Running Time Changes in Preexisting Benchmarks (n=8)
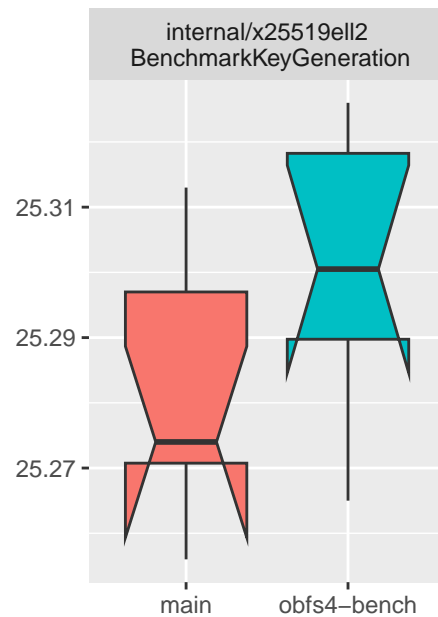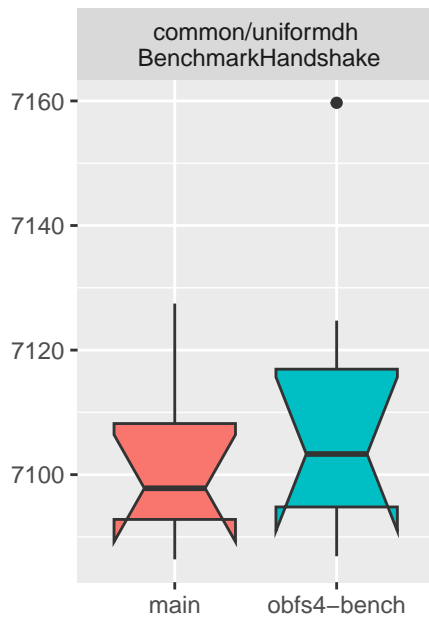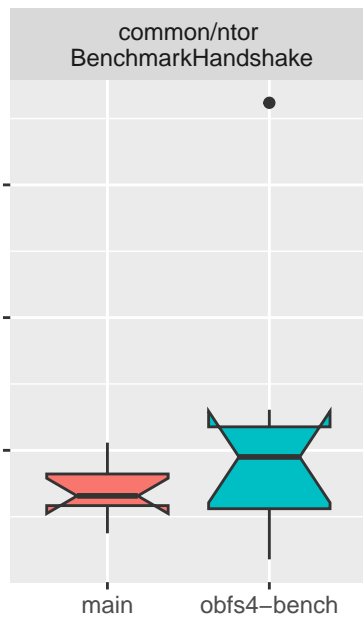