Journal of the Faculty of Engineering and Architecture of Gazi University 33:3 (2018) 1171-1182

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

The design and application of bank authenticator device with a novel chaos based random number generator

Serkan Akkaya[1], İhsan Pehlivan[2], Akif Akgül[2], Metin Varan[2]

[1]Sakarya University, Institute of Natural Sciences, Department of Electrical and Electronics Engineering, Sakarya, 54050, Turkey
[2]Sakarya University of Applied Sciences, Faculty of Technology, Department of Electrical and Electronics Engineering, Sakarya, 54050, Turkey

Highlights:

- An encryption device has been developed that uses the algorithm of generating random numbers by using the sensitive digits of floating-point numbers.
- Developed encryption device has successfully passed the statistical NIST-800-22 randomness tests.
- The obtained results show that developed device can be used as a high security authentication tools
-

Keywords:

- Chaos
- random number generator
- chaos based encryption,
- randomness tests

Article Info:

Received: 15.02.2017
Accepted: 10.01.2018

DOI:

10.17341/gazimmfd.416418

Acknowledgement:

Correspondence:

Author: Serkan Akkaya
e-mail: serkanakkaya26@gmail.com
phone: +90 264 295 6441

Graphical/Tabular Abstract

In the literature reviews, it has been generally seen that integer operations are used to generate bit sequences in random number generation(RNG) algorithms. Different from the literature, in this study, an encryption device has been developed that uses the algorithm of generating random numbers by using the sensitive digits of floating-point numbers

Figure A. A sample internet banking screen

Purpose: The purpose of this study, developing an encryption device that uses the algorithm of generating random numbers by using the sensitive digits of floating-point numbers.

Theory and Methods:
The developed encryption device has been based on a non-equilibrium point chaotic oscillator that makes impossible for Shilnikov decoding analysis. The encryption performance of the developed device has been realized through an exemplary banking system interface application.

Results:
Developed encryption device has successfully passed the statistical NIST-800-22 randomness test which is the highest international standard.

Conclusion:
The obtained results show that developed device can be used as a high security authentication tool in internet banking sector and remote terminal units of automation systems.

Journal of the Faculty of Engineering and Architecture of Gazi University 33:3 (2018) 1171-1182

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Yeni bir kaos tabanlı rastgele sayı üreteci kullanan banka şifrematik cihazı tasarımı ve uygulaması

Serkan Akkaya[1]*, İhsan Pehlivan[2], Akif Akgül[2], Metin Varan[2]

[1]Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik-Elektronik Mühendisliği Bölümü, Sakarya, 54050, Türkiye
[2]Sakarya Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, Sakarya, 54050, Türkiye

Ö N E Ç I K A N L A R

- Mikro Kaos ve kaotik uygulamalar
- Rastgele sayı üreteci tasarımı
- Rastgelelik testleri

Makale Bilgileri
Geliş: 15.02.2017
Kabul: 10.01.2018

DOI:
10.17341/gazimmfd.416418

Anahtar Kelimeler:
Kaos,
rastgele sayı üreteci,
şifrematik,
kaos tabanlı şifreleme,
rastgelelik testleri

ÖZET

Literatürde yapılan incelemelerde rastgele sayı üreteci(RSÜ) algoritmalarında bit dizilerinin üretilmesi için daha çok tam sayılı işlemler kullanıldığı görülmüştür. Bu makalede kayan noktalı sayıların hassas basamakları kullanılarak RSÜ algoritması kullanan bir şifreleme aracı oluşturulmuştur. Geliştirilen bu yeni şifreleme aracında Shilnikov şifre çözme analizlerinin yapılamaması için denge noktası olmayan bir kaos osilatör modeli seçilmiştir. Geliştirilen bu şifreleme aracı, uluslararası en üst rastgelelik standardı olan istatiksel NIST-800-22 testlerini başarı ile geçmiştir. Geliştirilen bu aracın şifreleme başarımı örnek bir bankacılık sistemi arayüz uygulaması üzerinden donanımsal olarak gerçekleştirilmiştir. Elde edilen başarım sonuçları ile geliştirilen bu donanımsal şifreleme aracının internet bankacılığı sektörü ve otomasyon sistemlerinin uzak masaüstü erişim platformlarında yüksek güvenlikli bir kimlik doğrulama aracı olarak kullanılabileceği öngörülmüştür.

The design and application of bank authenticator device with a novel chaos based random number generator

H I G H L I G H T S

- Chaos ve chaotic application
- Random number generator design
- NIST randomness test

Article Info
Received: 15.02.2017
Accepted: 10.01.2018

DOI:
10.17341/gazimmfd.416418

Keywords:
Chaos,
random number generator,
chaos based encryption,
randomness tests

ABSTRACT

In the literature reviews, it has been generally seen that integer operations are used to generate bit sequences in random number generation(RNG) algorithms. Different from the literature, in this study, an encryption device has been developed that uses the algorithm of generating random numbers by using the sensitive digits of floating-point numbers. The developed encryption device has been based on a non equilibrium point chaotic oscillator that makes impossible for Shilnikov decoding analysis. Developed encryption device has successfully passed the statistical NIST-800-22 randomness test which is the highest international standard. The encryption performance of the developed device has been realized through an exemplary banking system interface application. The obtained results show that developed device can be used as a high security authentication tool in internet banking sector and remote terminal units of automation systems.

*Sorumlu Yazar/Corresponding Author: serkanakkaya26@gmail.com / Tel: +90 264 295 6441

1. GİRİŞ (INTRODUCTION)

Bilimsel olarak "kaos" terimi, rastgele gözüken olayların içinde var olan olayları ve bu olayların temelini oluşturan birbirine bağlılıktan söz eder. Kaos bilimi, gizli biçim düzenleri, ince farklar, nesnelerin "duyarlılığı" ve tahmin edilemeyenin yeniye nasıl yol açtığına dair "kurallar" üzerine odaklanır. Kısaca kaos, düzensizliğin düzeni şeklinde tanımlanan, başlangıç koşullarına hassas bağımlı, doğrusal olmayan bir bilim dalıdır [1]. Diğer bir ifadeyle kaos, düzensizliğin düzenidir [2]. Gelişen teknoloji ile birlikte, oldukça rastgele ve hassas özelliklere sahip olan, analog veya sayısal olarak kolaylıkla gerçeklenebilen gerçek ortam gürültü kaynakları ve kaotik sistem gibi yapılar son zamanlarda Rastgele Sayı Üreteçleri (RSÜ) olarak kullanılmaya başlamıştır [3 ,4]. Ergün vd. ile Li vd. sıklıkla kullanılan sanal RSÜ'den farklı olarak gerçek RSÜ üzerine çalışmalar gerçekleştirmişlerdir [5, 6]. Koyuncu ise kriptolojik uygulamalar için FPGA tabanlı bir RSÜ tasarımı ve gerçeklemesi üzerine literatüre katkıda bulunmuştur [7]. RSÜ; şans oyunu çekilişleri, oyunlar, elektronik devre tasarımı, rastgele sayı örnekleme, genetik algoritma, kriptoloji, sanat, müzik gibi birçok alanda kullanılabilmektedir.

