

ChaosCrypto WP2 – Report

Inputs

- Benchmark CSV: `../bench/results.csv` (24 variants aggregated)
- Analyze CSV: `../analyze/analysis.csv` (24 variants aggregated)
- Token: not stored; only fingerprints in source CSV

Scope

- Profile: tobi
- Coord: (12,34)
- nbytes: 1048576
- Seed strategies: ['neighborhood3', 'window_mean_3x3']
- Memory types: ['opensimplex', 'perlin']
- Varying parameters:
 - dt: [0.01]
 - warmup: [100, 1000, 5000]
 - quant_k: [100000.0, 10000000.0]
 - size: [128]
 - scale: [0.1]

Benchmark Summary

Top throughput overall (mean over repeats):

dt	warmup	quant_k	size	scale	seed_strategy	memory_type	mean_tp_bps	keystream_sha256
0.01	100	100000.0	128	0.1	neighborhood3	opensimplex	0.295372	3.55e+06
0.01	100	100000.0	128	0.1	neighborhood3	perlin	0.302022	3.47e+06
0.01	100	100000.0	128	0.1	window_mean_3x3	opensimplex	0.303321	3.46e+06
0.01	100	100000.0	128	0.1	window_mean_3x3	perlin	0.305879	3.43e+06
0.01	100	10000000.0	128	0.1	neighborhood3	opensimplex	0.313002	3.35e+06

Top throughput per seed_strategy (best across memory types):

seed_strategy	dt	warmup	quant_k	memory_type	mean_tp_bps	keystream_sha256
neighborhood3	0.01	100	100000.0	opensimplex	3.55e+06	b8ce10e014ed53eb9dfab2ce1
window_mean_3x3	0.01	100	100000.0	opensimplex	3.46e+06	4c63b5572566e8129ff2fa6013

Top throughput per seed_strategy and memory_type:

seed_strategy	memory_type	dt	warmup	quant_k	size	scale	mean_tp_bps	keystream_sha256
neighborhood3	opensimplex	0.01	100	100000.0	128	0.1	3.55e+06	b8ce10e014ed53eb9dfab2ce1

seed_strategy	memory_type	dt	warmup	quant_k	size	scale	mean_tp_bps	keystream_sha256
neighborhood3	perlin	0.01	100	1000000.0	128	0.1	3.47e+06	265c51e4280be77c3198
window_mean_3x3	opensimplex	0.01	100	1000000.0	128	0.1	3.46e+06	4c63b5572566e8129ff2f
window_mean_3x3	perlin	0.01	100	1000000.0	128	0.1	3.43e+06	8961d882e761a738a1d6

Analyze Summary

- Bit ones ratio min/mean/max: (0.499577, 0.500057, 0.500528)
- Runs norm diff min/mean/max: (-0.000371, -1.7e-05, 0.000411)
- Byte chi2 norm min/mean/max: (0.896563, 1.051495, 1.135279)
- Autocorr lag1 min/mean/max: (-0.000823, 3.4e-05, 0.000742)

Per seed_strategy / memory_type (mean values):

seed_strategy	memory_type	bit_ones_ratio	byte_chi2_norm	runs_norm_diff	autocorr_lag_1
neighborhood3	opensimplex	0.500275	1.065996	0.000172	-0.000345
neighborhood3	perlin	0.499981	1.031055	-0.000095	0.000190
window_mean_3x3	opensimplex	0.499950	1.008068	-0.000053	0.000106
window_mean_3x3	perlin	0.500021	1.100860	-0.000092	0.000184

