Overview of NISTIR 8427

Darryl Buller, Aaron Kaufer

(National Security Agency, Cybersecurity Directorate)

Allen Roginsky, Meltem Sönmez Turan

(National Institute of Standards and Technology)

Background

- The SP 800-90 series requires full entropy for certain bit strings in RBG constructions
- SP 800-90C gives a definition of full entropy in terms of a numerical threshold
- NISTIR 8427 provides a practical operational way to produce bit strings meeting this threshold

What is full entropy?

- SP 800-90C: A bit string has full entropy if the entropy per bit is at least $1 - \varepsilon$, where $\varepsilon \leq 2^{-32}$
- Consider N bits from an IID stream with $p = \frac{1}{2}$
- Number of 1's is $\frac{N}{2} + \frac{z}{2}\sqrt{N}$ where z (# of standard deviations) is small
- To obtain a min-entropy estimate near $1 - 2^{-32}$ based on this sample, N must be on the order of 2^{64}
- Difficult to ensure that the threshold is satisfied with the required precision!

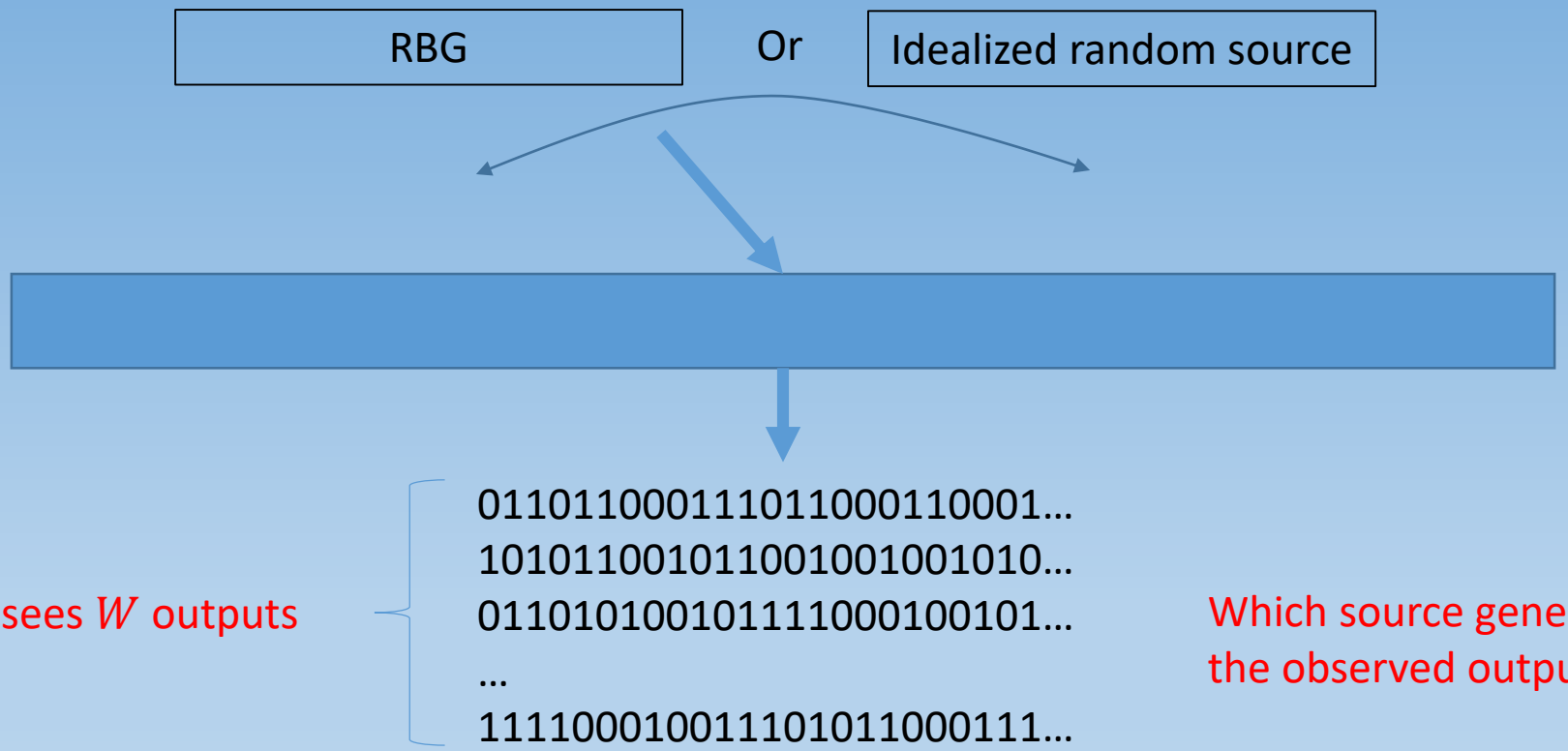
Problem statement

- It is infeasible to ensure compliance with the SP 800-90C definition by analyzing an RBG design or sample data
- Derive an alternative definition of full entropy
  - Compatible with SP 800-90C definition
  - Enable feasible verification of compliance

