Table 2: Optimisation matrix for Curve 25519  $\,$ 

					Cur	ve25	519					
	run on	1900X	2800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.05	1.10	1.11	1.10	1.07	1.09	1.09	1.20	1.17	1.10
	5800X	1.19		1.05	1.06	1.14	1.11	1.13	1.13	1.17	1.14	1.11
	5950X	1.18	0.95		1.03	1.10	1.07	1.09	1.10	1.15	1.11	1.08
	7950X	1.10	0.97	1.01		1.06	1.03	1.05	1.05	1.05	1.02	1.03
X	i7 6G	1.12	1.04	1.10	1.08		0.97	0.99	1.00	1.09	1.05	1.04
Multiply	i7 10G	1.14	1.09	1.12	1.12	1.03		1.02	1.06	1.22	1.18	1.10
ILT	i9 10G	1.14	1.09	1.16	1.14	1.00	0.97		1.02	1.11	1.08	1.07
Μſ	i7 11G	1.13	1.03	1.08	1.12	1.09	1.06	1.08		1.05	1.03	1.07
	i9 12G	1.15	1.03	1.08	1.07	1.08	1.05	1.07	1.01		0.97	1.05
	i9 13G	1.15	1.08	1.13	1.10	1.08	1.05	1.08	1.03	1.03		1.07
	Clang	1.30	1.24	1.31	1.27	1.33	1.29	1.32	1.29	1.24	1.18	1.28
	GCC	1.11	1.17	1.23	1.30	1.17	1.14	1.16	1.14	1.16	1.12	1.17
	Final	1.11	1.23	1.23	1.27	1.17	1.17	1.17	1.14	1.16	1.16	1.18
	1900X		1.08	1.06	1.09	1.03	1.05	1.10	1.07	1.12	1.12	1.07
	5800X	1.11		1.00	1.02	1.03	1.05	1.10	1.06	1.08	1.08	1.05
	5950X	1.10	1.00		1.03	1.07	1.10	1.15	1.08	1.18	1.18	1.09
	7950X	1.10	1.01	1.00		1.05	1.04	1.09	1.11	1.10	1.09	1.06
囝	i7 6G	1.12	1.12	1.11	1.17	0.00	1.02	1.07	1.06	1.06	1.06	1.08
AR	i7 10G	1.19	1.11	1.11	1.13	0.98	0.00	1.05	1.05	1.06	1.06	1.07
SQUARE	i9 10G	1.09	1.09	1.08	1.06	0.94	0.96	1.00	1.02	1.02	1.02	1.03
$\infty$	i7 11G	1.13	1.09	1.08	1.16	1.01	1.03	1.08	0.00	1.34	1.33	1.12
	i9 12G	1.07 1.10	1.02	1.02	1.05	0.98	1.00	1.04	0.99	1 01	0.99	1.02
	i9 13G		1.03	1.03	1.07	0.99	1.01	1.06	1.01	1.01		1.03
	Clang	1.25	1.21	1.19	1.24	1.19	1.22	1.26	1.18	1.19	1.28	1.22
	GCC	1.19	1.21	1.21	1.22	1.06	1.08	1.12	1.09	1.16	1.15	1.15
	Final	1.19	1.21	1.20	1.22	1.12	1.12	1.12	1.11	1.16	1.16	1.16

Table 1: Geometric means of  ${\sf CryptOpt}$  vs. off-the-shelf compilers.

	Mult	iply	Squ	are
Curve	Clang	GCC	Clang	GCC
Curve25519	1.28	1.17	1.22	1.15
Curve25519-Solinas	1.65	2.59	1.44	2.77
P-224	1.61	2.65	1.45	2.63
P-256	1.75	2.68	1.69	2.63
P-384	1.51	2.59	1.41	2.61
SIKEp434	2.05	2.96	1.88	2.65
Curve448	1.21	1.00	1.09	1.05
P-521	1.35	1.03	1.39	1.09
Poly1305	1.16	1.22	1.13	1.26
secp256k1-Dettman	1.10	1.24	1.06	1.14
secp256k1	1.88	2.72	1.81	2.66

Table 3: Optimisation matrix for Curve25519-Solinas

		1900X	5800X	5950X	7950X	99	10G	10G	11G	12G	13G	G.M.
	run on	19	58	59	79,	17	17	19	17	19	19	Ü
	opt on											
	1900X		1.08	1.08	1.08	1.09	1.09	1.09	1.10	1.08	1.09	1.08
	5800X	1.06		1.00	1.04	1.07	1.07	1.07	1.11	1.05	1.05	1.05
	5950X	1.07	1.00		1.03	1.05	1.05	1.05	1.03	1.04	1.04	1.03
	7950X	1.07	1.03	1.03		1.04	1.04	1.05	1.03	1.00	1.00	1.03
≻	i7~6G	1.09	1.13	1.12	1.09		1.00	1.00	1.04	1.02	1.02	1.05
[PL	i7 10G	1.08	1.10	1.09	1.04	1.00		1.00	1.03	1.01	1.01	1.03
E	i9 10G	1.07	1.09	1.09	1.08	1.00	1.00		1.03	1.01	1.01	1.04
Multiply	i7 11G	1.08	1.13	1.13	1.10	1.02	1.02	1.03		1.01	1.01	1.05
	i9 12G	1.06	1.07	1.07	1.08	1.02	1.02	1.02	1.04		1.00	1.04
	i9 13G	1.06	1.08	1.08	1.05	1.00	1.00	1.00	1.06	1.00		1.03
	Clang	1.66	1.81	1.81	1.77	1.50	1.50	1.50	1.75	1.60	1.62	1.65
	$\widetilde{\operatorname{GCC}}$	2.36	2.38	2.38	2.31	2.76	2.76	2.76	2.74	2.76	2.76	2.59
	Final	1.66	1.81	1.81	1.77	1.50	1.50	1.50	1.75	1.61	1.62	1.65
	Final	1.66	1.81	1.81	1.77	1.50	1.50	1.50	1.75	1.61	1.62	1.65
	Final 1900X	1.66	1.81	1.81	1.77	1.50	1.50	1.50	1.75	1.61	1.62	1.65
		1.66									1.06 1.10	
	1900X			1.09 1.01	1.09	1.03	1.03	1.06	1.07	1.10	1.06	1.06
