

Reducing polynomial												m					a								0
Input bits	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Reduction matrix																	⊕								⊕
																⊕	13							⊕	13
															⊕	14							⊕	14	
														⊕	15							⊕	15		
													⊕	16							⊕	16			
													17							⊕	17				⊕
												18				⊕	18		⊕	18			⊕	18	
												19				⊕	19		⊕	19			⊕	19	
												20			⊕	20		⊕	20			⊕	20		
												21		⊕	21		⊕	21				⊕	21		
												22		⊕	22		⊕				⊕	22			⊕
												23		⊕	23	⊕	23		⊕	23			⊕	23	
												24			24		24			24				24	
Output bits (vertically)													12	11	10	9	8	7	6	5	4	3	2	1	0