Assignment 4 – 2019.10.15

Submission deadline: 2019.11.6

1. Raindrop is one of the block cipher candidates submitted to the Chinese cryptographic algorithm design competition which is sponsored by the Chinese Association for CACR.
   a) Try your best to find an effective differential distinguisher ($\alpha \rightarrow \beta$) which holds with large probability (at least greater than 2^{-128}, the larger the better); and can cover large number of rounds (the longer the better).You should try different number of rounds to see the limit of your distinguisher (For example, if you successfully build a 4 rounds differential distinguisher, than you can keep going to try 5 rounds and so on).
   b) Launch the key recovery attack. Provide every concrete information in every steps of the key recovery phase, and provide your the computational and data complexity to show that it is indeed a legal attack (The computational complexity should be less than 2^{128}, and the data complexity, namely, the number of plaintext and ciphertext used by the attacker should be less than 2^{128}).The violation of either of the above condition should be treated as an invalid attack.

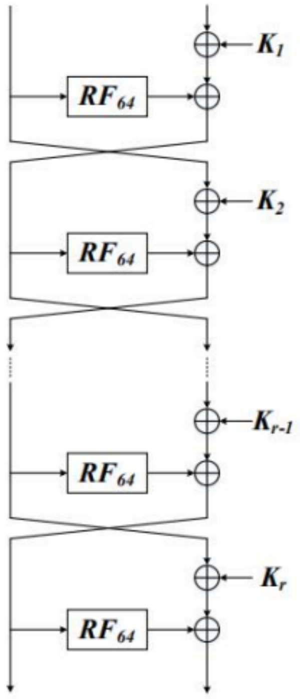
Raindrop128-128

Label the 128-bit plaintext from right to left, and the serial number from 0 to 127. 128-bit plaintext is divided into left and right branches in operation. 64-127 bits are the 64-bit state value of the left branch, and 0-63 bits are the 64-bit state value of the right branch.

The round function RF_{64} of Raindrop-128-128 operates on the 64-bit state, which can be expressed as a 4 × 4 two-dimensional array, called the state matrix. Given a 64-bit state $p_0p_1...p_{15}$, it can be mapped to a 4 × 4 state matrix in the following order:

$$\begin{pmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{pmatrix},$$

For 128-bit version, the length of P_i is donated as $|P_i|$, which satisfies the condition that: when i = 0, 4, 8, 12, 2, 6, 10, 14, $|P_i| = 3$; in other cases, $|P_i| = 5$.



Each P_i is called a word, so that 64-bit state can be divided into 16 word combinations. Round function RF_{64} updates the state matrix by three operations in turn: S-box, MixRow and BitRot.

1. S-box

S-boxes are designed from Keccak’ s S-boxes, which are 3-bit and 5-bit S-boxes, respectively.

3 bit	0	1	2	3	4	5	6	7
	0	5	3	2	6	1	4	7

5 bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	0	5	10	11	20	17	22	23	9	12	3	2	13	8	15	14
	16	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
	18	21	24	27	6	1	4	7	26	29	16	19	30	25	28	31

2. MixRow

Differential analysis shows that the row mixing operation provides strong diffusivity, and it is specific details as follows. The row mixing matrix is:

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

Through this matrix right-multiply and state matrix, we can get the values of the mixed rows, which is

$$\begin{Bmatrix} p_0 & p_4 & p_8 & p_{12} \\ p_1 & p_5 & p_9 & p_{13} \\ p_2 & p_6 & p_{10} & p_{14} \\ p_3 & p_7 & p_{11} & p_{15} \end{Bmatrix} \times \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \Rightarrow \begin{Bmatrix} p_4 \oplus p_{12} & p_8 \oplus p_{12} & p_8 & p_0 \oplus p_4 \\ p_5 \oplus p_{13} & p_9 \oplus p_{13} & p_9 & p_1 \oplus p_5 \\ p_6 \oplus p_{14} & p_{10} \oplus p_{14} & p_{10} & p_2 \oplus p_6 \\ p_7 \oplus p_{15} & p_{11} \oplus p_{15} & p_{11} & p_3 \oplus p_7 \end{Bmatrix}$$

3. BitRot

The cascade value of column i of the state matrix is $\mathrm{Col}_i = p_{4i} \,||\, p_{4i+1} \,||\, p_{4i+2}p \,||\, p_{4i+3}$, where $0 < i < 3$. For each column, the bit level is cyclically shifted in the following way:

Col_0 is unchanged,

Col_1 is cyclically 6 bits to the left,

Col_2 is cyclically 7 bits to the left,

Col_3 is cyclically 12 bits to the left.