

# **Lightweight Encryption Algorithm**

## **- LEA -**

Ji Yong-Hyeon

**Department of Information Security, Cryptology, and Mathematics**

College of Science and Technology  
Kookmin University

January 8, 2024



## List of Symbols

# Contents

- 1 Block Cipher LEA-128 . . . . . 1**
  - 1.1 Specification . . . . . 1
  - 1.2 Key Schedule . . . . . 1
    - 1.2.1 Round Constant . . . . . 2
    - 1.2.2 Rotation Function . . . . . 2
    - 1.2.3 Encryption Key Schedule of LEA-128 . . . . . 2
  - 1.3 Encryption of LEA-128 . . . . . 3
  - 1.4 Decryption Key Schedule of LEA-128 . . . . . 4
  - 1.5 Decryption of LEA-128 . . . . . 5
- A Additional Data A . . . . . 6**
  - A.1 Substitution-BOX . . . . . 6

# Chapter 1

## Block Cipher LEA-128

### 1.1 Specification

Table 1.1: Specification Comparison between AES and LEA Block Ciphers

Specification	AES	LEA
Block Size (bits)	128	128
Key Size (bits)	128/192/256	128/192/256
Structure	Substitution-Permutation Network	Generalized Feistel Network
Rounds	10/12/14 (depends on key size)	24/28/32 (depends on key size)
Designed By	Joan Daemen, Vincent Rijmen	Deukjo Hong et al.
Design Year	1998	2013

Table 1.2: Parameters of the Block Cipher LEA (1-word = 32-bit)

Algorithms	Block Size ( $N_b$ -byte)	Key Length ( $N_k$ -byte)	Number of Rounds ( $N_r$ )	Round-Key Length (byte)	Number of Round-Keys ( $N_r + 1$ )	Total Size of Round-Keys ( $N_b(N_r + 1)$ )
LEA-128	16(4-word)	16(4-word)	24	24	11	44 (176-byte)
LEA-192	16(4-word)	24(6-word)	28	24	13	52 (208-byte)
LEA-256	16(4-word)	32(8-word)	32	24	15	60 (240-byte)

### 1.2 Key Schedule

$$\text{KeySchedule}_{128}^{\text{enc}} : \{0, 1\}^{128=8 \cdot 16} \rightarrow \{0, 1\}^{4608=192 \cdot 24}$$

$$\text{KeySchedule}_{192}^{\text{enc}} : \{0, 1\}^{192=8 \cdot 24} \rightarrow \{0, 1\}^{5376=192 \cdot 28}$$

$$\text{KeySchedule}_{256}^{\text{enc}} : \{0, 1\}^{256=8 \cdot 32} \rightarrow \{0, 1\}^{6144=192 \cdot 32}$$

### 1.2.1 Round Constant

The constant  $\delta[i] \in \mathbb{F}_{2^{32}}$  ( $i \in \{1, \dots, 7\}$ ) is as follows:

$i$	$\delta[i]$	value
0	$\delta[0]$	0xc3efe9db
1	$\delta[1]$	0x44626b02
2	$\delta[2]$	0x79e27c8a
3	$\delta[3]$	0x78df30ec
4	$\delta[4]$	0x715ea49e
5	$\delta[5]$	0xc785da0a
6	$\delta[6]$	0xe04ef22a
7	$\delta[7]$	0xe5c40957

### 1.2.2 Rotation Function

---

#### Algorithm 1: Rotation to Left and Right

---

```

/* RotL :  $\{0, 1\}^{32} \times \{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$  */
1 Function RotL(value, shift):
2 |   return (value  $\ll$  shift) | (value  $\gg$  (32 – shift));
3 end

/* RotR :  $\{0, 1\}^{32} \times \{0, 1\}^{32} \rightarrow \{0, 1\}^{32}$  */
4 Function RotR(value, shift):
5 |   return (value  $\gg$  shift) | (value  $\ll$  (32 – shift));
6 end

