T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KİMYASAL REAKSİYONLARLA GERÇEK RASTGELE SAYI ÜRETME

Tuncay GENÇ

Yüksek Lisans Tezi

EKOBİLİŞİM ANABİLİM DALI

TEMMUZ 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ekobilişim Anabilim Dalı

Yüksek Lisans Tezi

KİMYASAL REAKSİYONLARLA GERÇEK RASTGELE SAYI ÜRETME

Tez Yazarı
Tuncay GENÇ

Danışman
Doç. Dr. Muharrem Tuncay GENÇOĞLU

TEMMUZ 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Ekobilişim Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Kimyasal Reaksiyonlarla Gerçek Rastgele Sayı Üretme
Yazarı:	Tuncay GENÇ
İlk Teslim Tarihi:	01.06.2022
Savunma Tarihi:	01.07.2022

TEZ ONAYI

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir.

		İmza	
Danışman:	Doç. Dr. Muharrem Tuncay GENÇOĞLU Fırat Üniversitesi, Teknik Bilimler MYO		Onayladım
Başkan:	Doç. Dr. Fatih ÖZKAYNAK Fırat Üniversitesi, Teknoloji Fakültesi		Onayladım
Üye:	Dr. Öğr. Üyesi Selman YAKUT İnönü Üniversitesi Mühendislik Fakültesi		Onayladım

Bu tez, Enstitü Yönetim Kurulunun ...../...../20..... tarihli toplantısında tescillenmiştir.

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım "Kimyasal Reaksiyonlarla Gerçek Rastgele Sayı Üretme" Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

01.07.2022

Tuncay GENÇ

ÖNSÖZ

Yüksek Lisans çalışmamı yapabilmem için, çalışmalarımı destekleyen ve yönlendiren değerli hocam ve danışmanım Doç. Dr. Muharrem Tuncay GENÇOĞLU'na,

Yardımlarını esirgemeyen Gökhan DEMİR ve İbrahim Eren SEYHAN'a,

Dualarını eksik etmeyen aileme,

Ve tez çalışmam sırasında bana desteği ve katkılarından dolayı çok kıymetli eşim Ezgi GENÇ'e teşekkürlerimi sunarım.

Bu tez çalışması, TÜBİTAK tarafından 121E323 protokol numaralı proje ile desteklenmiştir.

Tuncay GENÇ
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Kimyasal Reaksiyonlarla Gerçek Rastgele Sayı Üretme

Tuncay GENÇ

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Ekobilişim Anabilim Dalı

Temmuz 2022, Sayfa: x + 24

Rastgelelik şans oyunları, istatistik hesaplamaları, bilgisayar simülasyonları, bilgi güvenliği ve şifreleme gibi içerisinde rastgele olayların yaşandığı her türlü uygulamada kullanılmaktadır. Rastgele sayıları üretmek için kullanılan araçlara rastgele sayı üreteçleri (RSÜ) adı verilir. RSÜ, aralarında herhangi bir örüntü veya ilişki olmayacak şekilde tahmin edilemeyecek sayı dizileri üretilmesini sağlayan yazılımsal veya donanımsal bileşenlerdir. RSÜ ile ilgili farklı tekniklerle çeşitli çalışmalar yapılmıştır. Bu çalışmalarda rastgele sayı üretiminin zorlukları ve maliyetin yüksek olması geliştirilen üreteçlerin verimliliğini olumsuz etkilemektedir. Gerçek rastgele sayı üretiminde çok farklı yöntemler kullanılmış hatta tahmin edilebilirliği zorlaştırmak için radyoaktif rastgele sayı üreteçleri (kuantum rastgele sayı üreteci) dahi geliştirilmiştir. Kuantum Rastgele Sayı Üreteçleri (KRSÜ); klasik fizik yerine Kuantum fiziği yasalarının temel alındığı bir üreteç çeşididir.

Fotonik tabanlı KRSÜ'de fotonların belirsizliğinden faydalanılarak çeşitli yazılımsal ve donanımsal işlemlerden sonra rastgele sayılar üretilir. Üretilen bu sayılar, tahmin edilemeyecek seviyede güçlü rastgele sayılardır. Ancak bu yöntemin hem insan sağlığı hem de maliyet açısından olumsuzlukları mevcuttur. Bu çalışmada, özellikle radyoaktif rastgele sayı üreteçlerine alternatif olacak ve maliyeti düşürmek adına daha önce çalışılmamış olan kimyasal reaksiyonlar kullanılarak gerçek rastgele sayı üreteci geliştirilmesi amaçlanmıştır.

Donanımsal kaynaklar ve kimyasal reaksiyonlar birlikte kullanılarak gerçek rastgele sayılar üretilecektir. Bu üreteç geliştirilirken öncelikle bitki tohumu çimlendirilecektir. Sensörler ve diğer donanım elemanlarının (Kütle ölçer, nem ve sıcaklık ölçer gibi) ortak kullanımıyla veri üretilmiş, üretilen değerler tohum değeri olarak alınıp rastgele sayı üretmede kullanacağımız algoritmaya girdi olarak kullanılarak gerçek rastgele sayılar üretilmiş ve bu sayılar bilinen test yöntemleriyle detaylı olarak test edilmiştir.

Anahtar Kelimeler: Kimyasal Reaksiyon, Rastgele Sayı Üreteci, Gerçek Rastgele Sayı Üreteci.

ABSTRACT

Real Random Number Generation By Chemical Reactions

Tuncay GENÇ

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Eco-informatics

July 2022, Pages: x + 24

Randomness is used in all kinds of applications in which random events occur, such as games of chance, statistical calculations, computer simulations, information security and encryption. The tools used to generate random numbers are called random number generators (RSU). RSU are software or hardware components that enable the generation of unpredictable number sequences without any pattern or relationship between them. Various studies have been carried out with different techniques related to RSU. In these studies, the difficulties of random number generation and the high cost negatively affect the efficiency of the developed generators. Many different methods have been used in real random number generation, and even radioactive random number generators (quantum random number generator) have been developed to make predictability difficult.

Quantum Random Number Generators (KRSÜ); It is a type of generator based on the laws of quantum physics instead of classical physics. In photonics-based KRSÜ, random numbers are generated after various software and hardware processes by utilizing the uncertainty of photons. These generated numbers are unpredictably strong random numbers. However, this method has disadvantages in terms of both human health and cost. In this study, it is aimed to develop a real random number generator, which will be an alternative to radioactive random number generators and by using chemical reactions that have not been studied before in order to reduce the cost.

By using hardware resources and chemical reactions together, true random numbers will be generated. While developing this generator, first of all, plant seed will be germinated. With the common use of sensors and other hardware elements (such as mass meter, humidity and temperature meter), data was produced, real random numbers were produced by taking the values produced as seed values and using them as inputs to the algorithm we will use to generate random numbers, and these numbers were tested in detail with known test methods.

Keywords: Chemical Reaction, Random Number Generator, True Random Number Generator.

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Kısaltmalar

GRSÜ	: Gerçek Rastgele Sayı Üreteçleri
MEMS	: Mikro Elektromekanik Sistem
RFID	: Radyo Frekansı ile Tanımlama Teknolojisi
RS	: Rastgele Sayı
AES	: Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
SRSÜ	: Sözde Rastgele Sayı Üreteçleri
WISP RFID	: Kablosuz Kimlik Ve Algılama Platformu Radyo Frekansı ile Tanımlama Teknolojisi

1. GİRİŞ

Rastgele sayı (RS), üyeleri belli olan dizi içerisindeki elemanların matematiksel olarak düzgün bir biçimde dağılım yaparak, daha önceki seçimlerden yeni seçimlerin tahmininde bulunulmayacak şekilde elde ettiğimiz sayıdır [1].

Dalga denklemi fizik de çok önemli bir yere sahip olan kısmi difarensiyel denklemdir. Bu denklemin çözümlerinden ses, ışık ve su dalgalarının hareketlerini betimleyen fiziksel nicelikler çıkar. Oldukça geniş kullanım alanına sahip olan dalga denklemleri son yıllarda kriptografide de kullanılmaya başlamıştır [2].

1.1. RASTGELE SAYI ÜRETEÇLERİ

Rastgele kelimesi; gelişigüzel, düzensiz, nedeni olmayan, öngörülemeyen, tesadüf gibi anlamlara sahiptir. Bir dizi tesadüfi olayın art arda gelmesi rastgele süreçleri oluşturur. Bu durum bilimsel olarak ifade edilmek istenirse, rastgele bir süreçten elde edilen çıktılar arasında determinist ve matematiksel olarak ifade edilebilen bir irtibat bulunmaz [3].

1.1.1. Rastgele Sayı Üretecinin Tarihsel Gelişimi

Rastgele sayıların tarihi çok eskilere uzanmaktadır. Zar, bozuk para ve diğer aletler rastgele seçimler ve şans oyunlarında rastgele sayılar üretmek için uzun zaman önce kullanılmıştır. İran, Irak, Hindistan, Çin ve Mısır'da 4000-5000 yıllık zarlar bulunmuştur. Bulunduğu dönemde zarlar miras paylaşımı, başkanlık seçimi gibi önemli kararların alınmasında kullanılmıştır. Zarların yanı sıra kağıt oyunları, madeni paralar, döner tekerlekler vb. nesneler de erken dönem rastgele sayı üreteçleri olarak kullanılmıştır.