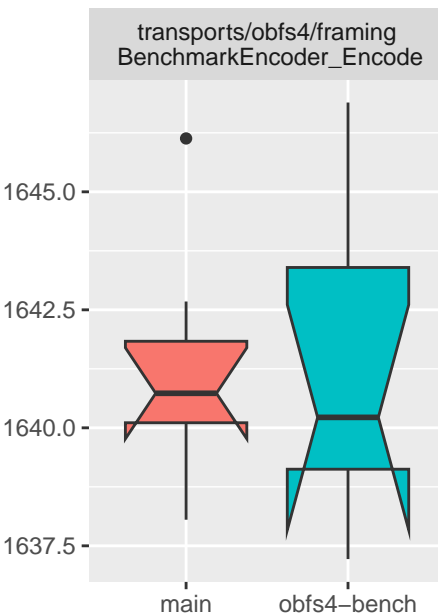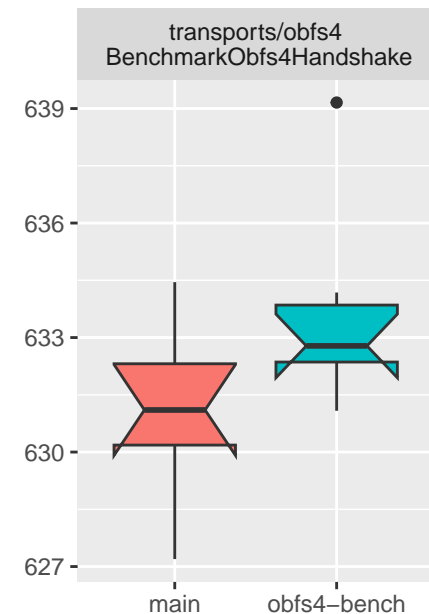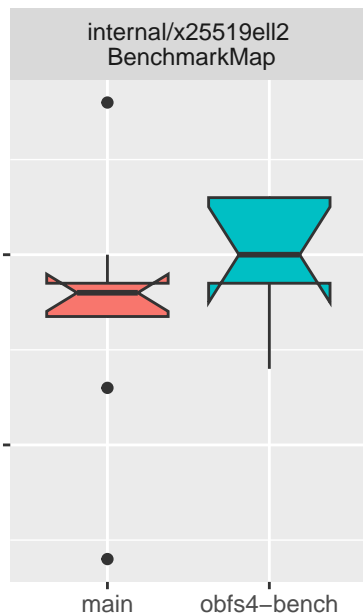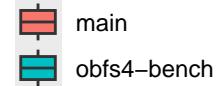
