KUANTUM RASTGELE SAYI ÜRETECİ TASARIMI VE UYGULAMASI

QUANTUM RANDOM NUMBER GENERATOR DESIGN AND IMPLEMENTATION

SAFA HANKÖYLÜ

PROF. DR. ALİ ZİYA ALKAR

Tez Danışmanı

Hacettepe Üniversitesi

Lisansüstü Eğitim - Öğretim ve Sınav Yönetmeliğinin

Elektrik ve Elektronik Mühendisliği Anabilim Dalı İçin Öngördüğü

YÜKSEK LİSANS TEZİ

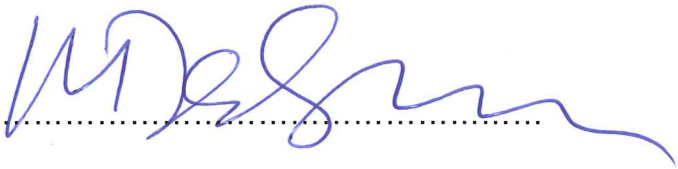
olarak hazırlanmıştır.

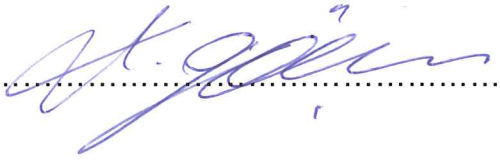
2019

SAFA HANKÖYLÜ' nün hazırladığı "**Kuantum Rastgele Sayı Üreteci Tasarımı ve Uygulaması**" adlı bu çalışma aşağıdaki jüri tarafından **ELEKTRİK ve ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI'** nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Dr. Öğr. Üyesi Gökhan SOYSAL
Başkan ..... 

Prof. Dr. Ali Ziya ALKAR
Danışman ..... 

Dr. Öğr. Üyesi Derya ALTUNAY
Üye ..... 

Dr. Öğr. Üyesi Dinçer GÖKCEN
Üye ..... 

Dr. Öğr. Üyesi Kadir DURAK
Üye ..... 

Bu tez Hacettepe Üniversitesi Fen Bilimleri Enstitüsü tarafından **YÜKSEK LİSANS TEZİ** olarak ..... / ..... / ..... tarihinde onaylanmıştır.

Prof. Dr. Menemşe GÜMÜŞDERELİOĞLU
Fen Bilimleri Enstitüsü Müdürü

ETİK

Hacettepe Üniversitesi, Fen bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

01/02/2019

SAFA HANKÖYLÜ

YAYIMLAMA VE FİKRİ MÜLKİYET HAKLARI BEYANI

Enstitü tarafından onaylanan lisansüstü tezimin/raporumun tamamını veya herhangi bir kısmını, basılı (kağıt) elektronik formatta arşivleme ve aşağıda verilen koşullarla kullanıma açma iznini Hacettepe Üniversitesine verdiğimi bildiririm. Bu izinle Üniversiteye verilen kullanım hakları dışındaki tüm fikri mülkiyet haklarım bende kalacak, tezimin tamamının ya da bir bölümünün gelecekteki çalışmalarda (makale, kittap, lisans ve patent vb.) kullanım hakları bana aittir.

Tezin kendi orijinal çalışmam olduğunu, başkalarının haklarını ihmal etmediğimi ve tezimin tek yetkili sahibi olduğumu beyan ve taahhüt ederim. Tezimde yer alan telif hakkı bulunan ve sahiplerinden yazılı izin alınarak kullanması zorunlu metinlerin yazılı izin alarak kullandığımı ve istenildiğinde suretlerini Üniversiteye teslim etmeyi taahhüt ederim.

Yükseköğretim Kurulu tarafından yayınlanan "Lisansüstü Tezlerin Elektronik Ortamda Toplanması Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" kapsamında tezimin aşağıda belirtilen koşullar haricinde YÖK Ulusal Tez Merkezi / H. Ü. Kütüphaneleri Açık Erişim Sisteminde erişime açılır.

- ☐ Enstitü / Fakülte Yönetim Kurulu kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren 2 yıl ertelenmiştir.
- ☐ Enstitü / Fakülte Yönetim Kurulu gerekçeli kararı ile tezimin erişime açılması mezuniyet tarihinden itibaren ..... ay ertelenmiştir.
- ☐ Tezim ile ilgili gizlilik kararı verilmiştir.

01 / 02 / 2019

SAFA HANKÖYLÜ

ÖZET

KUANTUM RASTGELE SAYI ÜRETECİ TASARIMI VE UYGULAMASI

Safa HANKÖYLÜ

Yüksek Lisans, Elektrik Elektronik Mühendisliği Bölümü
Tez Danışmanı: Prof. Dr. Ali Ziya Alkar
Şubat 2019, 64 Sayfa

Rastgelelik; şans/talih oyunları, istatistik hesaplamaları, bilgisayar simülasyonları, bilgi güvenliği ve şifreleme gibi içerisinde rastgele olayların yaşanması gereken her tür uygulamada karşımıza çıkmaktadır. Rastgeleliği kullanan olaylar için rastgelelik kalitesi oldukça önemlidir. Özellikle kriptoloji alanında kullanılan rastgele sayıların tahmin edilemez olması gerekliliği, rastgele sayı üreteçlerinin önemini artırmaktadır.

Rastgele Sayı Üreteçleri (RSÜ), aralarında herhangi bir örüntü, ilişki olmayacak şekillerde tahmin edilemeyecek sayı dizileri üretilmesini sağlayan yazılımsal veya donanımsal bileşenlerdir. Yazılım kaynaklı RSÜ'ler deterministik uygulamalar olup donanım kaynaklı RSÜ'ler ise sisteme entegre edilebilen aygıtlardır.

Yazılımsal RSÜ kullanılarak üretilen sayılarla yapılan şifreleme, deterministik yollarla geliştirildiği için, şifrelemenin gücüne göre değişen sürelerde, çözümlenmesi mümkün olan üreteçlerdir. Günümüzde geliştirilmeye çalışılan

kuantum bilgisayarların hayatımıza girmesi ile klasik bilgisayarlarla çözümlemenin çok uzun zaman aldığı şifre çözme durumları için sürelerin önemli ölçüde kısalması beklenmektedir. Donanımsal RSÜ'ler ise, rastgelelik kaliteleri yazılım kaynaklı üreteçlerden daha güçlü olmakla birlikte maliyetli ve kullanımı sınırlı üreteçlerdir.

Kuantum Rastgele Sayı Üreteçleri (KRSÜ) ise, 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.

Bu tez çalışmasında, tek LED'li bir ışık kaynağından alınan görüntülerin RGB (Red – Green - Blue) değerlerinden faydalanılarak bir KRSÜ elde edilmeye çalışılmış ve üretilen sayıların rastgelelik testleri, NIST (National Institute of Standards and Technology) tarafından sağlanan testlerle gerçekleştirilmiştir. Sonuçta, tek ledli, beyaz ışık kaynağından elde edilen görüntülerle NIST testlerini başarıyla geçmiş rastgele sayı dizileri elde edilmiştir.

Anahtar Kelimeler: kuantum rastgele sayı üreteci, NIST, RGB, foton, bilgi güvenliği.

ABSTRACT

QUANTUM RANDOM NUMBER GENERATOR DESIGN AND IMPLEMENTATION

Safa HANKÖYLÜ

Master of Science, Department of Electrical and Electronics Engineeering
Supervisor: Prof. Dr. Ali Ziya Alkar
February 2019, 64 pages

Randomness occurs in every kind of application in which random events should be experienced such as gambling, statistical calculations, computer simulations, information security and encryption. The quality of randomness is very important for the events using randomness. In particular, the need for random numbers used in the field of cryptology to be unpredictable increases the importance of random number generators.

Random Number Generators (RNGs) are software or hardware components that can be used to generate numbers that cannot be predicted in any pattern or relationship. Software-based RNGs are deterministic applications, while hardware-based RNGs are the devices that can be integrated into the system.

Encryption using numbers generated by software-based RNG can be broken in varying times depending on the strength of the encryption because it was developed in deterministic ways. It is expected that the decoding time will be

shortened considerably by the quantum computers which are tried to be developed today besides classic computers that takes a long time to analyze. The hardware RNGs are more powerful in randomness quality than software-based generators, but cost-effective and use-limited generators.

Quantum Random Number Generators (QRNGs) is a kind of generator based on quantum physics laws instead of classical physics. In photonic based QRNGs are produced the random numbers after various software and hardware operations by taking advantage of the uncertainty of photons. These generated numbers are unpredictably strong random numbers.

In this study, a QRNG was obtained by using the RGB (Red-Green-Blue) values of the images taken from a white-single LED light source and the randomness tests of the produced numbers were carried out with the tests provided by NIST (National Institute of Standards and Technology). As a result, the numbers derived from the images successfully passed NIST tests and true random number sequences were obtained.

Keywords: quantum random number generator, NIST, RGB, photon, information security.

TEŞEKKÜR

Lisansüstü eğitimim süresince değerli bilgi ve yönlendirmeleri ile yol gösterici olan danışmanım Sn. Prof. Dr. Ali Ziya Alkar'a emeklerinden ve anlayışından dolayı teşekkür ederim.

Tez çalışmalarım sırasında bilgileri ve destekleriyle yardımlarını esirgemeyen Sn. Prof. Dr. Murat Efe, Sn. Dr. Öğr. Üyesi Gökhan Soysal ve Sn. Dr. Öğr. Üyesi Kadir Durak'a ayrıca teşekkür ederim.

Son olarak, her daim destekleri ve sevgileriyle yanımda olan anneme, babama ve benim için çok değerli ve özel olan kız kardeşlerime çok teşekkür ederim.

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR DİZİNİ

RSÜ	:	Rastgele Sayı Üreteci (Random Number Generation - RNG)
RGB	:	Kırmızı – Yeşil – Mavi (Red – Green – Blue)
KRSÜ	:	Kuantum Rastgele Sayı Üreteci (Quantum Random Number Generation - QRNG)
LED	:	Işıma Yapan Diyot (Light Emitting Diode)
NIST	:	Ulusal Teknoloji ve Standartlar Enstitüsü (National Institute of Standards and Technology)
GPU	:	Grafik İşleme Ünitesi (Graphics Processing Unit
DES	:	Veri Şifreleme Standardı (Data Encryption Standard)
3DES	:	Üçlü DES (triple-DES)
AES	:	Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
RSA	:	Rivest – Shamir - Adleman
DSA	:	Sayısal İmza Algoritması (Digital Signature Algorithm)
TLS	:	Taşıma Katmanı Güvenliği (Transport Layer Security)
SSH	:	Güvenli Kabuk (Secure SHell)
SRSÜ	:	Sözde Rastgele Sayı Üreteci (Pseudo Random Number Generator)
GRSÜ	:	Gerçek Rastgele Sayı Üreteci (True Random Number Generator)
SSL	:	Güvenli Soket Katmanı (Secure Socket Layer)
GM	:	Geiger-Müller
LFSR	:	Doğrusal Geri Beslemeli Kaydırma Yazmacı (Linear Feedback Shift Register)

SÖZLÜKÇE

Ayrık Fourier Dönüşümü Testi	:	Discrete Fourier Transform, Spectral Test
Artık Özüt Lemma	:	The Leftover Hash Lemma
Bilgi sızıntısı	:	Information leakage
Bir Blok İçerisinde Frekans Testi	:	Frequency Test within a Block Test
Bir Blok İçerisindeki En Uzun Bir Tekrarı	:	Test For The Longest Run Of Ones In A Block
Birikerek Artan Toplamlar Testi	:	Cumulative Sums Test
Bütünlük	:	Integrity
Çakışmayan Şablon Eşleme Testi	:	Non-Overlapping/Aperiodic Template Matching Test
Çarpışma Entropisi	:	Collision Entropi
Çubuk grafik	:	Histogram
Değişimli Rastgele Gezinimler Testi	:	Random Excursions Variant Test
Doğrulama	:	Authentication
Doğrusal Karmaşıklık Testi	:	Linear Complexity Test
Doğrusal Kaydırmalı Geri Besleme Üreteçleri	:	Linear Shift Feedback Generators
Dolaşıklık	:	Entanglement
Elektronik Saçma Gürültülü KRSÜ'ler	:	Electronic Shot Noise QRNGs
Erişilebilirlik	:	Availability
Fotoçoklayıcı	:	Photomultiplier
Foton Sayıcı Üreteçler	:	Photon Counting Generators
Frame	:	Çerçeve
Frekans Testi	:	Frequency/Monobit Test
Gizlilik	:	Confidentiality
Ham veri	:	Raw data
Işın ayırıcı	:	Beam splitter
İkili Matris Rank Testi	:	Binary Matrix Rank Test
İnkar Edememe	:	Non-repudiation

Kasiski Yöntemi	:	Kasiski’s Method
Kesme	:	Interrupt
Kaba kuvvet saldırısı	:	Brute-force attack
Kübit	:	Qubit
Maurer'in Evrensel İstatistiksel Testi	:	Maurer's Universal Statistical Test
Optik KRSÜ’ler	:	Optical QRNGs
Optik Yol Üreteçleri	:	Optical Path Generators
Ortadaki Kişi Saldırısı	:	Man in the Middle Attack
Yaklaşık Entropi Testi	:	Approximate Entropy Test
Özüt	:	Hash
Çıkarım	:	Extraction
Radyoaktif Bozunmaya Dayalı Üreteçler	:	QRNGs Based on Radioactive Decay
Rastgele Gezinimler Testi	:	Random Excursions Test
Seri Test	:	Serial Test
Süperpozisyon	:	Superposition
Süreç sonrası	:	Postproccessing
Tekdüzelik	:	Uniform
Koşum Testi	:	Runs Test
Tesadüf endeksi	:	Index of coincidence
Tohum	:	Seed
Varış Zamanına Dayalı Üreteçler	:	Time of Arrival Generators)

1. GİRİŞ

Kriptoloji, güvenli haberleşmenin sağlanabilmesi üzerine kurulur ve bilginin güvenli bir şekilde aktarılabilmesi için çeşitli koşulların sağlanması beklenmektedir [1]. Bunlardan başlıcaları; gizlilik, bütünlük, doğrulama, erişilebilirlik ve inkâr edememedir. Gizlilik, haberleşmenin sağlanması istenen taraflar harici içeriğe ulaşılamaması olarak tanımlanmaktadır. Bütünlük, gönderilen ya da alınan mesajın eksiksiz olarak, bir değişikliğe maruz kalmadan gönderilmesi koşuludur. Doğrulama, gönderilen mesajın sadece belirli kişilere iletilmesi için uygulanan bir güvenlik unsurudur, böylece sadece yetkisi olanlar ilgili mesajı görebilmektedir. Erişilebilirlik, tarafların herhangi bir engelle karşılaşmadan, istenilen zamanda bilgiye ulaşılmasıdır. Son olarak, inkâr edememe ise yapılan haberleşmenin taraflarca yadsınamamasına yönelik alınan önlemlerdir [1-3].

Kriptolojinin geçmişi, oldukça eskiye dayanmaktadır. Gerçekleştirilen iletişimin gizli kalması her zaman bir ihtiyaç olmuştur. Örneğin, MÖ 50-60'lı yıllarda, Julius Caesar siyasi haberleşmeler yapması gerektiğinde metinlerde yer alan harflerin, kendilerinden sonraki üçüncü harf ile değiştirilmesi ile ortaya çıkan bir yöntem geliştirmiştir ve bu yönteme Sezar Şifrelemesi denmektedir. Şifreleme işlemi çok eskiye dayanmakla birlikte şifre çözme işlemlerine dair çalışmalar da yeni değildir. Orta çağda şifreli metinlerin çözülmesine yönelik yapılan çalışmalar da günümüzde şifre çözmede kullanılan frekans analizi yönteminin ortaya çıkmasına zemin hazırlamıştır [4]. Daha sonraları, savaşlarda gizli bilgilerin iletilmesi için ortaya çıkan çeşitli uygulamalarla geliştirilen şifreleme (Skytale şifrelemesi, Vigenere şifrelemesi, Damıtma şifrelemesi) ve şifre çözme (Enigma ve Sigaba makineleri) teknikleri, kriptolojinin ve bilgi güvenliğinin önemini ortaya koymuştur [5 - 6].

Kriptanaliz, güvenli olarak adlandırılan sistemlerin veya bileşenlerinin güvenilirliğini ortadan kaldırmaya yönelik her tür girişimdir. Bu girişimler sayesinde gizlenmek istenen bilgiler, üçüncü kişiler tarafından okunabilmektedir. İlgili saldırılar sistemin çalışma prensibini öğrenmeye yönelik olabileceği gibi, metinleri şifrelemek ve çözmek için kullanılan anahtarların

bulunmasına yönelik de olabilir. Kriptanalizin en yaygın kullanılan prensibi frekans analizidir. Metin içerisinde gelmesi muhtemel harfler veya harf çiftleri gibi kullanım sıklığına yönelik bir çıkarıma dayanmaktadır [7-8]. Bir diğer kriptanaliz yöntemi ise tesadüf endeksidir. Bu yöntemde, metin içerisinde kullanılan harflerin frekansı ike kullanılan dilin frekansı arasında bir ilişki kurularak şifreli metin çözülmektedir [9]. Üçüncü olarak, haberleşme iletim yollarından faydalanılarak da metin hakkında bilgi çıkarılabilir ve bu yönteme bilgi sızıntısı adı verilmektedir. GPU'da silinmeyen hafızalardan dolayı güvenlik sorunu yaşanması bir örnek olarak verilebilir [10]. Son olarak, Kasiski Yöntemi ise bloklara ayrılan şifreli metnin blok uzunluğunu bularak şifrelenen metni bulabilir [11]. Şifrelenmiş bütün metinlerin çözülmesine yönelik kritanaliz yönlemlerinin yanı sıra modern kriptografinin bir sonucu olarak anahtar şifrelerinin kırılmasına yönelik Boomerang saldırısı, kaba kuvvet saldırısı (bütün ihtimallerin tek tek denenmesi) ve ortadaki kişi saldırısı gibi çeşitli saldırılar da bulunmaktadır [12].

Bir önceki paragrafta kısaca değinilen anahtarların, günümüzde Kerckhoff İlkesine dayanılarak yapılan bilgisayar haberleşmelerinde, veri güvenliği için önemi oldukça büyüktür. Kerckhoff İlkesine göre, anahtar bilgisi gizli kalmak koşuluyla, sistem hakkında bilgi sahibi olunması herhangi bir tehlike teşkil etmemektedir [13]. Shannon tarafından matematiksel ifadesi verilen bu yaklaşım ile sistem gizliliğinin değil anahtar gizliliğinin önemli olduğu vurgulanmaktadır [14]. Anahtar gizliliğine yönelik güncel anahtar şifreleme algoritmaları ise simetrik ve asimetrik algoritma olarak ikiye ayrılmaktadır.

Simetrik anahtarlama (gizli anahtarlı) ile şifreleme, gönderici ve alıcı tarafından belirlenen ortak bir anahtar üzerine kurulmuştur. Gönderici mesajı şifreledikten sonra alıcı aynı anahtarı kullanarak şifreli mesajı çözmektedir. Simetrik anahtarlama ile şifrelemede kullanılan algoritmalar herkes tarafından bilinmekte olup güvenlik anahtarların gizliliği ile sağlanmaktadır. Bu nedenle anahtar yönetimi, simetrik anahtarlamada büyük önem taşımaktadır [15]. 1970'lerin başlarında, bankamatiklerin güvenli haberleşmeleri için IBM (International Business Machines) 'de çalışan bir ekip tarafından ortaya çıkarılan algoritma, 1976 yılında, şimdiki adıyla NIST tarafından güvenli haberleşme için bir standart

olarak kabul edilmiştir ve DES (Data Encryption Standard) adıyla bilinmektedir [16]. DES algoritması ile 56 bitlik anahtarlar kullanılarak 64 bitlik şifrelenmiş metin elde ediliyor olması, bit boyutunun az olmasından dolayı, kriptanaliz yöntemlerinden biri olan ve ikinci paragrafta bahsedilen kaba kuvvet saldırılarına açık olması sonucunu doğurmaktadır. Bununla ilgili olarak, 1998 yılında Electronic Frontier Foundation tarafından Deep Crack isimli bir donanım ile 56 saat içerisinde DES algoritmasına yönelik şifre çözme işlemi yapılmıştır [17]. Bununla birlikte, 56 saatten daha kısa sürelerde DES algoritmasının çözülebildiği çeşitli uygulamalar da günümüze kadar ortaya konmuştur [18 - 19]. DES'in anahtar uzunluğu dezavantajına yönelik olarak 1999 yılında yine NIST tarafından üçlü DES algoritması ortaya konmuştur. Daha güvenli olduğu ileri sürülen bu algoritma ile DES algoritması üç kez çalıştırılmaktadır. Bu sayede anahtar uzunluğu 112 ve 168 bite kadar çıkarılabilmektedir. Ancak, 3DES ve DES algoritmaları tekli kullanıma izin verilemeyecek şekilde NIST tarafından geri çekilmişlerdir [20]. Tekli kullanıma izin verilmeyen 3DES algoritması, 2005 yılında yayınlanan Amerika Birleşik Devletleri Resmi Gazetesinde yer alan bilgilendirme ile, NIST tarafından 2001 yılında duyurulan bir başka algoritma olan AES (Gelişmiş Şifreleme Standardı) algoritması gerekçe gösterilerek kullanımdan çekilmiştir [21 - 23]. AES algoritması, 128, 192 ve 256 bit uzunluğunda anahtarlar ile şifreleme ve şifre çözme işlemi yapabilmekte olup 3DES'e kıyasla daha fazla anahtar ihtimali ortaya koymaktadır. Sonuçta, kaba kuvvet ile şifrenin çözülebilme süreleri de önemli ölçüde değişmektedir; AES ile $5x10^{21}$ gün sürebiliyorken bu süre 3DES ile 112 bitlik anahtar için 800 güne düşmektedir [24]. AES, güvenlik avantajından dolayı, üretilen bütün bilgisayarlar tarafından çalıştırılan bir standart olarak karşımıza çıkmaktadır. DES ve AES gibi blok tipi şifrelemenin yanı sıra bit bit aktarımın mümkün olduğu RC4 gibi şifreleme yöntemleri alternatif olarak kullanılabilmektedir [25]. Ne yazık ki, en yaygın uygulamalardan biri olan RC4 ile yapılan şifrelemenin de güvenli olmadığına dair çalışmalar literatürde yer almaktadır [26-28]. Son olarak, simetrik anahtarlama ailesi altında özüt fonksiyonları adı altında yer alan bir başka algoritma daha yer almaktadır. Burada girdi olarak kullanılan veriler süreç sonunda daha kısa boyutlarda şifrelenmiş metinler şeklinde elde edilmektedir. Yalnız, özüt fonksiyonları genellikle şifrelemenin karmaşıklaştırılması gereken

durumlarda ek bir işlem olarak kullanılmaktadır; zira geri döndürülebilir algoritmalar değillerdir.