Literatürde, rastgele sayı üreteçleri ve uygulama alanları ile ilgili yapılmış birçok çalışma bulunmaktadır. Akgül vd., istatistiksel testlerin tümünden başarıyla geçen rastgele sayı üreteçleri tasarlayarak birçok alanda rastgele sayı üreteç uygulamaları yapmışlardır [8, 9]. Ayrıca yine Akgül vd. FIPS testlerinin hepsinden başarıyla geçen mikrodenetleyici tabanlı bir RSÜ tasarımı gerçekleştirmişlerdir [10]. NIST-800-22 testlerinin tümünden başarıyla geçen rastgele sayılar ile Wang vd. sinyal şifreleme uygulaması [11, 12], Volos vd. ses şifreleme uygulaması [13], Jafari vd. metin şifreleme uygulaması [14], Çavuşoğlu vd. ise TCP verilerinin şifrelemesine yönelik bir uygulama [15] gerçekleştirmişlerdir. Wieczorek vd., FPGA ile çift kararlı flip-flop kullanarak 50 MHz çalışma frekanslı ve 5 Mbit/s bit üretim hızında RSÜ tasarımı yaparak istatistiksel testlere tabi tutarak başarılı sonuçlar elde etmişlerdir [16]. Fischer vd. 1 Mbit/s bit üretim hızında, PLL tabanlı osilatörü FPGA kullanarak gerçekleştirmişler ve NIST testlerinden başarılı sonuçlar elde etmişlerdir [17]. István vd. ise yine FPGA tabanlı, 50 MHz çalışma frekanslı klasik jitter osilatör yöntemi ile rastgele sayı üretimi gerçekleştirerek, NIST testlerinden başarılı sonuçlar elde etmişlerdir [18].

Çiçek vd., CMOS teknolojisi ile ayrık zamanlı tek boyutlu kaotik harita kullanarak RSÜ tasarımı gerçekleştirmişler ve NIST testlerinin 11'inden başarılı sonuçlar elde etmişlerdir [19]. Yine Çiçek vd., FPAA (Field Programmable Analog Array) donanımı ile, tek boyutlu ayrık iki kaotik harita kullanarak 16 MHz çalışma frekanslı ve 1,5 Mbit/s bit üretim hızında RSÜ tasarımı yapmışlar ve NIST testlerinin hepsinden başarılı sonuçlar elde etmişlerdir [20]. Pareschi vd., CMOS teknolojisini kullanarak 80 Mbit/s bit üretim hızında kaos tabanlı RSÜ tasarımı gerçekleştirmişlerdir [21]. Callegari vd., şifreleme uygulamaları için ADC tabanlı gerçek rastgele sayı üreteci tasarımı gerçekleştirmişlerdir [22]. Pareschi vd. ise ADC tabanlı RNG'nin etkili simülasyonu için makro bir model geliştirmişlerdir [23]. Günümüzde teknolojinin hızla gelişmesiyle beraber internet bankacılığının kullanımı da çok ciddi oranda artış göstermiştir. Bu artış internet bankacılığında gizlilik ve güvenlik gibi konuların önemini de arttırmıştır. Çoğunlukla mobil ya da ağ üzerinden kullanılan internet bankacılığında güvenlik simetrik ve asimetrik şifreleme yöntemleri kullanılarak [24] genel olarak kullanıcının cep telefonu ile sağlanmaktadır. Mobil bankacılıkta [25] kullanıcının GSM numarası, cep telefonu MAC bilgisi, sim kart ID bilgisi gibi çeşitli referans değerler baz alınarak mobil bankacılık uygulamasının cep telefonuna kurulması ile internet bankacılığının kullanımı mümkün olmaktadır. Ağ (web) bankacılığında ise kullanıcının sms ile almış olduğu tek kullanımlık şifre ile banka sunucularına erişim sağlanmakta ve internet bankacılığının kullanımı gerçekleşmektedir. Mobil bankacılıkta kullanılmakta olan akıllı cep telefonları spam (istenmeyen mesaj), malware (zararlı yazılımlar), olta saldırıları (phishing), elektronik takip, elektronik dinleme gibi saldırılara açık olduğundan, uzaktan yönetilebilir hale gelebilmekte ve çeşitli riskler ile karşı karşıya kalabilmektedir. Ağ (web) bankacılığındaki sms uygulamasında da kullanıcının yine akıllı cep telefonuna sahip olması halinde, benzer risklerin ortaya çıkması söz konusu olmaktadır. Bu sebeple şifrematik cihazları, farklı düzey bir güvenlik uygulaması olarak bankalar tarafından müşterilerine sunulmaktadır [26].

Yapılan literatür taramasında çok sayıda şifreleme çalışmasının yapıldığı saptanmış ancak bu çalışmaların içerisinde doğrudan şifre üretimine dair az sayıda çalışmanın var olduğu görülmüştür. Yapılan çalışmalarda üretilen şifrelerin benzersizliği hususunda herhangi analize rastlanılmamıştır [27, 28]. Patent ve diğer benzeri çalışmalarda da benzer şekilde ilgili yaklaşımlar görülememektedir [29, 30]. Bu makaledeki çalışmada tasarım kendi özelinde irdelenmiş ve üretilmiş şifrelerin içerisindeki sadece iki adet şifrenin mükerrer olduğu gözlenmiştir.

Gerçek rastgele sayı üretecine sahip olan ARM tabanlı STM32F407VG mikrodenetleyicisi incelendiğinde kart üzerindeki RNG birimi tarafında üretilen sayıların sadece FIPS PUB 140-2 (2001 October 10) testinden %99 başarı oranı ile geçtiği görülmüştür [29].

WO2016153398 A1 patent dökümanında kullanıcı cihazının kimlik doğrulaması için bir yöntem ve kimlik doğrulama cihazı açıklanmaktadır. Kullanıcı cihazı bir seferlik bir şifre üretir. Kullanıcı cihazı, bir kimlik doğrulayıcı cihazına bir seferlik şifreyi bir akustik sinyal olarak gönderir; buradaki akustik sinyal, bir ultrason aralığı veya bir alt sınır aralığı içinde bir frekansı kapsar. Doğrulayıcı cihaz kullanıcı cihazından bir seferlik şifre alır. Doğrulayıcı cihazı, bir kerelik şifreyi doğrular. Bu yöntem ve cihaz kaos tabanlı olmamakla beraber şifrelerin benzersizliğine dair herhangi çıktı paylaşılmamıştır [30].

Bhole ve Chaudhari [31] mobil uygulama tabanlı tek kullanımlık şifre üretmeye dair yaptıkları çalışmada, özetleme fonksiyonu yardımı ile şifre üretimi yapmışlardır. Bu çalışmada üretilen şifrelerin benzersizliğine dair herhangi analizin olmadığı görülmektedir. Srinivasa ve Janakib [32] ise kullanıcının bir görsel öğe seçimine dayanan piksel bazlı ve matematiksel hesaplama modeline sahip tek kullanımlık şifre üretimiyle yeni bir çalışma gerçekleştirmişlerdir. Bu çalışmada da üretilen tek kullanımlık şifrelerin birbirleri arasında yapılmış herhangi analiz bulunmamaktadır.

Bu çalışmada, kaos tabanlı RSÜ kullanan, bir şifrematik cihazı tasarımı gerçekleştirmek amaçlanmıştır. II. Bölümde kaos tabanlı rsü tasarımına değinilmiştir. III. Bölümde rsü kullanan bir şifre üretme algoritması geliştirilmiş, sonrasında bu tasarımın bilgisayar ve mikrodenetleyicide uygulaması yapılmıştır. IV. Bölüm ise sonuçları içermektedir.

2. RSÜ TASARIMI VE NIST TESTLERİ
(RNG DESIGN AND NIST TESTS)

2.1. Rastgele Sayı Üreteci (RSÜ) Tasarımı
(Random Number Generator Design)

Günümüzde, bilişim dünyasındaki gelişmeler ve bilgi güvenliğine duyulan ihtiyaç rastgele olarak üretilen güçlü şifrelemelerin oluşturulmasını zorunluluk haline getirmiştir. Öte yandan rastgele olarak üretilen bu sayıların gerçekten rastgele olup-olmadığına dair ölçütler konusu gelişim göstermiş ve istatiksel rastgelelik testleri adıyla anılan çeşitli testlere ihtiyaç duyulmuştur. Bu bölümde de rastgele sayı üretecine değinilecektir.

Rastgele sayılar, önceden tahmin edilmesi güç olan ya da bir sonraki teriminin ne olacağı bilinme olasılığı çok düşük olan sayılardır. Diğer bir ifade ile: Bir fonksiyonun bir ya da birden fazla teriminin bilinmesi ile birlikte, sonraki terimleri arasındaki ilişkisinin formül haline getirilmesi güç olan sayılardır.

