AVR 8ビット マイクロ コントローラ

AVR284：megaAVRでのAES-128暗号化と復号用ソフトウェア ライブラリ

応用記述

序説

新暗号化規格(AES:Advanced Encryption Standard)は連邦情報処理規格(FIPS)197として2001年に米国国立標準技術研究所によって確定された電子データの暗号化のための仕様です。これは電子データの暗号化と復号のために使用される対称塊暗号算法です。この応用記述はAtmel® ATmega328PBでのAES暗号化と復号の算法の例を提供します。この応用を実演するのにATmega328PB Xplained Miniキットが使用されます。AESの理論についてはAT10764:AES-128暗号化と復号用ソフトウェア ライブラリを参照してください。

特徴

- FIPS公示197,新暗号化規格(AES:Advanced Encryption Standard)適合
- AES暗号化と復号の算法
- 128ビット暗号化鍵を支援
- FIPSで指定されたAESの5つの秘密性動作種別
  - 電子符号本動作 (ECB:Electronic Codebook mode)
  - 暗号塊連鎖動作 (CBC:Cipher Block Chaining mode)
  - 暗号回帰動作 (CFB:Cipher Feedback mode)
  - 出力回帰動作 (OFB:Output Feedback mode)
  - 計数器動作 (CTR)
- CFB動作で可能な8,16,32,64,128ビットのデータの大きさ

Rev. 42784A-09/2016, 42784AJ0-10/2016

目次

1. 事前必要条件

この資料で検討される解決策は以下が必要です。

- Atmel Studio 7.0またはそれ以降
- ATmega328PB Xplained Miniキット
- Atmel START(開始)からﾀﾞｳﾝﾛｰﾄﾞで入手可能な例ｿｰｽ ｺｰﾄﾞ

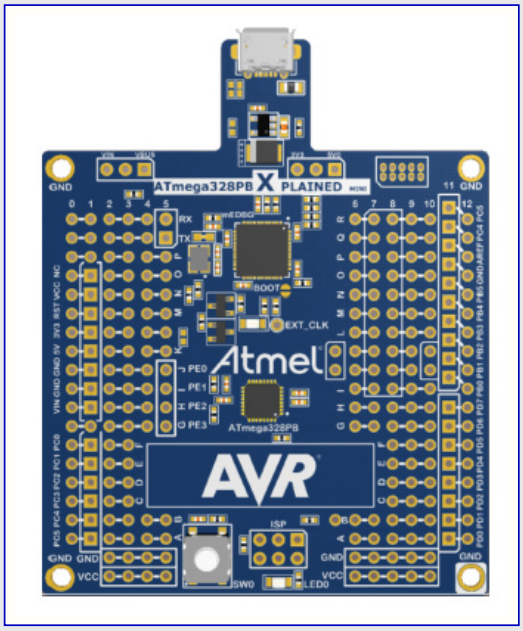
2. ATmega328PB Xplained Mini

2.1. 基板概要

ATmega328PB Xplained Mini評価ｷｯﾄはAtmel ATmega328PBﾏｲｸﾛ ｺﾝﾄﾛｰﾗを評価するためのﾊｰﾄﾞｳｪｱ基盤です。この評価ｷｯﾄはAtmel Studio 7.0(とそれ以降版)との継ぎ目のない統合を提供する完全に統合されたﾃﾞﾊﾞｯｶﾞと共にやって来ます。ｷｯﾄは独自設計でﾃﾞﾊﾞｲｽの容易な統合を許すATmega328PBの機能へのｱｸｾｽを提供します。

このｷｯﾄについてのより多くの詳細に関しては、http://www.atmel.com/Images/Atmel-42469-ATmega328PB-Xplained-Mini_User-Guide.pdfで入手可能な「Atmel ATmega328PB Xplained Mini使用者の手引き」を参照してください。

図2-1. ATmega328PB Xplained Miniｷｯﾄ



2.2. 列挙と検出

ATmega328PB Xplained MiniｷｯﾄがPCに接続されると、Windows®は装置を列挙(接続認証)して適切なﾄﾞﾗｲﾊﾞをｲﾝｽﾄｰﾙします。ﾄﾞﾗｲﾊﾞが成功裏にｲﾝｽﾄｰﾙされた場合、右の画面画像で示されるようにmEDBGはﾃﾞﾊﾞｲｽ ﾏﾈｰｼﾞｬでﾎﾟｰﾄ下のmEDBG仮想COMﾎﾟｰﾄとして一覧にされます。