Bir diğer anahtarlama algoritması olan asimetrik (açık anahtar) algoritmalar, simetrik anahtarlamanın bazı dezavantajlarını ortadan kaldırmak amacıyla ortaya çıkmıştır. Birincisi, simetrik anahtarlamada bilgi güvenliğinin korunması için anahtarın sadece alıcı ve gönderici tarafından bilinmesi, üçüncü bir kişi tarafından bilinmemesi gerekmektedir ki birbirlerini hiç tanımayan kullanıcılar tarafından yapılacak haberleşmelerde bir sorun olarak ortaya çıkmaktadır. İkinci olarak ise simetrik algoritmada n tane kullanıcının $n^2 - n$ çift iletişim ağı oluşturması beklenir ve bu da oldukça maliyetlidir [29]. Bu eksiklikler göz önünde bulundurularak, 1976 yılında, Whitfield Diffie ve Martin E. Hellman tarafından açık anahtarlama ile şifreleme yaklaşımı önerilmiştir [30]. Bu çalışma ile simetrik anahtarlamada yaşanan problemlerin giderilmesine yönelik uygulamaların yanı sıra gönderilmek istenen bir iletinin göndericinin imzasını taşıyacak şekilde dağıtımının sağlanması konusunda bir çözüm de sunulmuştur [31]. Asimetrik anahtarlama ile şifreleme işleminde, gönderilen mesaj herkes tarafından bilinen bir anahtar ile şifrelenebilirken sadece alıcının sahip olduğu gizli bir anahtar ile mesaj çözülebilmektedir. Bu durumda herhangi bir anahtar dağıtımı yapılmadan her kullanıcı kendi özel anahtarını kullanmaktadır. Bununla birlikte, açık anahtarın biliniyor olması gizli anahtarın ortaya çıkarılmasında kullanılamamaktadır. Açık anahtar şifreleme matematiğine dayanan ve en yaygın kullanılan algoritma RSA (Rivest-Shamir-Adleman) algoritması olarak bilinmektedir [32]. RSA algoritmasının gizliliği, büyük sayılar söz konusu olduğunda sayıların çarpanlarına ayırma işleminin zor olmasına dayanmaktadır. Başlangıçta seçilen asal sayıların aynı uzunlukta ve 75 veya daha fazla basamaklı uzunluğukta olması beklenmektedir [15]. Bununla birlikte, 1994 yılında NIST tarafından duyurulan DSA (Sayısal İmza Algoritması) da yaygın olarak kullanılan elektronik imza uygulamalarından biridir [3, 33]. Bir diğer açık anahtarlamalı şifreleme yöntemi ise ElGamal şifreleme yöntemidir [34]. ElGamal şifreleme yöntemi, RSA'nın asal çarpanlara ayırma zorluğundan farklı olarak ayrık logaritmanın çözülme zorluğu temeline dayanmaktadır. İşlem yükleri sebebiyle asimetrik şifreleme işlemleri simetrik anahtarlamaya göre daha yavaş çalışmaktadırlar. Bu nedenle, şifre çözme süreleri karşılaştırıldığında RSA

yöntemi ElGamal yöntemine göre daha yavaş kalmaktadır. Ayrıca, ElGamal yönteminin uygulanması RSA'ya göre daha kolay olduğundan ElGamal yöntemi RSA'ya göre tercih edilebilir olmaktadır [35 - 37]

Yukarıda bahsedilen simetrik ve asimetrik algoritmaların gizliliği, tek başlarına ya da birlikte kullanılmaları (TLS (Taşıma Katmanı Güvenliği) ve SSH (Güvenli Kabuk) katmanlarında olduğu gibi) fark etmeksizin kullanılan anahtarların gizliliği kuralına dayanmaktadır [38, 39]. Simetrik algoritmalar, gönderici ve alıcının aynı anahtarı kullanması sebebiyle ek bir güvenlik uygulaması (anahtar yönetimi) gerektiriyor olsa da hem simetrik hem de asimetrik algoritmalar için anahtarın üçüncü kişiler tarafından bilinemez olması güvenlik açısından büyük önem taşımaktadır. Bu nedenle de anahtar üretimi, bilginin korunması ve üçüncü kişiler tarafından müdahale edilmesinin önüne geçilmesi adına çok önemlidir. Hâlihazırda kullanılan bilgisayar sistemlerinde anahtarlar, dijital sayılar olarak karşımıza çıkmaktadır ve anahtarların güvenliğinin artırılması adına çeşitli fiziksel süreçler veya algoritmalar kullanılarak sayıların tahmin edilememezlik seviyeleri artırılmaya çalışılmaktadır. Bu rastgele sayılar da rastgele sayı üreteçleri tarafından oluşturulmaktadır.

Rastgele Sayı Üreteçleri, tahmin edilmesi güç sayı dizileri üretmek için kullanılmakta olup üretilme şekillerinden dolayı Sözde ve Gerçek Rastgele Sayı Üreteçleri şeklinde ikiye ayrılmaktadır. Sözde Rastgele Sayı Üreteçleri (SRSÜ), deterministik (matematiksel ya da hesaplanabilir) sayı üreteçleri olarak da geçmekte olup çeşitli algoritmalar yardımıyla tahmin edilmesi güç rastgele sayılar üretmektedirler [3]. Gerçek Rastgele Sayı Üreteçleri (GRSÜ) ise SRSÜ'lerin aksine deterministik değillerdir; algoritmalar yerine tahmin edilmesi zor fiziksel işleyişleri kullanarak rastgele sayı dizileri üretmektedirler. RSÜ'lere dair detaylı incelemeler Bölüm 2'de yapılmaktadır.

RSÜ'ler güvenli haberleşmeler için o kadar önemlidir ki yeterli rastgeleliğin sağlanamadığı üreteçlerle elde edilen anahtarlar ile yapılan şifrelemelerin güvenlik açıklarına neden olabileceğini gösteren çeşitli çalışmalar ile önemi vurgulanmaktadır. Örneğin, 2012 yılında yapılan bir çalışma ile açık anahtarlama yöntemiyle gerçekleştirilen iletişimlerde kullanılan sayı

üreteçlerinin güvenlik açıkları meydana getirdiği ve güvenli haberleşmeler için uygun olmadığı gösterilmiştir [40]. Benzer şekilde, 2008 yılında yapılan bir çalışma ile, DSA-1571-1 OpenSSL katmanında kullanılan rastgele sayı üretecinin rastgele olmadığı aksine öngörülebilir olduğu ortaya konmuştur [41]. Son olarak, yine 2012 yılında, internet ortamı için TLS ve SSH sunucularında kullanılan zayıf rastgele sayı üreteçlerinin ne gibi sonuçlar doğurabileceğini gösteren bir çalışma da yapılmıştır [42].

Donanım tabanlı rastgele sayı üreteçlerinin alt başlığı olarak kabul görebilecek Kuantum Rastgele Sayı Üreteçleri (KRSÜ) ise gürültü gibi klasik fizik yasalarını değil kuantum fizik yasalarını dikkate almaktadır ve Heisenberg'in Belirsizlik İlkesine dayanmaktadır [43, 44]. Eşitlik 1.1 ve eşitlik 1.2 ile ifade edilen Belirsizlik İlkesine göre, bir parçacığın konumundaki belirsizlik ne kadar az ise momentumundaki belirsizliksiz de o kadar fazla olur. Benzer ilişki zaman ve enerji ile de kurulabilmektedir. Bu durumda, konum-momentum ile zaman-enerji bilgileri aynı andaki kesin olarak tespit edilememektedir.

$$\sigma_x \, \sigma_p \geq \frac{\hbar}{2} \tag{1.1}$$

$$\sigma_t \, \sigma_E \geq \frac{\hbar}{2} \tag{1.2}$$

σ_x : Konumdaki belirsizlik

σ_p: Momentumdaki belirsizlik

σ_t : Zamandaki belirsizlik

σ_E: Enerjideki belirsizlik

$\hbar$: Planck sabiti

Kuantum fiziğine göre, kuantum objeler bir ölçüm yapılana kadar bütün durumların üst üste binmesi şeklinde bulunur (süperpozisyon) ve iki (veya daha fazla) cisimciği olan kuantum sistemleri, tek bir dalga fonksiyonu ile tarif edilebilir (dolaşıklık). Bu sebeple, klasik fizikte kullanılan bitler 0 veya 1 değerlerinden herhangi birini alabiliyorken kuantum bitleri (kübit), 0 ve 1 değerlerini aynı anda alabilmektedirler. Bu durumda, kuantum fiziği ile

başlangıç koşulları aynı olan durumlar için farklı sonuçlar elde edilebilmektedir [45]. Kuantum yasalarının bütün bu özellikleri birleştirildiğinde, KRSÜ'ler tarafından üretilen sayıların rastgeleliği ve dolayısıyla iletişimin güvenliği de artmaktadır.

Kuantum Rastgele Sayı Üreteçlerinin, SRSÜ ve klasik fizik GRSÜ'lerine göre avantajları yadsınamayacak boyutlardadır. SRSÜ'ler matematik temelli üreteçler olduğu için hesaplanabilirlerdir ve SRSÜ'ler ile üretilen sayıların kriptolojide kullanımı tercih edilmemektedir. Diğer yandan klasik fizik yasalarının kullanıldığı GRSÜ'ler ise, hızlı ve büyük boyutlarda bit değerleri üretememektedirler. Üstelik sıcaklık gibi çevre şartlarından da etkilenebilmektedirler [46]. KRSÜ'ler ise, üretim aşamasında kullanılan süreçlerden bağımsız olarak rastgele sayılar üretebildiği için kriptoloji uygulamalarına en uygun üreteçler olarak görülmektedirler. Hız ve rastgelelik açısından avantajları olsa da günümüzde hantal düzeneklerle üretim sağlanabilmektedir ki iletişimin hızlı olması gerektiği düşünüldüğünde bu bir eksikliktir. Bununla birlikte, üretim aşamasında kullanılan dedektörler de oldukça maliyetlidir [45]. Yapılan tez çalışması ile hantal düzeneklerle, maliyetli KRSÜ uygulamalarına bir alternatif sunulmaktadır.

KRSÜ'ler tarafından üretilen rastgele sayılar, fotonların belirli durumlarda rastgele davranışlarından yola çıkılarak oluşturulan sistemlerle elde edilmektedirler; ancak günümüzde ortaya konan KRSÜ'ler, tek başlarına yeterli düzeyde rastgelelik sağlayamadıkları için klasik fizikten yararlanarak rastgelelik kuvvetlendirilmektedir [47 - 49].

Kuantum tabanlı rastgele sayı üreteçlerinde yaşanan sıkıntıların daha küçük ölçekte ortadan kaldırılıp kaldırılamayacağı sorusu, motivasyon kaynağı olarak ortaya çıkmıştır. Literatürde var olan KRSÜ'lerden farklı olarak çok daha düşük maliyetli bir düzenekle oluşturulan Kuantum Rastgele Sayı Üreteci fikrinden yola çıkılarak bir KRSÜ çalışması yapılmıştır [45, 50]. Bu amaca yönelik olarak; tek LED'li beyaz ışık kaynağı ile belirli bir mesafeden alınan görüntülerin RGB değerleri ortalamasının rastgelelik taşıyıp taşımadığı sorusu irdelenmiştir. 2014 yılında yapılan bir çalışma, LED ve telefon kamerası kullanarak, hantal ve maliyetli uygulamalar dışında da restgeleliğin elde edilebileceğini göstermiştir

[134]. İlgili çalışmada, elektron sayımı ile rastgelelik elde ediliyorken; tez kapsamında, görüntülerin RGB değerlerine bakılmaktadır. Görüntülerin RGB değerleri ile elde edilen rastgele sayılar, NIST tarafından sunulan 15 adet istatiksel testten geçirilerek sayıların rastgelelik tayinleri yapılmıştır.

Bu tez çalışmasının ilk aşaması olan Bölüm 1'de rastgeleliğin kriptoloji alanındaki öneminden bahsedilmiştir. Bölüm 2'de ise öncelikle rastgele sayı üreteçlerine dair detaylı bir inceleme yapılmıştır. Bölüm 3'te, tezin de dâhil olduğu Kuantum Rastgele Sayı Üreteçleri ve ek uygulamalara dair bilgilendirmeler yer almaktadır. Bölüm 4'te, ilgili tez kapsamında gerçekleştirilen çalışmalar anlatılmış ve son bölümde, tez çalışmasının sonuçları verilmiştir.

2. RASTGELE SAYI ÜRETEÇLERİ

Rastgele sayılar, hayatımızın birçok alanında kullanılmakta olup istatistik hesaplamalarında, şans/talih oyunlarında, bilgisayar oyunlarında öngörü gerektiren bilimsel çalışmalarda ve kriptolojide kullanılmak üzere ayrıca özelleşmiş alanları da vardır [14, 51 - 53].

Rastgele sayı üreteçleri ile üretilen sayıların rastgele olabilmesi için birbirleriyle ilintisiz ve üretilecek bir sonraki sayının da tahmin edilemez olması beklenir. Maçlarda yarı sahanın belirlenme süreçlerinde olduğu gibi basit uygulamalar için yazı tura atılması gibi rastgelelik kaynakları olsa da bilgisayar sistemleri için kullanılan rastgelelik kaynakları çok daha karmaşıktır. Çözülmesi zor matematiksel işlemlerden ya da insan müdahalesi olmayan düzensizlik kaynaklarından yararlanarak rastgele sayılar üretilmektedir. İşlem karmaşasına dayanarak rastgele sayılar üreten üreteçlere Sözde Rastgele Sayı Üreteçleri denirken, entropi kaynaklarından faydalanılarak üretim yapanlar Gerçek Rastgele Sayı Üreteçleri adını almaktadır.

2.1. Sözde Rastgele Sayı Üreteçleri

SRSÜ'ler, deterministik yollarla rastgele sayılar üreten uygulamalardır. Rastgele sayı dizileri üretmeleri için tohum adı verilen bir başlangıç bit değerine ihtiyaçları vardır. Süreç sonunda elde edilen sayıların ilintisiz, uzun periyotlarda tekrarlanabilir, tekdüze ve verimli olması istenmektedir [54]. Lehmer tarafından 1951 yılında ortaya konan çalışma sonrası lineer üreteçler, en çok rağbet gören üreteç konumuna gelmişlerdir ve eşitlik 2.1'de yer alan formül baz alınarak çeşitlendirilebilmektedir [55 – 57]. Yeni bir sayı üretilmesi için bir önceki sayı kullanıldığı için bir başlangıç değerine ihtiyaç duyulmaktadır. Bununla birlikte, uzun veya kısa periyotlarda benzer sayıların üretilmesi, başlangıç değerlerinin uygun seçilmesine bağlı olduğundan uzun periyotlar için aşağıda belirtilen koşullara uyulmalıdır.

$$X_{n+1} = (aX_n + c) \bmod m \qquad n \geq 0 \tag{2.1}$$

X_n : rastgele sayı dizisinde n. sayı

m : modüler sayısı, $\mathrm{m} > 0$

a : çarpan, $0 \leq \mathrm{a} < m$

c : artış miktarı, $0 \leq \mathrm{c} < m$

1968 yılında IBM tarafından geliştirilen ve RANDU olarak isimlendirilen bir çeşit lineer SRSÜ için değişkenler a = 65539, c = 0 ve m = 231 olarak tanımlanmıştır. Bir süre kullanılmış olmakla birlikte 1981'de yapılan bir çalışmayla, RANDU algoritmasının tek veya çift boyutlu çizimlerde rastgele sonuçlar verebildiği buna rağmen üç boyutlu çizimler söz konusu olduğunda aynı performansı gösteremediği, rastgele sonuçlar elde edilemediği gösterilmiştir [58]. Lineer üreteçlere dair geniş incelemeler literatürde mevcuttur [59, 60].

Doğrusal Kaydırmalı Geri Besleme Üreteçleri de bir çeşit lineer sayı üretecidir ve Mersenne Twister algoritması (periyodu 2^{19937} - 1) olarak bilinen agoritma, çok hızlı olmasından dolayı birçok programlama dilinde ve bilimsel yazılımda varsayılan olarak tayin edilmiştir [61 - 65].

Sözde rastgele sayı üreteçleri hızlı olmaları ve başka bilgisayarlara taşınabilir olmaları sebebiyle çokça tercih edilmektedirler. Ayrıca, SRSÜ'ler aynı girişler için birebir aynı sonuçlar ürettiğinden simülasyon uygulamaları için oldukça kullanışlıdırlar. Bununla birlikte, sözde rastgele sayılar kullanılarak, rastgeleliği kuvvetlendirileceği ortaya konulan dönüşümlerle yine sözde rastgele sayılar üretebilirler. Bu dönüşümler, girdi ve çıktı arasındaki istatistiksel ilintiyi ortadan kaldırarak bazı GRSÜ'lere göre daha iyi istatiksel sonuçlar elde etmektedirler. Bununla beraber, üretim hızları da önemli ölçüde artmaktadır [66].

Tamamen deterministik olan Sözde Rastgele Sayı Üreteçleri, kriptografik uygulamalar için uygun değillerdir. Matematiksel karmaşıklıktan gücünü alan bu üreteçler için ortaya çıkan en büyük sıkıntı, şifrelerin sonlu bir sürede hesaplanabilir olmasıdır. Günümüz teknolojisi bilgisayarlarıyla kırılamayacak şifreleme işlemleri için Blum-Micali ve Blum-Blum-Shub algoritmaları kullanılabilmektedir; ancak işlem gücü çok yüksek olan kuantum bilgisayarlar ile

klasik bilgisayarlarla çözülmesi çok uzun süren işlemler kısa sürelerde çözülebilecektir [67, 68]. Örneğin, 16 bitlik bir şifre için ihtimal dâhilindeki bütün değerler klasik bilgisayarlarda tek tek denenerek bulunmaya çalışılıyorken kuantum bilgisayarlarla olasılıkların hepsi aynı anda denenebilir. Bu anlamda, bu tarz algoritmalar, şu anda kullanılıyor olsa da bilgi güvenliği için kullanışsız duruma geçeceklerdir.

2.2. Gerçek Rastgele Sayı Üreteçleri

GRSÜ'ler tahmin edilemez ya da edilmesi zor bazı fiziksel süreçleri kullanarak bir entropi kaynağı oluştururlar ve bu oluşturulan düzensizlik kaynağı ile rastgele sayılar üretirler. Entropi kaynağı, elde edilen sayıların tahmin edilemez ve tekrar üretilemez olması açısından önemlidir. Bu düzensizlikler, bilgisayarlar içerisindeki yazılım kaynaklı fiziksel verilerden elde edilebileceği gibi sistemle birleştirilebilen ayrı bir cihaz ile de sağlanabilmektedir [69]. Genel olarak çalışma mantıkları, ölçülen değerin belirlenen sınırların altında ya da üstünde olmasına göre 0 veya 1 değeri verilmesine dayanmaktadır. Johnson-Nyquist etkili, Zener (diyot) gürültülü, kaotik gürültülü, osilatörlerde frekans kayması ve kuantum tabanlı gibi çeşitli entropi kaynaklı üreteçler GRSÜ olarak kullanılmaktadır [70 - 77].

GRSÜ'ler ile sayılar üretilmeden önce, bilgisayar tarafından, bir tahmin edilemez fiziksel veriler havuzu oluşturulur ve bu havuza entropi denilmektedir. Bu veriler ses kartlarından, kesme zamanlarından, kullanıcılardan (klavye veya fare hareketleri), termal gürültüden vb. tahmin edilemez süreçlerden elde edilmektedir. Örneğin, Linux ve Windows (95'ten sonraki sürümleri) işletim sistemleri entropilerini klavye ya da fare hareketlerine göre oluşturmaktadır [78, 79]. Tahmin edilebilir kaynakların kullanımı güvenlik açıkları meydana getirdiğinden kaynağın çok iyi seçilmesi gerekmektedir. Kaynağın iyi seçilmesinin önemine yönelik 1996 yılında yapılan bir çalışma, Netscape tarayıcısının SSL (Güvenli Soket Katmanı)'de üretilen anahtarları için, tahmin edilebilir entropi kaynakları (saat değerleri gibi) kullanıldığı için çeşitli saldırılara maruz kalındığı ortaya konulmuştur [80]. Entropisini, termal gürültü veya boşta çalışan bir osilatör yardımıyla elektronik devrelerdeki değişikliklere göre

oluşturan sistemler de yukarıda bahsedilen kaynaklara ek olarak verilebilir [81 - 83].

Entropi kaynakları tek başlarına tam anlamıyla rastgelelik sağlayamadıklarından, rastgeleliğin kuvvetlendirilmesi, yanlılığın ve korelasyonun ortadan kaldırılması adına ek bir işlem olarak süreç sonrası işlemi uygulanmaktadır. John von Neuman tarafından temelleri atılmış olup Yuval Peres ve Ari vd. tarafından geliştirilen süreç sonrası işlemi, tamamen deterministik bir yöntemdir [84 - 86]. Entropi oluşturularak elde edilen rastgele sayılar girdi olarak kullanılır ve çıkışta, girişten daha kısa bit değerleri elde edilir. Entropiye dair geniş bir inceleme Bölüm 3.1'de verilmiştir.

