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

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

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

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

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

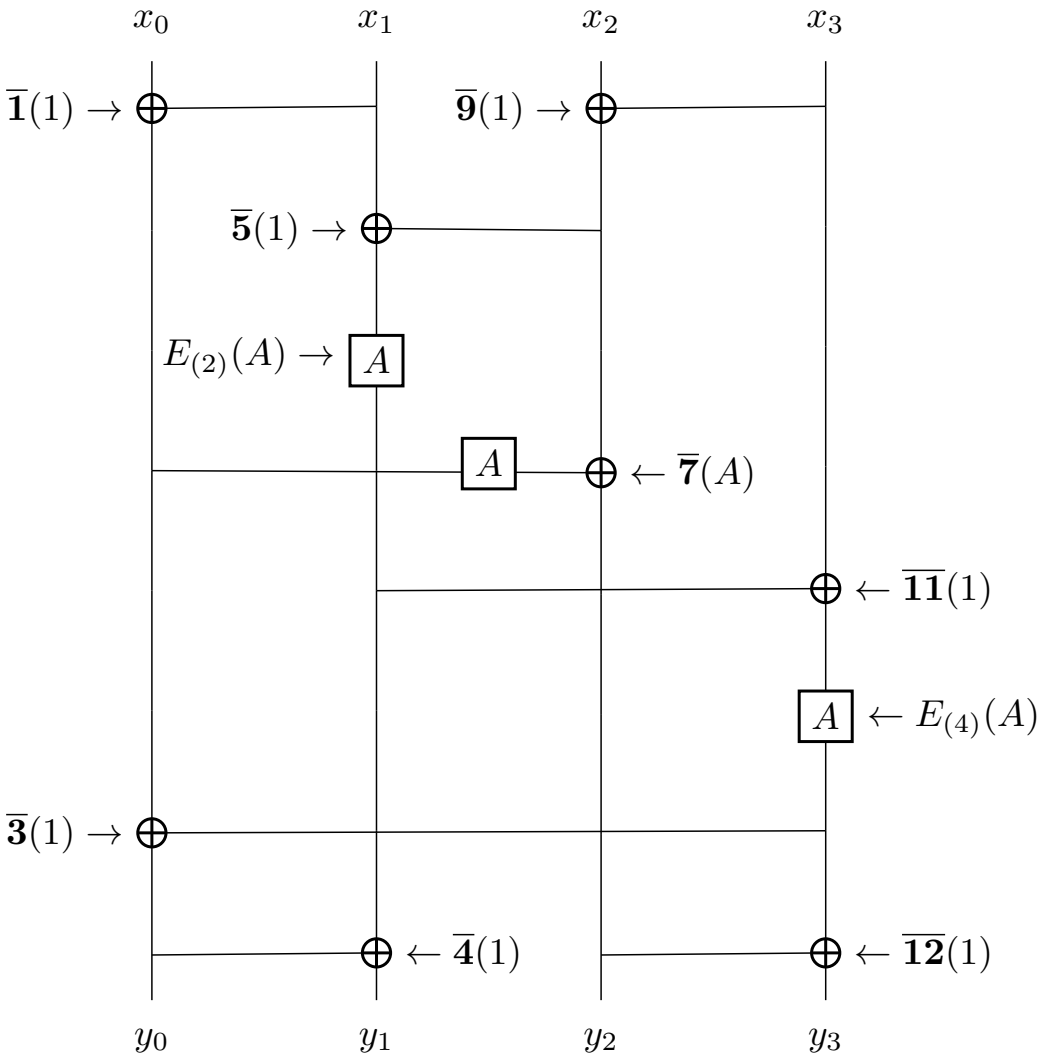

Figure 1: sequential xor count based on word

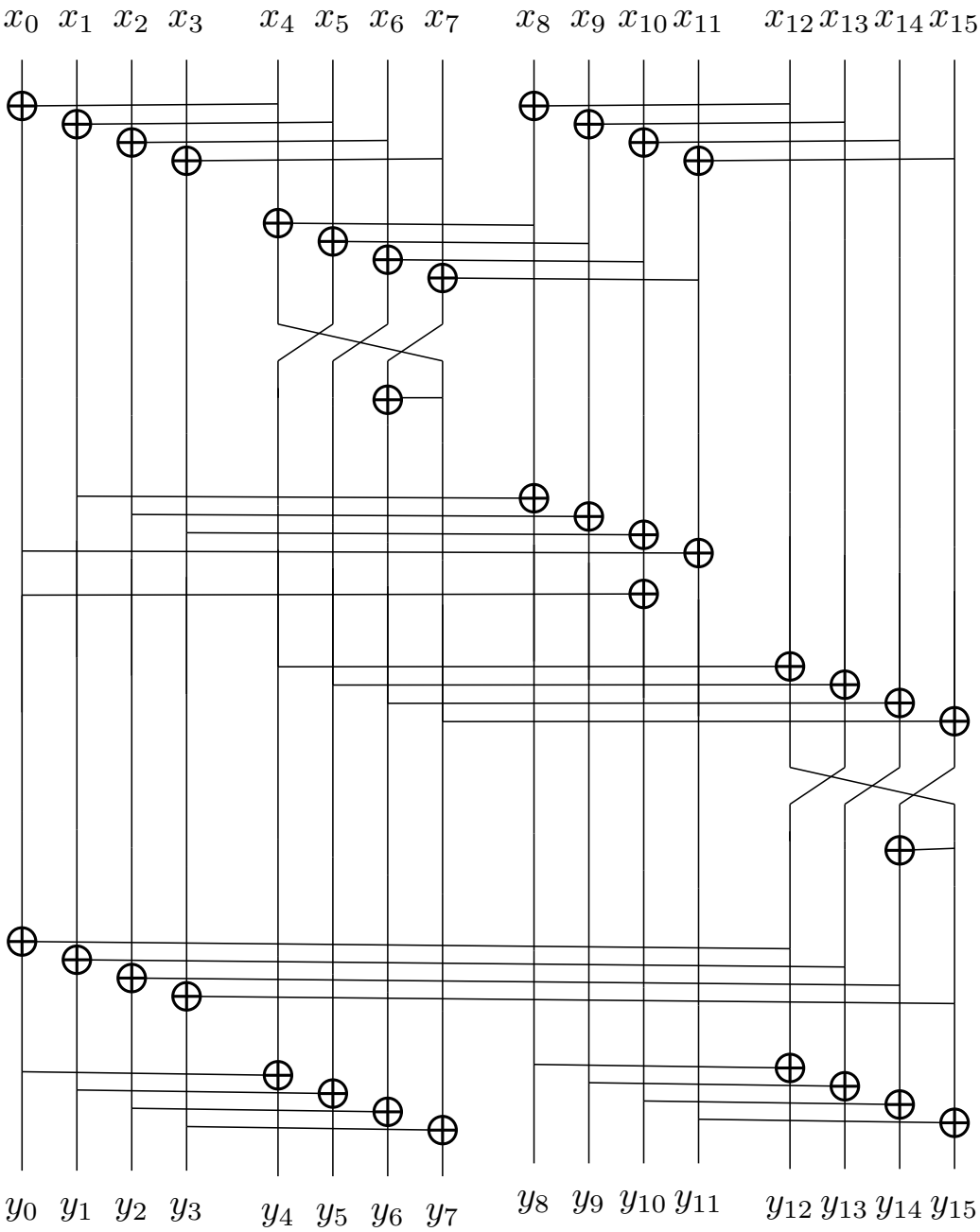

Figure 2: sequential xor count based on bits

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	$x_0 \leftarrow x_{12} \oplus x_0$
7	$x_2 \leftarrow x_6 \oplus x_2$	25	$x_1 \leftarrow x_{13} \oplus x_1$
8	$x_3 \leftarrow x_7 \oplus x_3$	26	$x_2 \leftarrow x_{14} \oplus x_2$