Rastgele sayı üreteçleri genel olarak Sözde RSÜ ve Gerçek RSÜ'ler olarak iki bölüm altında incelenmektedirler [33]. Sözde RSÜ'ler yazılımsal olarak gerçekleştirilirken, Gerçek RSÜ'ler donanımsal olarak gerçekleştirilmektedirler. Gerçek RSÜ'ler kendi içerisinde analog tabanlı RSÜ'ler ve sayısal tabanlı RSÜ'ler olarak iki başlık altında incelenebilir. Sürekli zamanlı kaotik RSÜ'ler analog tabanlı RSÜ'ler içerisinde ele alınırken, ayrık zamanlı kaotik RSÜ'ler sayısal tabanlı RSÜ'ler içerisinde ele alınmaktadırlar. Rastgele sayılar hayatın birçok alanında farklı şekillerde karşımıza çıkmaktadır. Günlük yaşamda internet bankacılığında cep telefonumuza gelen kısa mesajlarda, internet bankacılığı şifrematik uygulamalarında, e-posta hesaplarının aktifleştirilmesinde, birçok sitenin kullanıcı ekranlarına erişim esnasındaki güvenlik kodlarında, matematik alanında denklem çözme ve olasılık hesaplamalarında, otomobillerin araç kumandalarında, ağ güvenlik sistemlerinde, radar cihazlarında, bilgisayar oyunlarında ve birçok alanda çeşitli uygulamaları bulunmaktadır. Literatüre Akif ve Pehlivan tarafından yeni sunulan bir kaotik sistemin (bundan sonra "AP Kaotik Sistemi" olarak bahsedilecektir) denklemi aşağıda verilmiştir [34]. AP Kaotik Sistemi'nin elektronik devre elemanları; direnç, opamp, çarpma entegresi, kondansatör gibi temel elemanlardan meydana gelmektedir. Kaotik sistemin tasarımında başlangıç değerleri ve parametreler a =2,8, b=0,2, c=1,4, d=1, e=10, f=2 ve x=y=z=0 olarak alınmıştır. AP Kaotik Sistemi, "0" başlangıç özelliğine (x, y, z) sahip olan bir sistem olduğu için gerçekleme daha kolay yapılabilmiştir. Gerçek ortam uygulamaları içinde başlangıç şartlarının "0" olması kolaylık sağlamaktadır. Eş. 1'de verilen AP Kaotik Sistemi, Eş. 2'de RK4 algoritması yardımı ile ayrıştırılacaktır.

$$\begin{aligned} \dot{x}&=ay-x+zy \\ \dot{y}&=-bxz-cx+yz+d \\ \dot{z}&=e-fxy-x^2 \end{aligned} \tag{1}$$

$$\begin{aligned} k_1&=f(y_\lambda) \\ k_2&=f(y_\lambda+\frac{\Delta h}{2}k_1) \\ k_3&=f(y_\lambda+\frac{\Delta h}{2}k_2) \\ k_4&=f(y_\lambda+\Delta h k_3) \\ y_{\lambda+1}&=y_\lambda+\frac{1}{6}(k_1+2k_2+2k_3+k_4)\Delta h \end{aligned} \tag{2}$$

Eş. 3'de verilen AP Kaotik Sistemi; f, g ve δ fonksiyonlarına göre RK4(Runga-Kutta 4) algoritması ile ayrıklaştırılmış ve Eş. 4'de sistemin matematiksel modeli elde edilmiştir.

$$\begin{aligned} \dot{x}&=f(t,x,y,z)=2{,}8y-x+zy \\ \dot{y}&=g(t,x,y,z)=-0{,}2xz-1{,}4x+yz+1 \\ \dot{z}&=\delta(t,x,y,z)=10-2xy-x^2 \end{aligned} \tag{3}$$

$$\begin{aligned} x(k+1)&=x(k)+p(k) \\ p(k)&=\frac{1}{6}\Delta h[k_1(k)+2k_2(k)+2k_3(k)+k_4(k)] \\ y(k+1)&=y(k)+r(k) \\ r(k)&=\frac{1}{6}\Delta h[\lambda_1(k)+2\lambda_2(k)+2\lambda_3(k)+\lambda_4(k)] \\ z(k+1)&=z(k)+s(k) \\ s(k)&=\frac{1}{6}\Delta h\left[\xi_1(k)+2\xi_2(k)+2\xi_3(k)+\xi_4(k)\right] \end{aligned} \tag{4}$$

Eş. 4'de bulunan k, λ, ξ parametreleri, Eş. 5'de verildiği gibi hesaplanmaktadır. Eş. 4'de 1. basamaktaki tüm k parametreleri Eş. 3'deki kaotik sistemin ilk denklemine ait değerleri, 2. basamaktaki tüm λ parametreleri ikinci denkleme ait değerleri, 3. Basamaktaki tüm ξ parametreleri ise üçüncü denkleme ait değerleri ifade etmektedir. Bulunan katsayılar Eş. 4'deki RK4 algoritmasında yerlerine konularak, kaotik sistemin Δh kadar adım sonrası değeri olan ayrıklaştırılmış x(k+1), y(k+1) ve z(k+1) değerlerini hesaplanmaktadır. Her adım sonunda bulunan x(k+1), y(k+1) ve z(k+1) değerleri hem hesaplanan o adımda çıkış olarak, hem de bir sonraki adımda başlangıç şartı olarak kullanılmaktadır. Ayrıştırma sonucunda elde edilen bu sayılar bu sayılar kayan noktalı sayı yapısındadır. AP Kaotik Sistemi birinci durum değişkeni x'in RK4(Runga-Kutta 4) algoritması ile ayrıklaştırılmış ilk 10 adımı Tablo 1'de verilmiştir.

$$
\begin{aligned}
k_1&=f(x(k),y(k),z(k))\\
\lambda_1&=g(x(k),y(k),z(k))\\
\xi_1&=\delta(x(k),y(k),z(k))\\
k_2&=f(x(k)+\frac{1}{2}\Delta h k_1,y(k)+\frac{1}{2}\Delta h\lambda_1,z(k)+\frac{1}{2}\Delta h\xi_1)\\
\lambda_2&=g(x(k)+\frac{1}{2}\Delta h k_1,y(k)+\frac{1}{2}\Delta h\lambda_1,z(k)+\frac{1}{2}\Delta h\xi_1)\\
\xi_2&=\delta(x(k)+\frac{1}{2}\Delta h k_1,y(k)+\frac{1}{2}\Delta h\lambda_1,z(k)+\frac{1}{2}\Delta h\xi_1)\\
k_3&=f(x(k)+\tfrac{1}{2}\Delta h k_2,y(k)+\tfrac{1}{2}\Delta h\lambda_2,z(k)+\tfrac{1}{2}\Delta h\xi_2)\\
\lambda_3&=g(x(k)+\tfrac{1}{2}\Delta h k_2,y(k)+\tfrac{1}{2}\Delta h\lambda_2,z(k)+\tfrac{1}{2}\Delta h\xi_2)\\
\xi_3&=\delta(x(k)+\tfrac{1}{2}\Delta h k_2,y(k)+\tfrac{1}{2}\Delta h\lambda_2,z(k)+\tfrac{1}{2}\Delta h\xi_2)\\
k_4&=f(x(k)+\Delta h k_3,y(k)+\Delta h\lambda_3,z(k)+\Delta h\xi_3)\\
\lambda_4&=g(x(k)+\Delta h k_3,y(k)+\Delta h\lambda_3,z(k)+\Delta h\xi_3)\\
\xi_4&=\delta(x(k)+\Delta h k_3,y(k)+\Delta h\lambda_3,z(k)+\Delta h\xi_3)
\end{aligned}
\tag{5}
$$

Tablo 1. Kayan noktalı sayılar (Floating point number)

Adım Sayısı	Ayrıklaştırma Sonucu Elde Edilen Kayan Noktalı Sayılar (x durum değişkeni için)
1	0,003866508205357
2	0,017022109192077
3	0,042062260612412
4	0,082042775172218
5	0,140612988083349
6	0,222137744672527
7	0,331789743765176
8	0,475571084896906
9	0,660185655353679
10	0,892627200833881

Rastgele sayı üretimi için üretilen bu kayan noktalı türündeki sayıların öncelikle ikili sayılara dönüştürülmesi gerekmektedir. İlgili işlem 32-bit tek duyarlı IEEE 754-1985 kayan noktalı sayı standardına göre gerçekleştirilmiştir. Bu dönüşüm sonrası elde edilen AP Kaotik Sistemi birinci durum değişkeni x'in ilk 10 adımındaki sayıların ikili sayı formatı Tablo 2'de verilmiştir.

