On NIST's Standards on Random Numbers

Meltem Sönmez Turan
National Institute of Standards and Technology
meltem.turan@nist.gov

Special session:

National Institute of Standards and Technology (NIST) has published a number of guidelines and recommendations to provide guidelines and recommendations for generating random numbers for cryptographic applications. Namely, the NIST Special Publication (SP) 800-90 series have three parts: Part A [1] specifies mechanisms for the generation of random bits using deterministic methods; Part B [2] outlines the design principles and requirements for the entropy sources used by random bit generators; and Part C [3] specifies constructions for the implementation of random bit generators integrating deterministic mechanisms from Part A and utilizing entropy sources as specified in Part B. Additionally, NIST SP 800-22 [4] offers a suite of statistical tests to assess the randomness properties of binary sequences. This presentation offers an overview of these standards, highlighting their strengths, limitations, and NIST's strategies for their future revision.

[1] Barker EB, Kelsey JM (2015). *SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators* (National Institute of1385 Standards and Technology), https://doi.org/10.6028/NIST.SP.800-90Ar11386

[2] Sönmez Turan M, Barker EB, Kelsey JM, McKay KA, Baish ML, Boyle M (2018). *SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation* (National Institute of Standards and Technology), https://doi.org//10.6028/NIST.1389SP.800-90B1390

[3] Barker EB, Kelsey JM, McKay KA, Roginsky A, Sönmez Turan M (2022). *SP 800-90C Recommendation for Random Bit Generator (RBG) Constructions (3rd Draft)* (National Institute of Standards and Technology), https://doi.org//10.6028/NIST.SP.800-913930C.3pd

[4] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert N, Dray J, Vo S, and Bassham L. *SP 800-22 Rev.1a A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* Technical report, National Institute of Standards and Technology, 2010. https://csrc.nist.gov/pubs/sp/800/22/r1/upd1/final