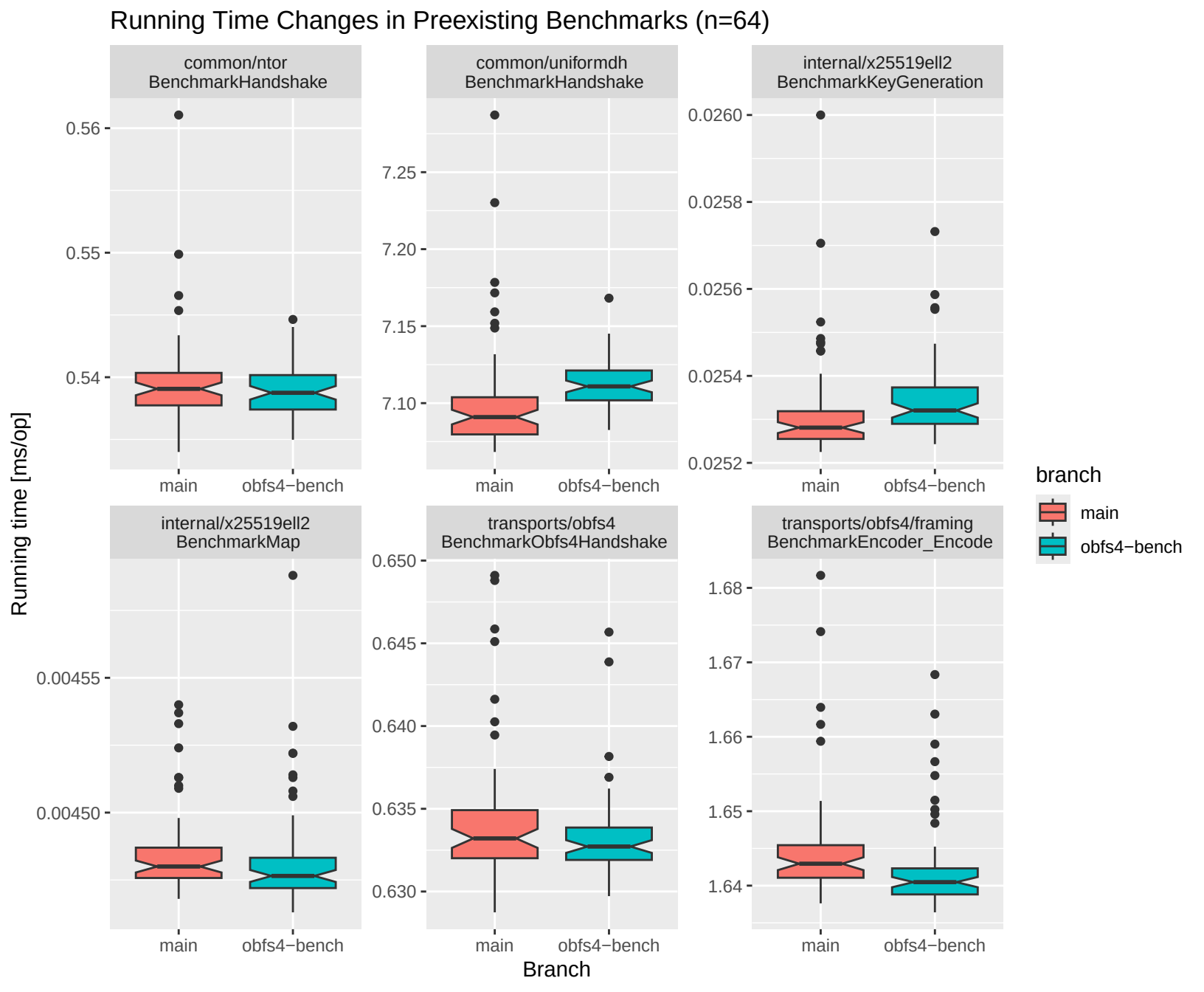
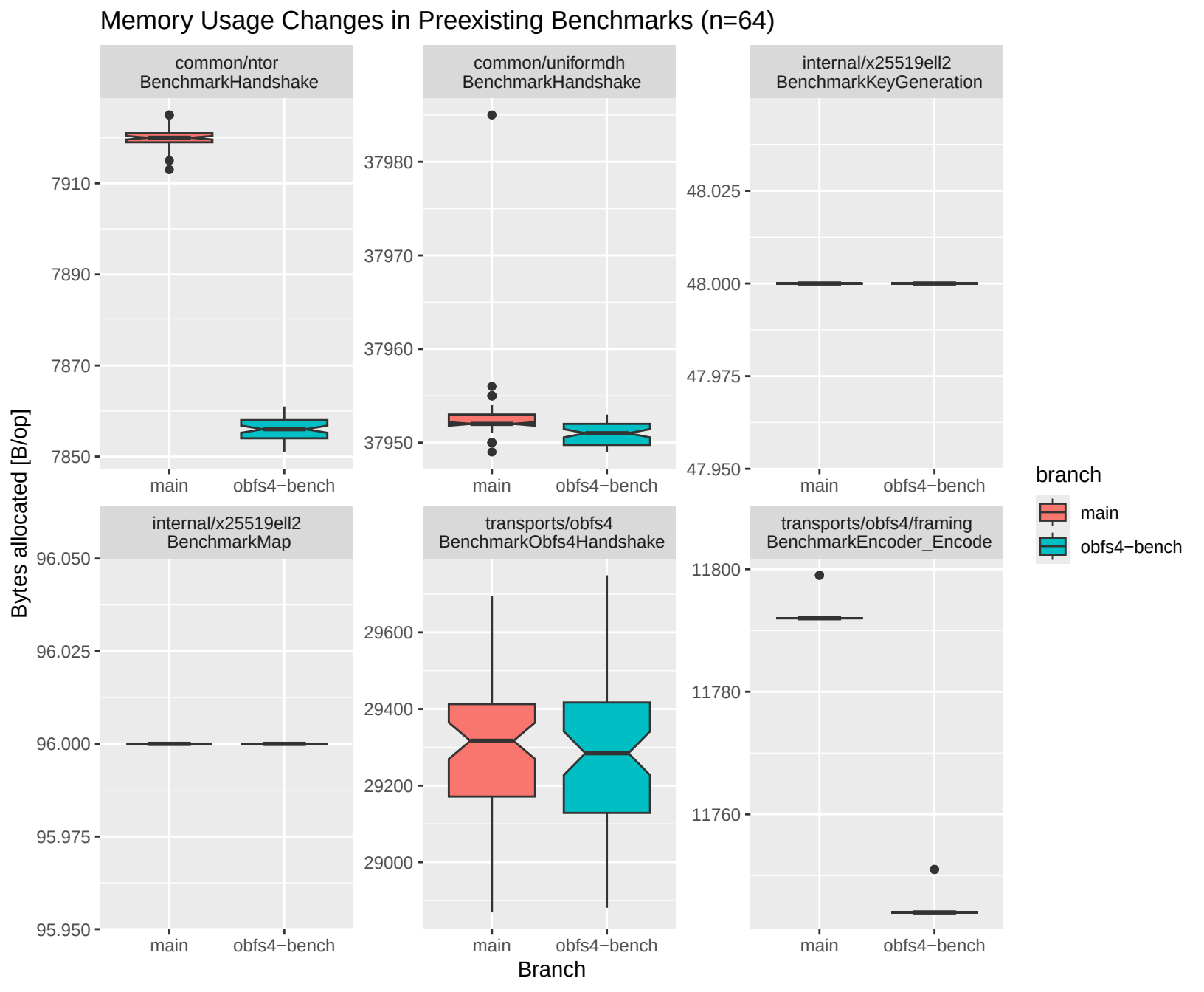