Tablo 2. İkili sayılar (Binary numbers)

Adım Sayısı	İkili Sayı Dönüşümleri
1	00111011011111010110010100111110
2	00111100100010110111000111110011
3	00111101001011000100100101111010
4	00111101101010000000011000001011
5	00111110000011111111110011011010
6	00111110011000110111100000010100
7	00111110101010011110000001011000
8	00111110111100110111111000001110
9	00111111001010010000000111101101
10	00111111011001001000001100110111

İkili sayı koduna dönüştürülen bu sayıların istatistiksel testlere tabi tutulmadan önce belirli bir fonksiyon haline getirilmesi gerekmektedir. Bu fonksiyon sonucu elde edilen rastgele sayıların güvenilirliğinden emin olmak için uluslararası kabul görmüş NIST-800-22 veya FIPS-140-1 gibi istatistiksel testlerden geçirilmesi gerekmektedir [35]. Test sonucu başarılı olmayan fonksiyon için testleri geçene kadar düzeltme işlemleri uygulanmalıdır. Şekil 1'de kaotik bir sistemden nasıl rastgele sayı üretimi gerçekleştirileceği anlatılmıştır. Makale neticesinde elde edilen şifreler tek kullanımlık (OTP – One time password – tek kullanımlık şifre) olmak üzere tasarlanmıştır. OTP üretim algoritmalarının detayları büyük farklılıklar göstermekle beraber genel olarak iki ana başlık altında toplandığı gözükmekte olup; zaman bazlı ve sayaç bazlı oldukları görülmektedir. Bu tasarımlar SHA-0, SHA-1, SHA-256, SHA-384 gibi özet fonksiyonu (hash fonksiyonu) ile gerçekleştirilebildikleri [36] gibi rastgele sayı üreteci kullanan matematiksel model ile yapılmaları da mümkündür [37].

Bu makaledeki rastgele sayı üretimi (RNG), üçüncü dereceden diferansiyel denklem içeren kaos tabanlı bir devrenin, durum denklerinden elde edilen kayan noktalı sayının IEEE-754 standartlarına göre 32 bitlik dönüşümü ile gerçekleştirilmiştir. Ancak bu dönüşüm ile gelen 32 bitlik sayı serisinin NIST-800-22 testlerinden doğrudan geçmesi her zaman mümkün olamamaktadır. Bu sebeple elde edilen bu sayı dizilerinin belli bir işleme tabi tutularak test edilmeleri gerekmektedir. Bu işlemde RNG'nin rastgeleliğinin sağlanması ve algoritmanın en hızlı şekilde çalışması beklendiğinden tasarımın mümkün olduğunca pratik olması gerekmektedir. Bu çalışmada elde edilen 32 bitlik serinin sadece 32.biti alınarak "bir aritmetik ve/veya mantıksal işlem algoritması" gereksinimi karşılanmıştır. Ardından bu çevrim bir milyon defa tekrarlanarak elde edilen sayılar(bitler) NIST testine tabi tutulmuş ve başarı ile testlerden geçtiği görülmüştür [35]. Son aşamada kaos tabanlı karmaşık yapıya sahip, RNG tasarımı ile rasgeliliği arttırılmış ve ayrıca NIST-800-22 testlerinden başarı ile geçmiş olan bit dizileri Şekil 3 deki matematiksel model ile şifre üretecek bir algoritmaya dönüştürülmüştür. Burada elde edilen şifrelerin oluştukları bitlerin haricinde kalan bitlerin atılması, ayrıca Kaos tabanlı denklemdeki diğer durum değişkenlerinin hiç kullanılmaması; şifre üretme algoritmasını tek yönlü ve geriye dönük olarak tahmin edilemez kılmaktadır. Kaotik devrelerin kendilerine özgün hassas yapıları göz önüne alındığında; başlangıç şartlarındaki ufak değişiklikler ile farklı değerlere sahip şifrematik tasarımları da mümkün olmaktadır.

2.2. NIST-800-22 Testleri ve Ap Kaotik Sistemin NIST-800-22. Test Sonuçları
(Nist-800-22 Tests and Nist Test Results of AP Chaotic System)

NIST-800-22 testlerinde bulunan testler rastgele üreteçler tarafından üretilen verilerin rastgelelik ölçüsünün belirlenebilmesi amacıyla geliştirilmiş istatistiksel testlerdir. Uluslararası düzeyde kabul görmüş olan NIST-800-22 testi, 15 farklı testi içermekte ve bit dizileri güçlü bir şekilde

testlere tabi tutulmaktadır. Bit dizisinin başarılı sayılabilmesi için 16 testin tamamından başarıyla geçmesi gerekmektedir [38]. Frekans testi, akış testi, ayrık fourier dönüşüm testi, yaklaşık entropi testi, birikimli toplamlar testi, rastgele gezinimler testi, örtüşen şablon eşleştirme testi: bu testlerden bazılarıdır ve açıklamaları aşağıda verildiği gibidir.

Frekans testi: Rastgele bit dizisinin içindeki 0 ve 1 değerlerinin sayısını tespit eden testtir. Bu değerlerin birbirine yakın olması gerekmektedir. Bu test sonucu diğer tüm testleri etkilemekte ve dizinin rassalığı hakkında önemli bilgi vermektedir. Frekans testi için gerekli denklem Eş. 6'da verilmiştir.

$$\text{p-value}=\text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) \quad (6)$$

Akış testi: Rastgele bit dizisindeki 0 ve 1 bloklarının uzunlukları analiz edilmektedir. Akış testindeki sonucun hesaplanmasında kullanılan denklem Eş. 7'de verildiği gibidir.

$$\text{p-value}=\text{erfc}\left(\frac{|V_n(obs)-2n\pi(1-\pi)|}{2\sqrt{2n}\pi(1-\pi)}\right) \quad (7)$$

Ayrık Fourier dönüşüm testi: Rastgele bit dizisinin fourier dönüşümü elde edilerek, elde edilen sonuçların genlik değerlerindeki periyodiklik sınaması gerçekleştirilmektedir.

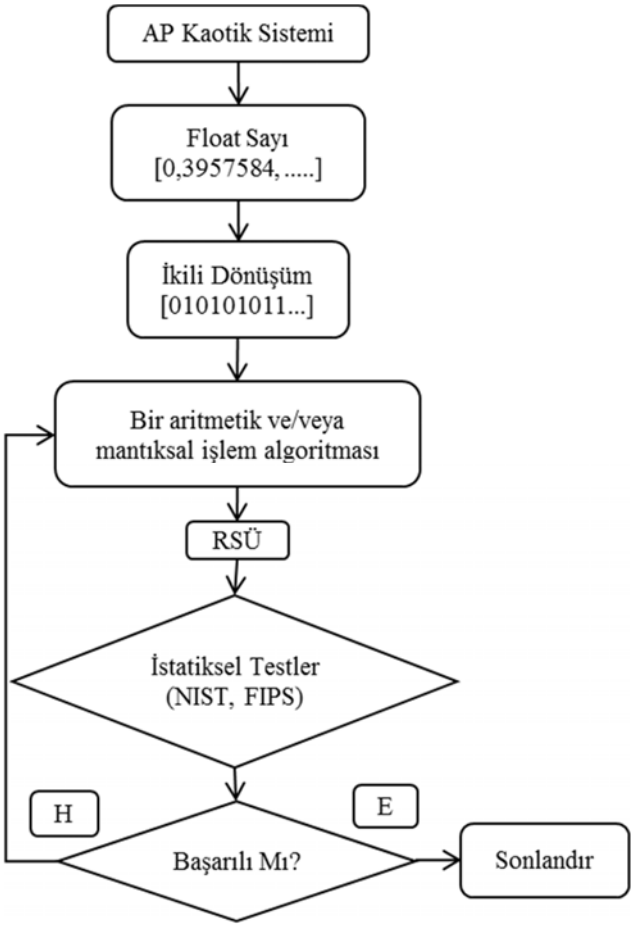
Yaklaşık entropi testi: Rastgele bir dizisi içinde yer alan (m) ve (m+1) bitlik katarların entropi değerlerini analiz etmektedir.

