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

| | | | | | Cur | ve25 | 519 | | | | | |
|------------|---|--------------|---------------------|--------------|-------------|--------------|--------|--------------|--------|--------------|---------------------|---------------------|
| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
| | opt on | | | | | | | | | | | |
| | 1900X | | 1.06 | 1.10 | 1.12 | 1.17 | 1.04 | 1.07 | 1.24 | 1.22 | 1.12 | 1.11 |
| | 5800X | 1.17 | | 1.02 | 1.09 | 1.14 | 1.06 | 1.11 | 1.11 | 1.22 | 1.12 | 1.10 |
| | 5950X | 1.18 | 0.98 | | 1.05 | 1.13 | 1.03 | 1.06 | 1.09 | 1.19 | 1.24 | 1.09 |
| | 7950X | 1.12 | 0.97 | 0.98 | | 1.12 | 0.98 | 1.03 | 1.05 | 1.09 | 1.01 | 1.03 |
| × | i7 6G | 1.10 | 1.06 | 1.08 | 1.10 | | 0.93 | 0.95 | 1.00 | 1.14 | 1.06 | 1.04 |
| Multiply | i7 10G | 1.13 | 1.10 | 1.11 | 1.13 | 1.02 | | 0.97 | 1.06 | 1.23 | 1.13 | 1.09 |
| 717 | i9 10G | 1.15 | 1.12 | 1.15 | 1.17 | 1.10 | 0.97 | 1.04 | 1.10 | 1.17 | 1.08 | 1.10 |
| Ξ | i7 11G | 1.14 | 1.06 | 1.07 | 1.11 | 1.09 | 1.01 | 1.04 | 1 01 | 1.12 | 1.03 | 1.07 |
| | i9 12G i9 13G | 1.12 1.24 | 1.03 1.13 | 1.05 1.15 | 1.10 | 1.15 1.15 | 1.01 | 1.03 | 1.01 | 1.08 | 0.92 | 1.04 1.12 |
| | | | | | | | | | | | | |
| | Clang | 1.28 | 1.22 | 1.25 | 1.27 | 1.33 | 1.22 | 1.25 | 1.27 | 1.24 | 1.14 | 1.25 |
| | GCC | 1.08 | 1.15 | 1.18 | 1.31 | 1.16 | 1.07 | 1.10 | 1.16 | 1.18 | 1.11 | 1.15 |
| | Final | 1.08 | 1.19 | 1.20 | 1.27 | 1.16 | 1.15 | 1.16 | 1.16 | 1.18 | 1.21 | 1.17 |
| | 400037 | | 4.0= | 4.0= | 4.00 | 1.00 | 4.0= | 4.0= | 4.00 | 4.04 | 4.00 | 4.00 |
| | 1900X | 1 11 | 1.07 | 1.07 | 1.09 | 1.02 | 1.07 | 1.07 | 1.09 | 1.24 | 1.22 | 1.09 |
| | 5800X | 1.11 | 1.09 | 1.00 | 1.03 | 1.04 | 1.07 | 1.09 | 1.13 | 1.15 | 1.08 | 1.07 |
| | 5950X | 1.17 | 1.03 | 1.02 | 1.08 | 1.12 | 1.13 | 1.15 | 1.15 | 1.19 1.21 | 1.17 1.19 | 1.12 |
| | 7950X i7 6G | 1.10 1.17 | 1.03 1.13 | 1.02 | 1.18 | 1.09 | 1.09 | 1.11 1.04 | 1.34 | 1.21 | 1.19 1.49 | 1.11 1.13 |
| 田 | i7 10G | 1.17 1.21 | 1.13 | 1.12 | 1.16 1.15 | 0.97 | 1.02 | 1.04 | 1.09 | 1.11 | 1.49 1.15 | 1.13 |
| JAF | i9 10G | 1.11 | 1.13 | 1.13 | 1.10 | 0.95 | 0.98 | 1.01 | 1.03 | 1.16 1.24 | 1.13 1.22 | 1.10 |
| SQUARE | i7 11G | 1.16 | 1.13 | 1.11 | 1.15 | 1.03 | 1.07 | 1.08 | 1.00 | 1.35 | 1.32 | 1.13 |
| J 1 | i9 12G | 1.08 | 1.02 | 1.03 | 1.04 | 0.98 | 1.01 | 1.03 | 1.04 | 1.00 | 0.98 | 1.02 |
| | i9 13G | 1.16 | 1.07 | 1.08 | 1.10 | 0.99 | 1.02 | 1.04 | 1.04 | 1.02 | 0.00 | 1.05 |
| | | 1.23 | 1.22 | 1.20 | 1.23 | 1.17 | 1.22 | 1.24 | 1.19 | 1.18 | 1.25 | 1.22 |
| | $\begin{array}{c} \text{Clang} \\ \text{GCC} \end{array}$ | 1.23 | $\frac{1.22}{1.24}$ | 1.20 1.24 | 1.23 1.20 | 1.17 | 1.22 | 1.24 | 1.19 | 1.18 1.22 | $\frac{1.25}{1.28}$ | $\frac{1.22}{1.16}$ |
| | GCC | 1.10 | 1.24 | 1.24 | 1.20 | 1.04 | 1.08 | 1.10 | 1.10 | 1.22 | 1.20 | 1.10 |
| | Final | 1.18 | 1.22 | 1.20 | 1.20 | 1.10 | 1.10 | 1.10 | 1.10 | 1.18 | 1.28 | 1.17 |

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

| | Mult | iply | Squ | are |
|--------------------|-------|------|-------|------|
| Curve | Clang | GCC | Clang | GCC |
| Curve25519 | 1.25 | 1.15 | 1.22 | 1.16 |
| Curve25519-Solinas | 1.61 | 2.52 | 1.43 | 2.74 |
| P-224 | 1.56 | 2.53 | 1.42 | 2.58 |
| P-256 | 1.69 | 2.60 | 1.64 | 2.58 |
| P-384 | 1.47 | 2.48 | 1.38 | 2.53 |
| SIKEp434 | 1.91 | 2.74 | 1.81 | 2.55 |
| Curve448 | 1.19 | 0.99 | 1.08 | 1.04 |
| P-521 | 1.32 | 1.00 | 1.36 | 1.06 |
| Poly1305 | 1.16 | 1.23 | 1.14 | 1.27 |
| secp256k1-Dettman | 1.08 | 1.22 | 1.05 | 1.14 |
| secp256k1 | 1.85 | 2.66 | 1.76 | 2.59 |

Table 3: Optimisation matrix for Curve25519-Solinas

Curve25519-Solinas

| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
|--------------|--------|-------|-------|-------|-------|-------|--------|--------|--------|--------|--------|------|
| | opt on | | 1.00 | 1 10 | 1.00 | 1.00 | 1 10 | 1 10 | 1 1 5 | 1 10 | 0.00 | 1.07 |
| | 1900X | 1.00 | 1.03 | 1.13 | 1.09 | 1.08 | 1.10 | 1.10 | 1.15 | 1.12 | 0.96 | 1.07 |
| | 5800X | 1.09 | 0.00 | 1.09 | 1.07 | 1.09 | 1.11 | 1.11 | 1.13 | 1.11 | 1.13 | 1.09 |
| | 5950X | 1.07 | 0.92 | 4 05 | 1.02 | 1.05 | 1.08 | 1.08 | 1.08 | 1.07 | 0.92 | 1.03 |
| | 7950X | 1.06 | 0.97 | 1.05 | | 1.04 | 1.07 | 1.07 | 1.06 | 1.06 | 0.91 | 1.03 |
| × | i7 6G | 1.10 | 1.04 | 1.13 | 1.09 | | 1.04 | 1.04 | 1.06 | 1.03 | 0.88 | 1.04 |
| IPI | i7 10G | 1.12 | 1.00 | 1.08 | 1.04 | 1.01 | | 1.00 | 1.03 | 1.02 | 0.87 | 1.01 |
| Multiply | i9 10G | 1.09 | 1.00 | 1.09 | 1.07 | 1.03 | 1.00 | | 1.02 | 1.01 | 1.02 | 1.03 |
| Δſ | i7 11G | 1.10 | 1.06 | 1.15 | 1.10 | 1.02 | 1.04 | 1.05 | | 1.02 | 0.88 | 1.04 |
| | i9 12G | 1.11 | 1.00 | 1.08 | 1.06 | 1.02 | 1.05 | 1.05 | 1.06 | | 0.86 | 1.03 |
| | i9 13G | 1.08 | 1.03 | 1.12 | 1.10 | 1.02 | 1.04 | 1.04 | 1.06 | 1.01 | | 1.05 |
| | Clang | 1.69 | 1.64 | 1.78 | 1.73 | 1.47 | 1.51 | 1.52 | 1.70 | 1.62 | 1.46 | 1.61 |
| | GCC | 2.36 | 2.15 | 2.33 | 2.29 | 2.71 | 2.77 | 2.77 | 2.66 | 2.82 | 2.43 | 2.52 |
| | T): 1 | 1.00 | | 1 70 | 1.70 | 1 47 | 1 21 | 1 50 | 1.70 | 1.00 | 1.00 | |
| | Final | 1.69 | 1.78 | 1.78 | 1.73 | 1.47 | 1.51 | 1.52 | 1.70 | 1.62 | 1.69 | 1.64 |
| | 100037 | | 1 1 1 | 1 1 2 | 1 1 2 | 1.00 | 1.07 | 1.05 | 1.10 | 1 11 | 1.05 | 1.00 |
| | 1900X | 1.00 | 1.14 | 1.15 | 1.15 | 1.06 | 1.07 | 1.07 | 1.13 | 1.11 | 1.07 | 1.09 |
| | 5800X | 1.06 | 4.04 | 1.02 | 1.05 | 1.08 | 1.10 | 1.09 | 1.19 | 1.15 | 1.11 | 1.09 |
| | 5950X | 1.16 | 1.01 | | 1.00 | 1.05 | 1.04 | 1.05 | 1.15 | 1.12 | 1.08 | 1.06 |
| | 7950X | 1.07 | 1.07 | 1.06 | | 1.08 | 1.07 | 1.09 | 1.10 | 1.13 | 1.09 | 1.07 |
| ſŦĨ | i7 6G | 1.06 | 1.10 | 1.12 | 1.10 | | 1.00 | 1.02 | 1.06 | 1.11 | 1.07 | 1.06 |
| \R! | i7 10G | 1.06 | 1.10 | 1.10 | 1.09 | 1.00 | | 1.04 | 1.05 | 1.11 | 1.07 | 1.06 |
| SQUARE | i9 10G | 1.06 | 1.07 | 1.07 | 1.06 | 1.02 | 1.01 | | 1.04 | 1.08 | 1.04 | 1.04 |
| \mathbf{S} | i7 11G | 1.06 | 1.08 | 1.09 | 1.08 | 1.02 | 1.02 | 1.03 | | 1.09 | 1.06 | 1.05 |
| | | | | | | | | | | | | |

