The 8-bit Sboxes of Midori-128 are constructed with 4-bit ones $Sb1$, where the internal structure is as Figure 1.

$$Sb1[16] = \{1, 0, 5, 3, e, 2, f, 7, d, a, 9, b, c, 8, 4, 6\}$$

We notice that the swap of the two 4-bit inputs to $SSbi$ leads to the swap of the output nibbles. Namely, assume that

$$SSbi(a_L||a_R) = (b_L||b_R)$$

then,

$$SSbi(a_R||a_L) = (b_R||b_L)$$

In a different notation: $SSbi(x \lll 4) = (SSbi(x)) \lll 4$. The reason behind this property is that the two layers of bit permutation in $SSbi$ are the inverse of each other.

As we have already show, $SSbi(x \lll 4) = (SSbi(x)) \lll 4$. The ShuffleCell operation merely moves the cells around, so the rotation on each cell is preserved. For the MixColumn operation,

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} = \begin{bmatrix} y_3 \\ y_2 \\ y_1 \\ y_0 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_3 \lll 4 \\ x_2 \lll 4 \\ x_1 \lll 4 \\ x_0 \lll 4 \end{bmatrix} = \begin{bmatrix} y_3 \lll 4 \\ y_2 \lll 4 \\ y_1 \lll 4 \\ y_0 \lll 4 \end{bmatrix}$$

The round key of Midori-128 is the same for every round, so if the round key has the cell rotation property, the rotational property will pass though key addition as well. And it leaves us with the constant addition.

Constant addition For Midori-128, the constants are 0 or 1 for each cell. When the constant is 0, it has no effect on the propagation of rotational property. When the constant

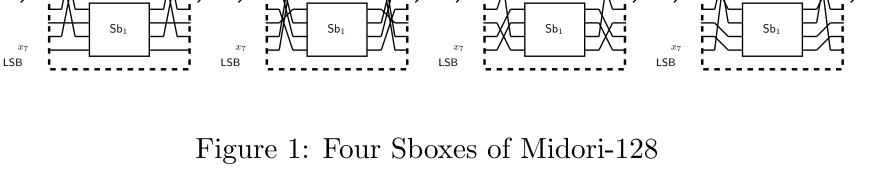

Figure 1: Four Sboxes of Midori-128

is 1,

$$(d_L||d_R) = (a_L||a_R) \oplus (0000||0001), (d'_L||d'_R) = (a_R||a_L) \oplus (0000||0001)$$

therefore,

$$(d'_L||d'_R) = ((d_L||d_R) \lll 4) \oplus (0001||0001)$$

The first round constant of Midori-128 is $\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

Sbox with rotational differences Assume the input pair of values to the Sbox being $(x_1||x_0)$ and $((x_0 \oplus \delta_L)||(x_1 \oplus \delta_R))$. Then the probability for the output pair being $((y_1 \oplus d_L)||(y_0 \oplus d_R))$ is the same as normal difference propagation from $(\delta_L||\delta_R)$ to $(d_R||d_L)$ through the S-box. In other words, the output difference (in ordinary difference definition) is rotated/swapped.

$$DP_{rot}((\delta_L||\delta_R) \rightarrow (d_L||d_R)) = DP((\delta_L||\delta_R) \rightarrow (d_R||d_L))$$

In the following, we give an example on 2-round rotational differential in Midori-128 (without the second SR and MC).

$$\begin{bmatrix} 00 & 02 & 5a & 00 \\ 20 & 00 & 00 & 00 \\ 78 & 00 & 00 & 00 \\ 99 & 01 & 00 & 00 \end{bmatrix} \overrightarrow{SB} \begin{bmatrix} 00 & 01 & 05 & 00 \\ 01 & 00 & 00 & 00 \\ 05 & 00 & 00 & 00 \\ 11 & 14 & 00 & 00 \end{bmatrix} \overrightarrow{SR} \begin{bmatrix} 00 & 00 & 00 & 14 \\ 00 & 01 & 11 & 00 \\ 00 & 00 & 00 & 05 \\ 00 & 01 & 00 & 05 \end{bmatrix} \overrightarrow{MC} \begin{bmatrix} 00 & 00 & 11 & 00 \\ 00 & 01 & 00 & 14 \\ 00 & 00 & 11 & 11 \\ 00 & 01 & 11 & 11 \end{bmatrix}$$

$$\overrightarrow{ARC} \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 10 & 00 & 14 \\ 00 & 00 & 00 & 00 \\ 11 & 10 & 00 & 00 \end{bmatrix} \overrightarrow{SB} \begin{bmatrix} 00 & 00 & 00 & 00 \\ 00 & 80 & 00 & 40 \\ 00 & 00 & 00 & 00 \\ 99 & 09 & 00 & 00 \end{bmatrix}$$

The probability of the RX-differential is 2^{-24}.