ストリーム暗号 *Enocoro*-128v2

参照ソースコード仕様書

株式会社 日立製作所

2010 年 2 月 2 日

目次

1　はじめに

本ドキュメントは、ストリーム暗号 *Enocoro*-128v2 のサンプルコードの仕様書である。このサンプルコードは、ストリーム暗号のコア機能である疑似乱数生成機能を提供するモジュールである。*Enocoro*-128v2 のアルゴリズムは *Enocoro*-128v2 仕様書を参照のこと [1]。

2　関数仕様

2.1　提供関数

本プログラムで提供する関数を表 1 に示す。

表 1　提供関数

#	関数概要	関数名称	機能概要
1	初期化関数	`ENOCORO_init()`	鍵、IV を設定し初期化を行なう。
2	疑似乱数生成関数	`ENOCORO_keystream()`	疑似乱数列の生成を行なう。

2.2 インターフェース

本プログラムで提供する関数のインターフェースを以下に示す。

2.2.1 初期化関数

■(1) **名称**　ENOCORO_init()

■(2) **機能概要**　与えられた秘密鍵、初期ベクトルをコンテキスト構造体 ENOCORO_Ctx に設定し、初期化を行なう。コンテキスト構造体は、秘密鍵、初期値の他に *Enocoro*-128v2 の内部状態を保持するための構造体である。

■(3) **引数**　引数の一覧は以下の表を参照のこと。

#	名称	型	入出力	説明
1	ctx	ENOCORO_Ctx *	出力	コンテキスト構造体のポインタ
2	key	uint8_t key *	入力	秘密鍵 (128bit) のポインタ
3	keysize	uint32_t	入力	鍵長
4	iv	uint8_t *	入力	初期ベクトル (64bit) のポインタ
5	ivsize	uint32_t	入力	ベクトル長

■(4) **戻り値**　なし

■(5) **特記事項**

1. 鍵長、ベクトル長には、鍵および初期ベクトルのバイト長を指定する。
2. 秘密鍵および初期ベクトルは、上位ビットから順に 8 ビット毎に配列に設定し、配列の先頭ポインタを指定する。
3. 本関数の内部では、エンディアン変換は行なわない。

2.2.2 疑似乱数生成関数

■(1) **名称**　ENOCORO_keystream()

■(2) **機能概要**　与えられたコンテキスト構造体を用いて、定められた長さのバイト列を出力する。

■(3) **引数**　引数の一覧は以下の表を参照のこと。

#	名称	型	入出力	説明
1	ctx	ENOCORO_Ctx *	入力	コンテキスト構造体 (初期化済み) のポインタ
2	keystream	uint8_t *	出力	出力列のポインタ
3	length	uint32_t	入力	出力長

■(4) **戻り値**　なし

■(5) **特記事項**

1. 乱数列を格納する配列のサイズは出力長以上とする (関数内部では出力長のチェックは行わない)。
2. 本関数の内部では、エンディアン変換は行わない。

3　入出力例

秘密鍵および初期ベクトルの設定例を以下に示す。

秘密鍵: 0x000102030405060708090a0b0c0d0e0f

```
key[0] = 0x00
key[1] = 0x01
key[2] = 0x02
key[3] = 0x03
key[4] = 0x04
key[5] = 0x05
key[6] = 0x06
```

```
key[7] = 0x07
key[8] = 0x08
key[9] = 0x09
key[10] = 0x0a
key[11] = 0x0b
key[12] = 0x0c
key[13] = 0x0d
key[14] = 0x0e
key[15] = 0x0f
```

初期ベクトル: 0x0010203040506070

```
iv2[0] = 0x00
iv2[1] = 0x10
iv2[2] = 0x20
iv2[3] = 0x30
iv2[4] = 0x40
iv2[5] = 0x50
iv2[6] = 0x60
iv2[7] = 0x70
```

また、上記の秘密鍵および初期ベクトルを初期値とした場合の疑似乱数生成結果を以下に示す。
疑似乱数: 0xc8c8ee433b0dc040e53bc506ea21ad82

```
keystream[0]  = 0xc8
keystream[1]  = 0xc8
keystream[2]  = 0xee
keystream[3]  = 0x43
keystream[4]  = 0x3b
keystream[5]  = 0x0d
keystream[6]  = 0xc0
keystream[7]  = 0x40
keystream[8]  = 0xe5
keystream[9]  = 0x3b
```

```
keystream[10] = 0xc5
keystream[11] = 0x06
keystream[12] = 0xea
keystream[13] = 0x21
keystream[14] = 0xad
keystream[15] = 0x82
```

4 ファイル一覧

本プログラムのファイルを表 4 に示す。

#	ファイルタイプ	ファイル名	内容
1	C ソースファイル	`enocoro.c`	初期化関数、乱数生成関数
2	C ヘッダファイル	`enocoro.h`	マクロ、構造体、提供関数定義

参考文献

[1] 株式会社日立製作所、「疑似乱数生成器 *Enocoro* 仕様書 Ver. 2.0」、`http://www.sdl.hitachi.co.jp/crypto/enocoro/` より入手可能.