dt	warmup	quant_k	size	scale	seed_strategy	memory_type	bit_ones_ratio	byte_chi2_norm	runs_norm_diff	autocorr_lag_1	keystream_sha256
0.01	100	1000000.0	128	0.1	neighborhood3	opensimplex	0.500501	1.012630	-0.000054	0.000108	b8ce10e014ed53eb
0.01	100	1000000.0	128	0.1	neighborhood3	perlin	0.499951	0.953018	0.000173	-0.000346	265c51e4280be77c3198
0.01	100	1000000.0	128	0.1	window_mean_3x3	opensimplex	0.500310	0.899140	-0.000094	0.000188	4c63b5572566e8129ff2f
0.01	100	1000000.0	128	0.1	window_mean_3x3	perlin	0.500280	1.079013	0.000026	-0.000052	8961d882e761a738a1d6
0.01	100	10000000.0	128	0.1	neighborhood3	opensimplex	0.500032	1.126147	0.000411	-0.000822	227a776499831b3a
0.01	100	10000000.0	128	0.1	neighborhood3	perlin	0.500010	1.116042	-0.000352	0.000704	38dd69fdca01279c
0.01	100	10000000.0	128	0.1	window_mean_3x3	opensimplex	0.499577	1.115259	-0.000011	0.000022	ba43d8241d8995c8
0.01	100	10000000.0	128	0.1	window_mean_3x3	perlin	0.499784	1.129220	-0.000216	0.000432	62be714da77289db
0.01	1000	100000.0	128	0.1	neighborhood3	opensimplex	0.500505	1.013369	-0.000060	0.000120	65adf6de4f974e02a
0.01	1000	100000.0	128	0.1	neighborhood3	perlin	0.499941	0.950057	0.000171	-0.000341	3dfa2a9120d6e39a
0.01	1000	100000.0	128	0.1	window_mean_3x3	opensimplex	0.500311	0.896563	-0.000092	0.000184	aedec9c276e06b68
0.01	1000	100000.0	128	0.1	window_mean_3x3	perlin	0.500270	1.076170	0.000016	-0.000032	906251a32a636296
0.01	1000	10000000.0	128	0.1	neighborhood3	opensimplex	0.500036	1.121121	0.000411	-0.000823	6f5d0740c3ea0fb01
0.01	1000	10000000.0	128	0.1	neighborhood3	perlin	0.500016	1.112573	-0.000358	0.000715	7705c6adc5b804bc
0.01	1000	10000000.0	128	0.1	window_mean_3x3	opensimplex	0.499581	1.115135	-0.000008	0.000015	8b8da750fe2c9113
0.01	1000	10000000.0	128	0.1	window_mean_3x3	perlin	0.499777	1.135279	-0.000204	0.000409	8944f4d6d7c5ee71
0.01	5000	100000.0	128	0.1	neighborhood3	opensimplex	0.500528	1.009965	-0.000076	0.000152	6e30cc395858c578
0.01	5000	100000.0	128	0.1	neighborhood3	perlin	0.499937	0.939493	0.000168	-0.000336	5e559163977b073f
0.01	5000	100000.0	128	0.1	window_mean_3x3	opensimplex	0.500325	0.905113	-0.000100	0.000200	a77608ec1121bd67
0.01	5000	100000.0	128	0.1	window_mean_3x3	perlin	0.500237	1.056376	0.000017	-0.000033	aacea544bd8f862cd
0.01	5000	10000000.0	128	0.1	neighborhood3	opensimplex	0.500049	1.112743	0.000403	-0.000806	0f107415bf46cf117
0.01	5000	10000000.0	128	0.1	neighborhood3	perlin	0.500032	1.115146	-0.000371	0.000742	5a8ae80949382632

dt	warmup	quant_k	size	scale	seed_strategy	memory_type	bit_ones_ratio	byte_chi2_norm	rms_norm	diffcorr_lag	lags_norm	keystream_sha256
0.01	5000	10000000.0	128	0.1	window_meanop3k3	simplex	0.499594	1.117199	-0.000012	0.000024	1ed6d7988da34544	
0.01	5000	10000000.0	128	0.1	window_meanpe3k3	simplex	0.499781	1.129103	-0.000190	0.000381	42acd5799babb391	

Best Candidates (heuristic score)

Top 5 overall:

dt	warmup	quant_k	size	scale	seed_strategy	memory_type	score	perf_score	rand_score	bit_ones_ratio	autocorr_lag	lags_norm	diff_chi2_norm
0.01	100	100000.0	128	0.1	neighborhood	opensimplex	0.992128	1.000000	0.986881	0.500501	0.000108	-0.000054	1.012630
0.01	100	100000.0	128	0.1	neighborhood	perlin	0.963975	0.978024	0.954609	0.499951	-0.000346	0.000173	0.953018
0.01	1000	100000.0	128	0.1	neighborhood	opensimplex	0.963248	0.928910	0.986140	0.500505	0.000120	-0.000060	1.013369
0.01	100	100000.0	128	0.1	window_mean	perlinBx3	0.942170	0.965727	0.926465	0.500280	-0.000052	0.000026	1.079013
0.01	5000	100000.0	128	0.1	neighborhood	opensimplex	0.935436	0.854500	0.989393	0.500528	0.000152	-0.000076	1.009965

Top 3 per seed_strategy:

seed_strategy	dt	warmup	quant_k	size	scale	memory_type	score	bit_ones_ratio	autocorr_lag	rms_norm	diff_chi2_norm
neighborhood	0.01	100	100000.0	128	0.1	opensimplex	0.992128	0.500501	0.000108	-0.000054	1.012630
neighborhood	0.01	100	100000.0	128	0.1	perlin	0.963975	0.499951	-0.000346	0.000173	0.953018
neighborhood	0.01	1000	100000.0	128	0.1	opensimplex	0.963248	0.500505	0.000120	-0.000060	1.013369
window_mean	0.01	100	100000.0	128	0.1	perlin	0.942170	0.500280	-0.000052	0.000026	1.079013
window_mean	0.01	100	100000.0	128	0.1	opensimplex	0.934302	0.500310	0.000188	-0.000094	0.899140
window_mean	0.01	1000	100000.0	128	0.1	perlin	0.907189	0.500270	-0.000032	0.000016	1.076170

Appendix

- CSV columns: benchmark includes timing/throughput; analyze includes keystream statistics.
- Reproducibility: same config → identical hashes/metrics.

Methodology Notes

- Benchmark results are averaged over `repeats` runs (as configured; BA1 kit uses repeats=3).
- Analyze metrics are deterministic per variant and computed once per variant (no repeats by default).
- Environment details for the run are stored in `out/ba1/run_meta.txt` (UTC date, python version, uname, pip freeze).
- Statistical metrics describe properties of the generated keystream for the tested length; they do not prove cryptographic security.