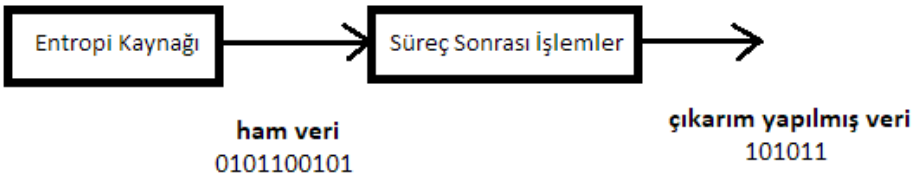
GRSÜ'ler tahmin edilememezlik konusunda SRSÜ'lerden daha iddialı olmalarına rağmen GRSÜ'lerle ilgili bazı kısıtlamalar vardır. İlk olarak, düzensizlik kaynağı kullanılarak 0 veya 1 sayılarının elde edilme olasılığı birbirlerine eşit olmayabilir [83]. Bu nedenle bazı uygulamalar için eğilimi engelleyici ek süreçler kullanılmaktadır [87 - 89]. Bununla birlikte, GRSÜ'ler daha düşük bit aralıklarında sayı ürettikleri için SRSÜ'ler kadar hızlı değillerdir. Bir diğer dikkat edilmesi gereken konu ise, kullanılan veriler, göz ardı edilen durumlardan yola çıkılarak elde edildiği için verilerin rastgeleliği konusunda kesin bir sonuca varılamamaktadır. Entropi süreçleriyle ilgili herhangi bir hata, yanlışlık olduğu takdirde bu yanlışlığın ortaya çıkarılması çok zordur [50]. Dahası, sistemlere ayrıca dâhil edilen GRSÜ'ler zahmetlidirler ve bu nedenle kullanımları zordur.

RSÜ'lerin elde edilme süreçlerine göre farklılaştığı ve birbirlerine göre olumlu / olumsuz yönlerinin ifade edildiği bu bölümden sonra, devamındaki bölümde, tez çalışmasının da dâhil olduğu, gerçek rastgele sayı üreteçlerinin bir alt kümesi de olan, Kuantum Rastgele Sayı Üreteçlerine dair incelemeler sunulacaktır.

3. KUANTUM RASTGELE SAYI ÜRETEÇLERİ

KRSÜ'ler, verilerin kuantum süreçlerden elde edildiği bir çeşit gerçek rastgele sayı üreteçleridir. Gerçek sayı üreteçlerinin genel özelliği olarak, üretilen sayıların rastgeleliğinin yanında fiziksel değişkenlerin de rastgele olması beklenir. Bölüm 2.2'de değinildiği gibi GRSÜ'lerin süreçlerinin ne kadar rastgele olabileceği tartışma yaratabiliyorken KRSÜ'lerde kuantum vakum dalgalanmaları gibi mutlak rasgelelik kaynağı olan ve doğal raslantısal süreçlerle ortaya çıkan olaylar kullanılmaktadır. Bu nedenle rastgelelik konusunda soru işareti bırakmamaktadır. Bunun yanı sıra, fiziksel süreç dikkate alındığında, diğer entropi kaynaklı (gerçek) rastgele sayı üreteçlerinin hız sorununa da bir çözüm olarak ortaya çıkmaktadır.

Şekil 3.1'de, gerçek rastgele sayı üreteçlerine yönelik genel bir blok şeması gösterilmiştir. Fiziksel kaynaklardan elde edilen ve belirli bir entropisi olan veriler, süreç sonrası işlemlerden geçirildikten sonra bir çıkarım elde edilir. Elde edilen bu çıkarım yapılmış sayı dizileri, ham veri boyutundan çok daha küçük boyutlara (bit) indirilmektedir.



Şekil 3.1. GRSÜ Blok Şeması

Entropiler, rastgele fiziksel süreçlerin okunmasıyla oluşturulmakta olup dijital uygulamalar için analog verilerden dijital veriler elde edilebilmesi adına dönüştürücüler kullanılmaktadır. Bu esnada dijital sayılara çeşitli gürültüler eklendiğinden bu aşamadaki sayılara "ham veri" denilmektedir. Fiziksel süreçler yardımıyla elde edilen dijital rastgele sayılardaki gürültülerden kurtulmak ve daha güçlü rastgele sayılar elde edebilmek için "süreç sonrası işlemler" denilen bir dizi işlem uygulanır. Süreç sonrası işlemlerle elde edilen çıkarım yapılmış veri, rastgeliği kuvvetlendirilmiş sayı dizileridir.

KRSÜ, sadece ham verinin elde edilmesi sırasında diğer GRSÜ'lerden farklılık gösterdiği için (klasik fizik yerine kuantum fizik yasaları kullanılmaktadır) KRSÜ'lerin de, bütün GRSÜ'lerin sahip olması gerektiği gibi, bir entropiye sahip olması beklenir. Bundan sonraki alt bölümde entropinin tanımı ve çeşitleri üzerine durulmuştur.

3.1. Entropi

Entropi, termodinamikte sistemin düzensizliği için kullanılan bir tabir iken bilgi güvenliğinde rastgeleliği ölçmek için kullanılır ve bit cinsinden ölçülür. Kullanılan bilginin, ham verinin, ne kadar sıkıştırılabilir olduğunun tayini için kullanılmaktadır [90]. Oluşturulan entropi, olayların olma olasılıkları bakımından bir yanlılık gösteriyorsa bilginin sıkıştırılabilirliği artarken; aksi durum için sıkıştırılabilirliği zorlaşmaktadır. Bilginin daha fazla sıkıştırılabilmesine sebebiyet veren olaylar için ilgili entropi kaynağının yeterli rastgelelikte olmadığı söylenebilmektedir.

Entropinin sıkıştırılabilir bilgi ile ilişkisi 1948 yılında Shannon tarafından yapılan bir çalışma ile gösterilmişken, Sheldon Ross tarafından yapılan çalışma ile de entropi ile bir olayın sonucunda yaşanan sürpriz arasındaki ilişki ortaya konmuştur [91, 92]. Bu çalışmaya göre, bir olayın olma olasılığı ne kadar düşükse, düşük olasılıklı olay meydana geldiğinde yaşanan sürpriz o kadar büyük olur. Bu durumda, elde etme olasılığı eşit sürprizli durumlar için bütün bitleri kullanmak gerekirken, daha düşük sürprizler içeren olaylar için kullanılacak bit sayısı düşmektedir.

İlk olarak Shannon entropi adı altında entropi ölçümleri yapılmaya başlanmış olup sonraki yıllarda farklı entropi ölçümlerine dayanan teoriler öne sürülmüştür. Devam eden alt kısımlarda, entropi teorilerine dair açıklamalar yer almaktadır.

3.1.1. Shannon Entropi

Shannon entropi, 1948 yılında C. E. Shannon tarafından bulunmuş bir entropi ölçümüdür ve

$$H(X) = -\sum_{x \in A} P_X(x)\ log_2 P_X(x) \tag{3.1}$$

eşitlik 3.1'de gösterildiği şekliyle tanımlanır [92]. Burada kullanılan $P_X(x)$, çıkıştan x alma olasılığını; X, rastgele değişkeni; A, sayısal veri setini ve x de çıkışı temsil etmektedir. Shannon entropisi, X rastgele değişkenin x değerini tanımlamak için ihtiyaç duyulan en küçük ortalama değeri verir.

Tablo 3.1. Olasılıkların eşit olduğu dağılım

x	$\mathrm{P}(x)$	Dizi
1	1/4	00
2	1/4	01
3	1/4	10
4	1/4	11

Tablo 3.1'de, entropi kavramı bir örnekle açıklanmıştır. X kümesinin 1, 2, 3 ve 4'ten oluştuğu varsayımı (4 kenarlı düzgün bir cisim gibi düşünülebilir) üzerine $\mathrm{P}(x)$' i her bir x değeri için düzgün cismin havaya atıldıktan sonra rastgele bir kenarın gelme olasılığı olarak tanımlayabiliriz. Üçüncü sütunda, her bir olası x değeri için atanan bit dizileri yer almaktadır. Bu dağılıma göre Shannon entropisini hesaplarsak:

$$x = 1\ için\ H(1) = -\left[\frac{1}{4}\ log_2 \frac{1}{4}\right] = \frac{1}{2}$$

$$x = 2\ için\ H(2) = -\left[\frac{1}{4}\ log_2 \frac{1}{4}\right] = \frac{1}{2}$$

$$x = 3\ için\ H(3) = -\left[\frac{1}{4}\ log_2 \frac{1}{4}\right] = \frac{1}{2}$$

$$x = 4\ için\ H(4) = -\left[\frac{1}{4}\ log_2 \frac{1}{4}\right] = \frac{1}{2}$$

O halde, sonuçta

$$H(X) = 4\left(\frac{1}{2}\right) = 2$$

bit elde edilir.

Yukarıdaki örnekten farklı olarak, Tablo 3.2'de, x değerlerinin elde edilme olasılığının eşit olmadığı, diğer bir deyişle 4 kenarlı cismin hileli olduğu, durum için geçerli örnek değerler gösterilmiştir.

Tablo 3.2. Olasılıkların eşit olmadığı dağılım

x	$\mathrm{P}(x)$	Dizi
1	1/4	00
2	3/8	110
3	5/16	1011
4	1/16	0111

Tablo 3.2'de yer alan değerlere göre hileli cismin Shannon entropisi:

$$x = 1\ için\ H(1) = -\left[\frac{1}{4}\ log_2 \frac{1}{4}\right] = 0{,}5$$

$$x = 2\ için\ H(2) = -\left[\frac{3}{8} log_2 \frac{3}{8}\right] = 0{,}53$$

$$x = 3\ için\ H(3) = -\left[\frac{5}{16}\ log_2 \frac{5}{16}\right] = 0{,}524$$

$$x = 4\ için\ H(4) = -\left[\frac{1}{16}\ log_2 \frac{1}{16}\right] = 0{,}25$$

O halde, sonuçta

$$H(X) = (0.5 + 0.53 + 0.524 + 0.25) = 1{,}805$$

bit değeri elde edilir.

Tablo 3.1 ve Tablo 3.2'de yer alan değerlere göre dağılımların farklı olduğu iki örnek için Sheldon Ross'un tanımını da kullanarak, dağılımın eşit olmadığı, daha az sürprizli, durumlar için daha az bit ihtiyacının; sürprizlerin eşit olduğu dağılımlarda ise bitlerin tamamına ihtiyacın olduğu görülmektedir. Ayrıca, Shannon entropinin değeri ne kadar büyükse dağılımın tekdüzeliği de o kadar kuvvetlidir şeklinde bir çıkarım yapmak mümkündür.

3.1.2. Rényi Entropi

Rényi entropi, 1961 yılında Alfred Rényi tarafından geliştirilmiştir [93].

$$H_\alpha(X) = \frac{1}{1-\alpha}\, log_2 \sum_{x \in A} P_X(x)^\alpha \tag{3.2}$$

Entropi, eşitlik 3.2 ile ifade edilmektedir ve limit $\alpha \to 1$ için Shannon entropisi elde edilmekte olduğundan Shannon ailesinden geldiği söylenebilir. Shannon entropi gibi Rényi entropi de toplanabilirdir ve (eşit $1/n$ olasılıkları için) maksimum entropisi $\ln n$ ile bulunabilir. Renyi entropi; ekoloji ve istatistik bilimlerinde çeşitlilik indeksi olarak, kuantum haberleşmede ise dolaşıklık ölçüsü olarak kullanılmaktadır [94, 95].

Rényi entropide Shannon entropiden farklı olarak, olasılık dağılımlarını daha hassas hale getirebilmek için kullanılan ek bir α değeri vardır ve α' nın farklı değerleri için farklı seviyelerde gizlilik ve rastgelelik sınırlamaları elde edilmiştir. Bunlara ilişkin ortaya çıkan entropi tanımları takip eden alt bölümlerde verilmiştir.

3.1.2.1. Hartley Entropi (Maksimum Entropi)

1928 yılında Hartley'in çalışmalarından yola çıkılarak çeşitli araştırmacıların birikimleri ile bilgi teknolojisi alanına uyarlanmıştır [96]. Rényi entropisi formülasyonunda $\alpha = 0$ değeri için kullanılan ve olasılıklardan bağımsız olarak (bütün olasılıklar birbirlerine eşittir) maksimum değerin elde edildiği entropidir (eşitlik 3.3). Diğer bir deyişle, gürültülü bir kanal üzerinde yapılacak kodlamanın en fazla ne kadarlık bir bit kapasitesinde olması gerektiğini belirtir.

$$H_{\alpha=0}(X) = \frac{1}{1-(\alpha=0)}\ log_2 \sum_{x\in A} P_X(x)^{\alpha=0} = log\ |X| \tag{3.3}$$

3.1.2.2. Shannon Entropi

limit $\alpha \to 1$ için elde edilen ve her bir değere karşılık gelen ihtimallerin dikkate alındığı entropidir. Bölüm 3.1.1.'de detaylandırılmıştır.

3.1.2.3. Çarpışma Entropisi

$\alpha = 2$ değeri için kullanılan entropi çeşididir (eşitlik 3.4). Çarpışma entropisi yerine daha çok Rényi entropisi tabiri kullanılmaktadır. Aynı olasılık dağılımına sahip birbirlerinden bağımsız iki rastgele değişkenin negatif logaritmasıdır.

$$H_{\alpha=2}(X) = \frac{1}{1-(\alpha=2)}\ log_2 \sum_{x\in A} P_X(x)^{\alpha=2} = -log\ P(X=Y) \tag{3.4}$$

3.1.2.4. Min (Minimum) Entropi

$$H_{\alpha=\infty}(X) = \frac{1}{1-(\alpha=\infty)}\ log_2 \sum_{x\in A} P_X(x)^{\alpha=\infty} = -log(max\ P_X(x)) \tag{3.5}$$

En yüksek olasılıklı olay üzerinden tahmin edilemezliğin ölçülmesi için en tedbirli yol olarak kullanılmaktadır (eşitlik 3.5). Minimum entropi, çıkışta elde edilecek sayıların ortalama tahmin edilebilirlik değerini veren Shannon entropiden daha büyük bir bit değeri vermemektedir. Bu nedenle, rastgeleliğin sağlanabileceği en kötü durum için kullanılan bit sayısı olarak da

tanımlanabilmekte olup dağılımların rastgeleliğini ölçmek için yaygın olarak kullanılmaktadır. Tablo 3.1'de gösterilen eşit olasılık dağılımlı örnek için minimum entropisini hesaplarsak:

$$x = 1,2,3,4\ için\ H(x) = -\left[log_2 \frac{1}{4}\right] = 2$$

bit değeri elde edilmektedir. Bir diğer örnek olarak verilen Tablo 3.2'deki eşit olmayan olasılık dağılımlı olayın minimum entropi ise en yüksek olasılık x' in 2 olduğu durumda geçerli olduğundan:

$$x = 2\ için\ H(2) = -\left[log_2 \frac{3}{8}\right] = 1{,}415$$

bit olarak elde edilir. Eşit olasılıkta olmayan dağılıma sahip bir olay için, güvenli bir sayı üretilmek isteniyorsa, Shannon entropiden elde edilen 1,805 bit değeri yerine 1,415 bitlik bir sayı üretilmesi gizlilik açısından daha güvenli olacaktır.

Rastgeleliğin sağlanabileceği en güvenli entropi çeşidi olarak görülen minimum entropiye göre entropi oluşturulduktan sonra bir üretecin GRSÜ olarak kullanılabilmesi tek başına yeterli olmamaktadır. Toplanan ham veriler üzerindeki gürültülerin ortadan kaldırılarak rastgeleliğin kuvvetlendirilmesi için, oluşturulan bu entropi havuzuna ayrıca süreç sonrası işlemler uygulanmaktadır ve süreç sonrası işlemlerle ilgili bilgilendirmeler bir sonraki bölümde ele alınmıştır.

3.2. Süreç Sonrası İşlemler

Üretilen ham bitler arasındaki bağıntıların ortadan kaldırılarak, normal dağılıma yakın olacak düzeyde, ham bitlerin rastgele bitlere dönüştürülmesi için uygulanan işlemler bütünüdür. Bölüm 3.1'de değinildiği üzere, entropinin fazla olması mutlak rastgeleliğin elde edilebileceği anlamına gelmediği için yeterli entropi sağlandıktan sonra ek işlemler uygulanarak rastgelelik kuvvetlendirilmektedir.

Tekdüzelik,

$$d(X,Y) = \max_{a \in A} |P_X(a) - P_Y(a)| \tag{3.6}$$

eşitliği ile ifade edilmektedir. Eğer bu fark,

$$d(X,Y) \leq \varepsilon \tag{3.7}$$

ile ifade edilebiliyorsa X ve Y dağılımları birbirlerine ε kadar yakın demektir. Rastgeleliğin çıkarımı aşamasında, çıkışta elde edilen rastgele sayıların, mümkün olduğu kadar tekdüze olması istenir. Diğer bir deyişle, n bitlik ham veri; 0 ve 1'lerden oluşan ϵ hatalı tekdüze bir dağılımla, m bitlik bit dizilerine dönüştürülür.

Çıkarım işleminde, ham veriye çok fazla müdahale edilmeden, çok küçük dış etkilerle rastgele sayıların elde edilmesi istenmektedir. Ham verinin minimum entropisi (bkz. 3.1.2.4), çıkarım işleminden sonra elde edilecek bit sayısının sınırını vermektedir. Yani, X dağılımlı n bitlik ham verinin minimum entropisi $H_\infty(X) = k$ olursa, çıkarım işleminden sonra tekdüzeliğe yakın, en çok k bit kadar veri elde edebiliriz.

Deterministik çıkarımcılar eşitlik 3.8'de yer alan ifade ile,

$$\{0,1\}^n \rightarrow \{0,1\}^m \tag{3.8}$$

Gösterilmektedir ve n bitlik ham verinin m bitlik çıkarım yapılmış veriye dönüştürülmesini ifade etmektedir. Sadece tek bir kaynaktan üretilen bit dizisi kullanılmasından dolayı basit bir işlem olsa da kaynağın rastgelelik gücüyle orantılı olarak kuvvetli rastgele sayılar elde edilmektedir. Farklı zayıf rastgelelik kaynaklarının kullanıldığı çalışmalar literatürde bulunmakta olup birden fazla zayıf kaynaktan yararlanılarak üretilen rastgele sayı örnekleri de bulunmaktadır [97 - 100].

Farklı kaynakların kullanılması prensibine dayanan tohumlu çıkarımcılar, bir tanesi zayıf diğeri ise tekdüzelik açısından güçlü olmak üzere iki farklı kaynak kullanmaktadır. Tohumlu çıkarımcılarda, n bitlik ham dizi ile d bitlik tekdüze bir rastgele bit dizisi, eşitlik 3.9'da görüldüğü gibi m bitlik bir çıkış üretirler. Burada d 'nin m 'den küçük olması beklenir. İlk olarak Nisan ve Zuckerman tarafından tanımlanmış olup çıkarımdan sonra elde edilen çıktı değeri, giriş entropisini taşımaktadır [101, 102].

$$\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m \tag{3.9}$$

Tohumlu çıkarımcılar, dış müdahalelere karşı bir koruma sağladığı için KRSÜ için tercih edilebilir olmaktadırlar [103]. Trevisian çıkarımcı ile özüt fonksiyonlarından faydalanılan çıkarımcı, en sık karşılaşılan çıkarımcılardır [104]. Trevisian çıkarımcılar, kuantum kaynaklı dış müdahalelere karşı dirençli olmaları ve tohum rastgeleliğini koruyabilmeleri sebebiyle tercih edilebilir olmaktadırlar; ancak Trevisian çıkarımcılarda bit üretimi sırasında yapılan hesaplamalar, rastgele sayı üretme hızını düşürmektedir. Bununla birlikte, özüt fonksiyonlarından biri olan Artık Özüt Lemma ile yeterince yüksek entropiye sahip bir giriş kullanılarak çıkışta neredeyse tekdüze rastgele sayılar elde edilebilmektedir. Fiziksel gürültülü (dinleyicinin müdahale edip rastgeleliği etkileyebileceği) KRSÜ'de bile, ilgili gürültü ortadan kaldırılarak gerçek rastgele sayılar elde edilebilmektedir [105]. Üstelik rastgeleliğin kuvvetli olmadığı kaynaklar ve gizli olmayan tohumlarla bile güvenli bir çıkarım işlemi yapılabilmektedir [106 - 107]. Artık Özüt çıkarımcılarda, büyük tohum kaynaklarının kullanılmasına ihtiyaç duyulsa da yine de Trevisian çıkarımcıya göre daha hızlıdırlar [108]. Özellikle, n bitlik ham veriler ile tohum matrisinin çarpılması sonucunda, birbirlerinden tamamen bağımsız bit değerlerinin elde edilmesinin mümkün olduğu Toeplitz özütleme işlemi, oldukça hızlıdır. Bütün bu olumlu özelliklerinin yanı sıra, özütleme işleminde rastgeleliğin korunabilmesi için tohumların her kullanımda değiştirilmesi gerekmektedir.

Belirli bir entropiye sahip ham verinin çıkarım işlemiyle rastgeleliği kuvvetlendirildikten sonra, çıkarım yapılan sayıların gerçekten rastgele olup

olmadıklarının tayin edilmesi gerekmektedir. Bir sayının gerçekten rastgele olup olmadığına yönelik net bir karar alınamamakla birlikte bazı istatistiksel teslerden geçirilerek bir sonuca varılabilmektedir.

3.3. Rastgelelik Testleri

1950 yılında Kolmogorov tarafından yapılan çalışma sonrası sayıların rastgeleliği, Kolmogorov karmaşıklığı adı altında tayin edilmekte idi; ancak daha sonraki yıllarda rastgeleliğin tayin edilmesi, doğrulanması için bazı istatistiksel testler kullanılmaya başlanmıştır [66, 109 – 112, 143]. Uygulanan testler, bir sayı dizisinin rastgeleliğini kanıtlamamakla birlikte (sonlu bir dizinin gerçek bir rastgele sayılar dizisi olup olmadığının tespiti mümkün değildir) sayılar arasında örüntüler olup olmadığını bulmaya yöneliktir. Böylece, üretilen sayı dizisinin tahmin edilebilirliği/edilemezliği, çeşitli istatistiksel algoritmalarla ölçülmektedir.

