Deterministic Random Bit Generators NIST techniques comparison

Tomas Bedoya
Daniel Andres Jaimes Cardenas
Eder Leandro Carbonero Baquero
Universidad de los Andes, Colombia

***Abstract*—Aquí va el resumen del artículo, una breve descripción del problema, la metodología y los resultados.**

I. Introduction

II. General defintions

With the aim of providing a broader understanding of the various concepts addressed in this document, the following are definitions of some of the acronyms that will be mentioned throughout the text.

Acronym	Meaning
CTR_DRBG	Counter mode Deterministic Random Bit Generator
NIST	National Institute of Standards and Technology
AES	Advanced Encryption Standard
RBG	Random Bit Generator
DRBG	Deterministic Random Bit Generator
PRNG	Pseudorandom Number Generator

Table I
Acronyms definitions.

III. methodologies

IV. Deep Learning Methods

Deep learning is a subset of machine learning that uses artificial neural networks with many layers to automatically learn complex patterns from large amounts of data.

V. techniques

VI. CTR_DRBG Counter mode Deterministic Random Bit Generator

CTR_DRBG (Counter mode Deterministic Random Bit Generator) is a standardized method for constructing a deterministic random bit generator (PRNG) using a block cipher operating in counter (CTR) mode. This technique is defined in NIST Special Publication 800-90A, titled *"Recommendation for Random Number Generation Using Deterministic Random Bit Generators"*. Essentially, CTR_DRBG transforms a secure symmetric cipher—such as AES—into a cryptographically strong source of pseudorandom bits. The counter mode ensures that each generated block is unique by systematically incrementing a counter value for each new data request, thus preventing the repetition of output sequences under the same key and seed. This approach is widely used in cryptographic applications requiring high security and reliability in random data generation, such as key generation, initialization vectors, and session tokens.

VII. Results

VIII. Conclusions

References