```
Last login: Thu Apr 25 00:39:47 on ttys017
jgorman@Jacobs-MacBook-Pro ~ % cd Documents/github/instarand_benchmarking/
jgorman@Jacobs-MacBook-Pro instarand_benchmarking % cargo bench
    Finished bench [optimized] target(s) in 0.05s
     Running unittests src/lib.rs (target/release/deps/instarand_benchmarking-ef17cf1c4e7d3b6f)

running 26 tests
test crypto::bn::hashes::test::test_hash_g1_to_bits_diff_inputs ... ignored
test crypto::bn::hashes::test::test_hash_g1_to_bits_same_input ... ignored
test crypto::bn::hashes::test::test_hash_to_fr_diff_inputs ... ignored
test crypto::bn::hashes::test::test_hash_to_fr_same_input ... ignored
test crypto::bn::hashes::test::test_hash_to_g1_diff_inputs ... ignored
test crypto::bn::hashes::test::test_hash_to_g1_same_input ... ignored
test crypto::bn::hashes::test::test_rand_fr ... ignored
test crypto::secp::test::test_hash_to_curve_diff_inputs ... ignored
test crypto::secp::test::test_hash_to_curve_same_input ... ignored
test crypto::secp::test::test_hash_to_scalar_diff_inputs ... ignored
test crypto::secp::test::test_hash_to_scalar_same_input ... ignored
test crypto::secp::test::test_rand_scalar ... ignored
test impls::bls_vrf::test::bls_vrf_eval_ver ... ignored
test impls::bls_vrf::test::bls_vrf_wrong_input_fails ... ignored
test impls::bls_vrf::test::bls_vrf_wrong_pk_fails ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_failure_insufficient_pevals_glow ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_failure_insufficient_pevals_glow_hashless ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_failure_invalid_pevals_glow ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_failure_invalid_pevals_glow_hashless ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_success_glow ... ignored
test impls::glow_dvrf::test::test_dvrf_aggregation_success_glow_hashless ... ignored
test impls::glow_dvrf::test::test_dvrf_partial_evals_glow ... ignored
test impls::glow_dvrf::test::test_dvrf_partial_evals_glow_hashless ... ignored
test impls::goldberg_vrf::test::bls_vrf_eval_ver ... ignored
test impls::goldberg_vrf::test::bls_vrf_wrong_input_fails ... ignored
test impls::goldberg_vrf::test::bls_vrf_wrong_pk_fails ... ignored

test result: ok. 0 passed; 0 failed; 26 ignored; 0 measured; 0 filtered out; finished in 0.00s

     Running unittests src/main.rs (target/release/deps/instarand_benchmarking-cbf1ad4aa4c49dc4)

running 0 tests

test result: ok. 0 passed; 0 failed; 0 ignored; 0 measured; 0 filtered out; finished in 0.00s

     Running benches/dvrf.rs (target/release/deps/dvrf-b429b92ff0466fc1)
Gnuplot not found, using plotters backend
bench_glow_dvrf/glow_dvrf/partial_evaluation
                        time:   [501.33 µs 501.59 µs 501.93 µs]
                        thrpt:  [1.9923 Kelem/s 1.9937 Kelem/s 1.9947 Kelem/s]
                 change:
                        time:   [-0.2299% -0.0915% +0.0214%] (p = 0.18 > 0.05)
                        thrpt:  [-0.0214% +0.0916% +0.2305%]
                        No change in performance detected.
bench_glow_dvrf/glow_dvrf/partial_verification
                        time:   [614.42 µs 614.73 µs 615.16 µs]
                        thrpt:  [1.6256 Kelem/s 1.6267 Kelem/s 1.6276 Kelem/s]
                 change:
                        time:   [-0.2731% -0.0860% +0.0620%] (p = 0.37 > 0.05)
                        thrpt:  [-0.0620% +0.0861% +0.2739%]
                        No change in performance detected.