	1900X 5800X 5950X 7950X	1.05 1.05 1.04	1.09 1.00 1.08	1.09 1.01 1.08	1.09 0.97	1.03 1.06	1.03 1.06	1.06 1.09	1.07 1.07	1.10 1.14 1.10 1.13	1.06 1.10 1.06 1.09	1.06 1.05
	1900X 5800X 5950X 7950X i7 6G	1.05 1.05 1.04 1.06	1.09 1.00 1.08 1.12	1.09 1.01 1.08 1.13	1.09 0.97 0.93	1.03 1.06 1.00	1.03 1.06 1.00	1.06 1.09 1.03	1.07 1.07 1.06	1.10 1.14 1.10 1.13 1.11	1.06 1.10 1.06 1.09 1.08	1.06 1.05 1.02
\RE	1900X 5800X 5950X 7950X i7 6G i7 10G	1.05 1.05 1.04 1.06 1.05	1.09 1.00 1.08 1.12 1.09	1.09 1.01 1.08 1.13 1.10	1.09 0.97 0.93 1.09 1.04	1.03 1.06 1.00	1.03 1.06 1.00 1.03 1.00	1.06 1.09 1.03 1.06	1.07 1.07 1.06 1.05	1.10 1.14 1.10 1.13 1.11 1.09	1.06 1.10 1.06 1.09 1.08 1.06	1.06 1.05 1.02 1.06
JUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G	1.05 1.05 1.04 1.06 1.05 1.04	1.09 1.00 1.08 1.12 1.09 1.09	1.09 1.01 1.08 1.13 1.10 1.09	1.09 0.97 0.93 1.09 1.04 1.02	1.03 1.06 1.00 1.03 1.00 0.97	1.03 1.06 1.00 1.03 1.00	1.06 1.09 1.03 1.06 1.03 1.03	1.07 1.07 1.06 1.05 1.02	1.10 1.14 1.10 1.13 1.11 1.09 1.06	1.06 1.10 1.06 1.09 1.08 1.06 1.02	1.06 1.05 1.02 1.06 1.06 1.05 1.03
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	1.05 1.05 1.04 1.06 1.05 1.04 1.06	1.09 1.00 1.08 1.12 1.09	1.09 1.01 1.08 1.13 1.10 1.09 1.11	1.09 0.97 0.93 1.09 1.04	1.03 1.06 1.00 1.03 1.00 0.97 1.00	1.03 1.06 1.00 1.03 1.00 0.97 1.00	1.06 1.09 1.03 1.06 1.03 1.03	1.07 1.07 1.06 1.05 1.02 1.04 1.05	1.10 1.14 1.10 1.13 1.11 1.09	1.06 1.10 1.06 1.09 1.08 1.06 1.02 1.04	1.06 1.05 1.02 1.06 1.06 1.05 1.03 1.05
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	1.05 1.05 1.04 1.06 1.05 1.04 1.06	1.09 1.00 1.08 1.12 1.09 1.09 1.11 1.14	1.09 1.01 1.08 1.13 1.10 1.09 1.11 1.15	1.09 0.97 0.93 1.09 1.04 1.02 1.07	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00	1.06 1.09 1.03 1.06 1.03 1.03 1.03	1.07 1.07 1.06 1.05 1.02 1.04 1.05	1.10 1.14 1.10 1.13 1.11 1.09 1.06 1.07	1.06 1.10 1.06 1.09 1.08 1.06 1.02	1.06 1.05 1.02 1.06 1.06 1.05 1.03 1.05 1.05
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	1.05 1.05 1.04 1.06 1.05 1.04 1.06	1.09 1.00 1.08 1.12 1.09 1.09	1.09 1.01 1.08 1.13 1.10 1.09 1.11	1.09 0.97 0.93 1.09 1.04 1.02 1.07	1.03 1.06 1.00 1.03 1.00 0.97 1.00	1.03 1.06 1.00 1.03 1.00 0.97 1.00	1.06 1.09 1.03 1.06 1.03 1.03	1.07 1.07 1.06 1.05 1.02 1.04 1.05	1.10 1.14 1.10 1.13 1.11 1.09 1.06	1.06 1.10 1.06 1.09 1.08 1.06 1.02 1.04	1.06 1.05 1.02 1.06 1.06 1.05 1.03 1.05
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	1.05 1.05 1.04 1.06 1.05 1.04 1.06	1.09 1.00 1.08 1.12 1.09 1.09 1.11 1.14	1.09 1.01 1.08 1.13 1.10 1.09 1.11 1.15	1.09 0.97 0.93 1.09 1.04 1.02 1.07	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00	1.06 1.09 1.03 1.06 1.03 1.03 1.03	1.07 1.07 1.06 1.05 1.02 1.04 1.05	1.10 1.14 1.10 1.13 1.11 1.09 1.06 1.07	1.06 1.10 1.06 1.09 1.08 1.06 1.02 1.04	1.06 1.05 1.02 1.06 1.06 1.05 1.03 1.05 1.05
$S_{QUARE}$	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G	1.05 1.05 1.04 1.06 1.05 1.04 1.06 1.04	1.09 1.00 1.08 1.12 1.09 1.09 1.11 1.14 1.09	1.09 1.01 1.08 1.13 1.10 1.09 1.11 1.15	1.09 0.97 0.93 1.09 1.04 1.02 1.07 1.11	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00	1.03 1.06 1.00 1.03 1.00 0.97 1.00 1.00 1.03	1.06 1.09 1.03 1.06 1.03 1.03 1.03 1.03	1.07 1.07 1.06 1.05 1.02 1.04 1.05	1.10 1.14 1.10 1.13 1.11 1.09 1.06 1.07	1.06 1.10 1.06 1.09 1.08 1.06 1.02 1.04 0.97	1.06 1.05 1.02 1.06 1.06 1.05 1.03 1.05 1.05 1.05

