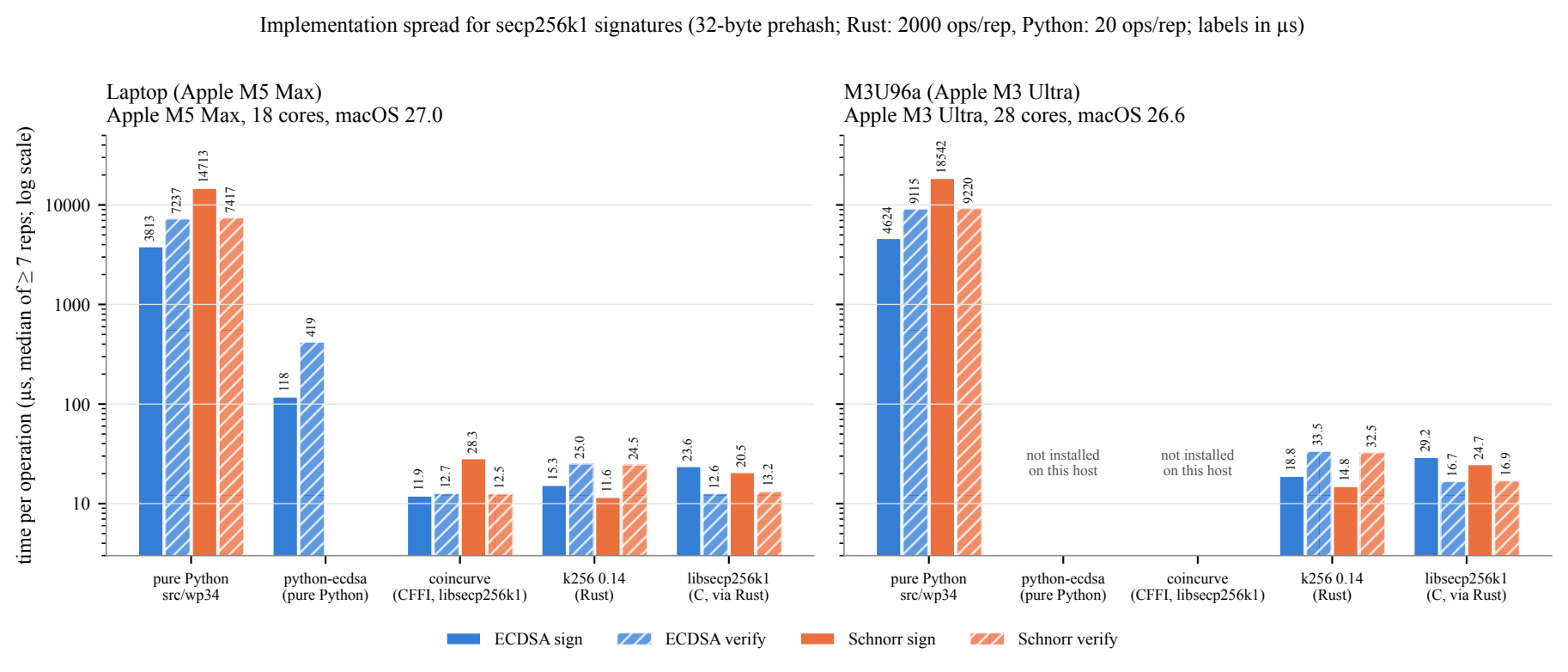

Implementation spread for secp256k1 signatures (32-byte prehash; Rust: 2000 ops/rep, Python: 20 ops/rep; labels in µs)
Laptop (Apple M5 Max)
Apple M5 Max, 18 cores, macOS 27.0
M3U96a (Apple M3 Ultra)
Apple M3 Ultra, 28 cores, macOS 26.6
time per operation (µs, median of ≥ 7 reps; log scale)
10000
1000
100
10
3813
7237
14713
7417
118
419
11.9
12.7
28.3
12.5
15.3
25.0
11.6
24.5
23.6
12.6
20.5
13.2
4624
9115
18542
9220
not installed on this host
not installed on this host
18.8
33.5
14.8
32.5
29.2
16.7
24.7
16.9
pure Python src/wp34
python-ecdsa (pure Python)
coincurve (CFFI, libsecp256k1)
k256 0.14 (Rust)
libsecp256k1 (C, via Rust)
ECDSA sign
ECDSA verify
Schnorr sign
Schnorr verify