Sum	128-bit					256-bit					1024-bit				
c	128	64	8	1	1^{KSMB}	256	128	16	1	1^{KSMB}	1024	512	32	1	1^{KSMB}
Total gates	5	10	80	634	1,443	5	10	80	1,274	2,951	5	10	160	5,114	11,999
Non-XOR	1	2	16	127	345	1	2	16	255	721	1	2	32	1,023	2,977
CS (B)	512	512	512	508	1,380	1,024	1,024	1,024	1,020	2,884	4,096	4,096	4,096	4,092	11,908
PFC	120	240	1,920	15,216	34,632	120	240	1,920	30,576	70,824	120	240	3,840	122,736	287,976
CSE	126.8	63.4	7.9	1.0	-	254.8	127.4	15.9	1.0	-	1022.8	511.4	32.0	1.0	-
PFD	1%	1%	1%	0%	-	0%	0%	0%	0%	-	0%	0%	0%	0%	-
CSE^{KSMB}	288.6	144.3	18.0	2.3	1.0	590.2	295.1	36.9	2.3	1.0	2399.8	1199.9	75.0	2.3	1.0
PFD^{KSMB}	-63%	-63%	-63%	-63%	0%	-64%	-64%	-64%	-65%	0%	-66%	-66%	-66%	-66%	0%