

// HARDWARE TRANSDUCTION DEVIATIONS

NON-IID BEHAVIOR

Let's have some example with actual data, this what always helps me understand things better : D

The idea is that the random bitstream we are analyzing is dependant on the time of day, due to environmental characteristics affecting the readings from the random number generator.

This will help illustrate some of the steps that we need to go through and also, learn what are the mathematics involved in the process.

My goal is not to become a mathematician but to understand a bit better the underlying fundamentals that make our systems secure or in-secure.

The goal is to use random source to generate a good encryption key.

// EMPIRICAL STATISTICAL METRICS

SAMPLE SIZE (N)

1,000,000 [64 Discrete Bins]

AUTOCORRELATION (TEMPORAL MEMORY)

Lag-1 (ρ_1): **+0.6012**

Lag-2 (ρ_2): **+0.4185**

SAMPLE VARIANCE (σ^2 OVER-DISPERSION)

68.42 vs. 42.50 Baseline

Significant over-dispersion relative to ideal Poisson model.

POWER SPECTRAL DENSITY (PSD)

24-Hour Diurnal Peak [Environmental Modulation]

WRONG INDEPENDANT ASSUMPTION

Underestimating non-IID characteristics leads to in-secure results. Assuming IID behavior ignores temporal persistence and invalidates real-world potential attacks.

STEP 01 - PEAK PROBABILITY

$P_{\max} = 0.0800$

Measured peak probability across 64 discrete bins under the initial observation model.

STEP 02 - UNCONDITIONAL MIN-ENTROPY

3.6438 bits / sample

Calculated via NIST SP 800-90B Most Common Value estimator:
 $H_{\text{IID}} = -\log_2(0.08)$.

STEP 03 - TOTAL CLAIMED ENTROPY

258.71 total bits

To get 256 bits of entropy we would need 71 samples at the current 3.6 bits/sample

STEP 04 - INCORRECT ASSUMPTIONS

2^{256} operations

Falsely concludes an impossible brute-force search, completely ignoring temporal persistence.

IMPORTANT: INDEPENDENT IDENTICALLY DISTRIBUTED (IID) ASSUMPTION OVERESTIMATES SECURITY BY IGNORING DATA CORRELATION.

MARKOV CHAIN MODELING & ENTROPY LOSS

An attacker checks for system data correlation by modeling the bitstream as a first-order Markov chain.

CONDITIONAL PEAK PROBABILITY $P(C_t | C_{t-1})$

0.4000

TRUE CONDITIONAL MIN-ENTROPY (H_{∞})

1.3219 bits/sample

TOTAL MIN-ENTROPY (71 SAMPLES)

93.85 bits

[-164.9 BITS ENTROPY OVERESTIMATION]

HERE IS THE REAL PROBLEM

SEARCH SPACE COLLAPSE

$2^{256} \rightarrow 2^{93.8}$

The attack only needs **$2^{93.8}$ operations** to bruteforce the key space, drastically reducing from the assumed 2^{256} search space.