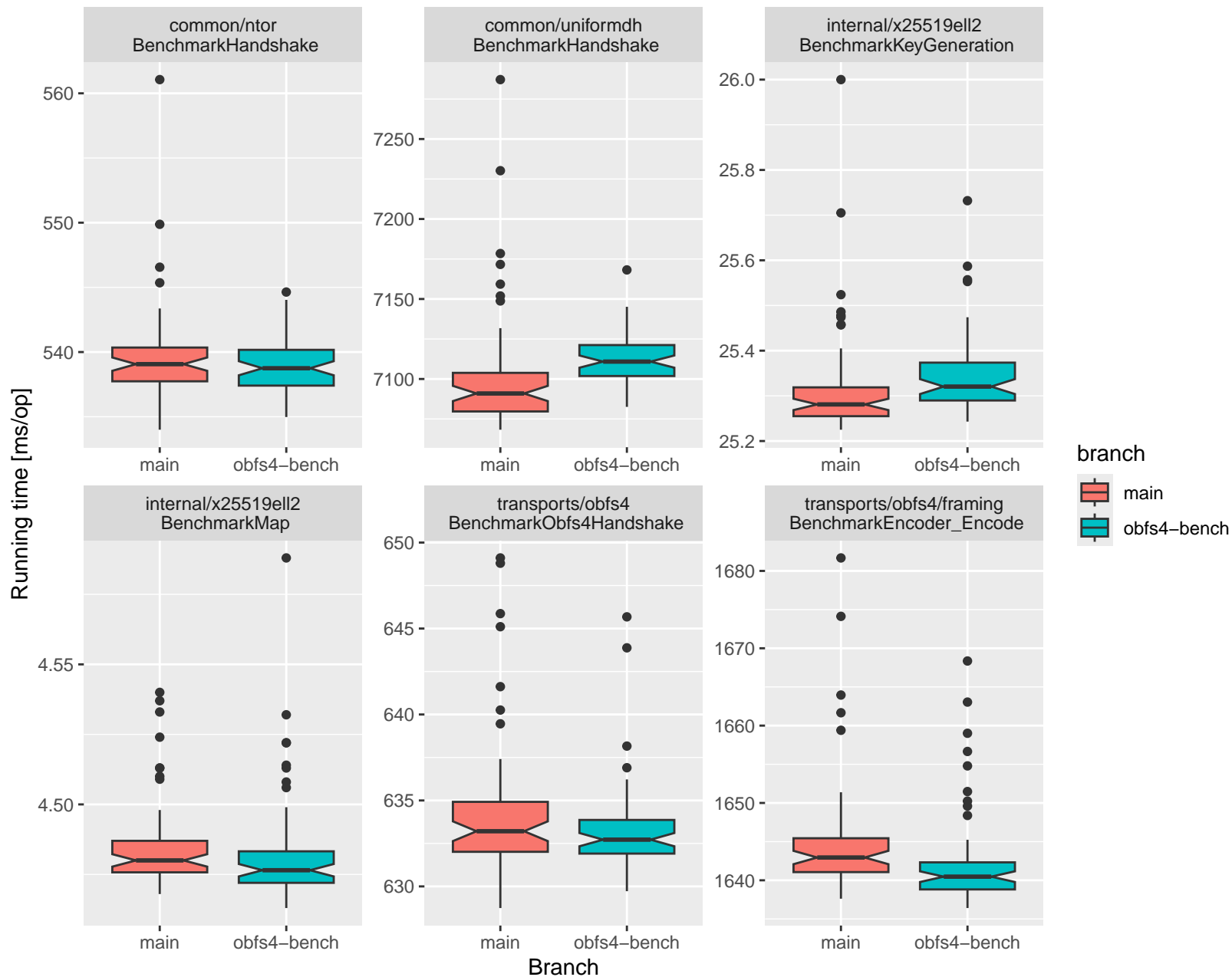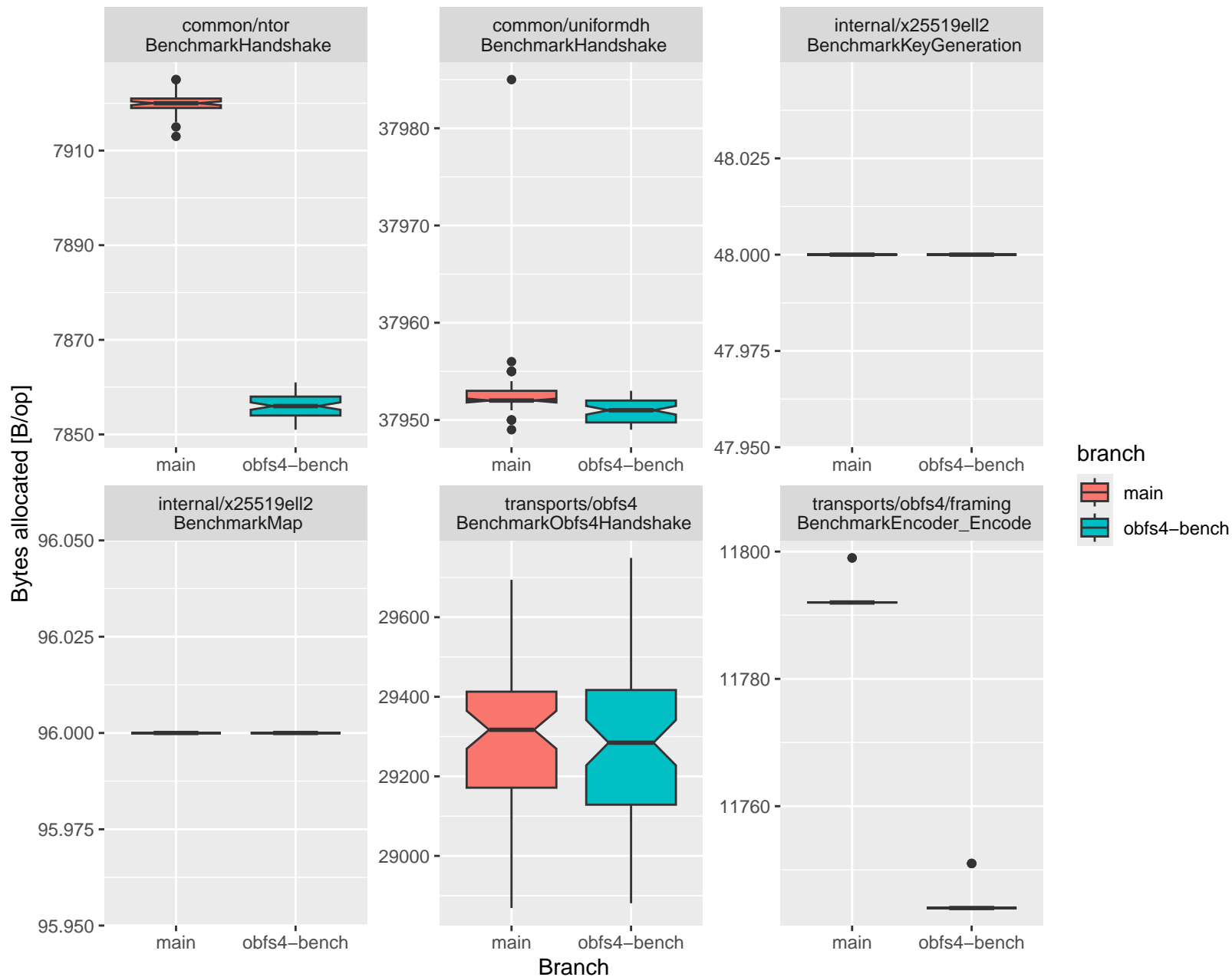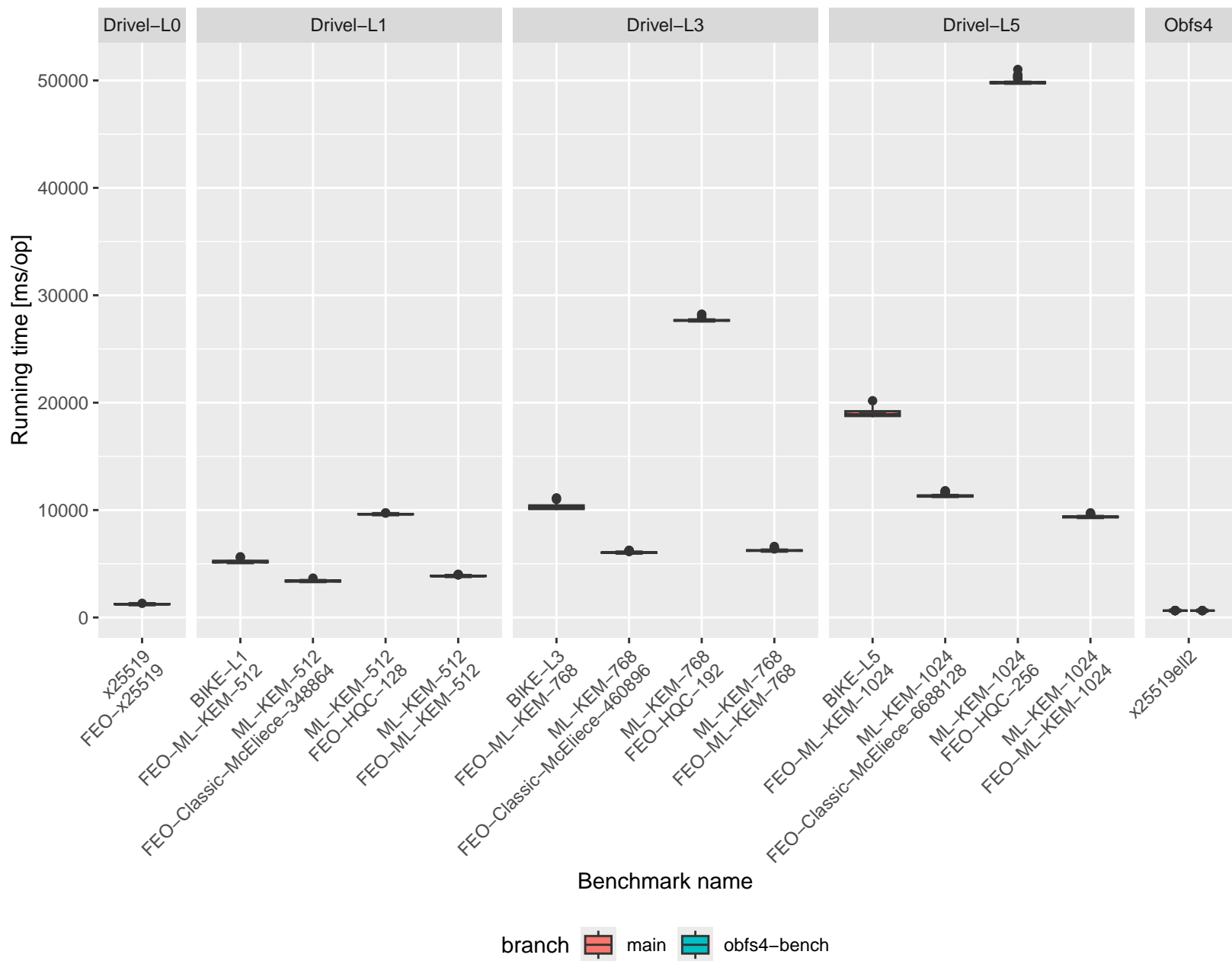