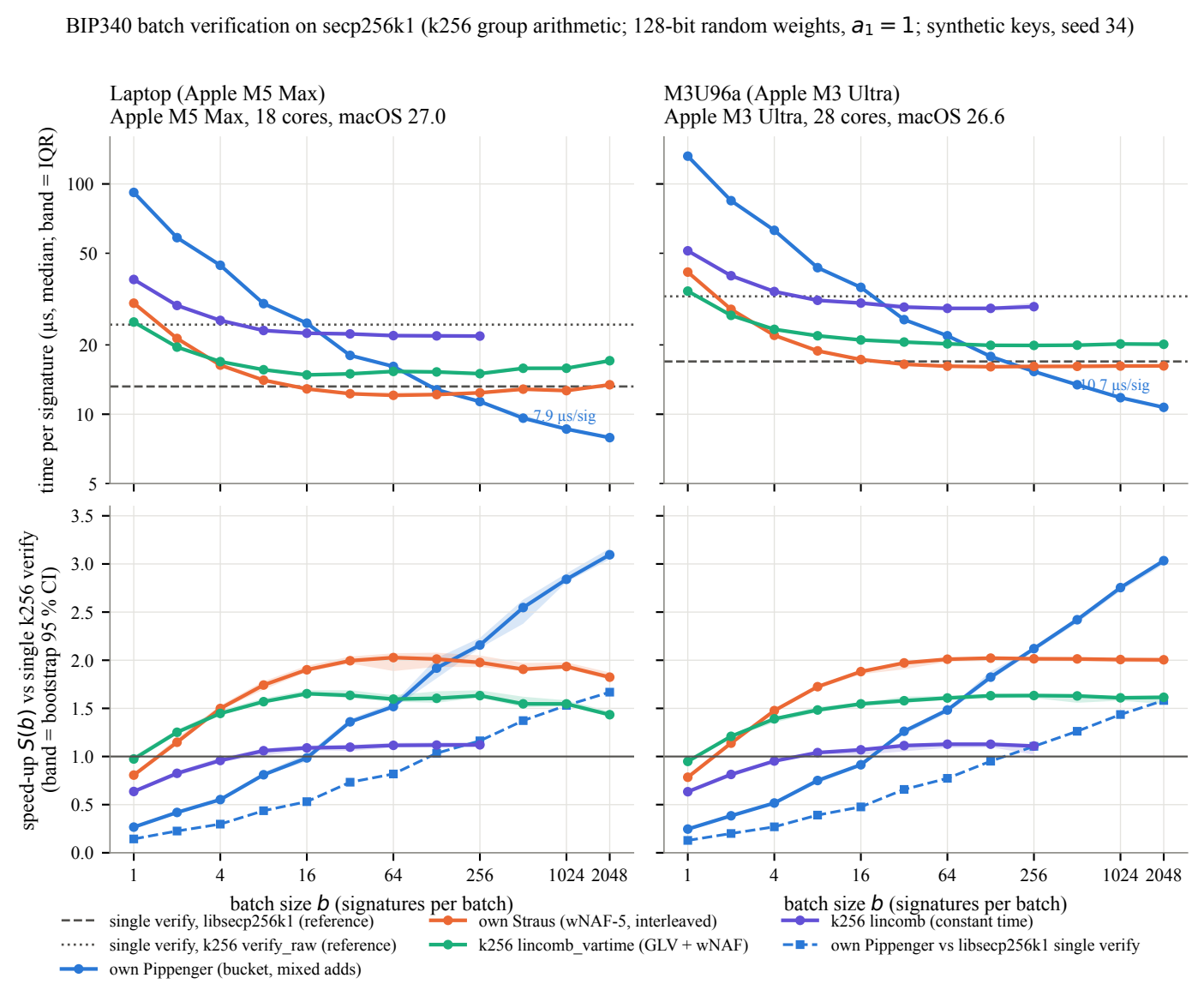

BIP340 batch verification on secp256k1 (k256 group arithmetic; 128-bit random weights, $a_1 = 1$; synthetic keys, seed 34)
Laptop (Apple M5 Max)
Apple M5 Max, 18 cores, macOS 27.0
M3U96a (Apple M3 Ultra)
Apple M3 Ultra, 28 cores, macOS 26.6
time per signature (µs, median; band = IQR)
100
50
20
10
5
7.9 µs/sig
10.7 µs/sig
speed-up $S(b)$ vs single k256 verify
(band = bootstrap 95 % CI)
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
1
4
16
64
256
1024
2048
batch size b (signatures per batch)
batch size b (signatures per batch)
single verify, libsecp256k1 (reference)
single verify, k256 verify_raw (reference)
own Pippenger (bucket, mixed adds)
own Straus (wNAF-5, interleaved)
k256 lincomb_vartime (GLV + wNAF)
k256 lincomb (constant time)
own Pippenger vs libsecp256k1 single verify