International Advanced Researches & Engineering Congress-2017
http://iarec.osmaniye.edu.tr/
Osmaniye/TURKEY
16-18 November 2017

FPGA-Based Design of a Novel TRNG

Murat Tuna[1], Can Bülent Fidan[2], İsmail Koyuncu[3*], İhsan Pehlivan[4]
[1]Department of Electric, Technical Sciences Vocational School, Kirklareli University, Kirklareli, Turkey
[2]Department of Mechatronics Engineering, Karabuk University, Karabuk, Turkey
[3]Department of Electric-Electronic Engineering, Afyon Kocatepe University, Afyon, Turkey
[4]Department of Electric-Electronic Engineering, Sakarya University, Sakarya, Turkey
* Corresponding author. Tel.: +90 272 228 14 47, Fax: +90 272 14 49, E-mail address: ismailkoyuncu@aku.edu.tr

Abstract

In this study, True Random Number Generator (TRNG) that is embedded on FPGA having high operation and bit rate was performed by using chaotic oscillator design having a new structure based on chaos. Since the chaotic oscillators have features such as noise-like and the ability to hide the sign of information, great efforts have been made in recent years on the development of chaos-based TRNG structures. TRNGs that is used in the field of cryptography and secure communications require fast, secure and intensive process of the physical methods that do not have deterministic character are used as entropy source. For this purpose, the equation structures of chaotic systems, which were presented in the literature in the last years, were investigated by performing their dynamic analysis. In the following parts, the chaotic systems, newly introduced to literature, were modeled by two different numerical integration methods (Euler, Heun) and chaos analysis was done by being examined the dynamic behaviors of the systems. The chaotic system was then modeled on the FPGA in hardware identification language VHDL in accordance with the 32 bit IQ-Math fixed point number standard. Two different algorithms as Euler and Heun were used in the modeling phase. The parameters belonging to the FPGA chip source usage and clock speeds of units were examined. According to the results obtained, the operating frequency of the chaotic oscillators changes about between 390-464 MHz. Subsequent to that, the TRNG design by using the Euler and Heun algorithms. The 32-bit IQ-Math fixed-point numbering standard was used in FPGA-based TRNG modelling. The developed model was encoded by using the VHDL hardware identification language. The TRNG units designed were synthesized for the XC6VLX550T-2FF1759 chip of the Virtex-6 family produced by Xilinx, and the statistics of parameters belonging to FPGA chip source usage and clock speeds of the units, were examined.

Keywords: Chaotic systems, FPGA, VHDL, TRNG

FPGA Tabanlı Yeni bir GRSÜ Tasarımı

Özet

Bu çalışmada, kaos tabanlı yeni bir yapı kullanılarak yüksek çalışma ve bit üretim hızına sahip FPGA üzerinde gömülü Gerçek Rasgele Sayı Üreteci (GRSÜ) gerçekleştirilmiştir. Kaotik osilatörlerin gürültü benzeri özellikler taşımaları ve bilgi işaretini gizleyebilme gibi özelliklerinden dolayı kaos tabanlı GRSÜ yapıların geliştirilmesi üzerine son yıllarda büyük çabalar sarf edilmektedir. Hızlı, güvenli ve yoğun işlem gerektiren kriptografi ve güvenli haberleşme alanlarında kullanılan GRSÜ' lerde entropi kaynağı olarak deterministik karaktere sahip olmayan fiziksel yöntemler kullanılmaktadır. Bu amaçla, son yıllarda literatüre sunulan yeni bir kaotik sistemin dinamik analizleri gerçekleştirilerek denklem yapıları incelenmiştir. Sonraki bölümlerde literatüre yeni sunulan kaotik sistem iki farklı nümerik integrasyon metodu (Euler, Heun) ile modellenmiş ve sistemlerin dinamik davranışları incelenerek kaos analizleri yapılmıştır. Daha sonra kaotik sistem FPGA üzerinde donanım tanımlama dili VHDL ile 32 bit IQ-Math sabit noktalı sayı standardına uygun olarak modellenmiştir. Modelleme aşamasında Euler ve Heun olmak üzere iki farklı algoritma kullanılmıştır. FPGA çip kaynak kullanımına ve ünitelerin saat hızlarına ait parametrelerin istatistikleri incelenmiştir. Elde edilen sonuçlara göre kaotik osilatörlerin çalışma frekansı yaklaşık 390-464 MHz arasında değişmektedir. Ardından, Euler ve Heun algoritmaları kullanılarak FPGA-tabanlı GRSÜ tasarımı gerçekleştirilmiştir. FPGA tabanlı GRSÜ modellemelerinde 32 bit IQ-Math sabit noktalı sayı standardı kullanılmıştır. Geliştirilen model VHDL donanım tanımlama dili kullanılarak kodlanmıştır. Tasarımı yapılan GRSÜ ünitesi Xilinx firmasının ürettiği Virtex-6 ailesinin XC6VLX550T-2FF1759 çipi için sentezlenerek, FPGA çip kaynak kullanımına ve ünitelerin saat hızlarına ait parametrelerin istatistikleri incelenmiştir.

Anahtar Kelimeler: Kaotik sistemler, FPGA, GRSÜ, VHDL