AVR1318 : XMEGA 組み込みAES加速器の使い方

要点

- AES(FIPS公布197,2002)完全適合
  - 暗号化と解読の両手順
- 128ビット鍵と状態配列メモリ
- 暗号塊符号化に有用な状態配列メモリへのXOR格納任意選択
- 状態配列と鍵のメモリへの順次アクセス
- AES完了でのDMA要求と割り込みの任意選択

1. 序説

XMEGA®のAES暗号部署は新暗号規格(AES)を支援し、その暗号化と解読を実行することができます。この部署は128ビット長の鍵を支援します。128ビットの鍵塊と128ビットのデータ塊(平文と暗号文)はAES暗号部署内の鍵と状態配列のメモリに格納されなければなりません。AESは鍵と状態配列のメモリが格納され、動作種別が選択された後、1つの暗号化/解読を実行するのに375クロック周期を費やします。

本応用記述は素早い準備と行動のための例と共にXMEGAのAES機能の基本的な機能を記述します。その上、Cで書かれたドライバ インターフェースが含まれています。

直接メモリ入出力(DMA)やXMEGA事象システムのような高度な使い方は本応用記述の範囲外です。これらの詳細についてはデバイスのデータシートと他の関連する応用記述を参照してください。

2. 理屈

暗号は秘密情報を保つ芸術または科学であり、暗号の手段を隠すか、または暗号鍵を保全することに基づいています。使用した手段の安全性に基くだけの方法は主に歴史的興味で、現実世界の要求に合致しません。現代の方法は暗号化と解読の制御に鍵を使用します。一致する鍵なしに、掻き回されたメッセージやデータを平文に整列することはできません。

暗号鍵に基く方法は対称と非対称の2つに分けられます。対称法は暗号化と解読に対して同じ鍵を用い、一方非対称法は異なる鍵を使用します。AESは対称鍵法です。

2.1. 新暗号化規格(AES)

本項はAES法の詳細な記述を意図していませんが、概要を簡単に説明します。より多くの詳細に関して、読者はAES仕様を学ぶべきです。AES法は有限体演算に基く関数を使用します。AES法は128ビットの固定塊容量を持つ一方で、鍵長は希望する安全性に依存して128,192,256ビットにすることができます。AES法の流れは図2-1.で図解されます。この流れ図の各種操作の説明についてはAES仕様をご覧ください。

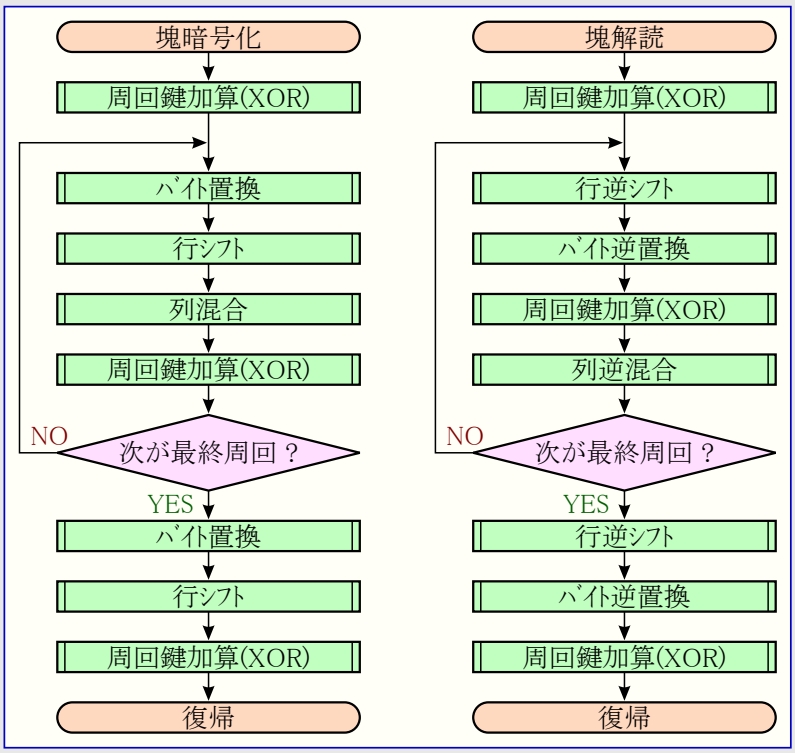
8ビット AVR® マイクロ コントローラ

応用記述

Rev. 8106A-04/08, 8106AJ4-03/14

この方法の周回数は鍵長に依存して走行することを必要とします。

図2-1. 暗号化と解読の流れ図



2.2. 暗号塊連鎖(CBC:Clipher Block Chaining)

