

G

	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7
	0	1	1	0	1	1	1	0
	1	1	1	0	0	0	1	0
\oplus	0	0	0	1	0	1	1	0
	<hr/>							
	1	0	0	1	1	0	1	0

$$(A_0 \oplus A_3 \oplus A_4 \oplus A_6) \oplus (X \oplus Y \oplus Z)$$

 E

	A_0	A_1	A_2	A_3	$A_4 \oplus \Delta$ \downarrow	A_5	A_6	A_7	Garbled Rows	
	0 1 1 0				1	1	1	0	$A_1 \oplus A_2 \oplus X$	$A_4 \oplus A_5 \oplus A_6 \oplus X$
	1	1	1 0		0	0	1 0		$A_0 \oplus A_1 \oplus Y$	$A_2 \oplus A_6 \oplus Y$
\oplus	0	0	0	1	0	1	1	0	$A_6 \oplus Z$	$A_3 \oplus A_5 \oplus Z$
	<hr/>									
	1	1	0	0	1	1	0	0		

$$\begin{aligned}
 & (A_0 \oplus A_1 \oplus (A_4 \oplus \Delta) \oplus A_5) \\
 & \oplus (A_1 \oplus A_2 \oplus X) \oplus (A_2 \oplus A_6 \oplus Y) \oplus (A_3 \oplus A_5 \oplus Z) \\
 & = (A_0 \oplus A_3 \oplus A_4 \oplus A_6) \oplus (X \oplus Y \oplus Z) \oplus \Delta
 \end{aligned}$$