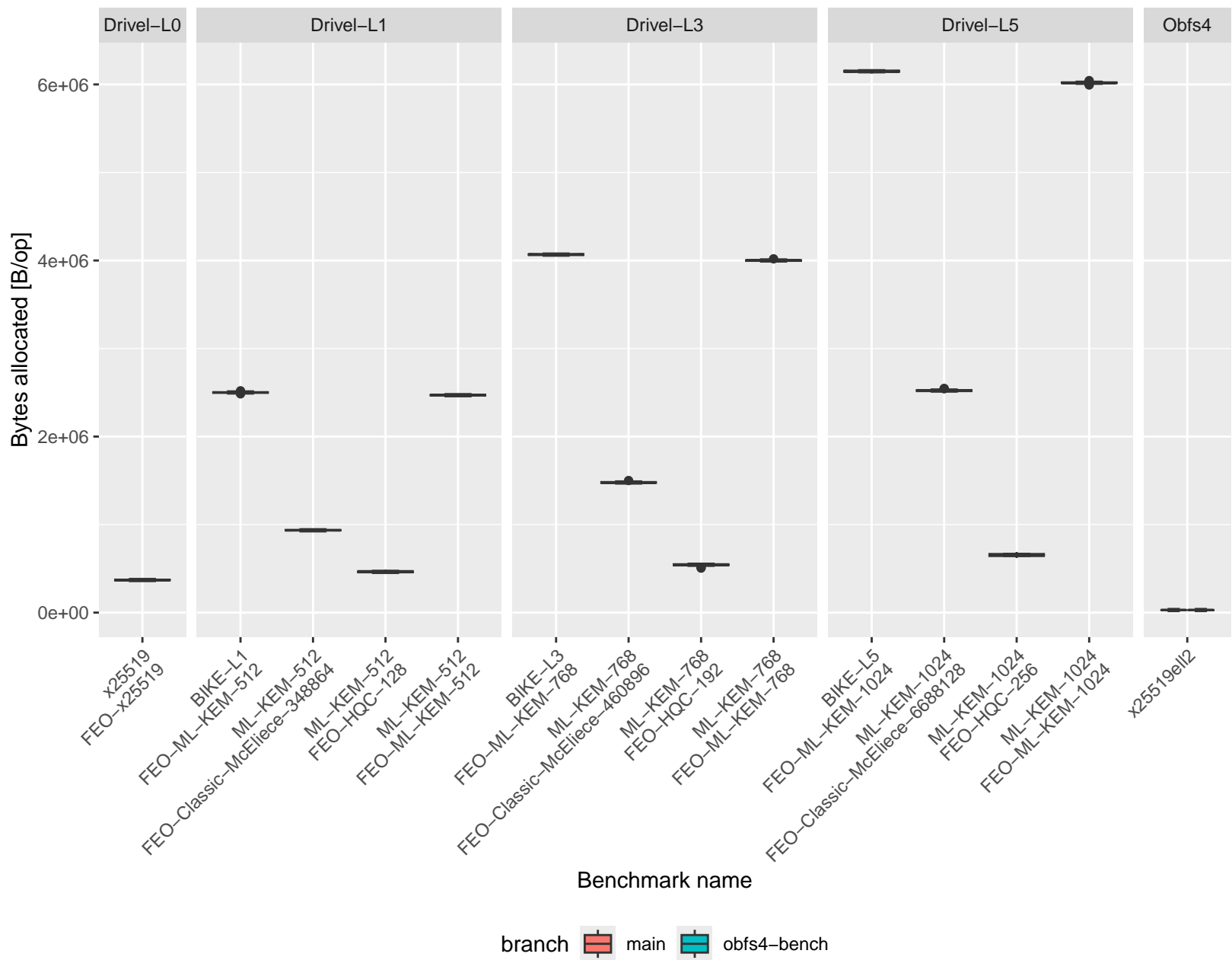Running Time Changes in Preexisting Benchmarks (n=64)