Rastgele sayıların ileriki zamanlarında kriptolojide Vernam şifreleme sistemi olarak isimlendirilen exclusive OR (XOR), veri dizisinin anahtarı şeklinde ifade edilen açık metinde (plaintext) gibi rastgele sayı metotları ortaya çıkmıştır. Bu dizi güvenli şifreleme protokolü olarak bilinmektedir. Bu şifreleme protokolünün temel uygulamalarda güvenilirliği sağlaması için her anahtarın (rastgele sayının) sadece bir defa kullanılması ve gerçek rastgele sayı kriterlerini sağlaması gerekmektedir. Bilgisayar tabanlı RSÜ'nün tasarım ve analizi için Knuth bir çalışma yayınlamıştır. Çalışmasında bilgisayar kullanıcılarının farklı uzman kişiler tarafından geliştirilen rastgele sayıları üretmek için oluşturdukları kütüphanelere erişim sorunlarını adreslemiştir. Rastgele sayılarla ilgili çalışma yapan Ripley ise kişisel bilgisayarlar üzerinde yeterli olmayan RSÜ kullanıcı programları ile yer değiştirilmiş üstel, normal ve Poisson dağılımlı diziler içeren metotlar geliştirmiştir. Başka bir çalışmasında Monte Carlo hesaplamaları için sözde rastgele sayı üreteçlerinin kullanımı ile ilgili çalışması olmuştur [4].

1.1.2. Rastgele Sayıların Kullanıldığı Alanlar

Günümüzde rastgele veriler kullanılarak belirli programlar ve bilgisayar aracılığıyla görüntü, desen ve 3 boyutlu cisimler oluşturulur; içeriği sadece alıcının ve vericinin bilmesi gereken güvenli haberleşme uygulamalarında veya sadece kullanıcı tarafından bilinmesi istenen veri gizleme uygulamalarında rastgele sayılar kullanılır [5]. Rastgele sayıların kullanıldığı alanları aşağıdaki gibidir [6-8]:

- Örnekleme,
- Eğlence,
- Modelleme,
- Simülasyon ve test etme,
- Karar verme,
- Kriptografi,
- Bilgisayar oyunları,
- Bilgisayar programlama,
- Elektronik tasarım.

Rastgele sayılar, şifreleme işleminin gizliliği ve güvenilirliği için önemlidir [9, 10] Kriptografik uygulamalar için RSÜ kullanmanın amacı rasgele sayılar üretmektir. Kriptografik rasgele sayıların kullanılması şifreleme gücünü artırır.

1.1.3. Rastgelelik Kaynağı Olarak Kullanılabilecek Durumlar

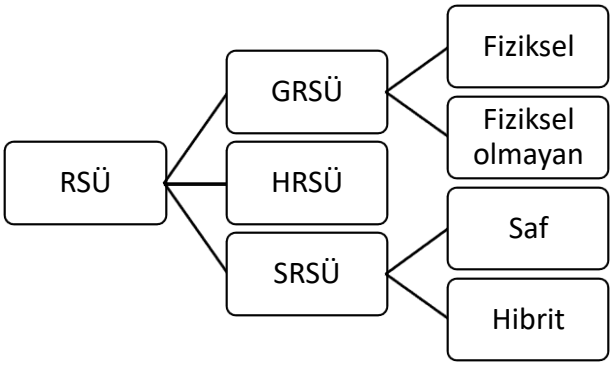
Rastgelelik kaynağı olarak kullanılabilecek durumlar şu şekildedir:

- Radyoaktif bozunma içinde elektrostatik salgılanması boyunca geçen süre
- Direnç veya diyot elemanından kaynaklanan termal gürültü
- Bağımsız çalışan osilatörler arasında parametre kararsızlığı
- Belirli bir süre için yarı iletken kapasitörün şarj süresi
- Sabit diskte hava türbülansı
- Yazılım tabanlı rastgele sayıda bir mikrofondan gelen ses veya bir kameradan gelen görüntü [11].

1.1.4. Rastgele Sayı Üreteçlerinin Sınıflandırılması

Rastgele sayı üretmek için çok sayıda ve farklı yapıda RSÜ bulunmakla birlikte genel olarak üç sınıfa ayırmak mümkündür. Bunlar Sözde Rastgele Sayı Üreteçleri (SRSÜ), Gerçek Rastgele Sayı

Üreteçleri (GRSÜ) ve Hibrit Rastgele Sayı Üreteçleri (HRSÜ) olarak adlandırılır Rastgele sayı üreteçlerinin sınıflandırılması Şekil 1.1'de gösterilmiştir [12]:



Şekil 1.1. Rastgele Sayı Üreteçlerinin Sınıflandırılması

1.1.4.1 Sözde Rastgele Sayı Üreteçleri

Tohum (seed) denilen giriş değerlerini algoritmik yaklaşımlarla genişletilerek çıkışta iyi istatistiksel özelliklere sahip, öğeleri arasında kolay ilinti kurulamayan sayılar üreten üreteçlere sözde rastgele sayı üreteçleri (SRSÜ) denir. GRSÜ'ye göre kolay gerçekleşmesi ve düşük maliyetli olması gibi avantajları vardır. Girdi algoritması bilindiğinde, herhangi bir andaki değere bakılarak sonraki çıktılar tahmin edilebilir. Bu aynı zamanda şifreleme algoritmalarında SRSÜ'nün kullanımını da kısıtlar. Bununla birlikte, kullanılan algoritmalar deterministiktir ve bu nedenle çıktılar istendiği gibi rastgele değildir. Sayısal analiz veya fiziksel süreç modelleme olarak daha düşük istatistiksel kalitenin yeterli olduğu durumlarda tercih edilirler [13]. SRSÜ'de aynı başlangıç şartlarıyla aynı veri dizisi üretilir [14]. Daha çok simülasyon ve modellemede SRSÜ kullanılmaktadır [15].

1.1.4.2 Saf Sözde Rastgele Sayı Üreteçleri

Saf sözde rastgele sayı üreteçleri giriş olarak entropi kaynağından üretilen tohum değerini alan deterministik yöntemler kullanılarak bu tohum değerinden rastgele sayı üretilmesine imkân tanıyan yapılardır. Burada üretilen rastgele sayılar düzgün bir dağılıma sahip olabilir. Bu üreteçler deterministik bir yapıya sahip olduğu için pratik olarak üretilen çıkış değeri girilen tohum değerini geçmesi mümkün değildir. Bunun yanında bu üreteçlerden üretilen diziler belli bir süre sonra kendini tekrar eder daha açık bir ifade ile belirtmek gerekirse bu üreteçler periyodik özellik gösterir [12, 16, 17].

1.1.4.3 Hibrit Sözde Rastgele Sayı Üreteçleri

Hibrit SRSÜ'nün güvenliğini üretece sağlanan ek girdilere dayanır. Ek girdiler, üretilen rastgele sayıların tahmin edilmesini veya hesaplanmasını engellediğinden üreteci güvenli hale getirir. Dolayısıyla bu üreteçlerde kullanılan geçerli iç durum değeri veya ara değerleri elde edilse bile, bu

değerlerin ardıl ve öncül değerleri ek girdiler bilinmeden hasaplanamaz. Güvenli bir GRSÜ'den alınan ek girdilerle güvenlik gereksinimi karşılanır [12].

1.1.4.4 Hibrit Rastgele Sayı Üreteçleri

Hibrit Rastgele Sayı Üreteçleri deterministik yöntemler ve bu yöntemlere sağlanan ek girdilerden oluşur. Deterministik yöntem olarak kaotik sistemler, özet veya şifreleme algoritmaları gibi kriptografik yapılar veya benzeri algoritmalar kullanılabilir. Ek girdiler ise GRSÜ kullanılarak üretilir. Bu üreteçleri oluşturan deterministik yöntemler ve ek girdiler üretecin güvenliği için belirleyici ve önemli iki parametredir. HRSÜ'de deterministik yöntemler olarak kriptografik özet algoritmaları gibi güçlü yapıların kullanılması bu üreteçlerin güvenliğini garanti eder. Bu algoritmaların tek yönlü olması ve çakışmaya karşı dirençli olması, ideal deterministik yapılar olarak kullanılmasını sağlar. Ayrıca bu üreteçler üzerinde yapılan kriptoanaliz çalışmalarıyla üretecin güvenliği tespit edilebilir. Özellikle Keccak gibi kriptografik özet algoritmalarının en son standardının kullanılması bahsedilen güvenlik parametreleri açısından önemlidir. HRSÜ'ye sağlanan ek girdilerle üretilen hibrit rastgele sayı dizilerinin tahmin edilmesi ve yeniden üretilmesi engellenir. Ek girdilerin üretilmesinde entropi kaynağı ring osilatörü yöntemleri ve kaos tabanlı uygulamalar kullanılabilir [12] .

1.1.4.5 Gerçek Rastgele Sayı Üreteçleri

Genel olarak rasgele sayı üretiminde rassal özelliklerini sağlaması gerekmektedir.

