FBE TEZ YAZIMINA BAŞLAMADAN ÖNCE

- ✓ Tez yazım kuralları hakkında birinci kaynak Tez Yazım Kılavuzudur.
- ✓ Bu şablon, Enstitü internet sayfasındaki "Şablon Açıklaması" dikkate alınarak hazırlandığında sadece şekil yönünden Tez Yazım Kılavuzundaki şartları sağlar. Bölüm içeriklerinin doğru hazırlanması tez yazarının sorumluluğundadır.
- ✓ Bu şablon MS Word Belge Şablonu olarak hazırlanmıştır. Sadece Enstitü internet sayfasından indireceğiniz şablonlara güveniniz. Başka kaynaklardan edindiğiniz şablonlara güvenmeyiniz. Bu konuda Enstitü sorumluluk kabul etmez.
- ✓ Word dosyaları yazıcı ayarlarına bağlı olarak sayfa kaymalarına neden olabilmektedir. Bu yüzden, yazımı tamamlanan tezin PDF formatında kaydedilmesi ve bu format üzerinde kontroller yapılıp PDF dosyasından baskısının alınması önerilir. Kağıt ortamındaki tez kopyasının Tez Yazım Kurallarına uymak zorunda olduğu unutulmamalıdır.
- ✓ Tüm paragraf işaretlerini (boşluklar ve tablar gibi) ve gizli biçimlendirme işaretlerini (sayfa sonu, bölüm sonu gibi) Word programında Giriş sekmesinde ¶ simgesine tıklayıp görebilir veya gizleyebilirsiniz. Bölüm sonu ve sayfa sonu ifadelerini gereksiz şekilde silmeyiniz. Aksi takdirde sayfa numaralandırma yapısı bozulacak ve yeniden yapılandırmak zorunda kalınacaktır.
- ✓ Şablon içindeki tüm açıklama yazıları tezinizin baskısından önce mutlaka silinmelidir.
- ✓ Bir sonraki sayfada bulunan tabloyu eksiksiz doldurduğunuzda İlk Sayfalar ve Ön Bölümler hazırlanmış olacaktır. Tablo içindeki tüm alanlar klavyeden giriş yapılarak doldurulmalı, kesinlikle stil galerisinden stil değişimi veya başka bir alandan kopyala/yapıştır yapılmamalıdır.
- ✓ Tez kitapçığının sadece şekil açısından değil aynı zamanda bazı bölümlerinin içeriklerinin de Tez Yazım Kurallarına uymak zorunda olduğu unutulmamalıdır. Önsöz, Özet, Abstract, Listeler ve Giriş Bölümü içeriklerinin nasıl hazırlanması gerektiği konusunda Tez Yazım Kılavuzu ve Şablon Açıklaması mutlaka incelenmelidir.
- ✓ Bu bilgilendirme sayfası ve bundan sonraki tablo sayfası tez kitapçığında bulunmamalıdır.

ÖNEMLİ HATIRLATMA

Lisansüstü eğitimde bir tez, bilimsel bir problemin çözümünü öngören hipotezlerin bilimsel metotlarla doğrulanmaya çalışılması sonucunda elde edilen bilgilerin sunulduğu yazılı bilimsel rapordur.

Bu nedenle, bir tezde aşağıdaki soruların cevapları net şekilde bulunmalıdır:

- Bilimsel probleminiz nedir? – Problem tanımı
- Bu problem neden önemlidir? – Problemin önemi
- Tezinizin nihai amacı nedir? – Amaç
- Problemin hangi değişkenleri arasında nasıl bir ilişki olabileceğini varsaydınız? – Hipotezler
- Değişkenler arasındaki ilişkinin varlığını hangi metotlarla göstermek, ispatlamak istiyorsunuz? – Metot
- Başka araştırmacıların probleminize veya benzer problemlere yaklaşımları nelerdir? – Literatür bilgisi
- Problemin çözümü kimlere ne gibi faydalar sağlar? – Toplumsal fayda.
- Ne tür materyaller ve metotlar kullandınız? – Materyal ve Metot
- Yaptığınız deneylerin ve/veya gözlemlerin sonucunda elde ettiğiniz veriler nelerdir? – Bulgular
- Her bir bulgunun analizinden sonra hangi yorumları yaptınız? – Tartışma ve yorum
- Tartışma ve yorumlarınızdan sonra insanlığa ve bilime kazandırdığınız bilgiler nelerdir? – Sonuç
- Hangi eserlerden yararlandınız? – Kaynaklar

İlk 7 sorunun cevabı Giriş Bölümünde bulunmalıdır. 5. Sorunun cevabı ayrıca bir bölüm veya alt bölüm olarak detaylı şekilde verilir. Diğer soruların cevapları için ayrı bölümler kullanılır.

Tez yazımınızda kolaylıklar dileriz.

1. **TABLOYU DOLDURURKEN** sadece klavyeden giriş yapınız, başka bir ortamdan kopyala/yapıştır yapmayınız. Ayrıca, stiller galerisinden farklı bir stil uygulamayınız.
2. Tez başlığında zorunlu durumlarda italik, üst-alt simge, Yunan karakterleri oluşturulabilir. İngilizce kelime var ise sadece o kelime işaretlenip "Gözden Geçir" sekmesinden dil İngilizce yapılır. Küçük harf kullanılması gerekiyor ise Pencere Altı ve İç Kapakta Tez Başlığı üzerinde metin kutusu (kırmızı bilgi kutuları gibi) oluşturup gerekli düzeltmeler yapılabilir.
3. Tezin Enstitüye ilk tesliminde Tez Onayı sayfası bulunmaz. Sadece danışman bilgileri tabloya girilir.
4. Tezin Enstitüye son tesliminde jüri üyeleri bilgilerini tabloya yazınız. Fazla olan haneleri aşağıdaki tabloda aynen bırakınız. Ancak, Onay Sayfasında satırları silerek gerekli düzenlemeyi yapınız.
5. Bilim Dalı yoksa, Pencere Alt Kapağında bulunan "Bilim Dalı" ifadesini bir boşluk vererek siliniz.
6. Mendeley eklentisi ile çalışıldığında hata mesajı alırsanız "End" seçimi yaparak işlemlerinize devam ediniz.
7. İkinci Danışman yoksa, Kapak Sayfasındaki "İkinci Danışman" satırını ve Onay Sayfasındaki İkinci Danışman satırlarını siliniz.

Tez Yazarı:	Beyzanur DURMUŞ	
	TÜRKÇE	**İNGİLİZCE**
Tez Başlığı, tez ilk teslimde Enstitü tescilli (transkriptteki) başlıktır. Son teslimde Jüri tarafından önerilen başlıktır.		
Tez Türü:	Yüksek Lisans Tezi	Master's Thesis
Tez Başlığı:	Biyometrik Sistemler Temelli Kriptolojik Anahtar Üreteç Tasarımı	Biometric Systems Based Cryptological Key Generator Design
Anabilim Dalı:	Yazılım Mühendisliği	Software Engineering
Programı (Teknoloji):		
Bilim Dalı:		
Tez İlk Teslim Tarihi:	09.12.2020	Tezin Enstitüye verildiği **İlk Tarih**
Savunma Tarihi:	15.08.2022	
Tez Ön Sayfa Sayısı:	xi	Kısaltmalar Listesinin bulunduğu sayfa numarasıdır
Tez Sayfa Sayısı:	61	Kaynaklar Bölümünün bitiş sayfa numarasıdır

	JÜRİ ORTAK KARARI	**<OYBİRLİĞİ>**
Danışman:	Doç. Dr. Fatih ÖZKAYNAK	<Onayladım>
Danısman Kurumu:	Fırat Üniversitesi, Teknoloji Fakültesi	
2. Danışman:	Yoksa boşluk vererek siliniz	<Onayladım>
2. Danışman Kurumu:	Yoksa boşluk vererek siliniz	
Jüri Başkanı:	Dr. Öğr. Üyesi Murat AYDOĞAN	<Onayladım>
Jüri Başkanı Kurumu:	Fırat Üniversitesi, Teknoloji Fakültesi	
Jüri Üyesi 1:	Dr. Öğr. Üyesi Muhammed YILDIRIM	<Onayladım>
Jüri Üyesi 1 Kurumu:	Malatya Turgut Özal Üniversitesi, Mühendislik ve Doğa Bilimleri	
Jüri Üyesi 2:	Unvan Adı SOYADI	<Onayladım>
Jüri Üyesi 2 Kurumu:	... Üniversitesi, ... Fakültesi	
Jüri Üyesi 3:	Unvan Adı SOYADI	<Onayladım>
Jüri Üyesi 3 Kurumu:	... Üniversitesi, ... Fakültesi	
Jüri Üyesi 4:	Unvan Adı SOYADI	<Onayladım>
Jüri Üyesi 4 Kurumu:	... Üniversitesi, ... Fakültesi	
Enstitü Müdürü:	Prof. Dr. Kürşat Esat ALYAMAÇ	

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİYOMETRİK SİSTEMLER TEMELLİ KRİPTOLOJİK ANAHTAR ÜRETEÇ TASARIMI

Beyzanur DURMUŞ

Yüksek Lisans Tezi

YAZILIM MÜHENDİSLİĞİ ANABİLİM DALI

AĞUSTOS 2022

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

BİYOMETRİK SİSTEMLER TEMELLİ KRİPTOLOJİK ANAHTAR ÜRETEÇ TASARIMI

Tez Yazarı
Beyzanur DURMUŞ

Danışman
Doç. Dr. Fatih ÖZKAYNAK

AĞUSTOS 2022
ELAZIĞ

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Yazılım Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Başlığı:	Biyometrik Sistemler Temelli Kriptolojik Anahtar Üreteç Tasarımı
Yazarı:	Beyzanur DURMUŞ
İlk Teslim Tarihi:	09.12.2020
Savunma Tarihi:	15.08.2022

TEZ ONAYI

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

		İmza
Danışman:	Doç. Dr. Fatih ÖZKAYNAK Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Başkan:	Dr. Öğr. Üyesi Murat AYDOĞAN Fırat Üniversitesi, Teknoloji Fakültesi	Onayladım
Üye:	Dr. Öğr. Üyesi Muhammed YILDIRIM Malatya Turgut Özal Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi	Onayladım

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

İmza

Prof. Dr. Kürşat Esat ALYAMAÇ
Enstitü Müdürü

BEYAN

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

15.08.2022

Beyzanur DURMUŞ

ÖNSÖZ

Bu çalışmam boyunca değerli vaktini bana ayırarak çalışmamın tamamlanmasında her türlü desteğini esirgemeyen sayın danışman hocam Doç. Dr. Fatih ÖZKAYNAK ‘a sonsuz teşekkürlerimi sunarım.

Bu tez çalışması TÜBİTAK tarafından 120E444 protokol numaralı Kaotik Entropi Kaynakları ve Optimizasyon Algoritmaları Kullanılarak Gürbüz Anahtar Üreteçlerin Tasarımı ve Mobil Platformlar İçin Pratik Uygulamaların Geliştirilmesi isimli proje ile desteklenmiştir. TÜBİTAK kurumuna teşekkürlerimi sunarım.

Son olarak hayatımın her alanında ilgi, anlayış ve desteklerini esirgemeyen aileme çok teşekkür ediyorum.

Beyzanur DURMUŞ
ELAZIĞ, 2022

İÇİNDEKİLER

Sayfa

ÖZET

Biyometrik Sistemler Temelli Kriptolojik Anahtar Üreteç Tasarımı

Beyzanur DURMUŞ

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü

Yazılım Mühendisliği Anabilim Dalı

Ağustos 2022, Sayfa: xi + 61

Dijital dönüşüm ile birlikte birçok alışkanlık gibi ödeme yöntemleri de büyük bir değişim geçirmiştir. Elektronik ticaretin sunmuş olduğu sürtünmesiz ortamın avantajları; birçok kişi için çeşitli fırsatlar sunmuştur. Ancak bu süreçte yaşanan güvenlik problemleri maddi ve manevi birçok olumsuzluk ile karşılaşılmıştır. Tez çalışmasının amacı bu problemi adresleyebilecek güvenlik çözüm önerilerinin geliştirilmesi ve pratik uygulamalarının tasarlanması olarak planlanmıştır.

Klasik şifrelerin çeşitli problemlere sahip olduğu son yirmi yılda birçok acı tecrübe ile doğrulanmıştır. Hem Gelir İdaresi Başkanlığı hem de Bankalar Birliği bu tip problemleri gidermek için çeşitli kurallar ve düzenlemeler ile bu problemleri adresleyebilmek için güvenli kimlik doğrulama süreçlerinin nasıl yapılması gerektiğine ilişkin yol haritalarını hazırlamışlardır. Belirlenen kurallar çerçevesinde ödeme sistemlerinin güvenliğinin matematiksel yaklaşımlarla kanıtlanması ciddi bir problemdir. Tez çalışmasında bu problemleri adresleyebilecek çözüm önerilerinin neler olabileceği araştırılmaya çalışılmıştır.

Ödeme sistemlerinin güvenliğini garanti edebilmek için çeşitli Donanım Güvenlik Modülleri bulunmaktadır. Ancak bu modüllerin maliyet ve performans bakımından problemleri bulunmaktadır. Donanım tabanlı önerilen çözümlerin yazılımsal olarak gerçeklenebileceği ve bu süreçte biyometrik ölçümlerin benzersiz değerler elde edebilmek için ciddi katkılar sunabileceği düşünülmektedir. Yapılan ön çalışmalar sonucunda elde edilen başarılı analiz sonuçları bu hipotezin desteklendiğini göstermiş ve ileride çeşitli pratik uygulamalarda başarılı bir şekilde kullanılabileceği düşünülmektedir.