```

---

### 1.2.3 Encryption Key Schedule of LEA-128

---

#### Algorithm 2: Encryption Key Schedule (LEA-128)

---

**Input:** User-key  $UK = (UK_0, \dots, UK_{15})$  ( $UK_i \in \{0, 1\}^8$ ) //  $UK \in \{0, 1\}^{128}$  is 16-byte

**Output:** Encryption Round-keys  $\{RK_i^{\text{enc}}\}_{i=0}^{23}$  ( $RK_i^{\text{enc}} \in \{0, 1\}^{192}$ )

```

/*  $\{RK_i^{\text{enc}}\}_{i=0}^{23} \in \{0, 1\}^{4608}$  is 576-byte */
1  $T \leftarrow UK$  //  $T \in \{0, 1\}^{128}$ 
2 for  $i = 0$  to 23 do
3 |    $T[0] \leftarrow \text{RotL}(T[0] \boxplus \text{RotL}(\delta[i \bmod 4], i + 0), 1)$  //  $T[i] \in \{0, 1\}^{32}$ 
4 |    $T[1] \leftarrow \text{RotL}(T[1] \boxplus \text{RotL}(\delta[i \bmod 4], i + 1), 3)$ 
5 |    $T[2] \leftarrow \text{RotL}(T[2] \boxplus \text{RotL}(\delta[i \bmod 4], i + 2), 6)$ 
6 |    $T[3] \leftarrow \text{RotL}(T[3] \boxplus \text{RotL}(\delta[i \bmod 4], i + 3), 11)$ 
7 |    $RK_i^{\text{enc}} \leftarrow T[1] \parallel T[3] \parallel T[1] \parallel T[2] \parallel T[1] \parallel T[0]$  //  $RK_i^{\text{enc}} \in \{0, 1\}^{196=32 \times 6}$ 
8 end
9 return  $\{RK_i^{\text{enc}}\}_{i=0}^{23}$ 

```

---

## 1.3 Encryption of LEA-128

---

**Algorithm 3:** Encryption of LEA-128
 

---

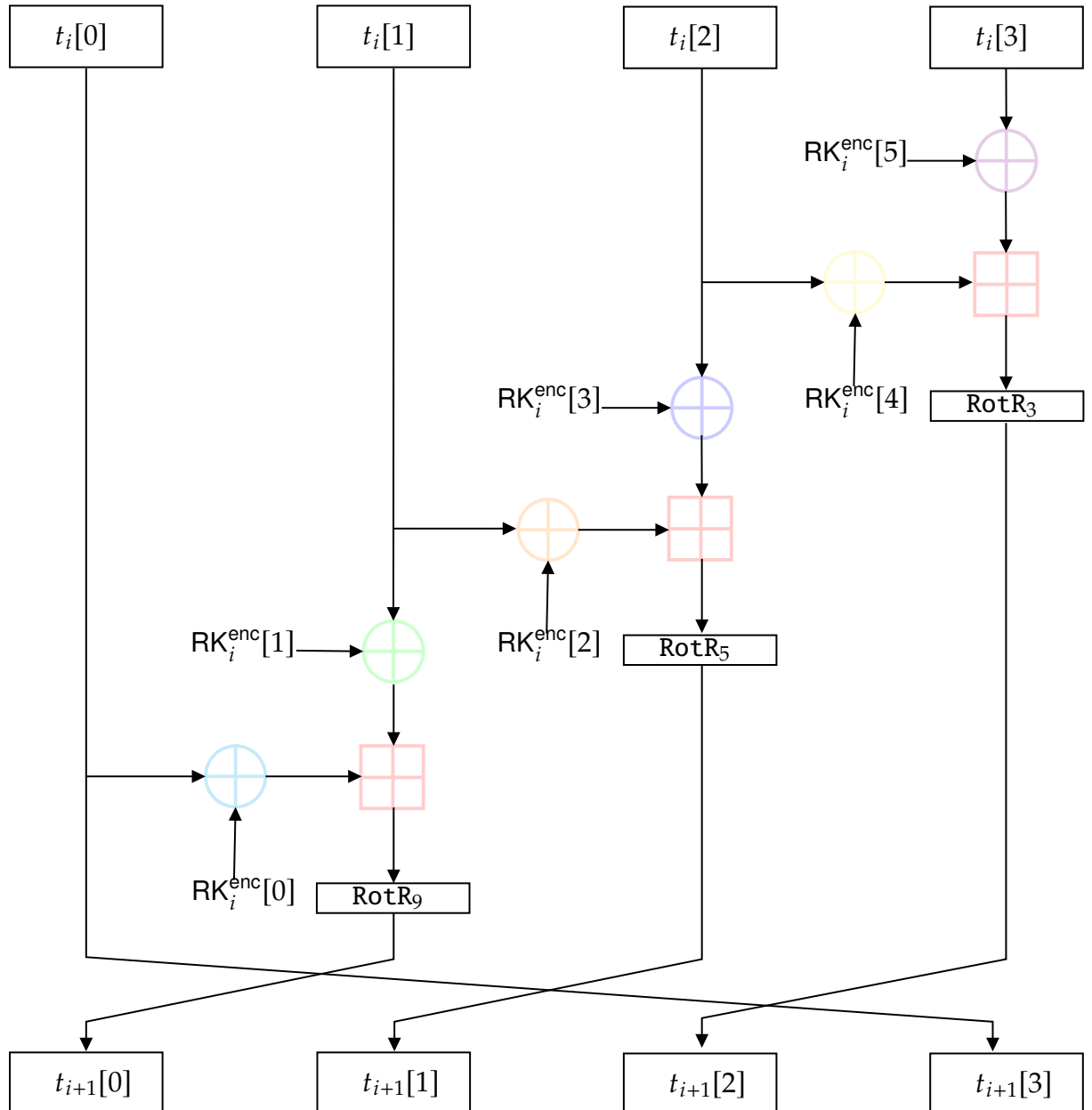
**Input:** block  $\text{src} \in \{0, 1\}^{128=8 \times 16}$ , encryption round-keys  $\{\text{RK}_i^{\text{enc}}\}_{i=0}^{N_r-1=23}$