bench_glow_dvrf/glow_dvrf/aggregation_threshold_8
                        time:   [493.50 µs 493.89 µs 494.52 µs]
                        thrpt:  [2.0221 Kelem/s 2.0247 Kelem/s 2.0263 Kelem/s]
                 change:
                        time:   [-0.3281% +0.0415% +0.4595%] (p = 0.85 > 0.05)
                        thrpt:  [-0.4574% -0.0415% +0.3291%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_glow_dvrf/glow_dvrf/aggregation_threshold_16
                        time:   [1.0141 ms 1.0152 ms 1.0168 ms]
                        thrpt:  [983.48  elem/s 985.08  elem/s 986.11  elem/s]
                 change:
                        time:   [-0.3212% +0.0117% +0.3550%] (p = 0.95 > 0.05)
                        thrpt:  [-0.3538% -0.0117% +0.3222%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_glow_dvrf/glow_dvrf/aggregation_threshold_32
                        time:   [2.1350 ms 2.1361 ms 2.1380 ms]
                        thrpt:  [467.72  elem/s 468.14  elem/s 468.39  elem/s]
                 change:
                        time:   [-0.3170% -0.0507% +0.2145%] (p = 0.74 > 0.05)
                        thrpt:  [-0.2140% +0.0507% +0.3180%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high severe
bench_glow_dvrf/glow_dvrf/aggregation_threshold_64
                        time:   [4.6761 ms 4.6813 ms 4.6869 ms]
                        thrpt:  [213.36  elem/s 213.61  elem/s 213.85  elem/s]
                 change:
                        time:   [-0.1816% -0.0525% +0.0645%] (p = 0.44 > 0.05)
                        thrpt:  [-0.0644% +0.0525% +0.1819%]
                        No change in performance detected.
bench_glow_dvrf/glow_dvrf/verify
                        time:   [2.8188 ms 2.8194 ms 2.8201 ms]
                        thrpt:  [354.59  elem/s 354.68  elem/s 354.76  elem/s]
                 change:
                        time:   [-0.1761% -0.0825% +0.0059%] (p = 0.09 > 0.05)
                        thrpt:  [-0.0059% +0.0826% +0.1764%]
                        No change in performance detected.
Found 3 outliers among 20 measurements (15.00%)
  2 (10.00%) high mild
  1 (5.00%) high severe

     Running benches/flexirand.rs (target/release/deps/flexirand-e880372537cf7c5a)
Gnuplot not found, using plotters backend
bench_flexirand/flexirand_glow_bn254/blinding
                        time:   [383.34 µs 383.45 µs 383.55 µs]
                        thrpt:  [2.6072 Kelem/s 2.6079 Kelem/s 2.6086 Kelem/s]
                 change:
                        time:   [-0.3004% -0.1444% -0.0189%] (p = 0.05 > 0.05)
                        thrpt:  [+0.0189% +0.1446% +0.3013%]
                        No change in performance detected.
Found 4 outliers among 20 measurements (20.00%)
  1 (5.00%) low mild
  3 (15.00%) high mild
bench_flexirand/flexirand_glow_bn254/input_verifcation
                        time:   [373.43 µs 373.63 µs 373.85 µs]
                        thrpt:  [2.6749 Kelem/s 2.6764 Kelem/s 2.6779 Kelem/s]
                 change:
                        time:   [-0.2373% -0.1240% -0.0207%] (p = 0.03 < 0.05)
                        thrpt:  [+0.0207% +0.1241% +0.2379%]
                        Change within noise threshold.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_flexirand/flexirand_glow_bn254/partial_evaluation
                        time:   [505.56 µs 505.91 µs 506.30 µs]
                        thrpt:  [1.9751 Kelem/s 1.9766 Kelem/s 1.9780 Kelem/s]
                 change:
                        time:   [-0.1712% -0.0500% +0.0724%] (p = 0.44 > 0.05)
                        thrpt:  [-0.0724% +0.0501% +0.1715%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  1 (5.00%) high mild
  1 (5.00%) high severe
bench_flexirand/flexirand_glow_bn254/partial_verification
                        time:   [618.88 µs 619.35 µs 619.96 µs]
                        thrpt:  [1.6130 Kelem/s 1.6146 Kelem/s 1.6158 Kelem/s]
                 change:
                        time:   [-0.1459% -0.0225% +0.1052%] (p = 0.73 > 0.05)
                        thrpt:  [-0.1050% +0.0225% +0.1461%]
                        No change in performance detected.
```

```
bench_flexirand/flexirand_glow_bn254_threshold_8
                        time:   [488.24 µs 488.74 µs 489.53 µs]
                        thrpt:  [2.0428 Kelem/s 2.0461 Kelem/s 2.0482 Kelem/s]
                 change:
                        time:   [−0.4112% −0.0634% +0.3040%] (p = 0.74 > 0.05)
                        thrpt:  [−0.3031% +0.0634% +0.4129%]
                        No change in performance detected.