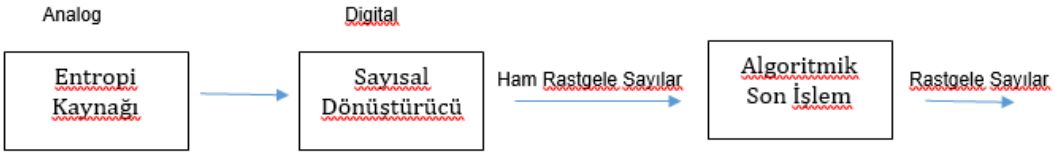
GRSÜ rastgele olduğu bilinen fiziksel bir duruma dayanmaktadır. Genellikle gürültü üreten kaynaklar veya doğada hazır bulunan gürültülü kaynakları bunlara örnek verilebilir. Başka bir deyişle GRSÜ tam olarak aynı koşullarda iki kere çalıştırılırsa bile birbiriyle ilişkisiz iki rastgele sayı dizisi üretir. SRSÜ önceden tahmin edilebilen denklemlere dayanan ve bünyesinde rastgele veri bulunduran, sınırlı durumda ve rastgele veri üretimini kendi işlemcisinde hesaplayan sayı üreteçleridir.

GRSÜ ve SRSÜ arasındaki farklılıklar Tablo 1.1'de gösterilmiştir [15]:

Tablo 1.1. GRSÜ ve SRSÜ Arasındaki Farklılıklar

Rastgele Sayı Üreteçleri	Yeterlik	Deterministlik	Periyodiklik
SRSÜ	Mükemmel	Determinist	Periyodik
GRSÜ	Zayıf	Nondeterminist	Periyodik değil

Şekil 1.2'de gerçek rastgele sayı üretiminin genel bir yapısı görülmektedir.



Şekil 1.2. Gerçek Rastgele Sayı Üreteçlerinin Genel Yapısı

Rastgele sayılar, güvenliğin ön planda olduğu birçok sistemin ve uygulamanın en önemli parçasını oluşturur. Kriptografik uygulamalar, şans oyunları, şifre üreteçleri gibi kritik alanlarda uygulamanın güvenliği rastgele sayılara dayanır [18]. Bu türden güvenlik uygulamalarında ise genellikle GRSÜ tercih edilir. Şifrelenmiş sistemlerin güvenliği, gizli verilerin (gizli anahtar gibi) yetki verilen bireyler tarafından bilinmesi ve diğer bireyler tarafından da tahmin edilememesi üzerine kurgulanmıştır. Burada gizli bilginin başkaları tarafından tahmin edilebilmesini zorlaştırmak için rastgele değerlere ihtiyaç vardır. Kötü niyetli kullanıcılar, rastgele sayı oluşturma yöntemlerinin zayıflıklarından faydalanarak güvenlik zafiyeti oluşturabilirler. Bu yüzden rastgele sayıların güvenlik gibi önemli alanlarda kullanılması bu sayıların gerçek rastgele sayılara yakın olmasını ve gerçek rastgele sayıların özelliklerini taşımasını önemli kılmaktadır [1, 19]. Güvenlik dışında gerçek olayların simulasyonunun yapılması işleminde de rastgele sayılar önemli rol oynamaktadır. GRSÜ'lerde entropi kaynağı olarak farklı kaynakların kullanımı literatürde mevcuttur [12]. Bununla beraber rastgele sayıların sistem dışındaki kontrolsüz ortamlarda üretimi sistemin güvenliği için problem olmaktadır [20].

GRSÜ genel olarak üç bloktan oluşur. Bunlar:

- Entropi (gürültü) kaynağı,
- Örnekleyici (sayısallaştırıcı),
- Son işlem algoritmalarıdır.

Entropi kavramı termodinamik teorisinin ikinci yasasını oluşturur. Entropi bir sistemin niteliksel düzensizliğinin ve rastgeleliğinin ölçüsü olarak tanımlanır [21]. Örnekleyici, gürültü sinyalinde gerekli örneklemelerin yapılmasını sağlar ve bu yapı fiziksel gürültü kaynakları için üretim mekanizması olarak ifade edilebilir [12]. Böylece analog sinyalden sayısallaştırılmış sinyal elde edilmesi sağlanır. Örnekleme için farklı yaklaşımlar mevcuttur ve üretilen sayıların kalitesini belirlemede entropi kaynağı ile beraber örnekleyici de önemli bir yere sahiptir. Son işlem genellikle sinyalde bulunan rastgeleliği artırmak için kullanılır. Bu işlem uzun bit dizileri üzerine uygulanır ve otokorelasyonel bir şekilde yayılım gösterir. Burada bağlantılı bit akışındaki yan yana iki bitin katsayısı, uzak bitler arasındaki katsayı bağlantısından daha fazla olmaktadır. Dolayısıyla birbirine uzak bitler arasında olan ilişkiden ziyade yakın bitler arasında ilişki daha güçlü olmaktadır. Son işlem algoritmalarında basit bir sıkıştırma işlemi yerine otokorelasyonu yeniden düzenleyerek

istatistiksel testlerden daha iyi sonuçlar alınır. Son işlem uygulanan sinyal, saf haline kıyasla daha düzenli bir dağılıma ve rassal görünüme sahiptir. Son işlemle üretilen rastgele sayılar yan kanal analizi saldırılarına daha dirençlidir ve çevresel etkenlerden daha az etkilenir. Dolayısıyla son işlem algoritmaları üretecin daha güvenli hale gelmesini sağlar. XOR doğrulama, Von Neumann doğrulama, extractor fonksiyonu, kriptografik özet algoritmaları ve resilient fonksiyonu gibi farklı son işlem algoritmaları mevcuttur [22]. FPGA da GRSÜ ve kriptolojik uygulamalar ve Kaos tabanlı SRSÜ ve GRSÜ uygulamaları yapılmıştır [23-26].

1.1.5. Literatürdeki GRSÜ Tasarımları

Voris ve arkadaşları yaptıkları çalışmada WISP üzerindeki ivmeölçer ve sıcaklığın diğer sensörlere göre daha iyi bir entropi kaynağı olduğunu öne sürmüşlerdir. Kablosuz Kimlik ve Algılama Platformu Radyo Frekansı ile Tanımlama Teknolojisi (WISP RFID) etiketinde de aynı durumun söz konusu olduğunu ifade etmişlerdir. Sabit halde ve hareketli halde veri elde etmişler ve bu verilerin kriptografik açıdan rastgele sayı gereksinimlerini karşıladığını savunmuşlardır [27]. Bunun yanında, hareketsiz ve sıcaklığın değişmediği ortamlarda sadece bu iki sensörün kullanılması rastgele sayı üretimi için yetersiz kalabilmektedir.

Mitra'nın yaptığı çalışmada tohum değerlerinin üretilmesi için uygun olan bir gerçek rastgele sayı üreteci önerilmiştir. GRSÜ, çift beslemeli işlemsel yükseltici ile gerçekleştirilmiştir. Bu, aynı zamanda, Radyo Frekansı ile Tanımlama Teknolojisi (RFID) etiketleri için yaygın olarak kullanılan bir MSP430 mikro denetleyicisinin tek beslemeli işlemsel yükselteçleri ile gerçekleştirilmiştir. Veriler, NIST testini geçmiştir. Orta güç tüketimi ve düşük veri hızı nedeniyle, veri SRSÜ'nün tohum değeri olarak uygun bulunmuştur. Üretecin, yerleşik MSP430 mikro denetleyicilere sahip WISP RFID etiketlerinde kullanılabileceği saptanmıştır [28].

Hennebert ve ark.'nın araştırmasında olası bir entropi kaynağı olarak sensörlerin bir koleksiyonunu değerlendirmişlerdir [29]. Entropi üretmek için en iyi adayların ivmeölçer, manyetometre, titreşim sensörü ve dâhili saat sensörü olduğunu saptamışlardır. Sıcaklık, hava basıncı gibi yüksek ataletle olayları ölçen diğer sensörlerin çok az entropi sağladığı bulunmuştur. Çalışmada, şartlı ortalama entropi tahmincisine ihtiyaç duyulduğu belirtilmiştir. Bir şifreleme anahtarı üretmek, kaynaklardan birçok örnek toplamayı gerektirmektedir. Bunun için koşullu ortalama entropi tahmincisinin, kaynak analizini iyileştirmek için değerli bir araç olacağı sonucuna varılmıştır [29].

Bedekar ve Shee yaptıkları çalışmada mikro elektromekanik sistem sensörleri (MEMS) (ivmeölçer, jiroskop ve pusula) kullanarak GRSÜ için pratik bir yol sunmuşlardır. Bu çalışmada, MEMS sensörü tamamen dinlendiğinde, yüksek kalitede rastgele sayı dizileri oluştuğu bulunmuştur. Bu, MEMS sensörleri için algılama mekanizmalarındaki ilk gürültü kullanılarak gerçekleştirilmiştir. Pusulanın ürettiği veri akışı NIST testi sonuçları değerlendirildiğinde en başarılı sonuçları verdiği saptanmıştır.

