けする配信サービスです。ご興味のある製品ファミリまたは開発ツールに関する変更、更新、リビジョン、エラッタ情報をいち早くメールにてお知らせします。

http://www.microchip.com/pcnにアクセスし、登録手続きをしてください。

お客様サポート

Microchip社製品をお使いのお客様は、以下のチャンネルからサポートをご利用頂けます。

- 正規代理店
- 技術サポート

サポートは正規代理店にお問い合わせください。本書の最後のページに各国の営業所の一覧を記載しています。

技術サポートは以下のウェブページからもご利用頂けます。www.microchip.com/support

Microchip社のデバイスコード保護機能

Microchip 社製品のコード保護機能について以下の点にご注意ください。

- Microchip社製品は、該当するMicrochip 社データシートに記載の仕様を満たしています。
- Microchip社では、通常の条件ならびに動作仕様書の仕様に従って使った場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- Microchip社はその知的財産権を重視し、積極的に保護しています。Microchip 社製品のコード保護機能の侵害は固く禁じられており、デジタル ミレニアム著作権法に違反します。
- Microchip社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。コード保護機能は常に進化しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。

法律上の注意点

本書および本書に記載されている情報は、Microchip 社製品を設計、テスト、お客様のアプリケーションと統合する目的を含め、Microchip 社製品に対してのみ使う事ができます。それ以外の方法でこの情報を使う事はこれらの条項に違反します。デバイス アプリケーションの情報は、ユーザの便宜のためにのみ提供されるものであり、更新

によって変更となる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。その他のサポートはMicrochip 社正規代理店にお問い合わせ頂くか、https://www.microchip.com/en-us/support/design-help/client-support-servicesをご覧ください。

Microchip 社は本書の情報を「現状のまま」で提供しています。Microchip 社は明示的、暗黙的、書面、口頭、法定のいずれであるかを問わず、本書に記載されている情報に関して、非侵害性、商品性、特定目的への適合性の暗黙的保証、または状態、品質、性能に関する保証をはじめとするいかなる類の表明も保証も行いません。

いかなる場合もMicrochip 社は、本情報またはその使用に関連する間接的、特殊的、懲罰的、偶発的または必然的損失、損害、費用、経費のいかんにかかわらず、またMicrochip 社がそのような損害が生じる可能性について報告を受けていた場合あるいは損害が予測可能であった場合でも、一切の責任を負いません。法律で認められる最大限の範囲を適用しようとも、本情報またはその使用に関連する一切の申し立てに対するMicrochip 社の責任限度額は、使用者が当該情報に関連してMicrochip 社に直接支払った額を超えません。

Microchip 社の明示的な書面による承認なしに、生命維持装置あるいは生命安全用途にMicrochip社の製品を使う事は全て購入者のリスクとし、また購入者はこれによって発生したあらゆる損害、クレーム、訴訟、費用に関して、Microchip 社は擁護され、免責され、損害をうけない事に同意するものとします。特に明記しない場合、暗黙的あるいは明示的を問わず、Microchip社が知的財産権を保有しているライセンスは一切譲渡されません。

商標

Microchip 社の名称とロゴ、Microchip ロゴ、Adaptec、AVR、AVRロゴ、AVR Freaks、BesTime、BitCloud、CryptoMemory、CryptoRF、dsPIC、flexPWR、HELDO、IGLOO、JukeBlox、KeeLoq、Kleer、LANCheck、LinkMD、maXStylus、maXTouch、MediaLB、megaAVR、Microsemi、Microsemi ロゴ、MOST、MOST ロゴ、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 ロゴ、PolarFire、Prochip Designer、QTouch、SAM-BA、SenGenuity、SpyNIC、SST、SST ロゴ、SuperFlash、Symmetricom、SyncServer、Tachyon、TimeSource、tinyAVR、UNI/O、Vectron、XMEGA は米国とその他の国におけるMicrochip Technology Incorporated の登録商標です。

AgileSwitch、APT、ClockWorks、The Embedded Control SolutionsCompany、EtherSynch、Flashtec、Hyper Speed Control、HyperLightLoad、Libero、motorBench、mTouch、Powermite 3、Precision Edge、ProASIC、ProASIC Plus、ProASIC Plus ロゴ、Quiet-Wire、SmartFusion、SyncWorld、Temux、TimeCesium、TimeHub、TimePictra、TimeProvider、TrueTime、ZL は米国におけるMicrochip Technology Incorporated の登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、Augmented Switching、BlueSky、BodyCom、Clockstudio、CodeGuard、CryptoAuthentication、CryptoAutomotive、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、Espresso T1S、EtherGREEN、GridTime、IdealBridge、In-Circuit Serial Programming、ICSP、INICnet、Intelligent Paralleling、IntelliMOS、Inter-Chip Connectivity、JitterBlocker、Knob-on-Display、KoD、maxCrypto、maxView、memBrain、Mindi、MiWi、MPASM、MPF、MPLAB Certified ロゴ、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PowerSmart、PureSilicon、QMatrix、REAL ICE、RippleBlocker、RTAX、RTG4、SAM-ICE、Serial Quad I/O、simpleMAP、SimpliPHY、SmartBuffer、SmartHLS、SMART-I.S.、storClad、SQI、SuperSwitcher、SuperSwitcher II、Switchtec、SynchroPHY、TotalEndurance、Trusted Time、TSHARC、USBCheck、VariSense、VectorBlox、VeriPHY、ViewSpan、WiperLock、XpressConnect、ZENAは米国とその他の国におけるMicrochip Technology Incorporated の商標です。