1.05

2.78

 $1.54 \quad 1.35$

1.02 1.04

1.15

1.12

2.77

1.15

1.12

2.84

1.05

2.76

1.38

1.03

1.05

1.36

2.79

1.36

1.11

2.72

1.52

0.97

2.58

1.46 1.43 1.44

1.04

2.66

1.06

1.07

2.74

i9 12G

i9 13G

Clang

GCC

1.05 1.14

Final 1.35 1.50 1.50

2.82

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 | | 0.98 | 1.06 | 1.06 | 1.04 | 1.02 | 1.08 | 1.06 | 1.06 | 0.91 | 1.02 |
| | 5800X | 1.17 | | 1.07 | 1.09 | 1.17 | 1.12 | 1.18 | 1.19 | 1.23 | 1.06 | 1.13 |
| | 5950X | 1.11 | 0.93 | | 1.04 | 1.09 | 1.07 | 1.12 | 1.12 | 1.15 | 0.98 | 1.06 |
| | 7950X | 1.09 | 0.95 | 1.02 | | 1.06 | 1.04 | 1.09 | 1.12 | 1.10 | 0.95 | 1.04 |
| >- | i7~6G | 1.10 | 1.00 | 1.06 | 1.07 | | 0.98 | 1.02 | 1.06 | 1.02 | 0.88 | 1.02 |
| PL | i7 10G | 1.11 | 0.99 | 1.06 | 1.11 | 1.03 | | 1.06 | 1.03 | 1.01 | 0.87 | 1.02 |
| Multiply | i9 10G | 1.07 | 0.97 | 1.04 | 1.05 | 0.96 | 0.95 | | 1.05 | 1.04 | 1.00 | 1.01 |
| $\Lambda 0$ | i7 11G | 1.08 | 0.99 | 1.07 | 1.07 | 1.07 | 1.03 | 1.08 | | 1.03 | 0.88 | 1.03 |
| 4 | i9 12G | 1.10 | 0.99 | 1.06 | 1.06 | 1.04 | 1.02 | 1.07 | 1.05 | | 0.86 | 1.02 |
| | i9 13G | 1.25 | 1.13 | 1.21 | 1.27 | 1.20 | 1.17 | 1.23 | 1.20 | 1.17 | | 1.18 |
| | Clang | 1.63 | 1.43 | 1.54 | 1.44 | 1.60 | 1.56 | 1.64 | 1.62 | 1.68 | 1.46 | 1.56 |
| | $\widetilde{\mathrm{GCC}}$ | 2.47 | 1.98 | 2.12 | 2.09 | 2.84 | 2.79 | 2.92 | 2.72 | 3.05 | 2.62 | 2.53 |
| | | | | | | | | | | | | |
| | Ein al | | | | | | | 1 64 | 1.69 | 1 60 | 1 71 | 1 61 |
| | Final | 1.63 | 1.53 | 1.54 | 1.44 | 1.66 | 1.65 | 1.64 | 1.62 | 1.68 | 1.71 | 1.61 |
| | | | 1.53 | 1.54 | 1.44 | 1.66 | 1.65 | | | | | |
| | 1900X | 1.63 | | 1.54 1.09 | 1.44 | 1.66 1.01 | 1.65 1.04 | 1.03 | 1.04 | 1.08 | 0.94 | 1.04 |
| | 1900X 5800X | 1.63 | 1.53 | 1.54 | 1.44 1.08 1.00 | 1.66 1.01 1.02 | 1.65 1.04 1.05 | 1.03 1.03 | 1.04 1.02 | 1.08 1.09 | 0.94 0.95 | 1.04 1.02 |
| | 1900X 5800X 5950X | 1.63 1.07 1.07 | 1.53 1.10 1.01 | 1.54 1.09 0.99 | 1.44 | 1.66 1.01 1.02 1.06 | 1.65 1.04 1.05 1.10 | 1.03 1.03 1.09 | 1.04 1.02 1.09 | 1.08 1.09 1.15 | 0.94 0.95 1.00 | 1.04 1.02 1.06 |
| | 1900X 5800X 5950X 7950X | 1.63 1.07 1.07 1.10 | 1.53 1.10 1.01 1.06 | 1.54 1.09 0.99 1.05 | 1.44 1.08 1.00 1.01 | 1.66 1.01 1.02 | 1.65 1.04 1.05 1.10 1.14 | 1.03 1.03 1.09 1.09 | 1.04 1.02 1.09 1.12 | 1.08 1.09 1.15 1.13 | 0.94 0.95 1.00 0.99 | 1.04 1.02 1.06 1.07 |
| 3E | 1900X 5800X 5950X 7950X i7 6G | 1.63 1.07 1.07 1.10 1.08 | 1.53 1.10 1.01 1.06 1.10 | 1.54 1.09 0.99 1.05 1.08 | 1.44 1.08 1.00 1.01 | 1.66 1.01 1.02 1.06 1.07 | 1.65 1.04 1.05 1.10 | 1.03 1.03 1.09 1.09 1.02 | 1.04 1.02 1.09 1.12 0.99 | 1.08 1.09 1.15 1.13 | 0.94 0.95 1.00 0.99 0.94 | 1.04 1.02 1.06 1.07 1.04 |
| JARE | 1900X 5800X 5950X 7950X i7 6G i7 10G | 1.63 1.07 1.07 1.10 1.08 1.06 | 1.53 1.10 1.01 1.06 1.10 1.08 | 1.54 1.09 0.99 1.05 1.08 1.07 | 1.44 1.08 1.00 1.01 1.06 1.06 | 1.66 1.01 1.02 1.06 1.07 | 1.65 1.04 1.05 1.10 1.14 1.03 | 1.03 1.03 1.09 1.09 | 1.04 1.02 1.09 1.12 0.99 1.04 | 1.08 1.09 1.15 1.13 1.07 1.05 | 0.94 0.95 1.00 0.99 0.94 0.92 | 1.04 1.02 1.06 1.07 1.04 1.02 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 | 1.65 1.04 1.05 1.10 1.14 1.03 | 1.03 1.03 1.09 1.09 1.02 0.98 | 1.04 1.02 1.09 1.12 0.99 | 1.08 1.09 1.15 1.13 1.07 1.05 1.07 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 | 1.04 1.02 1.06 1.07 1.04 1.02 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 1.15 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 1.18 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 1.15 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 1.10 | 1.65 1.04 1.05 1.10 1.14 1.03 1.02 1.13 | 1.03 1.03 1.09 1.09 1.02 0.98 | 1.04 1.02 1.09 1.12 0.99 1.04 1.04 | 1.08 1.09 1.15 1.13 1.07 1.05 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 | 1.04 1.02 1.06 1.07 1.04 1.02 1.04 1.13 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 1.15 1.07 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 1.18 1.14 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 1.17 1.12 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 1.15 1.11 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 1.10 1.04 | 1.65 1.04 1.05 1.10 1.14 1.03 1.02 1.13 1.07 | 1.03 1.03 1.09 1.09 1.02 0.98 | 1.04 1.02 1.09 1.12 0.99 1.04 1.04 | 1.08 1.09 1.15 1.13 1.07 1.05 1.07 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 | 1.04 1.02 1.06 1.07 1.04 1.02 1.04 1.13 1.05 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 1.15 1.07 1.17 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 1.18 1.14 1.22 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 1.17 1.12 1.21 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 1.15 1.11 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 1.10 1.04 1.16 | 1.65 1.04 1.05 1.10 1.14 1.03 1.02 1.13 1.07 1.18 | 1.03 1.03 1.09 1.09 1.02 0.98 1.11 1.06 1.16 | 1.04 1.02 1.09 1.12 0.99 1.04 1.04 | 1.08 1.09 1.15 1.13 1.07 1.05 1.07 1.11 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 1.18 0.87 | 1.04 1.02 1.06 1.07 1.04 1.02 1.04 1.13 1.05 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 1.15 1.07 1.17 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 1.18 1.14 1.22 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 1.17 1.12 1.21 1.43 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 1.15 1.11 1.18 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 1.10 1.04 1.16 1.45 | 1.65 1.04 1.05 1.10 1.14 1.03 1.02 1.13 1.07 1.18 1.49 | 1.03 1.03 1.09 1.09 1.02 0.98 1.11 1.06 1.16 | 1.04 1.02 1.09 1.12 0.99 1.04 1.04 1.00 1.11 | 1.08 1.09 1.15 1.13 1.07 1.05 1.07 1.11 1.14 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 1.18 0.87 | 1.04 1.02 1.06 1.07 1.04 1.02 1.04 1.13 1.05 1.15 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 1.63 1.07 1.07 1.10 1.08 1.06 1.08 1.15 1.07 1.17 | 1.53 1.10 1.01 1.06 1.10 1.08 1.10 1.18 1.14 1.22 | 1.54 1.09 0.99 1.05 1.08 1.07 1.09 1.17 1.12 1.21 | 1.44 1.08 1.00 1.01 1.06 1.06 1.08 1.15 1.11 | 1.66 1.01 1.02 1.06 1.07 0.97 0.98 1.10 1.04 1.16 | 1.65 1.04 1.05 1.10 1.14 1.03 1.02 1.13 1.07 1.18 | 1.03 1.03 1.09 1.09 1.02 0.98 1.11 1.06 1.16 | 1.04 1.02 1.09 1.12 0.99 1.04 1.04 | 1.08 1.09 1.15 1.13 1.07 1.05 1.07 1.11 | 0.94 0.95 1.00 0.99 0.94 0.92 0.93 1.18 0.87 | 1.04 1.02 1.06 1.07 1.04 1.02 1.04 1.13 1.05 |