Tahmin edilemezliğin ölçülmesi için ilk olarak 11 testten oluşan Knuth test takımları kullanılmaya başlanmıştır; ancak yeteri kadar rastgele olmayan bir dizi için istenen olumsuzlukta bir sonuç vermediği ortaya konulduğu için tercih edilebilir olmaktan çıkmıştır [54, 142]. Knuth'un test takımının eksikliğinin giderilmesine yönelik olarak 1996 yılında ortaya konan ve 16 testten oluşan DieHard testleri günümüzde de kullanılmaktadır; ancak testlerdeki giriş parametrelerinin değiştirilemiyor olması ve girişin 32 bitlik paketler halinde yapılma zorunluluğunu içeriyor olması sebebiyle kısıtlayıcı olabilmektedir [112, 143]. 2001 yılında, NIST (National Institute of Standards and Technology) tarafından, var olan ve yeni geliştirilen algoritmaların birlikte yer aldığı 15 testten oluşan bir test takımı sunulmuştur. Bu testlerde de parametreler sabitlenmiş olmakla birlikte uzun bit dizilerinin test edilebildiği kapsamlı bir test takımı olmasından dolayı tercih sebebi olmaktadır. Bu nedenle, tez çalışması kapsamında üretilen rastgele sayılara da NIST'nin hazırlamış olduğu test takımı uygulanmıştır [66, 142].

NIST tarafından sunulan istatiktiksel rastgelelik tayini takımı, 15 adet testten oluşmaktadır. Her bir testte P ile ifade edilen bir olasılık hesabı yapılmaktadır. P değeri, ürettiği her sayı dizisinin mutlak rastgelelikte olduğu var sayılan bir

üretecin, test edilen diziden daha az rastgelelik barındıran bir dizi üretilebilme olasılığını ifade etmektedir. Hesaplanan P değerlerinin anlamlandırılabilmesi için bir sınır değeri seçilir ve bu sınır değeri genellikle 0,001 ile 0,01 aralığındadır. Bu tez kapsamında sınır değeri 0,01 seçilmiştir. Bu durumda, P değerlerinin seçilen her bir test için 0,01'den büyük olması istenmektedir; küçük olduğu durumda istenen sınır değeri için üretilen sayıların yeterli rastgeleliği barındırmadığı sonucu çıkarılmaktadır. Eşit olduğu durumda ise, test edilen sayıların oldukça kuvvetli bir rastgelelik barındırdığı söylenebilmektedir [66].

NIST kapsamında uygulanan testlerle ilgili olarak sonraki alt bölümlerde bilgi verilmekte olup kullanılan algoritmalara dair detaylar [66]'da yer almaktadır.

3.3.1. Frekans Testi

Test edilecek dizide yer alan 0 ve 1'lerin görülme olasılıklarının hesaplanması üzerine kurulmuştur. 0 ve 1'lerin görülme olasılıklarının aynı, diğer bir deyişle $1/2$'ye eşit olmasının değerlendirmesi yapılmaktadır. Testin verimli olabilmesi adına test edilecek sayı dizileri için istenen başlangıç koşulu; test edilecek bit dizisinin (n) 100'den büyük olmasıdır.

3.3.2. Bir Blok İçerisinde Frekans Testi

Bit dizisinin, M bit dizilik bloklara ayrılarak her bir blok için 0 ve 1 görülme sıklığının hesaplanması üzerinedir. Başlangıç koşulu olarak; n $(n \geq MN)$'nin 100'den büyük, M'nin 20'den büyük ve N (blok sayısı)'nin 100'den küçük olması önerilmektedir.

3.3.3. Koşum Testi

Art arda gelen 0 ve 1 bit dizilerinin (tekrar), bütün bir veri setinde ne kadar meydana gelmiş olduğunun saptanmasına yöneliktir. Bununla birlikte algoritma, 0 ve 1'ler arasındaki salınımı (çok hızlı ya da çok yavaş) da hesaplamaktadır. Çok yavaş salınımlarda, rastgele sayılarda olması tercih edilmeyen çok uzun tekrarlar, dolayısıyla çok az değişiklik görülmektedir. Benzer şekilde, çok hızlı salınımlarda, yine rastgele sayılarda olması tercih edilmeyen çok kısa tekrarlar,

dolayısıyla daha fazla değişiklik görülmektedir. Başlangıç koşulu olarak n' nin en az 100 bit olması istenmektedir.

3.3.4. Bir Blok İçerisindeki En Uzun Bir Tekrarı Testi

Bölüm 3.3.3'ten farklı olarak M bitlik bloklar içerisinde en uzun 1 tekrarını (0'lar ile benzer olduğu için sadece 1 için yapılması yeterlidir) incelemektedir. Başlangıç koşulu olarak, Tablo 3.3'te belirtilen değerlere dikkat edilmesi önerilmektedir.

Tablo 3.3.43. Bir Blok İçerisindeki En Uzun Bir Tekrarı Testi için tavsiye edilen başlangıç koşulları

Minimum n	M
128	8
6272	128

3.3.5. İkili Matris Rankı Testi

Bütün bit dizisinin, ayrık alt matrislerle arasında doğrudan bir bağlantı olup olmadığının incelenmesi üzerine kurulmuştur. Başlangıç koşulu olarak, n' nin $38MQ$ çarpımından büyük veya eşit olması istenmekte olup birbirlerine eşit olan M (bu test için satır sayısı) ve Q (sütun sayısı) değerlerinin en az 32 olması önerilmektedir –ki bu da n 'nin en az 38,912 bit olması anlamına gelmektedir.

3.3.6. Ayrık Fourier Dönüşümü Testi

Birbirlerine yakın tekrarlanan örneklerin rastlantısallık varsayımından sapmasının tespit edilmesi üzerinedir. Başlangıç olarak n 'nin en az 1000 bit olması önerilmektedir.

3.3.7. Çakışmayan Şablon Eşleme Testi

Seçilen periyodik olmayan şablonun, çakışmayan bitleri de içerecek şekilde, bit dizilerinde görülme sıklığının bulunması üzerine oluşturulmuştur. İlgili şablon bulunduğu takdirde sayaç artırılarak ortalama görülme sıklığı üzerinden sonuca varılmaktadır. Başlangıç koşulu olarak; m (şablon bit sayısı), 2-10 bit arasında

olabilir; ancak sağlıklı bir test için 9 ve 10 bit olarak kullanılması önerilmektedir. Benzer şekilde, daha anlamlı P değeri elde edebilmek adına, değerler $n \geq MN$, $N \leq 100$ ve $M > 0.01n$ olacak şekilde seçilmelidir.

3.3.8. Çakışan Şablon Eşleme Testi

Bölüm 3.3.7'de belirtilen teknikten farklı olarak, sayacın değişmesine etki eden şablon bulunduğu takdirde bir sonraki bitten itibaren inceleme yapılmaktadır. m'nin 9 ve 10 seçilemediği durumlarda NIST, farklı başlangıç koşullarının kullanılmasını önermektedir.

3.3.9. Maurer'in Evrensel İstatistiksel Testi

Bit dizisinin ne kadar sıkıştırılabilir olduğunun tayini üzerinedir. Çok fazla sıkıştırılabilen dizilerin rastgele olmadığı kabul edilmektedir. Başlangıç koşulu olarak Tablo 3.4'ün kullanılması önerilmektedir.

3.3.10. Doğrusal Karmaşıklık Testi

Dizilerin, rastgele olabilecek kadar karmaşıklık içerip içermediğinin bulunması üzerinedir. Başlangıç koşulu olarak $n \geq 10^6$, $500 \leq m \leq 5000$ ve $N \geq 200$ şeklinde seçilmesi önerilmektedir.

Tablo 3.3.10. Maurer'in Evrensel İstatistiksel Testi için başlangıç koşulları

n	L(blok uzunluğu)	Q (blok sayısı)= $10\ x\ 2^L$
≥387.840	6	640
≥904.960	7	1280
≥2.068.480	8	2560
≥4.654.080	9	5120
≥10.342.400	10	10240
≥22.753.280	11	20480
≥49.643.520	12	40960
≥107.560.960	13	81920

≥231.669.760	14	163840
≥496.435.200	15	327680
≥1.059.061.760	16	655360

3.3.11. Seri Test

m bitlik şablonların görülme olasılığı farklı m bitlik şablonların görülme olasılıklarıyla aynı olmalıdır. O nedenle, m-bit çakışan örüntülerin meydana gelme sayısının, rastgele bir sıra için beklenen sayısıyla aynı olup olmadığı belirlenmeye çalışılmaktadır. Başlangıç koşulu olarak $m < \lfloor log2n \rfloor - 2$ dikkat edilmesi yeterlidir.

3.3.12. Yaklaşık Entropi Testi

m ve $m + 1$ uzunluğundaki bit bloklarının dizide ne kadar sıklıkla yer aldığınının belirlenmesi üzerine uygulanmaktadır. Başlangıç koşulu olarak $m < \lfloor log2n \rfloor - 5$ dikkat edilmesi yeterlidir.

3.3.13. Birikerek Artan Toplamlar Testi

Test edilecek dizide 0 değerleri için -1 verilerek çeşitli şekillerde bitler toplamı elde edilir ve rastgeleliğin sağlanıyor olması adına sonucun 0'a yakın olması beklenir. Dizi uzunluğunun en az 100 bit olması başlangıç için yeterlidir.

3.3.14. Rastgele Gezinimler Testi

Bölüm 3.3.13'te uygulanan yöntemden farklı olarak; elde edilen toplamlardan bir rastgele bit oluşturularak (bloklara bölünme suretiyle), ham rastgele dizide tekrarların kontrol edilmesi üzerinedir. Başlangıçta kullanılacak n dizisinin en az 10^6 bit uzunluğunda olması önerilmektedir.

3.3.15. Değişimli Rastgele Gezinimler Testi

Bu testin amacı rastgele yürüyüşteki çeşitli durumların beklenen değerinden sapmasının tespit edilmesidir. 3.3.14'te olduğu gibi başlangıçta kullanılacak n dizisinin en az 10^6 bit uzunluğunda olması önerilmektedir.

NIST kapsamında sunulan 15 test için, testlerin amaçları ve önerilen başlangıç değerleri toplu olarak sırasıyla Tablo 3.5 ve 3.6'da verilmiştir.

Tez çalışması kapsamında yapılanlara geçmeden önce, sonraki bölümde, yaygın olarak kullanılan bazı KRSÜ çeşitlerine değinilecektir.

3.4. Kauntum Rastgele Sayı Üreteçleri Çeşitleri

Kuantum rastgele sayı üreteçlerine dair detaylı bir inceleme [50]'de yapılmakta olup bu bölümde KRSÜ'ler içerisinde çokça bilinen üç çeşit KRSÜ'ye değinilecektir.

3.4.1. Radyoaktif Bozunmaya Dayalı Üreteçler

Radyoaktif bozunma; α, β ve γ ışınlarının yakalanmasına ve yükselteçten geçirilerek sayılmasına dayanan üreteçlerdir [113 – 115]. Geiger-Müller (GM) tüpleri adı verilen tüplerle yapılan iyonlaştırma işlemi yeterince güvenilir ve hassas ölçümler yapabilmektedir [116]. Radyoaktif bozunmaya dayalı KRSÜ'lerin güvenilir olmalarının yanı sıra bazı kısıtlamaları da bulunmaktadır. Öncelikle, üretilen sayıların bit sayısı görece azdır [117]. İkinci olarak, sayım için kullanılan detektör iyi bir şekilde izole edilmediği sürece, diğer radyoaktif materyalden gelen her tür parçacık sayılabilmektedir. Bu durum, radyoaktif bozunma KRSÜ'lerinin yaygın kullanımını engellemektedir. İstenen verimin elde edilmesi için de oldukça yüksek radyoaktiviteli kaynak kullanılması gerekmektedir. Bu da oldukça geniş güvenlik önlemlerine ihtiyaç duyulması anlamına gelmektedir. GM sayaçları, ucuz ve istikrarlı çalışırlar; ancak GM sayaçlarında "ölü zaman" adı verilen durumlar görülmektedir. Yaşanan ölü zamanlarda üretim hızı birkaç yüz milisaniyeden birkaç milisaniyelere düşmektedir [118]. Ölü zaman prensibi kabaca şöyledir: Pozitif iyonlar, tüpün içinde yer alan katodu çevrelediği an çığ çalışmayı durdurur ve iyonlar eski halini alana kadar tekrar bir çığ oluşumu gözlenemez. Bu durumda sayaçlar çalışamadığından verimli bir sayım yapıldığı söylenemez. GM sayaçlarında yaşanan ölü zamanların dezavantajını ortadan kaldırmaya yönelik bazı çalışmalar literatürde mevcuttur [119 – 121]. Yukarıda sıralanan

dezavantajlarına ek olarak, Geiger tüpleri ve yarıiletken detektörler radyasyondan zarar görebildikleri için ilgili koşullar sağlandığı takdirde gerçek rastgele sayı üretilmesi konusunda bazı sıkıntılar yaşanabilecektir. Bütün bu bahsedilen olumsuzluklarına rağmen yüksek hızın gerekli olmadığı ve şartların uygun olduğu SRSÜ uygulamaları için tercih edilebilmektedir.

3.4.2. Elektronik Saçma Gürültülü KRSÜ

Elektronik devrelerde görülen akımın bir çeşit elektron akışından ileri gelmesinden ve rastgele olmasından yola çıkılarak ortaya çıkmıştır [70, 71, 122]. Optik uygulamalarında da fotonların dalgalanmaları esnasında görülen rastgelelik kullanılmaktadır. Bu iki durum için de Poisson dağılımı gözlenmekte olup Poisson dağılımını takip eden olaylar ortalama bir hızda ve birbirinden bağımsız kabul edildiği için elektronik saçma gürültüsü ölçümü rastgele sayı üretimi için uygun varsayılabilmektedir; ancak, elektronik saçma gürültüye dayalı üretimin, dengeleyici voltaj dalgalanmaları nedeniyle, yeterince rastgele olamayabileceği [123]'te belirtilmektedir.

Tablo 3.5. NIST testlerinde bulunmaya çalışılan kusurlar [66]

Frekans Testi	Çok fazla 1 veya 0 olması
Bir Blok İçerisinde Frekans Testi	M bitlik bloklara ayrılan dizinin, her bir M bloğunda çok fazla 1 veya 0 olması
Koşum Testi	0 ve 1 değişikliklerinden meydana gelen salınımın çok hızlı veya çok yavaş olması
Bir Blok İçerisindeki En Uzun Bir Tekrarı Testi	M bitlik bloklara ayrılan dizinin, her bir M bloğundaki 1 değişim salınımının çok hızlı veya çok yavaş olması
İkili Matris Rankı Testi	Tekrar eden ayrık alt matrislerden dolayı rank dağılımında sapma olması
Ayrık Fourier Dönüşümü Testi	Bit dizisindeki periyodikliğin birbirlerinden önemli ölçüde farklı olması
Çakışmayan Şablon Eşleme Testi	Periyodik olmayan bir şablonun çok fazla görülmesi
Çakışan Şablon Eşleme Testi	M bitlik bloklara ayrılan dizide 1 koşumlarının çok fazla görülmesi
Maurer'in Evrensel İstatistiksel Testi	Çok fazla sıkıştırılabilirlik
Doğrusal Karmaşıklık Testi	LFSR uzunluğunun çok kısa olması
Seri Test	m bit eklenerek elde edilen dizilerin tekdüze olmayan dağılımı
Yaklaşık Entropi Testi	m ve $m+1$ bit eklenerek elde edilen dizilerin tekdüze olmayan dağılımı
Birikerek Artan Toplamlar Testi	Bitlerin artırılmasıyla oluşturulan rastgele bit dizilerinin toplamının 0'dan çok büyük çıkması
Rastgele Gezinimler Testi	Bitlerin artırılmasıyla oluşturulan rastgele bit dizilerinin toplamı dağılımlarının belirli bir durumdan sapması
Değişimli Rastgele Gezinimler Testi	Bitlerin artırılmasıyla oluşturulan rastgele bit dizilerinin toplamı dağılımlarının çeşitli durumların beklenen oluşum sayısından sapması

Tablo 3.6. NIST kapsamında yapılan testlerin başlangıç koşulları [66]

<table>
<tr><td>Frekans Testi</td><td>$n > 10$</td></tr>
<tr><td>Bir Blok İçerisinde Frekans Testi</td><td>$n \geq MN, n > 100, M > 20, N < 100$</td></tr>
<tr><td>Koşum Testi</td><td>$n \geq 100$</td></tr>
<tr><td>Bir Blok İçerisindeki En Uzun Bir Tekrarı Testi</td><td><table><tr><td>Minimum n</td><td>M</td></tr><tr><td>128</td><td>8</td></tr><tr><td>6272</td><td>128</td></tr><tr><td>750.000</td><td>10^4</td></tr></table></td></tr>
<tr><td>İkili Matris Rankı Testi</td><td>$n \geq 38MQ, M \geq 32, Q \geq 32$</td></tr>
<tr><td>Ayrık Fourier Dönüşümü Testi</td><td>$n \geq 1000$</td></tr>
<tr><td>Çakışmayan Şablon Eşleme Testi</td><td>$m = 2 - 10, n \geq MN, N \leq 100, M > 0{,}01n$</td></tr>
<tr><td>Çakışan Şablon Eşleme Testi</td><td>$m = 2 - 10, n \geq MN, N \leq 100, M > 0{,}01n$</td></tr>
<tr><td>Maurer’in Evrensel İstatistiksel Testi</td><td><table><tr><td>n</td><td>L(blok uzunluğu)</td><td>Q (blok sayısı)= $10\ x\ 2^L$</td></tr><tr><td>≥387.840</td><td>6</td><td>640</td></tr><tr><td>≥904.960</td><td>7</td><td>1280</td></tr><tr><td>≥2.068.480</td><td>8</td><td>2560</td></tr><tr><td>≥4.654.080</td><td>9</td><td>5120</td></tr><tr><td>≥10.342.400</td><td>10</td><td>10240</td></tr><tr><td>≥22.753.280</td><td>11</td><td>20480</td></tr><tr><td>≥49.643.520</td><td>12</td><td>40960</td></tr><tr><td>≥107.560.960</td><td>13</td><td>81920</td></tr><tr><td>≥231.669.760</td><td>14</td><td>163840</td></tr><tr><td>≥496.435.200</td><td>15</td><td>327680</td></tr><tr><td>≥1.059.061.760</td><td>16</td><td>655360</td></tr></table></td></tr>
<tr><td>Doğrusal Karmaşıklık Testi</td><td>$n \geq 10^6, 500 \leq m \leq 5000, N \geq 200$</td></tr>
<tr><td>Seri Test</td><td>$m < \lfloor log2n \rfloor - 2$</td></tr>
<tr><td>Yaklaşık Entropi Testi</td><td>$m < \lfloor log2n \rfloor - 5$</td></tr>
<tr><td>Birikerek Artan Toplamlar Testi</td><td>$n \geq 100$</td></tr>
<tr><td>Rastgele Gezinimler Testi</td><td>$n \geq 10^6$</td></tr>
<tr><td>Değişimli Rastgele Gezinimler Testi</td><td>$n \geq 10^6$</td></tr>
</table>

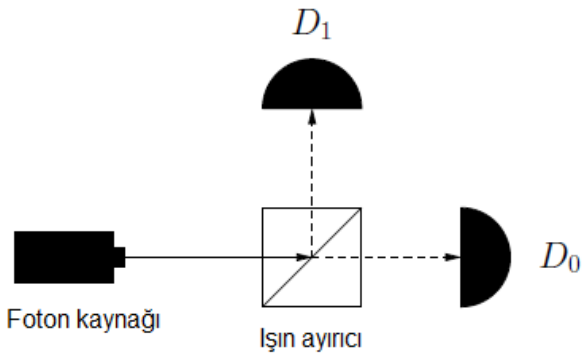
3.4.3. Optik KRSÜ

Lazer, diyot veya tek foton kaynakları gibi kaynaklar kullanılarak dedektörler yardımıyla çok hızlı rastgele sayılar üretilebilmektedir. Günümüzde kullanılan Optik KRSÜ'ler, radyoaktif ışımaların kullanıldığı üreteçlerle benzer mantıkla çalışmaktadır; ancak radyoaktif kaynak ve GM sayaçlarının yerini Optik KRSÜ'de foton kaynakları ve dedektörler almıştır.

Yaygın olarak kullanılan optik KRSÜ'lere dair bilgilendirmeler sonraki alt bölümde yer almaktadır.

3.4.3.1. Optik Yol Üreteçleri

Bu üreteçlerin çalışma prensibi kabaca Şekil 3.2 'de gösterilmiştir [50, 124]. Foton kaynağından gelen fotonlar, ışın ayırıcıdan geçirilir ve hangi detektör tarafından tespit edilirse, ilgili detektörün görevi gereği 1 (D1 veya D2) ve 0 (D2 veya D1) bitlerinden biri, üretilen sayının sonuna eklenerek bitlerden oluşan rastgele sayı dizisi elde edilmiş olur. İlgili düzenekte kullanılan ayırıcının, hiçbir şekilde yanlılık göstermediği ve eşit iletkenlik ve yansıtıcılığının olduğu varsayılmaktadır.