Anahtar Kelimeler: Rastgele Sayı Üreteçleri, Biyometrik Sistemler, Bilgi Güvenliği, Kriptoloji

ABSTRACT

Biometric Systems Based Cryptological Key Generator Design

Beyzanur DURMUŞ

Master's Thesis

FIRAT UNIVERSITY
Graduate School of Natural and Applied Sciences

Department of Software Engineering

August 2022, Pages: xi + 61

With the digital transformation, payment methods, like many habits, have undergone a great change. Advantages of the frictionless environment offered by electronic commerce; It has offered a variety of opportunities for many people. However, the security problems experienced in this process have faced many material and moral negativities. The aim of the thesis study is to develop security solution proposals that can address this problem and to design their practical applications.

It has been confirmed by many bitter experiences over the last twenty years that classical passwords have various problems. Both the Revenue Administration and the Banks Association have prepared various rules and regulations to solve such problems, and roadmaps on how secure authentication processes should be done to address these problems. It is a serious problem to prove the security of payment systems with mathematical approaches within the framework of the determined rules. In the thesis study, it was tried to investigate what could be the solution proposals that could address these problems.

Various Hardware Security Modules are available to guarantee the security of payment systems. However, these modules have problems in terms of cost and performance. It is thought that the proposed hardware-based solutions can be implemented in software and in this process, biometric measurements can make serious contributions to obtain unique values. The successful analysis results obtained as a result of the preliminary studies have shown that this hypothesis is supported and it is thought that it can be used successfully in various practical applications in the future.

Keywords: Random Number Generator, Biometric Systems, Information Security, Cryptology

ŞEKİLLER LİSTESİ

Sayfa

TABLOLAR LİSTESİ

Sayfa

SİMGELER VE KISALTMALAR

Simgeler

φ	: Durum geçiş fonksiyonu
Ψ	: Çıkış fonksiyonu

Kısaltmalar

RSÜ	: Rastgele Sayı Üreteci
GRSÜ	: Gerçek Rastgele Sayı Üreteci
SRSÜ	: Sözde Rastgele Sayı Üreteci
HRSÜ	: Hibrit Rastgele Sayı Üreteci
TRNG	: True Random Generator
NIST	: National Institute of Standarts and Technology
ERFC	: The Complementary Error Function
IGAMC	: Incomplete Complementary Gamma Function
IEEE	: The Institute of Electrical and Electronics Engineer
LFSR	: Linear Feedback Shift Register

1. GİRİŞ

Klasik şifrelerin çeşitli problemlere sahip olduğu son yirmi yılda birçok acı tecrübe ile doğrulanmıştır. Hem Gelir İdaresi Başkanlığı hem de Bankalar Birliği bu tip problemleri gidermek için çeşitli kurallar ve düzenlemeler ile bu problemleri adresleyebilmek için güvenli kimlik doğrulama süreçlerinin nasıl yapılması gerektiğine ilişkin yol haritalarını hazırlamışlardır. Belirlenen kurallar çerçevesinde ödeme sistemlerinin güvenliğinin matematiksel yaklaşımlarla kanıtlanması ciddi bir problemdir. Tez çalışması bu problemi adresleyecektir.

Günümüzde dijital kanallarda işlem yapan alıcılar PIN kodları ve şifrelerle uğraşmak zorundadır ve tüm uyarılara rağmen, genellikle birden fazla hesap için aynı şifreleri kullanmaktan dolayı suçludurlar. Mobil ödemelerin küresel düzeyde genişlemesi, daha güvenli bir alternatif kimlik doğrulama sistemine olan ihtiyacı artırmıştır. Biyometrik ödeme pazarı, ana oyuncular olarak MasterCard ve Visa ile büyümeye hazırlanırken, Google ve Apple gibi mobil cüzdan satıcıları ve Samsung gibi mobil cihaz şirketleri de bu konuya ciddi yatırımlar yapmaktadır.

Doğrulama veya komutlar için biyometri kullanımı giderek daha yaygın hale gelmesine rağmen, tüketiciler, özellikle finansal verilerini korumakla ilgili olarak, geçerlilikleri konusunda hala ihtiyatlı davranmaktadırlar. Araştırmalara göre, alıcıların yarısından fazlası (% 56) ödemeleri doğrulamak için hala mütevazı şifreyi tercih etmektedir. Ancak, güçlü müşteri kimlik doğrulamasını zorunlu kılan mevzuatlar tam olarak yürürlüğe girdikten sonra, biyometri tabanlı ödemelerin doğrulama süreçlerinin anahtarı olacağı düşünülmektedir.

Kimlik doğrulaması gerektiren kartsız ödemelerin aşağıdaki üç öğeden en az ikisi aracılığıyla yapılması gerektiğidir:

- Bildiğiniz bir şey (şifre / PIN)
- Sahip olduğunuz bir şey (telefon / donanım belirteci)
- Olduğunuz bir şey (parmak izi veya yüz tanıma)

Dijital dönüşüm ile birlikte birçok alışkanlık gibi ödeme yöntemleri de büyük bir değişim geçirmiştir. Elektronik ticaretin sunmuş olduğu sürtünmesiz ortamın avantajları; birçok kişi için çeşitli fırsatlar sunmuştur. Ancak bu süreçte yaşanan güvenlik problemleri maddi ve manevi birçok olumsuzluk ile karşılaşılmıştır. Tez çalışmasının amacı bu problemi adresleyebilecek güvenlik çözüm önerilerinin geliştirilmesi ve pratik uygulamalarının tasarlanması olarak planlanmıştır.

Belirlenen kriterler çerçevesinde kimliği doğrulanmayan tüm kartsız ödeme işlemleri, kart veren kuruluşlar tarafından genel olarak reddedilecektir. Bu yeni gereksinimler, hem e-ticaret hem de m-ticaret için çok faktörlü kimlik doğrulamayı zorunlu kılacaktır. Bu kimlik doğrulama yöntemleri uygulandığında, parolaları kimlik doğrulamasından tamamen çıkarma potansiyeli

bulunmaktadır. Bunu yaparken, kimlik doğrulama sürecine ek katmanlar olduğu için güvenlik artacak ve aynı zamanda tüketiciler için ödeme sürecini kolaylaştıracaktır.

Ödeme sistemlerinin güvenliğini garanti edebilmek için çeşitli Donanım Güvenlik Modülleri (Hardware Secure Module) bulunmaktadır. Ancak bu modüllerin maliyet ve performans bakımından problemleri bulunmaktadır. Donanım tabanlı önerilen çözümlerin yazılımsal olarak gerçeklenebileceği ve bu süreçte biyometrik ölçümlerin benzersiz değerler elde edebilmek için ciddi katkılar sunabileceği düşünülmektedir. Yapılan bazı ön çalışmalar bu hipotezi desteklediği gösterilmiştir.

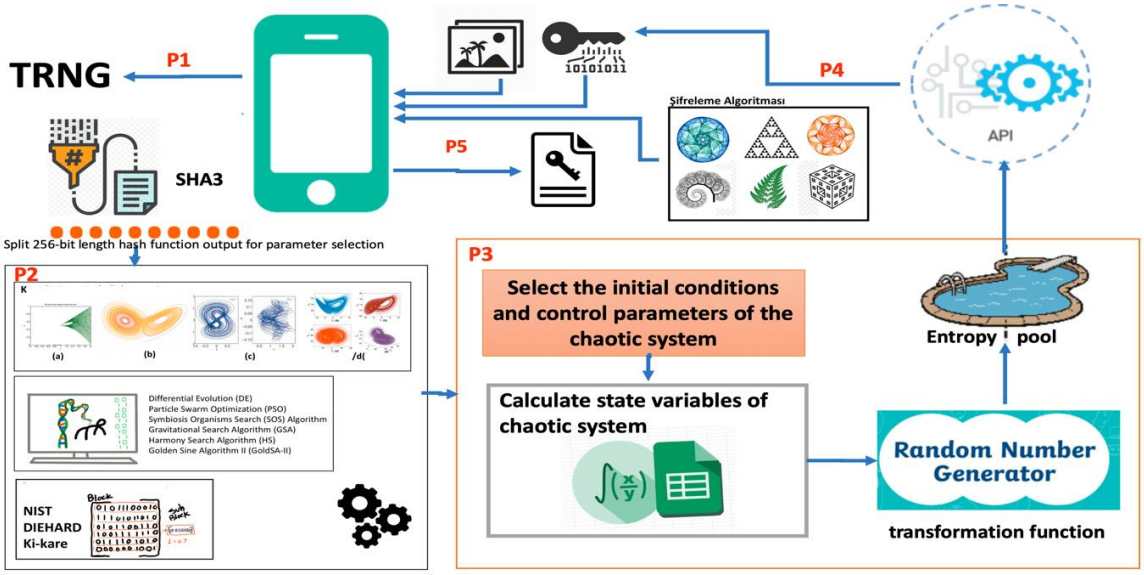
Bilim ve mühendislik çalışmaları tarih boyunca hep yeni şeylerin arayışı içerisinde olmuştur. Bu arayış serüveni boyunca araştırmacılar sürekli yeni bilgiler elde etmiş ve bu bilgi birikimini daha sağlıklı, daha rahat, daha huzurlu ve daha kaliteli yaşayabilmek için insanoğlunun hizmetine sunmuşlardır. Yaşadığımız yüzyılda ise bu yeni bilgileri elde etme süreci üstel bir hızla ilerlemektedir. Endüstri 4.0, yapay zeka ve nesnelerin interneti gibi kavramlar sayesinde artık tüm varlıkların birbiri ile etkileşim içerisinde olduğu devasa bir bilgi kümesi ortaya çıkmıştır. Büyük veri olarak tanımlanan bu devasa bilgi kümesi birçok alanı derinden etkilemiş ve etkilemeye de devam etmektedir. Ancak; büyük verinin içerisinde barındırdığı yıkıcı güç kötü emelli kişiler tarafından çok farklı amaçlar içinde kullanılmaktadır. Ne yazık ki bilim ve teknolojinin gelişmesinde en önemli rol oynatan etkenlerin başında savaşlar yer almaktadır. Barutun keşfinden, otomatik silahların tasarlanmasına; uçakların bir silah olarak kullanılmasından atom bombasına kadar birçok yıkıcı güç bilim ve mühendislik çalışmalarındaki ilerlemeler ile gerçekleşmiştir. 21. Yüzyıl ile birlikte savaş teknolojilerinde ciddi bir eksen kayması yaşanmıştır. Artık savaşlarda; tarafların gücü, orduların büyüklüğünden ziyade siber dünyadaki güçleri ile ilişkilendirilmeye başlanmıştır. ABD ve İsrail ortaklığı ile 2010 yılında İran nükleer santrallerine gerçekleştirilen Stuxnet isimli siber saldırı bu yeni savaş senaryosunun en çarpıcı örneklerinden biri olmuştur. Peki bu yeni nesil savaş tekniklerinin kişisel veri güvenliği özelliklede sağlık verilerinin güvenliği ile nasıl bir ilişkisi bulunmaktadır? Bu sorunun en çarpıcı yanıtı tez önerisinin kaleme alındığı dönemde ortaya çıkan ve Dünya Sağlık Örgütü tarafından tüm dünyanın kırmızı alarm ile önlemler alınmasına sevk eden çok ciddi bir hastalık ile yakından ilişkilidir. 2019-nCoV veya Vuhan korona virüsü olarak adlandırılan bu hastalığın insandan insana bulaşma hızı 2020 yılının Ocak ayı ortalarında hızlanmış ve ne yazık ki kısa zaman zarfında binin üzerinde kişi hayatını kaybetmiştir. Hastalığın içerisinde barındırdığı genetik materyal (genom) pozitif polariteli, tek iplikçikli RNA bugüne kadar tespit edilmiş en büyük RNA genomuna sahip virüslerden biridir. Her ne kadar bir komplo teorisi olarak nitelendirilse de bu hastalığın daha önce birçok yıkıcı güç tasarlayarak rakiplerine karşı üstünlük elde etme çabasının bir ürünü olup olmadığını akıllara getirmektedir. Bu noktada başka sorular da akıllara gelmektedir. Telefonunun kilidini açmak için yüz tanıma özelliğinden faydalanan, hastanelerde kimlik doğrulamak için avuç içi verini paylaşan ve çeşitli

bilgilere ulaşabilmek veya bir yardım kampanyasında yer almak için ilik, kan veya tükürük gibi genetik çeşitliliğini ortaya koyabilecek verileri paylaşmaktan çekinmeyen bir toplumu ileride hangi tehlikeler beklemektedir?

İnsanoğlu hala keşfedilmeyi bekleyen mükemmel bir varlıktır. Özellikle yüz, iris ve parmak izi gibi biyometrik veriler her insanda benzersiz özellikler barındıran parametrelerdir. Bu özelliklerin kimlik doğrulama süreçlerinde kullanılması sayısallaşan yaşantımız içerisinde önemli bir uygulama pratiğidir. Ancak bilginin güç olduğu çağımızda bu bilgilerin üçüncü kişiler tarafından kötü amaçlar için kullanılmayacağını beklemek hem milli hem de kişisel çıkarlar doğrultusunda büyük tehlikeler arz etmektedir. Bu bilgilerin üçüncü parti taraflarda herhangi bir güvenlik denetiminden geçirilmeden sunulması bir milletin genetik çeşitliliğinin kolaylıkla başka kişilerin eline geçmesine olanak sağlayacaktır. Bu yüzden genetik bilgiler kullanılarak gerçekleştirilebilecek siber saldırılara karşı veri gizliliğini garanti edebilecek çözümler mutlaka değerlendirilmelidir.

Bilginin önemi ve değeri yadsınamaz bir gerçektir. Dijital ortamların barındırdığı bilgi göz önüne alındığında problemin kritikliği daha fazla ön plan çıkmaktadır. Günümüzde yaşadığımız problemler ile bilginin üretim hızı birlikte değerlendirildiğinde gelecekte karşılaşacağımız problemlerin çok daha ciddi olacağı öngörülmektedir. Bu yüzden özellikle veri güvenliği ve risk analizi üzerine çeşitli çalışmaların yapılması gerekmektedir. Bu çalışmalardan bazıları aşağıda listelenmeye çalışılmıştır.

