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

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

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

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

$$\text{KeySchedule}^{\mathsf{enc}}_{256} : \{\mathtt{0}, 1\}^{256=8\cdot 32} \longrightarrow \{\mathtt{0}, 1\}^{6144=192\cdot 24}$$

1.2.1 Round Constant

The constant $\delta[i] \in \mathbb{F}_{2^{32}}$ ($i \in \{1, \ldots, 7\}$) 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 : $\{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32}$ */
Function RotL(value, shift):
  return (value $\ll$ shift) | (value $\gg$ (32 − shift));
end

/* RotR : $\{0,1\}^{32} \times \{0,1\}^{32} \to \{0,1\}^{32}$ */
Function RotR(value, shift):
  return (value $\gg$ shift) | (value $\ll$ (32 − shift));
end

1.2.3 Encryption Key Schedule of LEA-128

Algorithm 2: Encryption Key Schedule (LEA-128)

Input: User-key $\mathsf{UK} = (\mathsf{UK}_0, \ldots, \mathsf{UK}_3)$ ($\mathsf{UK}_i \in \{0,1\}^{32}$) // $\mathsf{UK} \in \{0,1\}^{128}$ is 16-byte
Output: Encryption Round-keys $\{\mathsf{RK}_i^{\mathsf{enc}}\}_{i=0}^{23}$ ($\mathsf{RK}_i^{\mathsf{enc}} \in \{0,1\}^{192}$)
/* $\{\mathsf{RK}_i^{\mathsf{enc}}\}_{i=0}^{23} \in \{0,1\}^{4608}$ is 576-byte */

$T \leftarrow \mathsf{UK}$ // $T \in \{0,1\}^{128=32*4}$
for $i = 0$ **to** 23 **do**
  $T[0] \leftarrow \mathtt{RotL}(T[0] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+0), 1)$ // $T[i] \in \{0,1\}^{32}$
  $T[1] \leftarrow \mathtt{RotL}(T[1] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+1), 3)$
  $T[2] \leftarrow \mathtt{RotL}(T[2] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+2), 6)$
  $T[3] \leftarrow \mathtt{RotL}(T[3] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+3), 11)$
  $\mathsf{RK}_i^{\mathsf{enc}} \leftarrow T[1] \parallel T[3] \parallel T[1] \parallel T[2] \parallel T[1] \parallel T[0]$ // $\mathsf{RK}_i^{\mathsf{enc}} \in \{0,1\}^{196=32*6}$
end
return $\{\mathsf{RK}_i^{\mathsf{enc}}\}_{i=0}^{23}$

1.3 Encryption of LEA-128

Algorithm 3: Encryption of LEA-128

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

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

$t_0 \leftarrow \mathsf{src}$

for $i = 0$ **to** $N_r - 1$ **do**

  $t_{i+1}[0] \leftarrow \mathtt{RotR}(\, t_i[0] \oplus \mathsf{RK}_i^{\mathsf{enc}}[0] \boxplus (t_i[1] \oplus \mathsf{RK}_i^{\mathsf{enc}}[1])\, , 9)$

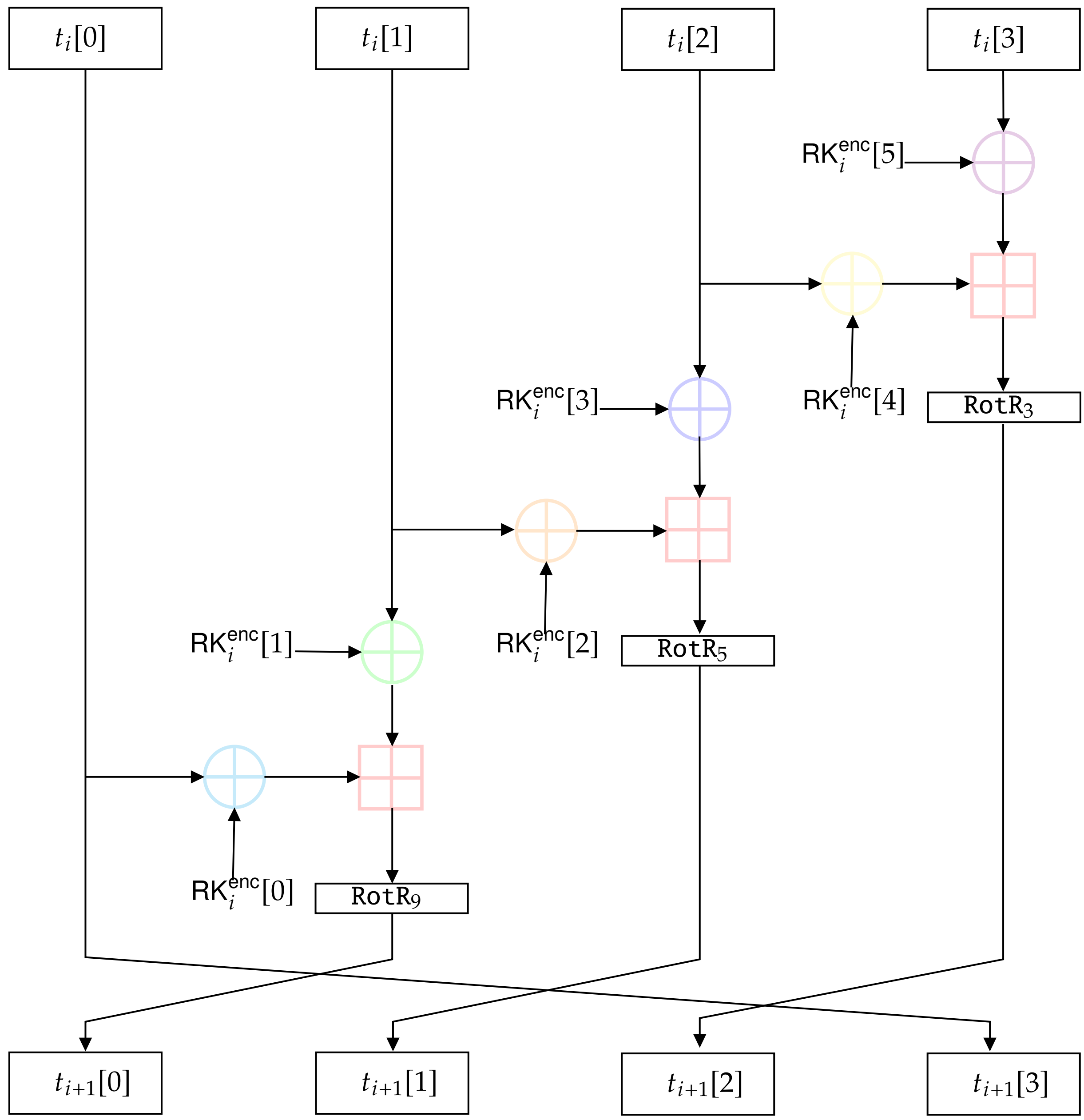
  $t_{i+1}[1] \leftarrow \mathtt{RotR}(\, t_i[1] \oplus \mathsf{RK}_i^{\mathsf{enc}}[2] \boxplus (t_i[2] \oplus \mathsf{RK}_i^{\mathsf{enc}}[3])\, , 5)$

