1163-94-385 **Thor Martinsen** and **Vikram Kanth*** (vkkanth@nps.edu), Naval Postgraduate School, Monterey, CA. *The Self-Shrinking Conflation Generator: A New Pseudorandom Bit Generator.* Preliminary report.

The backbone of many cyber security applications and algorithms requires random numbers. Due to the fact that true randomness is hard to capture and use, pseudo-random number generators (PRNG) are used to approximate it. One of the most commonly used pseudo-random generators is the Linear Feedback Shift Register (LFSR), which is fast, computationally inexpensive, and has excellent statistical properties. LFSRs have many weaknesses, some of which were addressed by decimation-based sequence generators like the self-shrinking generator (SSG). The SSG is also vulnerable to attack. We propose an improvement to the SSG called the self-shrinking conflation generator (SSCG). Our approach uses the observation that what is discarded during the self-shrinking process is from a cryptographic perspective, just as good as what is kept. By combining the normally discarded bits with those that are retained, we create a modified bitstream with improved characteristics. We provide some mathematical security analysis associated with this approach, apply the NIST statistical test suite to several different bitstreams created using LFSRs, and compare our results to that of the SSG. (Received September 04, 2020)