Table 5: Optimisation matrix for P-256

| $\mathbf{p}_{\scriptscriptstyle{-}}$ | 256 |
|--------------------------------------|-----|
| т - | 200 |

| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
|-------------|---|--|--|--|--|--|--|--|--|--|--|--|
| | opt on | | | | | | | | | | | |
| | 1900X | | 1.00 | 1.01 | 1.10 | 0.97 | 1.02 | 1.06 | 1.04 | 1.03 | 0.94 | 1.02 |
| | 5800X | 1.10 | | 1.02 | 1.12 | 1.08 | 1.14 | 1.19 | 1.16 | 1.12 | 1.02 | 1.09 |
| | 5950X | 1.10 | 0.97 | | 1.10 | 1.04 | 1.10 | 1.13 | 1.10 | 1.10 | 1.01 | 1.06 |
| | 7950X | 1.02 | 0.93 | 0.95 | | 0.96 | 1.01 | 1.05 | 1.05 | 1.06 | 0.98 | 1.00 |
| X | i7 6G | 1.11 | 1.05 | 1.07 | 1.17 | | 1.04 | 1.08 | 1.12 | 1.08 | 0.99 | 1.07 |
| IPI | i7 10G | 1.06 | 1.00 | 1.03 | 1.10 | 0.95 | | 1.01 | 1.04 | 1.03 | 0.95 | 1.02 |
| Ľ | i9 10G | 1.01 | 0.97 | 0.99 | 1.05 | 0.90 | 0.95 | | 0.98 | 1.00 | 1.13 | 1.00 |
| Мистірсу | i7 11G | 1.06 | 1.03 | 1.06 | 1.13 | 0.98 | 1.02 | 1.09 | | 1.01 | 0.92 | 1.03 |
| | i9 12G | 1.12 | 1.08 | 1.09 | 1.19 | 1.04 | 1.08 | 1.13 | 1.07 | | 0.92 | 1.07 |
| | i9 13G | 1.19 | 1.16 | 1.18 | 1.27 | 1.08 | 1.14 | 1.18 | 1.17 | 1.09 | | 1.14 |
| | Clang | 1.62 | 1.67 | 1.70 | 1.72 | 1.61 | 1.68 | 1.78 | 1.78 | 1.75 | 1.62 | 1.69 |
| | $\widetilde{\mathrm{GCC}}$ | 2.50 | 2.11 | 2.14 | 2.28 | 2.79 | 2.92 | 3.03 | 2.78 | 2.93 | 2.73 | 2.60 |
| | | | | | | | | | | | | |
| | Final | 1.62 | 1.79 | 1.80 | 1.72 | 1.78 | 1.77 | 1.78 | 1.81 | 1.75 | 1.77 | 1.76 |
| | Final | 1.62 | 1.79 | 1.80 | 1.72 | 1.78 | 1.77 | 1.78 | 1.81 | 1.75 | 1.77 | 1.76 |
| | | 1.62 | | 1.80 | 1.72 | | | | | | | |
| | 1900X | 1.62 | 1.79 | | | 1.78 0.98 1.02 | 1.77 1.04 1.10 | 1.78 1.03 1.08 | 1.81 0.98 1.02 | 1.75 1.02 1.07 | 1.77 1.25 1.06 | 1.04 |
| | | | | 1.07 | 1.06 | 0.98 | 1.04 | 1.03 1.08 | 0.98 | 1.02 | 1.25 | |
| | 1900X 5800X | 1.11 | 1.03 | 1.07 | 1.06 1.06 | 0.98 1.02 | 1.04 1.10 | 1.03 | 0.98 1.02 | 1.02 1.07 | 1.25 1.06 | 1.04 1.06 |
| | 1900X 5800X 5950X | 1.11 1.08 | 1.03 0.96 | 1.07 1.04 | 1.06 1.06 | 0.98 1.02 1.00 | 1.04 1.10 1.08 | 1.03 1.08 1.08 | 0.98 1.02 0.97 | 1.02 1.07 1.07 | 1.25 1.06 1.07 | 1.04 1.06 1.03 |
| RE | 1900X 5800X 5950X 7950X | 1.11 1.08 1.11 | 1.03 0.96 0.99 | 1.07 1.04 1.03 | 1.06 1.06 1.02 | 0.98 1.02 1.00 | 1.04 1.10 1.08 1.10 | 1.03 1.08 1.08 1.07 | 0.98 1.02 0.97 1.07 | 1.02 1.07 1.07 1.12 | 1.25 1.06 1.07 1.37 | 1.04 1.06 1.03 1.08 |
| UARE | 1900X 5800X 5950X 7950X i7 6G | 1.11 1.08 1.11 1.16 | 1.03 0.96 0.99 1.11 | 1.07 1.04 1.03 1.16 | 1.06 1.06 1.02 | 0.98 1.02 1.00 1.01 | 1.04 1.10 1.08 1.10 | 1.03 1.08 1.08 1.07 1.06 | 0.98 1.02 0.97 1.07 1.03 | 1.02 1.07 1.07 1.12 1.06 | 1.25 1.06 1.07 1.37 1.05 | 1.04 1.06 1.03 1.08 1.08 |
| Square | 1900X 5800X 5950X 7950X i7 6G i7 10G | 1.11 1.08 1.11 1.16 1.11 | 1.03 0.96 0.99 1.11 1.03 | 1.07 1.04 1.03 1.16 1.08 | 1.06 1.06 1.02 1.13 1.07 | 0.98 1.02 1.00 1.01 | 1.04 1.10 1.08 1.10 1.07 | 1.03 1.08 1.08 1.07 1.06 | 0.98 1.02 0.97 1.07 1.03 0.98 | 1.02 1.07 1.07 1.12 1.06 1.04 | 1.25 1.06 1.07 1.37 1.05 1.04 | 1.04 1.06 1.03 1.08 1.08 1.03 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G | 1.11 1.08 1.11 1.16 1.11 1.08 | 1.03 0.96 0.99 1.11 1.03 1.10 | 1.07 1.04 1.03 1.16 1.08 1.14 | 1.06 1.06 1.02 1.13 1.07 1.13 | 0.98 1.02 1.00 1.01 0.94 0.94 | 1.04 1.10 1.08 1.10 1.07 | 1.03 1.08 1.08 1.07 1.06 1.01 | 0.98 1.02 0.97 1.07 1.03 0.98 | 1.02 1.07 1.07 1.12 1.06 1.04 1.04 | 1.25 1.06 1.07 1.37 1.05 1.04 1.04 | 1.04 1.06 1.03 1.08 1.08 1.03 1.05 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G | 1.11 1.08 1.11 1.16 1.11 1.08 1.13 | 1.03 0.96 0.99 1.11 1.03 1.10 1.11 | 1.07 1.04 1.03 1.16 1.08 1.14 1.16 | 1.06 1.06 1.02 1.13 1.07 1.13 1.14 | 0.98 1.02 1.00 1.01 0.94 0.94 1.02 | 1.04 1.10 1.08 1.10 1.07 1.00 | 1.03 1.08 1.08 1.07 1.06 1.01 | 0.98 1.02 0.97 1.07 1.03 0.98 0.99 | 1.02 1.07 1.07 1.12 1.06 1.04 1.04 | 1.25 1.06 1.07 1.37 1.05 1.04 1.04 1.05 | 1.04 1.06 1.03 1.08 1.08 1.03 1.05 |
| S_{QUARE} | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 1.11 1.08 1.11 1.16 1.11 1.08 1.13 1.14 | 1.03 0.96 0.99 1.11 1.03 1.10 1.11 1.12 | 1.07 1.04 1.03 1.16 1.08 1.14 1.16 1.18 | 1.06 1.06 1.02 1.13 1.07 1.13 1.14 1.14 | 0.98 1.02 1.00 1.01 0.94 0.94 1.02 1.02 | 1.04 1.10 1.08 1.10 1.07 1.00 1.09 1.09 | 1.03 1.08 1.08 1.07 1.06 1.01 | 0.98 1.02 0.97 1.07 1.03 0.98 0.99 | 1.02 1.07 1.07 1.12 1.06 1.04 1.04 1.05 | 1.25 1.06 1.07 1.37 1.05 1.04 1.04 1.05 | 1.04 1.06 1.03 1.08 1.08 1.03 1.05 1.08 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G | 1.11 1.08 1.11 1.16 1.11 1.08 1.13 1.14 1.10 | 1.03 0.96 0.99 1.11 1.03 1.10 1.11 1.12 1.15 | 1.07 1.04 1.03 1.16 1.08 1.14 1.16 1.18 | 1.06 1.02 1.13 1.07 1.13 1.14 1.14 | 0.98 1.02 1.00 1.01 0.94 0.94 1.02 1.02 | 1.04 1.10 1.08 1.10 1.07 1.00 1.09 1.09 | 1.03 1.08 1.08 1.07 1.06 1.01 1.08 1.09 | 0.98 1.02 0.97 1.07 1.03 0.98 0.99 | 1.02 1.07 1.07 1.12 1.06 1.04 1.04 1.05 | 1.25 1.06 1.07 1.37 1.05 1.04 1.04 1.05 1.00 | 1.04 1.06 1.03 1.08 1.08 1.03 1.05 1.08 1.08 |