Table 4: Optimisation matrix for P-224

	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.03	1.06	1.07	1.03	0.99	1.07	1.09	1.00	1.01	1.03
	5800X	1.15		1.03	1.08	1.15	1.10	1.20	1.22	1.20	1.21	1.13
	5950X	1.07	0.96		1.00	1.10	1.06	1.15	1.15	1.09	1.10	1.07
	7950X	1.10	1.00	1.03		1.06	1.02	1.11	1.20	1.07	1.08	1.07
$\succ$	i7~6G	1.07	1.04	1.07	1.09		0.96	1.04	1.13	1.03	1.03	1.04
Мистірсу	i7 10G	1.11	1.03	1.06	1.07	1.04		1.09	1.11	0.99	0.99	1.05
5	i9 10G	1.06	1.01	1.05	1.05	0.96	0.92		1.08	1.02	1.03	1.02
$ m M_{ m U}$	i7 11G	1.07	1.01	1.05	1.04	1.01	0.97	1.06		0.98	0.99	1.02
	i9 12G	1.09	1.03	1.06	1.06	1.06	1.01	1.10	1.11		1.01	1.05
	i9 13G	1.07	1.03	1.06	1.07	1.05	1.00	1.09	1.10	0.99		1.04
	Clang	1.63	1.48	1.52	1.47	1.64	1.56	1.71	1.74	1.69	1.69	1.61
	$\widetilde{\operatorname{GCC}}$	2.49	2.11	2.18	2.13	2.95	2.82	3.07	2.94	3.01	3.09	2.65
	Final	1.62	1.5/	1.59	1 47	1 71	1.70	1 71	1 7/	1 72	1 71	1.64
	Final	1.63	1.54	1.52	1.47	1.71	1.70	1.71	1.74	1.73	1.71	1.64
		1.63										
	1900X		1.54	1.08	1.06	0.99	1.00	1.01	1.02	1.01	0.93	1.02
	1900X 5800X	1.08	1.08		1.06 0.98	0.99 1.02	1.00 1.03	1.01 1.05	1.02 1.04	1.01 1.05	0.93 0.96	1.02 1.02
	1900X 5800X 5950X	1.08 1.09	1.08	1.08 1.00	1.06	0.99 1.02 1.05	1.00 1.03 1.06	1.01 1.05 1.08	1.02 1.04 1.08	1.01 1.05 1.11	0.93 0.96 1.02	1.02 1.02 1.05
	1900X 5800X 5950X 7950X	1.08 1.09 1.11	1.08 1.00 1.07	1.08 1.00	1.06 0.98 1.00	0.99 1.02	1.00 1.03 1.06 1.08	1.01 1.05 1.08 1.09	1.02 1.04 1.08 1.09	1.01 1.05 1.11 1.06	0.93 0.96 1.02 0.97	1.02 1.02 1.05 1.06
3.E	1900X 5800X 5950X 7950X i7 6G	1.08 1.09 1.11 1.06	1.08 1.00 1.07 1.08	1.08 1.00 1.05 1.07	1.06 0.98 1.00	0.99 1.02 1.05 1.06	1.00 1.03 1.06	1.01 1.05 1.08 1.09 1.03	1.02 1.04 1.08 1.09 1.00	1.01 1.05 1.11 1.06 1.01	0.93 0.96 1.02 0.97 0.93	1.02 1.02 1.05 1.06 1.02
JARE	1900X 5800X 5950X 7950X i7 6G i7 10G	1.08 1.09 1.11 1.06 1.07	1.08 1.00 1.07 1.08 1.09	1.08 1.00 1.05 1.07 1.09	1.06 0.98 1.00 1.03 1.05	0.99 1.02 1.05 1.06	1.00 1.03 1.06 1.08 1.01	1.01 1.05 1.08 1.09	1.02 1.04 1.08 1.09 1.00 1.05	1.01 1.05 1.11 1.06 1.01 1.04	0.93 0.96 1.02 0.97 0.93 0.95	1.02 1.02 1.05 1.06 1.02 1.03
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G	1.08 1.09 1.11 1.06 1.07 1.10	1.08 1.00 1.07 1.08 1.09 1.06	1.08 1.00 1.05 1.07 1.09 1.06	1.06 0.98 1.00 1.03 1.05 1.02	0.99 1.02 1.05 1.06 0.99 0.97	1.00 1.03 1.06 1.08 1.01	1.01 1.05 1.08 1.09 1.03 1.01	1.02 1.04 1.08 1.09 1.00	1.01 1.05 1.11 1.06 1.01 1.04 1.02	0.93 0.96 1.02 0.97 0.93 0.95 0.93	1.02 1.02 1.05 1.06 1.02 1.03 1.02
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	1.08 1.09 1.11 1.06 1.07	1.08 1.00 1.07 1.08 1.09 1.06 1.11	1.08 1.00 1.05 1.07 1.09 1.06 1.11	1.06 0.98 1.00 1.03 1.05	0.99 1.02 1.05 1.06 0.99 0.97	1.00 1.03 1.06 1.08 1.01 0.99 1.07	1.01 1.05 1.08 1.09 1.03 1.01	1.02 1.04 1.08 1.09 1.00 1.05 1.06	1.01 1.05 1.11 1.06 1.01 1.04	0.93 0.96 1.02 0.97 0.93 0.95 0.93	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G	1.08 1.09 1.11 1.06 1.07 1.10 1.10	1.08 1.00 1.07 1.08 1.09 1.06	1.08 1.00 1.05 1.07 1.09 1.06	1.06 0.98 1.00 1.03 1.05 1.02 1.09	0.99 1.02 1.05 1.06 0.99 0.97	1.00 1.03 1.06 1.08 1.01	1.01 1.05 1.08 1.09 1.03 1.01	1.02 1.04 1.08 1.09 1.00 1.05	1.01 1.05 1.11 1.06 1.01 1.04 1.02	0.93 0.96 1.02 0.97 0.93 0.95 0.93	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06 1.04
$S_{QUARE}$	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G	1.08 1.09 1.11 1.06 1.07 1.10 1.10 1.15	1.08 1.00 1.07 1.08 1.09 1.06 1.11 1.10 1.16	1.08 1.00 1.05 1.07 1.09 1.06 1.11 1.10	1.06 0.98 1.00 1.03 1.05 1.02 1.09 1.06 1.13	0.99 1.02 1.05 1.06 0.99 0.97 1.06 1.03	1.00 1.03 1.06 1.08 1.01 0.99 1.07 1.04 1.13	1.01 1.05 1.08 1.09 1.03 1.01 1.09 1.06 1.15	1.02 1.04 1.08 1.09 1.00 1.05 1.06	1.01 1.05 1.11 1.06 1.01 1.04 1.02 1.04	0.93 0.96 1.02 0.97 0.93 0.95 0.93 0.95 0.92	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06 1.04
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang	1.08 1.09 1.11 1.06 1.07 1.10 1.10 1.15	1.08 1.00 1.07 1.08 1.09 1.06 1.11 1.10 1.16	1.08 1.00 1.05 1.07 1.09 1.06 1.11 1.10 1.16	1.06 0.98 1.00 1.03 1.05 1.02 1.09 1.06 1.13	0.99 1.02 1.05 1.06 0.99 0.97 1.06 1.03 1.12	1.00 1.03 1.06 1.08 1.01 0.99 1.07 1.04 1.13	1.01 1.05 1.08 1.09 1.03 1.01 1.09 1.06 1.15	1.02 1.04 1.08 1.09 1.00 1.05 1.06 1.02 1.12	1.01 1.05 1.11 1.06 1.01 1.04 1.02 1.04 1.09	0.93 0.96 1.02 0.97 0.93 0.95 0.93 0.95 0.92	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06 1.04 1.12
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang GCC	1.08 1.09 1.11 1.06 1.07 1.10 1.10 1.15 1.42 2.46	1.08 1.00 1.07 1.08 1.09 1.06 1.11 1.10 1.16 1.45 2.22	1.08 1.00 1.05 1.07 1.09 1.06 1.11 1.10 1.16	1.06 0.98 1.00 1.03 1.05 1.02 1.09 1.06 1.13 1.34 2.09	0.99 1.02 1.05 1.06 0.99 0.97 1.06 1.03 1.12	1.00 1.03 1.06 1.08 1.01 0.99 1.07 1.04 1.13	1.01 1.05 1.08 1.09 1.03 1.01 1.09 1.06 1.15 1.51 2.97	1.02 1.04 1.08 1.09 1.00 1.05 1.06 1.02 1.12	1.01 1.05 1.11 1.06 1.01 1.04 1.02 1.04 1.09 1.55 3.14	0.93 0.96 1.02 0.97 0.93 0.95 0.93 0.95 0.92	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06 1.04 1.12 1.45 2.63
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang	1.08 1.09 1.11 1.06 1.07 1.10 1.10 1.15	1.08 1.00 1.07 1.08 1.09 1.06 1.11 1.10 1.16	1.08 1.00 1.05 1.07 1.09 1.06 1.11 1.10 1.16	1.06 0.98 1.00 1.03 1.05 1.02 1.09 1.06 1.13	0.99 1.02 1.05 1.06 0.99 0.97 1.06 1.03 1.12	1.00 1.03 1.06 1.08 1.01 0.99 1.07 1.04 1.13	1.01 1.05 1.08 1.09 1.03 1.01 1.09 1.06 1.15	1.02 1.04 1.08 1.09 1.00 1.05 1.06 1.02 1.12	1.01 1.05 1.11 1.06 1.01 1.04 1.02 1.04 1.09	0.93 0.96 1.02 0.97 0.93 0.95 0.93 0.95 0.92	1.02 1.02 1.05 1.06 1.02 1.03 1.02 1.06 1.04 1.12

Table 5: Optimisation matrix for P-256

_	_		_
1.	$\alpha$	$\overline{}$	$\boldsymbol{\Gamma}$
$\boldsymbol{\mathcal{L}}$	٠,	h	$\sim$