Birikimli toplamlar testi: Bu testte, bit dizisi üzerinde ardışık uzunlukta bloklar oluşturularak, bu bloklar üzerinde 1 ve 0 değerlerinin frekansı belirlendikten sonra, bloklar arası dengesizlik değerleri karşılaştırılmaktadır.

Rastgele gezinimler testi: Bu testte, birikimli toplamlar testinde olduğu gibi bloklara ayırma ve 0-1 dengesi belirlendikten sonra, blokların dengesizlik dağılımı yerine denge dağılımı incelenmektedir.

Örtüşen şablon eşleştirme testi: Bu testtede örtüşmeyen şablon testinde olduğu gibi belirlenen m boyutlu bir dizinin bulunup bulunmadığı test edilir. Fakat aranılan bloğun bulunması veya bulunamaması durumunda rastgele bit dizisi üzerinde bit kaydırma işlemi ile arama işlemine devam edilmektedir.

NIST testlerinde her biri rastgele olduğu varsayılan verilerin, farklı istatistikî yöntemlerle incelenerek hipotezin karara bağlanmasını sağlamaktadır. İstatistiksel hipotez testleri, rastgele sayı üreteçlerinin ürettiği sayı dizilerine uygulanan istatistiksel testlerin sonuçlarını yorumlamak amacıyla kullanılmaktadır. Hipotez testlerinde öncelikle bir sıfır hipotezi (H_0) öne sürülür. Bu hipotezin tersi ise alternatif hipotez (H_a) olarak adlandırılmaktadır. H_0 hipotezi, üzerinde istatistiksel testler yapılan verilerin rastgele olduğu, Ha hipotezi ise üzerinde istatistiksel testler yapılan verilerin rastgele olmadığı anlamına gelmektedir [39]. Her istatistiksel testte, öne sürülen hipotez için bir test istatistik P-değeri hesaplanır. P-değeri teste tabi tutulan rastgele dizilerin rastgeleliğinin bir ölçütü olarak kabul edilmektedir. P-değeri gerçekten rastgele bir dizi için 1'e yakın, bunun tersi durumunda ise P-değeri 0'a yakın olmaktadır. Bu değere göre hipotez kabul edilmekte veya reddedilmektedir. Her istatistiksel test için bir α önem seviyesi (significance level) belirlenmektedir. P-değeri ≥ α ise H_0 hipotezi kabul edilmekte diğer bir deyişle üzerinde rastgelelik testi yapılan verilerin rastgele olduğu anlamına gelmektedir. P-değeri < α ise H_0 hipotezi reddedilir. Bir diğer deyişle verilerin rastgele olmadığı anlamına gelmektedir. Genellikle önem seviyesi değeri 0,01<α<0,001 aralığındadır. Eğer α=0,01 için P-değeri ≥ α ise H_0 hipotezi kabul edilerek üzerinde rastgelelik testi yapılan verilerin %99 doğrulukta rastgele olduğu kararına varılmaktadır. Eğer α=0,001 için P-değeri ≥ α ise H_0 hipotezi kabul edilerek üzerinde rastgelelik testi yapılan verilerin %99,9 doğrulukta rastgele olduğu kararı verilmektedir. Yapılan bu makale çalışmasında P-değeri=0,001 olarak alınmaktadır [7].



Şekil 1. Kaotik sistemler ile rastgele sayı üretimi
(Chaos based random number generation)

AP Kaotik Sistemi'nce üretilen rastgele sayıların, güvenlik açısından şifreleme çalışmalarında kullanılabileceğini göstermek için yapılan NIST-800-22 testleri ve sonuçları

Tablo 3'de verilmiştir. AP Kaotik Sistemi'nin bu testlerden başarı ile geçtiği görülmüştür.

Tablo 3. NIST-800-22 Testleri (NIST-800-22 tests)

İstatistiksel Testler	P-değeri	Sonuç
Frequency (Monobit) Test	0,5850	Başarılı
Block-Frequency Test	0,4921	Başarılı
Cumulative-Sums Test	0,7486	Başarılı
Runs Test	0,7858	Başarılı
Longest-Run Test	0,5146	Başarılı
Binary Matrix Rank Test	0,8459	Başarılı
Discrete Fourier Transform Test	0,5772	Başarılı
Non-Overlapping Templates Test	0,0114	Başarılı
Overlapping Templates Test	0,1298	Başarılı
Maurer's Universal Statistical Test	0,6092	Başarılı
Approximate Entropy Test	0,0409	Başarılı
Random-Excursions Test	0,9727	Başarılı
Random-Excursions Variant Test	0,4973	Başarılı
Serial Test-1	0,2679	Başarılı
Serial Test-2	0,5038	Başarılı
Linear-Complexity Test	0,0881	Başarılı

3. ŞİFREMATİK TASARIMI VE UYGULAMASI (DESIGN AND APPLICATION OF AUTHENTICATOR)

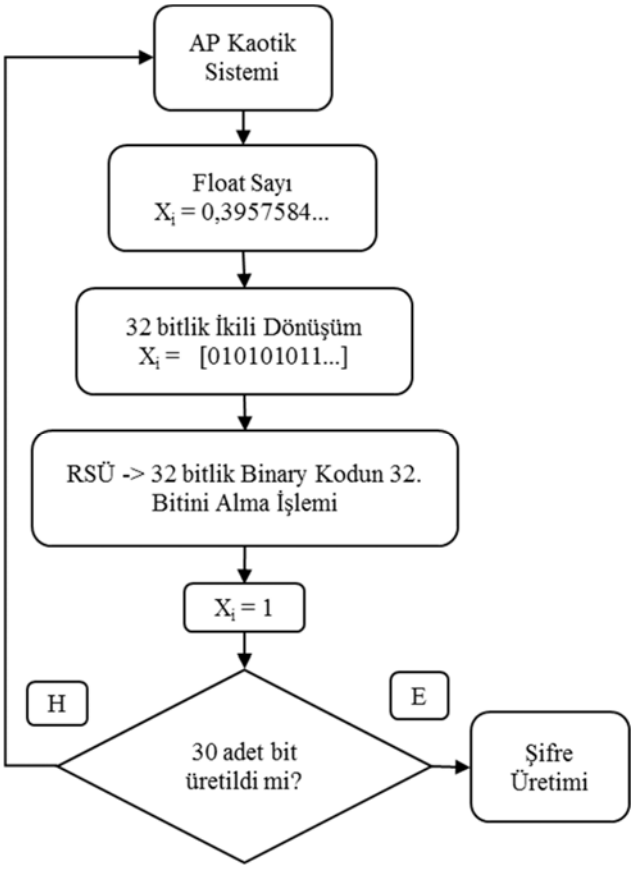
3.1. Gömülü Sistemler (Embedded Systems)

Gömülü sistemler, belirli bir fonksiyonu yerine getirmek üzere tasarlanmış yazılım ve donanım kombinasyoları olup, içinde bulunduğu sisteme karar verme yetisini kazandırmak üzere, çeşitli donanımlar vasıtasıyla yazılımsal olarak progamlanıp, bu program neticesinde sistemin üreteceği çıktıyı çeşitli şekillerde (ses, görüntü, gerilim vb…) dış birime aktaran sistemlerdir. Günlük yaşantımızda kullandığımız eşyalarımızın hemen hemen hepsinde bu sistemleri görmek mümkündür. Bilgisayar, yazıcı, tarayıcı, hesap makinesi, cep telefonu, televizyon, fotoğraf makinesi, bulaşık makinesi, buzdolabı, elektronik oyuncaklar, araçlar vb. alanlarda sıkça kullanılmaktadırlar.