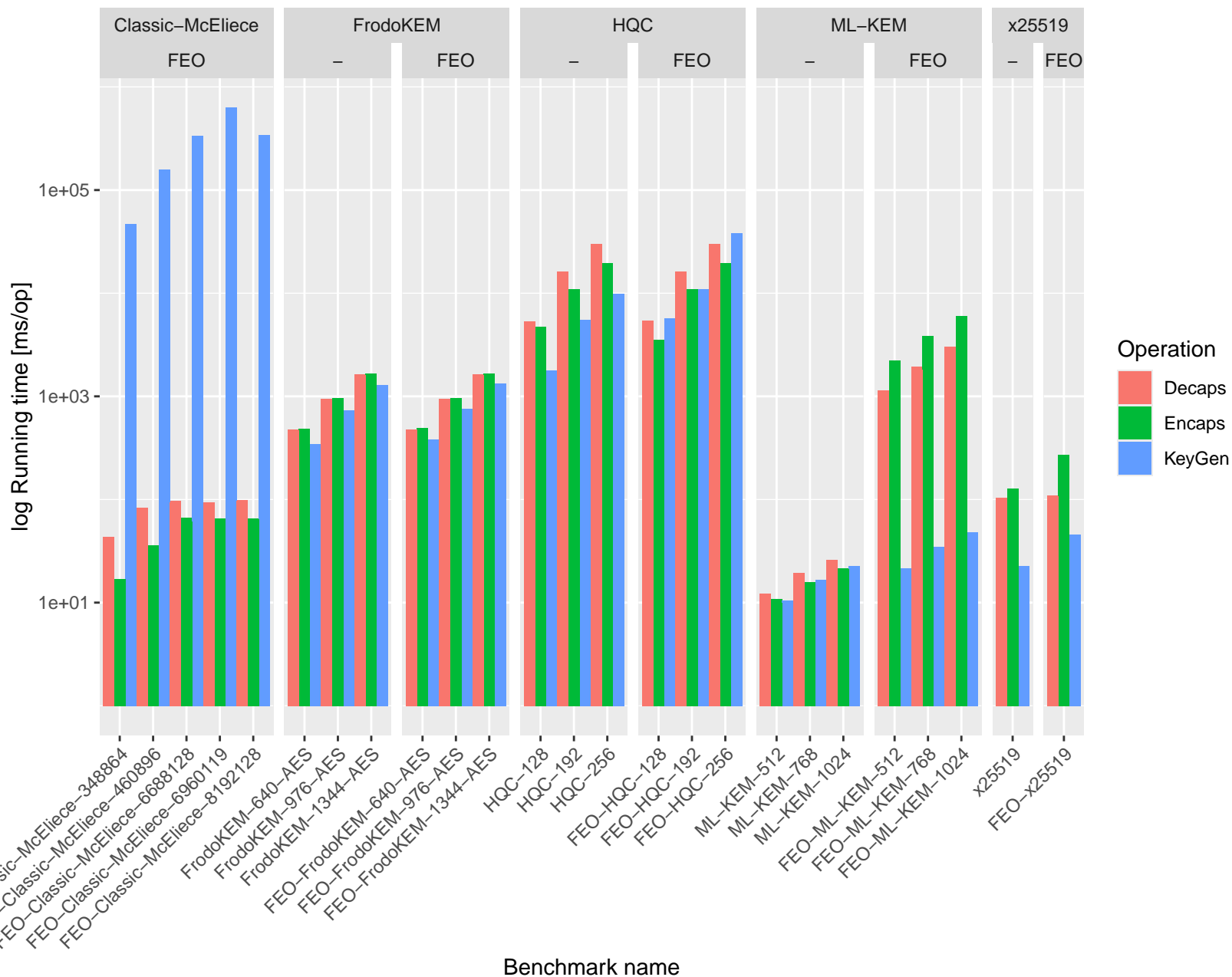Memory Usage Changes in Preexisting Benchmarks (n=64)