					-	200	,					
	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.02	1.03	1.09	1.02	1.05	1.07	1.08	1.01	0.99	1.03
	5800X	1.11		1.00	1.09	1.06	1.10	1.11	1.17	1.05	1.03	1.07
	5950X	1.10	0.98		1.09	1.10	1.13	1.15	1.12	1.09	1.07	1.08
	7950X	1.01	0.96	0.97		1.00	1.03	1.05	1.05	1.02	1.00	1.01
>	i7 6G	1.10	1.05	1.08	1.12		1.03	1.05	1.14	1.06	1.05	1.07
Multiply	i7 10G	1.04	1.02	1.04	1.08	0.97		1.02	1.09	1.03	1.02	1.03
E	i9 10G	1.01	0.99	1.01	1.04	0.95	0.98		1.02	0.99	0.97	1.00
ΔΩ	i7 11G	1.04	1.03	1.04	1.09	0.98	1.02	1.08		1.00	0.98	1.03
	i9 12G	1.10	1.07	1.09	1.13	1.06	1.10	1.11	1.08		0.99	1.07
	i9 13G	1.11	1.11	1.12	1.16	1.06	1.10	1.12	1.13	1.02		1.09
	Clang	1.63	1.73	1.76	1.69	1.70	1.76	1.79	1.88	1.76	1.76	1.75
	$\widetilde{\mathrm{GCC}}$	2.53	2.19	2.23	2.28	2.96	3.06	3.10	2.95	2.89	2.88	2.68
	Final	1 63	1.81	1.81	1 69	1 79	1 79	1 79	1.88	1 79	1.81	1 78
	Final	1.63	1.81	1.81	1.69	1.79	1.79	1.79	1.88	1.79	1.81	1.78
		1.63										
	1900X		1.81	1.08	1.05	1.02	1.05	1.06	0.99	1.06	1.04	1.04
	1900X 5800X	1.12	1.05		1.05 1.04	1.02 1.06	1.05 1.09	1.06 1.10	0.99 1.03	1.06 1.10	1.04 1.07	1.04 1.06
	1900X 5800X 5950X	1.12 1.09	1.05 0.97	1.08 1.03	1.05	1.02 1.06 1.03	1.05 1.09 1.07	1.06 1.10 1.07	0.99 1.03 0.99	1.06 1.10 1.11	1.04 1.07 1.08	1.04 1.06 1.04
	1900X 5800X 5950X 7950X	1.12 1.09 1.11	1.05 0.97 0.99	1.08 1.03	1.05 1.04 1.00	1.02 1.06	1.05 1.09 1.07 1.05	1.06 1.10 1.07 1.05	0.99 1.03 0.99 1.04	1.06 1.10 1.11 1.06	1.04 1.07 1.08 1.03	1.04 1.06 1.04 1.04
RE	1900X 5800X 5950X	1.12 1.09	1.05 0.97	1.08 1.03	1.05 1.04	1.02 1.06 1.03	1.05 1.09 1.07	1.06 1.10 1.07	0.99 1.03 0.99	1.06 1.10 1.11	1.04 1.07 1.08	1.04 1.06 1.04
UARE	1900X 5800X 5950X 7950X i7 6G	1.12 1.09 1.11 1.14	1.05 0.97 0.99 1.12	1.08 1.03 1.02 1.15	1.05 1.04 1.00	1.02 1.06 1.03 1.01	1.05 1.09 1.07 1.05	1.06 1.10 1.07 1.05 1.04	0.99 1.03 0.99 1.04 1.00	1.06 1.10 1.11 1.06 1.09	1.04 1.07 1.08 1.03 1.07	1.04 1.06 1.04 1.04 1.07
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G	1.12 1.09 1.11 1.14 1.09	1.05 0.97 0.99 1.12 1.01	1.08 1.03 1.02 1.15 1.04	1.05 1.04 1.00 1.10 1.04	1.02 1.06 1.03 1.01	1.05 1.09 1.07 1.05 1.03	1.06 1.10 1.07 1.05 1.04	0.99 1.03 0.99 1.04 1.00 1.00	1.06 1.10 1.11 1.06 1.09 1.05	1.04 1.07 1.08 1.03 1.07 1.02	1.04 1.06 1.04 1.04 1.07 1.02
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G	1.12 1.09 1.11 1.14 1.09 1.09	1.05 0.97 0.99 1.12 1.01 1.09	1.08 1.03 1.02 1.15 1.04 1.12	1.05 1.04 1.00 1.10 1.04 1.12	1.02 1.06 1.03 1.01 0.97 0.97	1.05 1.09 1.07 1.05 1.03	1.06 1.10 1.07 1.05 1.04 1.00	0.99 1.03 0.99 1.04 1.00 1.00	1.06 1.10 1.11 1.06 1.09 1.05 1.06	1.04 1.07 1.08 1.03 1.07 1.02 1.03	1.04 1.06 1.04 1.04 1.07 1.02
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	1.12 1.09 1.11 1.14 1.09 1.09	1.05 0.97 0.99 1.12 1.01 1.09 1.14	1.08 1.03 1.02 1.15 1.04 1.12 1.17	1.05 1.04 1.00 1.10 1.04 1.12 1.16	1.02 1.06 1.03 1.01 0.97 0.97 1.06	1.05 1.09 1.07 1.05 1.03 1.00	1.06 1.10 1.07 1.05 1.04 1.00	0.99 1.03 0.99 1.04 1.00 1.00	1.06 1.10 1.11 1.06 1.09 1.05 1.06	1.04 1.07 1.08 1.03 1.07 1.02 1.03 1.09	1.04 1.06 1.04 1.04 1.07 1.02 1.04
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G	1.12 1.09 1.11 1.14 1.09 1.09 1.15 1.09	1.05 0.97 0.99 1.12 1.01 1.09 1.14 1.05 1.04	1.08 1.03 1.02 1.15 1.04 1.12 1.17 1.07	1.05 1.04 1.00 1.10 1.04 1.12 1.16 1.07	1.02 1.06 1.03 1.01 0.97 0.97 1.06 1.02	1.05 1.09 1.07 1.05 1.03 1.00 1.10 1.05 1.05	1.06 1.10 1.07 1.05 1.04 1.00 1.10 1.05 1.05	0.99 1.03 0.99 1.04 1.00 0.96	1.06 1.10 1.11 1.06 1.09 1.05 1.06 1.11	1.04 1.07 1.08 1.03 1.07 1.02 1.03 1.09 0.97	1.04 1.06 1.04 1.04 1.07 1.02 1.04 1.11 1.04
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	1.12 1.09 1.11 1.14 1.09 1.09 1.15 1.09	1.05 0.97 0.99 1.12 1.01 1.09 1.14 1.05	1.08 1.03 1.02 1.15 1.04 1.12 1.17	1.05 1.04 1.00 1.10 1.04 1.12 1.16 1.07	1.02 1.06 1.03 1.01 0.97 0.97 1.06 1.02	1.05 1.09 1.07 1.05 1.03 1.00 1.10 1.05	1.06 1.10 1.07 1.05 1.04 1.00 1.10	0.99 1.03 0.99 1.04 1.00 1.00 0.96	1.06 1.10 1.11 1.06 1.09 1.05 1.06	1.04 1.07 1.08 1.03 1.07 1.02 1.03 1.09	1.04 1.06 1.04 1.04 1.07 1.02 1.04 1.11
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang	1.12 1.09 1.11 1.14 1.09 1.09 1.15 1.09 1.07	1.05 0.97 0.99 1.12 1.01 1.09 1.14 1.05 1.04	1.08 1.03 1.02 1.15 1.04 1.12 1.17 1.07 1.07	1.05 1.04 1.00 1.10 1.04 1.12 1.16 1.07 1.10	1.02 1.06 1.03 1.01 0.97 0.97 1.06 1.02 1.02	1.05 1.09 1.07 1.05 1.03 1.00 1.10 1.05 1.05	1.06 1.10 1.07 1.05 1.04 1.00 1.10 1.05 1.05	0.99 1.03 0.99 1.04 1.00 0.96 1.00 0.96	1.06 1.10 1.11 1.06 1.09 1.05 1.06 1.11 1.03	1.04 1.07 1.08 1.03 1.07 1.02 1.03 1.09 0.97	1.04 1.06 1.04 1.07 1.02 1.04 1.11 1.04 1.69

