Stream Cipher *Enocoro*-128v2

Specification for The Reference Code

Hitachi, Ltd.

2 February 2010

Contents

1 Introduction

This document specifies the reference code of *Enocoro*-128v2. It gives the pseudorandom number generation function which is the core function of the stream cipher. Please refer to [1] for the specification of the algorithm of *Enocoro*-128v2.

2 Specification of Functions

2.1 Supplied Functions

Table 1 shows the functions supplied in the code.

Table 1: Supplied functions

#	Section	Name	Function
1	Initialization	`ENOCORO_init()`	The function sets a key and an IV, then performs the internal state.
2	random number generation	`ENOCORO_keystream()`	The function generates a byte string.

2.2 Interfaces

Here we describe the I/O of the functions which the code provides.

2.2.1 Initialization

(1) Name `ENOCORO_init()`

(2) Function The function sets the given secret key and IV to the context structure `ENOCORO_Ctx`, which stores input values and the current internal state, then performs the initialization.

(3) Arguments See the following table for the arguments.

#	Name	Type	In/Out	Description
1	`ctx`	`ENOCORO_Ctx *`	Output	The pointer to the context structure.
2	`key`	`uint8_t key *`	Input	The pointer to the 16 bytes array for the secret key
3	`keysize`	`uint32_t`	Input	Key length
4	`iv`	`uint8_t *`	Input	The pointer to the 8 bytes array for the initial vector
5	`ivsize`	`uint32_t`	Input	IV length

(4) Return value None.

(5) Notes

1. The key length and the IV length specify the lengths in bytes of the secret key and the IV respectively.
2. The secret key and the IV should be aligned to the byte array, in which the most significant 8 bits of the key are set to `key[0]`, and so on.
3. This function does not perform the endian transformation.

2.2.2 Pseudorandom Number Generation

(1) Name `ENOCORO_keystream()`

(2) Function For a given context structure and an output length, the function performs the random number generation and outputs a required length of byte string.

(3) Arguments See the following table for the arguments.

#	Name	Type	In/Out	Description
1	`ctx`	`ENOCORO_Ctx *`	Input	The pointer to the initialized context
2	`keystream`	`uint8_t *`	Input	The pointer to the array for output string
3	`length`	`uint32_t`	Input	Output length in bytes

(4) Return value None.

(5) Notes

1. The function does not check the output length. I.e., the function expects that the length of the array `keystream[]` is at least `length`.
2. This function does not perform the endian transformation.

3 Example of Inputs And The Output Values

The following is an example of a secret key and an IV, and the corresponding output string.

Key: `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
```

Initial vector: `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
```

Output: `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 File List

The code consists of the following files.

#	Type	Name	Contents
1	C source file	`enocoro.c`	Initialization function and random number generation function are described.
2	C header file	`enocoro.h`	Macros, structures and functions are defined.

References

[1] Hitachi, Ltd., "Pseudorandom Number Generator *Enocoro*: Specification Ver. 2.0." Available at `http://www.sdl.hitachi.co.jp/crypto/`

`enocoro/`.