Simulated Handshake Running Time (n=64)

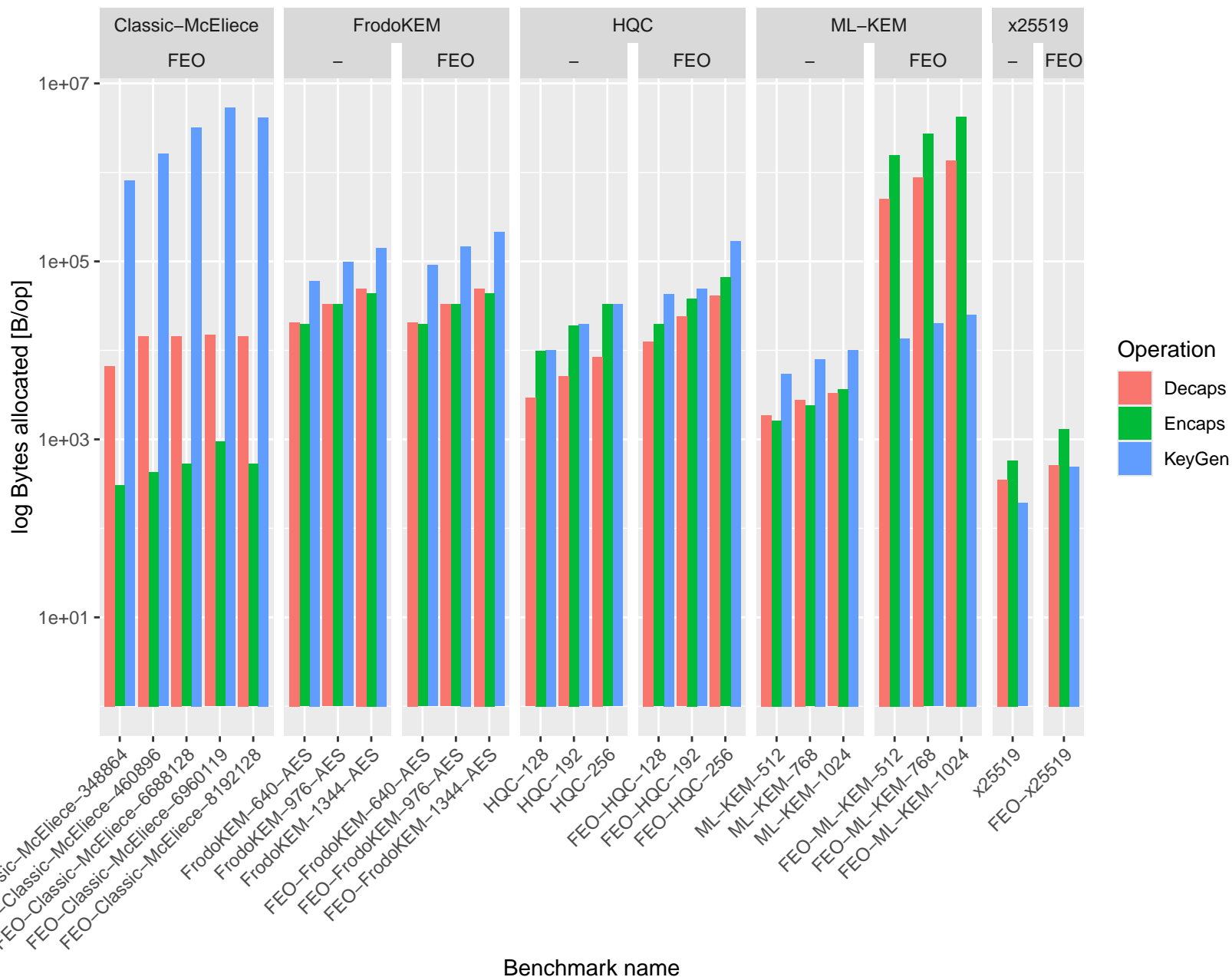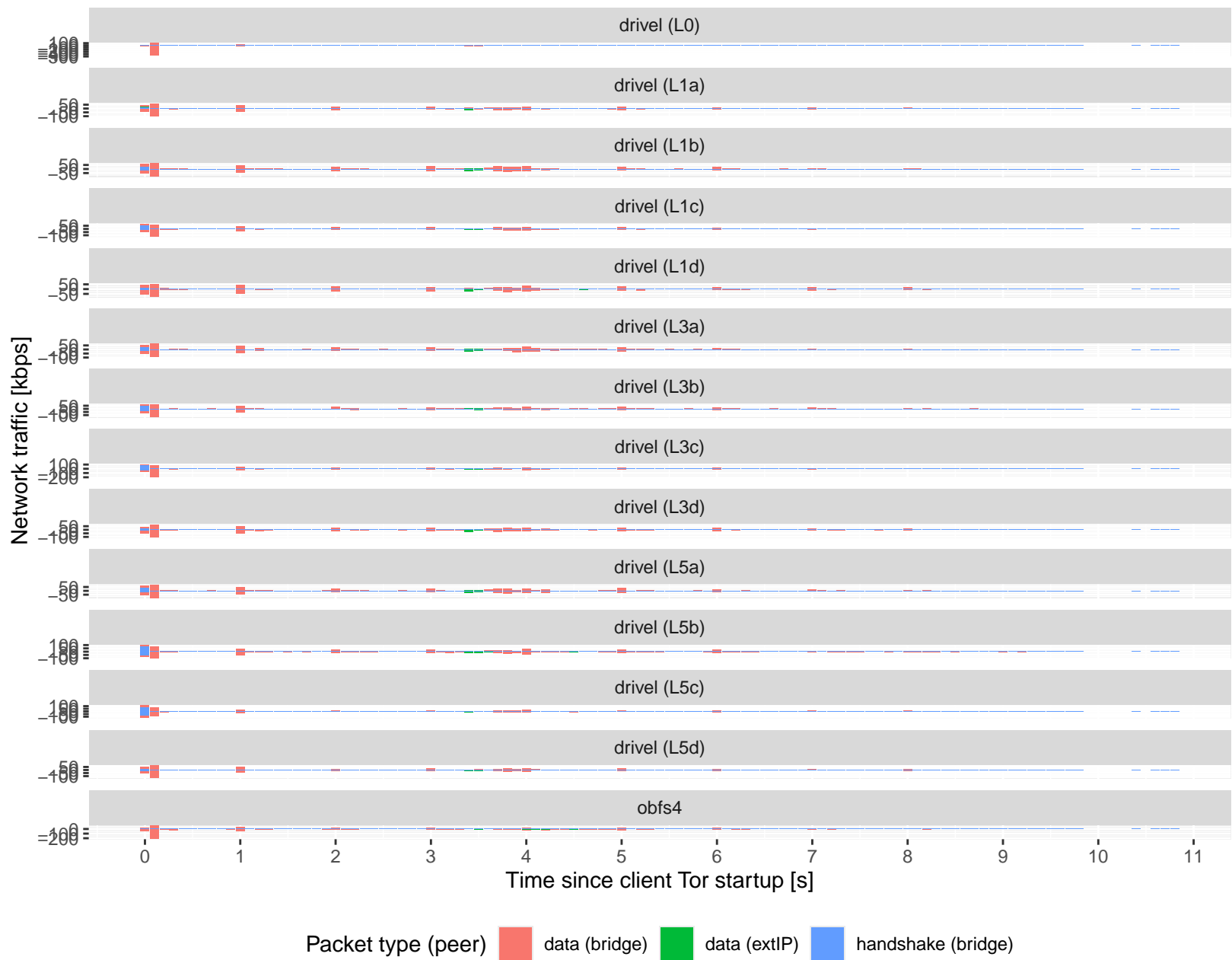Handshake Memory Usage (n=64)