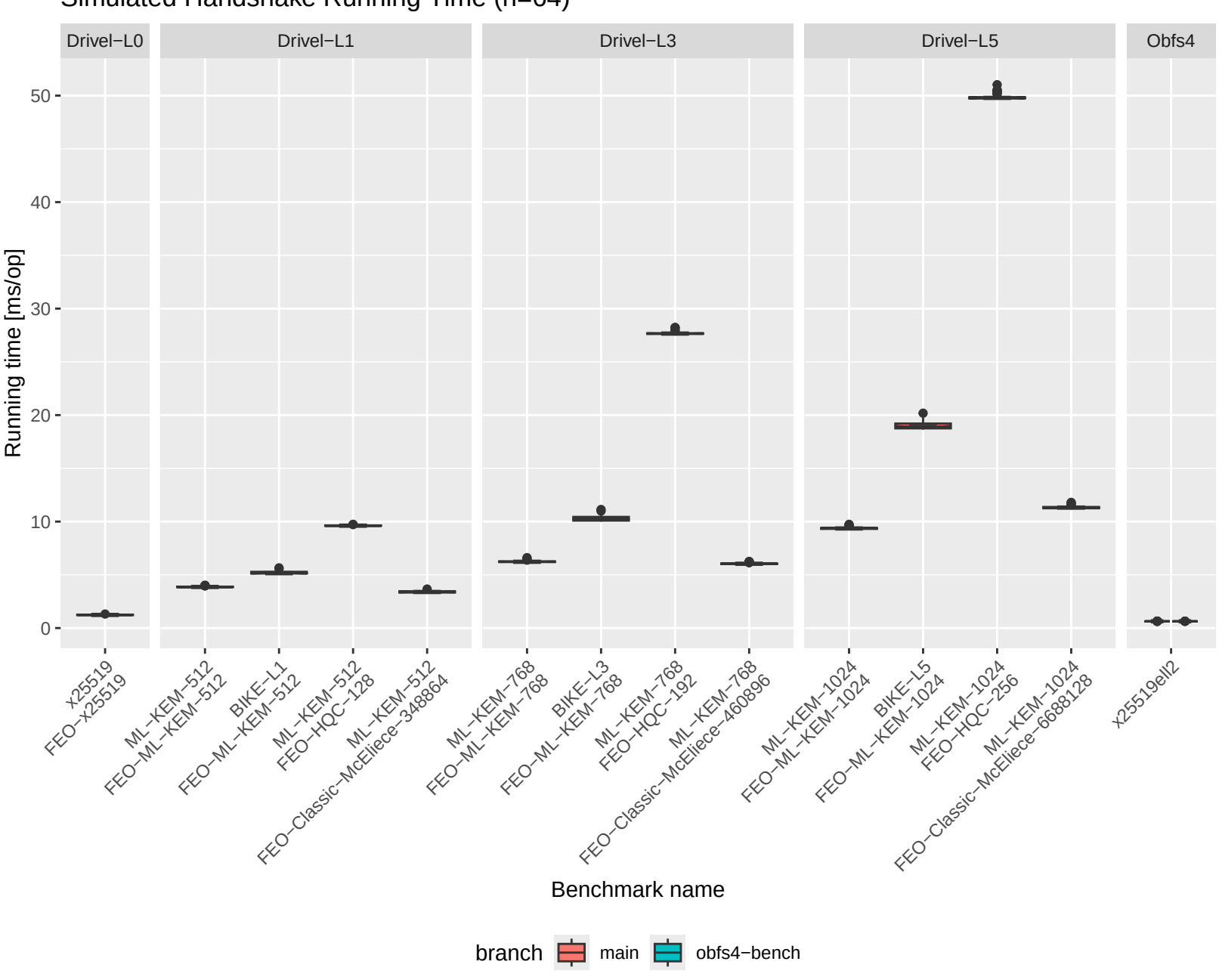
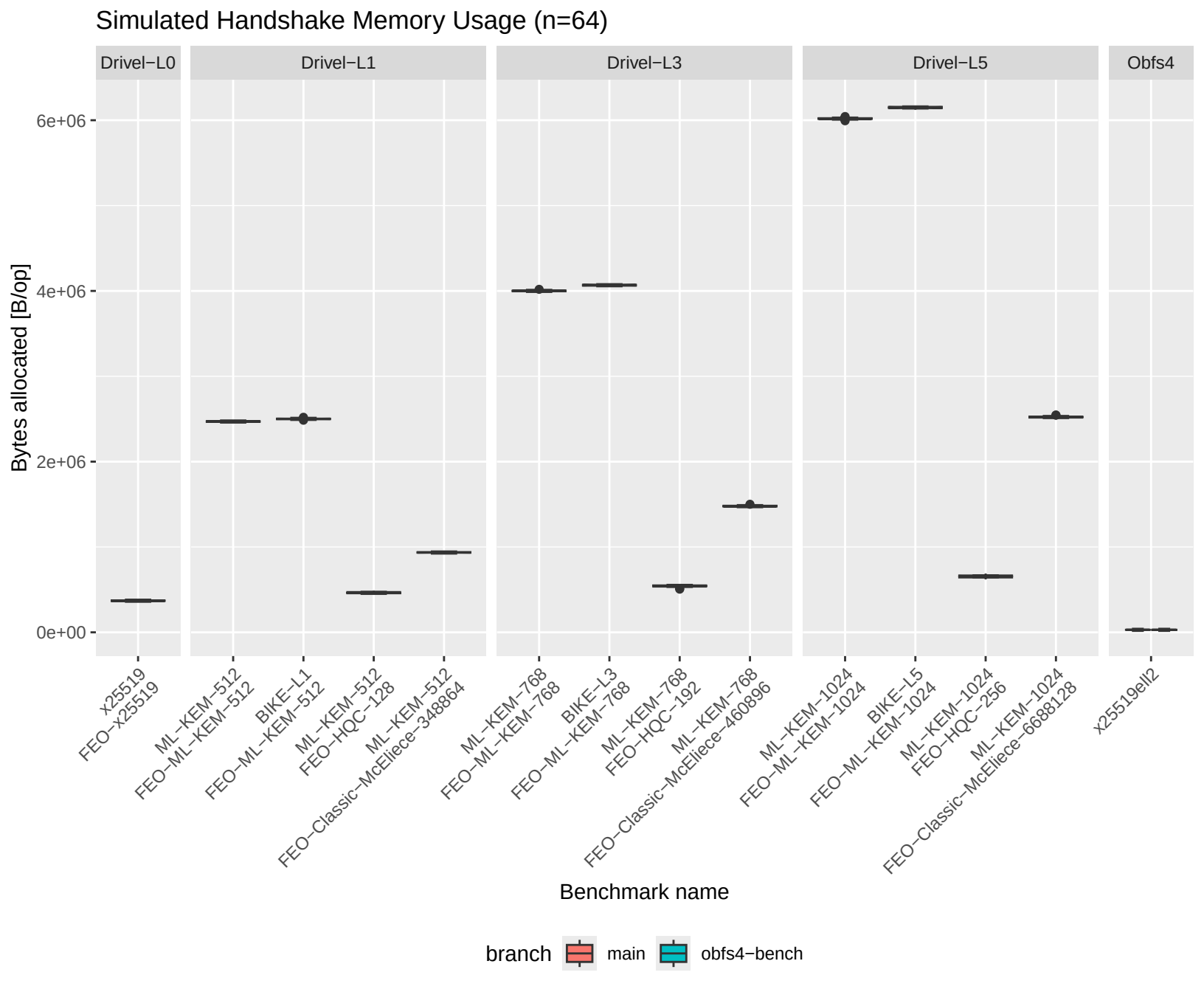
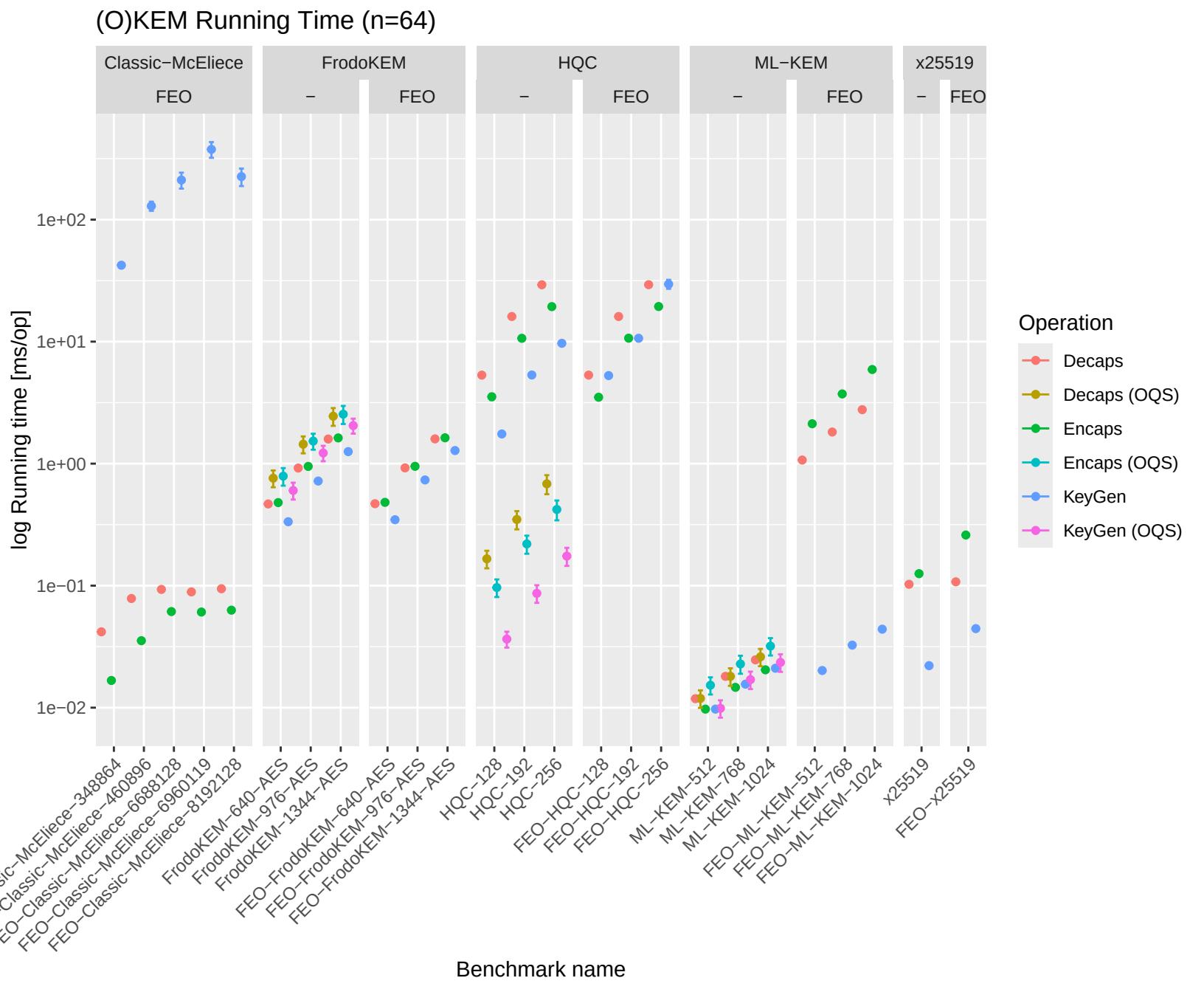
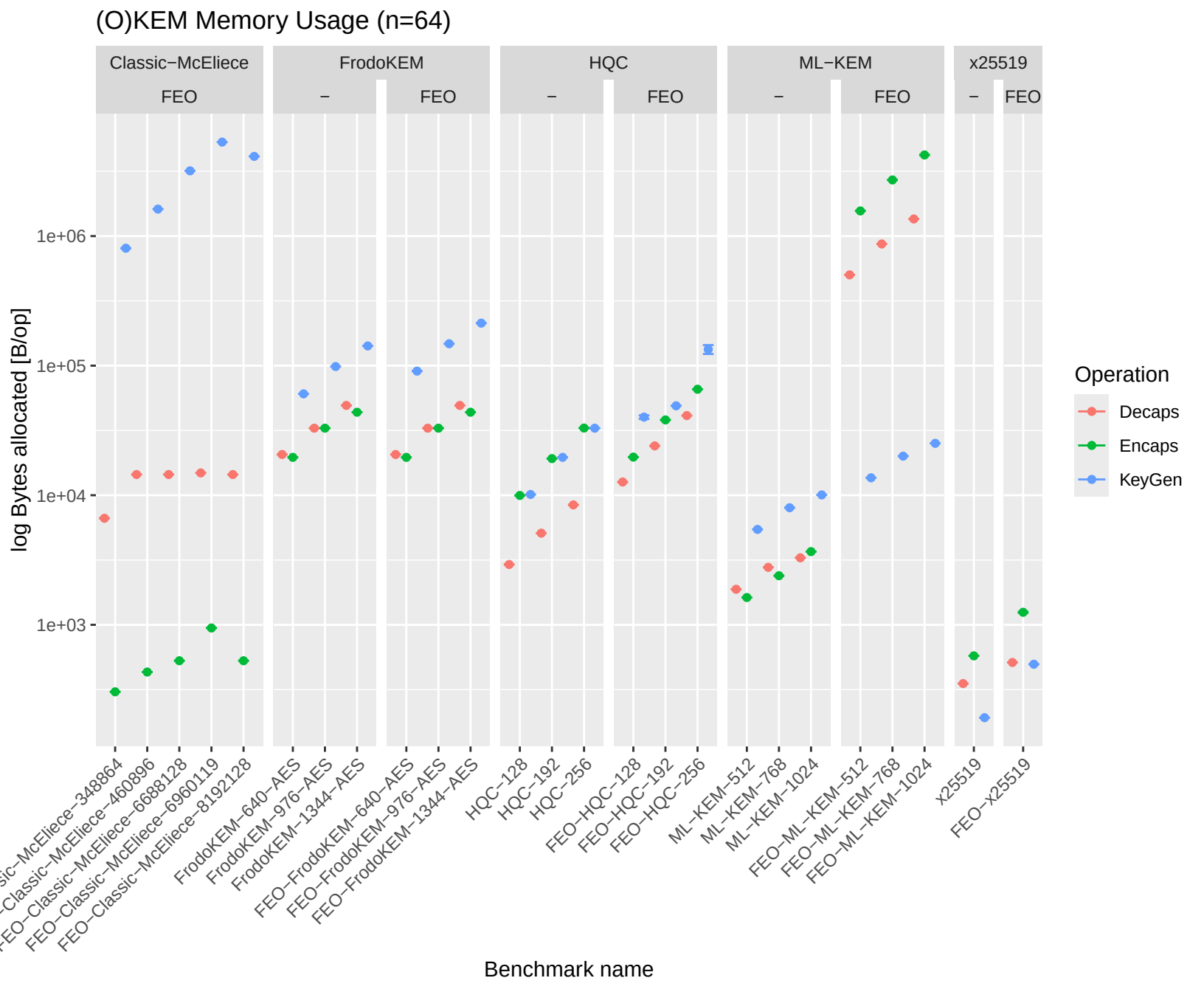

Running Time Changes in Preexisting Benchmarks (n=64)
common/ntor
BenchmarkHandshake
common/uniformdh
BenchmarkHandshake
internal/x25519ell2
BenchmarkKeyGeneration
internal/x25519ell2
BenchmarkMap
transports/obfs4
BenchmarkObfs4Handshake
transports/obfs4/framing
BenchmarkEncoder_Encode
0.56
0.55
0.54
7.25
7.20
7.15
7.10
0.0260
0.0258
0.0256
0.0254
0.0252
0.00455
0.00450
0.650
0.645
0.640
0.635
0.630
1.68
1.67
1.66
1.65
1.64
main
obfs4−bench
Running time [ms/op]
Branch
branch
main
obfs4−bench

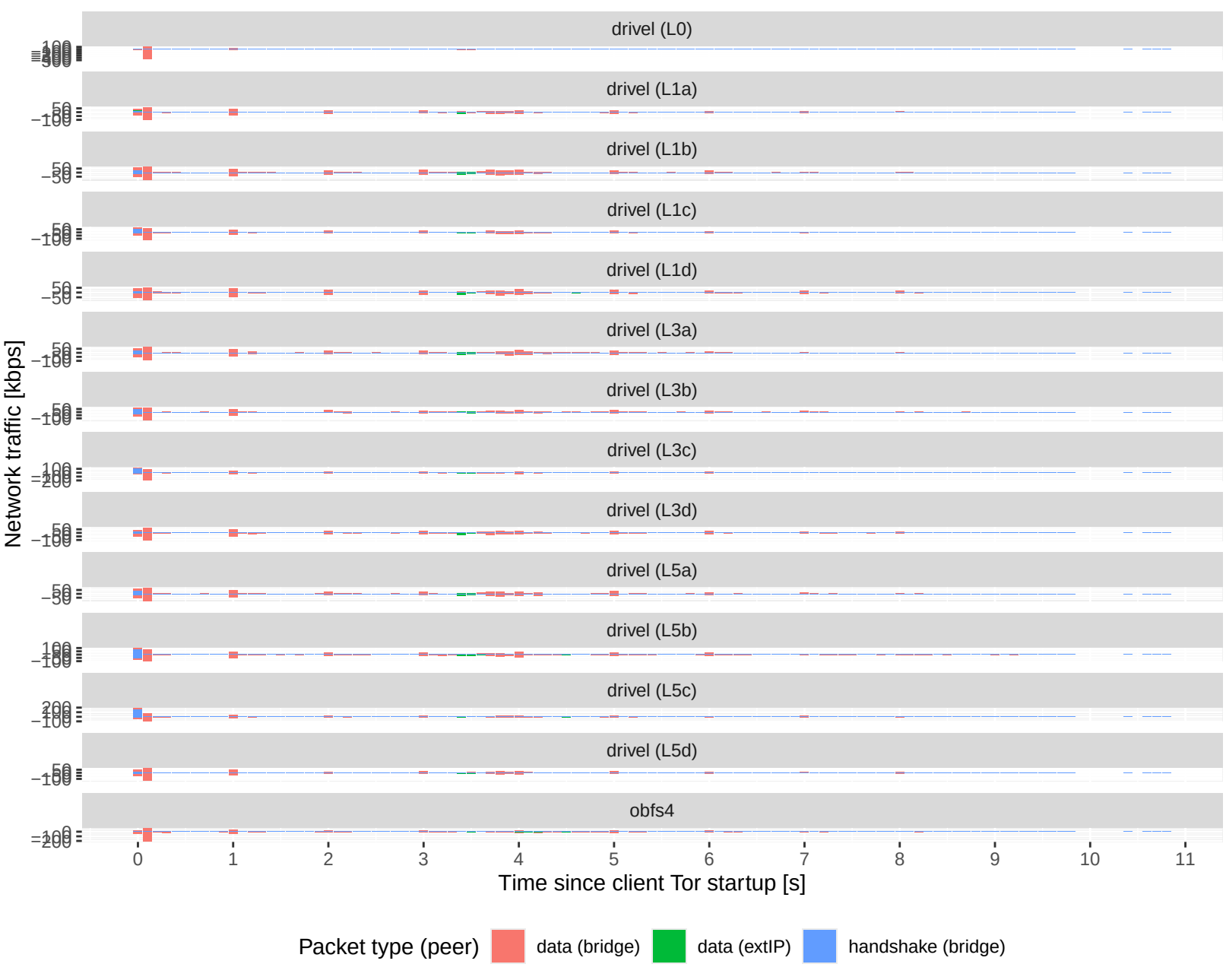

Memory Usage Changes in Preexisting Benchmarks (n=64)
common/ntor
BenchmarkHandshake
common/uniformdh
BenchmarkHandshake
internal/x25519ell2
BenchmarkKeyGeneration
internal/x25519ell2
BenchmarkMap
transports/obfs4
BenchmarkObfs4Handshake
transports/obfs4/framing
BenchmarkEncoder_Encode
Bytes allocated [B/op]
7910
7890
7870
7850
37980
37970
37960
37950
48.025
48.000
47.975
47.950
96.050
96.025
96.000
95.975
95.950
29600
29400
29200
29000
11800
11780
11760
main
obfs4−bench
Branch
branch
main
obfs4−bench

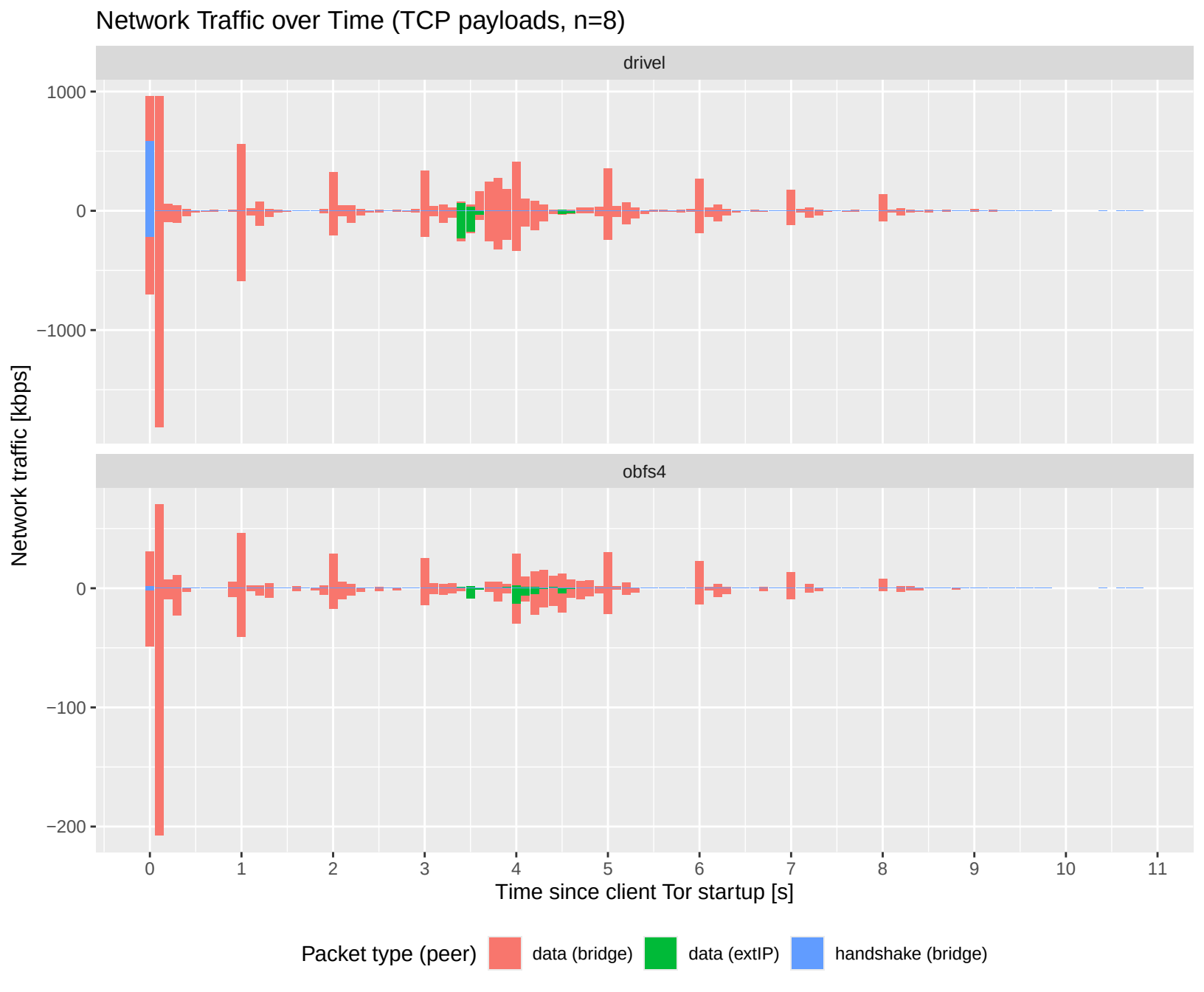

Simulated Handshake Running Time (n=64)
Drivel−L0
Drivel−L1
Drivel−L3
Drivel−L5
Obfs4
Running time [ms/op]
0
10
20
30
40
50
x25519
FEO−x25519
ML−KEM−512
FEO−ML−KEM−512
BIKE−L1
FEO−ML−KEM−512
ML−KEM−512
FEO−HQC−128
ML−KEM−512
FEO−Classic−McEliece−348864
ML−KEM−768
FEO−ML−KEM−768
BIKE−L3
FEO−ML−KEM−768
ML−KEM−768
FEO−HQC−192
ML−KEM−768
FEO−Classic−McEliece−460896
ML−KEM−1024
FEO−ML−KEM−1024
BIKE−L5
FEO−ML−KEM−1024
ML−KEM−1024
FEO−HQC−256
ML−KEM−1024
FEO−Classic−McEliece−6688128
x25519ell2
Benchmark name
branch
main
obfs4−bench

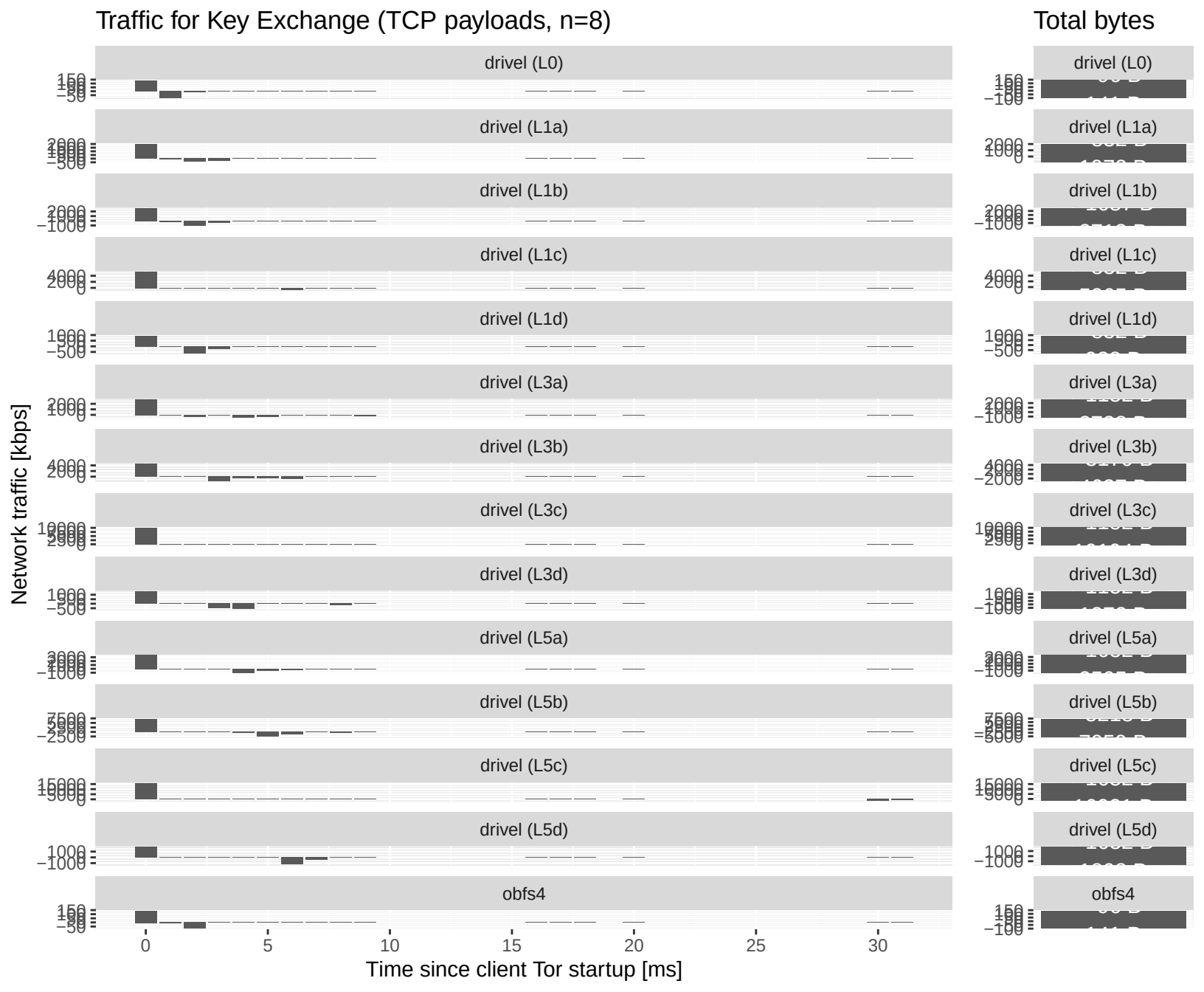

Simulated Handshake Memory Usage (n=64)
Drivel−L0
Drivel−L1
Drivel−L3
Drivel−L5
Obfs4
Bytes allocated [B/op]
6e+06
4e+06
2e+06
0e+00
x25519
FEO−x25519
ML−KEM−512
FEO−ML−KEM−512
BIKE−L1
FEO−ML−KEM−512
ML−KEM−512
FEO−HQC−128
ML−KEM−512
FEO−Classic−McEliece−348864
ML−KEM−768
FEO−ML−KEM−768
BIKE−L3
FEO−ML−KEM−768
ML−KEM−768
FEO−HQC−192
ML−KEM−768
FEO−Classic−McEliece−460896
ML−KEM−1024
FEO−ML−KEM−1024
BIKE−L5
FEO−ML−KEM−1024
ML−KEM−1024
FEO−HQC−256
ML−KEM−1024
FEO−Classic−McEliece−6688128
x25519ell2
Benchmark name
branch
main
obfs4−bench

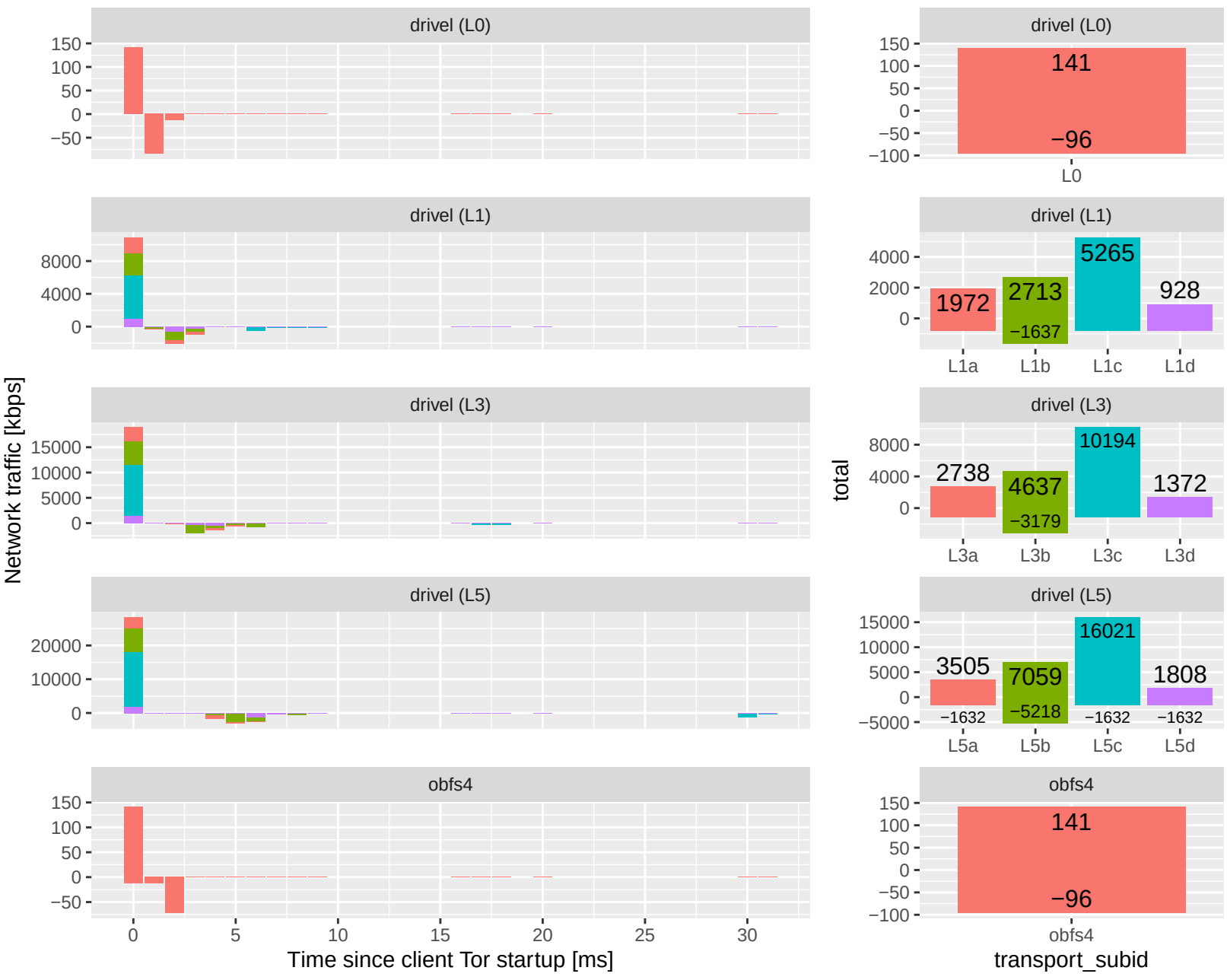

(O)KEM Running Time (n=64)
Classic−McEliece
FEO
FrodoKEM
−
FEO
HQC
−
FEO
ML−KEM
−
FEO
x25519
−
FEO
log Running time [ms/op]
1e+02
1e+01
1e+00
1e−01
1e−02
Classic−McEliece−348864
Classic−McEliece−460896
Classic−McEliece−6688128
Classic−McEliece−6960119
Classic−McEliece−8192128
FEO−Classic−McEliece−348864
FEO−Classic−McEliece−460896
FEO−Classic−McEliece−6688128
FEO−Classic−McEliece−6960119
FEO−Classic−McEliece−8192128
FrodoKEM−640−AES
FrodoKEM−976−AES
FrodoKEM−1344−AES
FEO−FrodoKEM−640−AES
FEO−FrodoKEM−976−AES
FEO−FrodoKEM−1344−AES
HQC−128
HQC−192
HQC−256
FEO−HQC−128
FEO−HQC−192
FEO−HQC−256
ML−KEM−512
ML−KEM−768
ML−KEM−1024
FEO−ML−KEM−512
FEO−ML−KEM−768
FEO−ML−KEM−1024
x25519
FEO−x25519
Benchmark name
Operation
Decaps
Decaps (OQS)
Encaps
Encaps (OQS)
KeyGen
KeyGen (OQS)