Durağan olduğunda 15 testin 11'inden, hareketliyken 15 testin 14'ünden geçmiştir [30]. Vivier ve arkadaşlarının yaptıkları başka bir çalışmada ise, Hamilton döngüsü olmayan bir n-küp üzerinden sözde rastgele sayı üreteci tasarlanmıştır. Klasik testlerden geçen bu yöntem sadece tamsayılar ile yürütüldüğünden NIST testi sonucunda güvenlik zayıf olarak değerlendirmiştir [31]. Bir başka çalışmada da Akgül ve arkadaşları sadece bir arayüz tasarlamış olup bir üreteç ortaya koymamışlardır [32]. 2020 yılında Rezk ve arkadaşları tarafından sadece sözde rastgele sayı üretimi üzerine bir çalışma yapılmış ve test edilmiştir [33]. Son çalışmalardan biri olan Avaroğlu ve Tuncer, S-box tabanlı yeni bir gerçek rastgele sayı üreteci tasarlamışlardır. Kriptografinin birçok alanında kullanılabilen ve test sonuçları da başarılı olan bu çalışmanın dezavantajı ise entropi kaynağından gelen genelleştirilmiş bit dizisiyle bir korelasyonun var olmasıdır [34].

Kriptografi, ağ güvenliğinin dolayısıyla siber güvenliğin temel bileşenidir [35]. Açık anahtarlı kriptografide şifrelemenin en önemli yanı eşsiz ve tekrarlanmayan anahtarın bulunmasıdır. Anahtarı üretmenin iki metodu vardır. İlki, Advanced Encryption Standard (Gelişmiş Şifreleme Standardı) (AES) algoritmasında olduğu gibi titiz ve güçlü bir matematiksel algoritmik yaklaşımdır. İkincisi ise doğayı taklittir.

Bu araştırmada kimyasal reaksiyonlarla elde edilen tohum değerleri kullanılarak kuantum dalga denklemi tabanlı algoritmaların kriptografide kullanılmasına yönelik yeni bir yöntem kullanılmıştır. Bu yaklaşım matematiksel hesaplamalar ile doğal olayların birleştirildiği hibrit bir yaklaşım olacağından önereceğimiz algoritmanın güçlü olacaktır.

2020 ve sonrasında çalışmalar kuantum rastgele sayı üreteçleri üzerine yoğunlaştırılmıştır [36-38]. Kuantum teknolojisi ile rastgele sayı üretimi üzerine yapılan bir araştırmada telefon kameralarından alınan fotoğraf karelerinden elde edilen fotonlardan faydalanılarak tahmin edilemeyen rastgele sayılar üretilmiştir [39]. Kuantum teknolojisi kullanarak rastgele sayı üretimi yüksek maliyetli olduğundan ve bu teknikler günümüzde çok yaygın kullanılmadığından dolayı, gelecekte kuantum teknolojisinin gelişmesiyle beraber yaygın olarak kullanılacağı üzerinde düşünceler bulunmaktadır [5].

Rastgele sayı üretimi ile ilgili olarak literatürde oldukça fazla çalışma mevcut olup, burada sadece genel amaçlı ve bu çalışmaya ışık tutacak olanlar incelenmiştir. Mevcut GRSÜ ve SRSÜ'lerin en büyük dezavantajları maliyetli olmaları ve tahmin edilebilir olmalarıdır. Tahmin edilemezlik noktasında en güvenilir olan KRSÜ'lerin dezavantajları, maliyet, radyoaktivitenin getirdiği olumsuzluklar ve kullanım zorluğudur. Önerdiğimiz modelde rastgele sayı üretme işleminde farklı tohum değerlerinden elde edilen sayılar bir f fonksiyonu ile birleştirileceğinden;

- Üretilen sayı dizisinin bir kısmına sahip olunsa bile diğer kısmın elde edilmesi imkânsızdır.
- Sayı dizisi periyodik sonuçlar içermez.
- Üretilen diziler kendi içinde herhangi bir gizli bağıntıya sahip olmayacaktır.

Rastgele sayı üreteci gerçek dünyadaki rastgele sayıları üretmek için oluşturulan yapının genel ismi olarak kullanılmaktadır. Rastgele sayı üretecinde sayı üretimi yapılırken belirli özelliklerin sağlanması önemlidir. Temel olarak mümkün olduğu kadar rastgele olması, büyük periyotlarda yani uzun bir seride tesadüfiliğin sağlanması, üretilen rastgele sayıların yeniden üretilebilir, hesaplanabilir ve gerektiği durumda tekrar kullanılabilir olması gerekmektedir. Tüm bu özellikleri sağlayan verimli, maliyeti düşük ve kullanımı kolay olan bir gerçek rastgele sayı üreteci oluşturulabilir mi? Sorusu bu araştırma için motivasyon kaynağı olmuştur.

Bu çalışmanın amacı, iyi istatistiksel özellikler gösteren, yeniden üretilemeyen, tahmin edilemeyen ve verimli gerçek rastgele sayı üretme (GRSÜ) için kimyasal reaksiyonlar kullanılarak kuantum dalga denklemi tabanlı, düşük maliyetli rastgele sayı üretmektir. Bu amaç kapsamında aşağıdaki hipotezler ortaya konulmuştur;

Bu araştırmanın hipotezleri:

1.Literatür incelendiğinde gerçek rastgele sayı üretme için çok sayıda yöntem olduğu görülmektedir. Kimyasal reaksiyonların gerçek rastgele sayı üretmede kullanılması üretilen rastgele sayıların verimliliği ve maliyeti hususunda pozitif olarak etkilidir.

2. Bilinen üreteçlerde entropi kaynağı olarak fiziksel olaylar, elektiriksel gürültü, kaotik sistemler kullanılmıştır. Gerçek rastgele sayı üretmede kimyasal reaksiyonların gürültü kaynağı olarak kullanılması iyi istatistiksel özellik göstermesi açısından önemlidir.

3. Radyoaktif rastgele sayı üreteçlerine alternatif olarak kullanılabilecek kimyasal reaksiyonlar, düşük maliyetli rastgele sayı üreteci geliştirilmesini olumlu yönde etkiler.

1.2. KUANTUM DALGA DENKLEMİ

Her bir parçacık bir dalga fonksiyonu tarafından temsil edilir. Bu dalga fonksiyonunun kendisiyle çarpılması belli bir zamanda belli bir konumda parçacığın bulunma ihtimalini verir dalga fonksiyonu Schrödinger denkleminde kullanılır. Bu denklem kuantum dalga fonksiyonu olarak da adlandırılır. Bu denklem dinamik bir sistemin gelecekteki davranışı hakkında bilgi verir bununla beraber olayların analitik ve hassas bir şekilde ihtimalini ön görerek sonuçların dağılımını tahmin eder.

Dalga fonksiyonu şu özelliklere sahiptir:

- Dalga fonksiyonu parçacık ile ilgili bütün ölçülebilir bilgilere sahiptir.
- Eğer parçacık varsa, parçacığın bulunma olasılığı bir olmalı, o halde $\Psi * \Psi$ tüm uzayda toplandığında 1'dir.
- Dalga fonksiyonu süreklidir.
- Dalga fonksiyonu Schrödinger denklemi sayesinde enerji hesaplamalarına imkan sağlar.
- Dalga fonksiyonu üç boyutlu olasılık dağılımını sağlar.

- Dalga fonksiyonu elimizde olan bir değişkenin ortalama değerinin hesaplanmasına müsade eder.
- Serbest bir parçacık için dalga fonksiyonu bir sinüs dalgasıdır. Bu hassas bir şekilde momentumun tespit edildiği ve konumun tamamen belirsiz olduğunu gösterir.

Bir parçacıktan oluşan fiziksel sistem ve dalga fonksiyonunun biraraya gelmesi kuantum mekaniğinin varsayımlarından bir tanesidir. Bu dalga fonksiyonu sistem hakkında bilinebilecek her şeyi belirler. Dalga fonksiyonu konum ve zamanın tek bir değerli fonksiyonu olarak kabul edilir, çünkü belirli bir konum ve zamanda parçacığın bulunma olasılığının belirsizliğe müsade etmeyen tam bir değer olmasını sağlaması yeterlidir. Dalga fonksiyonu karmaşık bir fonksiyon olabilir, belirli bir durumda parçacığın gerçek fiziksel bulunma olasılığını belirlemek amacıyla onun karmaşık eşleniği ile çarpılır [2].

2. MATERYAL VE METOT

Bu çalışma yapılırken izlenen kuramsal yaklaşım ve yöntemdeki ilk basamak tohum veri üretimidir. Bunun için, mısır koçanından bir tohum ekilerek çimlendirme ve yetiştirme sürecinde bitkide ve ortamda meydana gelen kimyasal reaksiyonlardan veri elde edilmiştir. Ardından bu veriler kuantum dalga denklemi tabanlı matematiksel bir algoritmada girdi olarak kullanılarak gerçek rastgele sayılar üretilmiştir.

Bu çalışma üç aşamadan oluşmaktadır. İlk aşamada verilerin kaydedilmesi ve tasnifi yapılmıştır. İkinci aşamada elde edilen verilere uygun kuantum dalga denklemi geliştirilerek, nem, ısı ve kütle değişimlerinden elde edilen değerlerin her biri tohum değer olarak alınarak farklı rastgele sayılar üretilmiştir. Üçüncü aşamada ise elde edilen rastgele sayıların test edilmiştir [40].