  $t_{i+1}[2] \leftarrow \mathtt{RotR}(\, t_i[2] \oplus \mathsf{RK}_i^{\mathsf{enc}}[4] \boxplus (t_i[3] \oplus \mathsf{RK}_i^{\mathsf{enc}}[5])\, , 3)$

  $t_{i+1}[3] \leftarrow t_i[0]$

end

return $\mathsf{dst} \leftarrow t_{N_r}$



1.4 Decryption Key Schedule of LEA-128

Algorithm 4: Decryption Key Schedule (LEA-128)

Input: User-key $\mathsf{UK} = (\mathsf{UK}_0, \ldots, \mathsf{UK}_{15})$ ($\mathsf{UK}_i \in \{0,1\}^8$) // $\mathsf{UK} \in \{0,1\}^{128}$ is 16-byte

Output: Decryption Round-keys $\{\mathsf{RK}_i^{\mathsf{dec}}\}_{i=0}^{23}$ ($\mathsf{RK}_i^{\mathsf{dec}} \in \{0,1\}^{192}$)

/* $\left\{\mathsf{RK}_i^{\mathsf{enc}}\right\}_{i=0}^{23} \in \{0,1\}^{4608}$ is 576-byte */

$T \leftarrow \mathsf{UK}$ // $T \in \{0,1\}^{128}$

for $i = 0$ **to** 23 **do**

  $T[0] \leftarrow \mathtt{RotL}(T[0] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+0), 1)$ // $T[i] \in \{0,1\}^{32}$

  $T[1] \leftarrow \mathtt{RotL}(T[1] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+1), 3)$

  $T[2] \leftarrow \mathtt{RotL}(T[2] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+2), 6)$

  $T[3] \leftarrow \mathtt{RotL}(T[3] \boxplus \mathtt{RotL}(\delta[i \bmod 4], i+3), 11)$

  $\mathsf{RK}_i^{\mathsf{dec}} \leftarrow T[1] \parallel T[3] \parallel T[1] \parallel T[2] \parallel T[1] \parallel T[0]$ // $\mathsf{RK}_i^{\mathsf{dec}} \in \{0,1\}^{196=32*6}$

end

return $\left\{\mathsf{RK}_i^{\mathsf{dec}}\right\}_{i=0}^{23}$

1.5 Decryption of LEA-128

Algorithm 5: Decryption of LEA-128

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

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

$t_0 \leftarrow \mathsf{src}$

for $i = 0$ **to** $N_r - 1$ **do**

$\quad t_{i+1}[0] \leftarrow t_i[3]$

$\quad t_{i+1}[1] \leftarrow (\mathtt{RotR}(t_i[0], 9) \boxminus (t_{i+1}[0] \oplus \mathsf{RK}_i^{\mathsf{dec}}[0])) \oplus \mathsf{RK}_i^{\mathsf{dec}}[1]$

$\quad t_{i+1}[2] \leftarrow (\mathtt{RotR}(t_i[1], 9) \boxminus (t_{i+1}[1] \oplus \mathsf{RK}_i^{\mathsf{dec}}[2])) \oplus \mathsf{RK}_i^{\mathsf{dec}}[3]$

$\quad t_{i+1}[3] \leftarrow (\mathtt{RotR}(t_i[2], 9) \boxminus (t_{i+1}[2] \oplus \mathsf{RK}_i^{\mathsf{dec}}[4])) \oplus \mathsf{RK}_i^{\mathsf{dec}}[5]$

end

return $\mathsf{dst} \leftarrow t_{N_r}$

Appendix A

Additional Data A

A.1 Substitution-BOX