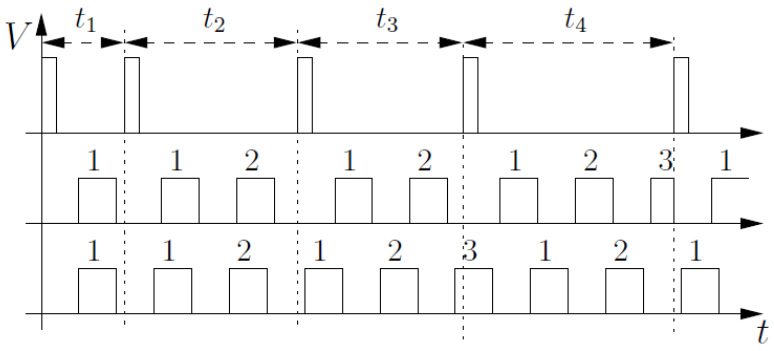
Şekil 3.2. Optik yol üreteci çalışma şeması [50]

Optik Yol Üreteçlerinde de bazı kısıtlamalar karşımıza çıkmaktadır. Fotodetektörlerin her bir tespitten sonra, GM sayaçlarına benzer şekilde, "ölü zaman" adı verilen süreçleri vardır. Ölü zamanlara denk gelen fotonların sayılamaması, bit üretme hızının azalmasına ve Mb/s seviyesinde kalmasına

neden olabilmektedir. Bununla birlikte, çoklu atım durumlarında birbiriyle ilişkili, birden fazla eşzamanlı tespitler üretilebilmekte olup ölü zamana denk gelen tespitler için düzenek, sanki foton gönderilmiş gibi davranarak bit oluşturulmasına sebebiyet verebilmektedir. Bu sorunlarla baş edebilmek adına geliştirilen çözümlere tüp voltajının ve fotodetektörlerin algılama eşiğinin ayarlanabileceği bir aşamanın yer aldığı bir çalışma örnek olarak verilebilir [125]. Ölü zamana yakalanmamak adına daha yavaş foton gönderen kaynakların kullanılması da alternatif bir yol olarak tercih edilebilmektedir. Hâlihazırda var olan türleri diğer kuantum tabanlı üreteçlere göre hızlı olmasına rağmen çok daha hızlı bit üretilmesi adına standart olarak kullanılan 2 adet çıkışlı üreteçler yerine 2'den fazla çıkışın yer aldığı üreteçler de literatürde mevcuttur [126].

3.4.3.2. Varış Zamanına Dayalı Üreteçler

Bu tarz üreteçlerde, zayıf bir foton kaynağı, bir detektör ve zamanlama devresi kullanılmaktadır. Bu şekilde her bir tespitin zamanı ve belirli bir zamanda gelen foton sayısı kaydedilir. Şekil 3.3'te [50] örnek bir rastgele sayı üreteci gösterilmiştir. En üstte yer alan grafik, tespit edilen fotonları göstermektedir ve tespit edilen fotonlarla zamanlayıcı çalışmaya başlar. Kullanılan zamanlayıcı, atımlardan bağımsız (Şekil 3.3, alttaki grafik) olabileceği gibi her bir atımdan sonra sıfırlanması da tercih edilebilmektedir (Şekil 3.3, ortadaki grafik). Kullanılan örnekte, $t_2 > t_1$ ve $t_4 > t_3$ olduğu için çıkışın 11 olması beklenir. Tespit edilen her fotondan sonra sıfırlanabilen zaman sayaçları için $n_1 = 1$, $n_2 = 2$, $n_3 = 2$, $n_4 = 3$ değerlerine göre $n_2 > n_1$ ve $n_4 > n_3$ olduğundan yine çıkış 11 elde edilir. Sabit zamanlayıcılı sayaçlar için ise $n_1 = 1$, $n_2 = 2$, $n_3 = 3$ ve $n_4 = 2$ elde ederiz; $n_2 > n_1$ ve $n_4 < n_3$ olduğundan çıkış 10 elde edilir. Sıfırlanabilir bir zamanlayıcın kullanılması, kesin olmayan zaman ölçümlerinden gelen yanlılığı ortadan kaldırdığından daha tercih edilebilir olmaktadır. Farklı bir uygulama olarak, foton gelme süresi içerisinde sayılan atımların tek veya çift olmasına göre 0 veya 1 değeri verilen üreteçler de kullanılabilmektedir [127]. Son olarak, varış zamanına dayalı üreteçlerde de rastgeleliğinin güçlendirilmesi için çeşitli algoritmalardan ve donanımlardan faydalanılmaktadır [76, 128].



Şekil 3.3. Varış Zamanına Dayalı Üreteçler için örnek bir rastgele sayı üretimi

3.4.3.3. Foton Sayıcı Üreteçler

Bu tip üreteçlerde, belirli bir zaman içerisinde tespit edilen elektronların sayıları dikkate alınarak rastgele sayılar üretilmektedir. Dijital sayıların oluşturulması, iki farklı ölçümden sonra elde edilen foton sayılarına göre yapılmaktadır. Örneğin, ilk ölçülen foton sayısının, ikinci ölçülenden büyük olduğu durum için 1, aksi durum için ise 0 verilmesi gibi uygulamaları vardır [129]. Foton sayısını ölçen üreteçlerde, yukarıda bahsedilen diğer optik tabanlı üreteçlerde görülen ve hızlı bit üretimini engelleyen ölü zamanlı detektörler kullanılmamaktadır, bunun yerine fotoçoklayıcılar tercih edilmektedir [130]. Elde edilen fotonlardan birden fazla bitin üretilmesine dayalı çalışmalar olduğu gibi günlük hayatta kullanabilecek kolaylıkta rastgele sayı üreteçleri de ortaya konulmuştur [131 – 134]. Özellikle, cep telefon kameraları kullanılarak yeterli hassasiyete sahip kuantum etkili rastgele sayıların üretilebildiğini gösteren uygulama, Kuantum Rastgele Sayı Üreteçlerinin hantal uygulamalarının dışında daha kolay uygulamalarının da olabileceği konusunda bir bakış açısı getirmiştir ve bu tez kapsamında yapılan araştırmalar için çıkış noktası olmuştur [134]. İlgili çalışma ile elektron sayıları üzerinden farklı kameralar denenmekte ve daha iyi rastgelelik sonuçlarının alınabilmesi için en uygun kamera bulunmaya çalışılmaktadır. Bununla birlikte, bu tez çalışması ise, kamera yardımıyla alınan görüntülerin RGB değerlerinin bir rastgelelik taşıyıp taşımadığına yöneliktir.

Yapılan tez çalışması, kuantum rastgele sayı üreteçlerinin daha az karmaşık düzeneklerle de elde edilebildiğini göstermekte olup hızla ilgili bir iddiada

bulunmamaktadır. Bununla birlikte, kullanılan kuantum yöntemlerine göre üreteç hızlarının ulaşabildikleri seviyelere dair bir karşılaştırma 2016 yılında yapılmıştır [50].

4. KUANTUM RASTGELE SAYI ÜRETECİ TASARIMI VE UYGULAMASI

Bilgi güvenliği kapsamında, çok önemli bir yere sahip olan rastgele sayı üreteçleri, Kuantum teknolojisinin de gelişmesiyle farklı bir boyuta taşınmıştır. Bölüm 1, 2 ve 3 içerisinde, rastgele sayı üreteçleri konusunda var olan eksikliklere ve yaşanan gelişmelere değinilmiş olup ilgili literatür incelemesinden sonra, kuantum prensiplerine dayanan, kullanıcıların günlük hayatta da maliyet ve kurulum açısından kolaylıkla oluşturabileceği, düşük maliyetli, tahmin edilemez veya edilmesi çok zor bir seviyede olan, özgün bir rastgele sayı üretecinin tasarlanmasına karar verilmiştir.

Tez kapsamında kullanılan ışık kaynağından gelen foton sayısı Poisson istatistiğinde olup, kameraya ulaşan foton sayısı, ortalama değerin ($\bar{n}$) karekökü ($\sqrt{\bar{n}}$) ile orantılı olarak değişir ki buna shot gürültüsü denir. Bu gürültünün ise kaynağı kuantum vakum dalgalanmaları olup bu olay klasik fizik ile açıklanamaz [135]. Dolayısıyla bu çalışmadaki RSÜ'nün entropi kaynağı bir kuantum olayıdır. Kamera pikselleri de bu dalgalanmayi ölçebilecek çözünürlüğe sahip olduğundan çalışmamız KRSÜ'dür.

Sonraki bölümlerde, tez kapsamında yapılan çalışmalar sırasıyla verilmektedir.

4.1. Fiziksel Model Oluşturma

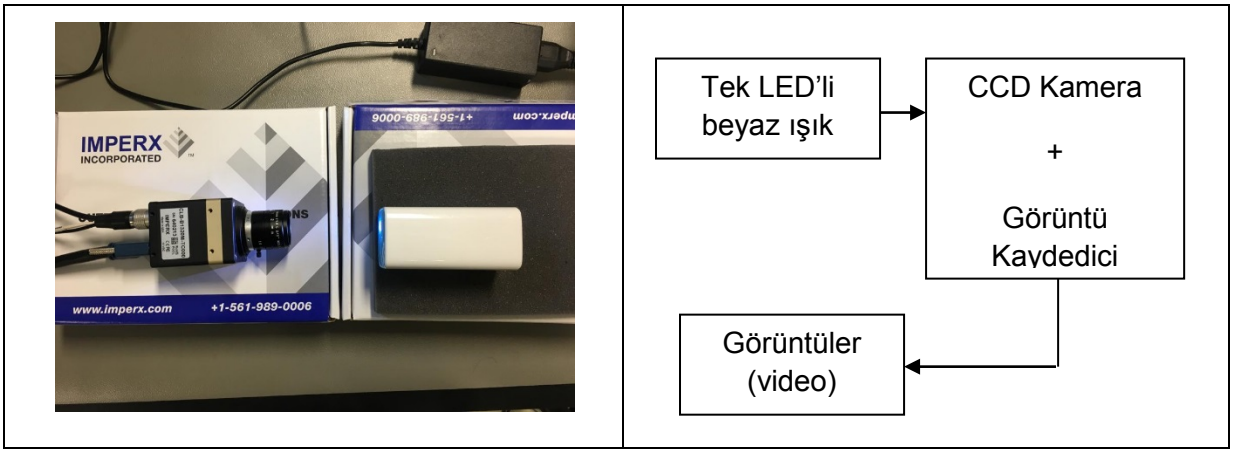
Rastgele sayıların üretilmesi için çalışma kapsamında kullanılan işlemler Şekil 4.1'de gösterilmiştir. Öncelikle, ham verinin elde edilmesi için ihtiyaç duyulan düzeneğin kurulması için çalışılmalar yapılmıştır. Daha sonrasında, düzenek ile elde edilen ham veriden çıkarım yapma işlemi yardımıyla kuvvetli rastgele sayı dizisi elde edilmiştir.

Şekil 0.1. Rastgele sayıların üretilmesi için uygulanan adımlar

4.2. Düzeneğin Kurulması ve Ölçümlerin Yapılması

Çok büyük altyapılar gerektirmeden, sadece bir kamera yardımıyla, bir led kaynağından alınan görüntülerle, tahmin edilmesi güç rastgele sayıların elde edilip edilemeyeceği sorusu motivasyon kaynağı olarak kullanılmıştır. Kuantum etkisinin dâhil olduğu bir rastgele sayı üreteci tasarlanmak istendiği için, kaynak olarak, tek ledli beyaz bir ışık kaynağı seçilmiştir.

Basit uygulamalar ile rastgeleliğin sağlanabilmesine yönelik olarak tek foton kaynaklarının, lazerlere göre daha fazla rastgelelik sağlanıyor olmasından dolayı bu çalışmada tercih sebebi olmuştur [136]. Gürültüyü en aza indirmek adına ortamın tamamen karanlık olmasına özellikle dikkat edilmiştir. CCD kameranın avantajları dikkate alınarak Imperx markasına ait B1320 Monochrome CCD Camera modeli fotoğraf makinesi kullanılmıştır [137]. Karanlık bir ortamdan alınan ışık görüntülerinin RGB değerlerine bakılarak güçlü bir rastgele sayı üreteci elde edilmek istenmiştir. Bu amaç doğrultusunda, kurulan düzenek ve düzenek şeması Şekil 4.2'de gösterilmiştir.

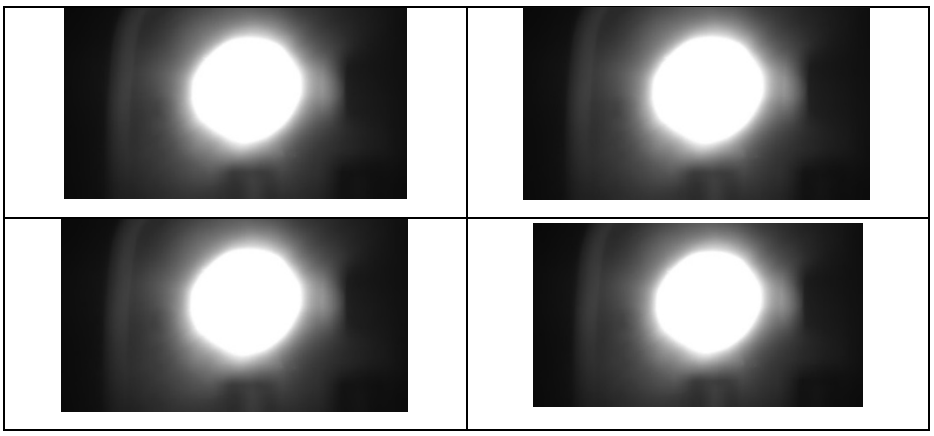


Şekil 0.2. Görüntülerin alınması için kullanılan düzenek

4.3. Ham Verilerin Elde Edilmesi ve Kuantum Etkisinin Tayini

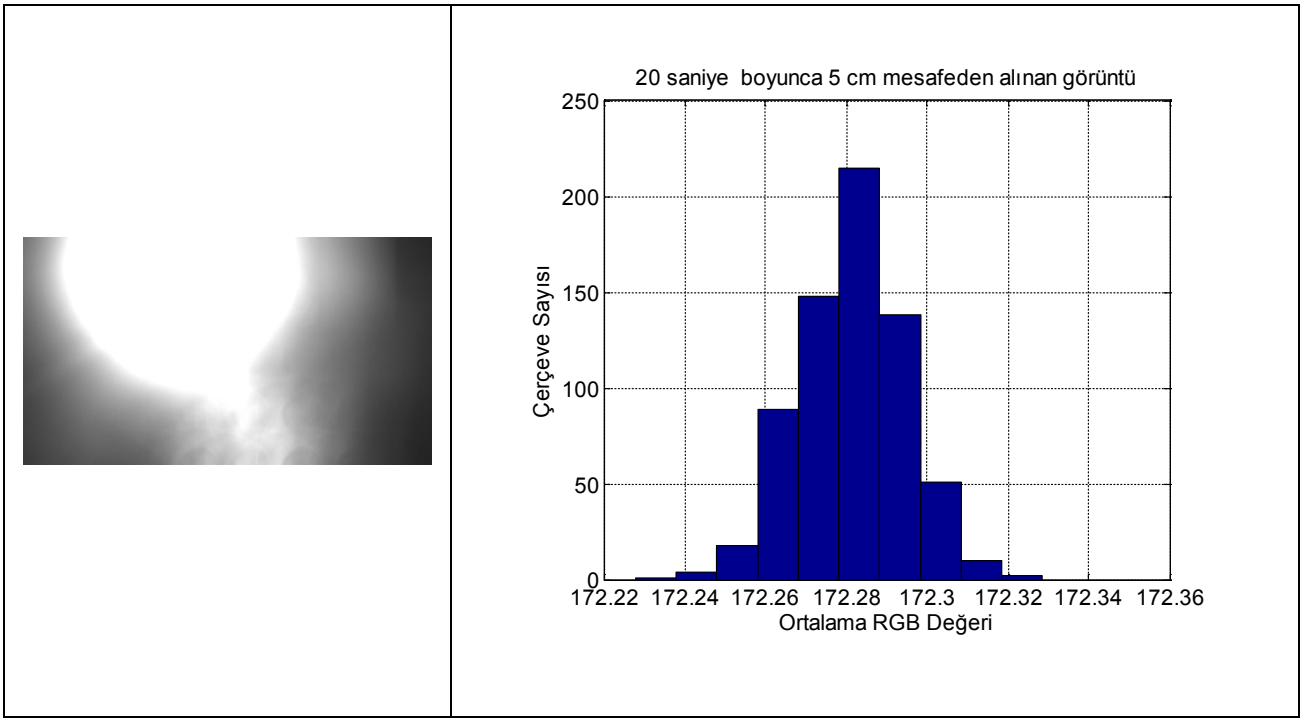
Kurulan düzenekle elde edilen görüntülerden birkaç tanesi Şekil 4.3'te verilmiştir. Verilen görüntüler, birbirlerine oldukça benzer görünmeleri sebebiyle RGB değerlerinin, dolayısıyla RGB değerleri ortalamalarının, rastgele sayı üretiminde kullanılabilecek kadar değişkenlik gösterip görmeyeceği sorusu ilk ele alınan durum olmuştur. Bu nedenle, alınan görüntülerin RGB değerlerinin ortalamasına bakılmış ve ne kadar benzer görünseler de çıplak gözle algılanamayacak kadar küçük farklılıklar içerdikleri anlaşılmıştır. İlgili şekiller, üzerinde işlem yapılmasına karar verilen görüntü olan 10 cm mesafeden alınan görüntülerdir.

Görüntülerin RGB değerlerinin farklılık gösteriyor olması, tek başına tez kapsamında kullanılabilir olduğunu garanti etmemektedir. Alınan görüntülerle işlem yapılabilmesi için bu RGB değerlerinin, Kuantum etkisi gösterip göstermediğinin tespit edilmesi gerekmektedir. Kuantum etkisi göstermeyen bir veri seti üzerinden rastgele sayıların üretilmesi, cevap aranan sorunun dışında kalınmasına sebebiyet verdiğinden, kuantum etkisinin gözlemlenebileceğine veya gözlemlenemeyeceğine dair ölçümler gerçekleştirilmiştir. Daha önce değinildiği gibi, belirli bir süre boyunca alınan görüntüler için kaynak tarafından üretilen foton sayısının öngörülemez (belirsiz) olmasından kaynaklı bir kuantum etkisinin, dolayısıyla Gauss dağılımının gözlenmesi beklenmekle birlikte en iyi Gauss dağılımının ne şekilde elde edilebildiğine dair incelemeler de yapılmıştır.

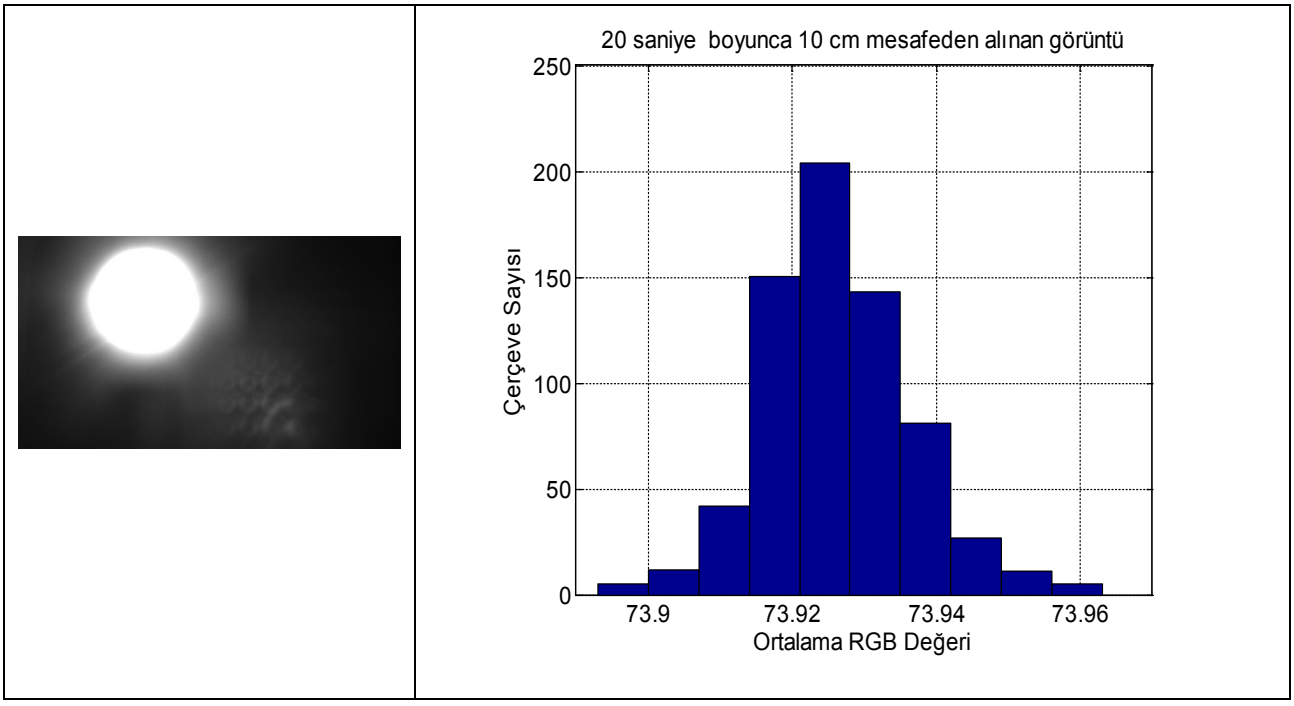


Şekil 0.3. 10 cm mesafeden alınan görüntünün farklı çerçeve örnekleri

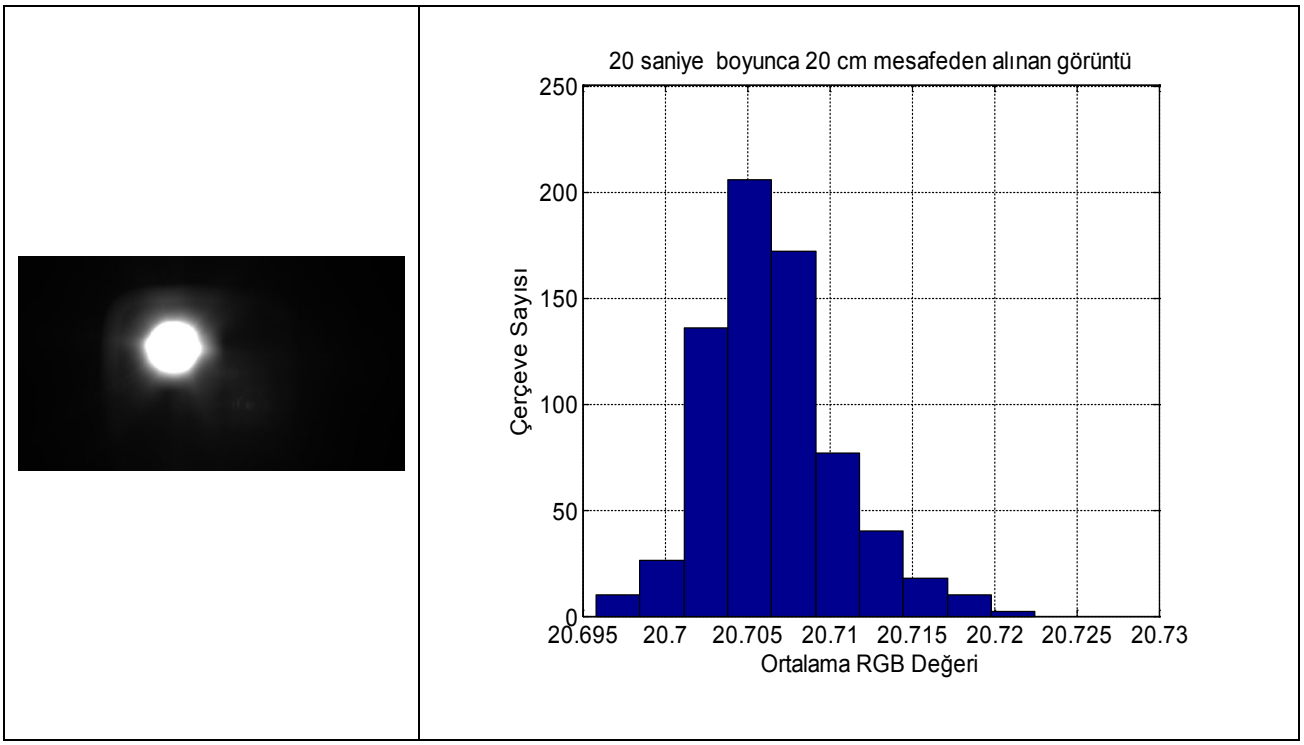
Bu kapsamda; 100 cm, 50 cm, 35 cm, 20 cm ve 10 cm gibi çeşitli kaynak – kamera uzaklıklarında çekilen görüntülerin RGB değerlerinin ortalaması alınmış ve daha sonrasında çubuk grafiklerine bakılmıştır. İlgili görüntüler ve grafikler Şekil 4.4 ile Şekil 4.9 aralığında gösterilmiştir. Görüntülerin RGB değerlerinin ortalaması alınırken değerler gri renk skalasına çevrilmektedir. Alınan histogram grafikleri ile kaynak kameraya yaklaştıkça Gauss dağılımının daha belirgin hale geldiği gözlenmiştir. Kaynak kameradan uzaklaştıkça yansıma, dolayısıyla gürültü gibi etmenler de eklenebildiğinden yakın çekimlerle alınan görüntüler üzerinden işlemlere devam edilmesine kadar verilmiştir.