Table 6: Optimisation matrix for P-384

T	<b>つ</b>	า	O	- 1	ı
I	_	. ``	$\sim$	4	L

	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	run on		23	23		•-	•		•-	•-	•-	Ŭ
	opt on											
	1900X		1.31	1.25	1.26	1.40	1.39	1.48	1.37	0.99	0.92	1.22
	5800X	0.86		0.96	0.97	1.09	1.12	1.15	1.13	0.82	0.77	0.98
	5950X	0.88	1.04		1.00	1.11	1.14	1.18	1.12	0.79	0.73	0.99
	7950X	0.87	1.05	1.01		1.13	1.16	1.19	1.15	0.81	0.75	1.00
$\succeq$	i7 6G	0.83	1.07	1.02	1.04		1.03	1.06	1.08	0.76	0.71	0.95
IPL	i7 10G	0.82	1.00	0.96	1.00	0.97		1.03	1.01	0.76	0.70	0.92
H	i9 10G	0.79	1.04	0.99	1.00	0.95	0.97		1.02	0.74	0.69	0.91
Multiply	i7 11G	0.81	1.00	0.95	0.97	0.98	1.01	1.04		0.73	0.67	0.91
	i9 12G	1.08	1.36	1.31	1.28	1.46	1.51	1.55	1.39		0.93	1.27
	i9 13G	1.07	1.37	1.32	1.32	1.39	1.44	1.47	1.45	1.08		1.28
	Clang	1.16	1.65	1.58	1.40	1.71	1.77	1.81	1.75	1.35	1.15	1.51
	GCC	2.01	2.22	2.13	2.17	3.27	3.33	3.45	3.18	2.42	2.24	2.59
		4 40	4 00	4 00		4 0 4	4 00	4 0 4		4 0 0		4 00
	Final	1.48	1.66	1.66	1.45	1.81	1.82	1.81	1.75	1.86	1.71	1.69
		1.48										
	1900X		1.66	1.28	1.32	1.44	1.43	1.43	1.39	0.90	0.90	1.22
	1900X 5800X	0.89	1.30		1.32 1.02	1.44 1.18	1.43 1.17	1.43 1.17	1.39 1.18	0.90 0.78	0.90 0.78	1.22 1.00
	1900X 5800X 5950X	0.89 0.86	1.30 1.00	1.28 0.98	1.32	1.44 1.18 1.16	1.43 1.17 1.16	1.43 1.17 1.16	1.39 1.18 1.20	0.90 0.78 0.80	0.90 0.78 0.81	1.22 1.00 1.01
	1900X 5800X 5950X 7950X	0.89 0.86 0.86	1.30 1.00 1.01	1.28 0.98 1.01	1.32 1.02 1.02	1.44 1.18	1.43 1.17 1.16 1.17	1.43 1.17 1.16 1.17	1.39 1.18 1.20 1.16	0.90 0.78 0.80 0.75	0.90 0.78 0.81 0.75	1.22 1.00 1.01 0.99
F1	1900X 5800X 5950X 7950X i7 6G	0.89 0.86 0.86 0.79	1.30 1.00 1.01 1.01	1.28 0.98 1.01 1.00	1.32 1.02 1.02	1.44 1.18 1.16 1.18	1.43 1.17 1.16	1.43 1.17 1.16 1.17 1.00	1.39 1.18 1.20 1.16 1.10	0.90 0.78 0.80 0.75 0.71	0.90 0.78 0.81 0.75 0.71	1.22 1.00 1.01 0.99 0.92
ARE	1900X 5800X 5950X 7950X i7 6G i7 10G	0.89 0.86 0.86 0.79 0.78	1.30 1.00 1.01 1.01 1.02	1.28 0.98 1.01 1.00 1.01	1.32 1.02 1.02 1.04 1.03	1.44 1.18 1.16 1.18	1.43 1.17 1.16 1.17 1.00	1.43 1.17 1.16 1.17	1.39 1.18 1.20 1.16 1.10 1.09	0.90 0.78 0.80 0.75 0.71 0.74	0.90 0.78 0.81 0.75 0.71 0.75	1.22 1.00 1.01 0.99 0.92 0.93
QUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G	0.89 0.86 0.86 0.79 0.78 0.79	1.30 1.00 1.01 1.01 1.02 1.02	1.28 0.98 1.01 1.00 1.01 1.01	1.32 1.02 1.02 1.04 1.03 1.02	1.44 1.18 1.16 1.18 1.00 1.00	1.43 1.17 1.16 1.17 1.00	1.43 1.17 1.16 1.17 1.00 1.00	1.39 1.18 1.20 1.16 1.10	0.90 0.78 0.80 0.75 0.71 0.74	0.90 0.78 0.81 0.75 0.71 0.75 0.73	1.22 1.00 1.01 0.99 0.92 0.93 0.93
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	0.89 0.86 0.86 0.79 0.78 0.79	1.30 1.00 1.01 1.01 1.02 1.02 1.00	1.28 0.98 1.01 1.00 1.01 1.01 0.99	1.32 1.02 1.02 1.04 1.03 1.02 1.00	1.44 1.18 1.16 1.18 1.00 1.00 1.01	1.43 1.17 1.16 1.17 1.00 1.00	1.43 1.17 1.16 1.17 1.00 1.00	1.39 1.18 1.20 1.16 1.10 1.09 1.11	0.90 0.78 0.80 0.75 0.71 0.74	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68	1.22 1.00 1.01 0.99 0.92 0.93 0.93
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	0.89 0.86 0.86 0.79 0.78 0.79 0.80	1.30 1.00 1.01 1.01 1.02 1.02 1.00 1.31	1.28 0.98 1.01 1.00 1.01 1.01 0.99 1.30	1.32 1.02 1.02 1.04 1.03 1.02 1.00	1.44 1.18 1.16 1.18 1.00 1.00 1.01	1.43 1.17 1.16 1.17 1.00 1.00 1.45	1.43 1.17 1.16 1.17 1.00 1.00	1.39 1.18 1.20 1.16 1.10 1.09 1.11	0.90 0.78 0.80 0.75 0.71 0.74 0.73	0.90 0.78 0.81 0.75 0.71 0.75 0.73	1.22 1.00 1.01 0.99 0.92 0.93 0.93 0.90 1.27
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	0.89 0.86 0.86 0.79 0.78 0.79	1.30 1.00 1.01 1.01 1.02 1.02 1.00	1.28 0.98 1.01 1.00 1.01 1.01 0.99	1.32 1.02 1.02 1.04 1.03 1.02 1.00	1.44 1.18 1.16 1.18 1.00 1.00 1.01	1.43 1.17 1.16 1.17 1.00 1.00	1.43 1.17 1.16 1.17 1.00 1.00	1.39 1.18 1.20 1.16 1.10 1.09 1.11	0.90 0.78 0.80 0.75 0.71 0.74	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68	1.22 1.00 1.01 0.99 0.92 0.93 0.93
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G	0.89 0.86 0.86 0.79 0.78 0.79 0.80	1.30 1.00 1.01 1.01 1.02 1.02 1.00 1.31	1.28 0.98 1.01 1.00 1.01 1.01 0.99 1.30 1.31	1.32 1.02 1.02 1.04 1.03 1.02 1.00	1.44 1.18 1.16 1.18 1.00 1.00 1.01 1.46 1.55	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.44	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.54	1.39 1.18 1.20 1.16 1.10 1.09 1.11 1.44 1.53	0.90 0.78 0.80 0.75 0.71 0.74 0.73 0.68	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68 1.01	1.22 1.00 1.01 0.99 0.92 0.93 0.93 0.90 1.27 1.28
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang	0.89 0.86 0.86 0.79 0.78 0.79 0.80 1.04 1.03	1.30 1.00 1.01 1.01 1.02 1.02 1.00 1.31 1.30	1.28 0.98 1.01 1.00 1.01 1.01 0.99 1.30 1.31	1.32 1.02 1.02 1.04 1.03 1.02 1.00 1.32 1.31	1.44 1.18 1.16 1.18 1.00 1.00 1.01 1.46 1.55	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.44	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.54	1.39 1.18 1.20 1.16 1.10 1.09 1.11 1.44 1.53	0.90 0.78 0.80 0.75 0.71 0.74 0.73 0.68	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68 1.01	1.22 1.00 1.01 0.99 0.92 0.93 0.93 0.90 1.27 1.28
$S_{QUARE}$	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang GCC	0.89 0.86 0.86 0.79 0.78 0.79 0.80 1.04 1.03	1.30 1.00 1.01 1.01 1.02 1.02 1.00 1.31 1.30 1.51 2.15	1.28 0.98 1.01 1.00 1.01 1.01 0.99 1.30 1.31 1.50 2.14	1.32 1.02 1.02 1.04 1.03 1.02 1.00 1.32 1.31	1.44 1.18 1.16 1.18 1.00 1.00 1.01 1.46 1.55 1.65 3.51	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.44 1.63 3.48	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.54 1.64 3.49	1.39 1.18 1.20 1.16 1.10 1.09 1.11 1.44 1.53 1.72 3.55	0.90 0.78 0.80 0.75 0.71 0.74 0.73 0.68 1.00	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68 1.01	1.22 1.00 1.01 0.99 0.92 0.93 0.93 0.90 1.27 1.28
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang	0.89 0.86 0.86 0.79 0.78 0.79 0.80 1.04 1.03	1.30 1.00 1.01 1.01 1.02 1.02 1.00 1.31 1.30	1.28 0.98 1.01 1.00 1.01 1.01 0.99 1.30 1.31	1.32 1.02 1.02 1.04 1.03 1.02 1.00 1.32 1.31	1.44 1.18 1.16 1.18 1.00 1.00 1.01 1.46 1.55	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.44	1.43 1.17 1.16 1.17 1.00 1.00 1.45 1.54	1.39 1.18 1.20 1.16 1.10 1.09 1.11 1.44 1.53	0.90 0.78 0.80 0.75 0.71 0.74 0.73 0.68	0.90 0.78 0.81 0.75 0.71 0.75 0.73 0.68 1.01	1.22 1.00 1.01 0.99 0.92 0.93 0.93 0.90 1.27 1.28

Table 7: Optimisation matrix for SIKEp434  $\,$ 

$\alpha$	rr		4.0	. 4
~	I K	$\operatorname{Er}$	<b>√</b> 1 3	
<b>L</b> 2.1	$\sim$	L/L	<b>/</b> T • .	, –

