1 sequential xor count based on words

Denote a 4×4 MDS matrix M_1 as

$$M_1 \quad = \quad \begin{pmatrix} I & A^2 \oplus I & A^2 & A^2 \oplus A \\ I & A^2 \oplus A \oplus I & A^2 \oplus A & A^2 \\ A & A & I & I \\ A & A^2 \oplus A & A^2 \oplus I & A^2 \oplus A \oplus I \end{pmatrix}.$$

Then, the matrix M_1 can be decomposed as

$$\begin{aligned} M_1 \quad = \quad & \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & I & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ I & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & I \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & A \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & I & 0 & I \end{pmatrix} \\ & \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ A & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & A & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & I & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & I & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{pmatrix} \begin{pmatrix} I & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & I \\ 0 & 0 & 0 & I \end{pmatrix}, \end{aligned}$$

which also can be represented as

$$M_1 = \overline{\mathbf{12}}(1)\overline{\mathbf{4}}(1)\overline{\mathbf{3}}(1)E_{(4)}(A)\overline{\mathbf{11}}(1)\overline{\mathbf{7}}(A)E_{(2)}(A)\overline{\mathbf{5}}(1)\overline{\mathbf{1}}(1)\overline{\mathbf{9}}(1).$$

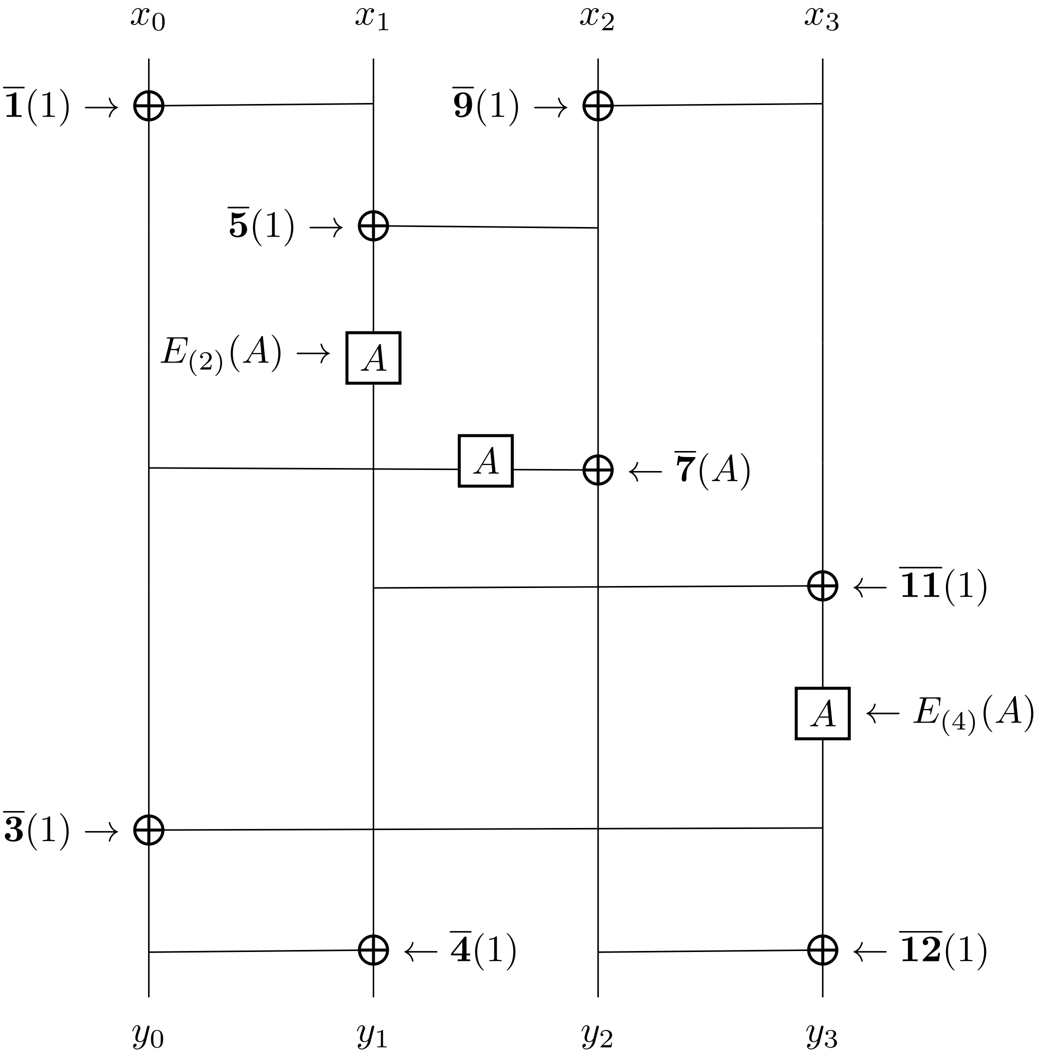
x_0
x_1
x_2
x_3
$\overline{\mathbf{1}}(1) \rightarrow$
$\overline{\mathbf{9}}(1) \rightarrow$
$\overline{\mathbf{5}}(1) \rightarrow$
$E_{(2)}(A) \rightarrow$
A
A
$\leftarrow \overline{\mathbf{7}}(A)$
$\leftarrow \overline{\mathbf{11}}(1)$
A
$\leftarrow E_{(4)}(A)$
$\overline{\mathbf{3}}(1) \rightarrow$
$\leftarrow \overline{\mathbf{4}}(1)$
$\leftarrow \overline{\mathbf{12}}(1)$
y_0
y_1
y_2
y_3