(O)KEM Running Time (n=64)
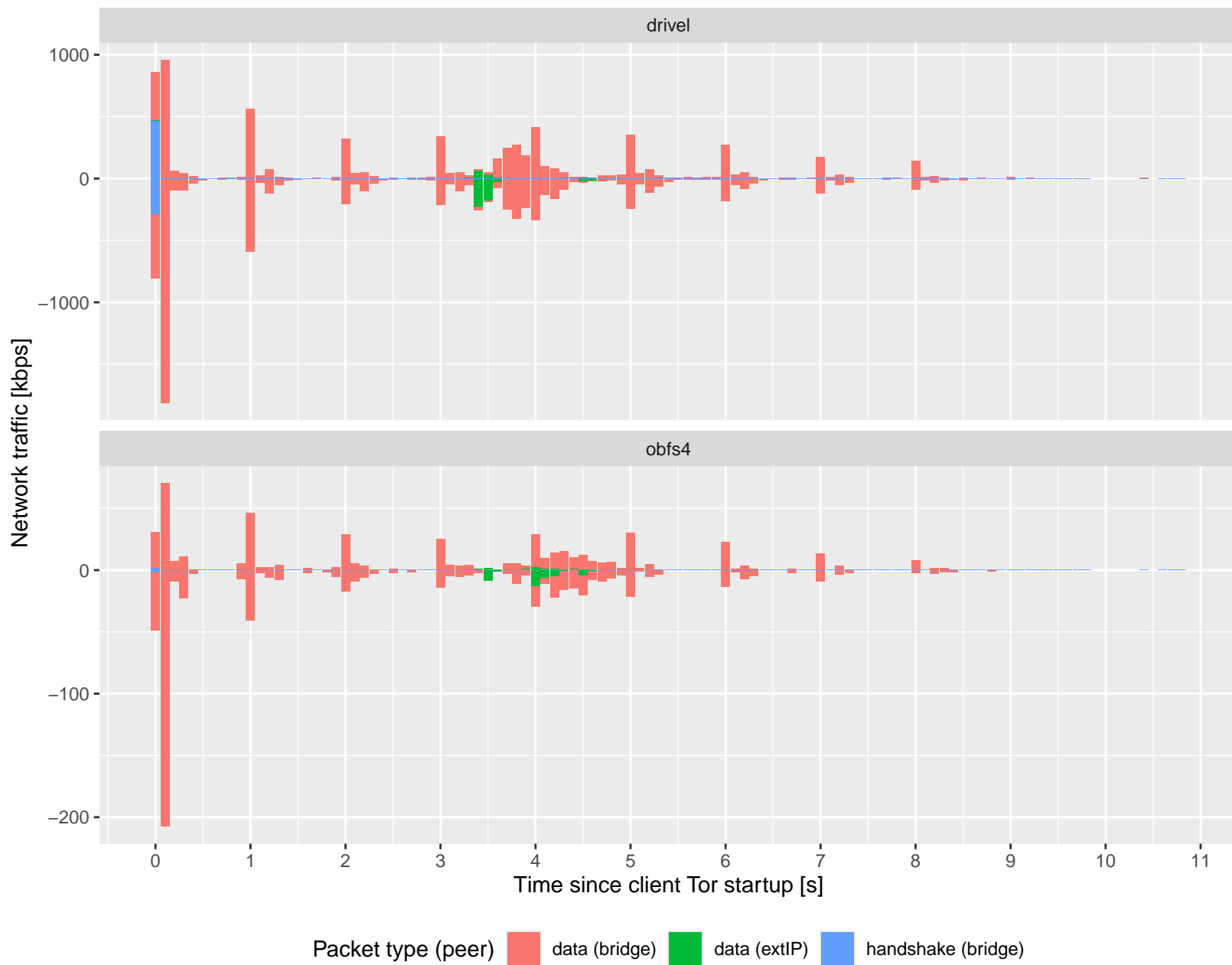
(O)KEM Memory Usage (n=64)