						1						
		$\bowtie$	$\bowtie$	$\bowtie$	$\bowtie$	75	10G	10G	11G	12G	13G	
		1900X	5800X	5950X	7950X	99	10			12	7	G.M.
	run on	19	58	59	79	17	17	9i	17	9i	91	Ü
	opt on											
	1900X		1.10	1.08	1.08	1.42	1.54	1.58	1.32	1.14	1.30	1.24
	5800X	0.98		0.99	0.99	1.27	1.40	1.43	1.23	1.04	1.22	1.14
	5950X	0.99	1.01		1.00	1.32	1.45	1.48	1.23	1.00	1.17	1.15
	7950X	1.00	1.03	1.01		1.39	1.53	1.56	1.26	1.05	1.22	1.19
>-	i7 6G	0.85	0.93	0.91	0.90		1.04	1.12	1.04	0.81	0.93	0.95
PĽ	i7 10G	0.84	0.87	0.86	0.86	0.91		1.03	1.00	0.81	0.95	0.91
Ē	i9 10G	0.82	0.86	0.85	0.84	0.89	0.97		1.00	0.83	0.97	0.90
MULTIPLY	i7 11G	0.82	0.89	0.87	0.88	0.92	1.01	1.04		0.86	1.00	0.93
$\prec$	i9 12G	1.03	1.08	1.09	1.06	1.42	1.56	1.60	1.26		1.16	1.21
	i9 13G	0.92	0.99	0.98	0.96	1.21	1.33	1.37	1.08	0.87		1.06
	Clang	1.64	1.89	1.86	1.65	2.17	2.37	2.44	2.33	1.97	2.36	2.05
	GCC	2.27	2.56	2.53	2.05	3.47	3.77	3.88	3.92	2.72	3.14	2.96
	Final	2.01	2.19	2.19	1.95	2.44	2.43	2.44	2.34	2.43	2.53	2.29
	rillai	2.01	2.13	2.13	1.50	2.44	4.40	4.44	4.04	4.40	4.00	4.40
	1000 <b>V</b>		1.10	1 10	1 1 1 1	1.00	1 7 /	1.70	1.20	1 15		
	1900X	0.07	1.10	1.10	1.15	1.68	1.54	1.79	1.32	1.15	0.86	1.24
	5800X	0.97		1.10 1.01	1.05	1.52	1.46	1.62	1.20	1.10	0.86 0.80	1.24 1.15
	5800X 5950X	0.98	0.99	1.01		$1.52 \\ 1.56$	$1.46 \\ 1.49$	$1.62 \\ 1.65$	$1.20 \\ 1.23$	1.10 1.07	0.86 0.80 0.80	1.24 1.15 1.15
	5800X 5950X 7950X	0.98 0.92	0.99 0.98	1.01 0.98	1.05 1.06	1.52	1.46 1.49 1.46	1.62 1.65 1.57	1.20 1.23 1.19	1.10 1.07 0.98	0.86 0.80 0.80 0.72	1.24 1.15 1.15 1.10
ы	5800X 5950X 7950X i7 6G	0.98 0.92 0.77	0.99 0.98 0.81	1.01 0.98 0.81	1.05 1.06	1.52 1.56 1.47	$1.46 \\ 1.49$	1.62 1.65 1.57 1.07	1.20 1.23 1.19 0.99	1.10 1.07 0.98 0.89	0.86 0.80 0.80 0.72 0.66	1.24 1.15 1.15 1.10 0.88
ARE	5800X 5950X 7950X i7 6G i7 10G	0.98 0.92 0.77 0.79	0.99 0.98 0.81 0.85	1.01 0.98 0.81 0.85	1.05 1.06 0.85 0.91	1.52 1.56 1.47 1.01	1.46 1.49 1.46 0.99	1.62 1.65 1.57	1.20 1.23 1.19 0.99 0.97	1.10 1.07 0.98 0.89 0.84	0.86 0.80 0.80 0.72 0.66 0.63	1.24 1.15 1.15 1.10 0.88 0.88
QUARE	5800X 5950X 7950X i7 6G i7 10G i9 10G	0.98 0.92 0.77 0.79 0.75	0.99 0.98 0.81 0.85 0.80	1.01 0.98 0.81 0.85 0.80	1.05 1.06 0.85 0.91 0.83	1.52 1.56 1.47 1.01 0.94	1.46 1.49 1.46 0.99	1.62 1.65 1.57 1.07 1.08	1.20 1.23 1.19 0.99	1.10 1.07 0.98 0.89 0.84 0.74	0.86 0.80 0.80 0.72 0.66 0.63 0.55	1.24 1.15 1.15 1.10 0.88 0.88 0.82
SQUARE	5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	0.98 0.92 0.77 0.79 0.75 0.81	0.99 0.98 0.81 0.85 0.80 0.86	1.01 0.98 0.81 0.85 0.80 0.86	1.05 1.06 0.85 0.91 0.83 0.91	1.52 1.56 1.47 1.01 0.94 1.04	1.46 1.49 1.46 0.99 0.95 1.03	1.62 1.65 1.57 1.07 1.08	1.20 1.23 1.19 0.99 0.97 0.92	1.10 1.07 0.98 0.89 0.84	0.86 0.80 0.80 0.72 0.66 0.63 0.55 0.67	1.24 1.15 1.15 1.10 0.88 0.88 0.82 0.91
$S_{QUARE}$	5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	0.98 0.92 0.77 0.79 0.75 0.81 0.95	0.99 0.98 0.81 0.85 0.80 0.86 1.02	1.01 0.98 0.81 0.85 0.80 0.86 1.03	1.05 1.06 0.85 0.91 0.83 0.91 1.07	1.52 1.56 1.47 1.01 0.94 1.04 1.44	1.46 1.49 1.46 0.99 0.95 1.03 1.43	1.62 1.65 1.57 1.07 1.08 1.11 1.53	1.20 1.23 1.19 0.99 0.97 0.92	1.10 1.07 0.98 0.89 0.84 0.74 0.89	0.86 0.80 0.80 0.72 0.66 0.63 0.55	1.24 1.15 1.15 1.10 0.88 0.88 0.82 0.91 1.12
$S_{QUARE}$	5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	0.98 0.92 0.77 0.79 0.75 0.81	0.99 0.98 0.81 0.85 0.80 0.86	1.01 0.98 0.81 0.85 0.80 0.86	1.05 1.06 0.85 0.91 0.83 0.91	1.52 1.56 1.47 1.01 0.94 1.04	1.46 1.49 1.46 0.99 0.95 1.03	1.62 1.65 1.57 1.07 1.08	1.20 1.23 1.19 0.99 0.97 0.92	1.10 1.07 0.98 0.89 0.84 0.74	0.86 0.80 0.80 0.72 0.66 0.63 0.55 0.67	1.24 1.15 1.15 1.10 0.88 0.88 0.82 0.91
SQUARE	5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G	0.98 0.92 0.77 0.79 0.75 0.81 0.95	0.99 0.98 0.81 0.85 0.80 0.86 1.02	1.01 0.98 0.81 0.85 0.80 0.86 1.03	1.05 1.06 0.85 0.91 0.83 0.91 1.07	1.52 1.56 1.47 1.01 0.94 1.04 1.44	1.46 1.49 1.46 0.99 0.95 1.03 1.43	1.62 1.65 1.57 1.07 1.08 1.11 1.53	1.20 1.23 1.19 0.99 0.97 0.92	1.10 1.07 0.98 0.89 0.84 0.74 0.89	0.86 0.80 0.80 0.72 0.66 0.63 0.55 0.67	1.24 1.15 1.15 1.10 0.88 0.88 0.82 0.91 1.12
SQUARE	5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G	0.98 0.92 0.77 0.79 0.75 0.81 0.95	0.99 0.98 0.81 0.85 0.80 0.86 1.02	1.01 0.98 0.81 0.85 0.80 0.86 1.03 1.30	1.05 1.06 0.85 0.91 0.83 0.91 1.07 1.35	1.52 1.56 1.47 1.01 0.94 1.04 1.44 2.02	1.46 1.49 1.46 0.99 0.95 1.03 1.43 1.99	1.62 1.65 1.57 1.07 1.08 1.11 1.53 2.15	1.20 1.23 1.19 0.99 0.97 0.92 1.20 1.55	1.10 1.07 0.98 0.89 0.84 0.74 0.89	0.86 0.80 0.80 0.72 0.66 0.63 0.55 0.67	1.24 1.15 1.15 1.10 0.88 0.88 0.82 0.91 1.12