Alternative definition

- Define full entropy in terms of a distinguishing game
- Consider two sources of random bits:
  - REAL: the RBG (or RBG component of interest)
  - IDEAL: an idealized random source
- Randomly choose one of these sources
- Generate a quantity of n-bit outputs from the selected source
- If an adversary with unlimited computing power cannot reliably determine which source was used, the RBG outputs are defined to have full entropy

Distinguishing game

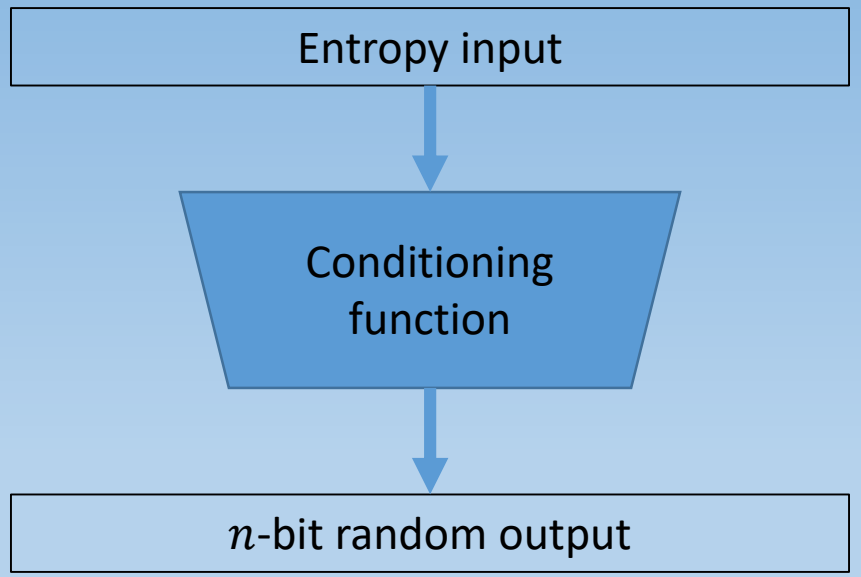


Distinguishing game, cont.

- Given parameters W and $\delta > 0$:
- If adversary cannot correctly guess which source produced W observed outputs with probability greater than $\frac{1}{2} + \delta$, the RBG output is said to have full entropy with respect to W and δ

Applying the definition

- Consider a vetted conditioning function that takes entropy inputs and produces n-bit outputs



Claims made

- NISTIR 8427 proves the following claims:
  - Claim 1: Output from a vetted conditioning function with sufficient input entropy satisfies the full entropy definition
  - Claim 2: Outputs that satisfy the definition of full entropy also satisfy the full entropy threshold in SP 800-90C

Assumptions

- Derivations and proofs required the following assumptions
  - Test statistic for likelihood ratio test used to distinguish between REAL and IDEAL is normally distributed (based on Central Limit Theorem)
  - Conditioning function output probabilities can be treated as random variables (the function's cryptographic properties make this reasonable)
  - Conditioning function output probabilities are normally distributed (based on second assumption and Central Limit Theorem)

Claim 1

- Let H be the min-entropy of the input entropy string
- Suppose $H \geq n + \log_2\left(\frac{W}{\delta^2}\right) - \log_2 \pi - 3$
- Then the conditioning function output satisfies the full-entropy definition wrt W and δ
- Selecting $W = 2^{48}$ and $\delta = 2^{-10}$ leads to the following
- If $H \geq n + 64$, the conditioning function output has full entropy
- This is the threshold for full entropy used in SP 800-90C

Summary of proof

- Probability distribution on n-bit outputs from conditioning function depends on input probability distribution and function details
- Define test statistic X used for likelihood ratio test: $X = \frac{Pr[B|REAL]}{Pr[B|IDEAL]}$ (where B is the set of observed outputs)
- Derive probability distribution for X in both REAL and IDEAL cases
- Compute probability of correct guess by adversary
- Find necessary condition on input entropy H

Claim 2

- Let H be the min-entropy of the input entropy string
- Suppose $H \geq n + 64$
- Then the conditioning function output has min-entropy at least $1 - 2^{-32}$ per bit
- That is, the conditioning function output satisfies the min-entropy threshold specified in SP 800-90C

Summary of proof

- Estimate largest output probability using normal distribution assumption
- Compute min-entropy based on largest output probability
- Min-entropy of outputs is at least approximately $n - \frac{2^{\frac{n-H}{2}}\sqrt{n}}{\ln 2}$
- For $H \geq n + 64$, min-entropy per bit is at least $1 - 2^{-32}$

Summary

- Presented alternative definition of full entropy
- Derived a testable condition for satisfying this definition
- Showed that satisfying this condition results in meeting the min-entropy threshold in SP 800-90C