AESは塊暗号で、この方法は固定量のﾃﾞｰﾀ塊で操作することを意味します。既知の入力塊と一定の暗号鍵に関して、その出力は常に同じです。この情報は暗号ｼｽﾃﾑの攻撃を欲する誰かにとって有用な提供かもしれません。

同じ平文の塊を違う暗号文の塊に暗号化させるのに一般的に使用される方法があります。そのような方法は暗号塊連鎖(CBC)と呼ばれます。

CBCは先行塊が全ての後行塊に影響を及ぼすような暗号塊を接続する方法です。これは(XOR操作の)結果を暗号化する前で、最初に平文の塊と直前の暗号文の塊でXOR操作を実行することによって成し遂げられます。これは1つの暗号文ﾋﾞｯﾄが依存するところの平文ﾋﾞｯﾄ数を増します。

図2-2. CBC暗号化

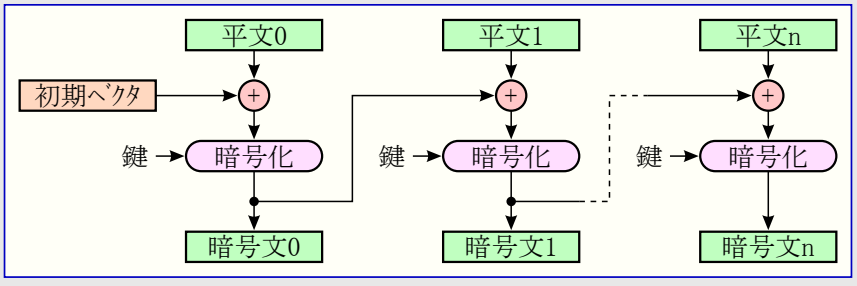
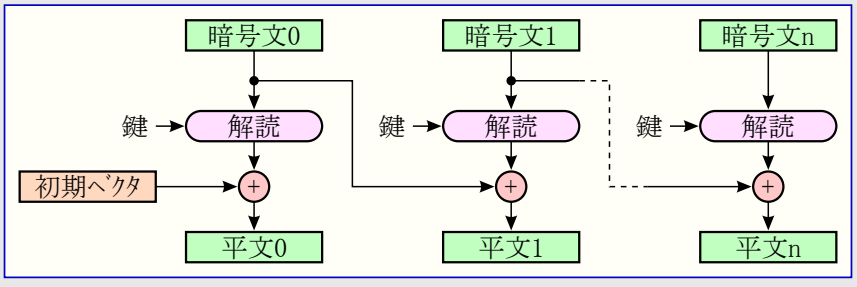


図2-2. CBC解読



3. AES暗号部署

後続の副項目はAES暗号部署操作法の導入を含みます。AES暗号部署が支援する各種機能も示されます。

XMEGAのAES暗号部署は128ﾋﾞｯﾄのAES鍵長を支援します。AES暗号部署の勤めは割り込み機構またはﾎﾟｰﾘﾝｸﾞを通して実行することができます。

DMAもAES暗号部署を扱うように設定できますが、これは本応用記述の範囲外です。より多くの情報についてはﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄまたは「**AVR1304:XMEGA DMA制御器の使い方**」応用記述を参照してください。

3.1. 鍵と状態配列のﾒﾓﾘ

AES暗号部署はAESの平文/暗号文と鍵を保持するのに必要とする2つの128ﾋﾞｯﾄ ﾒﾓﾘを含みます。AES暗号部署では次の鍵定義が使用されることに注意してください。

- 暗号化動作での鍵はAES規格で定義された1つです。
- 解読動作での鍵はAES規格で定義された鍵拡張の最終補助鍵です。

状態配列と鍵のﾒﾓﾘはAES状態配列(STATE)ﾚｼﾞｽﾀとAES鍵(KEY)ﾚｼﾞｽﾀを通してﾊﾞｲﾄ単位で順次読み書きすることができます。状態配列と鍵の両ﾒﾓﾘは読み書きｱｸｾｽに対してﾒﾓﾘをｱﾄﾞﾚｽ指定する(各々)2つの4ﾋﾞｯﾄ ｱﾄﾞﾚｽ ﾎﾟｲﾝﾀを持っています。AESﾒﾓﾘへのｱｸｾｽ後に適切なﾎﾟｲﾝﾀが自動的に増加(進行)されます。AES制御(CTRL)ﾚｼﾞｽﾀのAES開始/走行(START)ﾋﾞｯﾄが0の間だけ、鍵と状態配列のﾒﾓﾘのｱｸｾｽが可能です。