Table 6: Optimisation matrix for P-384

| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
|-------------|---|--|--|--|--|--|--|--|--|--|--|--|
| | | | | | | | | | | | | |
| | opt on | | 1.00 | 1.00 | 1.00 | 4 4 1 | 1 50 | 4 55 | 1.00 | 105 | 0.01 | 1.00 |
| | 1900X | 0.00 | 1.33 | 1.30 | 1.32 | 1.45 | 1.52 | 1.55 | 1.39 | 1.05 | 0.91 | 1.26 |
| | 5800X | 0.82 | 1 00 | 0.98 | 1.00 | 1.05 | 1.14 | 1.13 | 1.11 | 0.82 | 0.83 | 0.98 |
| | 5950X | 0.85 | 1.03 | 1 00 | 1.03 | 1.07 | 1.16 | 1.15 | 1.14 | 0.81 | 0.83 | 1.00 |
| | 7950X | 0.81 | 1.03 | 1.00 | 1.00 | 1.06 | 1.16 | 1.15 | 1.12 | 0.79 | 0.69 | 0.97 |
| ΓX | i7 6G | 0.80 | 1.08 | 1.06 | 1.09 | 0.00 | 1.10 | 1.08 | 1.10 | 0.78 | 0.68 | 0.96 |
| II. | i7 10G | 0.77 | 1.03 | 1.00 | 1.03 | 0.93 | 0.00 | 1.00 | 1.02 | 0.74 | 0.65 | 0.90 |
| Мистірсу | i9 10G i7 11G | 0.75 | 1.02 0.99 | 0.99 | 1.02 1.00 | 0.91 0.94 | 0.98 | 1.00 | 1.02 | $0.74 \\ 0.72$ | $0.64 \\ 0.62$ | $0.90 \\ 0.89$ |
| Ξ | i9 12G | 0.76 | | $\frac{0.96}{1.35}$ | | | 1.01 | | 1.39 | 0.72 | | 1.26 |
| | | 1.01 | 1.37 | | 1.33 | 1.43 | 1.57 | 1.54 | | 1.06 | 0.86 | |
| | i9 13G | 1.01 | 1.37 | 1.33 | 1.36 | 1.41 | 1.53 | 1.51 | 1.47 | 1.06 | | 1.29 |
| | Clang | 1.08 | 1.63 | 1.59 | 1.43 | 1.60 | 1.74 | 1.71 | 1.68 | 1.33 | 1.07 | 1.47 |
| | GCC | 1.88 | 2.15 | 2.10 | 2.16 | 3.06 | 3.29 | 3.27 | 3.05 | 2.31 | 2.03 | 2.48 |
| | | | | | | | | | | | | |
| | Final | 1.44 | 1.65 | 1.65 | 1.43 | 1.76 | 1.77 | 1.71 | 1.68 | 1.85 | 1.72 | 1.66 |
| | Final | 1.44 | 1.65 | 1.65 | 1.43 | 1.76 | 1.77 | 1.71 | 1.68 | 1.85 | 1.72 | 1.66 |
| | | 1.44 | | | | 1.76 1.41 | | | | 1.85 1.01 | | 1.66 |
| | 1900X | | 1.65 | 1.30 | 1.31 | 1.41 | 1.49 | 1.47 | 1.37 | 1.01 | 0.93 | 1.24 |
| | 1900X 5800X | 0.89 | | | 1.31 1.03 | | | | 1.37 1.18 | | 0.93 0.75 | 1.24 1.00 |
| | 1900X | | 1.29 | 1.30 | 1.31 | 1.41 1.13 | 1.49 1.18 | 1.47 1.16 | 1.37 | 1.01 0.80 | 0.93 | 1.24 |
| | 1900X 5800X 5950X | 0.89 0.85 | 1.29 0.99 | 1.30 1.01 | 1.31 1.03 | 1.41 1.13 1.13 | 1.49 1.18 1.20 | 1.47 1.16 1.17 | 1.37 1.18 1.16 | 1.01 0.80 0.81 | 0.93 0.75 0.75 | 1.24 1.00 1.00 |
| RE | 1900X 5800X 5950X 7950X | 0.89 0.85 0.86 | 1.29 0.99 1.00 | 1.30 1.01 1.02 | 1.31 1.03 1.03 | 1.41 1.13 1.13 | 1.49 1.18 1.20 1.22 | 1.47 1.16 1.17 1.22 | 1.37 1.18 1.16 1.19 | 1.01 0.80 0.81 0.83 | 0.93 0.75 0.75 0.77 | 1.24 1.00 1.00 1.02 |
| UARE | 1900X 5800X 5950X 7950X i7 6G | 0.89 0.85 0.86 0.80 | 1.29 0.99 1.00 0.99 | 1.30 1.01 1.02 1.00 | 1.31 1.03 1.03 | 1.41 1.13 1.13 1.17 | 1.49 1.18 1.20 1.22 | 1.47 1.16 1.17 1.22 1.03 | 1.37 1.18 1.16 1.19 | 1.01 0.80 0.81 0.83 0.75 | 0.93 0.75 0.75 0.77 0.70 | 1.24 1.00 1.00 1.02 0.93 |
| Square | 1900X 5800X 5950X 7950X i7 6G i7 10G | 0.89 0.85 0.86 0.80 0.79 | 1.29 0.99 1.00 0.99 0.99 | 1.30 1.01 1.02 1.00 1.01 | 1.31 1.03 1.03 1.05 1.02 | 1.41 1.13 1.13 1.17 | 1.49 1.18 1.20 1.22 1.04 | 1.47 1.16 1.17 1.22 1.03 | 1.37 1.18 1.16 1.19 1.07 1.03 | 1.01 0.80 0.81 0.83 0.75 0.74 | 0.93 0.75 0.75 0.77 0.70 0.69 | 1.24 1.00 1.00 1.02 0.93 0.91 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G | 0.89 0.85 0.86 0.80 0.79 0.78 | 1.29 0.99 1.00 0.99 0.99 1.02 | 1.30 1.01 1.02 1.00 1.01 1.04 | 1.31 1.03 1.03 1.05 1.02 1.04 | 1.41 1.13 1.13 1.17 0.96 0.96 | 1.49 1.18 1.20 1.22 1.04 | 1.47 1.16 1.17 1.22 1.03 0.98 | 1.37 1.18 1.16 1.19 1.07 1.03 | 1.01 0.80 0.81 0.83 0.75 0.74 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G | 0.89 0.85 0.86 0.80 0.79 0.78 0.80 | 1.29 0.99 1.00 0.99 0.99 1.02 0.98 | 1.30 1.01 1.02 1.00 1.01 1.04 1.00 | 1.31 1.03 1.03 1.05 1.02 1.04 1.00 | 1.41 1.13 1.13 1.17 0.96 0.96 0.97 | 1.49 1.18 1.20 1.22 1.04 1.01 1.02 | 1.47 1.16 1.17 1.22 1.03 0.98 | 1.37 1.18 1.16 1.19 1.07 1.03 1.08 | 1.01 0.80 0.81 0.83 0.75 0.74 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 0.64 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 0.90 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 0.89 0.85 0.86 0.80 0.79 0.78 0.80 1.06 | 1.29 0.99 1.00 0.99 0.99 1.02 0.98 1.35 1.41 | 1.30 1.01 1.02 1.00 1.01 1.04 1.00 1.38 1.44 | 1.31 1.03 1.03 1.05 1.02 1.04 1.00 1.36 1.42 | 1.41 1.13 1.13 1.17 0.96 0.96 0.97 1.49 1.64 | 1.49 1.18 1.20 1.22 1.04 1.01 1.02 1.56 1.74 | 1.47 1.16 1.17 1.22 1.03 0.98 1.02 1.57 1.71 | 1.37 1.18 1.16 1.19 1.07 1.03 1.08 | 1.01 0.80 0.81 0.83 0.75 0.74 0.72 0.69 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 0.64 0.94 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 0.90 1.29 1.38 |
| S_{QUARE} | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang | 0.89 0.85 0.86 0.80 0.79 0.78 0.80 1.06 1.10 | 1.29 0.99 1.00 0.99 0.99 1.02 0.98 1.35 1.41 | 1.30 1.01 1.02 1.00 1.01 1.04 1.00 1.38 1.44 | 1.31 1.03 1.03 1.05 1.02 1.04 1.00 1.36 1.42 | 1.41 1.13 1.13 1.17 0.96 0.96 0.97 1.49 1.55 | 1.49 1.18 1.20 1.22 1.04 1.01 1.02 1.56 1.74 | 1.47 1.16 1.17 1.22 1.03 0.98 1.02 1.57 1.71 | 1.37 1.18 1.16 1.19 1.07 1.03 1.08 | 1.01 0.80 0.81 0.83 0.75 0.74 0.72 0.69 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 0.64 0.94 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 0.90 1.29 1.38 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang GCC | 0.89 0.85 0.86 0.80 0.79 0.78 0.80 1.06 1.10 1.09 2.05 | 1.29 0.99 1.00 0.99 0.99 1.02 0.98 1.35 1.41 1.47 2.10 | 1.30 1.01 1.02 1.00 1.01 1.04 1.00 1.38 1.44 1.50 2.13 | 1.31 1.03 1.03 1.05 1.02 1.04 1.00 1.36 1.42 1.32 2.11 | 1.41 1.13 1.13 1.17 0.96 0.96 0.97 1.49 1.55 3.29 | 1.49 1.18 1.20 1.22 1.04 1.01 1.02 1.56 1.74 1.62 3.47 | 1.47 1.16 1.17 1.22 1.03 0.98 1.02 1.57 1.71 1.61 3.43 | 1.37 1.18 1.16 1.19 1.07 1.03 1.08 1.45 1.54 1.62 3.34 | 1.01 0.80 0.81 0.83 0.75 0.74 0.72 0.69 1.08 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 0.64 0.94 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 0.90 1.29 1.38 2.53 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang | 0.89 0.85 0.86 0.80 0.79 0.78 0.80 1.06 1.10 | 1.29 0.99 1.00 0.99 0.99 1.02 0.98 1.35 1.41 | 1.30 1.01 1.02 1.00 1.01 1.04 1.00 1.38 1.44 | 1.31 1.03 1.03 1.05 1.02 1.04 1.00 1.36 1.42 | 1.41 1.13 1.13 1.17 0.96 0.96 0.97 1.49 1.55 | 1.49 1.18 1.20 1.22 1.04 1.01 1.02 1.56 1.74 | 1.47 1.16 1.17 1.22 1.03 0.98 1.02 1.57 1.71 | 1.37 1.18 1.16 1.19 1.07 1.03 1.08 | 1.01 0.80 0.81 0.83 0.75 0.74 0.72 0.69 | 0.93 0.75 0.75 0.77 0.70 0.69 0.67 0.64 0.94 | 1.24 1.00 1.00 1.02 0.93 0.91 0.92 0.90 1.29 1.38 |

