Public Comments on NIST IR 8427 (Initial Public Draft) Discussion of the Full Entropy Assumption of the SP 800-90 Series

Comment period: September 7 – October 31, 2022

LIST OF COMMENTS

1. Comments from Dan Brown, BlackBerry, October 31, 2022

Re: NIST IR 8427 Initial Public Draft, Discussion of the Full Entropy Assumption of the SP 800-90 Series

Dear NIST,

BlackBerry commends NIST's efforts towards the security arguments for the generation of high-quality random bits for cryptographic and non-cryptographic use in NISTIR 8427. BlackBerry suggests that the security arguments, currently presented as an informal discussion, could be improved by being presented as a formal mathematical proof, with clearly identified conclusions, and assumptions necessary for these conclusions.

Various assumptions arising during the middle of the NISTIR 8427 discussion might be possible to replace with mathematically rigorous results. A "reasonable" enough assumption should be provable. A few assumptions might be too difficult to prove. The unproven assumptions should be listed up front before the arguments. A theorem statement lists all hypotheses used in its proof. Listing hypotheses helps to measure the strength of the theorem, helps to challenge its correctness, and helps to organize verification of the proof.

For example, NISTIR 8427 assumes a random variable pj is approximated by a normal distribution (citing the Central Limit Theorem). In the case of a uniform distribution on the inputs to the conditioning function, the random variable pj will have a binomial distribution. The Chernoff bound is a mathematically rigorous bound the binomial distribution. For some parameters of the binomial distribution, and large deviations from the mean, the normal approximation is too small, but the larger Chernoff bounds might still be small enough for security. If so, this assumption could be replaced by a mathematically rigorous result.

Respectfully submitted,

Dan Brown

Senior Standards Manager

2. Comments from Marek Leśniewicz, Military Communications Institute, Poland, September 21, 2022

Dear Sirs,

I've read with interest NIST IR 8427 and NIST SP800-90C.

I believe that the study of entropy in the sense of comparing the IDEAL entropy and the REAL entropy is the only correct way in the process of assessing the randomness of binary sequences (Kolmogorov: "*information theory must precede probability theory and not be based on it*").

However, IDEAL entropy and REAL entropy have different meanings and properties that need to be analyzed and interpreted differently.

The one concerns theoretical analyzes in terms of Shannon entropy and is based on probability theory and information theory.

In this case, entropy

$$\mathrm{H}(X) = -\sum_{i=1}^{2} \mathrm{P}(X) \log_2 \mathrm{P}(X) = 1 \ ,$$

if we can prove that for a given sequence of random variables the probabilities P (X) = P (1) = P (0) = 1/2. It should always be remembered that in probability theory, probability is a measure of predictability, not the ratio of the number of a given event to the total number of events (Kolmogorov vs. Laplace / Buffon / von Mises).

The second one concerns practical measurements of random sequence statistics and is based precisely on mathematical statistics. In this case, we are talking about the ratio of the number of a given event n_i to the total number of events *n*, measured for a given sample.

But in this case, even if the tested sample is the realization of a sequence of random variables with a proven probability P (*X*) = P (1) = P (0) = 1/2, then for any sample

$$\mathrm{H_E}(X) \mid n) = -\sum_{i=1}^{2} (n_i / n) \log_2 (n_i / n) = 1 - \frac{2^N - 1}{2 \ln 2\, n} < 1$$

thus the entropy of the attempt HE(*X*) | *n*) goes to 1 with $n \to \infty$.

It is easy to check.

If we have a sample of any random sequence (also pseudo-random – DES, AES, *sponge*, SHA-3 etc.) with a size of 1 GB = 1000 MB (1 MB = 8 x 1 048 576 bits), then using the above dependence in each case we get:

HE(*X*) | *n* = 1 MB) = 1 – 8.6 · 10_{-8},
HE(*X*) | *n* = 10 MB) = 1 – 8.6 · 10_{-9},
HE(*X*) | *n* = 100 MB) = 1 – 8.6 · 10_{-10},
HE(*X*) | *n* = 1 GB) = 1 – 8.6 · 10_{-11}, and for any other size *n*, respectively.

It follows that the values of H(*X*) and HE(*X*) | *n*), even for a perfectly random sequence, are never equal, i.e.

H(*X*) > HE(*X*) | *n*) ,

and if the sequence is not perfectly random, then

H(*X*) > HE(*X*) | *n*) – e(*X*),
where e(*X*) is a measure of the non-randomness of the sequence resulting from generator construction errors and other errors.
If this property is not included in the measurements of the string sample statistics, the comparison results of the IDEAL entropy and the REAL entropy in each case will be inconsistent.

I have described these issues in detail in my book:

Marek Leśniewicz, *Hardware generation of binary random sequences*, WAT, 2009, ISBN 978-83-61486-31-2,

unfortunately, only available in Polish (attached).

I've provided extensive summaries of the most important results of this work in two articles in English (attached):

Marek Leśniewicz, *Expected Entropy as a Measure and Criterion of Randomness of Binary Sequences* In Przeglad Elektrotechniczny, Volume 90, 1/2014, pp. 42– 46.

Marek Leśniewicz, *Analyses and Measurements of Hardware Generated Random Binary Sequences Modeled as Markov Chains* In Przeglad Elektrotechniczny, Volume 92, 11/2016, pp. 268-274.

and on the practical generation of random sequences in two others:

Mariusz Borowski, Marek Leśniewicz, *Modern usage of the "old" one-time pad*, In Communications and Information Systems Conference (MCC), 2012.

Mariusz Borowski, Marek Leśniewicz, Robert Wicik, Marcin Grzonkowski, *Generation of random keys for cryptographic systems*, Annales UMCS Informatica AI XII, 3 (2012) 75–87.

All the theoretical results presented in these papers have been repeatedly checked with measurements and they seem to be correct.

Since then, I’ve found several new mathematical relationships that theoretically justify some of the results obtained by the measurements. They concern entropy studies with the use of the $\chi2$ test. I expect these papers to be published soon.

I’m eager to join the further discussion on this topic.

Best regards, Marek Leśniewicz