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

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	Key	Number of	Round-Key	Number of	Total Size of
	Size	Length	Rounds	Length	Round-Keys	Round-Keys
	(N_b-byte)	(N_k-byte)	(N_r)	(byte)	($N_r + 1$)	($N_b(N_r + 1)$)
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

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

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

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

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`

Algorithm 1: 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: Round-keys $\{\mathsf{RK}_i\}_{i=0}^{23}$ ($\mathsf{RK}_i \in \{0, 1\}^{192}$);  // $\{\mathsf{RK}_i\}_{i=0}^{23} \in \{0, 1\}^{4608}$ is 576-byte
$rk_0 \leftarrow uk_0 \| uk_1 \| uk_2 \| uk_3$;
$rk_1 \leftarrow uk_4 \| uk_5 \| uk_6 \| uk_7$;
$rk_2 \leftarrow uk_8 \| uk_9 \| uk_{10} \| uk_{11}$;
$rk_3 \leftarrow uk_{12} \| uk_{13} \| uk_{14} \| uk_{15}$;
for $i = 4$ to $43$ do
    $t \leftarrow rk_{i-1}$;
    if $i \bmod 4 = 0$ then
        /* SubWord ∘ RotWord : $\{0, 1\}^{32} \longrightarrow \{0, 1\}^{32}$ */
        $t \leftarrow \mathrm{RotWord}(t)$;
        $t \leftarrow \mathrm{SubWord}(t)$;
        $t \leftarrow t \oplus (\mathtt{rCon}_{i/4} \| \mathtt{0x00} \| \mathtt{0x00} \| \mathtt{0x00})$;
    end
    $rk_i \leftarrow rk_{i-4} \oplus_{32} t$;
end
```

Appendix A

Additional Data A

A.1 Substitution-BOX