SQTP は米国におけるMicrochip Technology Incorporated のサービスマークです。

Adaptec ロゴ、Frequency on Demand、Silicon Storage Technology、Symmcom はその他の国におけるMicrochip Technology Incorporatedの登録商標です。

GestIC は、その他の国におけるMicrochip Technology Germany II GmbH & Co. KG (Microchip Technology Incorporated の子会社) の登録商標です。

その他の商標は各社に帰属します。

ISBN: 978-1-6683-1969-7

品質管理システム

Microchip社の品質管理システムについてはwww.microchip.com/qualityをご覧ください。

各国の営業所とサービス

南北アメリカ	アジア/太平洋	アジア/太平洋	欧州
本社 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 技術サポート: http://www.microchip.com/support URL: www.microchip.com **アトランタ** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **オースティン、TX** Tel: 512-257-3370 **ボストン** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **シカゴ** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **ダラス** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **デトロイト** Novi, MI Tel: 248-848-4000 **ヒューストン、TX** Tel: 281-894-5983 **インディアナポリス** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **ロサンゼルス** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **ローリー、NC** Tel: 919-844-7510 **ニューヨーク、NY** Tel: 631-435-6000 **サンノゼ、CA** Tel: 408-735-9110 Tel: 408-436-4270 **カナダ - トロント** Tel: 905-695-1980 Fax: 905-695-2078	**オーストラリア - シドニー** Tel: 61-2-9868-6733 **中国 - 北京** Tel: 86-10 -8569-7000 **中国 - 成都** Tel: 86-28-8665-5511 **中国 - 重慶** Tel: 86-23-8980-9588 **中国 - 東莞** Tel: 86-769-8702-9880 **中国 - 広州** Tel: 86-20-8755-8029 **中国 - 杭州** Tel: 86-571-8792-8115 **中国 - 香港SAR** Tel: 852-2943-5100 **中国 - 南京** Tel: 86-25-8473-2460 **中国 - 青島** Tel: 86-532-8502-7355 **中国 - 上海** Tel: 86-21-3326-8000 **中国 - 瀋陽** Tel: 86-24-2334-2829 **中国 - 深圳** Tel: 86-755-8864-2200 **中国 - 蘇州** Tel: 86-186-6233-1526 **中国 - 武漢** Tel: 86-27-5980-5300 **中国 - 西安** Tel: 86-29-8833-7252 **中国 - 厦門** Tel: 86-592-2388138 **中国 - 珠海** Tel: 86-756-3210040	**インド - バンガロール** Tel: 91-80-3090-4444 **インド - ニューデリー** Tel: 91-11-4160-8631 **インド - プネ** Tel: 91-20-4121-0141 **日本 - 大阪** Tel: 81-6-6152-7160 **日本 - 東京** Tel: 81-3-6880-3770 **韓国 - 大邱** Tel: 82-53-744-4301 **韓国 - ソウル** Tel: 82-2-554-7200 **マレーシア - クアラルンプール** Tel: 60-3-7651-7906 **マレーシア - ペナン** Tel: 60-4-227-8870 **フィリピン - マニラ** Tel: 63-2-634-9065 **シンガポール** Tel: 65-6334-8870 **台湾 - 新竹** Tel: 886-3-577-8366 **台湾 - 高雄** Tel: 886-7-213-7830 **台湾 - 台北** Tel: 886-2-2508-8600 **タイ - バンコク** Tel: 66-2-694-1351 **ベトナム - ホーチミン** Tel: 84-28-5448-2100	**オーストリア - ヴェルス** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **デンマーク - コペンハーゲン** Tel: 45-4485-5910 Fax: 45-4485-2829 **フィンランド - エスポー** Tel: 358-9-4520-820 **フランス - パリ** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **ドイツ - ガーヒンク** Tel: 49-8931-9700 **ドイツ - ハーン** Tel: 49-2129-3766400 **ドイツ - ハイルブロン** Tel: 49-7131-72400 **ドイツ - カールスルーエ** Tel: 49-721-625370 **ドイツ - ミュンヘン** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **ドイツ - ローゼンハイム** Tel: 49-8031-354-560 **イスラエル - ラーナナ** Tel: 972-9-744-7705 **イタリア - ミラノ** Tel: 39-0331-742611 Fax: 39-0331-466781 **イタリア - パドヴァ** Tel: 39-049-7625286 **オランダ - ドリューネン** Tel: 31-416-690399 Fax: 31-416-690340 **ノルウェー - トロンハイム** Tel: 47-7288-4388 **ポーランド - ワルシャワ** Tel: 48-22-3325737 **ルーマニア - ブカレスト** Tel: 40-21-407-87-50 **スペイン - マドリッド** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **スウェーデン - ヨーテボリ** Tel: 46-31-704-60-40 **スウェーデン - ストックホルム** Tel: 46-8-5090-4654 **イギリス - ウォーキンガム** Tel: 44-118-921-5800 Fax: 44-118-921-5820