Figure 1: An implementation circuit of MDS matrix M_1 based on the words, where $(x_0, \cdots, x_3)$ are input words, $(y_0, \cdots, y_3)$ are output words.

2 sequential xor count based on bits

Denote the matrix A is $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$. Then the matrix M_1 can be expressed as

$$\left(\begin{array}{cccc|cccc|cccc|cccc}
1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
\hline
1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
\hline
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1
\end{array}\right).$$

1	$x_8 \leftarrow x_{12} \oplus x_8$	19	$x_{12} \leftarrow x_4 \oplus x_{12}$
2	$x_9 \leftarrow x_{13} \oplus x_9$	20	$x_{13} \leftarrow x_5 \oplus x_{13}$
3	$x_{10} \leftarrow x_{14} \oplus x_{10}$	21	$x_{14} \leftarrow x_6 \oplus x_{14}$
4	$x_{11} \leftarrow x_{15} \oplus x_{11}$	22	$x_{15} \leftarrow x_7 \oplus x_{15}$
5	$x_0 \leftarrow x_4 \oplus x_0$	23	$x_{14} \leftarrow x_{15} \oplus x_{14}$
6	$x_1 \leftarrow x_5 \oplus x_1$	24	$y_0 \leftarrow x_{12} \oplus x_0$
7	$x_2 \leftarrow x_6 \oplus x_2$	25	$y_1 \leftarrow x_{13} \oplus x_1$
8	$x_3 \leftarrow x_7 \oplus x_3$	26	$y_2 \leftarrow x_{14} \oplus x_2$
9	$x_4 \leftarrow x_4 \oplus x_8$	27	$y_3 \leftarrow x_{15} \oplus x_3$
10	$x_5 \leftarrow x_5 \oplus x_9$	28	$y_4 \leftarrow y_0 \oplus x_4$
11	$x_6 \leftarrow x_6 \oplus x_{10}$	29	$y_5 \leftarrow y_1 \oplus x_5$
12	$x_7 \leftarrow x_7 \oplus x_{11}$	30	$y_6 \leftarrow y_2 \oplus x_6$
13	$x_6 \leftarrow x_6 \oplus x_7$	31	$y_7 \leftarrow y_3 \oplus x_7$
14	$y_8 \leftarrow x_8 \oplus x_1$	32	$y_{12} \leftarrow y_8 \oplus x_{12}$
15	$y_9 \leftarrow x_9 \oplus x_2$	33	$y_{13} \leftarrow y_9 \oplus x_{13}$
16	$x_{10} \leftarrow x_{10} \oplus x_3$	34	$y_{14} \leftarrow y_{10} \oplus x_{14}$
17	$y_{11} \leftarrow x_{11} \oplus x_0$	35	$y_{15} \leftarrow y_{11} \oplus x_{15}$
18	$y_{10} \leftarrow x_{10} \oplus x_0$		

Table: An implementation of MDS matrix M_1 with 35 xor gates, where $(x_0, \cdots, x_{15})$ are input bits, $(y_0, \cdots, y_{15})$ are output bits.

