

Function	PCF (*FastGC)		TinyGarble: Combinational			
	Non-XOR	Total gates	Non-XOR	Total gates	GTD <sup>PCF</sup>	MFE <sup>PCF</sup>
Sum 128	345	1,443	127	634	-63.2%	2.3
Sum 256	721	2,951	255	1,274	-64.6%	2.3
Sum 1024	2,977	11,999	1,023	5,114	-65.6%	2.3
Hamming 160	880	4,368	158	1,039	-82.0%	4.2
Hamming 1600	6,375	32,912	1,597	10,679	-74.9%	3.1
Hamming 16000	97,175	389,312	15,994	107,226	-83.5%	3.6
Compare 16384	32,229	97,733	16,384	65,536	-49.2%	1.5
Mult 64	24,766	105,880	3,925	11,439	-84.2%	9.3
Mult 128	100,250	423,064	16,046	47,620	-84.0%	8.9
Mult 256	400,210	1.66E+06	-	-	-	-
Mult 1024	6.37E+06	2.56E+07	-	-	-	-
MatxMult 3x3	27,369	92,961	27,369	91,305	0.0%	1.0
MatxMult 5x5	127,225	433,475	127,225	425,775	0.0%	1.0
MatxMult 8x8	522,304	1.78E+06	-	-	-	-
MatxMult 16x16	4.19E+06	1.43E+07	-	-	-	-
AES 128	5,760*	36,048*	5,760	29,811	0.0%	1.2
SHA3 1600	-	-	38,400	160,054	-	-