RADYOAKTİF BOZUNMADAN RASSALLIK

KUTADGU

RADYOAKTİF BOZUNMA TABANLI KUANTUM RASTGELE SAYI ÜRETECİ

Patent Numarası: TR 2022 015702

KUTADGU, ODTÜ İVMER bünyesinde geliştirilmiş, patentli ve USB arayüzlü bir kuantum rastgele sayı üretecidir. Sistem rastgeleliğini Amerikyum-241 izotopunun yaydığı alfa parçacıklarının yüksek hassasiyetli dedektörde oluşturduğu darbelerin pikosaniye çözünürlükte ölçülmesinden alır. Yüksek rastgeleliğe sahip ham veriler, SHAKE256 genişletilebilir çıktı fonksiyonu kullanılarak yüksek hızlarda kullanıcıya aktarılır.

Entropi Üretimi

Silisyum dedektöre ulaşan her alfa parçacığı bir akım darbesi üretir. Komparatör bu darbeyi sayısal bir sinyal kenarına çevirir; TDC-GPX2 bu kenarı ≈10 ps RMS hassasiyetle zaman ekseninde damgalar.

Koşullama Katmanı

IGLOO2 FPGA, zaman damgalarını entropi kaynağından sürekli yeniden tohumlanan bir SHAKE256 sünger yapısına (FIPS 202) besler. Çıkış verisi USB üzerinden 19,2 Mbit/sn'ye kadar hızla aktarılır.

IID ve Sağlık Testleri

Entropi kaynağının ham çıktısı, NIST SP 800-90B'de tanımlanan RCT ve APT sağlık testleriyle donanım üzerinde sürekli izlenir. Kaynak, 1 MB'lık veri bloklarında bayt başına ortalama 7,88 bit min-entropi sağlar; NIST SP 800- 90B Bağımsız ve Eş Dağılımlılık (IID) testlerindeki başarı oranı %97'dir.

Uygulama Alanları

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



Öne Çıkan Özellikler

01
Alfa bozunmalarının yüksek hassasiyetli dedektörde ürettiği darbelerden elde edilen kuantum entropi

02
TDC-GPX2 ile pikosaniye mertebesinde zaman damgalama

03
Bozunma darbelerini gürültüden ayıracak şekilde ayarlanmış eşik seviyesi

04
FPGA üzerinde donanımsal SHAKE256 koşullama katmanı ve sürekli yeniden tohumlama

05
19,2 Mbit/sn'ye kadar rastgele sayı üretim hızı

06
Tak ve çalıştır. USB arayüzü ile veri iletimi

Teknik Özellikler

PARAMETRELER	ÖZELLİKLER
ENTROPİ KAYNAKLARI VE KRİPTOGRAFİK TESTLERİ (Entropi Testleri Ham Verilere Yapılmıştır)	
Fiziksel Kaynak	Amerikyum-241
Min-Entropi (SP 800-90B)	7,88 bit/bayt · IID testlerinde %97.2 başarı
NIST SP800-22 STS Test Paketi	Hepsinden geçti
KOŞULLAMA KATMANI	
Kargaşa Fonksiyonu	Yok
Genişletilebilir Çıktı Fonksiyonu	SHAKE256
Rastgele Sayı Üretim Hızı	19.2 Mbit/sn
DONANIM VE ARAYÜZ	
FPGA	Microchip IGLOO2 M2GL005
Bilgisayar Arayüzü	USB 2.0, FTDI FT4232H; USB
Desteklenen İşletim Sistemleri	Windows, Linux, macOS (FTDI VCP sürücüsü olan tüm sistemler)
FİZİKSEL ÖZELLİKLER	
Çalışma Sıcaklığı	0 °C … +50 °C (Stokta); -20 °C … +70 °C (İstek üzerine)
Boyut · Ağırlık	97 mm x 33 mm x 20 mm · 33.2 gram
Güç Tüketimi	USB beslemeli (5 V, 1,25 W)

ODTÜ · İVMER

Orta Doğu Teknik Üniversitesi, Araştırma Parkı, 06800, Ankara, Türkiye

ivmer@metu.edu.tr