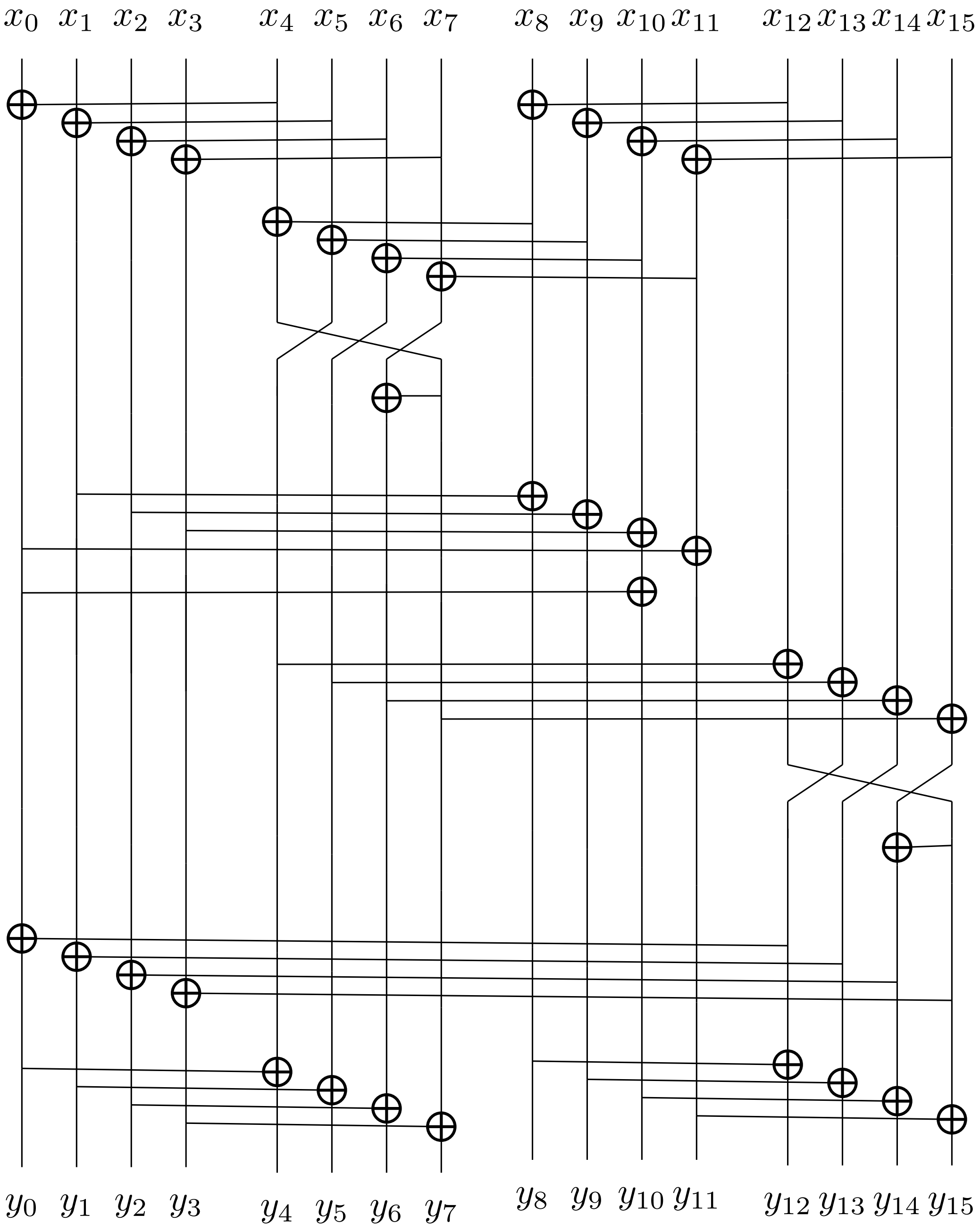

Figure 2: An implementation circuit of MDS matrix M_1 based on the bits, where $(x_0, \cdots, x_{15})$ are input signals, $(y_0, \cdots, y_{15})$ are output signals.