Table 2: Optimization results. We show the relative improvements in % for the multiplication (top) and squaring (bottom) operations; time savings are marked in blue. First, to observe hardware-specific optimization, the 9-by-9 matrix shows the performance the optimized operation that have been optimized on one machine and then run on another. The subsequent two rows (Clang/GCC) then show the time savings of our optimized operations over off-the-shelf-compilers. Lastly, "Final" shows the time savings of our best-performing implementation over the best-performing compiler-generated version.

BLS12-381 q

run on / opt on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 13G	G.M.
1900X		1.14	1.33	1.02	1.60	1.58	1.61	1.52	1.02	1.29
5800X	0.94		1.16	0.91	1.51	1.49	1.52	1.24	0.90	1.16
5950X	0.85	0.86		0.79	1.22	1.20	1.25	1.12	0.79	0.99
7950X	1.02	1.12	1.31		1.69	1.66	1.69	1.47	1.00	1.30
i7 6G	0.76	0.83	0.96	0.74		0.98	1.01	0.95	0.68	0.87
i7 10G	0.78	0.85	0.97	0.76	1.01		1.03	0.96	0.67	0.88
i9 10G	0.76	0.83	0.97	0.74	0.99	0.97		0.93	0.67	0.87
i7 11G	0.81	0.86	1.00	0.76	1.08	1.05	1.10		0.71	0.92
i9 13G	1.07	1.20	1.38	1.07	1.71	1.68	1.72	1.45		1.34
Clang	1.42	1.52	1.77	1.20	2.23	2.18	2.24	2.07	1.58	1.76
GCC	1.94	1.75	2.04	1.58	3.62	3.49	3.64	3.47	2.27	2.51
Final	1.87	1.85	1.85	1.61	2.25	2.24	2.24	2.22	2.36	2.04
1900X		1.21	1.31	1.12	1.75	1.75	1.81	1.60	1.14	1.38
5800X	0.86		1.08	0.94	1.46	1.43	1.49	1.38	0.94	1.15
5950X	0.79	0.93		0.88	1.31	1.29	1.36	1.23	0.85	1.05
7950X	0.90	1.09	1.17		1.63	1.68	1.67	1.55	1.05	1.27
i7 6G	0.68	0.84	0.92	0.81		1.03	1.03	1.07	0.69	0.89
i7 10G	0.68	0.83	0.90	0.79	0.97		0.99	1.05	0.67	0.87
i9 10G	0.67	0.82	0.89	0.78	0.98	1.02		1.06	0.69	0.87
i7 11G	0.68	0.81	0.88	0.77	0.98	1.02	1.01		0.66	0.86
i9 13G	0.97	1.13	1.23	1.06	1.64	1.68	1.68	1.49		1.29
Clang	1.21	1.58	1.71	1.28	2.15	2.19	2.21	2.07	1.63	1.74
GCC	1.80	2.11	2.27	1.65	3.54	3.65	3.64	3.72	2.25	2.61
Final	1.80	1.94	1.94	1.66	2.20	2.19	2.23	2.07	2.46	2.04

BLS12-381 p

run on / opt on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 13G	G.M.
1900X		1.04	1.05	1.06	0.97	1.05	1.02	1.07	1.08	1.04
5800X	1.06		1.00	1.04	1.00	1.07	1.03	1.09	1.03	1.03
5950X	1.09	1.00		1.05	1.02	1.11	1.08	1.15	1.14	1.07
7950X	1.05	1.00	1.01		0.99	1.08	1.05	1.10	1.08	1.04
i7 6G	1.10	1.08	1.08	1.14		1.10	1.06	1.12	1.10	1.09
i7 10G	1.08	1.04	1.05	1.06	0.92		0.97	1.09	1.04	1.03
i9 10G	1.08	1.05	1.06	1.07	0.95	1.04		1.11	1.08	1.05
i7 11G	1.03	1.03	1.03	1.05	0.94	1.04	1.00		1.00	1.01
i9 13G	1.09	1.10	1.09	1.11	1.01	1.12	1.07	1.10		1.08
Clang	1.78	1.68	1.68	1.63	1.73	1.87	1.81	1.95	2.09	1.80
GCC	2.34	2.03	2.04	2.06	2.77	2.99	2.91	2.78	3.11	2.52
Final	1.78	1.68	1.68	1.63	1.88	1.87	1.86	1.95	2.10	1.82
1900X		1.05	1.09	1.08	1.05	1.05	1.03	1.05	1.02	1.05
5800X	1.11		1.04	1.05	1.09	1.11	1.08	1.12	1.11	1.08
5950X	1.05	0.97		1.00	1.06	1.07	1.06	1.09	1.10	1.04
7950X	1.08	1.00	1.03		1.05	1.06	1.03	1.11	1.07	1.05
i7 6G	1.07	1.02	1.06	1.07		1.01	0.99	1.05	1.01	1.03
i7 10G	1.11	1.04	1.08	1.07	0.99		0.99	1.02	1.00	1.03
i9 10G	1.05	1.03	1.07	1.07	0.97	0.98		1.02	0.99	1.02
i7 11G	1.10	1.08	1.12	1.11	1.08	1.09	1.08		1.00	1.07
i9 13G	1.12	1.13	1.17	1.15	1.14	1.15	1.13	1.08		1.12
Clang	1.68	1.68	1.74	1.49	1.83	1.84	1.81	1.79	1.72	1.73
GCC	2.29	1.98	2.06	2.04	2.90	2.88	2.89	2.59	2.76	2.46
Final	1.68	1.73	1.74	1.49	1.88	1.88	1.83	1.79	1.75	1.75

Table 1: Geometric means of CryptOpt vs. off-the-shelf compilers.

	Multiply		Square	
Curve	Clang	GCC	Clang	GCC
BLS12-381 q	1.76	2.51	1.74	2.61
BLS12-381 p	1.80	2.52	1.73	2.46