9	$x_4 \leftarrow x_4 \oplus x_8$	27	$x_3 \leftarrow x_{15} \oplus x_3$
10	$x_5 \leftarrow x_5 \oplus x_9$	28	$x_4 \leftarrow x_0 \oplus x_4$
11	$x_6 \leftarrow x_6 \oplus x_{10}$	29	$x_5 \leftarrow x_1 \oplus x_5$
12	$x_7 \leftarrow x_7 \oplus x_{11}$	30	$x_6 \leftarrow x_2 \oplus x_6$
13	$x_6 \leftarrow x_6 \oplus x_7$	31	$x_7 \leftarrow x_3 \oplus x_7$
14	$x_8 \leftarrow x_8 \oplus x_1$	32	$x_{12} \leftarrow x_8 \oplus x_{12}$
15	$x_9 \leftarrow x_9 \oplus x_2$	33	$x_{13} \leftarrow x_9 \oplus x_{13}$
16	$x_{10} \leftarrow x_{10} \oplus x_3$	34	$x_{14} \leftarrow x_{10} \oplus x_{14}$
17	$x_{11} \leftarrow x_{11} \oplus x_0$	35	$x_{15} \leftarrow x_{11} \oplus x_{15}$
18	$x_{10} \leftarrow x_{10} \oplus x_0$		