

True Random Number Generation from Very Low Frequency Radio Noise

Thursday 18 September 2025 12:25 (15 minutes)

Radio noise use in True Random Number Generation is a popular and well understood strategy, but relatively undermined in research. Given that Very Low Frequency radio streams record chaotic weather events from around the world (like thunderstorms), this novel entropy source sparked our interest. Our choice is supported by prior research in statistical modeling, along with an appropriate combination of both signal and statistical methods. Hence, we describe in detail our processing pipeline for engineering a TRNG from VLF radio noise. It yields high entropy, unbiased and identically distributed outputs that pass FIPS 140-2 tests, regardless of the chosen VLF stream source. To strengthen reproducibility, we have based all of our experiments on publicly available data. We also provide an open-source, modular command-line tool for building stream-based processing pipelines. Furthermore, we offer an example implementing a TRNG from FM radio noise found between standard transmission bands.

Author: BARBU, Matei (University Politehnica of Bucharest)

Co-authors: TRANCĂ, Dumitru-Cristian (University Politehnica of Bucharest); STANCU, Florin-Alexandru (POLITEHNICA University of Bucharest)

Presenter: BARBU, Matei (University Politehnica of Bucharest)

Session Classification: Networking in Education and Research

Track Classification: Network Security