Gömülü sistemlerdeki yazılımlar genel olarak gerçek zamanlı çalışırlar. Tasarım olarak uzun soluklu çalışmak üzere ve hata yapmayacak şekilde programlanırlar. Ancak kullanılan sistemin kalitesine bağlı olmakla beraber çevresel koşullardan etkilenmeleri mümkündür. Sistemin çevresel koşullardan etkilenip, kilitlenme durumlarına karşın genelde reset olarak ifade edilen bir düğme ile ilk programlandığı yapısına geri dönmesi sağlanabilir. Düşük maliyet, düşük enerji tüketimi, çoğunlukla taşınabilir yapıda olmaları ve az yer kaplayan hacimleri nedeniyle elektronik dünyasında sıkça tercih edilmektedirler. Bu çalışmadaki şifrematik cihaz tasarımı, ARM mimarisine sahip Cortex-M4 işlemcisi içeren STM32F407VG isimli mikrodenetleyici ile gerçekleştirilmiştir. Mikrodenetleyicinin yazılımsal olarak programlanmasında C dili kullanılmıştır. Programlamanın tamamlanmasıyla birlikte yapılan yazılım, "mikroProg" isimli bir uygulama ile mikrodenetleyicinin içerisine yüklenmiştir.

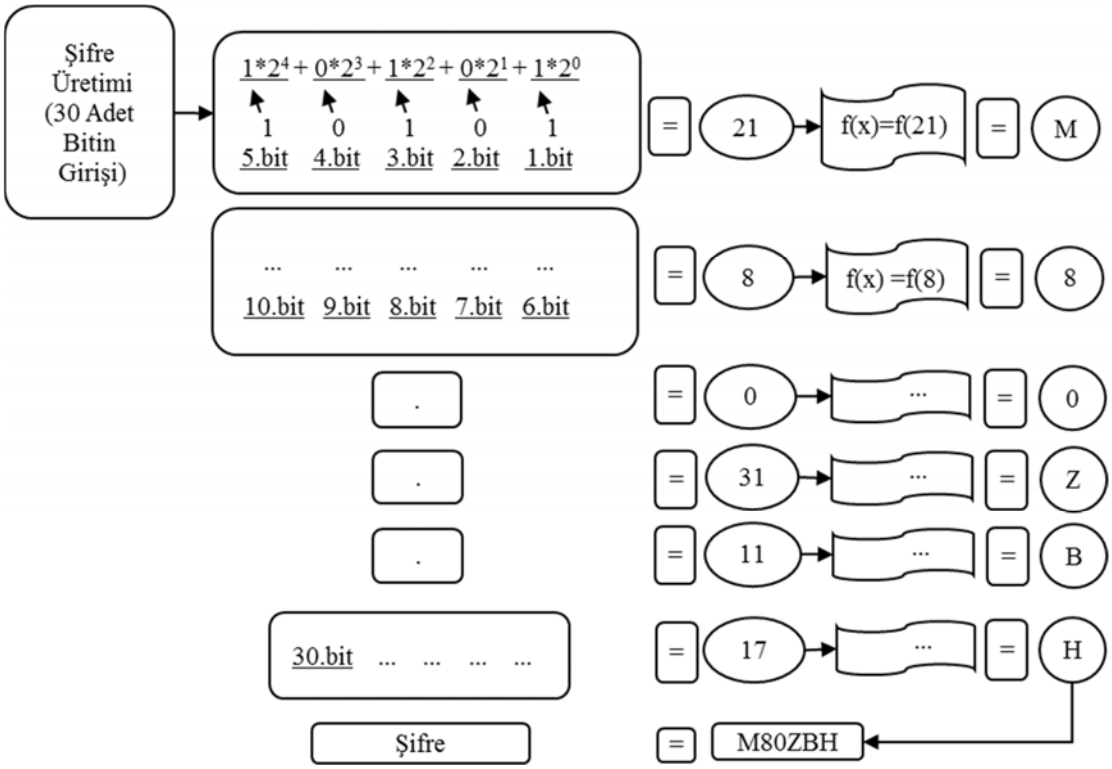
3.2. Rsü Tabanlı Şifre Üretimi ve Cihaz Tasarımı (Password Generator Based Rng and Device Design)

İstatiksel testlerden geçmiş olan Rsü tabanlı bitlerden elde edilen bitlerin akış diyagramı şekil 2'de verildiği gibidir. Bu akış diyagramında elde edilen bitler şekil 3' de verildiği gibi, bir algoritma yardımıyla şifrelere dönüştürülmektedir. Şifre üretme aşamasında öncelikle, RK-4 algoritmasının 30 çevrim boyunca çalışması ile 30 adet '1' ve '0'lardan oluşan bitler elde edilmektedir. Bu bitlerden aşağıda verilen akış yardımı yardımıyla şifreler üretilmektedir. Burada işlemler sonucu elde edilen sayıların karakter karşılıkları şifrelerin hanelerini oluşturmaktadır. Hangi sayının hangi karaktere ait olduğunu gösteren eşleştirme işlemi Tablo 4'de verilmiştir.



Şekil 2. Bitlerin elde edilmesi (Obtaining bits)

Şifrematik cihaz tasarımının elektronik olarak gerçeklenmesi için arm mimarisine sahip Cortex-M4 işlemcili STM32F407VG discovery kartı kullanılmıştır. Şifrelerin görüntülenmesini sağlamak için ise 2x16 LCD ekran kullanılmıştır. LCD ekran parlaklığını ayarlamak için de 1K ohm pots kullanılmıştır. Sonraki şifrelerin gösterimini gerçekleştirmek için kart üzerindeki buton kullanılmıştır. Besleme gerilimi 5V olarak ayarlanmıştır. Şekil 4'de şifrematik cihazının elektronik devre tasarımı görülmektedir.



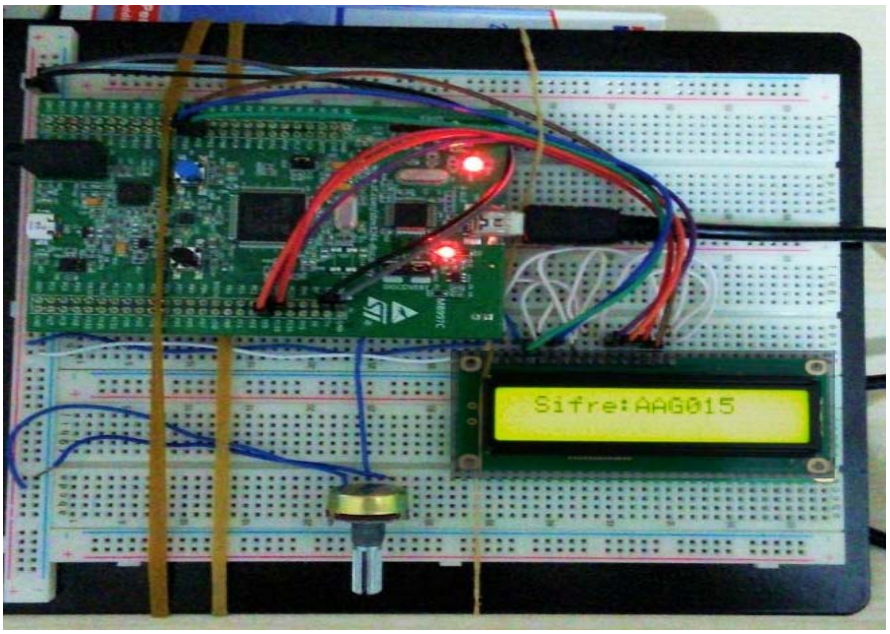
Şekil 3. Şifre üretme akış diyagramı (Password generation flow diagram)