- Sayısal ortamlarda işlenen, iletilen ve depolanan verilerin güvenliği için çeşitli kriptolojik protokoller kullanılmalıdır.
- Kullanılan kriptolojik protokollerin güvenlik analizleri matematiksel olarak kanıtlanmalıdır.
- Kriptolojik protokollerde gerek duyulan anahtar(lar) sadece veri sahibi ile ilişkilendirilmelidir.
- Şifreler saklanırken özet (hash) fonksiyonları kullanılmalıdır.
- Biyometrik verilerin alınması sürecinde kullanılan donanımların millileştirilmesi önem arz etmektedir. Bu verilerin üçüncü taraflarla paylaşılmadığı garanti edilmelidir.
- Tanı ve test cihazlarında işlenen verilerin güvenliğine ilişkin düzenlemeler getirilmelidir.
- Sağlık sektöründe kullanıcı senaryoları ve sorumlulukları detaylı şekilde tanımlanmalıdır. Bu tanımlamalar çerçevesinde çeşitli kural tabanlı sistemler tasarlanarak güvenlik ihlalleri minimize edilmelidir.
- Risk izleme, ölçme ve yönetme süreçleri ile sürekli olarak öğrenen bir sistem ile dinamik bir model benimsenmelidir.
- Kişisel veri güvenliği konusunda kullanıcılar bilinçlendirilme ve eğitim faaliyetlerine önem verilmelidir.



Şekil 1.1 Önerilen mimarinin genel görünümü

Şekil 1.1' de kırmızı ile gösterilen P1, P2, P3, P4 ve P5 yöntemin ana bölümlerini oluşturmaktadır. Bu bölümler aşağıdaki gibidir.

- P1: Biyometrik özellikleri kullanarak benzersiz değerlerin elde edilmesi
- P2: Benzersiz değerlerin ve kaotik entropi kaynaklarının kullanılarak zenginleştirilmiş yeni bir rasgelelik kaynağının kullanılması
- P3: Anahtar üreteci olarak hibrit bir üretecin oluşturulması
- P4: Web servis uygulama birimi – Uygulama Arayüz Birimi
- P5: Pratik uygulamalar

Tez çalışmasının özgün yönü mobil platformlardaki güvenlik endişelerini kanıtlanabilir güvenlik prensipleri çerçevesinde adresleyebilecek bir kriptolojik anahtar üreteç modülünün ve pratik uygulamalarının geliştirilmesidir. Literatürde kaos temelli rasgele sayı üreteçlerinin varlığı bilinmektedir. Tez çalışmasını bu açıdan benzerlerinden ayıran en önemli yenilik optimizasyon algoritmaları yardımıyla kriptolojik gereksinimler bakımından en uygun entropi kaynağının elde edilecek olmasıdır. İdeal entropi kaynağının oluşturulmasının ardından modern kriptolojinin güçlü yapıtaşları kaos teorisinin kendine has özellikleri ile birleştirilerek tasarlanacak mimarinin kanıtlanabilir güvenlik yaklaşımı ile güvenlik endişelerini adreslemesi sağlanacaktır.

Tez çalışmasının en önemli avantajlarından biri güvenlik konusu ile alakalı yasal düzenlemelerin geç de olsa yürürlüğe girmesi ve gelecek dönemlerde daha etkin şekilde gündemde olacağıdır. Bu kanunlar çıktıların birçok kurum ve kuruluş tarafından zorunlu olarak tercih edileceği için ekonomik/ticari/sosyal çıktı olarak önemli avantajlar sağlayacağı düşünülmektedir. Proje önerisi ile alakalı üç temel yasal düzenleme ve proje hedefleri ile örtüşen unsurları aşağıda tartışılmıştır.

7 Nisan 2016 tarihinde yayımlanarak yürürlüğe giren 6698 sayılı Kişisel Verilerin Koruması Kanunu (KVKK), Anayasa'da öngörülen başta özel hayatın gizliliği olmak üzere temel hak ve özgürlüklerin korunması, kişinin mahremiyet hakkının korunması, kişinin bilgi güvenliği hakkının korunmasını güvenceye almaktadır. KVKK, kişisel verilerin işlenmesinin kontrol altına alınmasını, kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülüklerini ve uyacakları usul ve esasları belirlenmesini sağlamayı hedeflemektedir. Kanun'un öngördüğü uyum süreci 7 Nisan 2018'de sona ermiştir. KVKK, kişisel verileri 'genel kişisel veriler' ve 'özel kişisel veriler' olmak üzere ikiye ayırıyor. Genel kişisel veriler Ad – soyad, TC Kimlik No, Doğum Yeri, Doğum Tarihi gibi klasik anlamda kişisel verilerimizden oluşmakta iken, hassas veriler olarak da nitelenen özel kişisel veriler Kanun'da "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak sayılıyor. 4 yıla kadar hapis, 1 milyon TL'ye kadar para cezası uygulanmasını gerektiğini ifade etmektedir. KVKK kapsamında zorunluluğu bulunan firmaların tez sonucunda üretilecek ekonomik çıktıları kullanabilme olasılığının yüksek olduğu öngörülmektedir.

5070 Sayılı Elektronik İmza Kanunu'nda 14.01.2016 tarihinde yapılan değişiklikle ise e-imza sağlayıcısı kurumlar, kişilerin kimliğini resmi belgelerin yanı sıra Türkiye Cumhuriyeti kimlik kartı vasıtasıyla uzaktan güvenilir bir biçimde tespit edebilecek ibaresi kapsamında kimlik doğrulama süreçlerinde etkin rol oynayabilecek anahtar üreteçlerinin potansiyel bir ekonomik çıktı olarak değerlendirilebileceği düşünülmektedir.

Türkiye'de 1 Temmuz 2020 ve 1 Ocak 2021 olmak üzere iki aşamada yürürlüğe girecek olan yeni BDDK Bilgi Sistemleri ve Elektronik Bankacılık Yönetmeliği uyarınca bankaların yeni nesil güvenlik gereksinimlerini göz önünde bulundurmasını bir zorunluluk haline gelecektir[1]. Özellikle iki seviyeli kimlik doğrulama sürecinde tek kullanımlık anahtarlara gereksinim duyulacak olması proje sonucunda üretilecek anahtar (rasgele sayı) üreteç modülünün önemli bir potansiyel uygulaması olması beklenmektedir. Tez çalışmasının geri kalan kısmı aşağıdaki gibi organize edilmiştir;

İkinci bölümde tezin çatı kavramı olan rastgelelik kavramı ve rastgelelik kavramı için temel koşullardan bahsedilmiş, RSÜ' lerin temel sınıfları tanıtılmış kriptografik bilimi içerisinde RSÜ' lerin önemine değinilmiş, üçüncü bölümde tez çalışması kapsamında incelenen temel GRSÜ donanımının genel özellikleri incelenmiş, dördüncü bölümde önerilen yöntemin detayları tartışılmıştır. Öncelikle üreteçlerden elde edilen verilerin rastgelelik özelliklerinin iyileştirilmesi kapsamında önerilen yeni yaklaşımların yapısı tanıtılmıştır. Ardından buradaki değerler biyometrik değerlerle bütünleştirilerek güvenliğin bir kademe daha arttırılacağı gösterilmiştir. Son olarak bu çözüm önerileri pratik mobil bir uygulamada kullanılarak gerçek dünyada nasıl kullanılabileceği

gösterilmiştir. Son bölümde elde edilen sonuçlar tartışılmış gelecek çalışmalara yönelik motivasyon verilerek tez çalışması özetlenmiştir.

2. RASTGELELİK KAVRAMI VE KOŞULLARI

Rastgele kelimesinin ‘gelişi güzel, seçmeden’ anlamları vardır. Rastgelelik, kısaca öncesi ve sonrasındaki belirsizliğin ve de tekrarın olmadığı durumlardır.

Üretilen rastgele sayılar, istatistiksel örneklemelerde, şans oyunlarında ve simülasyon uygulamalarında sıklıkla kullanılmaktadır. Kriptoloji biliminde rastgelelik, gizlilik ve çözülemezliği sağlamak için kullanılan en temel özelliklerdendir. Bir saldırganın gerçek verilere ulaşmasının engellenmesi için verinin şifreli halinin mümkün olabildiğince tahmin edilmesinin zor olması gerekmektedir.

Bilgisayarların ortaya çıkmasıyla birlikte, bilgisayar programlarına rastgelelik kazandırmanın yolları aranmıştır. Fakat bilgisayarları tamamen rassal yapmak göründüğünden daha zordur. Çünkü bilgisayarlar verilen talimatları sorgulamadan işler bundan dolayı da sonuçlar öngörülebilir hale gelir.

Kriptoloji bilimini temel alan uygulamalarda kullanılmak üzere rastgele sayı üreteçleri bulunmaktadır. RSÜ’ ler, çıkışında ürettikleri sayısal değerler istatistiksel açıdan birbirine bağımlılığı olmayan sistemlerdir. RSÜ’ ler sayısal analiz uygulamaları, bilgisayar benzetimleri, istatistiksel analiz ve özellikle şifreleme gibi alanlarda sıkça kullanılmaktadır.

Bir dizi veya küme elemanlarından bir bölümünün, istatistiksel olarak rastgele seçilmesiyle üretilen sayısal değerlere bilgisayar biliminin pek çok alanında ihtiyaç duyulmaktadır.

Bilgisayarlar gibi deterministik (belirlenirci) bir şeyden gerçekten rassal sayılar üretmesini beklemek mümkün değildir. Bu nedenle bilgisayarlarda tahmin edilmesi zor bir bilgi üretmek oldukça güçtür ve üretilmek istenen rastgele sayıları üretmek için bazı koşullara uymak gerekir. Bu koşullar aşağıdaki şekilde özetlenebilir;

- RSÜ’ nün n tane rastgele sayıyı üretmesi için kendini tekrar etme periyodu oldukça uzun olmalıdır. RSÜ’ ler matematiksel bir fonksiyona bağlı olarak sayı üretimini gerçekleştirirler. Bu sebeple belirli bir periyotta fonksiyonun kendisinin tekrar etmesi söz konusudur. Bu nedenden dolayı üretilen algoritmanın tekrarlanma periyodunun oldukça uzun olması gerekir.
- RSÜ’ de t zamanda oluşturulan n tane sayıdan oluşan dizinin elemanları t_i, t_{i+k} periyotlarında bir kümeleme göstermemelidir.
- RSÜ çalıştırılan bilgisayarın türüne, modeline vs. gibi özeliklerine bağımlı olmamalıdır.
- RSÜ’ nün n tane sayı ürettiği durumda ortaya çıkan dizinin elemanlarının ardışık bir şekilde birbirine bağımlılığının olmaması gerekir.

- RSÜ' ler sistemde bulunan bir X değişkeninin asimptotik dağılışına uyabilen bir esneklik içinde olmalıdır. Üretilmiş olan diziler bir zorluk yaşamadan kullanım amacına uygun hale geçebilmelidir.
- RSÜ' ler ile üretilmiş olan sayı dizilerinde bulunan sayılar bir önceki ve bir sonraki değerlerine bakıldığında bağımsız olmalıdır.

2.1. Kriptolojik Rastgele Sayı Üreteçlerinin Karakteristikleri

Bilgi gizliliğinin sağlanması gereken uygulamalarda kullanılacak rastgele sayıların ihtiyaç duyduğu temel bazı karakteristikler mevcuttur. Bir RSÜ' nün ideal karakteristiği, rastgele sayıların tanımlı bulunduğu aralıkta düzgün dağılım gösteren ve birbirlerinden bağımsız olmalarıdır. Fakat bu matematiksel bir karakteristik olan tasarımdır. Gerçek dünyada kullanılan uygulamalarda bulunan bu sayıların idealliği oldukça zordur. İdeal olarak adlandırılan bu rastgele sayıların üretilmesi mümkün olsa dahi bunu ispatlayabilmek de kritik bir problemdir.

Kriptolojik uygulamalarda rastgele sayı üretmek maksadıyla kullanılan RSÜ' lerin bazı güvenlik ihtiyaçlarını karşılamaları gerekmektedir, Kriptolojik RSÜ' lerin gereksinim karakteristikleri dört madde ile incelenmiştir;

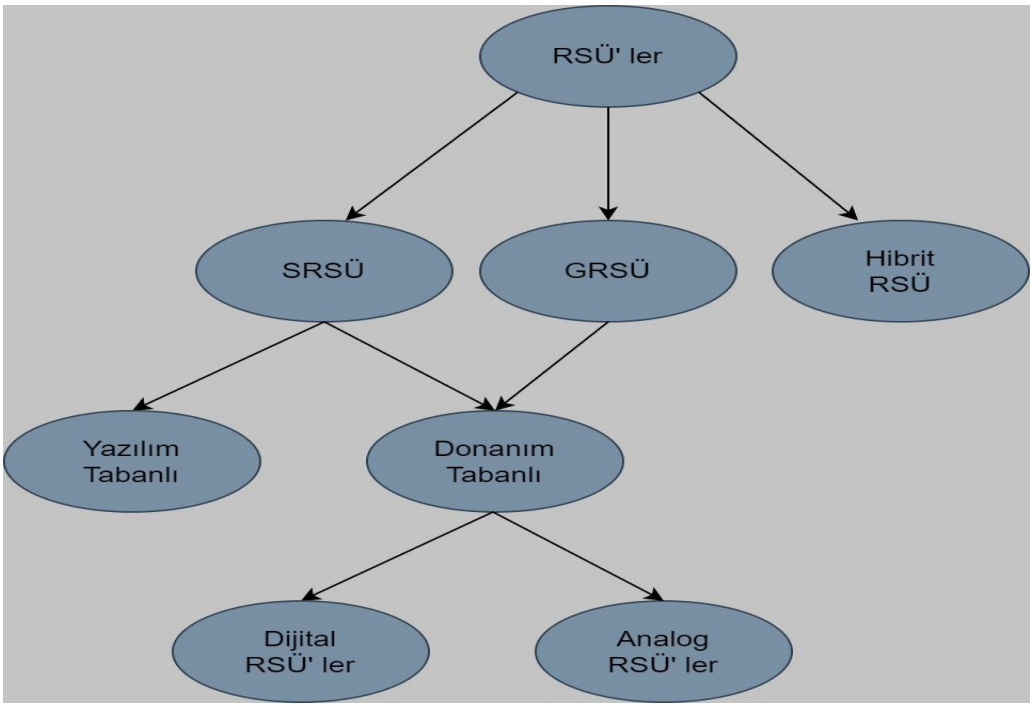
- Rastgele sayılar istatistiksel olarak bir zayıflık göstermemelidir,
- Bu sayıların bir alt dizilerini bilmek önceki ve sonraki rastgele sayıların tahmin edilmesine ve hesaplanmasına izin vermemelidir,
- RSÜ' nin iç durum değerinin bilinmesi veya tahmin edilebilmesi durumunda daha önce üretilmiş olan sayıların hesaplanması mümkün olmamalıdır,
- RSÜ' nin iç durum değerinin bilinmesi halinde ya tahmin edilebilmesi durumunda daha sonraki rastgele sayıların hesaplanması mümkün olmamalıdır.