1. Aşama

- Genel olarak GRSÜ için önemli bileşenlerinden biri gürültü kaynağıdır. Gürültü kaynakları; elektriksel, atmosferik, ses, fare hareketleri vb. olaylardır. Çalışmada uygulanan GRSÜ yapısında kimyasal reaksiyonlar gürültü kaynağı olarak kullanılmıştır. Işık kaynağı, toprak, su, ağırlık artışını hesaplamak için hassas tartı, ortam nem ve sıcaklığını ölçmek için nem ve ısıölçer kullanılarak mısır bitkisinin belirli aralıklarla hassas tartıdaki ağırlık değerleri ile beraber nem ve sıcaklık değişimi kaydedilmiştir. Bunun için ise; bitki, toprak ile doldurulmuş saksıda çimlendirilmiştir. Daha sonra; verilen su, bitki besini ve sabit ışık kaynağı ile oluşturulan ortamda belirli saat aralıkları ile bitkilerin kütleleri ölçülüp kütlelerindeki değişimler kaydedilmiştir. Ölçüm esnasında ortam nem miktarı ve ortam sıcaklığı da kaydedilmiştir. Bitki ağırlık, nem, sıcaklık ölçümü örneği Şekil 2.1'de gösterilmiştir.

Şekil 2.1. Bitki ağırlık, nem, sıcaklık ölçümü

Bu doğrultuda elde edilen veriler Excel dosyasına kaydedilmiştir. Ölçüm sırasına göre ağırlık, nem ve sıcaklık değerleri Tablo 2.1'de gösterilmiştir.

Tablo 2.1. Ölçüm Sırasına Göre Ağırlık, Nem Ve Sıcaklık Değerleri

Ölçüm Sırası	Ağırlık	Nem	Sıcaklık (°C)
1	277.33	51.0	26.8
2	271.81	45.0	28.1
3	272.24	52.0	23.6
4	271.41	55.0	24.1
5	270.68	54.0	24.3
6	268.67	44.0	24.1
7	268.35	48.0	24.3
8	263.73	54.0	23.0
9	262.33	47.0	23.0
10	261.8	42.0	22.6
11	261.28	53.0	23.0
12	260.0	52.0	22.6
13	258.50	53.0	22.9
14	258.31	48.0	22.3
15	258.07	55.0	23.1
16	257.75	44.0	27.2
17	257.61	45.0	27.1
18	257.37	45.0	27.3
19	257.27	46.0	27.4
20	257.1	48.0	27.5
21	255.12	48.0	27.3

22	299.15	47.0	28.8
23	298.91	46.0	28.8
24	298.48	48.0	28.9
25	296.28	45.0	28.9
26	295.88	45.0	29.0
27	295.41	44.0	29.7
28	288.49	45.0	29.5
29	287.42	46.0	29.6
30	286.92	43.0	29.3
31	286.74	43.0	29.4
32	286.45	42.0	29.6
33	286.02	40.0	29.8
34	283.39	41.0	28.3
35	282.82	41.0	29.3
36	281.79	45.0	28.3
37	281.63	47.0	28.4
38	281.42	52.0	23.7
39	281.34	51.0	23.8
40	281.14	50.0	23.5
41	280.98	56.0	24.1
42	280.85	53.0	24.2
43	279.71	51.0	24.4
44	278.92	51.0	22.9
45	278.77	51.0	23.7
46	277.39	51.0	24.2
47	276.92	57.0	24.5
48	276.82	56.0	24.5
49	276.67	55.0	24.7
50	276.39	52.0	24.0
51	276.32	56.0	24.3
52	276.23	63.0	24.4
53	276.06	59.0	24.2
54	276.0	62.0	24.4
55	275.84	59.0	24.3
56	275.77	60.0	24.3
57	275.38	57.0	24.0
58	274.7	57.0	23.6
59	287.25	53.0	23.1
60	287.18	52.0	23.1
61	287.05	55.0	23.3
62	286.99	57.0	23.4
63	285.50	51.0	23.1
64	285.30	55.0	23.3
65	285.11	55.0	23.4
66	284.93	57.0	23.5
67	376.64	49.0	23.1
68	375.85	51.0	24.0
69	375.65	50.0	24.0
70	375.54	50.0	24.1
71	375.45	52.0	24.2
72	375.21	49.0	24.3
73	374.91	50.0	24.3
74	374.83	50.0	24.4
75	374.75	54.0	24.4
76	374.53	53.0	24.3
77	374.37	50.0	24.1
78	374.22	53.0	24.0
79	374.08	54.0	24.0
80	373.82	70.0	24.5

81	373.73	59.0	24.3
82	373.50	57.0	24.3
83	372.63	57.0	23.9
84	372.45	60.0	24.0
85	372.36	61.0	24.0
86	371.32	51.0	23.1
87	371.10	57.0	23.4
88	370.81	58.0	23.6
89	370.59	57.0	23.6
90	392.11	58.0	23.4
91	392.00	56.0	23.3
92	391.66	53.0	23.6
93	391.50	67.0	23.6
94	391.34	54.0	23.8
95	391.28	61.0	23.8
96	391.16	60.0	23.9
97	391.13	63.0	23.9
98	389.20	47.0	21.9
99	388.56	51.0	22.6
100	388.49	54.0	22.9
101	388.42	55.0	23.0
102	388.04	54.0	23.3
103	388.00	55.0	23.3
104	387.79	55.0	23.5
105	387.55	54.0	23.6
106	387.41	55.0	23.6
107	387.22	50.0	23.5
108	387.05	50.0	23.3
109	386.84	52.0	23.3
110	386.72	52.0	23.4
111	385.76	54.0	23.2
112	385.62	57.0	23.7
113	385.58	63.0	23.8
114	384.43	54.0	23.7
115	384.22	52.0	23.5
116	384.07	51.0	23.5
117	383.90	53.0	23.5
118	383.42	55.0	23.5
119	382.12	55.0	23.9
120	381.95	57.0	24.1
121	381.81	51.0	24.1
122	391.60	46.0	23.7
123	389.68	48.0	23.8
124	389.52	53.0	24.0
125	389.45	54.0	24.1
126	389.33	53.0	24.2
127	389.24	51.0	24.1
128	387.40	49.0	23.1
129	386.45	48.0	23.8
130	386.32	49.0	23.9
131	386.07	48.0	23.8
132	385.55	47.0	23.7

2. Aşama

❖ Literatürde var olan uygulamalar dikkate alınarak matematik formülasyon geliştirilebilir. Bunun için optimizasyon metotları kullanılmıştır.

Kuantum dalga denklemi; Schrödinger denklemi olarak bilinen bir kuadrik diferansiyel denklemdir;

$$-\frac{\hbar^2}{2m}\frac{\partial^2\Psi(x)}{\partial x^2} + V(x)\Psi(x) = E\Psi(x) \quad (1)$$

Bu denklemin bir genel çözümü aşağıdaki gibi bir lineer kombinasyondur;

$$\Psi(x) = ACos(kx) + BSin(kx) \quad (2)$$

Burada, t: zaman, k: dalga vektörü (2π/λ), λ: dalga uzunluğu, x: konum ve w: frekans olmak üzere (2) denkleminin çözümünden yeni bir dalga fonksiyonu elde edilir [41, 42];

$$\psi(x,t) = \frac{1}{\sqrt{2}}[\cos(wt - kx) + sin(wt - kx)] \quad (3)$$

Nem, ısı ve kütle değişimlerinden elde edilen değerlerin her biri (3) denkleminde tohum değer olarak alınıp farklı rastgele sayılar üretilmiştir.