Table 7: Optimisation matrix for SIKEp434 $\,$

| α | rr | | 4 | \circ | 4 |
|----------|--------|------------------------|-------------|---------|----|
| ~ | I K | Er | ∖ /I | ∹≺ | ∕1 |
| k)] | \sim | $\perp \gamma_{\rm L}$ | ノコ | ., | 4 |

| | | | | | | тър. | | | | | | |
|-------------|---|--|--|--|--|--|--|--|--|--|--|--|
| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
| | ont on | | | | | | | | | | | |
| | opt on | | 1.00 | 1.00 | 1.13 | 1 49 | 1 50 | 1 07 | 1.00 | 1 1 1 | 0.06 | 1.21 |
| | 1900X | 1.13 | 1.06 | 1.09 | | 1.43 1.36 | 1.56 1.52 | 1.67 | 1.29 | 1.14 1.16 | $0.96 \\ 0.97$ | 1.21 |
| | 5800X 5950X | 1.13 | 0.97 | 1.00 | 1.07 1.05 | 1.35 | $\frac{1.52}{1.50}$ | 1.61 1.59 | 1.25 1.22 | 1.10 | 0.97 | 1.20 1.15 |
| | 7950X | 0.95 | 0.97 0.95 | 0.98 | 1.05 | 1.34 | 1.50 1.50 | 1.59 1.58 | 1.22 1.19 | 1.06 | 0.90 0.89 | 1.13 |
| | i7 6G | 0.93 | 0.90 | 0.98 | 0.94 | 1.54 | 1.10 | 1.38 1.19 | 1.19 | 0.89 | 0.89 0.75 | 0.95 |
| Ľ | i7 10G | 0.84 | 0.90 0.84 | 0.92 | 0.94 | 0.90 | 1.10 | 1.19 | 0.99 | 0.89 0.88 | 0.75 | 0.90 |
| Мистірсу | i9 10G | 0.81 0.79 | 0.84 0.81 | 0.80 | 0.90 0.85 | 0.90 0.85 | 0.94 | 1.07 | 0.99 0.95 | 0.86 | 0.73 | 0.86 |
| UL | i7 11G | 0.79 | 0.81 0.85 | 0.88 | 0.83 | 0.83 | 1.06 | 1.14 | 0.90 | 0.87 | 0.75 | 0.80 |
| \geq | i9 12G | 0.98 | 1.01 | 1.04 | 1.06 | 1.37 | 1.52 | 1.60 | 1.20 | 0.01 | 0.15 | 1.14 |
| | i9 13G | 1.31 | 1.16 | 1.19 | 1.23 | 1.56 | 1.71 | 1.83 | 1.43 | 1.19 | 0.00 | 1.34 |
| | | | | | | | | | | | | |
| | Clang | 1.55 | 1.74 | 1.78 | 1.64 | 2.04 | 2.27 | 2.40 | 2.20 | 1.94 | 1.69 | 1.91 |
| | GCC | 2.15 | 2.35 | 2.41 | 2.03 | 3.25 | 3.60 | 3.83 | 3.69 | 2.64 | 2.25 | 2.74 |
| | | | | | | | | | | | | |
| | Final | 1.96 | 2.15 | 2.15 | 1.93 | 2.41 | 2.41 | 2.40 | 2.32 | 2.25 | 2.30 | 2.22 |
| | Final | 1.96 | 2.15 | 2.15 | 1.93 | 2.41 | 2.41 | 2.40 | 2.32 | 2.25 | 2.30 | 2.22 |
| | Final 1900X | 1.96 | 2.15 1.08 | 2.15 | 1.93 1.16 | 2.41 1.59 | 2.41 1.60 | 2.401.70 | 2.32 1.30 | 2.25 1.11 | 2.300.86 | 2.22 1.22 |
| | | 1.96 | | | | | | | | | | |
| | 1900X | | | 1.10 | 1.16 | 1.59 | 1.60 | 1.70 | 1.30 | 1.11 | 0.86 | 1.22 |
| | 1900X 5800X | 1.04 | 1.08 | 1.10 | 1.16 1.07 | 1.59 1.49 | 1.60 1.48 | 1.70 1.59 | 1.30 1.23 | 1.11 1.08 | 0.86 0.83 | 1.22 1.16 |
| | 1900X 5800X 5950X 7950X i7 6G | 1.04 0.98 0.95 0.79 | 1.08 0.98 0.95 0.83 | 1.10 1.02 0.96 0.83 | 1.16 1.07 1.06 | 1.59 1.49 1.51 1.40 | 1.60 1.48 1.53 | 1.70 1.59 1.61 1.49 1.07 | 1.30 1.23 1.21 1.16 1.00 | 1.11 1.08 1.05 1.00 0.84 | 0.86 0.83 0.80 0.76 0.66 | 1.22 1.16 1.15 1.09 0.88 |
| ıre | 1900X 5800X 5950X 7950X i7 6G i7 10G | 1.04 0.98 0.95 0.79 0.80 | 1.08 0.98 0.95 0.83 0.83 | 1.10 1.02 0.96 0.83 0.85 | 1.16 1.07 1.06 0.88 0.90 | 1.59 1.49 1.51 | 1.60 1.48 1.53 1.43 | 1.70 1.59 1.61 1.49 | 1.30 1.23 1.21 1.16 | 1.11 1.08 1.05 1.00 | 0.86 0.83 0.80 0.76 0.66 0.63 | 1.22 1.16 1.15 1.09 |
| JUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G | 1.04 0.98 0.95 0.79 0.80 0.77 | 1.08 0.98 0.95 0.83 0.83 0.79 | 1.10 1.02 0.96 0.83 0.85 0.81 | 1.16 1.07 1.06 0.88 0.90 0.85 | 1.59 1.49 1.51 1.40 1.01 0.94 | 1.60 1.48 1.53 1.43 0.99 | 1.70 1.59 1.61 1.49 1.07 1.08 | 1.30 1.23 1.21 1.16 1.00 | 1.11 1.08 1.05 1.00 0.84 0.81 0.77 | 0.86 0.83 0.80 0.76 0.66 0.63 | 1.22 1.16 1.15 1.09 0.88 0.88 0.83 |
| Square | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G | 1.04 0.98 0.95 0.79 0.80 0.77 0.83 | 1.08 0.98 0.95 0.83 0.83 0.79 0.86 | 1.10 1.02 0.96 0.83 0.85 0.81 0.87 | 1.16 1.07 1.06 0.88 0.90 | 1.59 1.49 1.51 1.40 | 1.60 1.48 1.53 1.43 0.99 | 1.70 1.59 1.61 1.49 1.07 | 1.30 1.23 1.21 1.16 1.00 0.98 0.92 | 1.11 1.08 1.05 1.00 0.84 0.81 | 0.86 0.83 0.80 0.76 0.66 0.63 | 1.22 1.16 1.15 1.09 0.88 0.88 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G | 1.04 0.98 0.95 0.79 0.80 0.77 0.83 | 1.08 0.98 0.95 0.83 0.79 0.86 1.03 | 1.10 1.02 0.96 0.83 0.85 0.81 0.87 | 1.16 1.07 1.06 0.88 0.90 0.85 0.93 1.10 | 1.59 1.49 1.51 1.40 1.01 0.94 | 1.60 1.48 1.53 1.43 0.99 | 1.70 1.59 1.61 1.49 1.07 1.08 | 1.30 1.23 1.21 1.16 1.00 0.98 | 1.11 1.08 1.05 1.00 0.84 0.81 0.77 0.85 | 0.86 0.83 0.80 0.76 0.66 0.63 | 1.22 1.16 1.15 1.09 0.88 0.88 0.83 |
| S_{QUARE} | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G | 1.04 0.98 0.95 0.79 0.80 0.77 0.83 | 1.08 0.98 0.95 0.83 0.83 0.79 0.86 | 1.10 1.02 0.96 0.83 0.85 0.81 0.87 | 1.16 1.07 1.06 0.88 0.90 0.85 0.93 | 1.59 1.49 1.51 1.40 1.01 0.94 1.12 | 1.60 1.48 1.53 1.43 0.99 0.96 1.09 | 1.70 1.59 1.61 1.49 1.07 1.08 | 1.30 1.23 1.21 1.16 1.00 0.98 0.92 | 1.11 1.08 1.05 1.00 0.84 0.81 0.77 | 0.86 0.83 0.80 0.76 0.66 0.63 0.61 0.66 | 1.22 1.16 1.15 1.09 0.88 0.88 0.83 0.93 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 1.04 0.98 0.95 0.79 0.80 0.77 0.83 | 1.08 0.98 0.95 0.83 0.79 0.86 1.03 1.29 | 1.10 1.02 0.96 0.83 0.85 0.81 0.87 1.06 | 1.16 1.07 1.06 0.88 0.90 0.85 0.93 1.10 1.37 | 1.59 1.49 1.51 1.40 1.01 0.94 1.12 1.48 | 1.60 1.48 1.53 1.43 0.99 0.96 1.09 1.50 1.93 | 1.70 1.59 1.61 1.49 1.07 1.08 1.19 1.57 2.07 | 1.30 1.23 1.21 1.16 1.00 0.98 0.92 | 1.11 1.08 1.05 1.00 0.84 0.81 0.77 0.85 | 0.86 0.83 0.80 0.76 0.66 0.63 0.61 0.66 0.77 | 1.22 1.16 1.15 1.09 0.88 0.88 0.83 0.93 1.14 1.48 |
| SQUARE | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G | 1.04 0.98 0.95 0.79 0.80 0.77 0.83 0.99 | 1.08 0.98 0.95 0.83 0.79 0.86 1.03 | 1.10 1.02 0.96 0.83 0.85 0.81 0.87 | 1.16 1.07 1.06 0.88 0.90 0.85 0.93 1.10 | 1.59 1.49 1.51 1.40 1.01 0.94 1.12 1.48 1.95 | 1.60 1.48 1.53 1.43 0.99 0.96 1.09 1.50 | 1.70 1.59 1.61 1.49 1.07 1.08 | 1.30 1.23 1.21 1.16 1.00 0.98 0.92 | 1.11 1.08 1.05 1.00 0.84 0.81 0.77 0.85 | 0.86 0.83 0.80 0.76 0.66 0.63 0.61 0.66 | 1.22 1.16 1.15 1.09 0.88 0.88 0.83 0.93 1.14 |

