

Assignment III: Block Cipher Cryptanalysis

Deadline: 02/12/2022

IAI, TCG CREST

Consider a 64-bit block cipher Light-AES composed of 12 rounds each having 4 operations:

□ Sub-Cell: Uses a 4-bit S-Box GS and apply it to each cells. The S-Box operation is given in Fig.1, and the difference distribution table corresponding to the S-Box is given in Fig.3.

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$GS(x)$	1	a	4	c	6	f	3	9	2	d	b	7	5	0	8	e

Figure 1: S-Box for Light-AES

□ Shuffle-Cells: Shuffle the cells of the state as follows:

$$\begin{pmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{pmatrix} \rightarrow \begin{pmatrix} s_0 & s_{14} & s_9 & s_7 \\ s_{10} & s_4 & s_3 & s_{13} \\ s_5 & s_{11} & s_{12} & s_2 \\ s_{15} & s_1 & s_6 & s_8 \end{pmatrix}.$$

□ Mix-Columns: Multiply each column by the following matrix:

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

□ Add-Round-Key: XORs the round key with the state.

The 64-bit message is divided into 16 cells of 4-bit, and loaded in the initial state. The key whitening is done in the beginning. Answer the following:

1. Show that Light-AES achieves full diffusion in 3 rounds.
2. Prove or Refute: The order of Sub-Cell and Shuffle-Cells is invariant in Light-AES.
3. Show that if there exists exactly two positions with a non-zero differences in a column, then the two positions will contain a non-zero difference even after the mix column operation.
4. What is the branch number of matrix M ? Show that the matrix M is involutory (i.e., $M = M^{-1}$). State the main advantages and disadvantages of using this matrix as compared to the one used in AES.

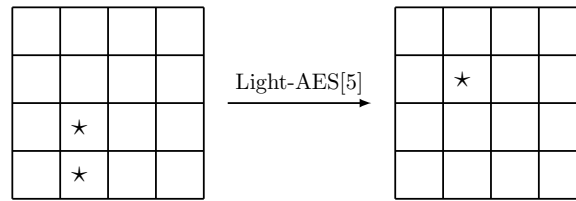


Figure 2: 5 round Impossible Differential of Light-AES.

5. Using the above property, prove that 5-round Light-AES has the following impossible differential depicted in Fig.2.
6. Assume that any r ($r \geq 2$) round differential characteristic of Light-AES has a minimum of $4r$ active S-Boxes. Find an estimate on the minimum number of rounds Light-AES should use to resist against differential cryptanalysis?
7. Mount an Integral attack (distinguishing) on 3-round Light-AES. Compute the data, time and memory complexity of your attack.

		Δ_o																
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	
Δ_r	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	1	0	0	0	0	0	2	2	0	2	2	2	2	2	2	0	0	2
	2	0	0	0	0	0	4	4	0	0	2	2	0	0	2	2	0	
	3	0	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2	
	4	0	0	0	2	0	4	0	6	0	2	0	0	0	2	0	0	
	5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4	
	6	0	0	4	6	0	0	0	2	0	0	2	0	0	0	2	0	
	7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0	
	8	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4	
	9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0	
	a	0	4	0	0	0	0	4	0	0	2	2	0	0	2	2	0	
	b	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0	
	c	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0	
	d	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2	
	e	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	0	
	f	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2	

Figure 3: DDT for Light-AES