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.

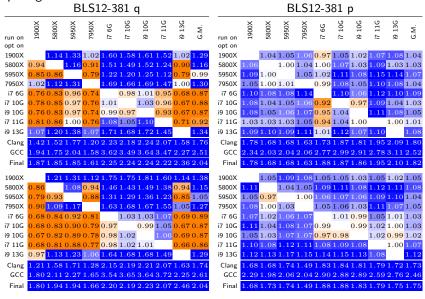


Table 1: Geometric means of CryptOpt vs. off-the-shelf compilers.

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