Memory Usage Changes in Preexisting Benchmarks (n=8)

Simulated Handshake Running Time (n=8)
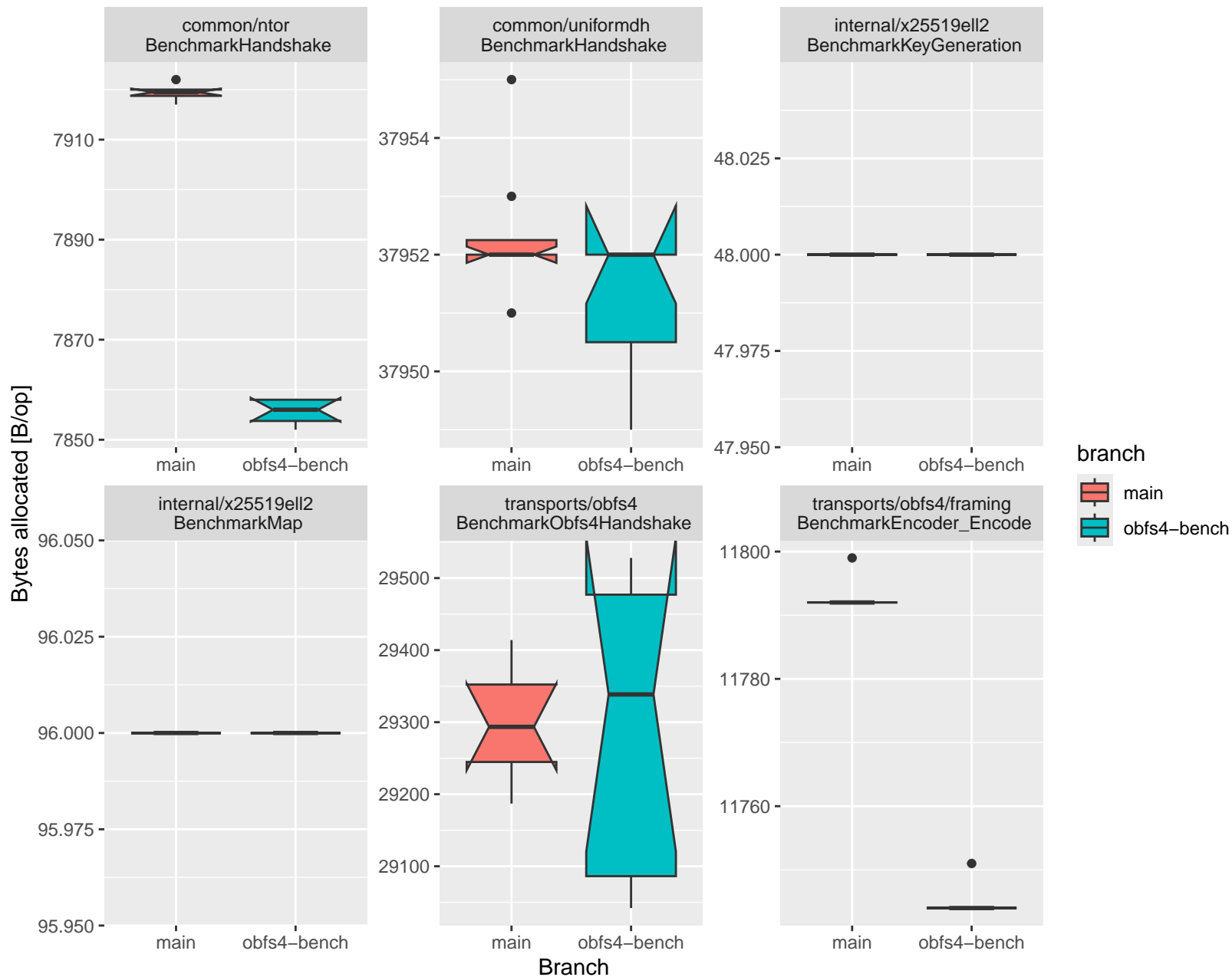