BAŞLIK: Chaos-Shuffle RNG Algoritmasının Çalışma Prensibi ve Mimari Tasarımı

1. Genel Amaç

Chaos-Shuffle RNG (Random Number Generator), klasik doğrusal sözde rastgele sayı üreteçlerinin (LCG gibi) periyodik sınırlamalarını aşmak ve Collatz tabanlı sistemlerin deterministik zayıflıklarını gidermek amacıyla tasarlanmıştır. Algoritma, Deterministik Kaos Teorisi'nin temel taşı olan "Lojistik Haritalama" (Logistic Map) fonksiyonunu, modern kriptografinin Karıştırma (Confusion) ve Yayılma (Diffusion) prensipleriyle birleştiren hibrit bir yapıdır.

Temel hedefler şunlardır:

- Kayan noktalı sayıların (floating point) kaotik davranışını dijital bit üretimine dönüştürmek.
- Sabit S-Box tabloları yerine dinamik maskeleme kullanarak yan kanal saldırılarını zorlaştırmak.
- Bit rotasyonları ile tohum (seed) üzerindeki 1 bitlik değişimin tüm çıktıya yayılmasını (Avalanche Effect) sağlamak.

2. İç Durum (State) Yapısı

Algoritma güvenliği sağlamak için iki katmanlı bir bellek yapısı kullanır:

- **Dijital Durum (S):** 64-bitlik işaretsiz tam sayı (unsigned integer). Tüm bit manipülasyonları bu değişken üzerinde yapılır ($S \in [0, 2^{64}-1]$).
- **Kaotik Çekirdek (x):** $[0, 1]$ aralığında tanımlı, çift hassasiyetli (double precision) bir reel sayı. Sistemin "öngörülemezlik" kaynağıdır.

3. Algoritmanın Ana Adımları

Her bir bitin üretimi, birbirini takip eden 5 kritik aşamadan oluşur:

3.1. Kaotik Evrim (The Chaos Step)

Sistem, matematiksel olarak kaosun en yoğun olduğu bölgede çalıştırılır. Lojistik harita denklemi:

$$x_{n+1} = \mu \cdot x_n \cdot (1 - x_n)$$
Burada $\mu = 3.99995$ olarak seçilmiştir. Bu değer, sistemin periyodik bir döngüye girmesini matematiksel olarak imkansız kılar (Lyapunov üssü pozitiftir). Berat'ın algoritmasındaki "Maskeli Collatz" yapısının aksine, bu yöntem kaos teorisine dayanır.

3.2. Dinamik Maskeleme (Dynamic Masking)

Sabit bir tablo kullanmak yerine, her adımda kaotik x değerinden anlık bir maske üretilir:

$$Maske = (x \cdot 10^{12}) \pmod{256}$$
Bu işlem, kaotik sayının virgülden sonraki, tahmin edilmesi en zor basamaklarını alır. Böylece maske her döngüde rastgele değişir.

3.3. Doğrusal Olmayan Karıştırma (XOR Mixing)

Üretilen dinamik maske, 64-bitlik durum (S) değişkeninin üst bitleriyle XOR işlemine tabi tutulur. Bu adım, sistemin lineerliğini bozar (Non-linearity).

3.4. Difüzyon ve Rotasyon (Rotation)

Sistemin en kritik adımıdır. Durum değişkeni 19 bit sola dairesel olarak kaydırılır (Circular Shift):

$$S = (S \ll 19) \lor (S \gg 45)$$
Neden 19? 19 bir asal sayıdır ve 64 ile aralarında asaldır. Bu seçim, bitlerin her döngüde farklı pozisyonlara taşınmasını garanti eder ve çakışmaları önler.

3.5. Döngü Kırıcı (Chaos Injection)

Eğer dijital durum (S) değeri çok küçülürse veya sıfıra yaklaşırsa (ki bu LCG'lerde kilitlenmeye yol açar), kaotik x değişkeninden alınan büyük bir sayı sisteme enjekte edilerek döngü kırılır.

4. Neden Bu Yapı Seçildi?

Algoritma tasarlanırken, literatürdeki mevcut yöntemlerin zayıflıkları analiz edilmiş ve şu çözümler üretilmiştir:

Klasik Problem	**Chaos-Shuffle Çözümü**
Sabit Döngüler (4-2-1)	Kaotik rejim ($\mu \approx 4.0$) asla kendini tekrar etmez.
Sabit Tablo (S-Box) Saldırısı	Dinamik olarak üretilen, her adımda değişen maskeler.
Düşük Difüzyon	19-bitlik asal rotasyon ile maksimum bit saçılımı.
Tohum Tahmini	Kayan nokta hassasiyeti (Chaos Sensitivity).

5. Tasarımın Sınırları

- **Donanım Bağımlılığı:** Kayan nokta aritmetiği (Floating Point Unit - FPU) gerektirir. Farklı işlemci mimarilerinde (örn. ARM vs x86) virgülden sonraki 15. basamakta mikroskobik farklar oluşabilir.

- **Kriptografik Sertifikasyon:** Henüz NIST SP 800-22 test bataryasının tamamından geçmemiştir; şu an için "Deneysel" statüdedir.
- **Hız:** Tam sayı aritmetiğine göre daha yavaş olan double çarpma işlemleri içerir.

6. Sonuç

Chaos-Shuffle RNG; deterministik kaosun matematiksel gücünü, modern bit manipülasyon teknikleriyle birleştiren hibrit bir tasarımdır. Berat'ın Box-Box algoritmasına kıyasla daha geniş bir durum uzayına (State Space) sahiptir ve periyodik tekrarlara karşı matematiksel garanti sunar. Yapılan testler, algoritmanın eğitim ve simülasyon amaçlı kullanımlarda yüksek entropi sağladığını göstermektedir.