Table 8: Optimisation matrix for Curve448

					Cı	ırve4	48					
	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.17	1.18	1.16	1.18	1.17	1.14	1.12	1.03	0.90	1.10
	5800X	0.96		1.01	0.99	1.12	1.11	1.07	1.03	1.01	0.89	1.02
	5950X	0.97	1.00		1.00	1.13	1.12	1.08	1.03	1.00	0.87	1.02
	7950X	0.96	1.03	1.04		1.13	1.12	1.08	1.02	0.99	0.87	1.02
75	i7 6G	0.94	1.00	1.02	0.99		0.99	0.95	0.97	0.91	0.80	0.96
ΊΡΙ	i7 10G	0.91	1.00	1.01	0.99	1.01		0.96	0.95	0.92	0.80	0.95
Мистірсу	i9 10G	0.96	1.01	1.02	1.02	1.05	1.04	4.05	0.98	0.94	0.81	0.98
$\mathbb{X}$	i7 11G	0.98	1.07	1.07	1.05	1.10	1.09	1.05	1.10	0.96	0.84	1.02
	i9 12G	1.03	1.16	1.17	1.17	1.19	1.18	1.14	1.12	1 1 /	0.85	1.10
	i9 13G	1.13	1.32	1.33	1.30	1.30	1.33	1.24	1.42	1.14		1.25
	Clang	1.07	1.10	1.11	1.09	1.43	1.42	1.37	1.30	1.18	1.11	1.21
	GCC	0.89	0.99	1.00	1.00	1.13	1.13	1.08	1.05	0.95	0.84	1.00
	Final	0.98	0.99	1.00	1.01	1.13	1.13	1.13	1.10	1.04	1.05	1.06
	1900X		1.01	1.01	1.00	1.07	1.00	1.06	1.00	1.07	1.00	1.04
	5800X	1.07	1.01	1.01	1.00	1.10	1.09 1.11	1.06	1.08	1.07 $1.12$	1.05	1.04
	5950X	1.07	1.00	1.01	1.04	1.10	1.11 $1.14$	1.11	1.03	1.12	1.03	1.06
	7950X	1.04	0.99	1.00	1.02	1.09	1.10	1.08	1.05	1.08	1.01	$\frac{1.00}{1.04}$
	i7 6G	1.05	1.07	1.07	1.07	1.00	1.01	0.99	1.00	1.12	1.05	1.04
RE	i7 10G	1.06	1.05	1.05	1.03	0.99		0.98	1.02	1.15	1.08	1.04
SQUARE	i9 10G	1.04	1.00	1.00	1.01	1.01	1.02		1.01	1.07	1.01	1.02
$S_{\mathcal{O}}$	i7 11G	1.08	1.03	1.04	1.04	1.05	1.06	1.04		1.06	0.99	1.04
	i9 12G	1.06	1.00	1.00	1.01	1.06	1.07	1.06	1.02		0.94	1.02
	$i9\ 13G$	1.08	1.07	1.08	1.07	1.14	1.16	1.13	1.13	1.07		1.09
	Clang	1.06	1.08	1.08	1.10	1.12	1.13	1.11	1.12	1.11	1.03	1.09
	GCC	1.04	1.07	1.08	1.06	1.06	1.07	1.05	1.06	1.04	0.98	1.05
	Final	1.04	1.09	1.09	1.06	1.07	1.07	1.07	1.06	1.04	1.04	1.06

Table 9: Optimisation matrix for P-521

D	L	0	1
Γ-	. )	/,	-1

	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.12	1.13	1.07	1.16	1.15	1.15	1.23	1.06	1.09	1.12
	5800X	1.00		1.01	0.97	1.12	1.10	1.11	1.09	1.06	1.08	1.05
	5950X	0.98	0.99		0.95	1.08	1.07	1.08	1.04	1.03	1.07	1.03
	7950X	1.02	1.05	1.04		1.16	1.15	1.16	1.16	1.07	1.10	1.09
$\succ$	i7~6G	0.97	1.01	1.02	0.98		0.99	1.00	1.01	1.03	1.07	1.01
Мистіргу	i7 10G	0.95	1.03	1.03	0.99	1.01		1.00	1.03	1.04	1.09	1.02
E	i9 10G	0.95	1.00	1.02	0.98	1.01	1.00		0.98	0.99	1.02	0.99
Μū	i7 11G	0.98	1.03	1.03	0.98	1.05	1.03	1.04		0.96	0.97	1.01
	i9 12G	1.04	1.15	1.16	1.10	1.18	1.17	1.17	1.25		1.01	1.12
	i9 13G	1.06	1.15	1.16	1.09	1.24	1.23	1.24	1.33	0.97		1.14
	Clang	1.14	1.25	1.27	1.19	1.52	1.50	1.51	1.43	1.40	1.35	1.35
	$\widetilde{\mathrm{GCC}}$	1.03	1.16	1.17	1.11	0.98	0.97	0.98	0.99	0.96	0.98	1.03
	Final	1.09	1.17	1.17	1.17	0.98	0.98	0.98	1.01	1.00	1.01	1.05
	ГШаг	1.09	1.17	1.11	1.17	0.90	0.90	0.90	1.01	1.00	1.01	1.05
	1900X		1.00	1.02	1.03	1.11	1.09	1.14	1.04	1.17	1.13	1.07
	5800X	1.04	1.00	1.02 $1.02$	1.03	1.16	1.13	1.14	1.04 $1.05$	1.20	1.16	1.07
	5950X	1.04	1.00	1.02	1.04	1.11	1.09	1.14	1.01	1.19	1.15	1.07
	7950X	1.04	1.02	1.03	1.00	1.12	1.10	1.15	1.05	1.15	1.12	1.08
	i7 6G	0.96	1.00	1.01	1.06	1.12	0.98	1.02	1.00	1.20	1.21	1.04
R E	i7 10G	0.97	1.00	1.02	1.02	1.02	0.00	1.04	0.94	1.18	1.18	1.03
SQUARE	i9 10G	0.99	1.01	1.02	1.03	0.98	0.96		1.01	1.23	1.19	1.04
SQ	i7 11G	1.03	1.03	1.04	1.04	1.12	1.10	1.14		1.17	1.13	1.08
	i9 12G	1.04	1.03	1.04	1.06	1.11	1.09	1.14	1.02		0.97	1.05
	i9 13G	1.03	1.04	1.05	1.07	1.13	1.11	1.16	1.01	1.03		1.06
	Clang	1.09	1.24	1.26	1.31	1.60	1.56	1.63	1.65	1.37	1.31	1.39
	GCC	1.07	1.12	1.14	1.17	1.03	1.01	1.05	0.99	1.21	1.18	1.09
	Final	1.11	1.13	1.14	1.17	1.05	1.05	1.05	1.06	1.21	1.21	1.12