bench_flexirand/flexirand_glow_bn254_threshold_16
                        time:   [1.0085 ms 1.0097 ms 1.0116 ms]
                        thrpt:  [988.54  elem/s 990.40  elem/s 991.54  elem/s]
                 change:
                        time:   [−0.3718% +0.0370% +0.4547%] (p = 0.87 > 0.05)
                        thrpt:  [−0.4527% −0.0370% +0.3732%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  2 (10.00%) high mild
bench_flexirand/flexirand_glow_bn254_threshold_32
                        time:   [2.1306 ms 2.1322 ms 2.1343 ms]
                        thrpt:  [468.54  elem/s 469.00  elem/s 469.35  elem/s]
                 change:
                        time:   [−0.1959% −0.0113% +0.1741%] (p = 0.91 > 0.05)
                        thrpt:  [−0.1738% +0.0113% +0.1963%]
                        No change in performance detected.
bench_flexirand/flexirand_glow_bn254_threshold_64
                        time:   [4.6751 ms 4.6786 ms 4.6826 ms]
                        thrpt:  [213.56  elem/s 213.74  elem/s 213.90  elem/s]
                 change:
                        time:   [−0.2013% −0.0815% +0.0393%] (p = 0.20 > 0.05)
                        thrpt:  [−0.0393% +0.0816% +0.2017%]
                        No change in performance detected.
bench_flexirand/flexirand_glow_bn254/prever
                        time:   [2.8185 ms 2.8195 ms 2.8207 ms]
                        thrpt:  [354.53  elem/s 354.67  elem/s 354.80  elem/s]
                 change:
                        time:   [−0.2919% −0.1204% +0.0196%] (p = 0.16 > 0.05)
                        thrpt:  [−0.0196% +0.1206% +0.2928%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_flexirand/flexirand_glow_bn254/unblinding
                        time:   [126.03 µs 126.16 µs 126.33 µs]
                        thrpt:  [7.9156 Kelem/s 7.9264 Kelem/s 7.9348 Kelem/s]
                 change:
                        time:   [−0.1140% +0.0455% +0.1903%] (p = 0.58 > 0.05)
                        thrpt:  [−0.1900% −0.0455% +0.1141%]
                        No change in performance detected.
bench_flexirand/flexirand_glow_bn254/verification
                        time:   [2.8140 ms 2.8158 ms 2.8189 ms]
                        thrpt:  [354.75  elem/s 355.14  elem/s 355.37  elem/s]
                 change:
                        time:   [−0.0766% +0.0969% +0.3156%] (p = 0.38 > 0.05)
                        thrpt:  [−0.3146% −0.0968% +0.0767%]
                        No change in performance detected.
Found 4 outliers among 20 measurements (20.00%)
  3 (15.00%) high mild
  1 (5.00%) high severe

     Running benches/instarand.rs (target/release/deps/instarand-5470924c2344a7b1)
Gnuplot not found, using plotters backend
bench_instarand/goldberg_vrf_secp256k1/keygen
                        time:   [16.928 µs 16.933 µs 16.939 µs]
                        thrpt:  [59.036 Kelem/s 59.056 Kelem/s 59.074 Kelem/s]
                 change:
                        time:   [−0.6662% −0.3316% −0.0352%] (p = 0.05 < 0.05)
                        thrpt:  [+0.0352% +0.3327% +0.6707%]
                        Change within noise threshold.
bench_instarand/goldberg_vrf_secp256k1/client_vrf_eval
                        time:   [181.42 µs 181.50 µs 181.60 µs]
                        thrpt:  [5.5065 Kelem/s 5.5097 Kelem/s 5.5121 Kelem/s]
                 change:
                        time:   [−0.1373% −0.0404% +0.0554%] (p = 0.43 > 0.05)
                        thrpt:  [−0.0554% +0.0405% +0.1375%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  2 (10.00%) high mild
bench_instarand/goldberg_vrf_secp256k1/client_vrf_ver
                        time:   [217.32 µs 217.54 µs 217.79 µs]
                        thrpt:  [4.5915 Kelem/s 4.5968 Kelem/s 4.6014 Kelem/s]
                 change:
                        time:   [−0.1070% −0.0198% +0.0752%] (p = 0.68 > 0.05)
                        thrpt:  [−0.0752% +0.0198% +0.1071%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_instarand/bls_vrf_bn254/server_vrf_eval
                        time:   [241.33 µs 241.56 µs 241.95 µs]
                        thrpt:  [4.1331 Kelem/s 4.1397 Kelem/s 4.1437 Kelem/s]
                 change:
                        time:   [−0.2085% −0.0273% +0.1816%] (p = 0.80 > 0.05)
                        thrpt:  [−0.1813% +0.0273% +0.2089%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  2 (10.00%) high severe
bench_instarand/bls_vrf_bn254/server_vrf_ver
                        time:   [2.8117 ms 2.8125 ms 2.8134 ms]
                        thrpt:  [355.44  elem/s 355.55  elem/s 355.66  elem/s]
                 change:
                        time:   [−0.3392% −0.1435% +0.0333%] (p = 0.16 > 0.05)
                        thrpt:  [−0.0333% +0.1437% +0.3403%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high severe
bench_instarand/glow_dvrf_bn254/server_dvrf_partial_eval
                        time:   [500.80 µs 501.00 µs 501.25 µs]
                        thrpt:  [1.9950 Kelem/s 1.9960 Kelem/s 1.9968 Kelem/s]
                 change:
                        time:   [−0.1695% −0.0464% +0.0889%] (p = 0.51 > 0.05)
                        thrpt:  [−0.0888% +0.0464% +0.1698%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  1 (5.00%) high mild
  1 (5.00%) high severe
bench_instarand/glow_dvrf_bn254/server_dvrf_partial_ver
                        time:   [613.91 µs 614.68 µs 615.48 µs]
                        thrpt:  [1.6248 Kelem/s 1.6268 Kelem/s 1.6289 Kelem/s]
                 change:
                        time:   [−0.0803% +0.0438% +0.1658%] (p = 0.51 > 0.05)
                        thrpt:  [−0.1655% −0.0438% +0.0803%]
                        No change in performance detected.