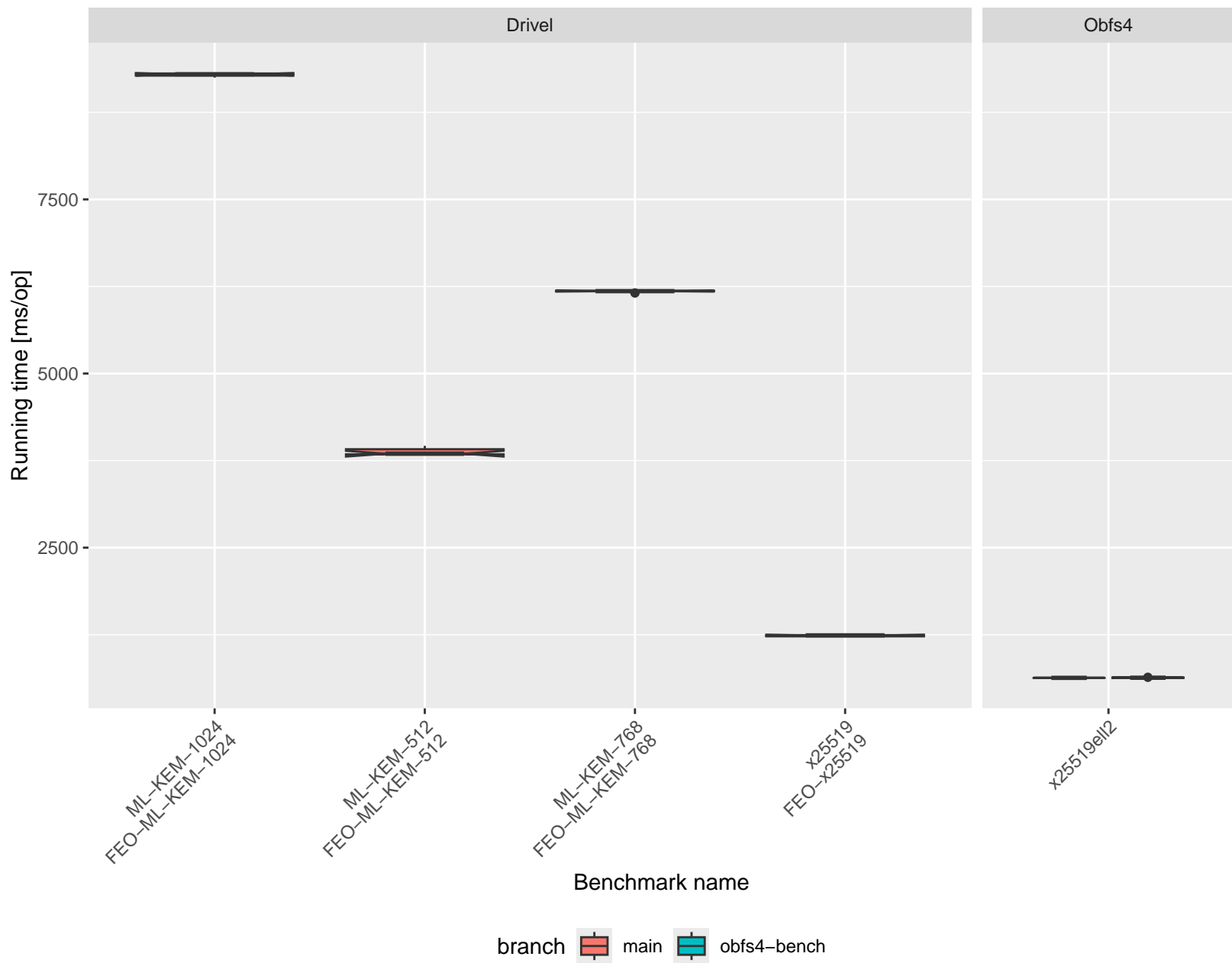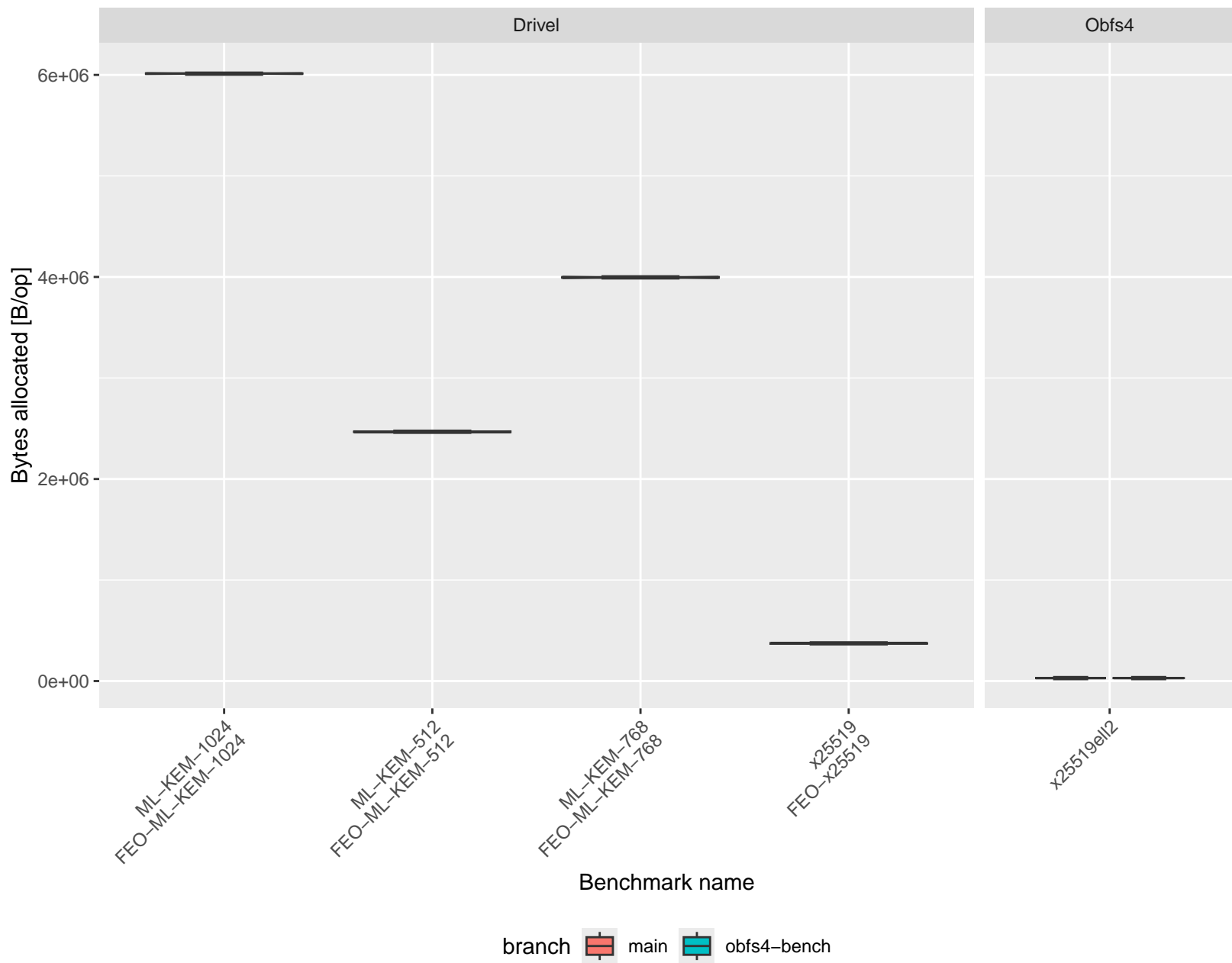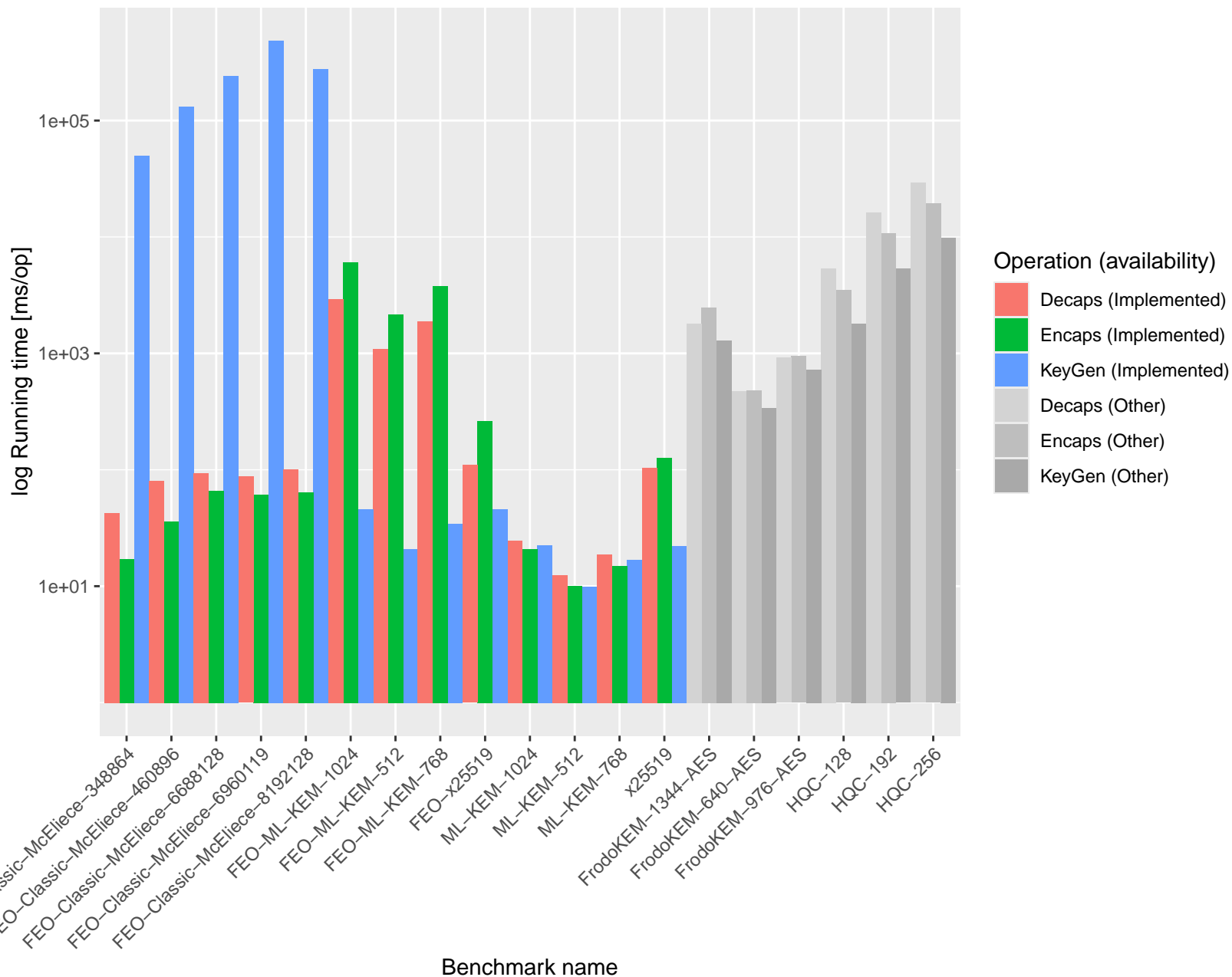
Handshake Memory Usage (n=8)

(O)KEM Running Time (n=8)

Figure showing log running time [ms/op] on the y-axis (log scale from below 1e+01 to above 1e+05) versus benchmark name on the x-axis.