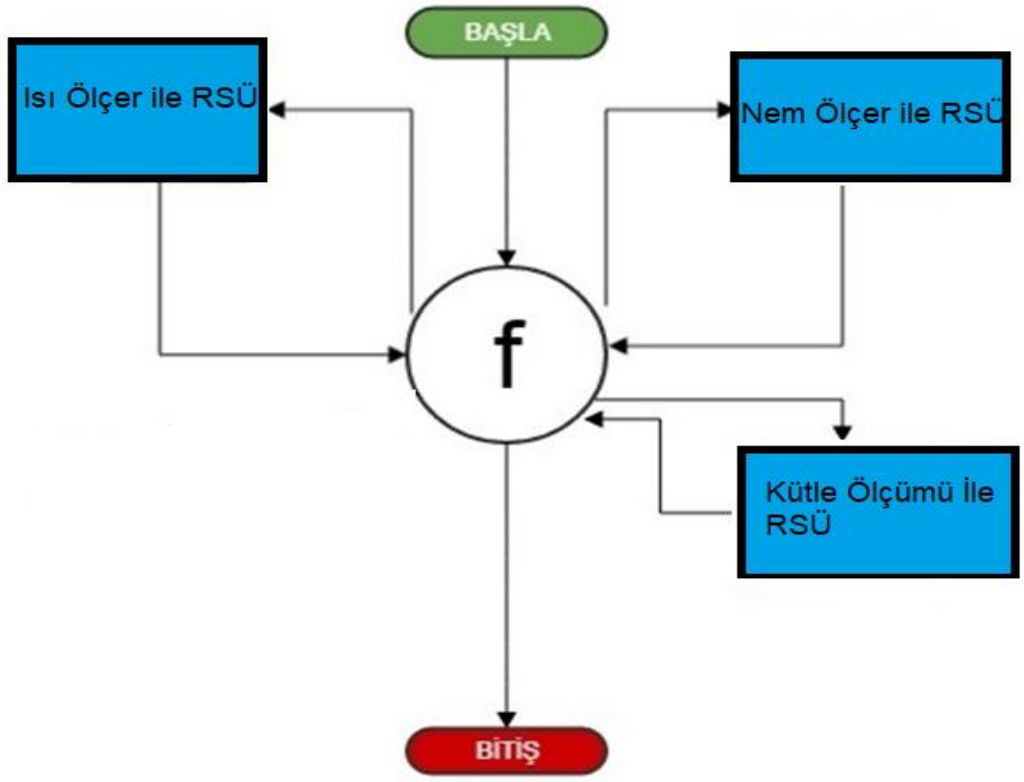
❖ Kuantum dalga denklemini esas alan GRSÜ için kullanılan algoritmalar Python programı kullanılarak Excel üzerinden verileri alıp tekrar Excel olarak rastgele sayıları çıkaracak şekilde yazılmıştır. Python kodları Şekil 2.2'de gösterilmiştir.

```
import math
import xlrd
import xlwt

#excelin olduğu adres
loc = ("C:\\Users\\Tuncay\\Desktop\\proje\\veri.xlsx")
wb = xlrd.open_workbook(loc)
sheet = wb.sheet_by_index(0)
EXCEL_FILES_FOLDER = 'C:\\Users\\Tuncay\\Desktop\\proje\\'
workbook = xlwt.Workbook()
worksheet = workbook.add_sheet('data')
#excel_file_path = EXCEL_FILES_FOLDER+'result.xlsx'
#workbook.save(excel_file_path)
#k=277.33
#n=51
#s=26.8

#k=1. satır 1. sütun
#n=1. satır 2. sütun
#n=1. satır 3. sütun
for i in range(132):
    k=float(sheet.cell_value(i, 0))
    n=float(sheet.cell_value(i, 1))
    s=float(sheet.cell_value(i, 2))

    x1=1/math.sqrt(2)*(math.cos(0.5777*1.6-42.6630*k)+math.sin(0.5777*1.6-42.6630*k))
    x2=1/math.sqrt(2)*(math.cos(4.2817*1.6-5.7567*n)+math.sin(4.2817*1.6-5.7567*n))
    x3=1/math.sqrt(2)*(math.cos(0.2493*1.6-98.7421*s)+math.sin(0.2493*1.6-98.7421*s))


    h1=5*x1*(1-x1)+(3-0.9999)*math.sin(math.pi*x1)/3
    h2=5*x2*(1-x2)+(3-0.9999)*math.sin(math.pi*x2)/3
    h3=5*x3*(1-x3)+(3-0.9999)*math.sin(math.pi*x3)/3

    i1, d1 = divmod(h1, 1)
    o1=round(d1,4)

    i2, d2 = divmod(h2, 1)
    o2=round(d2,4)

    i3, d3 = divmod(h3, 1)
    o3=round(d3,4)

    top=o1+o2+o3
    sonuc=math.pow(math.e,math.sin(math.pi*top))
    worksheet.write(i, 0,sonuc)
    workbook.save('result.xls')
```

Şekil 2.2. Rastgele Sayı Üreteci

Sıcaklık, nem ve kütle değişimi ile elde edilen değerlerin Python dili kullanılarak oluşturulan Şekil 2.2'deki algoritmalarda tohum değer olarak girilip sonucunda gerçek rastgele sayılar oluşturulmuştur.

Bu sayıların oluşumu Şekil 2.3'te gösterilmiştir.



Şekil 2.3. Rastgele Sayı Üreteçlerinin f Fonksiyonu İle Birleştirilmesi

Tablo 2.2'de verilerle elde edilen gerçek rastgele sayılar gösterilmiştir.

Tablo 2.2. Verilerle Elde Edilen Rastgele Sayılar

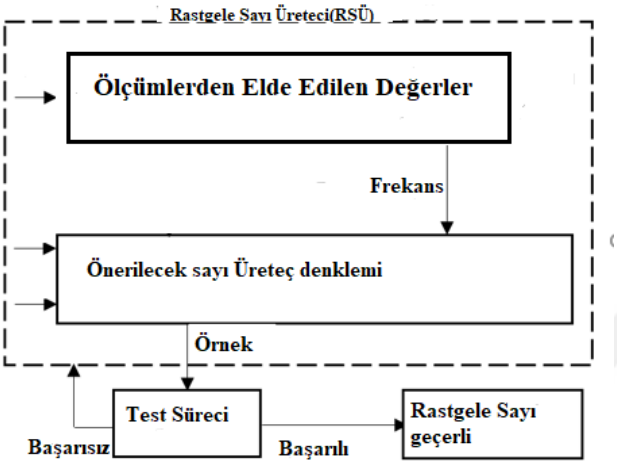
Ölçüm Sırası	Ağırlık	Nem	Sıcaklık (°C)	Gerçek Rastgele Sayı
1	277.33	51.0	26.8	0,408450076048656
2	271.81	45.0	28.1	1,031585308327140
3	272.24	52.0	23.6	2,538025925145950
4	271.41	55.0	24.1	0,448962909024277
5	270.68	54.0	24.3	2,675906481163010
6	268.67	44.0	24.1	1,898469161462790
7	268.35	48.0	24.3	0,468529084932782
8	263.73	54.0	23.0	1,554365333924150
9	262.33	47.0	23.0	2,499585695485250
10	261.8	42.0	22.6	0,377185672378410
11	261.28	53.0	23.0	1,706594505013500
12	260.0	52.0	22.6	1,143812162393650
13	258.50	53.0	22.9	0,709519045706567
14	258.31	48.0	22.3	0,894674346760875
15	258.07	55.0	23.1	0,443417738816881
16	257.75	44.0	27.2	0,607963634520569

17	257.61	45.0	27.1	0,395656050383763
18	257.37	45.0	27.3	0,368556078451696
19	257.27	46.0	27.4	0,961802744376804
20	257.1	48.0	27.5	1,614901643525000
21	255.12	48.0	27.3	1,031261432252350
22	299.15	47.0	28.8	2,245699366201990
23	298.91	46.0	28.8	0,747938151558086
24	298.48	48.0	28.9	0,547617969839769
25	296.28	45.0	28.9	0,761359451114418
26	295.88	45.0	29.0	0,826063931161887
27	295.41	44.0	29.7	2,568720781506800
28	288.49	45.0	29.5	0,396311912165177
29	287.42	46.0	29.6	0,398672124103672
30	286.92	43.0	29.3	0,651407557824324
31	286.74	43.0	29.4	0,371293639929994
32	286.45	42.0	29.6	1,982873600452040
33	286.02	40.0	29.8	0,444230904283943
34	283.39	41.0	28.3	0,368001522994430
35	282.82	41.0	29.3	1,178799720000650
36	281.79	45.0	28.3	0,470459655854515
37	281.63	47.0	28.4	0,423051277211668
38	281.42	52.0	23.7	0,667606571838650
39	281.34	51.0	23.8	0,415502402591649
40	281.14	50.0	23.5	1,829296750098070
41	280.98	56.0	24.1	0,397938884977477
42	280.85	53.0	24.2	1,390354599767800
43	279.71	51.0	24.4	1,962410358715270
44	278.92	51.0	22.9	0,500653625664374
45	278.77	51.0	23.7	0,374256782916214
46	277.39	51.0	24.2	0,384330002896548
47	276.92	57.0	24.5	2,660849758018030
48	276.82	56.0	24.5	0,901124483209645
49	276.67	55.0	24.7	0,368119581675466
50	276.39	52.0	24.0	0,966646232005611
51	276.32	56.0	24.3	0,589559834324099
52	276.23	63.0	24.4	0,747713352890063
53	276.06	59.0	24.2	0,429918531923881
54	276.0	62.0	24.4	0,850426594026618
55	275.84	59.0	24.3	0,734826760453760
56	275.77	60.0	24.3	1,961955009066700
57	275.38	57.0	24.0	2,236551618920170
58	274.7	57.0	23.6	0,438800342614714
59	287.25	53.0	23.1	0,444885075788031
60	287.18	52.0	23.1	0,373601956958629
61	287.05	55.0	23.3	0,385811472965945
62	286.99	57.0	23.4	0,546384533797670
63	285.50	51.0	23.1	0,382914965368709
64	285.30	55.0	23.3	1,369015512969960
65	285.11	55.0	23.4	0,399564563901004
66	284.93	57.0	23.5	0,368385973779824
67	376.64	49.0	23.1	1,053178851167540
68	375.85	51.0	24.0	0,414880495229164
69	375.65	50.0	24.0	2,713794497779030
70	375.54	50.0	24.1	0,376388011321994
71	375.45	52.0	24.2	0,372473324813178
72	375.21	49.0	24.3	0,368245622323102
73	374.91	50.0	24.3	0,624562463897039
74	374.83	50.0	24.4	0,556404768959412
75	374.75	54.0	24.4	2,717567111946000

