KAOTİK SİSTEMLERDEN RASTGELE SAYI ÜRETİMİ
Sıcaklık Farkından Kaynaklanan Kaldırma Kuvvetiyle Yönlendirilen Sıvı Akışı

ENTROPİ LAMBASI SİSTEMİ

Kaldırma Kuvvetiyle Yönlendirilen Sıvı Akışıyla Kriptografik Rastgele Sayı Üretimi

Patent Başvuru Tarihi · Numarası: 16.10.2026 · 2026/018051

Entropi Lambası Sistemi ODTÜ İVMER'de üretilen kriptografik güvenlikli rastgele sayı üretecidir. Öngörülemezlik, lambaların içerisinde bulunan çok renkli entropi parçalarının sıvı içerisindeki kaotik davranışından elde edilmektedir. Kaotik hareketin dayandığı fiziksel olay şişe tabanı ve tavanı arasındaki sıcaklık farkından kaynaklanan sıvı yoğunluğu değişimidir.

Entropi Üretimi

Entropi lambası içerisindeki renkli parçalar sıcaklık farkından kaynaklanan sıvı akışı içerisinde kaotik hareket ederler. RGB renk bilgileri canlı alınan görsellerdeki piksellerden alınır ve 8 bitlik çıktılar damıtma fonksiyonu ile elde edilir. Oluşan veriler ham verilerdir.

Koşullama Katmanı

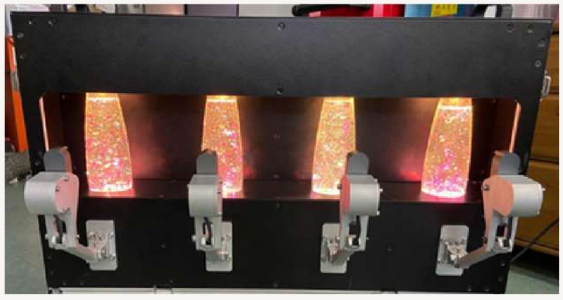
Ham veriler, kullanıcının isteğine bağlı olarak SHA256 ve SHAKE256 koşullama katmanına girdi olarak verilir. Koşullama katmanın amacı ham verilerde oluşabilecek yanlılığı kırmaktır.

IID ve Sağlık Testleri

Ham veriler NIST800-90B standardında verilen sağlık testleriyle, RCT ve APT, sürekli olarak kontrol edilmektedir. Entropi Lambası Sisteminin ham verileri tüm permütasyon hepsinden geçmektedir, Ki-Kare testlerinden kaldığı için sistem non-IID'dir.

Uygulama Alanları

- Güvenli Anahtar Üretimi
- Oyun ve Şans Oyunları Sektörleri
- Bilimsel Simülasyonlar



Öne Çıkan Özellikler

01
Kaotik hareket içerisinde bulunan çok renkli parçaların piksellerinden alınan RGB bilgileriyle entropi üremi

02
50 kg Taşınabilir sistem

03
Rastgele sayı üretecinin sürekli sağlık testleri ve canlı bilgilendirmesi

04
SHA256 ve SHAKE256 koşullama katmanı

05
761 Mbit/sn kriptografik güvenlikli rastgele sayı üretim hızı

06
Terminal seviyesinde kullanıcı dostu etkileşim

Teknik Özellikler

PARAMETRELER	ÖZELLİKLER
ENTROPİ KAYNAKLARI VE KRİPTOGRAFİK TESTLERİ (Entropi Testleri Ham Verilere Yapılmıştır)	
Fiziksel Kaynak	Kaotik sistemdeki parçacıkların RGB renk uzayı bilgisi - Damıtma fonksiyonu
Min-Entropi (SP 800-90B)	7.17 bit/bayt · non-IID/IID
NIST SP800-22 STS Test Paketi	Hepsinden geçti
KOŞULLAMA KATMANI	
Kargaşa Fonksiyonu	SHA256
Genişletilebilir Çıktı Fonksiyonu	SHAKE256
Rastgele Sayı Üretim Hızı	761 Mbit/sn ± 5%
DONANIM	
Tek Kartlı Bilgisayar (SBC)	Tinkerboard 2S x4
Desteklenen OS	Linux
Web Kamera	Logitech BRIO 4K x4
FİZİKSEL ÖZELLİKLER	
Çalışma Sıcaklığı	+65 °C (Şişenin merkezinden sıvıdan alınan ölçüm)
Boyut· Ağırlık	202,5×805×455 mm³ · 50 kg
Isıtıcı Lambalar x4	35 W/ 230V / 350 – 400 lm / 2800 K – 3000 K
Güç Tüketimi	220 V/ 0.73 A / 160.6 W

ODTÜ · İVMER
Orta Doğu Teknik Üniversitesi, Araştırma Parkı, 06800, Ankara, Türkiye
ivmer@metu.edu.tr