Specification of MAKryept

Alaa Kryeem (mzcdzdamri_f_)

June 03, 2020

1. Cipher:

The block cipher MAKryept has a 64-bit blocksize and a 64-bit key. MAKryept is based on a feistel network with 4-bit sboxes and a bit permutation as the linear layer, combined with Shift rows (SR) and Mix columns (MC) operation for stronger diffusion, see Cipher diagram section (1.6) below for a visual representation.

MAKryept cipher consists of 12 rounds.

1.1. Round function:

Given a word x=$\mathcal{l} \mid r$ where $\mathcal{l}$ consists of the 32 most significant bits and r consists of the 32 least significant bits, we can define the round function F as follows:
As first and last steps we apply key whitening:

X = X $\oplus$ WKL $\oplus$ WKR

As a second step we apply the following:

We divide $\mathcal{l}$ into two parts: $\mathcal{ll}$ and $\mathcal{lr}$. (each is 16 bits)

We define:

$$MAK(\mathcal{l}_{=32bits}) = (\sigma(\mathcal{ll} \oplus \mathcal{lr}) << 16) \mid \sigma(\sigma(\mathcal{ll} \oplus \mathcal{lr}) \oplus \mathcal{lr})$$

$$Semi\text{-}F(\mathcal{l}, r, K_i) = S(MAK(S(\mathcal{l}))) \oplus r \oplus K_i$$

$$F(\mathcal{l}, r, K_i) = MC(SR((Semi\text{-}F(\mathcal{l}, r, K_i) \texttt{ << 32) | right}))$$

Where S is the parallel application of the 4-bit sbox S to the state and σ is a bit permutation. The sbox S is defined as follows:

S = [0x3,0xe,0x5,0xd,0x9,0xa,0x1,0xf,0x7,0xc,0x0,0x8,0x6,0x2,0xb,0x4]

We create a 8bit Sbox based on S, for better performance. (Hardcoded in the code)

and the bit permutation σ is defined as follows (Taken from TC05):

$$\sigma = \left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 6 & 0 & 1 & 7 & E & 8 & 9 & F & 2 & 4 & 5 & 3 & A & C & D & B \end{array} \right)$$

MC is mix columns, SR is shift rows, defined as follows:

1.2. Shift rows:

In the shift rows layer (SR) we rotate the nibbles in the rows by 0, 1, 2 and 3 places to the left.

1.3. Mix Columns

In the Mix Columns (MC) layer we mix the nibbles in every column according to a matrix. The matrix is given by:

$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

1.4. Key schedule:

Given master key $K=k_0|k_1$ the round key k is defined as follows:

$$k_i = k_{i-1} \oplus \sigma(k_{i-2}) \oplus (\sigma(k_{i-2} >> 16) << 16) \oplus 0xC5A1B9D2$$

1.5. Test vectors:

Plain-text	Cipher-text	Key
0x0000000000000000	0x5db04e75e8355076	0x0000000000000000
0x123456789ABCDEF	0xab09ddda9ca20444	0x0000000000000000
0x123456789ABCDEF	0x182373787299b587	0x0000000000000001
0x123456789ABCDEF	0x1f7bf9657ca87d1d	0x0000000000000002

1.6. Cipher diagram: