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

Branch

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

obfs4-bench

Branch

main

obfs4-bench

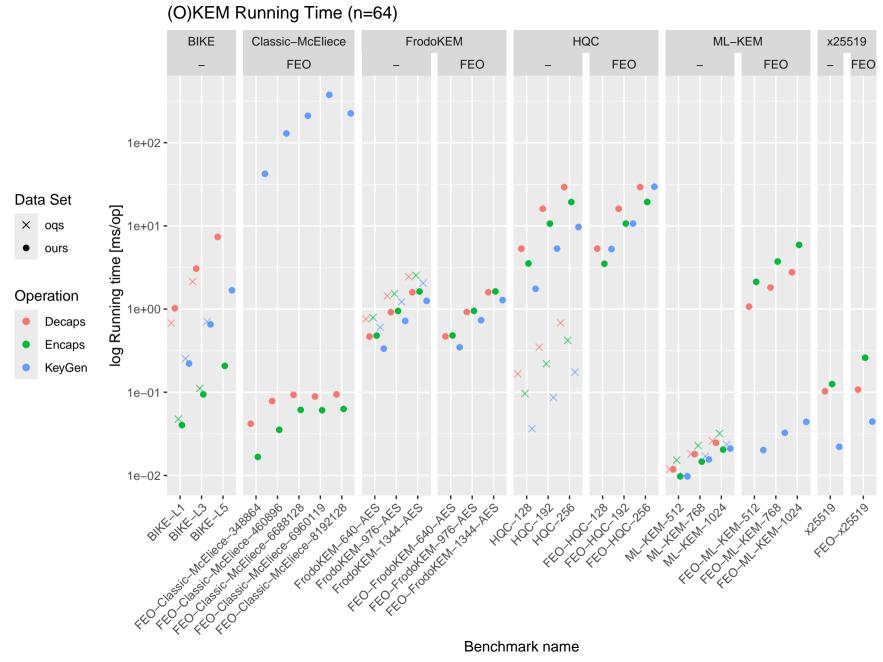
main

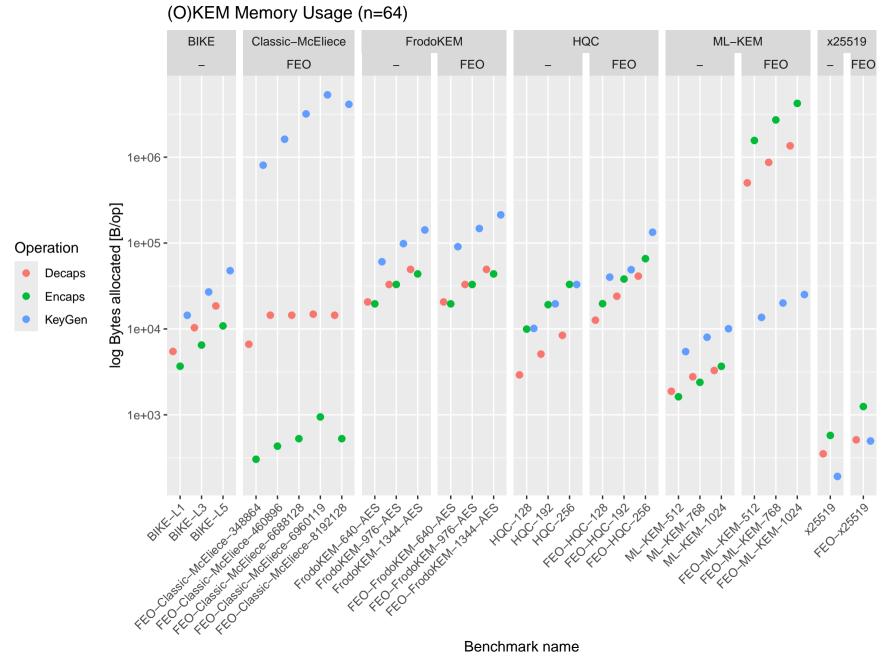
obfs4-bench

main

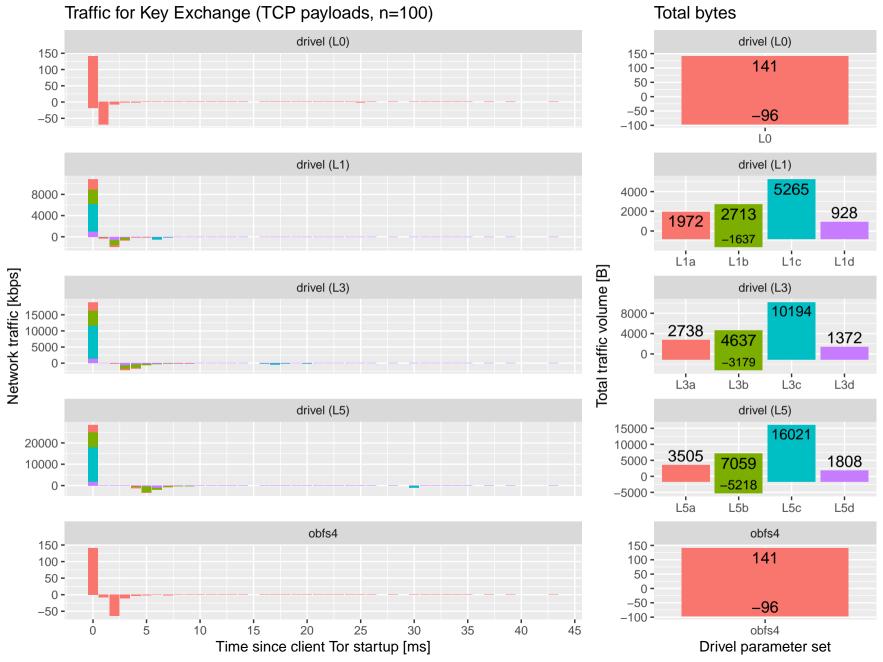
Simulated Handshake Running Time (n=64) Drivel-L0 Drivel-L1 Drivel-L3 Drivel-L5 Obfs4 50 -40 -Running time [ms] 10 -FEO. Classic Inclined State of PHO Cassic Notileos es 88 28 0 -160 10 to 10 Benchmark name

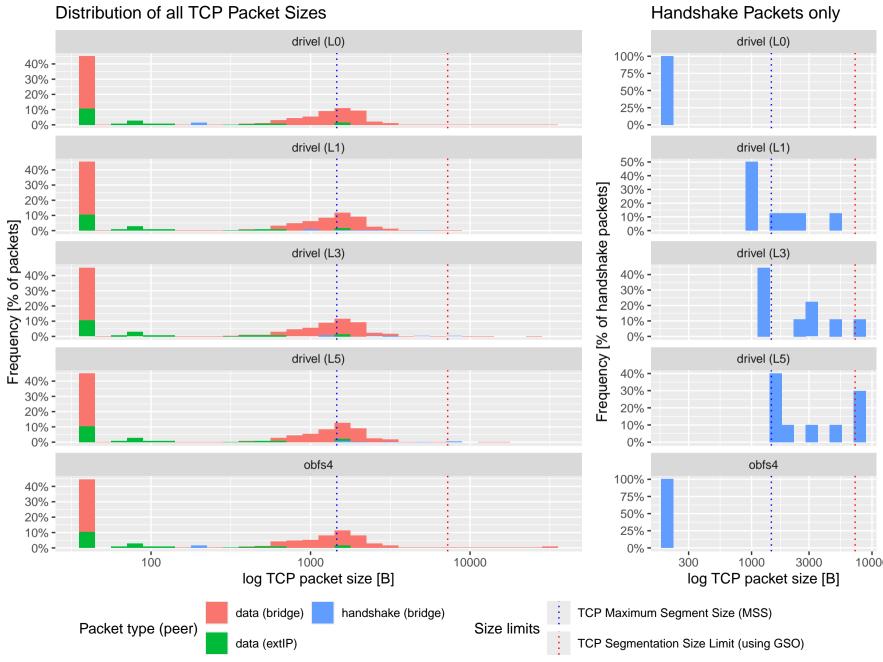
Simulated Handshake Memory Usage (n=64) Drivel-L0 Drivel-L1 Drivel-L3 Drivel-L5 Obfs4 6e+06 -Bytes allocated [B] 2e+06 -EED Classic natiles 888 28 Benr 0e+00 -LEO COSSIC WELLS TO SHELL STORE THE STORE OF Benchmark name





Network Traffic over Time (TCP payloads, n=100) drivel 50 **-**0 --50 **-**Network traffic [kbps] Packet type (peer) data (bridge) obfs4 data (extIP) 100 handshake (bridge) 0 --100 **-**-200 **-**2.5 5.0 15.0 0.0 17.5 7.5 10.0 12.5 20.0 Time since client Tor startup [s]





Composition of Handshake Packets

