Mult.	64-bit				128-bit				256-bit				1024-bit			
c	64	16	1	1^{KSMB}	128	32	1	1^{KSMB}	256	64	1	1^{KSMB}	1024	256	1	1^{KSMB}
Total gates	358	738	11,439	1.1E+05	742	1,506	47,620	4.2E+05	1,526	4,812	-	1.7E+06	6,134	35,518	-	2.6E+07
Non-XOR	122	311	3,925	2.5E+04	250	631	16,046	1.0E+05	510	1,777	-	4.0E+05	2,046	24,253	-	6.4E+06
CS (B)	8.6E+03	1.8E+04	2.7E+05	2.5E+06	1.8E+04	3.6E+04	1.1E+06	1.0E+07	3.7E+04	1.2E+05	-	4.0E+07	1.5E+05	8.5E+05	-	6.1E+08
PFC	3.1E+04	2.0E+04	1.6E+04	9.9E+04	1.3E+05	8.1E+04	6.4E+04	4.0E+05	5.2E+05	4.5E+05	-	1.6E+06	8.4E+06	2.5E+07	-	2.5E+07
CSE	32.0	15.5	1.0	-	64.2	31.6	1.0	-	-	-	-	-	-	-	-	-
PFD	99%	27%	0%	-	99%	26%	0%	-	-	-	-	-	-	-	-	-
CSE^{KSMB}	195.0	143.5	9.3		570.2	280.9	8.9		1087.7	344.9	-	1.0	4172.2	720.5	-	1.0
PFD^{KSMB}	-76%	-80%	-84%		-68%	-80%	-84%		-67%	-72%	-	0%	-67%	-3%	-	0%