Table 10: Optimisation matrix for Poly1305

	Poly1305											
	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.16	1.16	1.14	1.09	1.10	1.10	1.10	1.15	1.14	1.11
	5800X	1.11		1.00	0.99	1.08	1.08	1.08	1.08	1.08	1.07	1.06
	5950X	1.12	1.00		1.00	1.11	1.12	1.13	1.12	1.19	1.19	1.10
	7950X	1.06	1.06	1.06		1.08	1.09	1.08	1.10	1.13	1.11	1.08
$\geq$	i7 6G	1.15	1.14	1.14	1.09		1.01	1.01	1.05	1.12	1.10	1.08
Multiply	i7 10G	1.13	1.15	1.15	1.11	0.99		1.00	1.03	1.33	1.36	1.12
15	i9 10G	1.14	1.14	1.15	1.14	1.00	1.01	4.04	1.04	1.41	1.42	1.14
M	i7 11G	1.11	1.09	1.09	1.07	1.01	1.02	1.01	4.04	1.32	1.32	1.10
	i9 12G	1.11	1.05	1.05	1.05	1.00	1.01	1.01	1.01	1.01	0.99	1.03
	i9 13G	1.13	1.05	1.07	1.07	1.01	1.02	1.02	1.02	1.01		1.04
	Clang	1.14	1.12	1.13	1.14	1.15	1.15	1.15	1.14	1.23	1.22	1.16
	GCC	1.13	1.18	1.18	1.14	1.26	1.27	1.26	1.22	1.30	1.30	1.22
	Final	1.13	1.13	1.13	1.15	1.15	1.15	1.15	1.14	1.23	1.23	1.16
	1900X		1.06	1.06	1.00	1.09	1.15	1.15	1.11	1.11	1.11	1.08
	5800X	1.06		1.00	1.00	1.05	1.10	1.10	1.04	1.05	1.05	1.04
	5950X	1.12	1.00		1.00	1.05	1.10	1.10	1.04	1.08	1.08	1.06
	7950X	1.17	1.06	1.06		1.10	1.13	1.14	1.05	1.11	1.11	1.09
(÷)	i7 6G	1.12	1.17	1.17	1.17		1.05	1.05	1.03	1.33	1.39	1.14
SQUARE	i7 10G	1.13	1.13	1.13	1.11	0.95		1.00	1.02	1.40	1.41	1.12
'n	i9 10G	1.10	1.17	1.17	1.15	0.95	1.00		1.04	1.33	1.35	1.12
$\tilde{\mathbf{S}}$	i7 11G	1.16	1.06	1.06	1.10	1.00	1.05	1.06		1.42	1.42	1.12
	i9 12G	1.08	1.08	1.08	1.03	1.00	1.05	1.05	1.02		0.99	1.04
	i9 13G	1.09	1.06	1.06	1.06	1.00	1.05	1.05	1.03	1.00		1.04
	Clang	1.06	1.11	1.11	1.11	1.09	1.14	1.14	1.10	1.20	1.20	1.13
	GCC	1.13	1.28	1.28	1.17	1.28	1.34	1.34	1.28	1.28	1.28	1.26
	Final	1.06	1.11	1.11	1.12	1.14	1.14	1.14	1.10	1.20	1.21	1.13

Table 11: Optimisation matrix for secp256k1-Dettman

	${ m secp}256{ m k}1 ext{-}{ m Dettman}$											
	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
	opt on											
	1900X		1.13	1.09	1.11	1.12	1.13	1.10	1.07	1.22	1.17	1.11
	5800X	1.08		0.97	1.04	1.05	1.07	1.03	1.05	1.21	1.17	1.06
	5950X	1.06	1.03		1.05	1.09	1.11	1.08	1.09	1.16	1.12	1.08
	7950X	1.05	1.05	1.02		1.04	1.06	1.03	1.02	1.15	1.11	1.05
$\succ$	i7 6G	1.02	1.11	1.09	1.08		1.02	0.98	1.06	1.08	1.04	1.05
IPL.	i7 10G	1.00	1.08	1.05	1.07	0.98		0.97	1.01	1.22	1.17	1.05
Multiply	i9 10G	1.02	1.11	1.08	1.08	1.01	1.03		1.02	1.14	1.09	1.06
$\Lambda$ U	i7 11G	1.00	1.07	1.05	1.07	1.01	1.03	1.00		1.10	1.06	1.04
	i9 12G	1.00	1.03	1.01	1.02	1.00	1.02	0.98	1.01		0.96	1.00
	i9 13G	1.07	1.09	1.06	1.07	1.05	1.06	1.03	1.03	1.04		1.05
	Clang	0.96	1.09	1.06	1.08	1.15	1.16	1.13	1.10	1.17	1.07	1.10
	$\widetilde{\mathrm{GCC}}$	1.17	1.40	1.36	1.37	1.20	1.22	1.19	1.13	1.22	1.18	1.24
	Final	0.96	1.09	1.09	1.08	1.17	1.16	1.17	1.10	1.17	1.11	1.11
	1900X		1.06	1.06	1.06	1.12	1.13	1.12	1.14	1.17	1.19	1.10
	5800X	1.09		0.99	1.03	1.08	1.09	1.09	1.02	1.10	1.12	1.06
	5950X	1.10	1.00		1.03	1.08	1.09	1.09	1.12	1.16	1.18	1.08
	7950X	1.07	1.03	1.03		1.06	1.07	1.07	1.08	1.14	1.16	1.07
	i7 6G	1.08	1.06	1.06	1.10		1.01	1.01	1.01	1.25	1.26	1.08
SQUARE	i7 10G	1.12	1.06	1.07	1.09	0.99		0.99	1.04	1.13	1.15	1.06
Ω	i9 10G	1.08	1.08	1.08	1.11	1.00	1.01		0.99	1.15	1.17	1.07
$\mathbf{S}$	i7 11G	1.07	1.11	1.11	1.10	1.04	1.06	1.04		1.18	1.20	1.09
	i9 12G	1.04	1.05	1.05	1.07	1.04	1.06	1.04	1.00		1.01	1.04
	i9 13G	1.07	1.07	1.07	1.00	1.01	1.02	1.01	1.00	0.99		1.02
	Clang	0.93	1.03	1.03	1.02	1.08	1.08	1.08	1.13	1.11	1.14	1.06
	GCC	1.10	1.15	1.15	1.20	1.17	1.19	1.17	1.16	1.08	1.09	1.14
	Final	0.93	1.03	1.04	1.02	1.09	1.08	1.09	1.13	1.09	1.09	1.06

Table 12: Optimisation matrix for secp256k1

	${ m secp256k1}$											
	run on	1900X	5800X	5950X	7950X	i7 6G	i7 10G	i9 10G	i7 11G	i9 12G	i9 13G	G.M.
MULTIPLY	opt on 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang GCC	1.08 1.08 1.04 1.17 1.03 1.09 1.05 1.07 1.10	1.07 1.02 1.00 1.10 1.01 1.05 1.03 1.11 1.92	1.02 0.99 0.98 1.07 0.98 0.97 1.04 1.01 1.09	1.05 1.05 1.07 1.14 1.04 1.04 1.11 1.11 1.14	0.98 0.98 0.99 0.96 0.92 0.91 0.95 0.98 1.00	1.06 1.08 1.05 1.09 0.99 1.03 1.06 1.09	1.08 1.09 1.06 1.10 1.01 1.04 1.08 1.10	1.06 1.04 1.10 1.08 1.14 1.06 1.01 1.03 1.05	1.08 1.09 1.11 1.09 1.11 1.10 1.05 1.05	1.03 1.05 1.06 1.04 1.07 1.05 1.01 1.00 0.96	1.04 1.04 1.06 1.03 1.10 1.02 1.01 1.03 1.03 1.07
	Final	2.51	2.28 1.93	2.23 1.93	2.33 1.83	1.95	3.05	3.09 1.95	2.86 1.97	3.19 1.90	3.07 1.89	2.72 1.92
SQUARE	1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G	1.08 1.06 1.09 1.09 1.11 1.06 1.07	1.05 0.95 1.02 1.09 1.06 1.05 1.03	1.11 1.05 1.07 1.14 1.12 1.11 1.09	1.05 1.08 1.00 1.09 1.10 1.07 1.07	1.03 1.06 1.04 1.05 0.99 0.99 1.01	1.04 1.07 1.05 1.06 1.01 1.00 1.02	1.04 1.08 1.05 1.06 1.01 1.01	1.04 1.16 1.06 1.10 1.11 1.09 1.08	1.04 1.09 1.08 1.09 1.09 1.08 1.03 1.04	1.00 1.06 1.04 1.06 1.06 1.05 1.00 1.01	1.04 1.07 1.03 1.06 1.07 1.06 1.04 1.04
<b>3</b> 1	i9 12G i9 13G Clang GCC	1.10 1.11 1.71 2.47	1.14 1.07 1.85 2.23	1.19 1.13 1.94 2.34	1.15 1.10 1.71 2.25	1.04 1.04 1.81 2.88	1.05 1.05 1.82 2.90	1.06 1.06 1.82 2.90	1.04 1.09 1.83 2.74	1.03 1.83 3.09	0.97 1.79 3.02	1.07 1.07 1.81 2.66

Final 1.71 1.95 1.94 1.72 1.83 1.82 1.82 1.83 1.83 1.85 1.83