2.2. Rastgele Sayı Üreteçleri

Birçok kriptografik uygulamanın temelini oluşturan rastgele sayıları üretmek için RSÜ' ler bulunmaktadır. RSÜ' ler, çıkışında üretilmiş olan sayılar istatistiksel açıdan bağımsızlık gösteren sistemlerdir. RSü' ler imza, oturum parametreleri ve anahtarları, geçici anahtarlar, kimlik doğrulama protokolleri, sayısal analiz uygulamaları, istatistiksel analiz ve daha çok şifreleme gibi alanlarda oldukça fazla kullanılmaktadır. RSÜ' ler ile çıkış ve girişlerde üretilen sayıların istatiksel açıdan bağımsızlığı sağlanır. Üretilen değerin bir önceki değerine bakılıp bir sonraki değeri tahmin edilemiyorsa üretecin rastgeleliğinin iyi olduğu sonucuna ulaşılır. Çözülmezliği yani gizliliği sağlayan en önemli unsurların başında rastgelelik gelir. İyi bir şifreleme iyi bir RSÜ gerektirir.

Rastgele sayılar çeşitli kriptografik uygulamalar için bir zorunluluktur. Çünkü kriptografi biliminde başlangıç vektörü oluşturulmasında, anahtar üretimi ve dağıtımında, asal sayı ve şifre

üretiminde ve kimlik doğrulama protokollerinde rastgele sayıların üretilmesine ihtiyaç duyulmaktadır. kriptografik bir sistemin güvenliği üretilmiş bu sayıların gerçek rastgeleliğine bağlıdır. Bu nedenle, RSÜ' ler güvenlik alanlarının bir kısmını oluşturur.



Şekil 2.1 Rastgele sayı üreteçlerinin sınıflandırılması

2.3. Rastgele Sayı Üreteçlerinin Sınıflandırılması

RSÜ tekrar etmeyen bitler üretmeyi sağlayan, tahmin edilmesi zor sayı dizileri üreten bir aygıt ya da sistemdir. RSÜ' ler tarafından üretilmiş diziler aralarında bağlantı bulunmayan ve istatistiksel açıdan bağımsızlık gösteren sayılardan oluşur. RSÜ' ler;

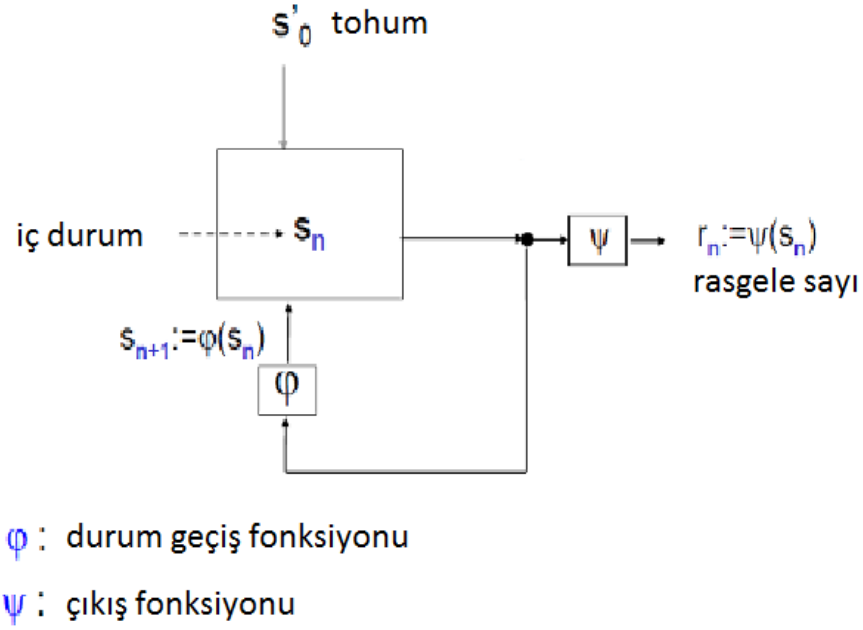
- Gerçek Rastgele Sayı Üreteçleri(GRSÜ)
- Sözde Rastgele Sayı Üreteçleri(SRSÜ)
- Hibrit Rastgele Sayı Üreteçleri

olmak üzere Şekil 2.1' de gösterildiği gibi üç farklı şekilde sınıflandırılmaktadır. Hem GRSÜ hem de SRSÜ ile beraber tasarlanan üreteçler hibrit RSÜ olarak isimlendirilir. SRSÜ' lerin güvenliği muhtemele saldırılara karşı hesaplama karmaşıklığına bağlıyken GRSÜ' lerin güvenliği çıkışlarının tahmin edilemez olmasına bağlıdır. SRSÜ, çoğu uygulamanın ihtiyaçlarını karşılamak için yeterlidir, fakat kriptografik uygulamalarda kullanmak için daha güçlü RSÜ' lere ihtiyaç duyulmaktadır. Rastgele sayıların hepsinin güvenli bir kaynaktan sağlanması için GRSÜ kullanılmalıdır. SRSÜ' leri yazılım ve donanım tabanlı RSÜ' ler olmak üzere bir alt sınıfa

ayrılırken GRSÜ' leri yalnızca donanım tabanlı olacak şekilde üretilebilmektedir. Donanım tabanlı rastgele sayı üretiminde rastgelelik kaynağı olarak fiziksel durumlar kullanılmaktadır. Fiziksel RSÜ' ler elektronik devrelerin gerekirci olmayan etkilerini (diyot ya da direnç elemanından elde edilecek termal görüntü, yarı iletkendeki termal ısı, mikrofondan elde edilen ses ve kameradan elde edilen görüntü gibi) veya fiziksel deneyleri (kuantum, radyo aktif bozulma arasında geçen zaman gibi rastgele süreçler) kullanır. Fiziksel olmayan GRSÜ' ler ise gerekirci olmayan olaylarda (fare hareketleri, kullanıcı giriş değerleri, sistem zamanı, kullanıcı etkileşimleri gibi) ortaya çıkmaktadır.

2.3.1. Sözde Rastgele Sayı Üreteçleri

SRSÜ' ler, sonlu durum makinalarıyla gerçeklenen deterministik bir algoritmayla, sayı üreten sistemlerdir. GRSÜ' lerle kıyaslandığında, düşük maliyetle üretilme ve kolay gerçeklenme gibi artıları vardır. Ancak kullanılan algoritmalar deterministik olduğu için çıkışta üretilen sayılar tam rastgele değildir. Girişte kullanılan algoritma bilindiği takdirde, rastgele bir zamandaki değere bakılarak daha sonra üretilmesi beklenen çıkışlar tahmin edilebilmektedir. Bu durum verinin gizliliğini hedefleyen şifreleme algoritmalarında istenmeyen bir durumdur. GRSÜ' lere kıyasla SRSÜ' leri, istatistiki açıdan başarım oranı daha düşük RSÜ' lerdir. Ayrıca fiziksel süreç modelleme veya sayısal analiz gibi daha düşük seviyedeki istatistiksel rastgeleliğin yeterli olduğu durumlarda tercih edilmektedirler. Buradaki algoritmalarda herhangi bir rastgelelik söz konusu değildir ve algoritmalar çoğunlukla açıktır. Burada elde edilen rastgelelik algoritmaların ilk girdileriyle sağlanır. Bu nedenden dolayı algoritmaların tahmin edilebilme olasılıklarının çok az olmalı ve girdileri gizli tutulmalıdır. Girdi ve algoritmanın bilinmesi halinde, sayı dizisinin tümü elde edilebilir.



Şekil 2.2 SRSÜ' nin tasarım mimarisi

SRSÜ' nin çıkışta verdiği değerlerinin ne kadar rastgele olduğu, yani giriş değerlerinden elde edilen çıkış değerleri ile arasındaki bağımsızlığın değerlendirmesi için yapılan matematiksel işlemlerle net bir sonuca ulaşılamadığından, bu üreteçler için hazırlanmış istatiksel testler uygulanarak sonuca dair bir yorum getirilebilmiştir. Şekil 2.2' de SRSÜ' lerinin tasarım mimarisi detaylı olarak gösterilmiştir.

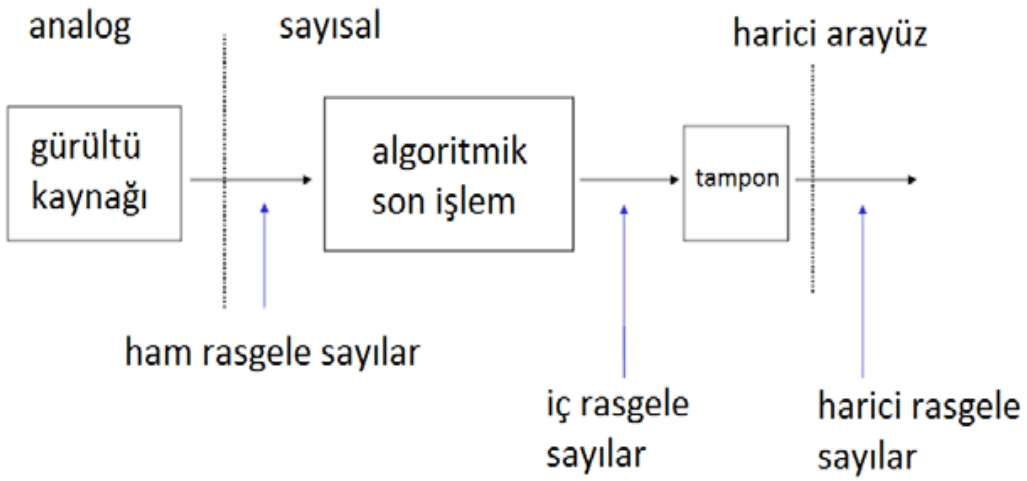
SRSÜ' lerinin eksisi çıkışta üretilen değerlerin tohum değeri vasıtasıyla tamamen belirlenebilmesi ve daha sonra üretilecek rastgele sayıların yalnızca var olan iç duruma bağlı olmasıdır. Bu nedenle cihaz aktif değilken dahi iç durum korunmalıdır SRSÜ' lerinin artısı ise bir donanıma ihtiyaç olmadığından dolayı daha ucuz olmalarıdır. Fakat SRSÜ' leri aracılığıyla üretilen rastgele sayıların kullanılmış olunan fonksiyonlar yeterli düzeyde karmaşık olmadığı durumlarda veya tohum değerinin tahmin edildiği durumlarda tahmin edildiği görülmüştür. Ek olarak belirli bir zamandan sonra üretilen sayı dizisi kendisini tekrar etmeye (periyodiklik) başlamıştır. Belirtilen bu dezavantajlar sebebiyle SRSÜ' leri kriptografik uygulamalarda kullanılmak için uygun değildir.

2.3.2. Gerçek Rastgele Sayı Üreteçleri

Bilgisayar programı kullanmayarak, fiziksel bir işleyiş Şekil 2.3' te gösterilen mimariyi temel alarak rassal sayı üreten üreteçlerdir. Bu cihazlar genel olarak ısıl gürültü, istatistiksel olarak rassal gürültü sinyalleri içeren fiziksel olayları kullanır. Bu üreteçlerin en önemli avantajları:

- Dizinin bir kısmı biliniyorken kalan kısımlarının bilinmiyor olması;
- Üretilen dizilerin kendi içinde bir bağıntının olmaması;

- Periyodik olmamalarıdır.



