Summary of Changes – NIST SP 800 90B

Comment period: January 25, 2016 through May 9, 2016

This document summarizes the (non-editorial) changes made after the comment period of the Second Draft of NIST SP 800 90B.

Section	Change
Page iv	"Note to Reviewers" that includes questions to the reviewers is removed.
1.1 Introduction	The purpose and the intended users of the document are added.
1.2 Symbols 1.3 Organization	Organization section is moved before the Symbols section.
1.2 Symbols	Some missing symbols and functions are added to the list.
2.1 Min-entropy	Typo in the mathematical formula of to calculate min-entropy definition is corrected.
Figure 1	"Noise source" is changed to "Analog Noise Source". Post-processing is removed. Digital noise source boundary is added.
2.2.1 Noise Source	The concept of post-processing of the noise source is removed. Definitions for physical and non-physical noise sources are added. The discussion on multiple noise sources is removed from this section.
3.1.1 Data Collection	The parts related to multiple noise sources are moved to Section 3.1.6.
3.1.3 Initial Entropy Estimate	Some editorial changes are done.
3.1.4 Restart Tests	More discussion on restart tests is added.
3.1.4.3 Sanity Check - Most Common Value in the Rows and Columns	Discussion on the sanity check is added. α is set to 0.000 005. The description of the test is modified.
3.1.5 Entropy Estimation for Entropy Sources Using a Conditioning Component	The notation for narrowest internal width is changed to *nw* from *q*, since *q* was used to define a few other mathematical values. A new requirement on the input sizes for the conditioning component is added, this is needed for new entropy calculated given in Section 3.1.5.1.2.
3.1.5.1.1 List of Vetted Conditioning Components	The requirements on the keys used in conditioning component is moved to Section 3.2.3.
3.1.5.1.2 Entropy Assessment using Vetted Conditioning Components	The entropy assessment method for the vetted conditioning components is updated, mainly due to the objections to the 0.85 constant.
3.1.5.2 Using Non-vetted Conditioning Components	The entropy assessment method for the non-vetted conditioning components is updated, mainly due to the objections to the 0.85 constant. Instead a constant of 0.999 is used to make sure that non-vetted conditioning components cannot generate full-entropy outputs.
Figure 3	The size of the input is added to the figure.
3.1.6 Using Multiple Noise Sources	Section is renamed to "Additional Noise Sources".

	Final version assumes that the entropy sources have a unique primary noise sources. Final version allows concatenation of outputs of additional noise sources, only when the conditioning components is used. No entropy is credited to the outputs of additional noise sources.
3.2.1 Requirements on the Entropy Source	The requirements on the range of operating conditions are slightly relaxed. Requirement 5 and 6 are merged. Requirement 8 and 9 on the multiple noise sources are removed.
3.2.2 Requirements on the Noise Source	The requirement on the ordered ranking of the bits is removed. The requirements on the post-processing functions is removed. As a new requirement, the noise sources are expected to be stationary. If additional noise source outputs are used, a new requirement on documentation is added.
3.2.3 Requirements on the Conditioning Component	The requirements on the keys used in conditioning component are added.
3.2.4 Requirements on Data Collection	On Requirement 2, raw data can no longer be post-processed, as the concept has been removed. The documentation explaining why the data collection method does not interfere with the noise source is now required.
4 Health Tests	Two footnotes are added.
4.2 Types of Health Tests	A footnote is added.
4.3 Requirements for Health Tests	The requirements are rewritten for clarity. The bound on the false positive probability of 2^{-50} is removed, recommended upper and lower limits are provided. The requirement on the number of consecutive samples is reduced from 4096 to 1024.
4.4 Approved Continuous Health Tests	The requirement on the false positive probability is removed.
4.4.1 Repetition Count Test	The formula for the cutoff value is slightly updated. The pseudocode of the Repetition count test is updated for clarity.
4.4.2 Adaptive Proportion Test	The pseudocode of the Adaptive Proportion test is updated. The discussion about the probability of detecting a loss of 50% of the entropy is removed.
Section 4.5 and 4.6	Sections are merged, and renamed as “Developer defined Alternatives to the Continuous Health Tests”. The terms vendor and designer are replaced by developer.
Figure 4	The pseudocode is updated for clarity.
Figure 5	The pseudocode is updated for clarity.
5.1.7 Average Collision Test Statistic	The typo in Step 3c is corrected. “i=i+j+1” is changed to “i=i+j”.
5.1.8 Maximum Collision Test Statistic	The typo in Step 3c is corrected. “i=i+j+1” is changed to “i=i+j”.
5.2.1 Testing Independence for Non-Binary Data	The test description and the example are updated.
5.2.2 Testing Goodness-of-fit for Non-Binary Data	The notation for the number of bins is changed from q to n_{bin}.