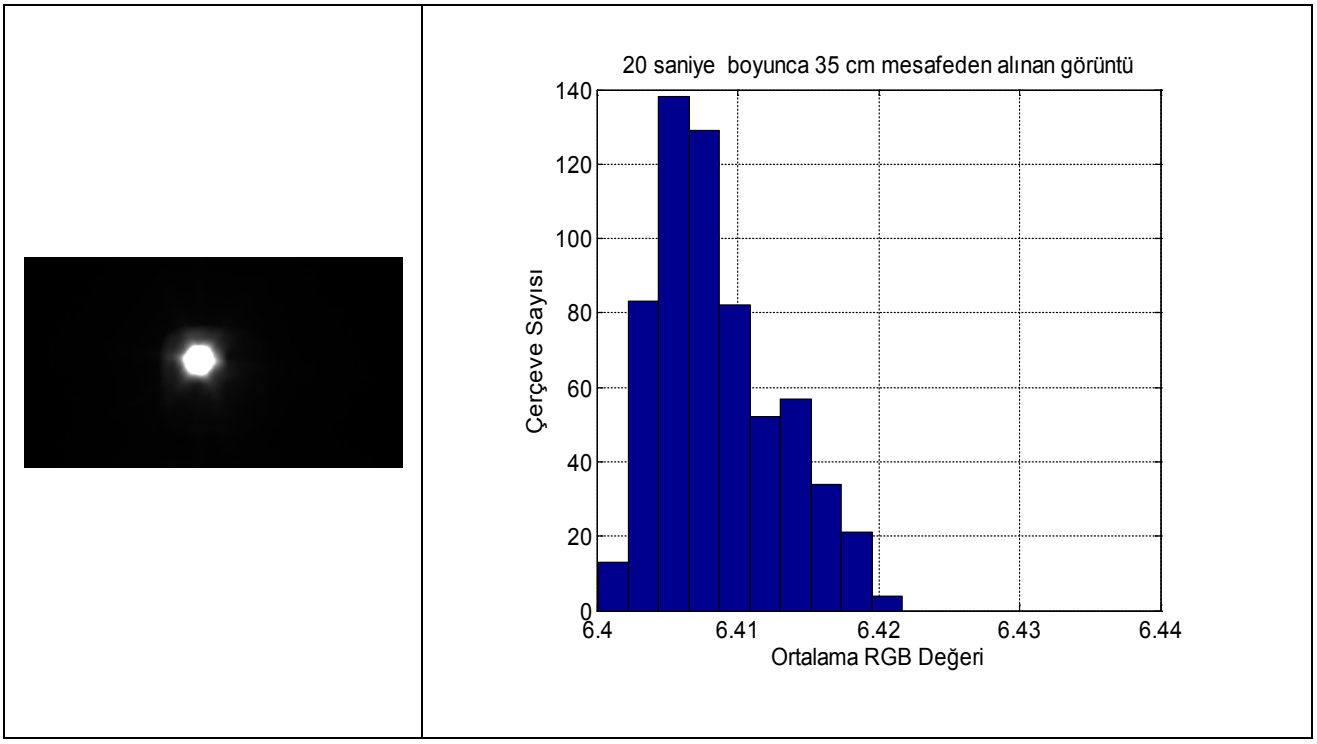
Şekil 0.4. 5 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı



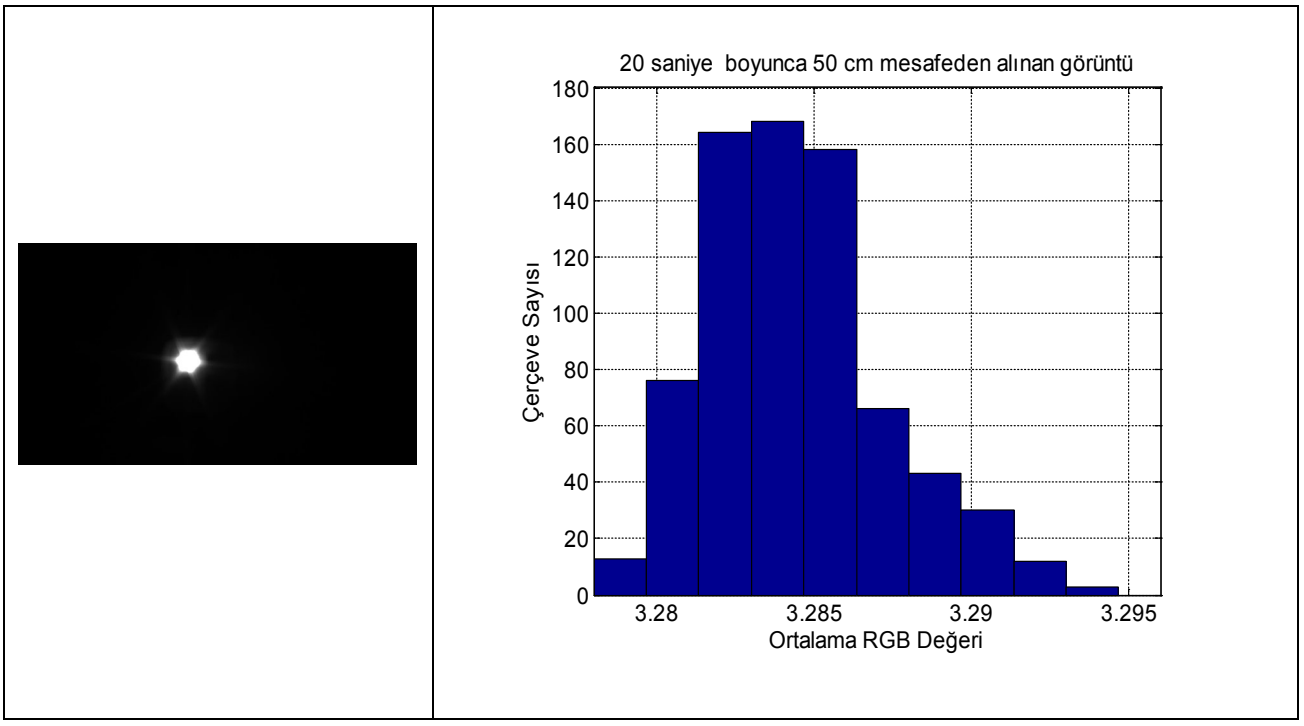
Şekil 0.5. 10 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı



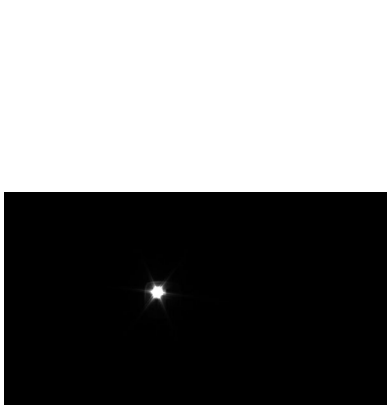
Şekil 0.6. 20 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı

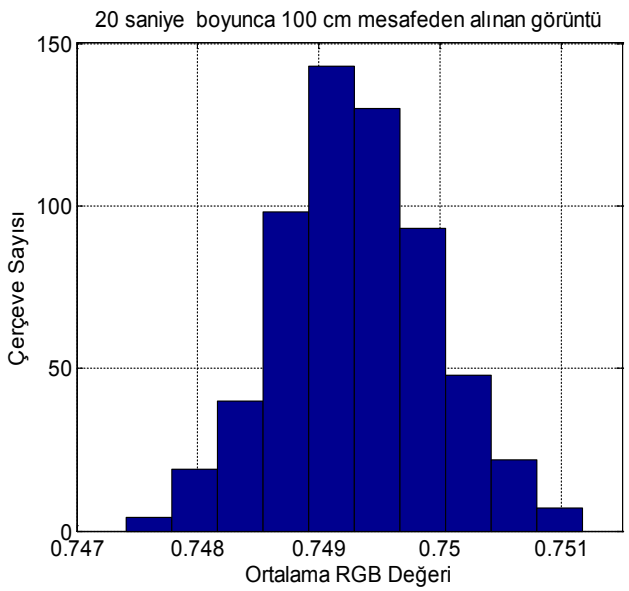


Şekil 0.7. 35 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı



Şekil 0.8. 50 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı

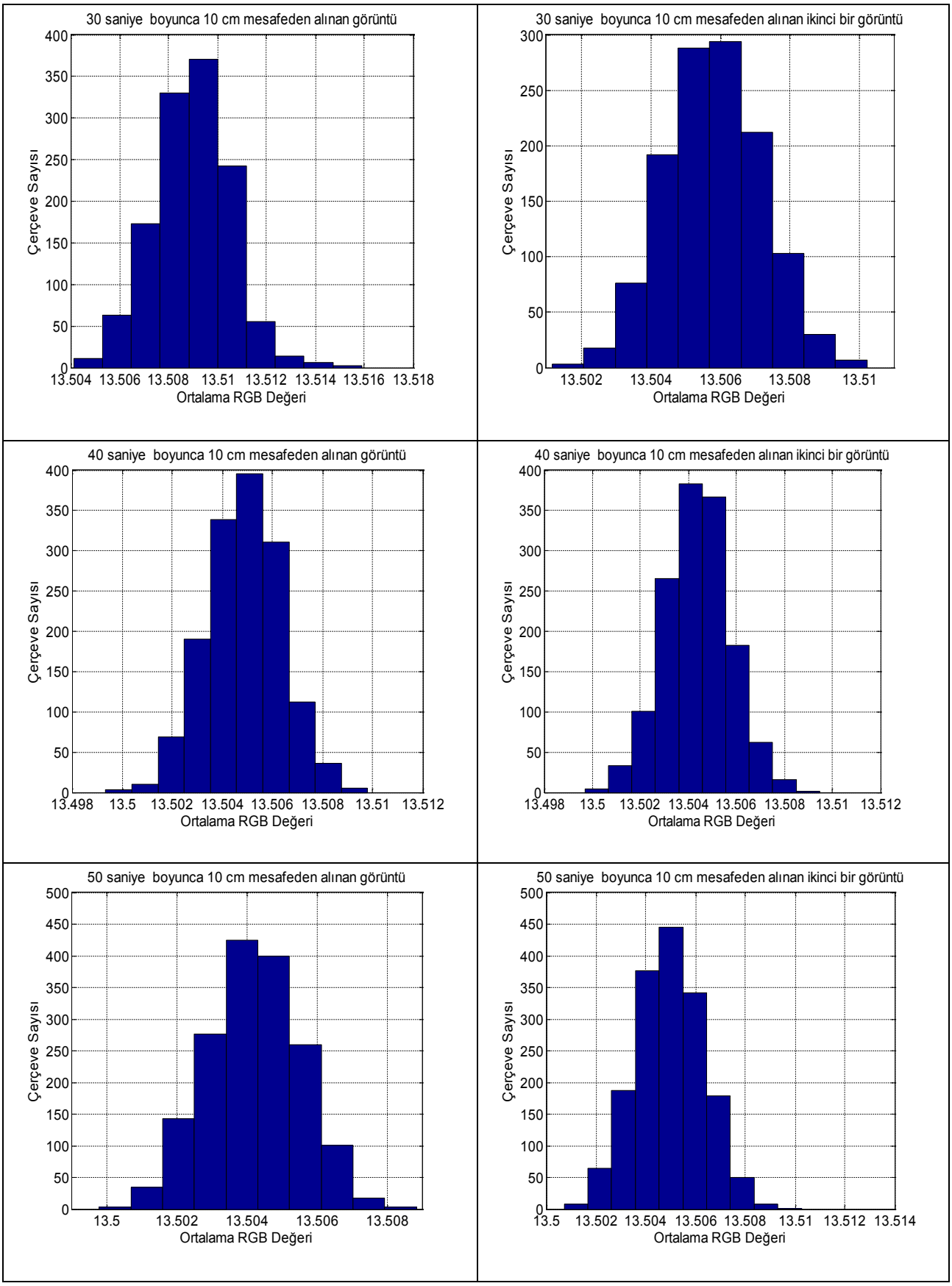




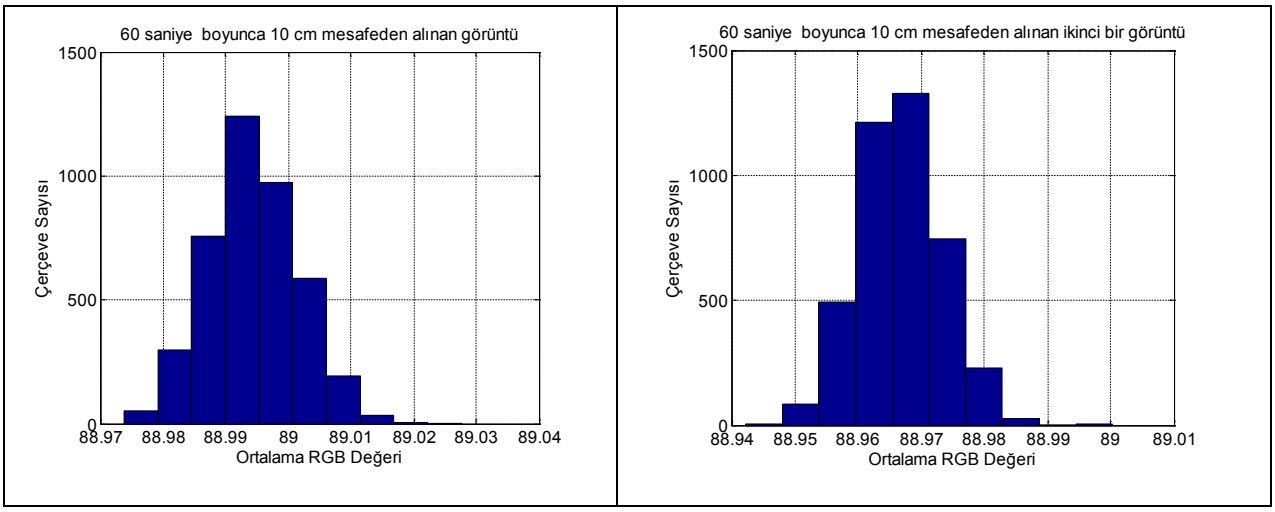
Şekil 0.9. 100 cm mesafeden 20 sn boyunca alınan görüntünün ilk çerçevesi ve histogram diyagramı

Şekil 4.5 ile Gauss dağılımının diğer mesafelere göre en net görültüğü histogram eğrisinin 5 cm mesafede alınan görüntülerden elde edildiğinin çıkarımını yapabiliyoruz. Bu durumda rastgele sayı üretilmesi için en uygun mesafenin 5 cm uzaklıktan alınan görüntülerle elde edilebileceği düşünülebilir. Ancak, yine Şekil 4.5'te görüldüğü üzere, bu mesafede görüntü dışında kalan ışık verileri olabilmektedir. Bu nedenle, diğer histogram eğrilerinden alınan sonuçlar da dikkate alındığında, rastgele sayıların üretilmesi için 10 cm mesafeden elde edilen görüntülerin kullanılmasına karar verilmiştir.

Bununla birlikte, alınan görüntü süresinin Gauss dağılımını nasıl etkilediğinin anlaşılmasına yönelik ayrıca bir inceleme yapılmıştır. Şekil 4.10'da, 10 cm mesafeden farklı sürelerde alınan görüntülerin RGB değerleri ortalamasının gösterildiği çubuk grafikler yer almaktadır. Alınan örnek süreleri arttıkça Gauss dağılımı daralmaktadır, bu da örnek alınma süresinin arttığı durumlar için kuantum etkisinin daha net gözlenmesi anlamına gelmektedir. Şekil 4.11'de gösterilen sonuçlar dikkate alınarak 1 dakika süresince alınan görüntüler ile işlemler devam ettirilmiştir.



Şekil 0.10a. 10 cm mesafeden farklı sürelerde alınan görüntülerin histogram grafikleri



Şekil 0.11b. 10 cm mesafeden farklı sürelerde alınan görüntülerin histogram grafikleri

Bu aşamada ham veriler elde edilebildiği için çalışmanın bir sonraki aşaması olan çıkarım işlemine geçilmiştir.

4.4. Çıkarım İşlemi

Kurulan düzenekle Kuantum etkisi gözlemlenebildiği sonucu elde edildikten sonra rastgele sayı üretme işlemlerine başlanmıştır. Görüntülerden elde edilen ham verinin gerçek rastgele sayı olarak kullanılabilmesi için uyguladığımız çıkarım işleminin amacı, ham veriler içerisinde yer alan gürültüleri (çevresel faktörler, elektonik etkiler vb.) ortadan kaldırarak kuantum, bir anlamda gerçek, rastgele sayıların elde edilmesidir. Gürültüye sebebiyet veren koşulların bilinmesi üretilen rastgele sayıların kimliğine müdahale şansı doğurmaktadır ve rastgele sayıların tahmin edilebilirliğini artırmaktadır.

Çıkarım işlemi için Toeplitz özütleme yöntemi kullanılmıştır [108]. Toeplitz özütleme çıkarımcısının uygulanması aşamasında başvurulan adımlar aşağıdaki gibidir:

1) Çıkarımcı çıkışının m bitlik boyutunun bulunması:

n bitlik ham verinin k bitlik minimum entropisi ile ε gizlilik parametresinden yararlanılarak m bitlik çıkarımcı çıkışı eşitlik 4.1'de gösterilen formül ile bulunmaktadır.

$$m = k - 2\,log\varepsilon \tag{4.1}$$

10 cm uzaklıktan CCD kamera ile çekilen 1 dakikalık görüntü (8 bitlik çerçeveler)'den elde edilen 4144 çerçeve için minimum entropi, eşitlik 3.5'te verilen formülle bulunmuştur. 4144 çerçeve için RGB değerlerinin ortalaması ile alınan en yüksek olasılık değeri 0,008 bulunmuştur. Bu nedenle, ilgili eşitlik ile minimum entropi 6,9724 (k) bit olarak elde edilmiştir. Bu durumda, 8 bitlik görüntü verileri, 6,9724 bitlik sıkıştırılmış veri şeklinde ifade edilebilmektedir sonucuna ulaşılmıştır.

Bir sonraki aşama olan gizlilik parametresinin belirlenmesi eşitlik 4.2 ile gösterilen formülden faydalanılarak mümkün olmuştur. Bunun için aynı koşullarda alınan iki örnek üzerinden hesaplamalar yapılmıştır. Bir dakika boyunca alınan görüntülerden ilki, yukarıda da belirtildiği gibi 4144; diğer örnek kümesi ise 4133 çerçeveden oluşmaktadır. Bu iki örnek kullanılarak, parametre değeri 0,065101 olarak elde edilmiştir.

$$\|\mathrm{X} - \mathrm{Y}\| \equiv \frac{1}{2}\sum \; \mid \mathrm{Prob}[\mathrm{X} = \mathrm{v}] - \mathrm{Prob}\,[\mathrm{Y} = \mathrm{v}] \; \mid \; \leq \; \varepsilon \tag{4.2}$$

Eşitlik 3.5 ve eşitlik 4.2 yardımıyla bulunan minimum entropi ve parametre değerleri, eşitlik 4.1 ile çıkarım işlemi sonunda ne kadarlık bir bit değerinde rastgele sayı dizisi elde edileceğinin bulunması aşamasında kullanılmıştır. Yapılan hesaplamalar sonunda girişte kullanılan 4100 bitlik veri için minimum entropinin korunması adına çıkışta 3565 bitlik bir sayı dizisi elde edilecektir.