bench_instarand/glow_dvrf_bn254_threshold_8
                        time:   [486.60 µs 487.43 µs 488.75 µs]
                        thrpt:  [2.0460 Kelem/s 2.0516 Kelem/s 2.0551 Kelem/s]
                 change:
                        time:   [−0.2918% +0.1297% +0.5702%] (p = 0.58 > 0.05)
                        thrpt:  [−0.5670% −0.1296% +0.2927%]
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_instarand/glow_dvrf_bn254_threshold_16
                        time:   [1.0058 ms 1.0068 ms 1.0085 ms]
                        thrpt:  [991.61  elem/s 993.24  elem/s 994.21  elem/s]
                 change:
                        time:   [−0.3609% +0.0163% +0.3851%] (p = 0.94 > 0.05)
                        thrpt:  [−0.3836% −0.0163% +0.3622%]
                        No change in performance detected.
bench_instarand/glow_dvrf_bn254_threshold_32
                        time:   [2.1311 ms 2.1326 ms 2.1343 ms]
                        thrpt:  [468.53  elem/s 468.92  elem/s 469.24  elem/s]
                 change:
                        time:   [−0.2896% −0.0871% +0.1240%] (p = 0.41 > 0.05)
                        thrpt:  [−0.1238% +0.0871% +0.2905%]
```

```
                        No change in performance detected.
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_instarand/glow_dvrf_bn254_threshold_64
                        time:   [4.6743 ms 4.6813 ms 4.6923 ms]
                        thrpt:  [213.12  elem/s 213.62  elem/s 213.94  elem/s]
                 change:
                        time:   [-0.1290% +0.0252% +0.1902%] (p = 0.77 > 0.05)
                        thrpt:  [-0.1899% -0.0252% +0.1291%]
                        No change in performance detected.
Found 3 outliers among 20 measurements (15.00%)
  2 (10.00%) high mild
  1 (5.00%) high severe
bench_instarand/glow_dvrf_bn254/server_dvrf_verify
                        time:   [2.8115 ms 2.8124 ms 2.8134 ms]
                        thrpt:  [355.44  elem/s 355.56  elem/s 355.68  elem/s]
                 change:
                        time:   [-0.2123% -0.0692% +0.0520%] (p = 0.35 > 0.05)
                        thrpt:  [-0.0520% +0.0693% +0.2128%]
                        No change in performance detected.
Found 2 outliers among 20 measurements (10.00%)
  2 (10.00%) high mild

     Running benches/vrf.rs (target/release/deps/vrf-cb0d0ddc2d16e07f)
Gnuplot not found, using plotters backend
bench_vrf/goldberg_secp256k1/evaluation
                        time:   [179.71 µs 179.76 µs 179.81 µs]
                        thrpt:  [5.5613 Kelem/s 5.5630 Kelem/s 5.5645 Kelem/s]
Found 1 outliers among 20 measurements (5.00%)
  1 (5.00%) high mild
bench_vrf/goldberg_secp256k1/verification
                        time:   [215.69 µs 215.77 µs 215.86 µs]
                        thrpt:  [4.6327 Kelem/s 4.6346 Kelem/s 4.6363 Kelem/s]

jgorman@Jacobs-MacBook-Pro instarand_benchmarking %
```