Şekil 2.3 GRSÜ' nin genel tasarım mimarisi

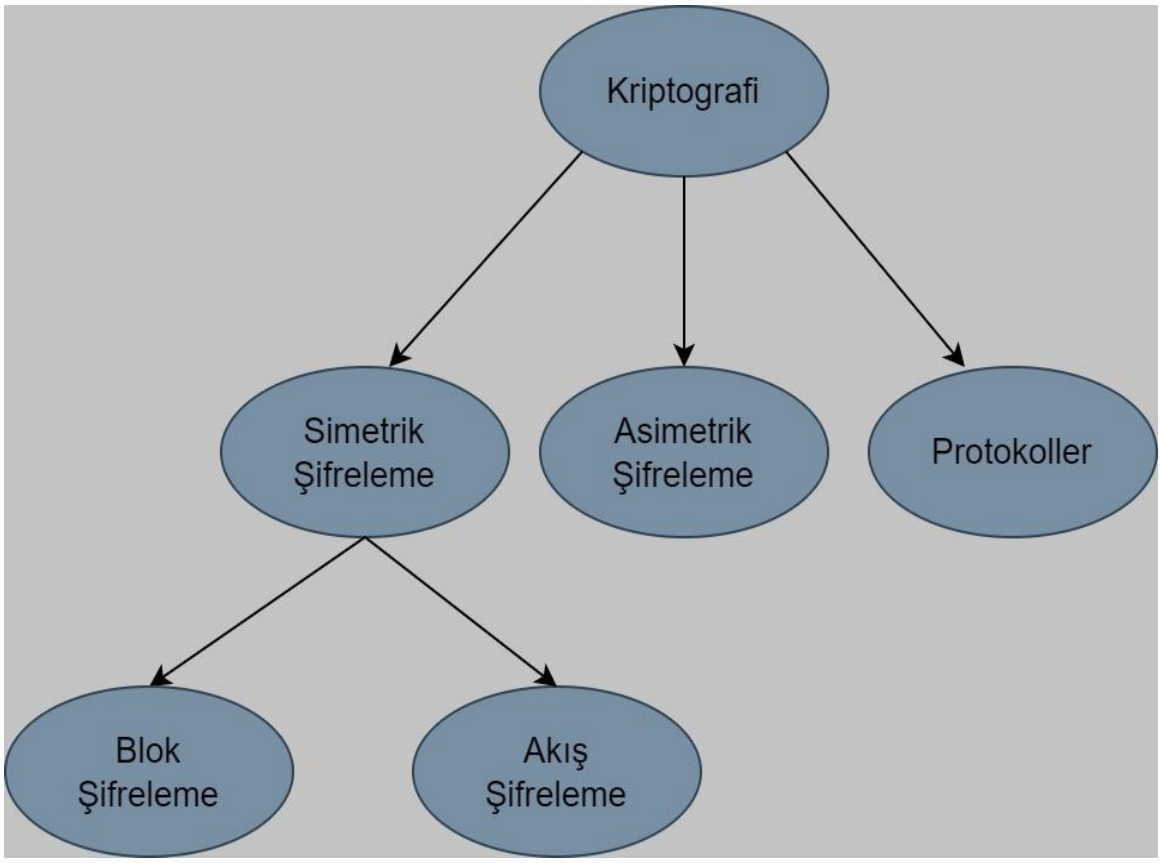
Bu artılarına ek olarak, GRSÜ' lerinin önemli eksileri da bulunur. Bu üreteçler genellikle verimsizdir, belirli uzunlukta rastgele sayı dizilerini üretmenin maliyeti yüksektir. Elde edilmiş bir sayı dizisini deneyi tekrarlayarak bir kez daha oluşturmak mümkün değildir. Farklı iki teknikle yazılım tabanlı ve donanım tabanlı olmak üzere gerçekleştirirler. Donanım kaynaklı üreteçler, bir direncin veya yarı iletken bir diyotun ısıl gürültüsü, radyoaktif bir bozulma sırasında parçacıkların yayılmaları arasında geçen zaman, bir ossilatörün faz gürültüsü gibi fiziksel olayların rastgeleliğini kullanır. Bu süreçlerin sonucunda elde edilen işaretler de birbiri ile bağlantılı olabileceği için tam rastgeleliği sağlamak amacıyla çıkış değeri tekrar bir algoritmayla düzenlenebilir. Yazılım tabanlı üreteçler, fare hareketleri arasındaki zaman, sistemin zamanı gibi bilgisayar kaynaklı olayları temel alır. Donanım tabanlı üreteçleri gerçeklemek yazılım tabanlı üreteçleri gerçeklemekten daha az zahmetli ve daha çok güvenilirdir.

GRSÜ' lerin temelini entropi kaynağı oluşturmaktadır. Entropi kaynağı fiziksel deneyler (radyoaktif bozulma veya ışığın kuantum etkisi) ya da elektronik devreler (gürültülü diyot veya serbest çalışan ossilatör) ile gerçekleştirilir. Entropi kaynağı sürekli zamanlı analog sinyaller üretirken aynı zamanda da bu değerler periyodik olarak sayısallaştırılarak ikili (binary) değerlere dönüştürülmektedir. Bu sayısal değerler, sayısallaştırılmış analog sinyaller olarak isimlendirilirler. GRSÜ' lerin potansiyel zayıflıklarını azaltmak amacıyla elde edilen sayısal değerlere bazı algoritmik son işlem metotları uygulanabilir.

Rassal sayı üretmede kullanılan bilgisayar programlarından olan SRSÜ' lerine kıyasla daha güvenilir bir alternatif oluştururlar. Kriptografik uygulamalar için şart olan tekrar üretilememe, tahmin edilememe ve iyi istatistiksel nitelikler sağlaması nedeniyle kriptolojinin birçok alanında kullanılmıştır.

2.4. Kriptografi Biliminin Sınıflandırılması

Birçok bilimsel çalışmada önemli bir gereklilik olan rastgelelik, kriptoloji çalışmalarında da ayrıcalıklı bir role sahiptir [1]. Şekil 2.4' de gösterildiği gibi, kriptoloji bilimi birkaç alt disipline ayrılmıştır. Rastgelelik bu alt disiplinlerin her biri için önemli bir gereklilik olmasına rağmen, akla gelen en yaygın uygulama alanlarından biri akış şifreleme sistemleri olarak bilinir.

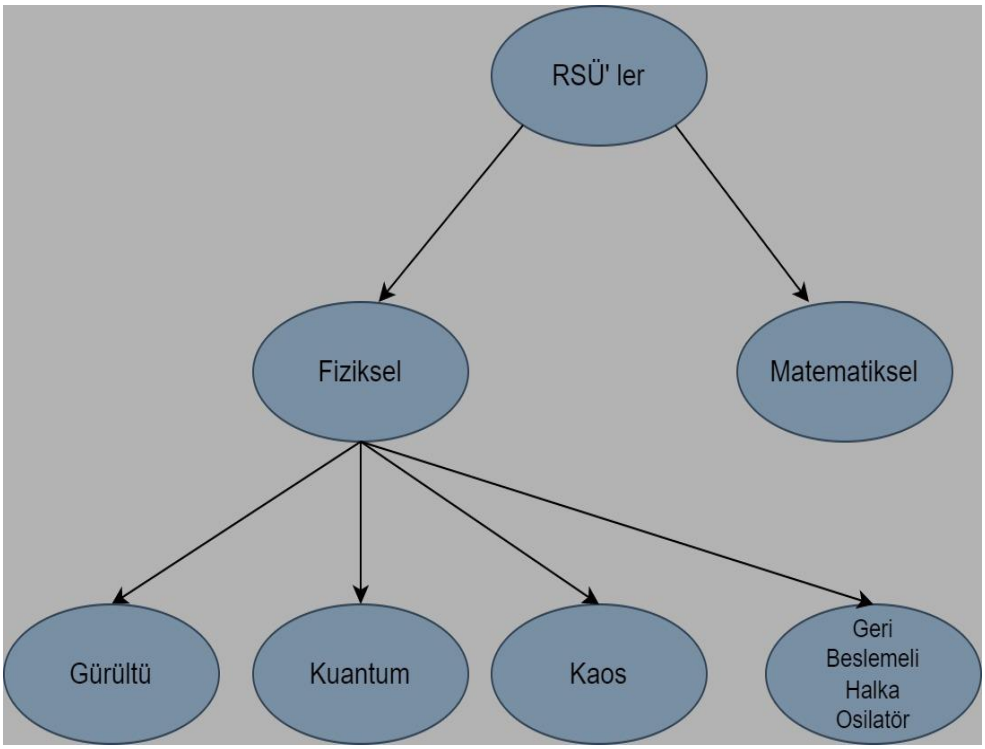


Şekil 2.4 Kriptografi biliminin hiyerarşisi

Akış şifrelerinin tasarımına ek olarak, oturum anahtarlarının, başlangıç vektörlerinin oluşturulmasında ve siber fiziksel sistemlerde kullanılan maskelerin tasarımında rasgelelik gereksinimi ele alınmalıdır [2]. Ancak kriptografik uygulamalar için rastgelelik gereksinimini sağlamak kolay bir süreç değildir [3, 4]. Çünkü kriptografik rastgeleliğin farklı açılardan değerlendirilmesi gerekiyor. Bunlara istatistiksel rastgelelik ve öngörülemezlik denir [5, 6].

Aslında bu bakış açıları kapsamında rasgele sayı üreteçlerinin sıralandığı iki temel kategoride konumlanmıştır. Deterministik rasgele sayı üreteçleri (DRNG) olarak adlandırılan yapılar istatistiksel rasgeleliği en uygun şekilde karşılarken, gerekli yapıları nedeniyle öngörülemeyen gereksinimin karşılanmasında sorun teşkil etmektedir. Aksine, gerçek rasgele sayı üreteçleri (GRSÜ) doğal kaynaklara dayalı oldukları için oldukça tahmin edilemez, ancak bu

tasarımlarda istatistiksel gereksinimleri karşılamakta yetersiz kalıyorlar. Şekil 2.5' te rasgele sayı üreteçlerinin (RNG) sınıflandırmasının genel görünümü verilmektedir [3].



Şekil 2.5 RSÜ için bir sınıflandırma

3. KRİPTOGRAFİK MODÜLLER İÇİN GÜVENLİK GEREKSİNİMLERİ

3.1. FIPS 140 Standardı

Çağlar boyunca bilgi güvenliği insanlar ve toplumlar arasında daima önemli bir yer almış, sadece yetkilendirilmiş kişilerin bilmesi gereken sırlar çeşitli yöntemlerle korunmaya çalışılmıştır. Teknoloji öncesi kullanılan her sistem kendi içinde sorgulanırken teknolojinin gelişmesi ve yaygınlaşması ile bilgi teknolojilerinde kullanılan bileşenlerin güvenilirliği de bu ürünlerin kullanılmasıyla birlikte tartışılmaya başlamıştır. Günümüzde devletler, kurumlar ve insanlar kritik altyapı ve sistemlerde kullanılan bilgiyi korumak için kriptografiye güvenmektedir. Bu ürün ve sistemlerde, gizlilik, bütünlük, inkâr edememe ve kimlik doğrulama gibi kriptografik hizmetleri sağlamak için kriptografik modüller kullanılmaktadır. Devletler, kurumlar ve insanlar, test edilmiş ve onaylanmış ürünleri kullanmak ister ve bundan fayda sağlarlar. Yeterli test yapılmayan, zayıf tasarım ve algoritma içeren veya kriptografik modülün yanlış uygulanmasından doğan sonuçlar güvensiz ürünlerin ortaya çıkmasına yol açar. Bilgi teknolojilerinde kullanılan bileşenlerin güvenilirliğini sağlamak, gereksinimlerini belirlemek, onaylanmasını ve doğrulanmasını sağlamak vb. gibi işlemleri yapmak ve bunu uluslararası bir düzeyde geçerli kılmak için bazı standartlar ortaya çıkmıştır. İşte bunlardan biri olan FIPS (Federal Information Processing Standard) 140 standardı (Şifreleme Modülleri için Güvenlik Gereksinimleri), kriptografik modüllerin tasarlanmasında, uygulanmasında ve çalıştırılmasında kullanılmasının yanı sıra modüllerin test edilmesi ve doğrulanması için de yöntemler tanımlamaktadır. Kriptografik modül, şifreleme, şifre çözme, dijital imzalar, kimlik doğrulama teknikleri ve rasgele sayı üretimi gibi kriptografik işlevleri uygulayan donanım ve veya yazılım olarak tanımlanır. Bu modüller yaptıkları işi eksiksiz ve aksatmadan yapmalıdır. NIST (Ulusal Standartlar ve Teknoloji Enstitüsü) tarafından yayınlanan FIPS 140 Standart serisi, ABD devlet daireleri ve kurumları tarafından kullanılmak üzere hem donanım hem de yazılım bileşenlerini içeren kriptografik modüller için gereksinimleri belirlemek ve standartları koordine etmek amacını taşımaktadır. Standart herkese açıktır ve isteyen uygulayabilir.

3.2. FIPS 140 Standartlar Serisi

Serinin ilk yayını olan FIPS 140-1 11 Ocak 1994 tarihinde yayınlanmıştır. 25 Mayıs 2002'de sona eren bir geçiş döneminin ardından yerini FIPS 140-2'ye bırakmıştır. Kullanımda olan sürümler FIPS 140-2 ve FIPS 140-3'tür.

Standart kullanıcılardan ve satıcılardan oluşan bir hükümet ve endüstri çalışma grubu tarafından geliştirilmiştir. Çalışma grubu, geniş bir uygulama (örneğin, düşük değerli idari veriler,

yüksek değerli fon transferleri vb.) ve ortam yelpazesi (örneğin, korumalı bir tesis, bir ofis veya tamamen korumasız bir konum) sağlamak amacıyla kriptografik modül gereksinimleri için dört güvenlik seviyesi belirlemiştir. Her güvenlik seviyesi, önceki seviyeye göre güvenlikte bir artış sunmaktadır. Bu dört artan güvenlik seviyesi, farklı veri hassasiyeti dereceleri ve farklı uygulama ortamları için uygun olan uygun maliyetli çözümlere izin vermektedir.

Yukarıda da belirtildiği gibi bilgi sistemlerinde kullanılan kriptografik modüller sağladığı hizmete göre (anahtar yönetimi, e-imza, şifreleme vb.) farklı güvenlik gereksinimlerine ihtiyaç duyabilir. Gereksinimler, yalnızca kriptografik modüllerin kendisini değil, aynı zamanda belgelerini ve kaynak kodda bulunan yorumların bazı alanlarını da kapsar. Bu alanlar arasında temel tasarım ve belgelendirme, modül arayüzleri, yetkili roller ve hizmetler, fiziksel güvenlik, yazılım güvenliği, işletim sistemi güvenliği, anahtar yönetimi, kriptografik algoritmalar, elektromanyetik girişim / elektromanyetik uyumluluk (EMI / EMC) ve kendi kendine testler yer alır. FIPS 140 Standardı, kendi gereksinimlerine uyan bir modülün güvenli olduğunu garanti etmez.

FIPS 140-1, NIST'in en başarılı standartlarından birisidir ve Kriptografik Modül Doğrulama Programının (CMVP) temelini oluşturur. FIPS 140-1, kriptografik modüller için standart olarak yaygın bir şekilde tanınmış ve çok sayıda standart kuruluşu ve uluslararası test kuruluşu tarafından referans alınmış ve /veya bütünüyle kullanılmıştır[7].