注: 鍵と状態配列の両ﾒﾓﾘは暗号化/解読を始め得る前に、完全に格納されていなければなりません。そうでない場合、AES状態(STATUS)ﾚｼﾞｽﾀのAES異常(ERROR)ﾌﾗｸﾞが設定(1)されます。

3.2. 暗号化

AES暗号部署を使用してAES暗号化を実行するには以下が行われるべきです。

- AES割り込み制御(INTCTRL)ﾚｼﾞｽﾀの割り込み優先権と許可(INTLVL)ﾋﾞｯﾄ領域を設定(1)/解除(0)することにより、AES割り込みを許可/禁止してください。
- AES制御(CTRL)ﾚｼﾞｽﾀのAES解読/方向(DECRYPT)ﾋﾞｯﾄを解除(0)することにより、AES暗号化方向を選択してください。
- AES鍵ﾒﾓﾘ内にAES鍵を格納してください。
- AES状態配列ﾒﾓﾘ内にﾃﾞｰﾀ塊を格納してください。
- AES制御(CTRL)ﾚｼﾞｽﾀのAES開始/走行(START)ﾋﾞｯﾄを設定(1)することにより、暗号化を開始してください。

暗号化が完了されると、AES状態(STATUS)ﾚｼﾞｽﾀのAES状態配列準備可割り込み要求(SRIF)ﾌﾗｸﾞが設定(1)されます。割り込み機構が使用されているなら、割り込みが生成されます。暗号化完了後のAES状態配列ﾒﾓﾘは生成された暗号文を含み、一方AES鍵ﾒﾓﾘはAES規格で定義された鍵拡張の最終補助鍵を含みます。

3.3. 解読

AES暗号部署を使用してAES解読を実行するには以下が行われるべきです。

- AES割り込み制御(INTCTRL)ﾚｼﾞｽﾀの割り込み優先権と許可(INTLVL)ﾋﾞｯﾄ領域を設定(1)/解除(0)することにより、AES割り込みを許可/禁止してください。
- AES制御(CTRL)ﾚｼﾞｽﾀのAES解読/方向(DECRYPT)ﾋﾞｯﾄを設定(1)することにより、AES解読方向を選択してください。
- AES鍵ﾒﾓﾘ内にAES規格で定義された鍵拡張の最終補助鍵を格納してください。
- AES状態配列ﾒﾓﾘ内にﾃﾞｰﾀ塊を格納してください。
- AES制御(CTRL)ﾚｼﾞｽﾀのAES開始/走行(START)ﾋﾞｯﾄを設定(1)することにより、解読を開始してください。

解読が完了されると、AES状態(STATUS)ﾚｼﾞｽﾀのAES状態配列準備可割り込み要求(SRIF)ﾌﾗｸﾞが設定(1)されます。割り込み機構が使用されているなら、割り込みが生成されます。解読完了後のAES状態配列ﾒﾓﾘは生成された平文を含み、一方AES鍵ﾒﾓﾘはAES規格で定義された原型鍵を含みます。

注: 解読を行うのに必要とする拡張された鍵の最終補助鍵は2つの任意の方法で生成することができます。それはｿﾌﾄｳｪｱでの鍵拡張手順実行により、またはAES暗号部署によって生成することができます。AES暗号部署は原型鍵を使用して、暗号化動作で擬似ﾃﾞｰﾀ塊を処理することによって拡張された鍵の最終補助鍵を生成することができます。この暗号化終了後、鍵ﾒﾓﾘは最終補助鍵を含みます。

3.4. AES状態配列XOR格納

AES状態配列XOR格納機能が許可されると、AES状態配列ﾒﾓﾘに格納される値はAES状態配列ﾒﾓﾘの現在値とﾋﾞｯﾄ毎にXORされます。AES状態配列XOR格納機能を許可するにはAES制御(CTRL)ﾚｼﾞｽﾀのXOR格納許可(XOR)ﾋﾞｯﾄを設定(1)してください。この機能はCBCまたは他の暗号化動作種別が実行される時に非常に有用です。