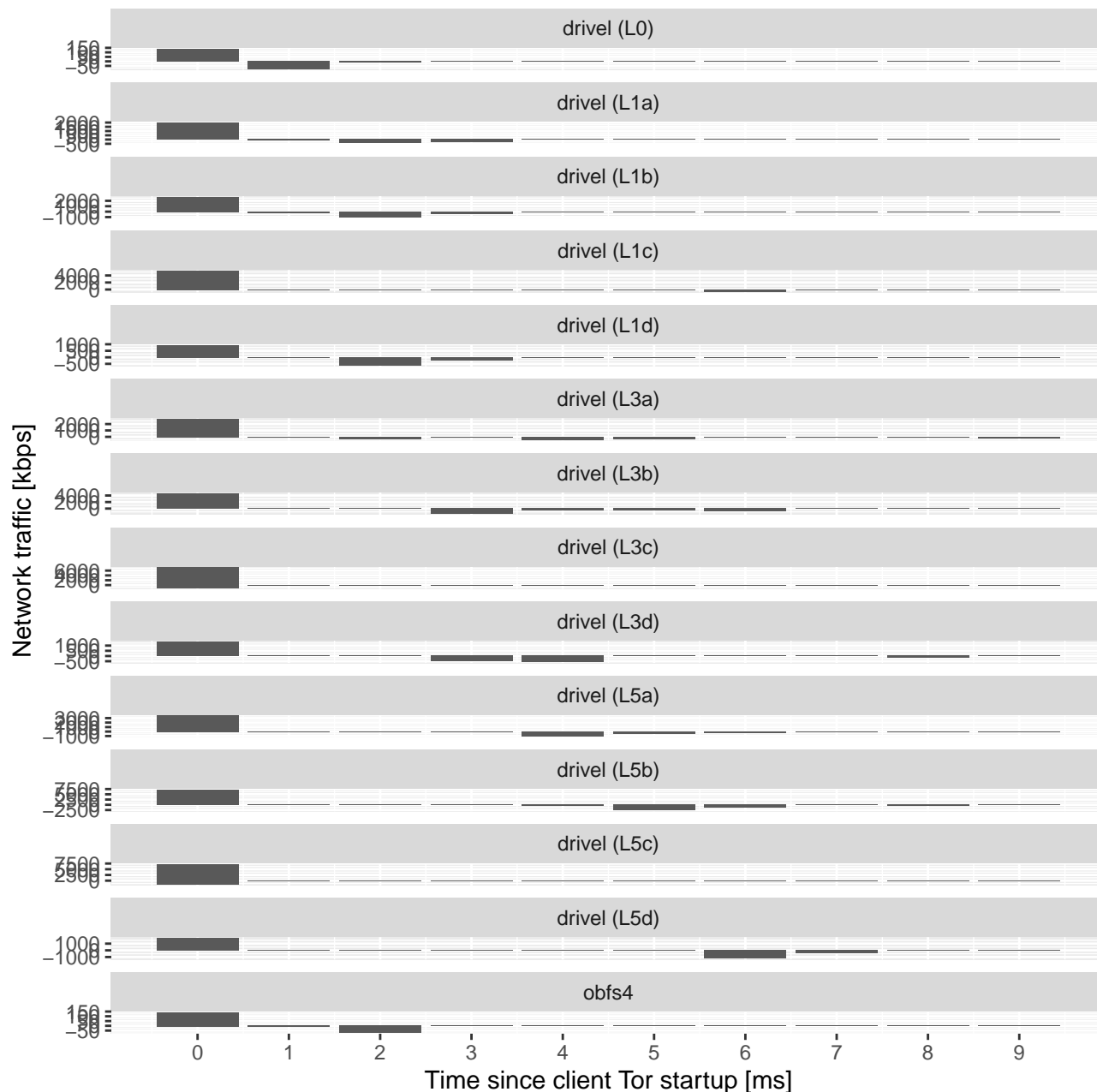Network Traffic over Time (TCP payloads, n=8)