Table 8: Optimisation matrix for Curve448

| | Cu | ırve4 | 48 |
|------|-------|-------|-------|
| 950X | 7950X | 59 Z | 7 10G |

| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
|-------------------|----------------------------------|-------|-------|-------|-------|-------|--------|--------|--------|--------|--------|------|
| | opt on | | | | | | | | | | | |
| | 1900X | | 1.18 | 1.18 | 1.16 | 1.14 | 1.14 | 1.13 | 1.16 | 1.04 | 0.91 | 1.10 |
| | 5800X | 0.96 | | 1.00 | 0.99 | 1.08 | 1.08 | 1.06 | 1.06 | 1.01 | 0.90 | 1.01 |
| | 5950X | 0.97 | 1.02 | | 0.99 | 1.11 | 1.09 | 1.07 | 1.06 | 1.00 | 0.88 | 1.02 |
| | 7950X | 0.97 | 1.04 | 1.04 | | 1.08 | 1.09 | 1.07 | 1.03 | 0.99 | 0.88 | 1.02 |
| × | i7 6G | 0.95 | 1.01 | 1.02 | 1.00 | | 0.99 | 0.97 | 0.98 | 0.92 | 0.81 | 0.96 |
| Multiply | i7 10G | 0.92 | 1.03 | 1.03 | 1.00 | 1.00 | | 0.98 | 0.98 | 0.94 | 0.82 | 0.97 |
| T.T | i9 10G | 0.95 | 1.03 | 1.03 | 1.02 | 1.03 | 1.00 | | 0.99 | 0.93 | 0.83 | 0.98 |
| Σ | i7 11G | 0.97 | 1.08 | 1.08 | 1.06 | 1.08 | 1.08 | 1.04 | | 0.97 | 0.86 | 1.02 |
| | i9 12G | 1.03 | 1.21 | 1.19 | 1.16 | 1.16 | 1.16 | 1.13 | 1.15 | | 0.86 | 1.10 |
| | i9 13G | 1.13 | 1.34 | 1.33 | 1.31 | 1.32 | 1.32 | 1.29 | 1.47 | 1.12 | | 1.26 |
| | Clang | 1.07 | 1.10 | 1.10 | 1.08 | 1.37 | 1.37 | 1.34 | 1.29 | 1.15 | 1.11 | 1.19 |
| | $\widetilde{\operatorname{GCC}}$ | 0.88 | 0.99 | 0.99 | 0.99 | 1.09 | 1.08 | 1.06 | 1.04 | 0.95 | 0.84 | 0.99 |
| | Final | 0.96 | 0.99 | 0.99 | 1.00 | 1.09 | 1.10 | 1.10 | 1.06 | 1.03 | 1.03 | 1.04 |
| | 1900X | | 1.01 | 1.02 | 1.00 | 1.05 | 1.08 | 1.08 | 1.05 | 1.10 | 0.99 | 1.04 |
| | 5800X | 1.08 | - | 1.01 | 1.02 | 1.08 | 1.11 | 1.11 | 1.03 | 1.13 | 1.02 | 1.06 |
| | 5950X | 1.08 | 1.00 | | 1.00 | 1.09 | 1.11 | 1.11 | 1.07 | 1.15 | 1.04 | 1.06 |
| | 7950X | 1.05 | 1.01 | 1.02 | | 1.06 | 1.09 | 1.09 | 1.04 | 1.13 | 1.02 | 1.05 |
| | i7 6G | 1.07 | 1.06 | 1.07 | 1.06 | | 1.01 | 1.01 | 1.00 | 1.14 | 1.02 | 1.04 |
| RE | i7 10G | 1.06 | 1.05 | 1.06 | 1.04 | 0.97 | | 0.99 | 1.01 | 1.18 | 1.06 | 1.04 |
| SQUARE | i9 10G | 1.05 | 1.02 | 1.03 | 1.01 | 0.99 | 1.02 | | 1.01 | 1.11 | 1.01 | 1.02 |
| $S_{\mathcal{O}}$ | i7 11G | 1.08 | 1.06 | 1.05 | 1.04 | 1.02 | 1.07 | 1.04 | | 1.12 | 1.01 | 1.05 |
| | i9 12G | 1.06 | 1.03 | 1.03 | 1.03 | 1.02 | 1.06 | 1.07 | 1.00 | | 0.91 | 1.02 |
| | i9 13G | 1.13 | 1.10 | 1.12 | 1.08 | 1.15 | 1.19 | 1.20 | 1.15 | 1.11 | | 1.12 |
| | Clang | 1.06 | 1.06 | 1.08 | 1.08 | 1.08 | 1.11 | 1.11 | 1.10 | 1.11 | 0.99 | 1.08 |
| | $\widetilde{\operatorname{GCC}}$ | 1.03 | 1.07 | 1.08 | 1.06 | 1.01 | 1.05 | 1.05 | 1.03 | 1.05 | 0.94 | 1.04 |
| | Final | 1.03 | 1.07 | 1.08 | 1.06 | 1.05 | 1.05 | 1.06 | 1.03 | 1.05 | 1.04 | 1.05 |

Table 9: Optimisation matrix for P-521

| \mathbf{D} | \mathbf{r} | 0 | 1 |
|--------------|--------------|---|---|
| Ρ- | റ | 1 | п |

| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
|---|---|--------------------------------------|--|--|--|--|--|--|--|--|--|--|
| | opt on | | | | | | | | | | | |
| | 1900X | | 1.14 | 1.14 | 1.10 | 1.18 | 1.17 | 1.21 | 1.23 | 1.07 | 0.97 | 1.12 |
| | 5800X | 0.99 | | 1.00 | 0.98 | 1.09 | 1.08 | 1.13 | 1.08 | 1.06 | 0.94 | 1.03 |
| | 5950X | 0.99 | 1.00 | | 0.96 | 1.09 | 1.07 | 1.12 | 1.05 | 1.07 | 0.96 | 1.03 |
| | 7950X | 1.03 | 1.07 | 1.06 | | 1.16 | 1.13 | 1.20 | 1.18 | 1.06 | 0.97 | 1.08 |
| × | i7 6G | 0.97 | 1.01 | 1.01 | 0.98 | | 0.97 | 1.03 | 1.00 | 1.03 | 0.95 | 1.00 |
| Multiply | i7 10G | 0.97 | 1.04 | 1.04 | 1.00 | 1.05 | | 1.05 | 1.01 | 1.05 | 0.96 | 1.02 |
| E | i9 10G | 0.94 | 1.00 | 1.01 | 0.98 | 1.02 | 0.97 | | 0.99 | 1.02 | 0.92 | 0.98 |
| Mu | i7 11G | 0.97 | 1.05 | 1.05 | 0.99 | 1.05 | 1.05 | 1.08 | | 0.97 | 1.03 | 1.03 |
| | i9 12G | 1.05 | 1.19 | 1.20 | 1.13 | 1.22 | 1.22 | 1.23 | 1.30 | | 0.91 | 1.14 |
| | i9 13G | 1.15 | 1.28 | 1.28 | 1.22 | 1.42 | 1.37 | 1.47 | 1.46 | 1.10 | | 1.27 |
| | Clang | 1.13 | 1.25 | 1.25 | 1.19 | 1.47 | 1.45 | 1.51 | 1.46 | 1.39 | 1.19 | 1.32 |
| | $\overline{\mathrm{GCC}}$ | 1.02 | 1.15 | 1.16 | 1.10 | 0.96 | 0.94 | 0.98 | 0.95 | 0.94 | 0.87 | 1.00 |
| | Final | 1.09 | 1.16 | 1.16 | 1.14 | 0.96 | 0.97 | 0.98 | 0.96 | 0.97 | 0.96 | 1.03 |
| | | | | | | | | | | | | |
| | 1900X | | 1.04 | 1.06 | 1.05 | 1.14 | 1.12 | 1.13 | 1.07 | 1.20 | 1.01 | 1.08 |
| | 5800X | 1.04 | | 1.02 | 1.04 | 1.18 | 1.15 | 1.15 | 1.18 | 1.25 | 1.06 | 1.10 |
| | 5950X | 1.02 | 0.99 | | | | | | 1.10 | | 1.00 | |
| | F0F037 | | 0.99 | | 1.01 | 1.15 | 1.16 | 1.15 | 1.08 | 1.26 | 1.07 | 1.09 |
| | 7950X | 1.03 | 1.01 | 1.03 | 1.01 | $1.15 \\ 1.16$ | | | | | | 1.09 1.07 |
| 63 | i7~6G | 0.98 | 1.01 1.01 | 1.02 | 1.06 | 1.16 | 1.16 | 1.15 1.15 0.99 | 1.08 1.06 1.03 | 1.26 1.18 1.22 | 1.07 1.00 1.08 | 1.07 1.03 |
| \RE | i7 6G i7 10G | $0.98 \\ 0.97$ | 1.01 1.01 0.99 | 1.02 1.00 | 1.06 1.02 | 1.16 | 1.16 1.14 0.98 | $1.15 \\ 1.15$ | 1.08 1.06 1.03 0.98 | 1.26 1.18 1.22 1.25 | 1.07 1.00 1.08 1.08 | 1.07 1.03 1.03 |
| QUARE | i7 6G i7 10G i9 10G | 0.98 0.97 0.98 | 1.01 1.01 0.99 1.02 | 1.02 1.00 1.02 | 1.06 1.02 1.04 | 1.16 1.02 0.99 | 1.16 1.14 0.98 0.97 | 1.15 1.15 0.99 0.99 | 1.08 1.06 1.03 | 1.26 1.18 1.22 1.25 1.28 | 1.07 1.00 1.08 1.08 1.09 | 1.07 1.03 1.03 1.04 |
| SQUARE | i7 6G i7 10G i9 10G i7 11G | 0.98 0.97 0.98 1.03 | 1.01 1.01 0.99 1.02 | 1.02 1.00 1.02 1.07 | 1.06 1.02 1.04 1.08 | 1.16 1.02 0.99 1.12 | 1.16 1.14 0.98 0.97 1.10 | 1.15 1.15 0.99 0.99 | 1.08 1.06 1.03 0.98 1.01 | 1.26 1.18 1.22 1.25 | 1.07 1.00 1.08 1.08 1.09 1.05 | 1.07 1.03 1.03 1.04 1.08 |
| $\mathbf{S}_{\mathbf{Q}\mathbf{U}\mathbf{A}\mathbf{R}\mathbf{E}}$ | i7 6G i7 10G i9 10G i7 11G i9 12G | 0.98 0.97 0.98 1.03 1.03 | 1.01 1.01 0.99 1.02 1.06 1.04 | 1.02 1.00 1.02 1.07 1.08 | 1.06 1.02 1.04 1.08 1.04 | 1.16 1.02 0.99 1.12 1.11 | 1.16 1.14 0.98 0.97 1.10 1.10 | 1.15 1.15 0.99 0.99 1.11 1.10 | 1.08 1.06 1.03 0.98 1.01 | 1.26 1.18 1.22 1.25 1.28 1.22 | 1.07 1.00 1.08 1.08 1.09 | 1.07 1.03 1.03 1.04 1.08 1.03 |
| $\mathbf{S}_{\mathbf{Q}\mathbf{U}\mathbf{A}\mathbf{R}\mathbf{E}}$ | i7 6G i7 10G i9 10G i7 11G | 0.98 0.97 0.98 1.03 | 1.01 1.01 0.99 1.02 | 1.02 1.00 1.02 1.07 | 1.06 1.02 1.04 1.08 | 1.16 1.02 0.99 1.12 | 1.16 1.14 0.98 0.97 1.10 | 1.15 1.15 0.99 0.99 | 1.08 1.06 1.03 0.98 1.01 | 1.26 1.18 1.22 1.25 1.28 | 1.07 1.00 1.08 1.08 1.09 1.05 | 1.07 1.03 1.03 1.04 1.08 |
| $\mathbf{S}_{\mathbf{Q}\mathbf{U}\mathbf{A}\mathbf{R}\mathbf{E}}$ | i7 6G i7 10G i9 10G i7 11G i9 12G | 0.98 0.97 0.98 1.03 1.03 | 1.01 1.01 0.99 1.02 1.06 1.04 | 1.02 1.00 1.02 1.07 1.08 | 1.06 1.02 1.04 1.08 1.04 | 1.16 1.02 0.99 1.12 1.11 | 1.16 1.14 0.98 0.97 1.10 1.10 | 1.15 1.15 0.99 0.99 1.11 1.10 | 1.08 1.06 1.03 0.98 1.01 | 1.26 1.18 1.22 1.25 1.28 1.22 | 1.07 1.00 1.08 1.08 1.09 1.05 | 1.07 1.03 1.03 1.04 1.08 1.03 |
| SQUARE | i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G | 0.98 0.97 0.98 1.03 1.03 | 1.01 1.01 0.99 1.02 1.06 1.04 | 1.02 1.00 1.02 1.07 1.08 1.12 | 1.06 1.02 1.04 1.08 1.04 1.13 | 1.16 1.02 0.99 1.12 1.11 1.30 | 1.16 1.14 0.98 0.97 1.10 1.29 | 1.15 1.15 0.99 0.99 1.11 1.10 1.29 | 1.08 1.06 1.03 0.98 1.01 1.02 | 1.26 1.18 1.22 1.25 1.28 1.22 | 1.07 1.00 1.08 1.08 1.09 1.05 0.85 | 1.07 1.03 1.03 1.04 1.08 1.03 1.18 |

Table 10: Optimisation matrix for Poly1305

| | | | | | Po | oly13 | 05 | | | | | |
|----------|------------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|--------------|
| | 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 | 1.15 | 1.14 | 1.10 | 1.11 | 1.13 | 1.00 | 1.20 | 1.18 | 1.11 |
| | 5800X | 1.10 | | 1.03 | 1.03 | 1.09 | 1.10 | 1.11 | 0.98 | 1.12 | 1.87 | 1.12 |
| | 5950X | 1.16 | 0.99 | | 1.02 | 1.12 | 1.13 | 1.13 | 1.05 | 1.25 | 1.23 | 1.11 |
| | 7950X | 1.11 | 1.04 | 1.05 | 1 10 | 1.12 | 1.12 | 1.14 | 1.02 | 1.19 | 1.17 | 1.09 |
| ΓΥ | i7 6G i7 10G | 1.18 1.17 | 1.13 1.12 | 1.14 1.16 | 1.10 1.10 | 1.03 | 1.00 | 1.05 | 0.94 | 1.26 1.35 | 1.25 1.36 | 1.10 1.12 |
| TIF. | i9 10G | 1.17 | 1.14 | 1.10 | 1.16 | 1.00 | 1.00 | 1.00 | 0.90 | 1.33 1.43 | 1.42 | 1.12 |
| Multiply | i7 11G | 1.15 | 1.12 | 1.11 | 1.11 | 1.03 | 1.07 | 1.03 | 0.00 | 1.35 | 1.37 | 1.13 |
| 2 | i9 12G | 1.15 | 1.02 | 1.03 | 1.05 | 1.02 | 1.03 | 1.03 | 0.91 | | 0.98 | 1.02 |
| | $i9\ 13G$ | 1.20 | 1.06 | 1.07 | 1.06 | 1.03 | 1.06 | 1.03 | 0.91 | 1.02 | | 1.04 |
| | Clang | 1.14 | 1.09 | 1.13 | 1.12 | 1.15 | 1.15 | 1.15 | 1.02 | 1.28 | 1.34 | 1.16 |
| | \overline{GCC} | 1.13 | 1.15 | 1.15 | 1.13 | 1.27 | 1.29 | 1.27 | 1.09 | 1.46 | 1.46 | 1.23 |
| | Final | 1.13 | 1.10 | 1.13 | 1.12 | 1.15 | 1.15 | 1.15 | 1.12 | 1.28 | 1.37 | 1.17 |
| | 1900X | | 1.07 | 1.08 | 1.05 | 1.10 | 1.18 | 1.14 | 1.15 | 1.17 | 1.16 | 1.11 |
| | 5800X | 1.09 | 1.01 | 1.00 | 1.03 | 1.05 | 1.10 | 1.14 | 1.16 | 1.24 | 1.25 | 1.09 |
| | 5950X | 1.34 | 0.99 | 1.01 | 1.03 | 1.10 | 1.15 | 1.15 | 1.16 | 1.12 | 1.11 | 1.11 |
| | 7950X | 1.14 | 1.08 | 1.07 | | 1.18 | 1.16 | 1.16 | 1.10 | 1.16 | 1.75 | 1.17 |
| (c) | i7 6G | 1.10 | 1.20 | 1.21 | 1.21 | | 1.05 | 1.04 | 1.05 | 1.41 | 1.44 | 1.16 |
| ARI | i7 10G | 1.12 | 1.13 | 1.14 | 1.12 | 0.95 | | 1.00 | 1.05 | 1.45 | 1.66 | 1.15 |
| SQUARE | i9 10G | 1.11 | 1.20 | 1.21 1.13 | 1.24 | 0.96 | 1.05 | 1.00 | 1.13 | 1.39 | 1.40 | 1.16 |
| ∞ | i7 11G i9 12G | 1.15 1.08 | 1.13 1.09 | 1.13 | 1.14 | 1.02 1.02 | 1.07 1.07 | 1.06 1.06 | 1.03 | 1.43 | 1.44 0.99 | 1.15 1.05 |
| | i9 13G | 1.08 | 1.09 | 1.10 | 1.07 | 1.02 | 1.05 | 1.05 | 1.05 | 1.01 | 0.33 | 1.03 |
| | Clang GCC | 1.04 1.11 | 1.11 1.27 | 1.11 1.28 | 1.11 1.21 | 1.10 1.28 | 1.15 1.35 | 1.15 1.33 | 1.13 1.28 | 1.21 1.29 | 1.34 1.28 | 1.14 1.27 |
| | Final | 1.04 | 1.12 | 1.11 | 1.11 | 1.15 | 1.15 | 1.15 | 1.13 | 1.21 | 1.29 | 1.14 |