İhtiyaçlar doğrultusunda standardın geliştirmesi gerektiğinden akıllara şu soru gelmiştir. "Başarılı ve kanıtlanmış bir standart nasıl geliştirilir?" İşte FIPS 140-2, sorulardan ve yorumlardan çıkarılan dersler ele alınarak ve teknolojideki değişiklikler de eklenerek yazılmıştır. 140-1'in içeriği minimum düzeyde yeniden yapılandırılmış, gereksiz bilgileri kaldırmış, açıklık ve tutarlılık sağlamak için kullanılan dil ve terminoloji standartlaştırılmış ve standardın formatı iyileştirilmiştir. Ayrıca şu anda özel testleri bulunmayan kriptografik modüllere yönelik yeni saldırı türlerini detaylandıran yeni bir bölüm eklenmiştir. Böylece standart daha da güçlendirilmiş, ancak odak veya vurgu değişmemiştir.

FIPS 140-3 bir kriptoprafik modülün tasarım aşamasından başlayarak uygulama ve son dağıtıma kadar uzanan güvenlik gereksinimlerini tanımladığı için daha geniş bir tehdit ve güvenlik açığı yelpazesini kapsar. FIPS 140-3, daha önce var olan iki uluslararası standart olan ISO / IEC 19790: 2012 "Şifreleme Modülleri için Güvenlik Gereksinimleri" ve ISO 24759: 2017 "Kriptografik Modüller için Test Gereksinimleri" ni temel alır.

Üreticiler şu anda bir şifreleme modülünü FIPS 140-2 veya FIPS 140-3'e göre doğrulayabilirler. İki sürüm eşdeğerdir ve FIPS 140-2'yi seçmenin herhangi bir sakıncası yoktur.

FIPS 140-1 yayından kaldırıldığı için güvenlik Seviyeleri FIPS 140-2 standardına göre incelenmiştir.

3.3. FIPS 140 Güvenlik Seviyeleri

3.3.1. Seviye 1

Bu seviye bir kriptografik modül için belirlenen en düşük düzeydeki temel güvenlik gereksinimlerini belirtir. Seviye 1, üretim sınıfındaki bileşenler için temel gereksinimlerin ötesinde hiçbir fiziksel güvenlik mekanizması gerektirmez ve bir kriptografik modülün değerlendirilmemiş bir işletim sistemi kullanılarak genel amaçlı bir bilgisayarda yürütülmesine izin verir. Güvenlik Düzeyi 1 şifreleme modülüne bir örnek, kişisel bir bilgisayardaki (PC) bir şifreleme kartıdır. Seviye 1'de yer alan bazı önemli noktalar.

- Kriptografik modül, onaylı çalışma modunda en az bir adet onaylı güvenlik işlevi uygulamalıdır. Onaylanmamış güvenlik işlevleri onaylı olmayan çalışma modlarına dahil edilebilir. Operatör, onaylı çalışma modunun ne zaman seçileceğini belirleyebilmelidir.
- Bir kriptografik modül, tüm bilgi akışını (şifreleme anahtarları ve bileşenlerinin, kimlik doğrulama verilerinin modüle giden ve modüle gelen tüm giriş ve çıkış noktaları) fiziksel bağlantı noktaları ve mantıksal arabirimlerle (örneğin, aynı port üzerinden giriş verileri girebilir ve çıkış verileri çıkabilir) sınırlandırmalıdır. Fiziksel bağlantı noktaları ve mantıksal arabirimler, kriptografik modüldeki diğer bağlantı noktaları ve arabirimlerle fiziksel ve mantıksal olarak paylaşılabilir.
- Kriptografik modül, operatörler için aşağıdaki yetkili rolleri desteklemelidir: Kullanıcı rolü, Kripto Görevlisinin Rolü, Bakım Rolü. Kriptografik modül tarafından desteklenen tüm yetkili roller dokümantasyonda yer almalıdır.
- Kriptografik modül, operatörlere şu hizmetleri sağlamalıdır: Şifreleme modülünün mevcut durumu gösterilmeli, kendi kendine testler yapabilmeli ve en az bir onaylı güvenlik işlevi gerçekleştirmeli. Hizmetler, kriptografik modül tarafından gerçekleştirilebilecek tüm işlemlere veya işlevlere atıfta bulunmalı, her hizmet girdisi bir hizmet çıktısı ile sonuçlanmalıdır.
- Modüle erişimi denetlemek için kimlik doğrulama mekanizmalarının kullanıldığı bir şifreleme modülü gerekmez. Kimlik doğrulama mekanizmaları şifreleme modülü tarafından desteklenmiyorsa, modül bir veya daha fazla rolün operatör tarafından örtük veya açıkça seçilmesini gerektirir.
- Şifreleme modülünün çalışması, durum geçiş diyagramı ve/veya durum geçiş tablosu tarafından temsil edilen sonlu bir durum modeli (veya eşdeğeri) kullanılarak belirtilmelidir.
- Bir kriptografik modülün işletim ortamı, modülün çalışması için gerekli olan yazılım ve / veya donanım bileşenlerinin yönetimini ifade eder. İşletim ortamı değiştirilemez (ROM) veya değiştirilebilir (RAM) olabilir. Güvenlik Düzeyi 1'de işletim sistemi tek bir operatör çalışma modu ile sınırlandırılmıştır. Kriptografik modül, şifreleme modülünün çalıştığı

süre boyunca diğer işlemlerin düz metin özel ve gizli anahtarlara, ara anahtar oluşturma değerlerine vb. erişimini engellemelidir. Kriptografik modül tarafından oluşturulan işlemler modüle aittir ve yürütme sırasında kriptografik olmayan işlemler tarafından kesintiye uğramamalıdır. Tüm kriptografik yazılımlar, yürütülebilir kodu yetkisiz ifşa ve değişikliklere karşı koruyan bir biçimde kurulmalıdır. Onaylanmış bütünlük tekniğini kullanan bir kriptografik mekanizma (örneğin, onaylanmış mesaj kimlik doğrulama kodu veya dijital imza algoritması), kriptografik modül içindeki tüm kriptografik yazılım ve ürün yazılımı bileşenlerine uygulanmalıdır.

- Anahtar yönetimi, rastgele sayı ve anahtar oluşturma, anahtar dağıtımı, anahtar giriş / çıkış işlemleri, anahtar depolama ve anahtar sıfırlamayı da içeren bir yaşam döngüsü içinde yapılır. Gizli anahtarlar, özel anahtarlar ve kritik güvenlik parametreleri, yetkisiz ifşa, değişiklik ve değiştirmeye karşı şifreleme modülü içinde açık anahtarlar ise kriptografik modül içinde korunmalıdır. Gerektiğinde kriptografik modül başka bir kriptografik modülün anahtar yönetim mekanizmalarını da kullanabilir. Algoritmada kullanılan sayılar gerekli testlerden geçmiş rastgele sayı üretme fonksiyonları ile sağlanmalıdır. Bu fonksiyonlarda kullanılan geri besleme değeri vb. değerlere de yetkisiz erişim engellenmelidir ve gizli kalmalıdır. Güvenlik Seviyesi 1 ve 2 için, otomatikleştirilmiş yöntemler kullanılarak oluşturulan gizli ve özel anahtarlar, kriptografik modüle şifrelenmiş biçimde girmeli ve çıkmalıdır. Manuel yöntemler kullanılarak oluşturulan gizli ve özel anahtarlar, şifreleme modülüne düz metin biçiminde girilebilir veya buradan çıkarılabilir.

3.3.2. Seviye 2

Seviye 1'e ilave üç ana gereksinim eklenmiştir.

- Kriptografik modüle yapılacak bir fiziksel müdahaleyi tespit edebilmek için fiziksel kilit (koruma kaplaması, conta vb.) veya kurcalama karşıtı mühürler kullanılmalıdır.
- Şifreleme modülü modüle erişimi denetlemek için rol tabanlı kimlik doğrulaması kullanacaktır.
- Kriptografik modülün onaylanmış veya değerlendirilmiş güvenilir bir işletim sisteminden yararlanan genel amaçlı bir bilgisayarda yürütülmesine izin verir. İşletim sistemleri Ortak Kriterler (CC) değerlendirme güvence seviyesi EAL2 veya daha yüksek bir seviyede değerlendirilmelidir.

3.3.3. Seviye 3

Seviye 2' ye ilave dört ana gereksinim eklenmiştir.

- Saldırganın kriptografik modül içindeki kritik güvenlik parametrelerine erişimini önlemek için fiziksel güvenlik sağlanmalıdır. Kurulacak mekanizmanın amacı kriptografik modüle fiziksel olarak yetkisiz erişim, kurcalama veya kullanma girişimlerini tespit etme ve bunlara tepki verme olasılığını yükseltmektir. Herhangi bir kurcalama tespit edilirse, cihaz kritik güvenlik parametrelerini silebilmelidir.
- Şifreleme modülü modüle erişimi denetlemek için rol tabanlı kimlik doğrulamadan daha ayrıntılı bir kimlik doğrulama yöntemi olan kimlik tabanlı kimlik doğrulama mekanizması kullanmalıdır. Bu, belirli bir kullanıcının rolünü doğrulamak yerine belirli bir kullanıcının kimliğini doğrulayarak elde edilir.
- Düz metin şifreleme anahtarı bileşenlerinin, kimlik doğrulama verilerinin ve kritik güvenlik parametrelerin girişi ve çıkışı için kullanılan bağlantı noktaları fiziksel veya mantıksal olarak (örneğin, güvenilir bir yol veya doğrudan bağlanan kablo aracılığıyla) ayrılmalıdır.
- İşletim sistemi gereksinimleri Seviye 2'den daha katıdır ve bir CC değerlendirme güvence düzeyi EAL3 veya daha üstünü içerir. Güvenlik Düzeyi 3 işletim sistemi gereksinimleri hakkında daha fazla bilgi FIPS 140-2 yayınında Bölüm 1.3'te bulunabilir.

3.3.4. Seviye 4

Bu seviye diğer güvenlik düzeylerinden daha yüksek düzeyde güvenlik sağlar ve fiziksel olarak korumasız ortamlarda çalışan kriptografik modüller için idealdir. Fiziksel olarak korunmasız ortamlara örnek olarak uydular ve insansız hava araçları verilebilir. Güvenlik Düzeyi 4'ün amacı, şifreleme modülünü tüm yetkisiz fiziksel erişim girişimlerine karşı korumasını sağlamaktır. Mekanizmalar, bir saldırı tespitinde çok yüksek bir olasılık sağlamalı ve bir saldırı tespit edilmesi durumunda tüm düz metin kritik güvenlik parametrelerini derhal sıfırlayacak şekilde tasarlanmalıdır.

Elektronik cihazlar ve devreler, belirli bir çevre koşulları aralığında çalışmak üzere tasarlanmıştır. Belirtilen normal çalışma voltaj ve sıcaklık aralıkları dışındaki kasıtlı veya kazara gezintiler, şifreleme modülünün güvenliğini tehlikeye atabilecek elektronik cihazların veya devrelerin hatalı çalışmasına veya arızalanmasına neden olabilir. Bir kriptografik modülün güvenliğinin aşırı çevresel koşullar tarafından tehlikeye atılamayacağına dair makul güvence, modülün çevresel arıza koruma (EFP) özelliklerini kullanması veya çevresel hata testine (EFT) tabi tutulmasıyla sağlanabilir. Güvenlik Düzeyi 4'te, bir kriptografik modül ya çevresel arıza koruma (EFP) özelliklerini kullanacak ya da çevresel hata testine (EFT) tabi tutulacaktır.

Saldırganlar modülün güvenliğini tehlikeye atmak için şifreleme modülünü normal voltaj ve sıcaklığının dışına itme yöntemini (aşırı ısıtma veya soğutma) yaygın olarak kullanmaktadır.

Kriptografik modül normal çalışma aralığı dışındaki dalgalanmaları tespit ederse, çevre koruma önlemleri kritik güvenlik parametrelerini sıfırlayabilir. Örneğin saldırgan sıvı nitrojen kullanarak kriptografik modüldeki kilidi dondurmak ve kırmak için müdahalede bulunduğunda çevre koruma önlemleri kilidin belirlenen bir eşiğin altındaki sıcaklığa maruz kaldığını tespit eder ve modülü sıfırlar. Bu noktadan sonra saldırgan modüle erişse bile işine yaramaz.

İşletim sistemi gereksinimi daha üst bir seviyeye taşınmıştır. Bir şifreleme modülünün FIPS 140-2 Seviye 4 uyumlu olması için, üzerinde çalıştığı işletim sisteminin EAL4 veya daha yüksek bir CC değerlendirmesi alması gerekir.

3.4. Rastgele Sayı Üreteçleri İçin İstatistiksel Testler

Bu bölümde modelleme, simülasyon ve kriptografik uygulamalarını içeren amaçlar için kullanılabilen GRSÜ ve SRSÜ' lerine uygulanan rastgelelilik testleri incelenecektir. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), bahsedilen işlemlerin, ikili bir dizinin rastgeleliğinde bir sapmanın var olup olmadığının tespit edilmesi için faydalı olduğuna inanmaktadır.

Hipotez tabanlı NIST Test Suite, donanım veya yazılım tabanlı kriptografik rastgele veya sahte rastgele sayı üreteçleri tarafından üretilen (keyfi uzun) ikili dizilerin rastgeleliğini test etmek için geliştirilmiş 15 testten oluşan istatistiksel bir pakettir. Bu testler, bir dizide var olabilecek çeşitli farklı rastgele olmayan türlere odaklanır. Bazı testler çeşitli alt testlere ayrılabilir. 15 test şunlardır:

1. Frekans (monobit) testi
2. Bir blok içinde frekans testi
3. Akış (Runs) testi
4. Bir blok içinde en-uzun-birlerin akış (longest-run-of-ones) testi
5. İkili matris rankı testi
6. Ayrık Fourier dönüşümü (spektral) testi
7. Örtüşmeyen şablon eşleştirme (Non-overlapping template matching) testi
8. Örtüşen şablon eşleştirme (Overlapping template matching) testi
9. Maurer'in "Evrensel İstatistik" testi
10. Doğrusal karmaşıklık (linear complexity) testi
11. Seri (serial) test
12. Yaklaşık entropi (approximate entropy) testi
13. Kümülatif toplamlar (cumulative sums – cusums) testi
14. Rastgele gezinimler (random excursions) testi
15. Rastgele gezinimler değişken (random excursions variant) testi

Burada bulunan 15 adet testin uygulanma sırasının bir önemi yoktur ve isteğe bağlıdır. Fakat ilk uygulanacak testin frekans testi olması tavsiye edilmektedir. Uygulanan frekans testi başarılı sonuçlanmazsa kalan 14 testin de başarısız olma ihtimali fazladır. NIST test paketindeki bazı testler, ki-kare (X^2) ve standart normal dağılımlarını referans dağılımı olarak kullanır[9].