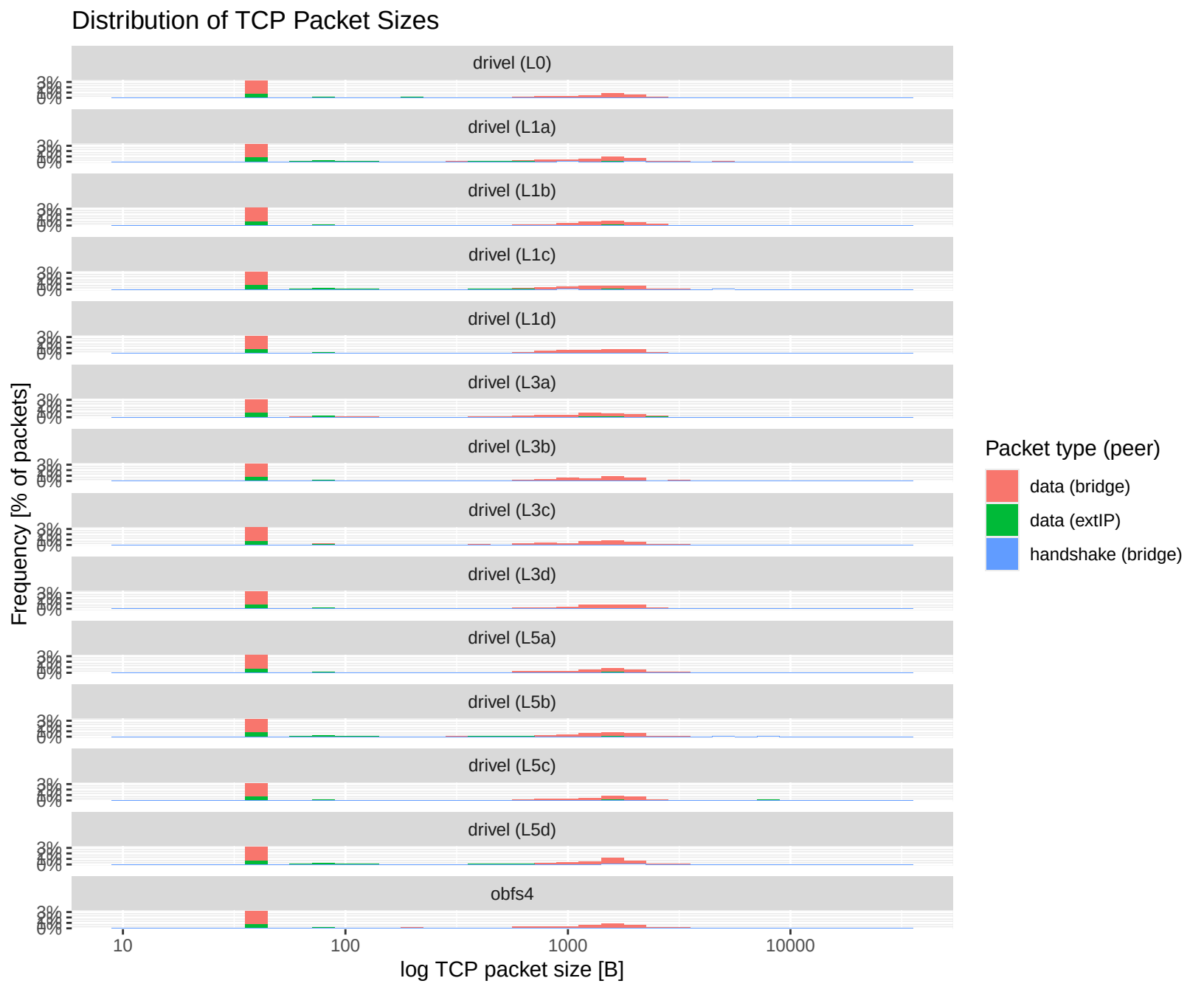

(O)KEM Memory Usage (n=64)
Classic−McEliece
FEO
FrodoKEM
−
FEO
HQC
−
FEO
ML−KEM
−
FEO
x25519
−
FEO
log Bytes allocated [B/op]
1e+06
1e+05
1e+04
1e+03
Operation
Decaps
Encaps
KeyGen
Classic−McEliece−348864
FEO−Classic−McEliece−460896
FEO−Classic−McEliece−6688128
FEO−Classic−McEliece−6960119
FEO−Classic−McEliece−8192128
FrodoKEM−640−AES
FrodoKEM−976−AES
FrodoKEM−1344−AES
FEO−FrodoKEM−640−AES
FEO−FrodoKEM−976−AES
FEO−FrodoKEM−1344−AES
HQC−128
HQC−192
HQC−256
FEO−HQC−128
FEO−HQC−192
FEO−HQC−256
ML−KEM−512
ML−KEM−768
ML−KEM−1024
FEO−ML−KEM−512
FEO−ML−KEM−768
FEO−ML−KEM−1024
x25519
FEO−x25519
Benchmark name


Network Traffic over Time (TCP payloads, n=8)
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
Network traffic [kbps]
0
1
2
3
4
5
6
7
8
9
10
11
Time since client Tor startup [s]
Packet type (peer)
data (bridge)
data (extIP)
handshake (bridge)

