CSEC 508: Applied Cryptanalysis
Homework 2

DEADLINE: 25 May 2023 13:40

1. Obtain the inverses of the S-boxes that are given in Table 1. Name them as S_i^{-1}.
2. Compute the Difference Distribution Tables (DDTs) of the S-boxes that are given in Table 1. What is their differential uniformity?
3. Compute the DDTs of the S-boxes S_i^{-1}. In terms of differential uniformity, can you see a relation between S_i and S_i^{-1}?
4. For a specific input difference α of an S-box, if some bits of the output difference remain invariant for every (x, y) pair where $x \oplus y = \alpha$, then we call such bits *undisturbed*. Obtain the undisturbed bits of the S-boxes that are given in Table 1.
5. Let S be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$. For all $x, y \in \mathbb{F}_2^n$ that satisfy $S(x) \oplus S(y) = \mu$ where $\mu \neq 0$, if we also have $S(x \oplus \lambda) \oplus S(y \oplus \lambda) = \mu$, then we say that the S-box has a *differential factor* λ for the output difference μ. (i.e. μ remains invariant for λ). Check the S-boxes that are given in Table 1 for differential factors. If they contain any, provide the λ and corresponding μ values.
6. Compute the differential factors of the S-boxes S_i^{-1}. In terms of λ and μ values, can you see a relation between S_i and S_i^{-1}?
7. Compute the Linear Approximation Tables (LATs) of the S-boxes that are given in Table 1. What is their linear uniformity? (Please note that the previous questions are related to differential properties of S-boxes. Hence we are always considering the difference of two inputs x and x' and the difference of the outputs $S(x)$ and $S(x')$. However, linear cryptanalysis deals with the relation between the input and output, namely x and $S(x)$. Hence we are no longer considering input pairs. Let's consider 4-bit values a and x where their bit-representation is $a = a_3a_2a_1a_0$ and $x = x_3x_2x_1x_0$. We define the masking operation "$\cdot$" as $a \cdot x = a_3x_3 \oplus a_2x_2 \oplus a_1x_1 \oplus a_0x_0$. Thus, masking operation result can either be 0 or 1. ij-entry of a LAT can be computed as

$$\left[\sum_{x=0}^{15} (i \cdot x) \oplus (j \cdot S(x))\right] - 8$$

   Thus, LAT values are in $[-8, 8]$. Linear uniformity is the maximum absolute value of this table, except the first entry).
8. Compute the LATs of the S-boxes S_i^{-1}. In terms of linear uniformity, can you see a relation between S_i and S_i^{-1}?

Table 1: 4×4 S-boxes

S-box	`0123456789abcdef`
S_0	`c56b90ad3ef84712`
S_1	`e4d12fb83a6c5907`
S_2	`0bc5619a3fe8d427`