76	374.53	53.0	24.3	1,946002931623340
77	374.37	50.0	24.1	0,460475446847338
79	374.08	54.0	24.0	1,404005223677250
81	373.73	59.0	24.3	2,502411408613550
82	373.50	57.0	24.3	0,382579859224164
84	372.45	60.0	24.0	0,384542642605319
85	372.36	61.0	24.0	2,351209740177430
86	371.32	51.0	23.1	2,307471087619830
87	371.10	57.0	23.4	0,368454936193273
88	370.81	58.0	23.6	0,436938654679970
89	370.59	57.0	23.6	0,551490094331144
90	392.11	58.0	23.4	1,786735684392000
91	392.00	56.0	23.3	0,421839123223159
92	391.66	53.0	23.6	2,406724952160600
93	391.50	67.0	23.6	0,552047567780681
94	391.34	54.0	23.8	0,464545979472797
95	391.28	61.0	23.8	0,496826858728528
96	391.16	60.0	23.9	1,977876686436170
97	391.13	63.0	23.9	1,851746007599180
98	389.20	47.0	21.9	0,858112274607791
99	388.56	51.0	22.6	1,792679236448340
100	388.49	54.0	22.9	0,391377561788498
101	388.42	55.0	23.0	2,712815645175140
102	388.04	54.0	23.3	0,887444692856862
103	388.00	55.0	23.3	0,538432063397117
104	387.79	55.0	23.5	0,537503797952593
105	387.55	54.0	23.6	0,963616097133282
106	387.41	55.0	23.6	2,010965826402350
107	387.22	50.0	23.5	0,659620668975796
108	387.05	50.0	23.3	1,828838703823320
109	386.84	52.0	23.3	0,604173067602842
110	386.72	52.0	23.4	0,400015934949712
111	385.76	54.0	23.2	2,694082974235720
112	385.62	57.0	23.7	0,373872174671912
113	385.58	63.0	23.8	0,684410238372642
114	384.43	54.0	23.7	1,845789415850700
115	384.22	52.0	23.5	0,449555486836599
116	384.07	51.0	23.5	0,999371878861350
117	383.90	53.0	23.5	0,383083989738652
118	383.42	55.0	23.5	0,619916326007713
119	382.12	55.0	23.9	0,941498984851697
120	381.95	57.0	24.1	0,372184038470988
121	381.81	51.0	24.1	0,536051580778511
122	391.60	46.0	23.7	0,526486301706152
123	389.68	48.0	23.8	0,530579237872018
124	389.52	53.0	24.0	0,574194927857638
125	389.45	54.0	24.1	0,679856291323955
126	389.33	53.0	24.2	0,913321483094817
127	389.24	51.0	24.1	0,494828739604293
128	387.40	49.0	23.1	0,376692445737655
129	386.45	48.0	23.8	1,174058955713670
130	386.32	49.0	23.9	1,441226091365110
131	386.07	48.0	23.8	0,819977399261284
132	385.55	47.0	23.7	2,113273693284340

- Nihai olarak, şifrelemede kullanılan anahtar üretimi gerçekleştirilmiştir.

Rastgele sayı üreteci algoritması için önerilen mimarinin genel görünümü Şekil 2.4'te verilmiştir. Şekil 2.4'te önerilen mimari, belirlenen parametreler kullanılarak analizi yapılan verilere uygun olarak önerilen matematiksel fonksiyon tabanlı rastgele sayı üreteci mimarisidir. Kesikli oklar dışındaki bloklar, oluşturulan rastgele sayılar için karşılanması gereken temel koşul olan istatistiksel rastgelelik süreçlerinin analiz aşamalarını temsil eder.



Şekil 2.4. Önerilen Mimarinin Genel Görünümü

3. Aşama

Çıkan sonuçların rastgeleliğini kontrol etmek için Run testinden yararlanılmıştır.

Run rastgelelik testi, verilerdeki rastgeleliği kontrol etmek için kullanılan istatistiksel bir testtir. Bu parametrik olmayan bir testtir ve sunulan verilerin rastgele mi yoksa bir örüntüyü takip etme eğiliminde mi olduğuna karar vermek için veri dizilerini kullanır. Bir çalışma, artan değerler veya azalan değerler dizisi olarak tanımlanır. Artan veya azalan değerlerin sayısı, çalışmanın uzunluğudur [43].

Çalıştırma testindeki ilk adım, veri dizisindeki çalıştırma sayısını saymaktır. Çalışmaları tanımlamanın birkaç yolu vardır, ancak her durumda formülasyonun ikili bir değerler dizisi üretmesi gerekir. Bizim durumumuzda, medyanın üzerindeki değerler pozitif, medyanın altındaki değerler negatif olarak kabul edilir. Bir çalışma, bir dizi ardışık pozitif veya negatif değer olarak tanımlanır.

$$Z = \frac{R - \bar{R}}{S_R}$$

Burada,

R=Gözlenen çalıştırma sayısı

$\bar{R}$=Beklenen çalıştırma sayısı

$$R = \frac{2n_1 n_2}{n_1 + n_2} + 1$$

S_R=Çalışma sayısının standart sapması

$S_R{}^2 = \frac{2n_1n_2(2n_1n_2-n_1-n_2)}{(n_1+n_2)^2(n_1+n_2-1)}$

n_1 ve n_2= serideki pozitif ve negatif değerlerin sayısı

Hesaplanan Z-istatistiğinin değerini, belirli bir güven düzeyi için Z kritik değeriyle karşılaştırılınca (%95 güven düzeyi için Z kritik =1.96), eğer |Z|>Z kritik ise sayılar rastgele değildir [43]. Şekil 2.5'te Run Testi Python kodları verilmiştir.

```
import random
import math
import statistics
import xlrd
import xlwt

def runsTest(l, l_median):

        runs, n1, n2 = 0, 0, 0

        # Checking for start of new run
        for i in range(len(l)):

                # no. of runs
                if (l[i] >= l_median and l[i-1] < l_median) or \
                                (l[i] < l_median and l[i-1] >= l_median):
                        runs += 1
                # no. of positive values
                if(l[i]) >= l_median:
                        n1 += 1

                # no. of negative values
                else:
                        n2 += 1

        runs_exp = ((2*n1*n2)/(n1+n2))+1
        stan_dev = math.sqrt((2*n1*n2*(2*n1*n2-n1-n2))/ \
                                        (((n1+n2)**2)*(n1+n2-1)))

        z = (runs-runs_exp)/stan_dev

        return z


loc = ("C:\\Users\\Tuncay\\Desktop\\test\\result.xls")
wb = xlrd.open_workbook(loc)
sheet = wb.sheet_by_index(0)
l = []
for i in range(132):
    k=float(sheet.cell_value(i, 0))
    print(k)
    l.append(k)

l_median= statistics.median(l)
Z = abs(runsTest(l, l_median))
print('Z-statistic= ', Z)
```

Şekil 2.5. Run Testi Python Kodları

3. BULGULAR VE TARTIŞMA

Tez kapsamında mısır bitkisi kullanılarak hazırlanan gerçek rastgele sayı üreteci tasarımında bitkinin ağırlık değişimi ve bitkinin ağırlığı ölçüldüğü andaki ortamın nem ve sıcaklık değerleri; tohum değer olarak alınmış ve bu değerler Python dili kullanılarak hassas fonksiyonlarda rasgele sayı üretilmiştir. Sayıların güvenirliğini ölçmek için Run testinden yararlanılmıştır.

Verilerin homojenliğini test etmek için kullanılan yöntemlerden biri olan run testi ile incelenecek verinin aynı toplumdan geldiği ve birbirinden bağımsız olduğu kabulü ya da tam tersi iki varsayımın kontrol edilebildiği bir testtir. Bu test sonucuna göre veriler aynı toplumdan ve birbirinden bağımsız ise bu serilere basit rastgele sayılar denir. Bu nedenle elimizdeki verilere göre en sağlıklı analizin run testi ile yapılabileceği değerlendirilmiştir.

Run testinde sayıların rasgele olduğunu söylenebilmesi için Z değerinin 1.96 değerinden küçük bir değer çıkması gerekmektedir. Çalışmamızda Run testi sonucunda Z değeri 0.5242377083205431 çıkmıştır.

4. SONUÇLAR

Bu tez çalışmasında mısır bitkisi kullanılarak rastgele sayı üretimi gerçekleştirilmiştir. Hazırlanan gerçek rastgele sayı üreteci tasarımında bitkinin büyümesindeki ağırlık değişimi ve bitkinin ağırlığı ölçüldüğü anda ortamın nem ve sıcaklık değerleri ölçülerek kaydedilmiş, kaydedilen değerler Python dili kullanılarak hazırlanan kuantum dalga denklemi üzerinde tohum değer olarak kullanılıp rastgele sayılar üretilmiştir. Bu sayıları test edebilmek için Run testi kullanılmıştır. Yaptığımız çalışmanın anlamlı olabilmesi için Run testi sonucunda çıkan değerin 1.96 dan küçük çıkması gerekmektedir. Bu durumda çıkan sonuçların birbiriyle ilişkili olmadığı ve yeterli rastgeleliğe sahip olduğu sonucuna varılmaktadır.