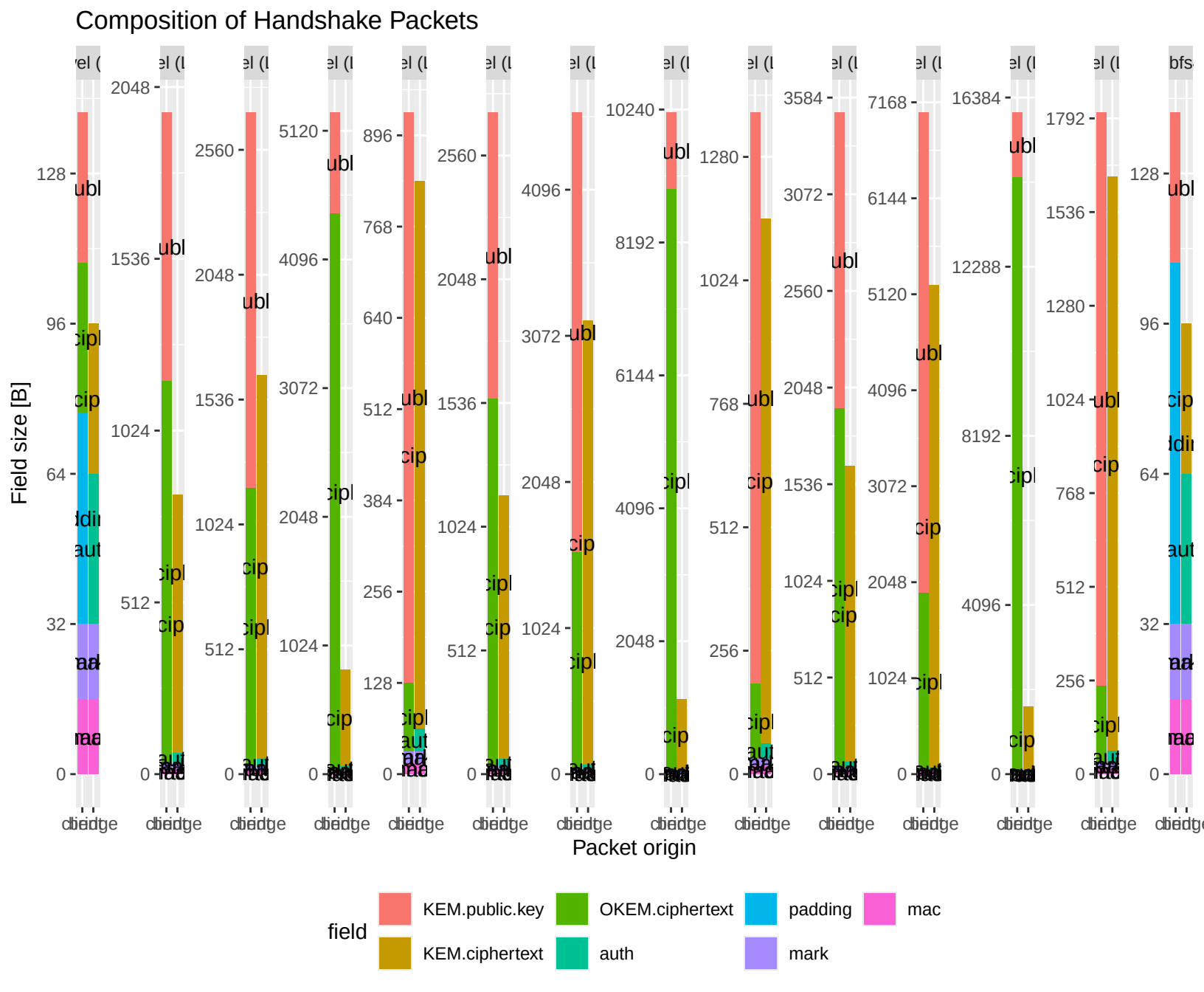

Network Traffic over Time (TCP payloads, n=8)
drivel
obfs4
1000
0
−1000
0
−100
−200
Network traffic [kbps]
0
1
2
3
4
5
6
7
8
9
10
11
Time since client Tor startup [s]
Packet type (peer)
data (bridge)
data (extIP)
handshake (bridge)

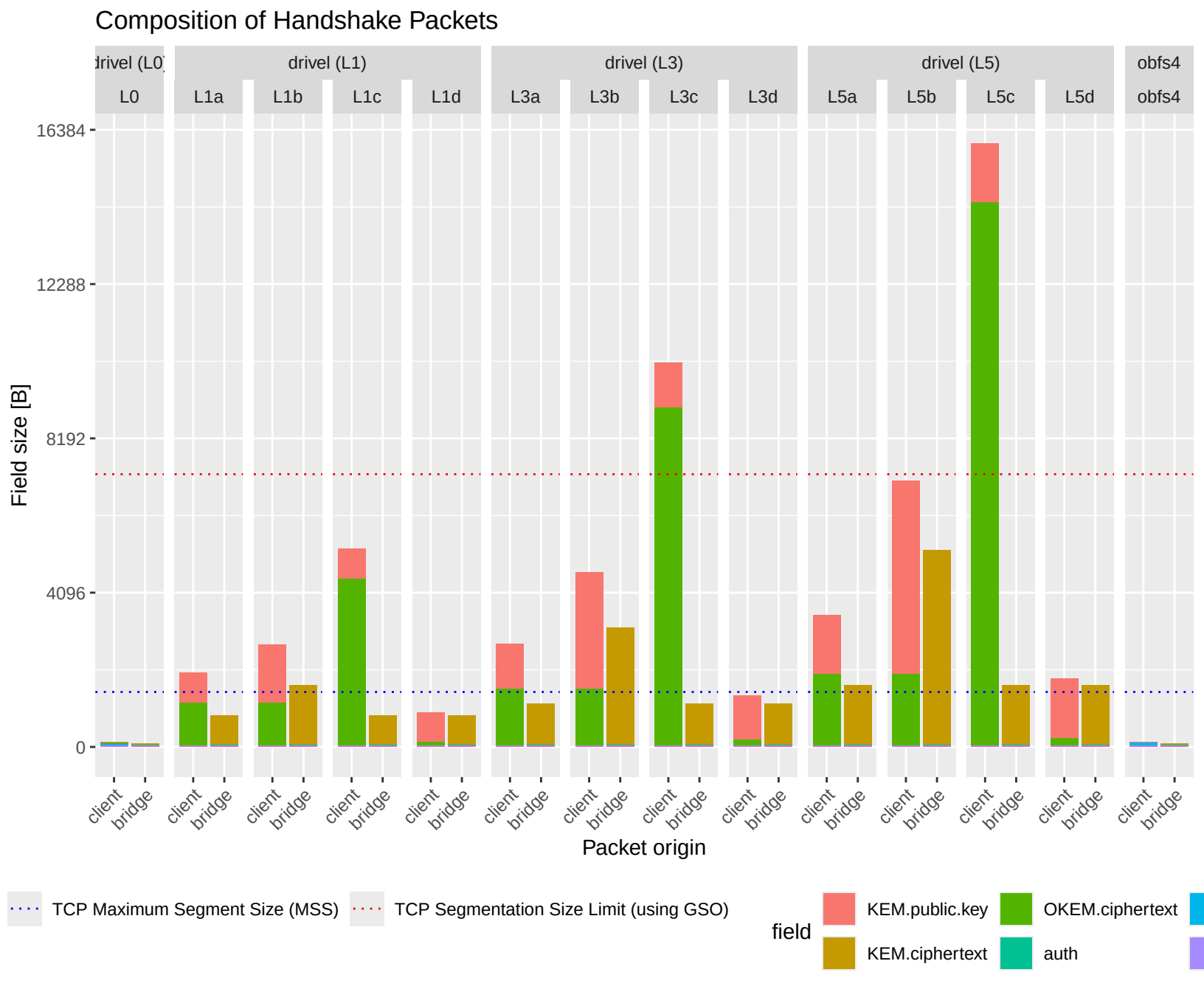

Traffic for Key Exchange (TCP payloads, n=8)
Total bytes
drivel (L0)
drivel (L1a)
drivel (L1b)
drivel (L1c)
drivel (L1d)
drivel (L3a)
drivel (L3b)
drivel (L3c)
drivel (L3d)
drivel (L5a)
drivel (L5b)
drivel (L5c)
drivel (L5d)
obfs4
Network traffic [kbps]
Time since client Tor startup [ms]
0
5
10
15
20
25
30


Traffic for Key Exchange (TCP payloads, n=8)
Total bytes
drivel (L0)
drivel (L1)
drivel (L3)
drivel (L5)
obfs4
Network traffic [kbps]
total
Time since client Tor startup [ms]
transport_subid
L0
L1a
L1b
L1c
L1d
L3a
L3b
L3c
L3d
L5a
L5b
L5c
L5d
141
−96
1972
2713
−1637
5265
928
2738
4637
−3179
10194
1372
3505
−1632
7059
−5218
16021
1808


Distribution of TCP Packet Sizes
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
3%
2%
1%
0%
Frequency [% of packets]
10
100
1000
10000
log TCP packet size [B]
Packet type (peer)
data (bridge)
data (extIP)
handshake (bridge)


Distribution of TCP Packet Sizes
drivel (L0)
drivel (L1)
drivel (L3)
drivel (L5)
obfs4
3%
2%
1%
0%
10%
5%
0%
Frequency [% of packets]
10
100
1000
10000
log TCP packet size [B]
Packet type (peer)
data (bridge)
data (extIP)
handshake (bridge)


Composition of Handshake Packets
Field size [B]
Packet origin
field
KEM.public.key
KEM.ciphertext
OKEM.ciphertext
auth
padding
mark
mac


Composition of Handshake Packets
drivel (L0)
drivel (L1)
drivel (L3)
drivel (L5)
obfs4
L0
L1a
L1b
L1c
L1d
L3a
L3b
L3c
L3d
L5a
L5b
L5c
L5d
obfs4
16384
12288
8192
4096
0
Field size [B]
client
bridge
Packet origin
TCP Maximum Segment Size (MSS)
TCP Segmentation Size Limit (using GSO)
field
KEM.public.key
OKEM.ciphertext
KEM.ciphertext
auth