3.4.1. Frekans(Monobit) Testi

Frekans testinin amacı, GRSÜ' de olması ön görülen özellik olarak dizideki "0" ve "1" sayılarının aynı olup olmadığının yaklaşık olarak ölçülmesidir. Burada kullanılan referans dağılım yarı normal dağılımdır ve bu testte parametre yoktur. Test edilen dizinin uzunluğu minimum 100 bit olmalıdır. Testteki denklemler kullanılarak elde edilen değer p > 0.01 ise elde edilen bu dizinin rastgeleliği kabul edilir.

n: Bit dizisinin boyutu

ε: RNG veya PRNG ile üretilen bit dizisi

***Sn*:** Bit dizisinin toplam değeri (Bit dizisindeki 0'lar (-1), 1'ler ise kendi değeri kabul edilerek toplama işlemi yapılarak elde edilmiş sonuçtur).

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \tag{1}$$

erfc: hata fonksiyonu

$$erfc(z) = \frac{2}{\sqrt{n}} \int_2^{\infty} e^{u^2}\, du \tag{2}$$

P-değeri= $\boldsymbol{erfc\left(\frac{S_{obs}}{\sqrt{2}}\right)}$ (3)

$$S_n = X_1 + X_2 + \cdots + X_n \qquad X_i = 2\varepsilon_i - 1 \tag{4}$$

Örnek: ε=1011010101

$\varepsilon = \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{10}$ $\qquad x_1 = 2\varepsilon_1 - 1 = 2 * 1 - 1 = 1$

$n = 10$ $\qquad x_2 = 2\varepsilon_2 - 1 = 2 * 0 - 1 = -1$

$S_n = 1 + (-1) + 1 + 1 + (-1) + 1 + (-1) + 1 + (-1) + 1 = 2$

$$P - değeri = erfc\left(\frac{S_{obs}}{\sqrt{2}}\right) = 0.527089 \qquad S_{obs} = \frac{2}{\sqrt{10}} = 0.6324$$

elde edilen p değeri 0.01 den büyük olduğu için dizinin rastgele olduğu sonucuna ulaşılır.

3.4.2. Blok Frekans Testi

Bu test sayı dizisinde var olan 1 ve 0' ların oranını *m* bit uzunluklu bloklar içerisinde kontrol eder. Bu testin bir parametresi vardır o da var olan blok uzunluğudur. Buradaki blok uzunluğunun 1 bit olması durumunda frekans testine dönüşür. Her bir bloktaki 1'lerin beklenen oranı m/2 dir. Kullanılan referans dağılımı ki-kare dağılımıdır. Dizinin test sonucunun başarılı olması için uzunluğunun minimum 100 bit, blok uzunluğu da 20 bit olmalıdır.

n: dizi uzunluğu

m: blok uzunluğu

$X^2_{(obs)}$: Beklenen oran (1/2) ile karşılaştırılan verilmiş m bit blok içerisindeki 1'lerin gözlemlenen oranının nasıl olduğunun ölçüsüdür.

ε: RSÜ veya SRSÜ tarafından üretilen bit dizisi

- $N = \frac{n}{m}$ örtüşmeyen bloklar şeklinde girilen dizi bölünür. Kullanılmayan bitler atılır.

ε=0110011010 n=10 m=3 $N = \frac{10}{3} = 3$

011, 001 ve 101 bloklarından oluşur.

- $\pi_i = \frac{\sum_{j=1}^{m} \varepsilon_{(i-1)m+1}}{m}$ denklemi kullanılarak her bir m bit bloktaki 1' lerin oranı π_i' ye karar verilir.

$$1 \le i \le N \qquad \pi_1 = \frac{2}{3}, \pi_2 = \frac{1}{3}, \pi_3 = \frac{2}{3}$$

- X^2 istatistiği hesaplanır.

$$X^2_{(obs)} = 4m \sum_{i=1}^{N} \left(\pi_i - \frac{1}{2}\right)^2$$

$$X^2_{(obs)} = 4 * 3 * \left(\left(\frac{2}{3} - \frac{1}{2}\right)^2 + \left(\frac{1}{3} - \frac{1}{2}\right)^2 + \left(\frac{2}{3} - \frac{1}{2}\right)^2\right) = 1$$

- P-değeri hesaplanır.

$$P - değeri = igamc\left(\frac{N}{2}, \frac{X^2_{(obs)}}{2}\right) \quad (5)$$

$P - değeri = igamc\left(\frac{3}{2}, \frac{1}{2}\right) = 0.801252 \geq 0.01$ olduğundan dizi rastgeledir.

3.4.3. Akış Testi

Akış testi aynı (özdeş), sürekli (devamlı) bit dizisi olarak tanımlanan akışların toplam sayısı ile ilgilidir. Akış elde edilen dizideki art arda gelen aynı bit sıralamasını ifade eder. Bu şekilde 1' ler ve 0' lar arasındaki dalgalanmaların kontrolünü yapıp üretilen bit dizisinin hızlı veya yavaş olacağını söyler. Akış testi için referans dağılımı olarak X^2 dağılımı kullanılmıştır. Testin adımları aşağıdaki gibidir;

n: Bit dizisinin boyutu

ε: RNG veya PRNG ile üretilen bit dizisi

V_n(obs)= Tüm n bitlerin arasında toplam tekrar sayısı (yani, var olan 0' ların toplam tekrarı + var olan 1' lerin toplam tekrarı(Akışların toplam sayısı))

- $\pi = \frac{\sum j\varepsilon_j}{n}$ dizide bulunan 1' lerin sayısını hesaplamak amacıyla kullanılır.

Örneğin : ε= 0001101001 $\pi = \frac{4}{10} = \frac{2}{5}$ ve n=10

- Birinci şart olarak dizi frekans testini geçtiyse karar verme aşamasına gidilir ve $\left|\pi - \frac{1}{2}\right| \geq \tau$ gösterilir. Bu durum gerçekleşmezse akış testi uygulanmayabilir. Test uygulanmazsa p değeri 0.000 olur. Bu test için $\tau = \frac{2}{\sqrt{n}}$ test kodu daha önceden tanımlanmıştır. Buradaki örnek için $\tau = \frac{2}{\sqrt{10}} = 0.63246$ olduğu için $\left|\pi - \frac{1}{2}\right| = \left|\frac{3}{5} - \frac{1}{2}\right| = 0.1 < \tau$ olur ve test çalışmaz.
- $V_n(obs) = \sum_{k=1}^{n-1} r(k) + 1$, $\varepsilon_k = \varepsilon_{k+1}$ ise $r(k) = 0$ değilse $r(k) = 1$ alınır.

Örneğin : ε= 100110101 $V_{10}(obs)(1 + 0 + 1 + 0 + 1 + 1 + 1 + 1 + 0) + 1 = 7$

$P - değeri = erfc\left(\frac{|V_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi}(1-\pi)}\right) \geq 0.01$ ise dizi rastgeledir.

Akış testinin gerçekleştirilebilmesi için dizi uzunluğu minimum 100 bit olmalıdır. .$V_n(obs)$ 'nin, küçük değerleri için yavaştır, büyük değerleri için dizide osilasyon hızlı (bir osilasyon 1'den

0'a veya tersine bir değişimdir). Osilasyonun hızlı gerçekleşmesi değişimin çok fazla gerçekleşiyor olmasına bağlıdır. Ne kadar hızlı değişim varsa osilasyon da o kadar hızlıdır.

3.4.4. Bloktaki En Uzun Birler

Bu test, üretilen dizideki en uzun birlerin akışının incelenmesine dayanır. Bu testte blok uzunluğu(m) tek parametredir. Elde edilen dizi n tane m bitlik bloğa bölünür ve her bir blok içerisindeki bulunan en uzun birlerin akışı incelenir. Bu değerlerin frekansları beklenen değerler ile kıyaslanır ve sapma durumunun var olup olmamasına bakılır. Blok sayısına ve uzunluğuna bakılarak dizi uzunluğuna karar verilir.

m:Her bir bloğun uzunluğu

n: bit dizisinin uzunluğu

N: Örtüşmeyen blokların sayısı

ε: RSÜ veya SRSÜ ile üretilen bit dizisi

Tablo 3.1 Bloktaki En Uzun Birler Test Parametreleri

Minimum n	M
128	8
6272	128
750000	10^2

Var olan dizi Tablo 3.1' de verilen değerlere göre M bitlik bloklara ayrılır ve kategori şeklinde en uzun birlerin akışının frekansı v_i her bir blok için hesaplanır. Bahsedilen değerler aşağıdaki tabloda yer almaktadır. Tablo 3.2 ve Tablo 3.3' te bulunan her hücre belirli bir uzunluğu olan 1' lerin akış sayısını içerir.

Tablo 3.2 Belirli Uzunluktaki Birlerin Akış Sayıları

V_i	M=8	M=128	$M=10^4$
V_0	≤1	≥4	≤10
V_1	2	5	11
V_2	3	6	12
V_3	≥4	7	13
V_4		8	14
V_5		≥9	15
V_6			≥16

$$X^2(obs) = \sum_{i=0}^{k} \frac{(V_i - N\pi_i)^2}{N\pi_i}$$

Aşağıdaki tabloda uygun olan m değerine göre K ve N değerlerine karar verilir.

Tablo 3.3 Blok Uzunluğuna Göre Kullanılması Gereken K ve N Değerleri

M	K	N
8	3	16
128	5	49
10^4	6	75

N değeri toplam dizi sayısının blok sayısına bölümünden bulunmaktadır.

$$X^2(obs) = \frac{\left(4 - 16(0.2148)\right)^2}{16(0.2148)} + \frac{\left(4 - 16(0.2148)\right)^2}{16(0.2148)} + \frac{\left(4 - 16(0.2148)\right)^2}{16(0.2148)} + \frac{\left(4 - 16(0.2148)\right)^2}{16(0.2148)} = 4.882605$$

$P - değeri = igamc\left(\frac{K}{2}, \frac{X^2(obs)}{2}\right) = igamc\left(\frac{3}{2}, \frac{4.882605}{2}\right) = 0.180 \geq 0.01$ olduğundan dizi rastgeledir.

3.4.5. Rank Testi

Rank testi, var olan dizinin ayrık alt matrislerinin ranklarını hedef alır. Rank testinin amacı, alt dizileri ve orijinal dizi arasında lineer bir bağıntının bulunup bulunmadığını araştırmaktır. Oluşturulan matrislerin rankının hesaplanması için sıra M x M-bit olacak şekilde parçalanır ve yeni oluşturulan matrislerin her birinin rankı hesaplanır. Beklenen frekansla arasında kritik bir sapmanın var olup olmadığını kontrol etmek için ilk olarak bu matrislerin ranklarının frekansları hesaplanır.
M: Her bir matristeki satır sayısı. Test için bu sayı 32 kabul edilir.

N: Matris sayısı $\left[\frac{n}{M.Q}\right]$

Q: Her bir matristeki sütun sayısı. Test için bu sayı 32 kabul edilir.

R1: Her bir matrisin rankı

n: Bit dizisinin boyutu

F*M*: R1=M olan matris sayısı

F_{M-1}: R1=M-1 olan matris sayısı

N-F_M-F_{M-1}: Arta kalan matrislerin sayısı

$$X^2(obs) = \frac{(F_m - 0.2888N)^2}{0.2888N} + \frac{(F_{m-1} - 0.5776N)^2}{0.5776N} + \frac{(N - F_m - F_{m-1} - 0.1336N)^2}{0.1336N}$$

P − Değeri: $e^{-x^{2(obs)/2}}$ ≥0.01 olduğunda dizi rastgeledir.

3.4.6. Ayrık Fourier Dönüşüm Testi

Dizinin tepe yüksekliklerine bakarak, periyodik olup olmadığını inceler. Dizide restgeleliği engelleyen herhangi baskın bir harmoninin bulunup bulunmadığını test etmektedir. Rassallık varsayımından bir sapma gösteren, birbirine yakın olan yinelemeli kalıpları ortaya çıkarır. Tepe yüksekliklerinin %95 i geçtiği haller rastgelelilik açısından iyi bir sonuç olarak sayılmaktadır.

T: %95 zayıflıktaki eşik değeri $T = \sqrt{\left(\log\frac{1}{0.05}\right)^2}$

d: %95 eşik değerinden fazla olan elemanların beklenen ve gerçekleşen sayısı arasındaki farkın normalize değeri.

M: Modül(S′) ≡ |S'|, S′ bit dizisinin ilk n/2 elemanı içindeki alt dizileri temsil eder ve modül fonksiyonu zayıf eşik değerlerinin serisini üretir.

n: Bit dizisinin boyutu

N_0: Teorik olarak T değerinden daha az sayıda beklenen eşik değeri sayısı

$$N_0 = 0.95n/2$$

N_1:Gözlenen ve *M*'deki T değerinden daha az sayıda beklenen eşik değeri sayısı

$$d = \frac{(N_1 - N_0)}{\sqrt{(n(0.95)(0.05))/4}}$$

$$\boldsymbol{P - değeri: erfc\left(\frac{|d|}{\sqrt{2}}\right)} \qquad \textbf{(6)}$$

P-değeri ≥ 0.01 olduğu durumda dizinin rastgele olduğu kabul edilir.