Y-axis label: log Running time [ms/op]
X-axis label: Benchmark name

X-axis categories: Classic-McEliece-348864, FEO-Classic-McEliece-460896, FEO-Classic-McEliece-6688128, FEO-Classic-McEliece-6960119, FEO-Classic-McEliece-8192128, FEO-ML-KEM-1024, FEO-ML-KEM-512, FEO-ML-KEM-768, FEO-x25519, ML-KEM-1024, ML-KEM-512, ML-KEM-768, x25519, FrodoKEM-1344-AES, FrodoKEM-640-AES, FrodoKEM-976-AES, HQC-128, HQC-192, HQC-256

Legend — Operation (availability):
- Decaps (Implemented)
- Encaps (Implemented)
- KeyGen (Implemented)
- Decaps (Other)
- Encaps (Other)
- KeyGen (Other)
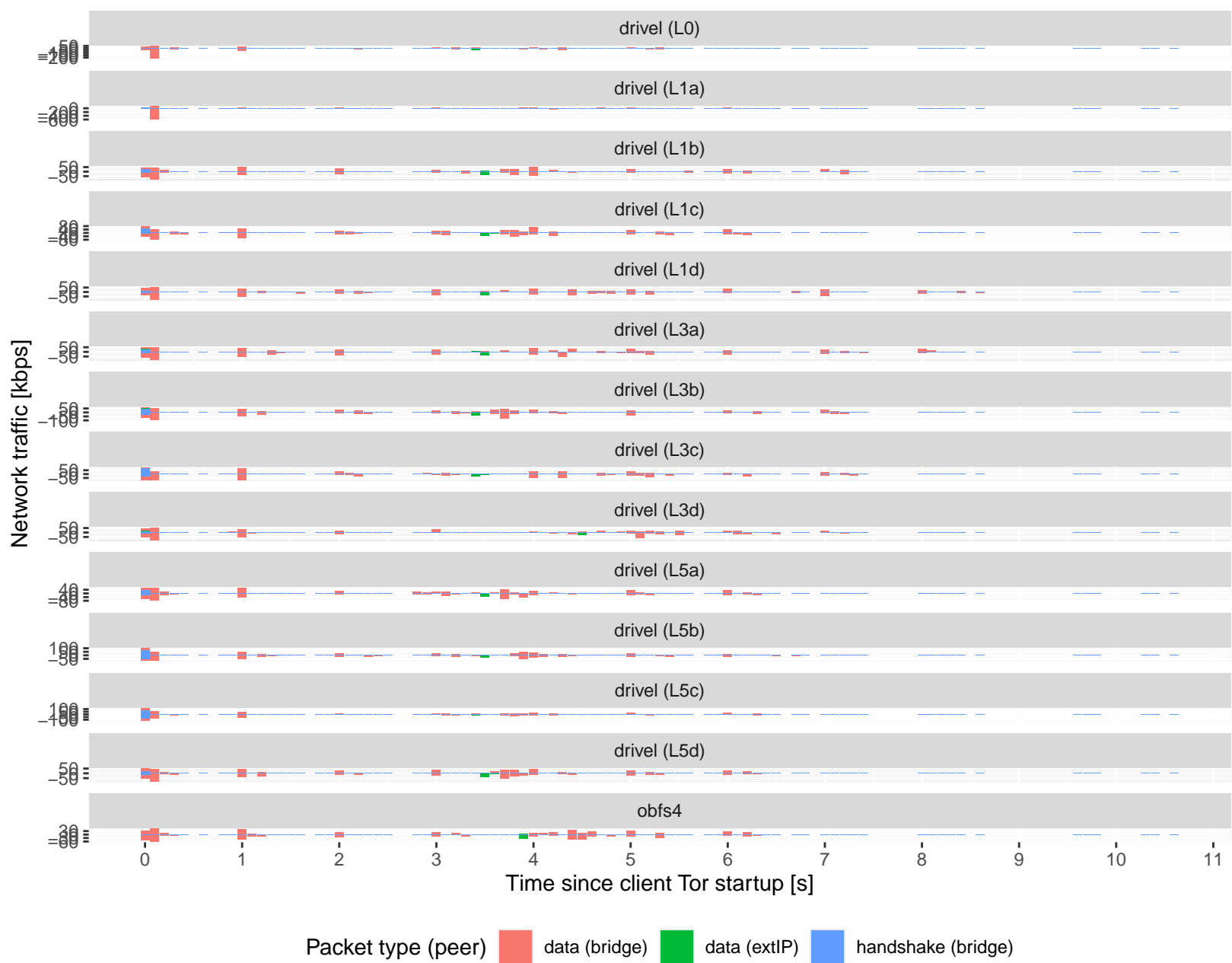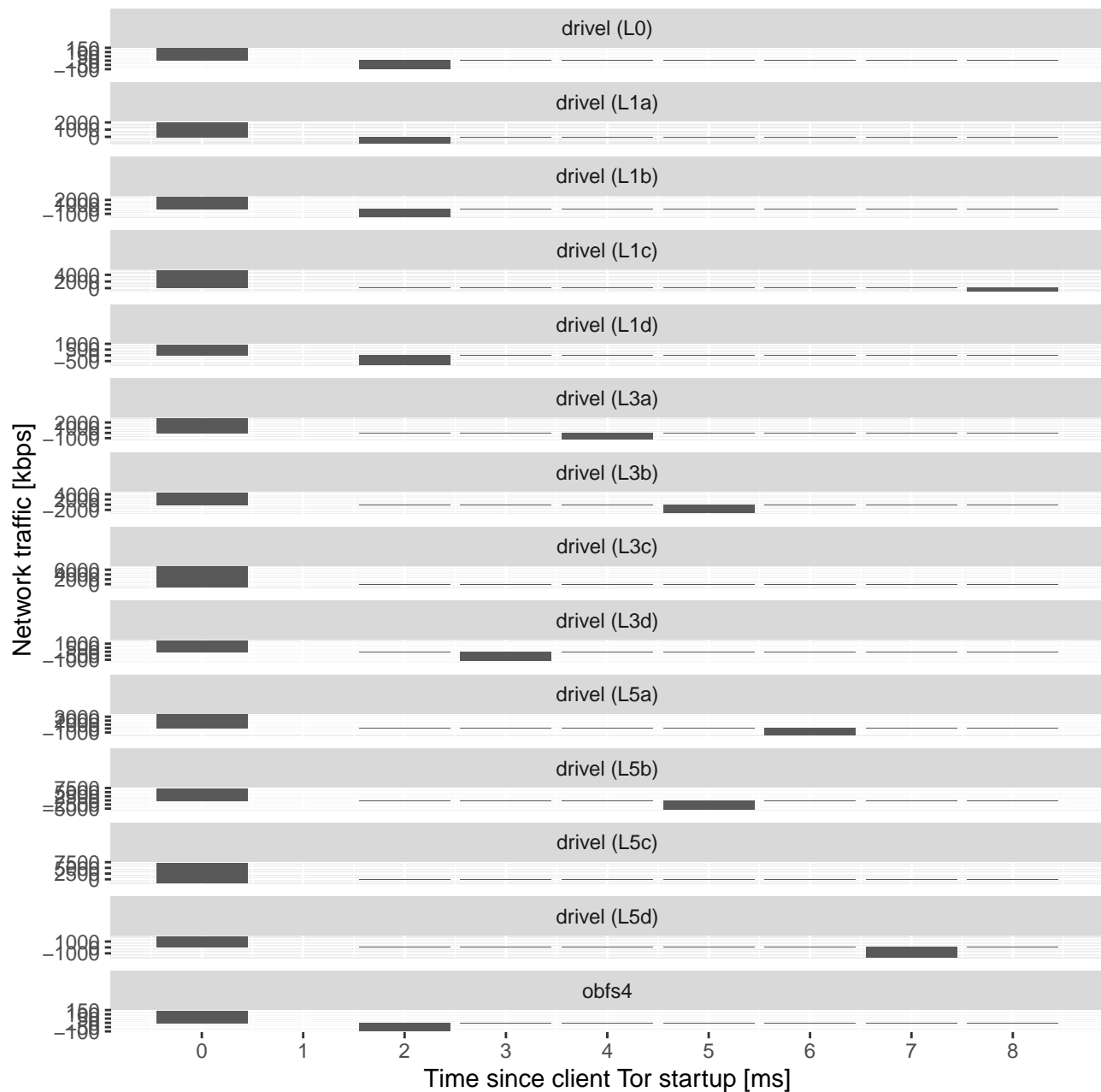
(O)KEM Memory Usage (n=8)

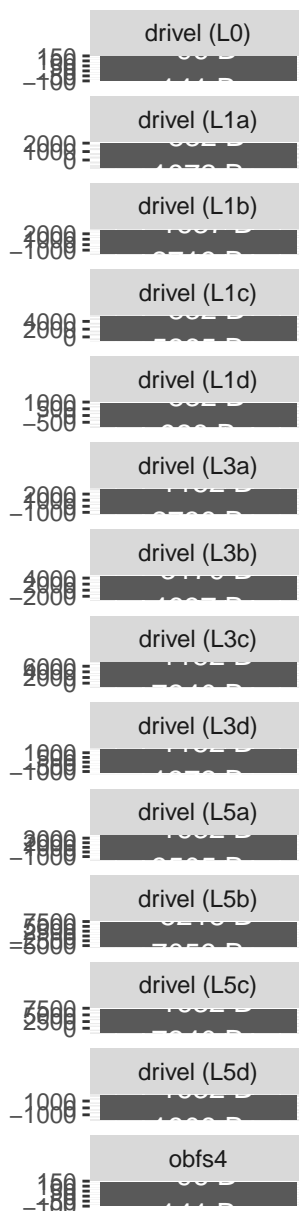Network Traffic over Time (TCP payloads, n=1)