図2-2. ﾂｰﾙ列挙

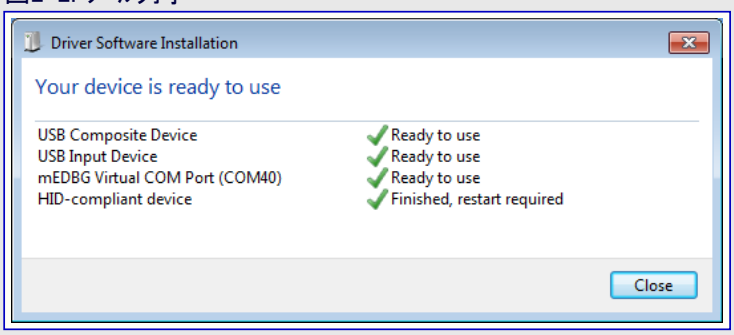
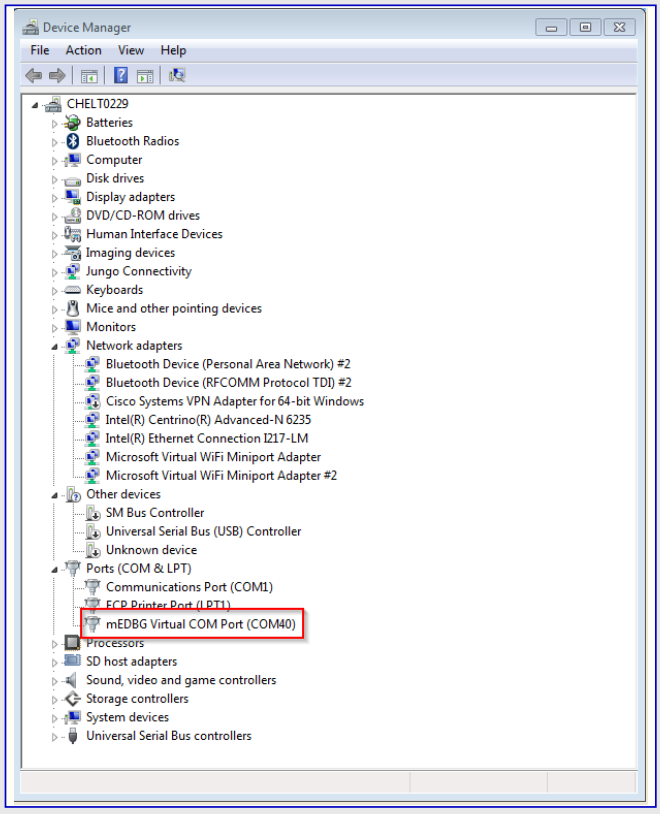


図2-3. 成功したmEDBGﾄﾞﾗｲﾊﾞ ｲﾝｽﾄｰﾙ



3. ATmega328PBでのAES-128ｿﾌﾄｳｪｱ例

この応用記述はATmega328PBでのAES暗号化と復号の算法の例を提供します。ｿｰｽ ｺｰﾄﾞはAtmel START(開始)からのﾀﾞｳﾝﾛｰﾄﾞで入手可能です。

3.1. 説明

本項は5つ全ての動作種別を網羅するAES-128の例についての短い説明を与えます。

- AES-128と5つの秘密性動作種別は2つのﾚﾍﾞﾙで実装されます。AES算法はaes.c/aes.hのﾌｧｲﾙで実装されます。
- 5つの秘密性動作種別はcrypt.c/crypt.hのﾌｧｲﾙで実装さます。
- 例は全ての動作種別を独立して用いて64ﾊﾞｲﾄ(即ち、16入力塊)の平文が暗号化されて復号されるように実装されます。
- 復号しているﾒｯｾｰｼﾞは端末ｳｨﾝﾄﾞｳで見ることができます。
- 復号されたﾃﾞｰﾀが平文と同じ場合の結果から、これは各動作種別の動きと一致します。
- 動作種別は下で示されるようにconf_example.hで独立して許可または禁止することができます。既定では全ての動作種別が許可されます。