Çıkarım işlemi sonunda elde edilecek bit sayısının bulunmasından önce, ortalama RGB değerleri virgülden kurtarılarak tam sayı haline getirilmiştir. Ortalama değerlerinin tam sayı haline getirilmesi aşamasında virgülden sonraki dördüncü basamaktan sonrası ihmal edilmiştir. Tam sayı haline getirilen RGB değerleri, sonrasında 1 ve 0'lardan oluşan ikili bit haline getirilmiştir.

2) $n + m - n$ bit uzunluğunda rastgele bir Toeplitz matrisi oluşturmak:

Çıkarım aşamasında kullanacağımız Toeplitz matrisi uzunluğu; girişte kullanılan 4100 bit değeri ile birinci adımda bulunan çıkış bit değeri olan 3565 bit uzunluğunda olması gerektiği için matris, 4100x3565 boyutunda olacaktır. 4100x3565 boyutunda Toeplitz matrisi için Matlab programının rastgele sayı üretmek için kullandığı algoritmadan faydalanılmış olup "randi" komutu ile sözde rastgele sayı dizisi oluşturulmuştur.

3) Ham veri ile Toeplitz matrisi çarpılarak çıkarım yapılmış rastgele sayı dizisi elde etmek:

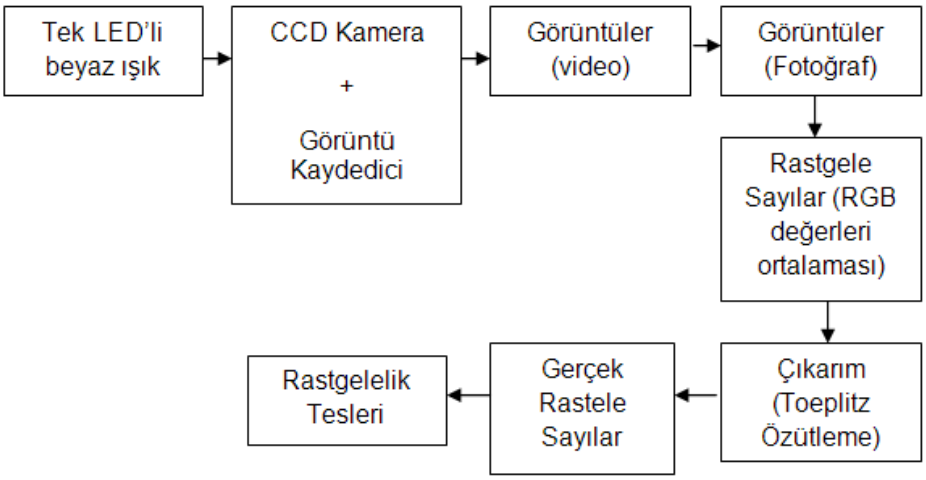
Çıkarım işlemi ile 3565 bitlik rastgele sayı dizisi elde edilebilmesi adına, 4100 bitlik giriş matrisi ile 4100x3565 boyutunda Toeplitz matrisi çarpılmıştır. Yapılan çarpma işlemiyle, 3565 elemanlı dizi, 1 ve 0'lardan farklı değerden oluşmuştur. Tez kapsamında, 3565 bitlik 1 ve 0'lardan oluşan bir sayı dizisi elde edilmek istendiğinden çarpma işleminden sonra sayılar mantıksal değerlere, 1 ve 0'a, dönüştürülmüştür.

Bu aşamada, çıkarım işlemiyle, rastgele sayı dizileri elde edilmiştir. Bu sayıların gerçekten rastgele olup olmadığının tayini işlemi ve sonuçları sonraki bölümde verilmiştir.

4.5. Rastgelelik Testleri ve Deneysel Sonuçlar

Şekil 4.12'de gösterilen adımlar uygulanarak elde edilen ham verilerden çıkarım işlemi sonunda rastgele sayı bitleri çıkarımı yapılmış olup NIST tarafından

sunulan algoritmalar ile rastgelelik testlerine tabi tutulmuştur [66]. Bu testlere dair kodlar NIST tarafından sunulmakla birlikte [144]; tez kapsamında kullanılan kodlar, algoritmalardan faydalanılarak MATLAB programında ayrıca oluşturulmuştur.



Şekil 0.12. Rastgele sayıların elde edilmesi için uygulanan adımlar

Çıkarım işleminden sonra elde ettiğimiz 3565 bitlik sayı dizisi, Bölüm 3.3'te detayları verilen 15 adet istatistiksel testin tamamından geçmiştir. Bu testler sonucunda elde edilen P değerlerine ait sonuçlar Tablo 4.1'de gösterilmiştir.

Rastgeleliğin kuvvetlendirilmesi adına her adımda veya uygulama sırasında değişmesi gereken Toeplitz matrisi ile koşturulan testlerin P değerleri her seferinde farklılık göstermiştir. Koşturulan testlerde P değeri, sınır olarak belirlenen 0,01 değerinin altına hiç düşmemiştir. Bu da, tez kapsamında sunulan KRSÜ'den elde edilen sayı dizilerinin %99 doğruluk payıyla rastgele sayılar üretebildiğini göstermektedir.

Bununla birlikte, Tablo 4.2'de verilen sonuçlara göre, ham verilerden elde edilen rastgele sayı dizisi NIST tarafından sunulan 15 adet testin sadece 8 tanesinden geçebilmektedir. Bu durumda, görüntülerin RGB değerleri ortalamalarının oluşturduğu rastgele sayı dizisinin, ham verilerin sıkıştırılmasıyla rastgeleliğin artırıldığı çıkarım işlemi sonunda elde edilen rastgele sayı dizisine göre daha az rastgelelik gösterdiği görülmektedir.

Tablo 4.1. Elde edilen rastgele sayılar için test sonuçları

Test Adı	**P_değeri**	**Sonuç**
Frekans	0,4923	Geçti
Bir Blok İçerisinde Frekans	0,8468	Geçti
Koşum	0,0613	Geçti
Bir Blok İçerisindeki En Uzun Bir Tekrarı	0,7344	Geçti
Matris Rank	0,0249	Geçti
Ayrık Fourier Dönüşümü	0,6040	Geçti
Çakışmayan Şablon Eşleme	0,8351	Geçti
Çakışan Şablon Eşleme	0,2439	Geçti
Maurer'in Evrensel İstatistiksel	0,1042	Geçti
Doğrusal Karmaşıklık	0,8774	Geçti
Seri	P_değeri1= 0,2761 P_değeri2 = 0,7164	Geçti
Yaklaşık Entropi	0,9221	Geçti
Birikerek Artan Toplamlar	P_değeri_ileri = 0,1410 P_değeri_geri = 0,0475	Geçti
Rastgele Gezinimler	0,9732 0,6488 0,9448 0,8175 0,8175 0,9625 0,9315 0,9794	Geçti
Değişimli Rastgele Gezinimler	0,3994 0,5040 0,3515 0,4875 0,2662 0,9049 0,0698 0,9195 0,0405 0,9290 0,0263 0,8403 0,0121 0,8821 0,0641 0,8091 0,2850 0,9225	Geçti

Tablo 4.2. Ham verilerden elde edilen rastgele sayılar için test sonuçları

Test Adı	**P_değeri**	**Sonuç**
Frekans	0,1421	Geçti
Bir Blok İçerisinde Frekans	1.0062e-309	Kaldı
Koşum	1.9655e-315	Kaldı
Bir Blok İçerisindeki En Uzun Bir Tekrarı	0.6305	Geçti
Matris Rank	0.0011	Geçti
Ayrık Fourier Dönüşümü	9.5068e-23	Kaldı
Çakışmayan Şablon Eşleme	0.8572	Geçti
Çakışan Şablon Eşleme	0.1648	Geçti
Maurer'in Evrensel İstatistiksel	0.0132	Geçti
Doğrusal Karmaşıklık	8.3955e-106	Kaldı
Seri	P_değeri1= 0 P_değeri2 = 2.5097e-305	Kaldı
Yaklaşık Entropi	0	Kaldı
Birikerek Artan Toplamlar	P_değeri_ileri = 8.6931e-16 P_değeri_geri = 3.8195e-22	Kaldı
Rastgele Gezinimler	0,0078 0,7546 0,4077 0,3021 0,0281 0,2435 0,4746 0,4651	Geçti
Değişimli Rastgele Gezinimler	0,6496 0,1601 0,9038 0,4490 0,7356 0,7062 0,6514 0,9718 0,6848 0,9751 0,5473 0,5916 0,3791 0,5677 0,1443 0,6988 0,0752 0,6014	Geçti

5. SONUÇLAR

Tez kapsamında, kuantum etkisi gösteren tek ledli bir ışık kaynağı kullanılarak karanlık bir ortamdan alınan görüntülerin RGB değerlerinden faydalanılmış ve bu sayede rastgele sayı üretimi gerçekleştirilmiştir. Elde edilen rastgele sayıların tahmin edilemezlikleri, çıkarım işlemi ile artırılmıştır ve sonrasında koşturulan NIST testleri ile tahmin edilemezliklerinin kuvveti gösterilmiştir. Test sonuçları göstermektedir ki çıkarım işleminden sonra elde ettiğimiz bit dizisi, güvenli haberleşme kapsamında anahtar olarak kullanılabilir. Klasik kriptografide, anahtarların kullanılabilir olması için tekrar üretilebilir olması gerekirken KRSÜ ile elde edilen rastgele sayıları tekrar üretmek mümkün değildir. O nedenle, KRSÜ'lerin ürettiği rastgele sayılar ile oluşturulan anahtarların dağıtımı, kuantum fiziğinin belirsizlik ve dolaşıklık ilkelerine göre geliştirilen protokollerle gerçekleştirilmektedir [138-141].

Tablo 5 içeriğinde, her bir test için P değerleri verilmiştir. P değerleri 0.01'den ne kadar büyükse rastgelelik o kadar kuvvetlenmekte iken (1'den büyük olamaz) 0,01'e yakın olması da rastgeleliğini bir o kadar zayıflatmaktadır. Bu anlamda, 0.01'e en yakın değer "Matris Rank" testinde alınmıştır. Sınırın üstünde olmasına rağmen düşük bir değere ulaşılması, başlangıç koşullarının sağlanamamış olmasından kaynaklanabilir. İlgili teste dair sağlıklı sonuçların elde edilebilmesi adına 32x32'lik matrislerle işlem yapılması ve başlangıç bit değerinin en az 38.912 bit olması istenmektedir. Önerilen başlangıç koşulları ile Toeplitz matrisi ve başlangıç bitinin çarpılması işlemi, erişim sağlanabilen bilgisayarların hafıza miktarını aşması sebebiyle, istenilen başlangıç koşulları ile yapılamamıştır. Bu durumda, testin başarılı bir şekilde uygulanması için ne kadar daha hafızanın gerekli olduğuna dair net bir bilgi elde edilememiştir; çünkü kullanılan uygulamada sadece hafızanın yetersiz olduğuna dair bir uyarı verilmiştir. Bu nedenle, hafıza sorunu/hatası yaşanılan/alınan Matris Rank testi için elde edilen sonuç, daha kısa bit değerleri ile elde edilmiştir. Hafızası yeterli bilgisayarlarla yapılan işlemler, ilgili test için daha doğru bir sonuç verecektir. Bunun yanı sıra, matris ölçülerinin tavsiye edilen değerlere çıkarılması mümkün olmuş olsaydı yaklaşık 4096 bitlik bir dizi elde etme isteğimizin dışına çıkılmasına neden olacaktı.

Bununla birlikte, görüntü almak için oluşturulan düzenekte, ortamın çok karanlık olmasına ve sadece tek ledli bir kaynağın yaydığı ışığın görüntülenmesine, gürültünün en aza indirilmesi adına, özellikle dikkat edilmiştir. Alınan görüntüler, gri renk aralığına denk geldiği için kırmızı, yeşil veya mavi renklerden herhangi biri üzerinden çalışma yapılması gerekliliği ortadan kaldırılmıştır. Bu anlamda, diğer uygulamalardan farklılık göstermektedir.

Bir diğer konu ise, kaynak seçimidir. Bu çalışmada, herhangi bir görüntüden yola çıkılarak üretilen rastgele sayılarda yaşanılan güvenlik zafiyetleri (görüntüyle oynanabilme, yansıma gibi), bağımsız ışık kaynağının parlaklık seviyelerine göre alınan görüntülerle giderilmektedir. Kaynakla ilgili alınabilecek en güvenli tedbir, müdahalelerin mümkün olmadığı bir kaynak olarak Güneş'in seçilmesi olacaktır; ancak kontrollü bir ortamda Güneş ışınlarından faydalanma konusunda bazı kısıtlamalar yaşanmıştır. Tek başına Güneş'ten gelen ışınların sağlıklı bir şekilde elde edilmesi, yansıma veya gelen ışınların açısının görüntü alınırken değişmesi gibi değişkenler sebebiyle, sahip olduğumuz koşullarla mümkün olamamıştır. Bu nedenle, kuantum etkisinin gözlemlenbildiği tek ledli bir kaynak kullanılarak giriş verilerinin oluşturulmasına karar verilmiştir. Farklı bir çalışma konusu olarak, ham verinin oluşturulması aşamasında sadece Güneş'ten gelen ışınların dikkate alınabileceği bir düzenek kurularak yine alınan görüntünün RGB değerleri ile tahmin edilememezlik düzeyi bulunmaya çalışılabilinir.

Yukarıda bahsedilenlere ek olarak, Toeplitz matrisin oluşturulması aşamasında sözde rastgele sayı üreteci kullanılmıştır. Yapılan çalışma kapsamında hız ve kolaylığı için tercih edilen sözde rastgele sayı üreteci daha güvenilir bir üreteç ile değiştirilebilir; ancak kullandığımız yöntemin Bölüm 4'te belirtilen avantajları ile bu durum bir sorun teşkil etmemektedir. Yine de yavaşlatılacağı dikkate alınarak GRSÜ kaynaklı bir matris ile süreç yenilenebilir.

Çalışma kapsamında dikkat edilmesi gereken bir diğer husus ise örnek görüntülerin alınması esnasında mesafelerin dikkatli ölçülmesidir. Rastgele sayı üretilmesi için en uygun mesafe olarak seçilen yaklaşık 10 cm mesafenin her

seferinde aynı hassasiyetle ölçülemeyebileceği, bu nedenle de elde edilen değerlerin her zaman istenilen şekilde alınamayabileceği çalışma kapsamında görülmüştür. Şekil 4.10 ve Şekil 4.11 için aynı mesafeler üzerinden örnekler alınmaya çalışılmış olmasına rağmen benzer ortalamalar elde edilememiştir. Alınan sonuçların hata payları olabileceği düşünülerek yaklaşık 10 cm mesafeden alındığı göz önünde bulundurulmalıdır. Bu durum, sistemlere birleşik olarak kullanılan düzenekler için sorun olmayacaktır.

Son olarak, tez kapsamında ortaya konulan rastgele sayı üretecinin hızıyla ilgili herhangi bir iddiada bulunulmamakla birlikte, bu tez çalışmasında kullanılan CCD kameranın piksel çözünürlüğü olan 720x1280'den farklı olarak sonraki çalışmalar için çözünürlüğü daha güçlü olan kameralar kullanılarak, 1Mb/s'nin altında görülen bit üretim hızı Gbit seviyelerine getirilebilir.

Sonuç olarak, kuantum etkisinden faydalanılarak maliyeti düşük ve geliştirilmeye açık gerçek bir rastgele sayı üreteci elde edilmiştir. Şekil 4.2'de gösterilen düzeneğin çok daha küçük, minimal versiyonları halihazırda kullanılan sistemlere entegre edilerek güvenilir bir şekilde rastgele sayılar üretilebilir. Bu sayede ortam ve mesafe gibi olumsuzluklar da ortadan kaldırılmış olur. Başka bir uygulama konusu olarak sistemlere birleşik olarak kullanılmasına yönelik çalışmalar yapılabilir.

KAYNAKLAR

[1] R. L. Rivest, Cryptography,. In J. Van Leeuwen. Handbook of Theoretical Computer Science, 1. Elsevier, **1990.**

[2] W. Diffie, M. E. Hellman, Privacy and Authentication: An Introduction to Cryptography, Proceedings of the IEEE, Vol 67, No 3, **1979.**

[3] E.Barker, W. Barker, W. Burr, W. Polk, M. Smid, Recommendation for Key Management – Part 1: General (Revision 3), NIST Special Publication 800-57, **2012.**

[4] U. M. Maurer, A Universal Statistical Test for Random Bit Generators, Journal of Cryptology, **1992.**

[5] T. Kelly, The myth of the skytale, Cryptologia, Vol. 22, Issue 3, pp. 244–260, **1998.**

[6] J. F. Dooley, A Brief History of Cryptology and Crptographic Algorithms, Knox College, **2013.**

[7] S. Singh, The Black Chamber, http://www.simonsingh.net/The_Black _Chamber/hintsandtips.html (Erişim tarihi **27.01.2019**).

[8] I. A. Al-Kadit, Origins Of Cryptology: The Arab Contributions, Cryptologia, Vol. 16, Issue 2, **1992.**

[9] W. F. Friedman, The Index of Coincidence and Its Applications in Cryptology, War Department Office of the Chief Signal Officier Washington, **1992.**

[10] S. Mittal, S. B. Abhinaya, M. Reddy, I. Ali, A Survey of Techniques for Improving Security of GPUs, Journal of Hardware and Systems Security, Vol. 2, Issue 3, pp 266–285, **2018**.

[11] F. W. Kasiski, Die Geheimschriften und die Dechiffrirkunst (Cryptography and the Art of Decryption), Mittler und Sohn, Berlin, **1863.**

[12] D. Wagner, The Boomerang Attack, Fast Software Encryption, pp 156-170, **1999**

[13] A. Kerckhoffs, La cryptographie militaire, J. Sci. Milit., vol. IX, pp 5–38, 161–191, **1883.**

[14] C. E. Shannon, Communication Theory of Secrecy Systems, Bell Labs

Technical Journal, Vol. 28, Issue 4, pp. 656-715, **1949.**

[15] J. Nechvatal, Publıc-Key Cryptography, NIST Special Publication 800-2, **1991.**

[16] D. Coppersmith, The Data Encryption Standard (DES) and Its Strength Against Attacks, IBM J. Res, Develop., Vol. 38 No. 3, **1994.**

[17] Electronic Frontier Foundation, Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. O'Reilly & Associates Inc., 1st edition, **1998.**

[18] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer, A. Rupp, M. Schimmler, Breaking Ciphers with COPACOBANA –A Cost-Optimized Parallel Code Breaker, CHES 2006, LNCS 4249, pp 101–118, **2006.**

[19] ToorCon Information Security Conference, The World's Fastest Des Cracker, https://crack.sh/ (Erişim tarihi **27.01.2019**).

[20] E. Barker, M. Nicky, NIST Special Publication 800-67 Revision 2: Recommendation 53ort he Triple Data Encryption Algorithm (TDEA) Block Cipher, NIST., Retrieved **2017.**

[21] Federal Information Processing Standards Publication, Announcing the Advanced Encryptıon Standard (AES), vol 197, **2001.**

[22] J. Daemen, Vincent Rijmen, AES Proposal: Rijndael, NIST Archieves, **1999.**

[23] Federal Register, Vol. 70, No. 96, Notices, page 28907, **2005.**

[24] H. O. Alanazi, B.B.Zaidan, A.A.Zaidan, H. A.Jalab, M.Shabbir, Y. Al-Nabhani, New Comparative Study Between DES, 3DES and AES within Nine Factors, Journal Of Computıng, Vol 2, Issue 3, **2010.**

[25] R. L. Rivest, J. C. N. Schuldt, Spritz—a spongy RC4-like stream cipher and hash function, at Charles River Crypto Day, **2014.**

[26] N. J. AlFardan, D. J. Bernstein, K. G. Paterson, B. Poettering, J. C. N. Schuldt, On the Security of RC4 in TLS and WPA, USENIX Security Symposium, **2013.**

[27] A. Popov, Prohibiting RC4 Cipher Suites, https://www.rfc-editor.org/info/rfc7465, **2015.**

[28] Microsoft, https://support.microsoft.com/en-us/help/2960358/microsoft-security-advisory-vulnerability-in-the-net-framework-may-13, 2014

(Erişim tarihi **27.01.2019**).

