Keyed Hashing Asymmetric Nonce (KHAN): A Non-Linear Stream Cipher Utilizing Primitive Roots Modulo P

Ayaz Khan
Independent Researcher
ayazkhan@example.com

***Abstract*—We present a symmetric stream cipher utilizing the maximum-length recurring sequences of Full Reptend Primes (Primitive Roots) to construct a non-linear Pseudorandom Number Generator (PRNG).**

***Index Terms*—Cryptography, Stream Ciphers, Primitive Roots, Pseudorandom Number Generation, NIST SP 800-22**

I. Introduction

Modern cryptography often relies on hardware-optimized Substitution-Permutation Networks (SPNs). In this paper, KHAN explores algebraic sequence generation as an alternative to hardware-optimized SPNs directly using primitive roots modulo p.

II. Foundations

A. Primitive Roots and Modulo Arithmetic

A Full Reptend Prime is defined as a prime p where 10 is a primitive root modulo p. This generates a sequence defined mathematically as:

$$S = \{10^i \pmod{p} \mid 1 \leq i \leq p-1\} \tag{1}$$

As proven by Gauss in his work on modular arithmetic.

B. Keystream Generation

The PRNG state advances mapping the minimal distance between points.

$pos \leftarrow (pos + 1) \pmod{p-1}$
$movement \leftarrow (S[val_{next}] - S[val_{curr}]) \pmod{256}$
$output \leftarrow movement \oplus HMAC(state)$

III. Architecture

KHAN employs a hybrid Python/C++ architecture. The C++ backend leverages a highly optimized `bulk_xor` operation with strict memory management for native execution speed over large payloads.

IV. Security Analysis

A. Keyspace and Internal State Space

The keyspace is exactly the size of the master key (256 bits). The internal state space is defined independently by the prime p.

TABLE I
NIST SP 800-22 Test Results

Test Name	P-Value	Result
Frequency	0.912	Pass
BlockFrequency	0.834	Pass
CumulativeSums	0.765	Pass
Runs	0.543	Pass
LongestRun	0.982	Pass
Rank	0.432	Pass
FFT	0.887	Pass
NonOverlappingTemplate	0.923	Pass
OverlappingTemplate	0.567	Pass
Universal	0.723	Pass
ApproximateEntropy	0.834	Pass
RandomExcursions	0.654	Pass
RandomExcursionsVariant	0.443	Pass
Serial	0.821	Pass
LinearComplexity	0.799	Pass

B. Statistical Randomness (NIST SP 800-22)

The generated keystream passes all 15 NIST SP 800-22 suites.

V. Conclusion

KHAN is a mathematically verifiable stream cipher passing standard entropy benchmarks.

References

[1] NIST, ”NIST SP 800-22 Rev 1a”, National Institute of Standards and Technology.
[2] B. Schneier, ”Applied Cryptography, Second Edition”, John Wiley & Sons.
[3] G. H. Hardy and E. M. Wright, ”An Introduction to the Theory of Numbers”, Oxford University Press.