5.2.3 Testing Independence for Binary Data	The expected value calculated is updated. The degree of freedom is changed from 2^m-1 to 2^m-2.
5.2.4. Testing Goodness-of-fit for Binary Data	The expected value calculations are updated.
5.2.5 Length of the Longest Repeated Substring Test	Typo in the probability of success (Step 5) is corrected.
6 Estimating Min-Entropy	A note that says "…entropy estimation methods described in this section rely on some statistical assumptions that may not hold for all types of noise sources. The methods should not replace in-depth analysis of noise sources, but should be used to support the initial entropy estimate of the submitter …" is added.
6.1 IID Track: Entropy Estimation for IID Data	Footnote is added.
6.2 Non-IID Track: Entropy Estimation for Non-IID Data	The quality of the collision, Markov and compression estimates entropy estimates vary a lot on the size of the sample. We decided to apply these tests only to binary inputs.
6.3.1 Most Common Value Estimate	The typos in the example is corrected.
6.3.2 Collision Estimate	The collision estimate description is updated to reflect that it is only applied to binary inputs. The input in the example is changed to a binary input. Lower bound of 1/k is included for the binary search.
6.3.3 Markov Estimate	The Markov estimate description is updated to reflect that it is only applied to binary inputs. The input in the example is changed to a binary input.
6.3.4 Compression Estimate	The details of the compression estimate and the example are updated. Lower bound of 1/k is included for the binary search.
6.3.5 t-Tuple Estimate	The details of the t-tuple estimate and the example are updated. In Step 7, n is replaced by 2^b. To be consistent with other methods, 99% confidence interval to the estimate is added.
6.3.6 Longest Repeated Substring (LRS) Estimate	The details of the LRS estimate are updated. The threshold value in Step 1 is changed from 20 to 35. To be consistent with other methods, 99% confidence interval to the estimate is included.
6.3.7 Multi Most Common in Window Prediction Estimate	Calculation of P'_{global} is updated. A note regarding calculation of p_{local} values is included. The min-entropy calculation is updated. In the example, the typos in p_{local} and min entropy calculation are corrected. In predictor estimates, $\max(P'_{global}, P_{local})$ is replaced with $\max(P'_{global}, P_{local}, \frac{1}{k})$. This is done to guarantee that min-entropy estimate is not greater than $\log_2 k$.
6.3.8 The Lag Prediction Estimate	Calculation of P'_{global} is updated. A note regarding calculation of p_{local} values is included. The min-entropy calculation is updated.

	In the example, the typos in p_{local} and min entropy calculation are corrected. In predictor estimates, $\max(P'_{global}, P_{local})$ is replaced with $\max(P'_{global}, P_{local}, \frac{1}{k})$. This is done to guarantee that min-entropy estimate is not greater than $\log_2 k$.
6.3.9 The MultiMMC Prediction Estimate	The pseudocode of MultiMMC prediction estimate and the min-entropy calculation are updated. In the example, the typo in the p_{local} calculation are corrected. Test description is updated to include a limit on the number of observed previous states to make it feasible to compute across large files.
6.3.10 The LZ78Y Prediction Estimate	The P_{global} calculation is updated. A note regarding calculation of p_{local} values is included. In the example, the typo in the p_{local} calculation are corrected.
6.4 Reducing the Symbol Space	Section title is changed to Reducing the Symbol Space. The requirement to use the algorithm provided in Section 6.4 to reduce symbol size is removed. The submitters are allowed to use alternative methods to reduce symbol size.
Appendix A Acronyms	The acronyms API, CBC-MAC and RAM are added to the list.
Appendix B Glossary	The definitions of *Alphabet size, biased, binary data, bitstring, confidence interval, global performance metric, local performance metric, non-physical non-deterministic random bit generator, physical non-deterministic random bit generator, stochastic model, symbol* are updated.
Appendix C References	The references [CoNa98], [HaFis15], [RaSt98] are added.
Appendix E Post-processing functions	The section is removed.
Appendix G.1.1 Approximation of F(1/z)	The formula for F(1/z) is updated, for consistency *n* is replaced by *k.*
Appendix G.2 Predictors	Detailed explanations of predictors and a table of precomputed p_{local} values are included.