**Output:** block  $\text{dst} \in \{0, 1\}^{128=8 \times 16}$

```

1  $t_0 \leftarrow \text{src}$ 
2 for  $i = 0$  to  $N_r - 1$  do
3    $t_{i+1}[0] \leftarrow \text{RotR}(t_i[0] \oplus \text{RK}_i^{\text{enc}}[0] \boxplus (t_i[1] \oplus \text{RK}_i^{\text{enc}}[1]), 9)$ 
4    $t_{i+1}[1] \leftarrow \text{RotR}(t_i[1] \oplus \text{RK}_i^{\text{enc}}[2] \boxplus (t_i[2] \oplus \text{RK}_i^{\text{enc}}[3]), 5)$ 
5    $t_{i+1}[2] \leftarrow \text{RotR}(t_i[2] \oplus \text{RK}_i^{\text{enc}}[4] \boxplus (t_i[3] \oplus \text{RK}_i^{\text{enc}}[5]), 3)$ 
6    $t_{i+1}[3] \leftarrow t_i[0]$ 
7 end
8 return  $\text{dst} \leftarrow t_{N_r}$ 
  
```

---



## 1.4 Decryption Key Schedule of LEA-128

---

**Algorithm 4:** Decryption Key Schedule (LEA-128)

---

**Input:** User-key  $UK = (UK_0, \dots, UK_{15})$  ( $UK_i \in \{0, 1\}^8$ ) //  $UK \in \{0, 1\}^{128}$  is 16-byte

**Output:** Decryption Round-keys  $\{RK_i^{\text{dec}}\}_{i=0}^{23}$  ( $RK_i^{\text{dec}} \in \{0, 1\}^{192}$ )

/\*  $\{RK_i^{\text{enc}}\}_{i=0}^{23} \in \{0, 1\}^{4608}$  is 576-byte \*/

```

1  $T \leftarrow UK$  //  $T \in \{0, 1\}^{128}$ 
2 for  $i = 0$  to 23 do
3    $T[0] \leftarrow \text{RotL}(T[0] \boxplus \text{RotL}(\delta[i \bmod 4], i + 0), 1)$  //  $T[i] \in \{0, 1\}^{32}$ 
4    $T[1] \leftarrow \text{RotL}(T[1] \boxplus \text{RotL}(\delta[i \bmod 4], i + 1), 3)$ 
5    $T[2] \leftarrow \text{RotL}(T[2] \boxplus \text{RotL}(\delta[i \bmod 4], i + 2), 6)$ 
6    $T[3] \leftarrow \text{RotL}(T[3] \boxplus \text{RotL}(\delta[i \bmod 4], i + 3), 11)$ 
7    $RK_i^{\text{dec}} \leftarrow T[1] \parallel T[3] \parallel T[1] \parallel T[2] \parallel T[1] \parallel T[0]$  //  $RK_i^{\text{dec}} \in \{0, 1\}^{196=32*6}$ 
8 end
9 return  $\{RK_i^{\text{dec}}\}_{i=0}^{23}$ 

```

---



## 1.5 Decryption of LEA-128

---

**Algorithm 5:** Decryption of LEA-128
 

---

**Input:** block  $\text{src} \in \{\mathbf{0}, \mathbf{1}\}^{128=8 \times 16}$ , decryption round-keys  $\{\text{RK}_i^{\text{dec}}\}_{i=0}^{N_r-1=23}$

**Output:** block  $\text{dst} \in \{\mathbf{0}, \mathbf{1}\}^{128=8 \times 16}$

```

1  $t_0 \leftarrow \text{src}$ 
2 for  $i = 0$  to  $N_r - 1$  do
3    $t_{i+1}[0] \leftarrow t_i[3]$ 
4    $t_{i+1}[1] \leftarrow (\text{RotR}(t_i[0], 9) \boxminus (t_{i+1}[0] \oplus \text{RK}_i^{\text{dec}}[0])) \oplus \text{RK}_i^{\text{dec}}[1]$ 
5    $t_{i+1}[2] \leftarrow (\text{RotR}(t_i[1], 9) \boxminus (t_{i+1}[1] \oplus \text{RK}_i^{\text{dec}}[2])) \oplus \text{RK}_i^{\text{dec}}[3]$ 
6    $t_{i+1}[3] \leftarrow (\text{RotR}(t_i[2], 9) \boxminus (t_{i+1}[2] \oplus \text{RK}_i^{\text{dec}}[4])) \oplus \text{RK}_i^{\text{dec}}[5]$ 
7 end
8 return  $\text{dst} \leftarrow t_{N_r}$ 

```

---

# **Appendix A**

## **Additional Data A**

### **A.1 Substitution-BOX**