Tablo 4. Onlu ve ikili tabandaki sayıların karakter karşılıkları (Character equivalents of numbers in decimal and binary)

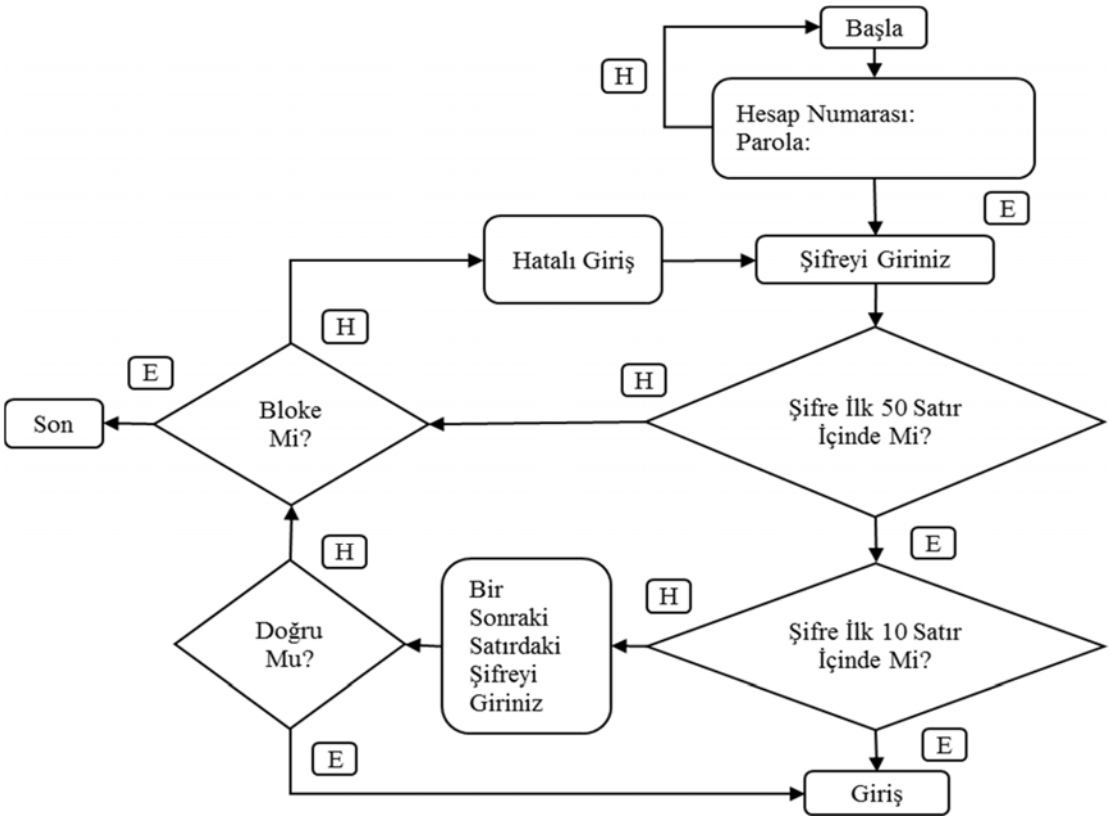
Onluk Tabandaki Değer	Bit Karşılığı	Karakter Karşılığı	Onluk Tabandaki Değer	Bit Karşılığı	Karakter Karşılığı
0	0	0	16	10000	G
1	1	1	17	10001	H
2	10	2	18	10010	J
3	11	3	19	10011	K
4	100	4	20	10100	L
5	101	5	21	10101	M
6	110	6	22	10110	N
7	111	7	23	10111	O
8	1000	8	24	11000	P
9	1001	9	25	11001	R
10	1010	A	26	11010	S
11	1011	B	27	11011	T
12	1100	C	28	11100	U
13	1101	D	29	11101	V
14	1110	E	30	11110	Y
15	1111	F	31	11111	Z

3.3. Kullanıcı Arayüz Ekran Tasarımı
(User Interface Screen Design)

Geliştirilen şifrematik cihazının test edilebilmesi amacıyla, örnek bir internet bankacılığı kullanıcı arayüz ekranı tasarlanmıştır. Bu arayüz ekranları mobil bankacılıkta genelde IOS ve Android tabanlı uygulamalar ile yönetilirken, ağ (web) bankacılığında Asp.Net ya da Php tabanlı sunucular tarafından yönetilmektedir. Arayüz programına ait akış diyagramı Şekil 5'de verildiği gibidir. Eşleştirme işlemi için, daha önceden AP kaotik sistemi yardımı ile üretilen şifreler sunucunun veri tabanına kayıt edilmiştir. Şifrematik



Şekil 4. Şifrematik cihazının elektronik devre tasarımı (Electronic circuit design of authenticator device)



Şekil 5. Arayüz programına ait akış diyagramı (Flow diagram of the interface program)

Şekil 6. Örnek bir internet bankacılığı ekranı (A sample internet banking screen)

cihazındaki şifrelerde algoritma gereği buradaki belli bir sıra ile şifre üretmektedir. Cihaz tarafından üretilen şifreler ile sisteme giriş yapılmak istendiğinde sistem kullanıcıdan örneğin ilk 10 adet şifrenin girilmesini beklemektedir. Bu aralık için giriş sağlanmakta aksi halde giriş yapılamamaktadır. Bu süreç mükerrer hatalı giriş, bloke olma, şifrematik cihazınca üretilip sisteme giriş yapılmayan şifre üretimi gibi durumlarda sistemin nasıl davranması gerektiği modellenmiştir. Eşleştirme ile ilgili detaylı gösterimler aşağıdaki akış diyagramlarında verildiği gibidir. Şekil 6'da örnek internet bankaclığı ekranı verilmektedir.

4. SONUÇLAR (CONCLUSION)

Bu makale çalşmasında, uluslararası en üst standart olan NIST-800-22 istatistiksel testinden başarıyla geçmiş, AP kaotik sistemi ile yeni bir şifre üretme algoritması tasarlanarak, fiziksel ve sanal ortamlarda uygulamaları gerçekleştirilmiştir. Şifrematik cihazınca üretilen otuz bin adet şifrenin birbirleri arasında benzerlik testleri yapıldığında; %99,9933 farklı oldukları görülmüştür. Literatürde böyle bir değerlendirmeye rastlanılmamakla birlikte sadece FIPS testi yapılan ARM cihazı için paylaşılan başarı oranı %99 olarak görülmektedir. Şifrematik cihazının gerçek hayatta uygulanabilirliğini test etmek amacıyla örnek bir kullanıcı arayüz programı tasarlanarak uygulanabilirliği gösterilmiştir. İstenildiği takdirde gerçeklenen tasarım FPGA, DSP ve farklı mikrodenetleyiciler üzerinde de çalıştırılabilmektedir.

Teknolojinin hızla gelişmesiyle birlikte, mobil çözümlerin en etkili tasarım alanı olan cep telefonlarının gizlilik ve güvenlik açısından casus yazılımlara açık olması, mobil bankacılık ve internet bankacılığının çeşitli riskler altında olduğunu doğrulamaktadır. Ayrıca müşteri ile banka arasındaki köprünün, üçüncü kişi olarak GSM operatörlerince kurulması da güvenlik zaafiyetine neden olmaktadır. Bu nedenlerle çeşitli riskler göze önünde alındığında, şifrematik cihazının bireysel kullanıcı ve küçük ölçekli işletmelerden ziyade, özellikle çok sayıda mobil, web ve uzak masaüstü erişim hizmeti abonesi veya müşterisi bulunan büyük ölçekli hizmet sağlayıcı şirketlerce kullanılması önemli bir güvenlik gereksinimini sağlamış olacaktır.

