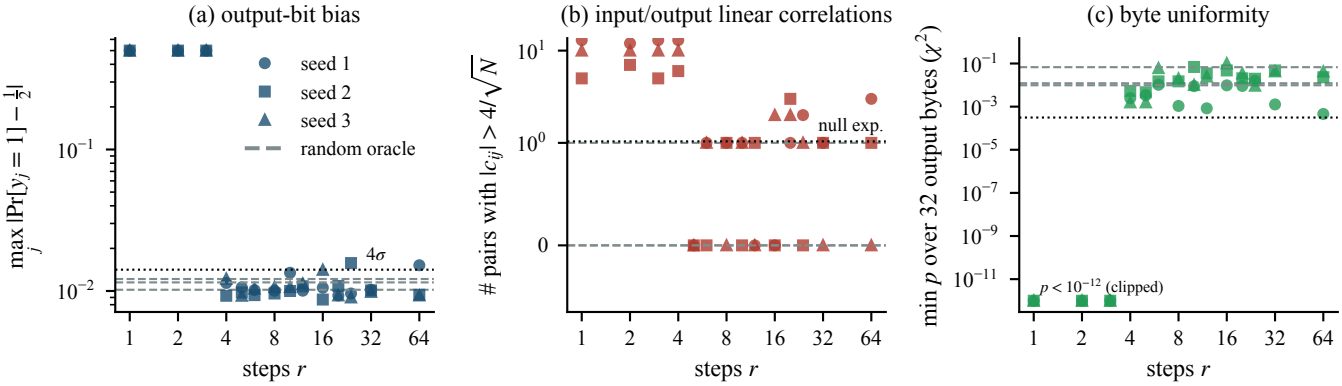

Statistical regularity of r-step SHA-256 (N = 20000 messages per seed, 3 seeds)
(a) output-bit bias
max_j |Pr[y_j = 1] − 1/2|
seed 1
seed 2
seed 3
random oracle
4σ
steps r
(b) input/output linear correlations
pairs with |c_ij| > 4/√N
null exp.
steps r
(c) byte uniformity
min p over 32 output bytes (χ²)
p < 10^−12 (clipped)
steps r