Uluslararası Mühendislik Araştırmaları Sempozyumu (UMAS'2017), 11-13 Eylül 2017, Düzce, TÜRKİYE
International Engineering Research Symposium, 11-13 Sept. 2017 Düzce, TURKEY
ISBN: 978-605-60595-9-9

KAOTİK OSİLATÖR TABANLI GÖMÜLÜ GERÇEK RASGELE SAYI ÜRETECİ

Murat Tuna[1], Can Bülent Fidan [2], İsmail Koyuncu[3], İhsan Pehlivan[4]

Kırklareli Üniversitesi, Teknik Bilimler MYO, Elektrik Teknolojisi, , 39000, Kırklareli, Türkiye

Karabük Üniversitesi Mühendislik Fakültesi, Mekatronik Mühendisliği, , 79000, Karabük, Türkiye

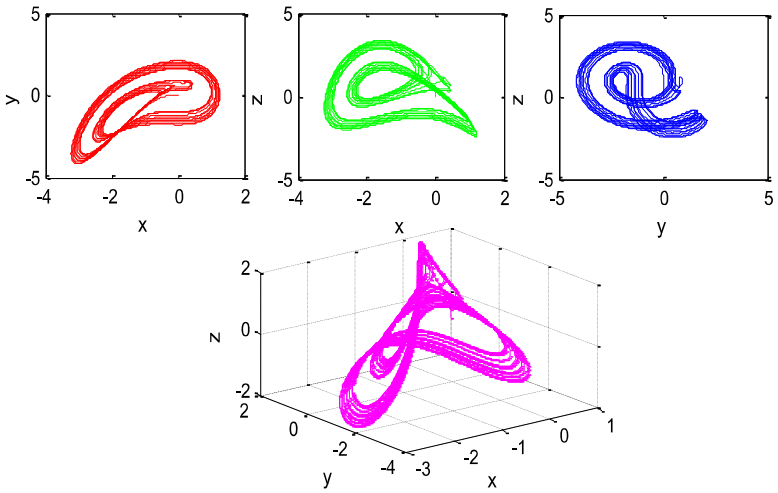
Afyon Kocatepe Üniversitesi, Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği, 03200, Afyon, Türkiye

Sakarya Üniversitesi, Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği, 54000, Sakarya, Türkiye

murat.tuna@klu.edu.tr (corresponding author)

ÖZET

Kaotik sistemler başlangıç koşullarına hassas bağlı, karmaşık ve düzensiz görünümlüdür ve deterministik doğrusal olmayan zamanla değişen sistemlerde ortaya çıkarlar. Kaos tanımı incelendiğinde başlangıç koşullarına üstel duyarlı, nonlineer, deterministik karakterli, uzun vadede periyodik olmayan dinamik sistemler olduğu görülmektedir. En kısa tarifiyle ise, düzensizliğin düzeni şeklinde tanımlanan ve doğrusal olmayan olayları açıklamaya yarayan bir bilim dalıdır. Karmaşık, ama kendi iç düzenine sahip bir süreçtir. Özellikle dikkat edilmesi gereken bir nokta, kaosun rastgelelik olmadığıdır. Dinamik sistemlerde bilinen en karmaşık kararlı hal davranışı kaos' tur. Kaos ile ilgili çalışmalar, doğrusal olmayan dinamik sistemler teorisinin bir kısmıdır. Bu çalışmada kullanılan kaotik sistemin faz görünümleri Şekil 1'de gösterilmektedir. Kaotik işaretlerin sahip oldukları farklı özellikleri sebebiyle, bu sistemler son yıllarda bilgi güvenliği amacıyla güvenli haberleşme düzenekleri oluşturma, gürültü üreteçleri, şifreleme ve rasgele sayı üreteçleri (RSÜ) alanlarında kullanılmaktadırlar.



Şekil 1. GRSÜ üretimde kullanılan kaoitk sistemin faz görünümleri.

Rasgele sayı üreteçleri Sözde Rasgele Sayı Üreteçleri (SRSÜ), Gerçek Rasgele Sayı Üreteçleri (GRSÜ) ve Hibrit Rasgele Sayı Üreteçleri (HRSÜ) olmak üzere 3 sınıfa

ISBN: 978-605-60595-9-9

ayrılmaktadır. GRSÜ' leri belirsizlik kaynağı olarak gerçek entropi kaynakları kullanmaktadır. Bu yapı daha güvenli bir kaynak oluşturduğu için kriptografide anahtar olarak öngörülemeyen bit dizisi oluşturmada sıklıkla kullanılmaktadır. Ancak anahtarların sistem dışında kontrolsüz ortamlarda üretimi sistemin güvenilirliğini azaltmaktadır. Bu dezavantajı ortadan kaldırmak için günümüzde donanımsal kriptolojinin ve güvenli haberleşmenin gelişimi, programlanmış kripto aritmetiğinin DSPs, ASIC ve FPGA gibi entegre içerisinde gerçekleştirilmesi yönündedir. FPGA çipleri bu problemin üstesinden gelmekle birlikte aynı zamanda bu işlemleri yüksek frekanslarda da gerçekleştirebilmektedir. FPGA yüksek hız ve kapasiteleri nedeniyle özellikle yüksek performans ve işlemci gücü gerektiren kriptoloji ve güvenli haberleşme gibi uygulamalarda bilgi güvenliği kapasitesini iyileştirmede önemli bir potansiyele sahiptir.

Şekil 2. FPGA üzerinde kaos tabanlı tasarlanan GRSÜ Xilinx ISE Simülatör sonucu.

GRSÜ' inde entropi kaynağı olarak deterministik olmayan fiziksel olaylar kullanılmaktadır. GRSÜ' ler yavaş, maliyetli ve donanıma bağımlı olması gibi dezavantajlara sahiptir. Ancak GRSÜ' lerin kriptografik uygulamalar için zorunlu olan kestirilememe, tekrar üretilememe ve istatistiksel rasgelelik testlerinden oldukça başarılı bir şekilde geçmesi onun kriptolojide birçok alanda kullanımını arttırmıştır. Bu çalışmada; FPGA üzerinde gerçek zamanlı, Heun nümerik diferansiyel denklem çözüm yöntemiyle yüksek bit üretim hızına sahip yeni kaotik sistem ile yüksek çalışma frekanslı halka osilatörler kullanılarak yüksek çalışma frekansına ve yüksek bit üretim hızına sahip GRSÜ tasarımı gerçekleştirilmiştir (Şekil 2). Sistemin çalışma frekansı 400 MHz olarak tespit edilmiş ve yapılan tüm istatistiki testlerden başarılı bir şekilde geçmiştir. Bu sistem Xilinx Virtex-6 FPGA çipinde VHDL dilinde 32 bit IQ-Math Fixed-Point Number (Sabit-Noktalı Sayı) formatında tasarlanmıştır. Literatürdeki IEEE 754-1985 kayan nokta sayı formatındaki tasarımlarına nazaran sabit noktalı sayı formatının daha az FPGA çip istatistikleri kullandığı ve bu sayede çalışma frekansının ve bit üretim hızını arttığı gözlemlenmiştir. VHDL tamamen sayısal tabanlı olduğundan reel sayılar üzerinde işlem yapmak için sayıların sabit noktalı veya kayan noktalı biçimde ifade edilmesi gerekir. Sabit noktalı sayı biçimi hızlı ve kolay uygulanabilmesine rağmen, kayan noktalı sayı biçimi daha duyarlı işlemler için kullanılır.

Keywords: Kaotik sistemler, Gerçek rasgele sayı üreteçleri, FPGA, VHDL.