3.5. AES自動開始起動

AES自動開始起動機能が許可されると、状態配列ﾚｼﾞｽﾀ(ﾒﾓﾘ)が完全に格納された時に暗号化/解読が自動的に開始します。

4. ﾄﾞﾗｲﾊﾞ実装

本応用記述はCで実装されたAES基本ﾄﾞﾗｲﾊﾞの一括ｿｰｽ ｺｰﾄﾞを含みます。それはIAR Embedded Workbench®ｺﾝﾊﾟｲﾗで書かれています。

AESﾄﾞﾗｲﾊﾞは単一ﾃﾞｰﾀ塊とCBCの暗号化と解読を支援します。割り込みとﾎﾟｰﾘﾝｸﾞの両ﾄﾞﾗｲﾊﾞが支援されます。

AESﾄﾞﾗｲﾊﾞが高性能ｺｰﾄﾞでの使用に対して意図されていないことに注意してください。それはAES加速器使用の開始に際するﾗｲﾌﾞﾗﾘとして設計されています。より多くの詳細についてはﾄﾞﾗｲﾊﾞのｿｰｽ ｺｰﾄﾞとﾃﾞﾊﾞｲｽのﾃﾞｰﾀｼｰﾄを参照してください。

4.1. ﾌｧｲﾙ

一括ｿｰｽ ｺｰﾄﾞは4つのﾌｧｲﾙから成ります。

- AES_driver.c : AES加速器ﾄﾞﾗｲﾊﾞ ｿｰｽ ﾌｧｲﾙ
- AES_driver.h : AES加速器ﾄﾞﾗｲﾊﾞ ﾍｯﾀﾞ ﾌｧｲﾙ
- AES_example_polled.c : AES加速器ﾎﾟｰﾘﾝｸﾞ ﾄﾞﾗｲﾊﾞを使用するｺｰﾄﾞ例
- AES_example_interrupt.c : AES加速器割り込みﾄﾞﾗｲﾊﾞを使用するｺｰﾄﾞ例

利用可能なﾄﾞﾗｲﾊﾞ ｲﾝﾀｰﾌｪｰｽ関数とそれらの使用の完全な概要についてはｿｰｽ ｺｰﾄﾞの資料を参照してください。

4.2. Doxygen資料化

全てのｿｰｽ ﾌｧｲﾙはDoxygenを使用する自動資料生成用に準備されています。Doxygenは特別なｷｰﾜｰﾄﾞを使用してｿｰｽ ｺｰﾄﾞを分析することによって、ｿｰｽ ｺｰﾄﾞから資料を作成するﾂｰﾙです。Doxygenについてのより多くの詳細に関してはhttp://www.doxygen.orgを訪ねてください。予めｺﾝﾊﾟｲﾙされたDoxygen資料は本応用記述に伴うｿｰｽ ｺｰﾄﾞと共に供給され、ｿｰｽ ｺｰﾄﾞ ﾌｫﾙﾀﾞのreadme.htmlﾌｧｲﾙから利用可能です。

本社

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
TEL 1(408) 441-0311
FAX 1(408) 487-2600

国外営業拠点

Atmel Asia
Unit 1-5 & 16, 19/F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
Hong Kong
TEL (852) 2245-6100
FAX (852) 2722-1369

Atmel Europe
Le Krebs
8, Rue Jean-Pierre Timbaud
BP 309
78054 Saint-Quentin-en-
Yvelines Cedex
France
TEL (33) 1-30-60-70-00
FAX (33) 1-30-60-71-11

Atmel Japan
104-0033 東京都中央区
新川1-24-8
東熱新川ﾋﾞﾙ 9F
ｱﾄﾒﾙ ｼﾞｬﾊﾟﾝ株式会社
TEL (81) 03-3523-3551
FAX (81) 03-3523-7581

製品窓口

ｳｪﾌﾞｻｲﾄ
www.atmel.com

技術支援
avr@atmel.com

販売窓口
www.atmel.com/contacts

文献請求
www.atmel.com/literature

本応用記述はATMELのAVR1318応用記述(doc8106.pdf Rev.8106A-04/08)の翻訳日本語版です。日本語では不自然となる重複する形容表現は省略されている場合があります。日本語では難解となる表現は大幅に意訳されている部分もあります。必要に応じて一部加筆されています。頁割の変更により、原本より頁数が少なくなっています。

必要と思われる部分には( )内に英語表記や略称などを残す形で表記しています。

青字の部分はﾘﾝｸとなっています。一般的に赤字の0,1は論理0,1を表します。その他の赤字は重要な部分を表します。