Table 11: Optimisation matrix for secp256k1-Dettman

| | secp 256k1-Dettman | | | | | | | | | | | |
|----------------------------|--------------------|-------|-------|-------|-------|-------|--------|--------|--------|--------|--------|------|
| | run on | 1900X | 5800X | 5950X | 7950X | i7 6G | i7 10G | i9 10G | i7 11G | i9 12G | i9 13G | G.M. |
| | opt on | | | | | | | | | | | |
| | 1900X | | 1.12 | 1.12 | 1.11 | 1.09 | 1.16 | 1.10 | 1.07 | 1.28 | 1.18 | 1.12 |
| | 5800X | 1.07 | | 0.98 | 1.04 | 1.02 | 1.07 | 1.00 | 1.03 | 1.22 | 1.13 | 1.05 |
| | 5950X | 1.08 | 1.01 | | 1.06 | 1.09 | 1.10 | 1.04 | 1.11 | 1.20 | 1.11 | 1.08 |
| | 7950X | 1.05 | 1.04 | 1.03 | | 1.03 | 1.07 | 1.01 | 1.03 | 1.18 | 1.09 | 1.05 |
| χ | i7 6G | 1.05 | 1.15 | 1.14 | 1.16 | | 1.06 | 0.97 | 1.05 | 1.21 | 1.45 | 1.12 |
| Multiply | i7 10G | 1.02 | 1.07 | 1.07 | 1.07 | 0.98 | | 0.94 | 0.98 | 1.25 | 1.15 | 1.05 |
| ILT | i9 10G | 1.08 | 1.15 | 1.12 | 1.15 | 1.02 | 1.08 | | 1.11 | 1.18 | 1.09 | 1.10 |
| M | i7 11G | 1.03 | 1.07 | 1.06 | 1.08 | 1.03 | 1.06 | 1.00 | | 1.17 | 1.08 | 1.06 |
| . , | i9 12G | 1.01 | 1.03 | 1.03 | 1.02 | 0.97 | 1.03 | 0.94 | 0.98 | 4 00 | 0.92 | 0.99 |
| | i9 13G | 1.07 | 1.12 | 1.11 | 1.11 | 1.06 | 1.10 | 1.03 | 1.04 | 1.09 | | 1.07 |
| | Clang | 0.95 | 1.07 | 1.07 | 1.08 | 1.11 | 1.15 | 1.08 | 1.07 | 1.18 | 1.09 | 1.08 |
| | GCC | 1.16 | 1.37 | 1.36 | 1.35 | 1.16 | 1.20 | 1.14 | 1.12 | 1.22 | 1.13 | 1.22 |
| | Final | 0.95 | 1.07 | 1.09 | 1.08 | 1.15 | 1.15 | 1.16 | 1.09 | 1.18 | 1.18 | 1.11 |
| | | 0.00 | | | | | | | | | | |
| | 1900X | | 1.05 | 1.06 | 1.08 | 1.12 | 1.12 | 1.12 | 1.14 | 1.17 | 1.16 | 1.10 |
| | 5800X | 1.08 | | 0.99 | 1.04 | 1.08 | 1.09 | 1.10 | 1.07 | 1.13 | 1.65 | 1.11 |
| | 5950X | 1.11 | 0.99 | | 1.06 | 1.09 | 1.10 | 1.10 | 1.10 | 1.18 | 1.18 | 1.09 |
| | 7950X | 1.08 | 1.04 | 1.05 | | 1.07 | 1.08 | 1.08 | 1.08 | 1.14 | 1.14 | 1.07 |
| | i7 6G | 1.10 | 1.07 | 1.07 | 1.11 | | 1.01 | 1.01 | 1.03 | 1.27 | 1.26 | 1.09 |
| RE | i7 10G | 1.11 | 1.11 | 1.12 | 1.13 | 1.00 | | 1.01 | 1.03 | 1.23 | 1.22 | 1.09 |
| SQUARE | i9 10G | 1.11 | 1.10 | 1.10 | 1.10 | 1.00 | 1.01 | | 0.99 | 1.19 | 1.19 | 1.08 |
| $\mathbf{S}_{\mathcal{C}}$ | i7 11G | 1.10 | 1.12 | 1.11 | 1.12 | 1.05 | 1.06 | 1.07 | | 1.25 | 1.24 | 1.11 |
| | i9 12G | 1.04 | 1.05 | 1.05 | 1.09 | 1.04 | 1.05 | 1.04 | 1.03 | | 0.99 | 1.04 |
| | i9 13G | 1.10 | 1.07 | 1.08 | 1.06 | 1.04 | 1.06 | 1.04 | 1.00 | 1.01 | | 1.04 |
| | Clang | 0.93 | 1.02 | 1.02 | 1.01 | 1.06 | 1.07 | 1.07 | 1.09 | 1.11 | 1.19 | 1.05 |
| | GCC | 1.09 | 1.13 | 1.13 | 1.21 | 1.17 | 1.18 | 1.18 | 1.13 | 1.10 | 1.12 | 1.14 |

Final 0.93 1.03 1.02 1.01 1.06 1.07 1.07 1.10 1.10 1.12 1.05

Table 12: Optimisation matrix for secp256k1

| | | | | | sec | ep256 | ik1 | | | | | |
|---------------|---|--|--|--|--|--|--|--|--|--|--|--|
| | 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 | 1.09 1.07 1.18 1.06 1.10 1.09 | 1.07 1.00 1.00 1.11 1.03 1.03 | 1.04 0.99 0.99 1.10 1.02 1.02 | 1.07 1.11 1.07 1.14 1.09 1.08 1.15 | 1.00 1.02 1.02 0.97 0.93 0.92 1.02 | 1.07 1.09 1.09 1.04 1.07 1.02 | 1.09 1.11 1.11 1.05 1.09 1.01 | 1.06 1.08 1.07 1.05 1.09 1.02 0.99 | 1.12 1.15 1.14 1.11 1.13 1.10 1.06 1.09 | 1.02 1.04 1.03 1.01 1.02 0.99 0.96 0.98 | 1.05 1.07 1.06 1.03 1.09 1.03 1.01 |
| N | i9 12G i9 13G Clang GCC Final | 1.07 1.17 1.86 2.52 1.86 | 1.04 1.15 1.89 2.21 1.90 | 1.03 1.13 1.88 2.19 1.91 | 1.11 1.19 1.82 2.29 1.82 | 0.98 1.04 1.76 2.80 1.92 | 1.05 1.12 1.89 3.00 1.89 | 1.06 1.13 1.93 3.04 1.93 | 1.01 1.10 1.87 2.70 1.89 | 1.11 1.91 3.21 1.91 | 1.71 2.89 1.89 | 1.02 1.11 1.85 2.66 1.89 |
| ${ m SQUARE}$ | 1900X 5800X 5950X 7950X i7 6G i7 10G i9 10G i7 11G i9 12G i9 13G Clang GCC | 1.09 1.08 1.10 1.12 1.11 1.08 1.08 1.12 1.12 1.73 2.48 | 1.04 0.97 1.04 1.11 1.07 1.05 1.06 1.12 1.09 1.82 2.18 | 1.06 1.01 1.06 1.14 1.09 1.07 1.09 1.14 1.12 1.85 2.22 | 1.04 1.07 1.04 1.12 1.10 1.06 1.09 1.13 1.12 1.68 2.21 | 1.01 1.07 1.02 1.01 0.98 0.96 1.00 1.02 1.00 1.71 2.73 | 1.07 1.10 1.06 1.05 1.03 1.00 1.04 1.07 1.06 1.78 2.84 | 1.08 1.14 1.08 1.07 1.05 1.02 1.06 1.09 1.07 1.82 2.88 | 1.10 1.20 1.10 1.09 1.07 1.05 1.05 1.77 2.64 | 1.09 1.15 1.12 1.10 1.09 1.09 1.04 1.05 1.06 1.81 3.13 | 0.98 1.02 0.99 0.98 0.97 0.97 0.92 0.93 0.89 | 1.05 1.08 1.04 1.05 1.07 1.05 1.02 1.04 1.06 1.07 1.76 2.59 |