Traffic for Key Exchange (TCP payloads, n=1)
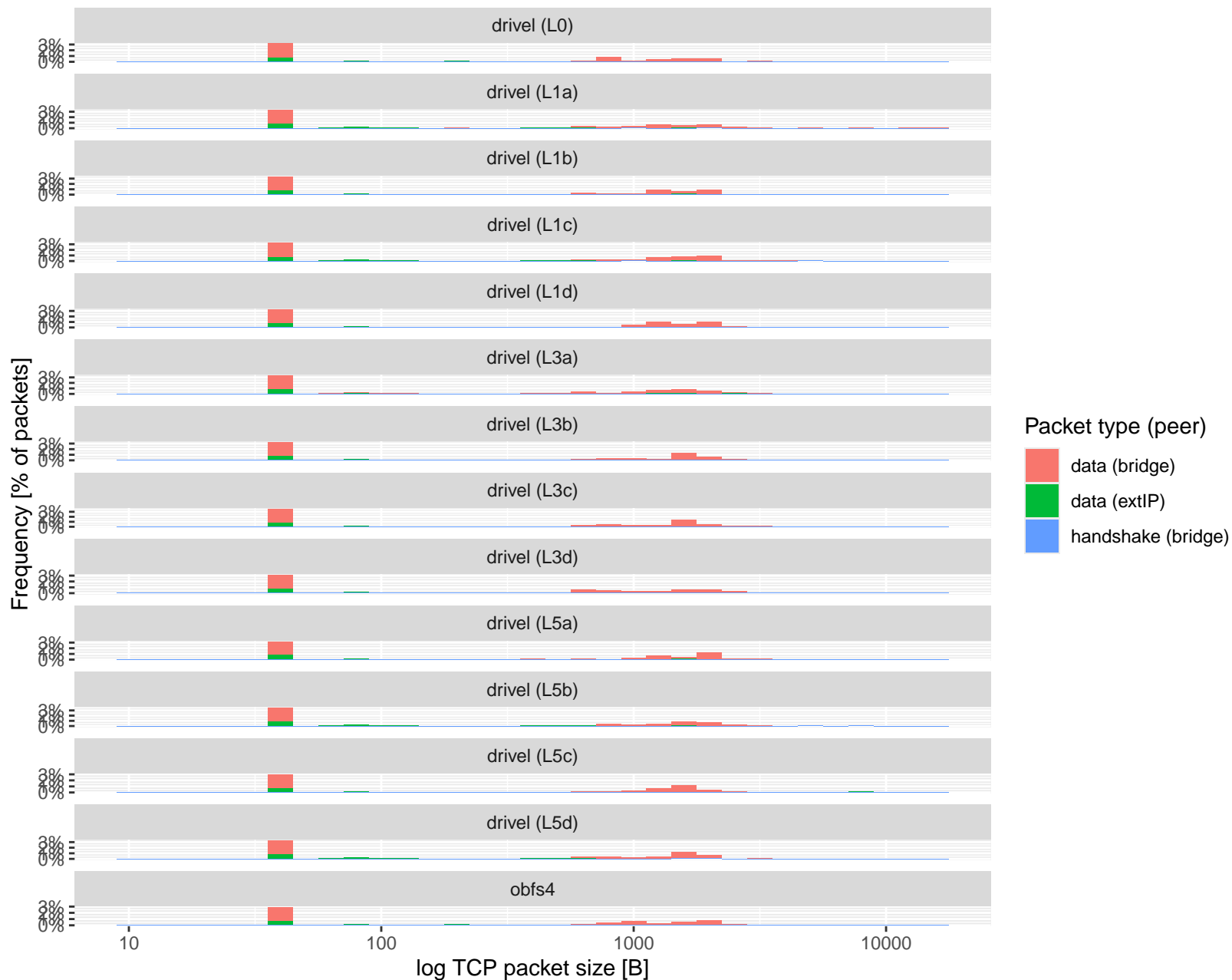
Distribution of TCP Packet Sizes

Composition of Handshake Packets

Figure: Composition of Handshake Packets. Field size [B] (y-axis) versus Packet origin (x-axis).

field:
- KEM.public.key
- KEM.ciphertext
- OKEM.ciphertext
- auth
- padding
- mark
- mac