KAYNAKLAR (REFERENCES)

1. Tuna M., Fidan C. B., A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems. Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (2), 473-491, 2018.
2. Pehlivan İ., Yeni Kaotik Sistemler: Elektronik Devre Gerçeklemeleri, Senkronizasyon ve Güvenli Haberleşme Uygulamaları, Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya, 2007.
3. Beirami A., Nejati H., Ali WH., zigzag map: a variability-aware discrete-time chaotic-map truly random number generator. electronics lett., 48 (24):1537-1538, 2012.
4. Zhao L., Liao X., Xiao D., Xiang T., Zhou Q., Duan S., TRNG from mobile telephone photo based on chaotic cryptography. chaos, solitons & fract., elsevier, 42 (3):1692-1699, 2009.
5. Ergün S., Özoğuz S., TRNGs based on a non-autonomous chaotic oscillator. Int. J. of Electronics and Comm., 61 (4):235-242, 2007.
6. Li Q., Liu Q., Niu J., Chaotic oscillator with potentials in TRNG and ADC. 35th Int. Conf. on Telecomm. and Signal Proc., 397-400, 3-4 July, 2012.

7. Koyuncu İ., Kriptolojik Uygulamalar İçin Fpga Tabanlı Yeni Kaotik Osilatörlerin ve Gerçek Rastgele Sayı Üreteçlerinin Tasarımı Ve Gerçeklenmesi. Doktora Tezi, Sakarya Üniversitesi, , Fen Bilimleri Enstitüsü, Sakarya, 2014.

8. Akgul A., Moroz I., Pehlivan I., Vaidyanathan S., A new four-scroll chaotic attractor and its engineering applications. Optik-International Journal for Light and Electron Optics, 127 (13), 5491-5499, 2016.

9. Akgül A., Calgan H., Koyuncu İ., Pehlivan İ., İstanbullu A., (2016). Chaos-based engineering applications with a 3D chaotic system without equilibrium points. Nonlinear Dynamics, 84 (2), 481-495, 2016.

10. Akgul A., Li C., Pehlivan İ., Amplitude Control Analysis of a Four-Wing Chaotic Attractor, its Electronic Circuit Designs and Microcontroller-Based Random Number Generator. Journal of Circuits, Systems and Computers, 1750190, 2017.

11. Wang Z., Akgül A., Pham V. T., Jafari S., Chaos-based application of a novel no-equilibrium chaotic system with coexisting attractors. Nonlinear Dynamics, 1-11, 2017.

12. Çavuşoğlu Ü., Uyaroğlu Y., Pehlivan İ., Design of a continuous-time autonomous chaotic circuit and application of signal masking. Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (1), 79-87, 2014.

13. Volos C., Akgül A., Pham V.T., Stouboulos I., Kyprianidis I., A simple chaotic circuit with a hyperbolic sine function and its use in a sound encryption scheme. Nonlinear Dynamics, 1-15, 2017.

14. Jafari M. A., Mliki E., Akgül A., Pham V. T., Kingni S. T., Wang X., Jafari, S., Chameleon: the most hidden chaotic flow. Nonlinear Dynamics, 1-15, 2017.

15. Çavuşoğlu Ü., Akgül A., Kaçar S., Pehlivan İ., Zengin A., A novel chaos-based encryption algorithm over TCP data packet for secure communication. Security and Communication Networks, 2016.

16. Wieczorek PZ., Golofit K., Dual-metastability time-competitive TRNG. IEEE Trans. on Circuits and Syst., 61 (1):134-145, 2014.

17. Fischer V., Drutavosky M., Simka M., Bochard N., High performance TRNG in sltera stratix FPLDs.Field Program. Logic and App., Springer, 555–564, 2004.

18. Istvan H., Suciu A., Cret, O., FPGA based TRNG using automatic calibration. Intelligent Comp. Comm. and Proc., IEEE 5th Int. Conf. on ICCP, 373-376, 2009.

19. Çicek İ., Pusane AE., Dundar G., A novel design method for discrete time chaos based true random number generators. Integration, the VLSI Journal, 47 (1), 38-47, 2014.

20. Çicek İ., Pusane AE., Dundar G., A novel dual entropy core TRNG. IEEE 8th Int. Conf. on Elec. and Electronics Eng., 332-335, 2013.

21. Pareschi F., Setti G., Rovatti R., Implementation and testing of high-speed CMOS TRNGs based on chaotic systems, IEEE Trans. on Circuits and Syst., 57 (12), 3124-3137, 2010.

22. Callegari S., Rovatti R., Setti G., Embeddable ADC-Based True Random Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos, IEEE Trans. On Signal Processing, 53 (2),793-805, 2005.

23. Pareschi F., Setti G., Rovatti R., A macro-model for the efficient simulation of an ADC-based RNG, Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on , 5, 4349-4352, 2005.

24. Yıldırım K., & Demiray H. E., Methods for integrating symmetric and asymmetric encryption schemes: Scrambled and combined kem-dem. Journal of the Faculty of Engineering and Architecture of Gazi University, 23 (3), 539-548, 2008.

25. Özdemir S., Secure data aggregation in wireless sensor networks via homomorphic encryption. Journal of the Faculty of Engineering and Architecture of Gazi University, 23 (2), 365- 373, 2008.

26. Akkaya S., Yeni bir kaos tabanlı rastgele sayı üreteci kullanan banka şifrematik cihazı tasarımı ve uygulaması. Yüksek Lisans Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya, 2016.

27. Türk Ö., ARM işlemciler ile tek kullanımlık şifre uygulamasının gerçekleştirilmesi. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ, 2011.

28. Açıkkapı M. Ş., Mobil aygıtlar için tek kullanımlık şifre üretilmesi ve güvenliğinin sınanması. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ, 2011.

29. STM32F405xx/07xx, STM32F415xx/17xx, STM32F42xxx and STM32F43xxx advanced ARM®-based 32-bit MCUs. Reference manual.www.st.com.

30. Karapantelakis A., Niclas J., and Anna V., Methods and user device and authenticator device for authentication of the user device. U.S. Patent Application No. 15/559,854.

31. Bhole A. T., Chaudhari S. Web Based Security using Online Password Authentication in Mobile Application, International Journal of Science and Research (IJSR), 2319-7064, 2, 74-77, Haziran, 2013.

32. Srinivasa K., Janakib V., A Novel Approach For Generation Of OTP'S Using Image's, Procedia Computer Science 85, 511-518, December, 2016.

33. Zhengxing H., Wei D., Huilong D., Haomin L., Similarity measure between patient traces for clinical pathway analysis: problem, method, and applications. IEEE J. of Biomedical and Health Inf., 18 (1), 4-14, 2014.

34. Akgül A., Pehlivan İ., A New Three-Dimensional Chaotic System Without Equilibrium Points, Its Dynamical Analyses And Electronic Circuit Application. Technical Gazette, 23 (1), 209-214, 2016.

35. Akgül A., Yeni Kaotik Sistemler ile Rastgele Sayı Üreteci Tasarımı ve Çoklu-Ortam Verilerinin Yüksek Güvenlikli Şifrelenmesi. Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya, 2015.

36. Özsoy M., Mobil telefonda üretilen tkş ile rastlantısal değişken ve konumsal bazlı kimlik doğrulama. Yüksek Lisans Tezi, Gazi Üniversitesi, Bilişim Enstitüsü, Ankara, 2013.

37. Yakut S., Tek kullanımlık şifre üreteci. Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ 2014.

38. National institute of stand. and tech.. A statistical test suite for random and pseudo RNGs for cryptographic applications NIST- 800-22. http://csrc.nist.gov/-publications/nistpubs/800-22-rev1a/SP800-22rev1a.pdf. Yayınlanma tarihi 2001. Güncellenme tarihi Nisan 2010. Erişim tarihi Ocak 17, 2017.

39. Yayık A., Kutlu Y., Improving PNRG using artificial neural networks. The Institute of Electrical and Electronics Engineers (IEEE) 21st Signal Processing and Comm. App. Conf., 1-4, 2013.