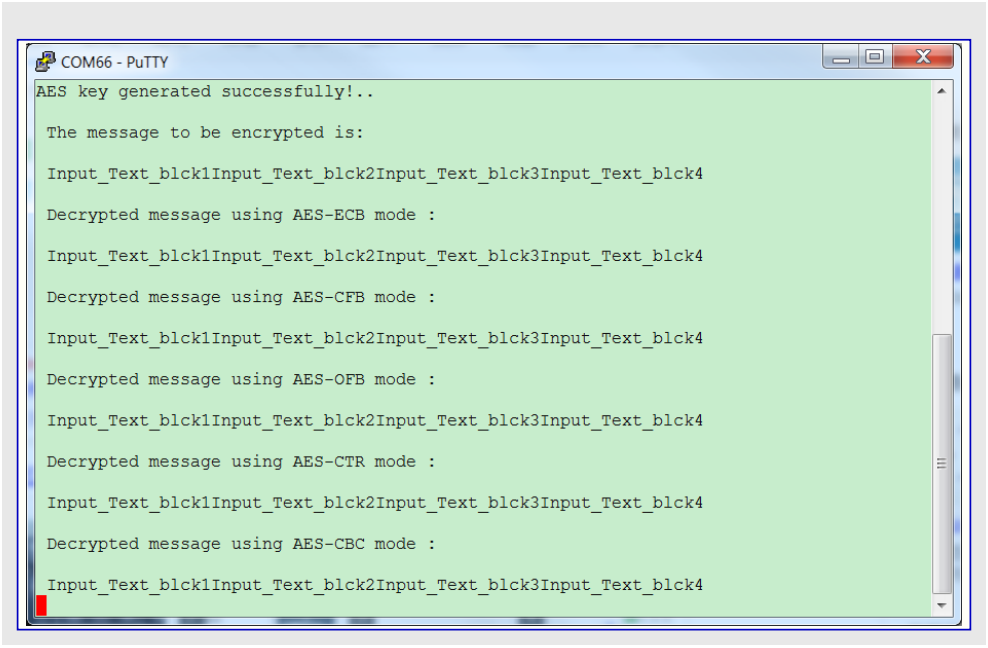
```
/* 各々の動作種別を許可するにはtrueに設定してください。
 * 各々の動作種別を許可するにはfalseに設定してください。
 */
// ECB動作 許可/禁止
#define AES_ECB   true

// CBC動作 許可/禁止
#define AES_CBC   true

// CFB動作 許可/禁止
#define AES_CFB   true

// OFB動作 許可/禁止
#define AES_OFB   true

// CTR動作 許可/禁止
#define AES_CTR   true
```

3.2. 構成設定

この例はﾒｯｾｰｼﾞを出力するのにUSART0単位部を使用します。ﾃﾞｰﾀを受け取るのにPD0が使用され、ﾃﾞｰﾀを送るのにPD1が使用されます。この例でのUSART0は以下の設定で形態設定されます。

- 非同期動作
- 38400bpsのﾎﾞｰﾚｰﾄ
- 8ﾋﾞｯﾄ ﾃﾞｰﾀ、ﾊﾟﾘﾃｨなし、1停止ﾋﾞｯﾄ

全てがOKなら、実際の入力ﾒｯｾｰｼﾞと復号は端末ｳｨﾝﾄﾞｳで下のように見ることができます。



4. 参照

- ATmega328PBﾃﾞｰﾀｼｰﾄ (http://www.atmel.com/devices/ATMEGA328PB.aspx)
- ATmega328PB Xplained Miniｷｯﾄ (http://www.atmel.com/tools/MEGA328PB-XMINI.aspx)
- Atmel Studio (http://www.atmel.com/tools/atmelstudio.aspx?tab=overview)
- Atmel START (http://start.atmel.com)
- AT10764 (http://www.atmel.com/images/atmel-42508-software-library-for-aes-128-encryption-and-decryption_applicationnote_at10764.pdf)

5. 改訂履歴

資料改訂	日付	注釈
42784A	2016年9月	初版資料公開

Atmel Corporation　1600 Technology Drive, San Jose, CA 95110 USA　TEL:(+1)(408) 441-0311　FAX: (+1)(408) 436-4200　|　www.atmel.com

本応用記述はAtmelのAVR284応用記述(Rev.42784A-09/2016)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。