[29] A. Beutelspacher, Cryptography, The Mathematical Association of America, İng Çeviri: Chris J. Fisher, **1996.**

[30] W. Diffie, M. E. Hellman, Multiuser cryptographic techniques, AFIPS Conference Proceedings Vol.45: National Computer Conference, **1976.**

[31] W. Diffie, The first ten years of public-key cryptography, Proceedings of the IEEE, Vol. 76, No. 5, pp. 560-577, **1988.**

[32] S.L. Graham, R.L. Rivest, A Method for Obtaining Digital Signatures and PublicKey Cryptosystems, Communications of the ACM, Volume 21 Issue, Pages 120-126, **1978.**

[33] NIST, Announcing the Standard for Dıgıtal Sıgnature Standard (DSS), Federal Information Processing Standards Publication 186, **1994.**

[34] T. Elgamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Transactıons On Informatıon Theory, Vol. IT-31, No. 4, **1985.**

[35] A. Shetty, K. S. Shetty, K. Krithika, A Review on Asymmetric Cryptography –RSA and ElGamal Algorithm, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 5, **2014.**

[36] M. Kim, J. Kim, J. H. Cheon, Compress Multıple Cıphertexts Usıng Elgamal Encryptıon Schemes, Journal Of The Korean Mathematical Society, Vol. 50, Issue 2, Pp.361-377, **2013.**

[37] S. Farah, M. Y. Javed, A. Shamim, T. Nawaz, An experimental study on Performance Evaluation of Asymmetric Encryption Algorithms, WSEAS 3rd European Conference of Computer Science, **2012.**

[38] T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, RFC 5246, August **2008.**

[39] Network Working Group of the IETF, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January **2006.**

[40] A. K. Lenstra, J. P. Hughes, M. Augier, J. W. Bos, T. Kleinjung, C. Wachter, Public Keys, CRYPTO 2012: Advances in Cryptology, pp 626-642, **2012.**

[41] L. Bello, DSA-1571-1 OpenSSL—Predictable random number generator,

Debian Security Advisory, 2008**.** http://www.debian.org/security/2008/dsa-1571 (Erişim tarihi: **27.01.2019**)

[42] N. Heninger, Z. Durumeric, E. Wustrow, J. A. Halderman, Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices, Proceedings of the 21st USENIX Security Symposium, pp. 206–220, **2012.**

[43] H. Schmidt, Quantum-Mechanical Random-Number Generator, Journal Of Applied Physics Volume 41, Number 2, February **1970.**

[44] W. Heisenberg, Uber den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik, Z. Phys. 43, 172 (1927). / The Physical Content of Quantum Kinematics and Mechanics see in: Quantum Theory of Measurement, ed. By J. A. Wheeler, W. H. Zurek, Princeton University Press, N.J. **1983.**

[45] M. Stipcevic, Ç. K. Koç, True Random Number Generators, Open Problems in Mathematics and Computational Science, **2014.**

[46] M. Siswanto, B. Rudiyanto, Designing of Quantum Random Number Generator(QRNG) for Security Application, 3rd International Conference on Science in Information Technology (ICSITech), **2017.**

[47] W. Wei, H. Guo, Bias-Free True Random-Number Generator, Optics Letter, Vol. 34, Issue 12, pp. 1876-1878, **2009.**

[48] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, G. Leuchs, A Generator for Unique Quantum Random Numbers Based on Vacuum States, Nature Photonics, Vol. 4, No. 10, pp. 711-715, **2010.**

[49] Y. Shen, L. A. Tian, H. X. Zou, Practical Quantum Random Number Generator Based on Measuring the Shot Noise of Vacuum States, Physics Review, Vol. 81, Iss. 6, **2010.**

[50] M. Herrero-Collantes, J. C. Garcia-Escartin, Quantum Random Number Generators, Review of Modern Physics, Vol. 89, page 015004, Oct 24, **2016.**

[51] B. Hayes, Randomness as a Resource, American Scientist, Vol. 89, No. 4, pp. 300-304, **2001.**

[52] N. Metropolis, S. Ulam, The Monte Carlo Method, Journal of the

American Statistical Association, Vol. 44, No. 247, pp. 335-341, **1949.**

[53] Artificial Intelligence and Interactive Digital Entertainment, https://sites.google.com/ncsu.edu/aiide-2018/home, (Erişim tarihi **27.01.2019**).

[54] D. E. Knuth, The Art of Computer Programming, Volume 2 (3rd edition), Seminumerical Algorithms, Addison-Wesley Longman Publishing Co., Inc., Boston, **1997.**

[55] D. H. Lehmer, Mathematical Methods in Large-scale Computing Units, Annals of the Computation Laboratory of Harvard University 26, pp 141–146, **1951.**

[56] G. Marsaglia, Xorshift RNGs, Journal of Statistical Software, Vol. 8, Issue 14, **2003.**

[57] F. Panneton, P. L'ecuyer, Improved Long-Period Generators Based on Linear Recurrences Modulo 2, ACM Transactions on Mathematical Software, Vol. 32, No. 1, Pages 1–16, **2006**.

[58] D.E. Knuth, The Art of Computer Programming, volume 2: Seminumerical Algorithms. Addison-Wesley, 2nd edition, **1981.**

[59] K. Entacher, A Collection of Selected Pseudo-Random Number Generators with Linear Structures, Tech. Report Series Nr. ACPC/TR 97-1, Austrian Center for Parallel Computation, **1997**.

[60] P. L'Ecuyer, Random Number Generation, Hand-book of Computational Statistics, edited by J.E. Gentle, W.K. Hardle, and Y. Mori, pp 35–71, **2012.**

[61] M. Matsumoto, T. Nishimura, Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator, ACM Transactions on Modeling and Computer Simulation, pp 3–30, **1998.**

[62] MATLAB,http://www.mathworks.com/help/matlab/ref/randstream.list.html (Erişim tarihi **27.01.2019**).

[63] PYTHON,https://docs.python.org/release/2.6.8/library/random.html (Erişim tarihi **27.01.2019**).

[64] C++, Standard C++ Foundation, Random Number Generation in C++11, 2013 (Erişim tarihi **27.01.2019**).

[65] Mathematica:https://reference.wolfram.com/language/tutorial/Random

NumberGeneration.html (Erişim tarihi **27.01.2019**).

[66] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J.Dray, S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Special Publication 800-22 Revision 1a, Revised: **2010.**

[67] M. Blum, S. Micali, How to Generate Cryptographically Strong Sequaneces of Pseudo-Random Bits, **1984.**

[68] M. Blum, L. Blum, M. Shub, A Simple Unpredictable Pseudo-Random Number Generator, SIAM Journal on Computing, Vol. 15, Issue 2, pp 364-383, **1986.**

[69] W. Killmann, W. Schindler, A Design for a Physical RNG with Robust Entropy Estimators, Lecture Notes in Computer Science, Vol. 5154, pp 146–163, **2008.**

[70] H. Nyquist, Thermal Agitation of Electric Charge in Conductors, American Physical Society, Physical Review 32, pp 110–113, **1928.**

[71] J. B. Johnson, Thermal agitation of electricity in conductors, Physical Review 32, page 97, **1928.**

[72] W. T. Holman, J. A. Connelly, A. B. Dowlatabadi, An Integrated Analog/Digital Random Noise Source, IEEE Transactıons On Cırcuıts And Systems—I: Fundamental Theory And Applıcatıons, Vol. 44, No. 6, pp 521-527, **1997.**

[73] M. Stipčević, Fast nondeterministic random bit generator based on weakly correlated physical events, American Institute of Physics, Vol. 75, Issue 11, pp. 4442 – 4449, **2004.**

[74] G. Kolumban, M. P. Kennedy, L. O. Chua, The Role of Synchronization in Digital Communications Using Chaos—Part I: Fundamentals of Digital Communications, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 44, Issue 10, pp 927-936, **1997.**

[75] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, A High-Speed Oscillator-Based Truly Random Number Source for Cryptographic Applications on a Smart Card IC, IEEE Transactıons On Computers, Vol.

52, No. 4, pp. 403 – 409, **2003.**

[76] B. Sunar, W. J. Martin, D. R. Stinson, A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks, IEEE Transactıons On Computers, Vol. 56, No. 1, pp. 109 – 119, **2007.**

[77] M. Stipčević, B. Medved Rogina, Quantum random number generator based on photonic emission in semiconductors, Review of Scientific Instruments, Vol. 78, **2007.**

[78] LINUX, https://linux.die.net/man/4/random, (Erişim tarihi **27.01.2019**).

[79] WINDOWS,https://lists.gnupg.org/pipermail/gnupg-users/2001-November/ 010831.html (Erişim tarihi **27.01.2019**).

[80] I. Goldberg, D. Wagner, R. Thomas, E. A. Brewer, A Secure Environment for Untrusted Helper Applications (Confining the Willy Hacker), in Proceedings of Sixth USENIZ UNIX Security Symposium, California, **1996.**

[81] H.F. Murry, A General Approach for Generating Natural Random Variables, IEEE Transactions on Computers, Vol. C-19 , Issue 12, pp. 1210 – 1213, **1970.**

[82] C.S. Petrie, J.A. Connelly, A noise-based IC random number generator for applications in cryptography, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 47, Issue 5, pp. 615 – 621, **2000.**

[83] P. Kohlbrenner, K. Gaj, An embedded true random number generator for FPGAs, SIGDA 12th International Symposium on Field Programmable Gate Arrays, New York, pp. 71 – 78, **2004.**

[84] J. von Neumann, Various techniques for use in connection with random digits, Von Neumann's Collected Works, pp. 768–770, **1963.**

[85] Y. Peres, Iterating von Neumann's procedure for extracting random bits, The Annals of Statistics, vol 20, no 1, pp. 590–597, **1992.**

[86] A. Juels, M. Jakobsson, E. Shriver, B. K. Hillyer, How to turn loaded dice into fair coins, IEEE Transactıons On Informatıon Theory, Vol. 46, No. 3, **2000.**

[87] V. Bagini, M. Bucci, A Design of Reliable True Random Number Generator for Cryptographic Applications, Cryptographic Hardware and

Embedded Systems, pp. 204-218, **1999.**

[88] M. Stipcevic, Apparatus and method for generating true random bits based ontime integration of an electronic noise source, WIPO Patent Number WO03040854, October 17, **2001**.

[89] G.Taylor, George Cox, Digital randomness, IEEE Spectrum, Vol. 48 Issue 9, pp. 32 – 58, **2011**.

[90] C. Cachin, Entropy Measures and Unconditional Security in Cryptography, PhD thesis, Swıss Federal Instıtute Of Technology, Zurıch, **1997.**

[91] S. Ross, A first course in probability, Pearson Education, 9th edition, **1998.**

[92] C. E. Shannon, A Mathematical Theory of Communication, The Bell System Technical Journal, Vol. 27, Issue 3, pp. 379–423, 623–656, **1948.**

[93] A. Renyi, On Measures of Entropy and Information, In Proceedings of the 4th Berkeley symposium on mathematics, statistics and probability, pp. 547–561, **1961.**

[94] P. Jizba, T. Arimitsu, The world according to Renyi: Thermodynamics of multifractal systems, Vol. 312, Issue 1, Pp. 17-59, **2004**.

[95] P. Jizba, T. Arimitsu, On observability of R´enyi's entropy, Physical Review E, Vol. 69, Iss. 2, **2004.**

[96] O. Rioul, J. C. Magossi, On Shannon's Formula and Hartley's Rule: Beyond the Mathematical Coincidence, Entropy, Vol 16, pp. 4892 – 4910, **2014.**

[97] B. Barak, R. Impagliazzo, A. Wigderson, Extracting randomness using few independent sources, 45th Annual IEEE Symposium on Foundations of Computer Science, pp. 384-393, **2004.**

[98] J. Bourgain, More on the sum–product phenomenon in prime fields and its applications, International Journal of Number Theory, Vol. 01, No. 01, pp. 1-32, **2005.**

[99] A. Rao, Extractors for a constant number of polynomially small min-entropy independent sources, SIAM Journal on Computing, Vol. 39, Issue 1, pp. 497-506, **2006.**

[100] B Chor, O. Goldreich, Unbiased bits from sources of weak randomness and probabilistic communication complexity, SIAM Journal on Computing, Vol. 17, No. 2 : pp. 230-261, **1988** .

[101] N. Nisan, D. Zuckerman, Randomness is linear in space, Journal of Computer and System Sciences, Vol. 52, Issue 1, pp. 43-52, **1996.**

[102] N. Alon, J.H. Spencer, The Probabilistic Method (Wiley Series in Discrete Mathematics and Optimization), 4th edition, **2016.**

[103] A. Ben-Aroya, A. Ta-Shma, Better short-seed quantum-proof extractors, Theoretical Computer Science, vol. 419, pp. 17–25, **2012.**

[104] L. Trevisan, Extractors and pseudorandom generators, Journal of the ACM, Vol. 48, pp. 860–879, **2001.**

[105] R. König, R. Renner, Sampling of Min-Entropy Relative to Quantum Knowledge, IEEE Transactions on Information Theory, Vol. 57 Issue 7, pp. 4760–4787, **2011.**

[106] B. Barak, R. Shaltiel, E. Tromer, True Random Number Generators Secure in a Changing Environment, CHES 2003: Cryptographic Hardware and Embedded Systems, ,pp. 166-180, **2003.**

[107] M. Skorski, True random number generators secure in a changing environment: Improved security bounds, SOFSEM 2015: Theory and Practice of Computer Science, pp. 590-602, **2015.**

[108] X.Ma, F. Xu, H. Xu, X. Tan, B. Qi, H. Lo, Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction, Phys. Rev. A, vol. 87, p. 062327, **2013.**

[109] A. N. Kolmogorov, On tables of random numbers, Theoretical Computer Science, vol. 207, pp. 387 – 395, 6 November **1998.**

[110] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Defense Technical Information Center, ADA393366, **2001.**

[111] TestU01, http://simul.iro.umontreal.ca/testu01/tu01.html (**Erişim tarihi 27.01.2019**).

[112] G. Marsaglia, Diehard: a battery of tests of randomness, http://stat.fsu.edu/˜geo/diehard.html, 1996 (Erişim tarihi **27.01.2019**).

[113] A. Figotin, I. Vitebskiy, V. Popovich, G. Stetsenko, S. Molchanov, A. Gordon, J. Quinn, N. Stavrakas, Random number generator based on the spotaneous alpha-decay, U.S. patent Appl. No.: 10/127,221, **2003.**

[114] M. Rohe, RANDy – A True-Random Generator Based On Radioactive Decay, Security and Cryptography Research Group Saarland University, pp. 1-36, **2003.**

[115] HotBits, http://www.fourmilab.ch/hotbits/ (Erişim tarihi **27.01.2019**).

[116] H. Geiger, Geiger Counter Tubes, Proceedings of the IRE, Vol. 37 Issue 7, pp. 791 – 808, **1949.**

[117] J. L. Brady, Limitations of a True Random Number Generator in a Field Programmable Gate Array, Air Force Institute of Technology, AFIT/GE/ENG/08-01, Degree of Master of Science in Electrical Engineering, **2007.**

[118] J.H. Lee, I.J. Kim, H.D. Choi, On the dead time problem of a GM counter, Applied Radiation and Isotopes, Vol. 67 Issue 6, pp. 1094-1098, **2009**.

[119] H. G. Stever, The Discharge Mechanism of Fast G-M Counters from the Deadtime Experiment, Phys. Rev., Vol. 61, page 38, **1942.**

[120] S. H. Lee, R. P. Gardner, A new G-M counter dead time model, Applied Radiation and Isotopes, Vol. 53, pp. 731-737, **2000.**

[121] S. H. Lee, M. Jae, R. P.Gardner, Non-Poisson counting statistics of a hybrid G–M counter dead time model, Nuclear Instruments and Methods in Physics Research Section B: Beam Interactions with Materials and Atoms, Vol. 263, Issue 1, Pages 46-49, **2007.**

[122] W. Schottky, Uber spontane Stromschwankungen in verschiedenen Elektrizit¨atsleitern, Annalen der Physik, Vol. 362 Issue 23, pp. 541–567, **1918.**

[123] C. W. J. Beenakker, M. Büttiker, Suppression of shot noise in metallic diffusive conductors, Phys. Rev. B, Vol. 46 Issue 3, **1992**.

[124] J.G. Rarity, P.C.M. Owens, P.R. Tapster, Quantum Random-number Generation and Key Sharing, Journal of Modern Optics, Vol. 41, Issue 12, pp. 2435-2444, **1994.**

[125] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, A fast

and compact quantum random number generator, Review of Scentific Instruments, Vol. 71, Issue 4, pp. 1675-1680, **2000**.

[126] M. Gräfe, R. Heilmann, A. Perez-Leija, R. Keil, F. Dreisow, M. Heinrich, H. Moya-Cessa, S. Nolte, D. N. Christodoulides, A. Szameit, On-chip generation of high-order single-photon W-states, Nature Photonics, Vol. 8, pp. 791 – 795, **2014.**

[127] J. F. Dynes, Z.L. Yuan, A.W. Sharpe, A.J. Shields, A high speed, postprocessing free, quantum random number generator, Applied Physics Letters, Vol. 93, Issue 3, page 031109, **2008.**

[128] R. C. Bose, D. K. Ray-Chaudhurı, On A Class of Error Correcting Binary Group Codes, Information and Control, Vol. 3, Issue 1, pp 68-79, **1960.**

[129] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, H.Zeng, Quantum random-number generator based on a photon-number-resolving detector, Phys. Rev. A, Vol. 83, pp. 1293–1304, **2011.**

[130] M. Fürst, H. Weier, S. Nauerth, D.G. Marangon, C. Kurtsiefer, H.Weinfurter, High speed optical quantum random number generation, Optics Express, Vol. 18, Issue 12, pp. 13029 – 13037, **2010.**

[131] Y. Jian, M. Ren, E. Wu, G. Wu, and H. Zeng, Two-bit quantum random number generator based on photonnumber- resolving detection, The Review of Scientific Instuments, Vol 82, Issue 7, page 073109, **2011.**

[132] S. Tisa, F. Villa, A. Giudice, G. Simmerle, and F. Zappa, High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors, IEEE Journal of Selected Topics in Quantum Electronics, Vol. 21, Issue 3, **2015.**

[133] Micro Photon Devices, http://www.micro-photon-devices.com/Products (Erişim tarihi **27.01.2019**).

[134] B. Sanguinetti, A. Martin, H. Zbinden, N. Gisin, Quantum Random Number Generation on a Mobile Phone, Physıcal Revıew X, Vol. 4, page 031056, **2014.**

[135] D. F. Walls, Squeezed states of light, Nature, Vol. 306, pp. 141–146, **1983.**

[136] L. Oberreiter, I. Gerhardt, Light on a beam splitter: More randomness with single photons", Laser Photonics Rev., Vol.10, Issue 1, pp. 108–

115, **2016.**

[137] R. Hain, C. J. Kähler, C. Tropea, Comparison of CCD, CMOS and intensified cameras, Experiments in Fluids, Vol. 42, Issue 3, pp 403–411, **2007.**

[138] C. H. Bennett, G. Brassard, Quantum cryptography: Public key distribution and coin tossing, In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. 175, page 8, **1984**.

[139] E. Artur, Quantum cryptography based on Bell's theorem, Physical review Letters, Vol. 67, No. 6, pp 661-663, **1991**.

[140] H. Singh, D.L. Gupta, A.K. Singh, Quantum Key Distribution Protocols: A Review, IOSR Journal of Computer Engineering, Vol. 16, Issue 2, pp. 1-9, **2014**.

[141] J. Yin, Y. Cao, Y.H. Li, S.K. Liao, L. Zhang, J.G. Ren, W.Q. Cai, W.Y. Liu, B. Li, H. Dai, G.B. Li, Q.M. Lu, Y.H. Gong, Y. Xu, S.L. Li, F.Z. Li, Y.Y. Yin, Z.Q. Jiang, M. Li, J.J. Jia, G. Ren, D. He, Y.L. Zhou, X.X. Zhang, N. Wang, X. Chang, Z.C. Zhu, N.L. Liu, Y.A. Chen, C.Y. Lu, R. Shu, C.Z. Peng, J.Y. Wang, J.W. Pan, Satellite-based entanglement distribution over 1200 kilometers, Science, Vol. 356, Issue 6343, pp. 1140–1144, **2017.**

[142] C. Kenny, Random number generators: An evaluation and comparison of random.org and some commonly used generators, Trinity College Dublin, Management Science and Information Systems Studies Project report, **2005**

[143] P. L'Ecuyer, R. Simard, TestU01: A C library for empirical testing of random number generators, ACM Transactions on Mathematical Software (TOMS), Vol. 33 Issue 4, **2007**

[144] NIST, Computer Security Resource Center, SP 800-22: Download Documentation and Software, https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software (Erişim tarihi: **27.01.2019**)

ÖZGEÇMİŞ

Kimlik Bilgileri:

Adı Soyadı	: Safa HANKÖYLÜ
Doğum Yeri	: Ankara
Medeni Hâl	: Bekâr
E-posta	: safahankoylu@gmail.com

Eğitim:

Lisans	: Gazi Üniversitesi, Elektrik ve Elektronik Mühendisliği, 2013
Yüksek Lisans	: Hacettepe Üniversitesi, Elektrik ve Elektronik Mühendiliği, 2019

İş Tecrübesi:

Aralık 2014 - Ocak 2019	: Bilimsel Programlar Uzman Yardımcısı, TÜBİTAK Başkanlık, ANKARA
Şubat 2019 - …	: Sistem Mühendisi, ROKETSAN A.Ş., ANKARA

Yabancı Dil:

İngilizce	: İyi

HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
YÜKSEK LİSANS/DOKTORA TEZ ÇALIŞMASI ORJİNALLİK RAPORU

HACETTEPE ÜNİVERSİTESİ
FEN BİLİMLER ENSTİTÜSÜ
ELEKTRİK VE ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI BAŞKANLIĞI'NA

Tarih: 12./02./2019

Tez Başlığı / Konusu: Kuantum Rastgele Sayı Üreteci Tasarımı ve Uygulaması / Tek LED'li beyaz bir ışık kaynağından alınan görüntülerin RGB (Red – Green - Blue) değerlerinden faydalanılarak bir Kuantum Rastgele Sayı Üreteci elde edilmiştir.

Yukarıda başlığı/konusu gösterilen tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler d) Sonuç kısımlarından oluşan toplam 52 sayfalık kısmına ilişkin, 11/02/2019 tarihinde tez danışmanım tarafından *Turnitin* adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı % 1 'dir.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar ~~hariç~~ / dâhil
3- ~~5 kelimeden daha az örtüşme içeren metin kısımları hariç~~

Hacettepe Üniversitesi Fen Bilimleri Enstitüsü Tez Çalışması Orjinallik Raporu Alınması ve Kullanılması Uygulama Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Gereğini saygılarımla arz ederim.

Tarih ve İmza

12.02.2019

S. Hankoylu

Adı Soyadı:	Safa HANKÖYLÜ
Öğrenci No:	N13223855
Anabilim Dalı:	Elektrik ve Elektronik Mühendisliği
Programı:	Tezli
Statüsü:	☒ Y.Lisans ☐ Doktora ☐ Bütünleşik Dr.

DANIŞMAN ONAYI

UYGUNDUR.

A. O. Alkar

Prof. Dr. Ali Ziya ALKAR