Network Traffic over Time (TCP payloads, n=8)

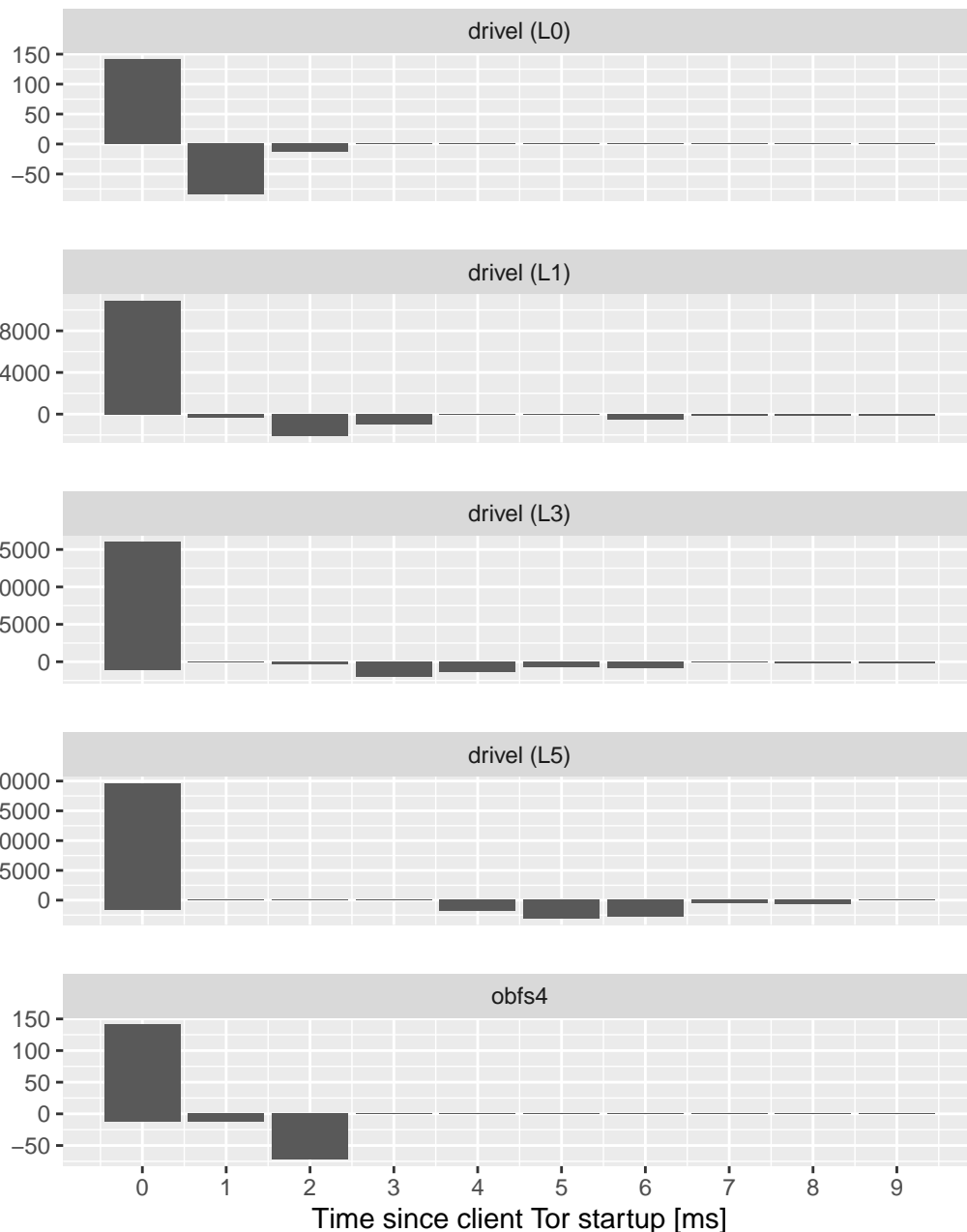Packet type (peer): ■ data (bridge) ■ data (extIP) ■ handshake (bridge)
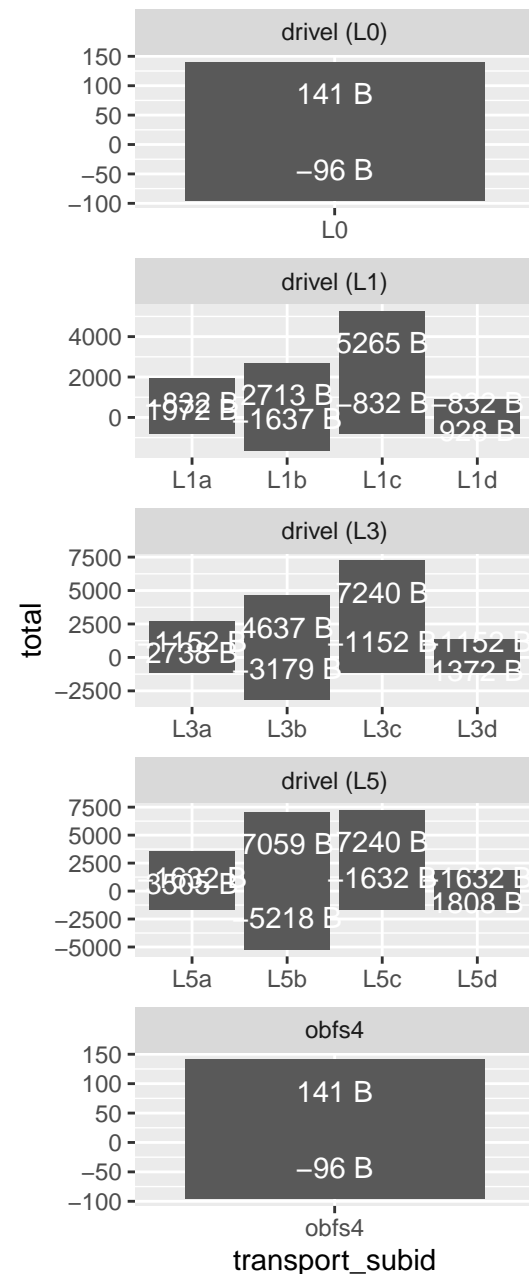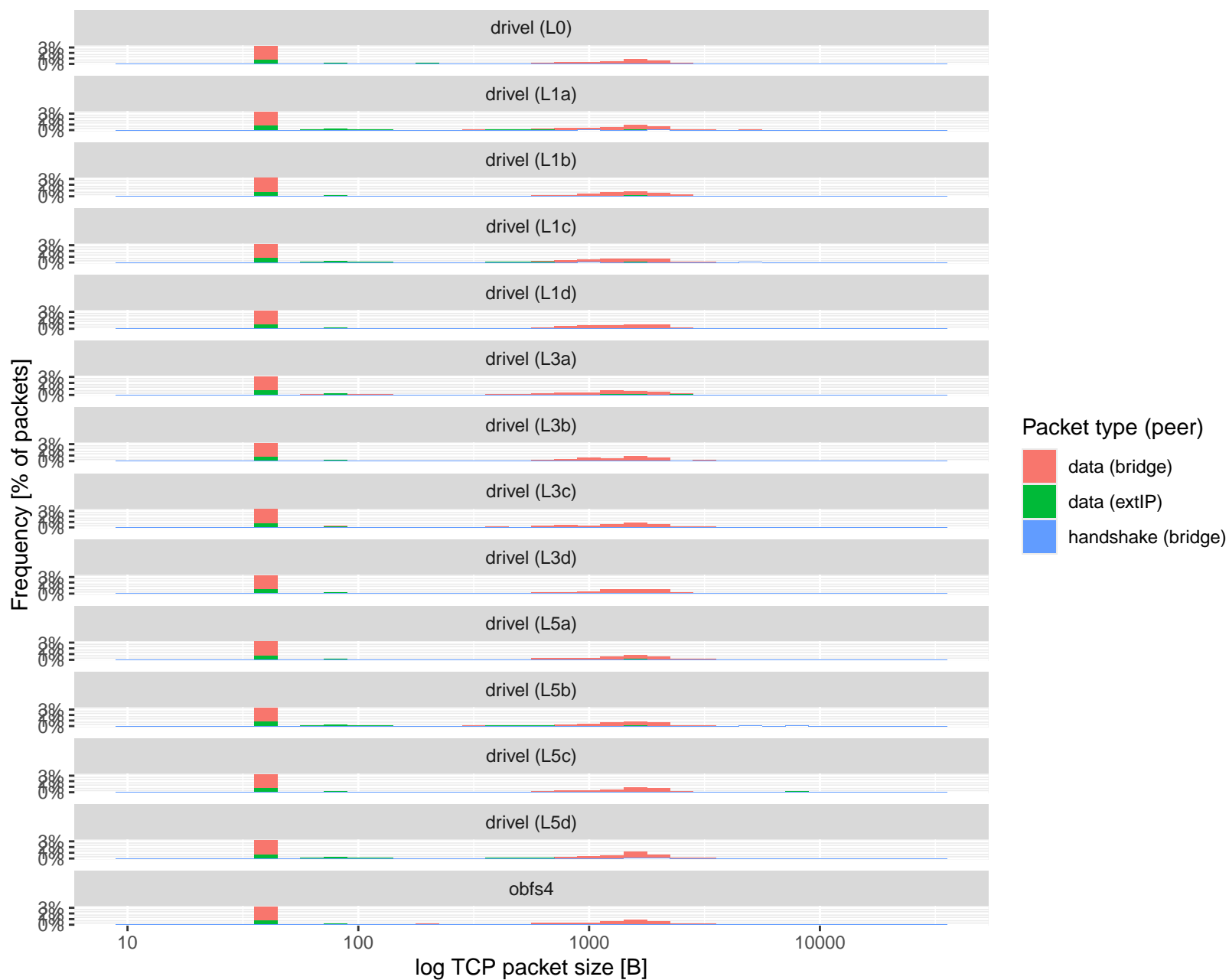
Traffic for Key Exchange (TCP payloads, n=8) / Total bytes

Traffic for Key Exchange (TCP payloads, n=8)

Total bytes

Distribution of TCP Packet Sizes

Figure: Distribution of TCP Packet Sizes. X-axis: log TCP packet size [B]. Y-axis: Frequency [% of packets]. Panels (top to bottom): drivel (L0), drivel (L1a), drivel (L1b), drivel (L1c), drivel (L1d), drivel (L3a), drivel (L3b), drivel (L3c), drivel (L3d), drivel (L5a), drivel (L5b), drivel (L5c), drivel (L5d), obfs4. Legend — Packet type (peer): data (bridge), data (extIP), handshake (bridge).

Distribution of TCP Packet Sizes

Composition of Handshake Packets

Figure: Composition of Handshake Packets. X-axis: Packet origin. Y-axis: Field size [B]. Legend — field: KEM.public.key, KEM.ciphertext, OKEM.ciphertext, auth, padding, mark, mac.

Composition of Handshake Packets