RSA	256-bit				512-bit				1024-bit				2048-bit	4096-bit	8192-bit
c	2^{17}	2^{16} 1		1^{KSMB}	2^{19}	2^{18} 1		1^{KSMB}	2^{21}	2^{20} 1		1^{KSMB}	2^{23}	2^{25}	2^{26}
Total gates	10,747	19,185	-	6.7E+08	21,499	38,385	-	5.4E+09	43,003	76,785	-	4.2E+10	86,011	172,027	344,059
Non-XOR	2,827	4,880	-	2.4E+08	5,643	9,744	-	1.9E+09	11,275	19,472	-	1.5E+10	22,539	45,067	90,123
CS (B)	2.6E+05	4.6E+05	-	1.6E+10	5.2E+05	9.2E+05	-	1.3E+11	1.0E+06	1.8E+06	-	1.0E+12	2.1E+06	4.1E+06	8.3E+06
PFC	1.5E+09	1.3E+09	-	1.6E+09	1.2E+10	1.0E+10	-	1.3E+10	9.5E+10	8.2E+10	-	1.0E+11	7.6E+11	6.0E+12	4.8E+13
CSE	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
PFD	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
CSE^{KSMB}	6.3E+04	3.5E+04	-	1.0	2.5E+05	1.4E+05	-	1.0	9.8E+05	5.5E+05	-	1.0	-	-	-
PFD^{KSMB}	57%	36%	-	0%	54%	33%	-	0%	56%	35%	-	0%	-	-	-