Test sonucunda çıkan değer 0.524 olup çalışmamızın güvenirliğini göstermektedir. Rastgele sayı üretmek için birden fazla yöntem kullanılabilmektedir. Rastgele sayı üreteci tercihinde göz önünde bulundurulan hususlardan bazıları maliyet, hız, kurulum ve performans değerleridir. Bu araştırmada ortaya konulan kimyasal reaksiyonlar ile gerçek sayı üretiminin hem maliyet hem de kullanım kolaylığı açısından rakiplerine üstünlük sağladığı görülmüştür. Çalışmamız, bu alandaki gelecek çalışmalara kaynaklık edebilecek farklı bir bakış açısı sunmaktadır, yapılacak ileri araştırmalara ışık tutacağı düşünülmektedir.

Bu doğrultuda önerilerimiz:

- Uygun düzenekler kullanılarak mevcutta yetişmiş olan bitkilerden alınacak verilerle çeşitli üreteçler tasarlanabilir.

Çalışmamızda kullanılan teknik geliştirilip bir kabin sistemine konularak daha kısa sürede daha fazla veri elde edilerek hibrit bir rastgele sayı üreteci tasarımı yapılabilir.

KAYNAKLAR

[1] Chaitin, GJ. (2001). *Exploring Randomness*, London, Springer.

[2] Gençoğlu, MT. (2021). Quantum cryptography, quantum communicatıon and quantum computing problems and solutions, *Turkish Journal of Science and Technology*, C. 16 (1), 97-101.

[3] Viniotis, Y. (1998). *Probability and Random Processes For Electrical Engineers*, Boston, WCB/McGraw-Hill.

[4] Genç, Y. (2019). *İnsan Hareketleri Tabanlı Gerçek Rastgele Sayı Üretimi*, Yüksek Lisans Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü.

[5] Daemen, J.; Rijmen V. (2013). *The Design Of Rijndael: AES-The Advanced Encryption Standard*, New York, Springer Science & Business Media.

[6] Robinson SO.; Dessart, DJ. (1998). *Teaching and Learning of Algorithms in School Mathematics*, USA, National Council of Teachers of Mathematics.

[7] Schoukens, J.; Pintelon, R; van der Ouderaa, E.; Renneboog, J. (1988). Survey of excitation signals for FFT based signal analyzers, *IEEE Transactions on Instrumentation and Measurements*, C. 37(3), 342-352.

[8] Schindler, W.; Killmann, W. (2002). Evaluation criteria for true (physical) random number generators used in cryptographic applications, *Cryptographic Hardware and Embedded Systems*.

[9] Avaroğlu, E. (2017). LFSR soru girdisi ile puf tasarımının gerçeklenmesi, *Fırat Üniversitesi Mühendislik Bilimleri Dergisi*, C. 29(2), 15–21.

[10] Tuncer, SA.; Genç, Y. (2019). İnsan hareketleri tabanlı gerçek rastgele sayı üretimi, C.8(1), 261–269.

[11] Yalçın M., Suykens J.; Vandewalle J. (2004). True Random Bit Generation from a Double Scroll Attractor, *IEEE Trans. Circuits Syst*. C. 51(7), 1395-1404.

[12] Koç, ÇK. (2009). *Cryptographic Engineering*, Springer-Verlag.

[13] Yusuf, AY. (2021). *Generation and Realization of True Random Numbers Based on Physical Unclonable Functions*, Master's Thesis, Fırat University, Graduate School of Natural and Applied Sciences.

[14] Toyran, M. (2007). Efficient use of random numbers, *In Signal Processing and Communications Applications*, IEEE 15th.

[15] Von Neumann, J. (1951). Various Techniques Used in Connection With Random Digits, *National Bureau of Standards Applied Mathematics Series*, C. 12, 36-38.

[16] Dastgheib, MA.; Farhang, M. (2017). A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period, *Nonlinear Dynamics*, C.89(4), 2957–2966.

[17] Demirhan, H.; Bitirim, N. (2016). Statistical testing of cryptographic randomness, *Journal of Statisticians: Statistics and Actuarial Sciences*, C.1, 1-11.

[18] Wold, K. (2011). S*ecurity Properties of a Class of True Random Number Generators in Programmable Logic*, Doctoral Degree, Gjøvik University College, Doctor of Philosophy in Information Security.

[19] Sanguinetti, B.; Martin, A.; Zbinden, H.; Gisin, N. (2014). Quantum random number generation on a mobile phone, *Physical Review*, C.4(3), 031056.

[20] Avaroğlu, E. (2014). *Donanım Tabanlı Rastgele Sayı Üretecinin Gerçekleştirilmesi*, Doktora Tezi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü.

[21] Kapur, JN.; Kesavan, HK. (1992). *Entropy Optimization Principles and Their Applications*, Netherlands, Springer.

[22] Dichtl, M. (2007). Bad and good ways of post-processing biased physical random numbers, International Workshop on Fast Software Encryption.

[23] Yıldırım, S. (2012). *A True Random Number Generator In FPGA For Cryptographıc Applications*, Master's degree, Middle East Technical University, Graduate School of Natural and Applied Sciences.

[24] Özkaynak, F. (2013). Security problems for a pseudorandom sequence generator based on the Chen chaotic system, *Computer Physics Communications*, C.184(9), 2178-2181.

[25] Özkaynak, F. (2014). Cryptographically secure random number generator with chaotic additional input, *Nonlinear Dynamics*, C. 78, 2015-2020.

[26] Özkaynak, F. (2015). Kriptolojik Rasgele Sayı Üreteçleri, *Türkiye Bilişim Vakfi Bilgisayar Bilimleri ve Mühendisliği Dergisi*, C. 8(2), 37-45.

[27] Voris, J.; Saxena, N.; Halevi, T. (2011). Accelerometers and randomness: perfect together, *Proceedings of the fourth ACM conference on Wireless network security*, Hamburg, Germany.

[28] Mitra, M. (2012). A Low-Cost Lightweight Random Number Generator Implementation, *International Journal of Engineering Research & Technology*, C. 1(10), 1-9.
[29] Hennebert, C.; Hossayni, H.; Lauradoux, C. (2013). Entropy harvesting from physical sensors, *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, Budapest, Hungary.
[30] Bedekar, N.; Shee, C. (2015). A Novel Approach to True Random Number Generation in Wearable Computing Environments Using MEMS Sensors. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics*, C. 8957, 530-546.
[31] Contassot-Vivier, S.; Couchot, JF.; Guyeux, C.; Heam, PC. (2017). Random Walk in a N-Cube Without Hamiltonian Cycle to Chaotic Pseudorandom Number Generation: Theoretical and Practical Considerations, *International Journal of Bifurcation and Chaos*, C. 27(1), 1750014.
[32] Akgül, A.; Arslan, C., Arıcıoğlu, B. (2019). Design of an Interface for Random Number Generators based on Integer and Fractional Order Chaotic Systems, *Chaos Theory and Applications*, C. 1(1), 1-18.
[33] Rezk, A.; Madian, A.; Radwan, A.; Soliman, AM. (2019). Multiplierless Chaotic Pseudo Random Number Generators, *AEU - International Journal of Electronics and Communications*, C. 113, 152947.
[34] Avaroğlu, E.; Tuncer T. (2020). A novel S-box-based postprocessing method for true random number generation, *Turk J Elec Eng & Comp Sci.*, C. 28, 288-301.
[35] Khan, FU; Bhatia, S. (2012). A Novel Approach to Genetıc Algorıthm Based Cryptography, *International Journal of Research in Computer Science*, C. 2(3), 7-10.
[36] Hurley-Smith, D. Hernandez-Castro, J. (2020). Quantum Leap and Crash: Searching and Finding Bias in Quantum Random Number Generators, *ACM Transactions on Privacy and Security*, C. 23(3), 1-25.
[37] Lin, X.; Wang, S.; Yin, ZQ.; *et al*. (2020). Security analysis and improvement of source independent quantum random number generators with imperfect devices, *Npj Quantum Information*, C. 6(1), 100.
[38] Kavulich, J.; Van Deren, B.; Schlosshauer, M. (2021). Searching for evidence of algorithmic randomness and incomputability in the output of quantum random number generators, *Physics Letters*, C. A(388), 127032.
[39] Dutang, C.; Wuertz. D. (2009). A note on random number generation, *Overview of Random Generation Algoritms.*
[40] Gençoğlu, MT.; Agarwal, P. (2021). Use of Quantum Differential Equations in Sonic Processes, *Applied Mathematics and Nonlinear Science*, C. 6(1), 21-8.
[41] Gençoğlu, MT. (2013). Complex solutions for Burgers-Like equation, *F.U. Türkish Journal Of Science and Technology*, C. 8(2), 121-123.
[42] Dereli, T.; Verçin, A. (2014). *Kuantum Mekaniği Temel Kavramlar ve Uygulamaları*, TÜBA Der Kitapları.
[43] Bujang MA.; Sapri, F. (2018). An Application of the Runs Test to Test for Randomness of Observations Obtained from a Clinical Survey in an Ordered Population, *Malaysian Journal of Medical Sciences*, C. 25, 146-151.

ÖZGEÇMİŞ

Tuncay GENÇ

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]