3.4.7. Örtüşmeyen Şablon Eşleştirme Testi

Daha önceden belirlenmiş olan hedef dizisinin bu dizi içerisinde bulunma sıklığının tespit edilmesidir. Testin temel amacı, RSÜ' nün oluşturmuş olduğu periyodik olmayan örneklerin gözlemlenmesidir. Örtüşmeyen ve örtüşen şablon eşleştirme testlerinde, m bitten oluşan bir örneği aramak için m bitten oluşan bir pencere kullanılır. Aranan örneğin bulunmadığı durumlarda ise m bitten oluşan pencere bir bit yana kaydırılarak işlem devam ettirilir. Aranan örneğin bulunduğu durumdaysa, pencere bu örnekten sonraki ilk bite tekrar geçer ve arama işlemi bu bitten devam eder.

M: test edilecek ε alt dizilerinin bit uzunluğu

m : Her bir şablonun bit uzunluğu. Şablon hedef dizidir.

N: Bağımsız blokların sayısı

B:Eşleştirilecek m bit şablon; B test kodu içerisinde bulunan periyodik olmayan örnekler şablon kütüphanesinde tanımlı 0 ve 1'lerden oluşan dizidir.

Wj (j = 1, …, N): j. blok içinde oluşan *B*'lerin sayısı.

n: Test edilen bütün bit dizisi uzunluğu

ε: RSÜ veya SRSÜ ile üretilen bit dizisi

Örnek: ε = 10100100101110010110 için B=001 m=3 olarak alınırsa W1=2 ve W2=1 olur. Her bir adım Tablo 3.4' te gösterilmektedir. 10 bitlik 1010010010 ve 1110010110 iki blok olacak şekilde 20 bitlik dizi ikiye ayrılır.

Tablo 3.4 Blok İçerisindeki B Şablonlarının Bulunma Sayısı

Bit Pozisyonları	**Blok 1**		**Blok 2**	
	Bitler	**W_1**	**Bitler**	**W_2**
1-3	101	0	111	0
2-4	010	0	110	0
3-5	100	0	100	0
4-6	001	1 arttırma	001	1 arttırma
	(bulundu)		(bulundu)	
5-7	(Test edilmedi)		(Test edilmedi)	
6-8	(Test edilmedi)		(Test edilmedi)	
7-9	001	2 arttırma	011	1
8-10	010(bulundu)	2	110	1

$$\mu = \frac{M - m + 1}{2^m} \qquad \sigma^2 = M\left(\frac{1}{2^m} - \frac{2m-1}{2^{2m}}\right) \tag{7}$$

$$X^2(obs = \sum_{j=1}^{N} \frac{(W_j - \mu)^2}{\sigma^2}) \tag{8}$$

$$P - değeri = igamc(\frac{N}{2}, \frac{X^2(obs)}{2}) \tag{9}$$

p-değeri ≥0.01 olduğu durumda dizinin rastgele olduğu kabul edilir.

3.4.8. Örtüşen Şablon Eşleştirme

Daha önceden belirlenmiş olan hedef dizisinin bu dizi içerisinde bulunma sıklığının tespit edilmesidir. Bu testin amacı, Örtüşmeyen Şablon Eşleştirme testinde tanıtılan RSÜ' nün oluşturmuş olduğu birden fazla periyodik özellik göstermeyen örneğin aranmasıdır. Örtüşen ve Örtüşmeyen Şablon Eşleştirme testlerinde, m bit uzunluğunda bir pencere m bit uzunluğundaki bir örneği aramak için kullanılır. Örneğin bulunmadığı durumlarda, belirlenen pencere bir bit daha kaydırılarak işleme devam edilir. Bu testin bir önceki başlıkta bahsedilen testten tek farkı, örneğin bulunması durumunda pencere bulunan örüntüden sonraki ilk bitin yerine yalnızca o zamanda bulunan konumdan bir sonraki bite tekrar yerleşir ve arama işlemine devam edilir.

m:Her bir şablonun bit uzunluğu. Şablon hedef dizidir.

n:Test edilen bütün bit dizisi uzunluğu

ε:RSÜ veya SRSÜ ile üretilen bit dizisi

K:Bağımsızlık derecesi sayısı burada K 5 olarak sabitlenmiştir.

M:Test edilecek ε alt dizilerinin bit uzunluğu M test kodunda 1032 alınmıştır.

N:Bağımsız blokların sayısı. N test kodunda 968 alınmıştır.

Π_i: Teorik olasılıklar

B:Eşleştirilecek m bit şablon; B test kodu içerisinde bulunan periyodik olmayan örnekler şablon kütüphanesinde tanımlı sıfır ve birlerden oluşan dizidir.

V_i (i = 0, …, 5): i. blok içinde oluşan *B*'lerin sayısı

Örnek:

ε = 10111011110010110100011100101110111110000101101001 *n*=50 *K*=2 *M*=10 ve *N*=5 kabul edilmiştir. Daha sonra alınan dizi 1011101111, 0010110100, 0111001011, 1011111000 ve

0101101001 şeklinde 5 tane bloğa ayrılmıştır. Her bir *N* bloktaki *B* şablonunun sayısı hesaplanır. *m*=2 için *B*=11 alınır ve ayrılan birinci blokta 1011101111 aranırsa;

Tablo 3.5 Blok İçerisindeki B Şablonlarının Bulunma Sayısı

Bit Pozisyonu	Bitler	B=11' in bulunma sayısı
1-2	10	0
2-3	01	0
3-4	11(bulundu)	1 arttırma
4-5	11(bulundu)	2 arttırma
5-6	10	2
6-7	01	2
7-8	11(bulundu)	3 arttırma
8-9	11(bulundu)	4 arttırma
9-10	11(bulundu)	5 arttırma

Tablo 3.5' teki sonuçlar incelendiğinde birinci bloktaki arama işleminde 11'e 5 kez denk gelinmiştir. v_5 arttırılır ve v_5=0, v_5=0, v_5=0, v_5 =0 ve v_5=1.

$$\lambda = (M - m + 1)/2^m \qquad \eta = \lambda/2 \tag{10}$$

Bu örnek için λ=(10-2+1)/2^2=2.25 ve η=2.25/2=1.125 değerleri bulunur.

$$X^2(obs) = \sum_{i=1}^{5} \frac{(v_i - N\pi_i)^2}{N\pi_i} \tag{11}$$

Bu örnek için hesaplanan X^2(obs) değeri 3,167729 bulunmuştur.

$$P - değeri = igamc(\frac{K}{2}, \frac{X^2(obs)}{2}) \tag{12}$$

Hesaplanan P-değeri 0,274932 bulunmuştur. Bu değer de 0.01 den büyük olduğu için dizi rastgele olduğu sonucuna ulaşılır.

3.4.9. Maurer' s Evrensel Testi

Üretilmiş olan dizinin yeteri kadar sıkıştırılıp sıkıştırılamayacağını test eder. Bu dizinin fazlasıyla sıkıştırılmaya açık olması durumu, rastgelelikten söz edilemez olduğunu gösterir. Bu

testte, dizi *L* bit uzunluğundan oluşan bloklara ayrılır. Ve testin başlangıç kısmında bu blokların bir bölümü uygulanır. Burada kullanılan referans dağılımı yarım normal dağılımdır. *L*-bit uzunluğundaki kalıpların birbirlerini ne kadar sıklıkla yinelediği hesaplanır elde edilen değerler beklenen değerler ile kıyaslanır. Blok uzunluğu 6 olarak seçildiğinde, dizi uzunluğunun minimum 387,840 olması gerekmektedir.

n : Bit dizisinin uzunluğu.

L :Her bir bloğun büyüklüğü.

sum : K bloklarında tespit edilen farklılıkların log2 tabanında toplamı

T*j* : Her bir L-bitlik bloğun blok sayısını tutan j'ye bağlı tablo değeri

fn : Eşleşen L-bitlik şablonlar arasındaki mesafelerin log2 tabanında toplamı

***ε* :** Teste tabi tutulan bit dizisi

σ : Standart sapma.

K : Test edilen blokların sayısı

Q : Başlangıç dizisindeki blokların sayısı.

c : Sezgisel yaklaşım

$\boldsymbol{\varepsilon} = \varepsilon 1\, \varepsilon 2 \ldots\ldots \varepsilon n$

$$n \geq (Q + K) * L$$

$$6 \leq L \leq 16 \qquad\qquad Q = 10 * 2^L$$

$$K = \left(\frac{N}{L}\right) - Q \approx 1000x2^L \tag{13}$$

Q, n, L değerleri Tablo 3.6' daki değerlere göre seçilir;

Tablo 3.6 Blok İçerisindeki L, Q, n Değerleri

n	L	$Q=10.2^L$
≥387.840	6	640
≥904.960	7	1.280
≥2.068.480	8	2.506
≥4.654.080	9	5.120
≥1.342.400	10	10.240
≥22.753.280	11	20.480
≥49.643.520	12	40.960
≥107.560.960	13	81.920
≥231.669.760	14	163.840
≥496.435.200	15	327.680
≥1.059.061.760	16	655.360

$$f_n = \frac{1}{K}\sum_{i=Q+1}^{Q+K} \log_2(i - T_j) = \frac{sum}{K} \tag{14}$$

$$P - değeri = erfc\left(\left|\frac{f_n - BeklenenDeğer(L)}{\sqrt{2}\sigma}\right|\right) \tag{15}$$

BeklenenDeğer(L) Tablo 3.7' den elde edilir:

Tablo 3.7 beklenenDeğer Sonuçları

L	***beklenenDeğer***	***varyans***
6	5.2177052	2.954
7	6.1962507	3.125
8	7.1836656	3.238
9	8.1764248	3.311
10	9.1723243	3.356
11	10.170032	3.384
12	11.168765	3.401
13	12.168070	3.410
14	13.167693	3.416
15	14.167488	3.419
16	15.167379	3.421

$$\sigma = c\sqrt{\frac{varyans(L)}{K}} \tag{16}$$

$$c = 0.7 - \frac{0.8}{L} + \left(4 + \frac{32}{L}\right) X \frac{K^{-3/L}}{15} \tag{17}$$

P-Değeri ≥ 0.01 olduğu durumlarda dizinin rastgele olduğu kabul edilir.

3.4.10. Doğrusal Karmaşıklık Testi

Üretilen bit dizisinin LFSR uzunluğuna bakılarak karmaşıklığı gözlemlenir. Test edilen dizinin rastgelelik için yeterli ölçüde kompleks olup olmadığını test eder. Bu diziler LFSR çıktıları olarak kabul edilir ve diziyi meydana getirecek en küçük LFSR' nin uzunluğu küçükse, dizinin rastgele olması için yeterli ölçüde kompleks olmadığı sonucuna ulaşılır. Teste tabi tutulan dizi *M* bit uzunluklu bloklara parçalanır ve bloktaki bitlerin doğrusal karmaşıklıkları Berlekamp-Massey algoritması ile hesaplanır. Bulunan doğrusal karmaşıklıkların beklenen dağılıma uygunluğu gözden geçirilir. Bu testte kullanılan referans dağılım ki-kare dağılımıdır. Bu testi gerçekleştirmek için üretilen dizinin uzunluğunun en az 1,000,000; blok uzunluğunun da 500 ve 5000 arasında olması gerekmektedir.

M:Bloktaki bit uzunluğu

n: Bit dizisinin uzunluğu. n=M.N

N: M bitlik bağımsız blok sayısı

K: Serbestlik derecesi. Test kodunda *K = 6* olarak alınmıştır.

T_i: Alt dizi sayısı

$$\mu = \frac{M}{2} + \frac{(9 + (-1)^{M+1})}{36} - \frac{M/3 + 2/9}{2^M} \tag{18}$$

$$T_i = (-1)^M . (L_i - \mu) + 2/9 \tag{19}$$

T_i değerleri için v_0, ….. v_6 değerleri şu şekilde hesaplanır:

$T_i \leq$ -2.5 v_0 1 arttırılır

-2.5 < $T_i \leq$ -2.5 v_1 1 arttırılır

-1.5 < $T_i \leq$ -0.5 v_2 1 arttırılır

-0.5 < $T_i \leq$ 0.5 v_3 1 arttırılır

0.5 < $T_i \leq$ 1.5 v_4 1 arttırılır

1.5 < $T_i \leq$ 2.5 v_5 1 arttırılır

$T_i > 2.5$ v_6 1 arttırılır

$$X^2(obs) = \sum_{i=1}^{K} \frac{(v_i - N\pi_i)^2}{N\pi_i}$$

$$P - değeri = igamc\left(\frac{K}{2}, \frac{X^2(obs)}{2}\right) \quad (20)$$

P-değeri ≥ 0.01 olduğu halde dizinin rastgele olduğu kabul edilir.

3.4.11. Seri Testi

Bütün dizideki m-bit uzunluklu örtüşen olası örneklerin frekansına dayanır. Buradaki amaç, 2^m tane m-bit uzunluklu örtüşen örneklerin adedinin, rassal bir dizide olması beklenen adede ne kadar yakın olduğunun gözlemlenmesidir. Rassal dizilerde önemli bir özellik olan tek-biçimlilikte her m-bit uzunluklu örneğin diğer m-bit uzunluklu örnekler gibi oluşma olasılığının aynı olması beklenir. m=1 alındığı zaman bu test frekans testine dönüşür.

$$\Psi_m^2 = \frac{2^m}{n} \sum_{i=1}^{m} v_i^2 - n$$

$$\Psi_{m-2}^2 = \frac{2^{m-2}}{n} \sum_{i=1}^{m-2} v_i^2 - n$$

$$\Psi_{m-1}^2 = \frac{2^{m-1}}{n} \sum_{i=1}^{m-1} v_i^2 - n$$

$$\nabla\Psi_m^2 = \Psi_m^2 - \Psi_{m-1}^2 \qquad \nabla^2\Psi_m^2 = \Psi_m^2 - \Psi_{m-1}^2 + \Psi_{m-2}^2 \quad (21)$$

$$P - değeri.1 = igamc\left(2^{m-2}, \frac{\nabla\Psi_m^2}{2}\right)$$

$$P - değeri.2 = igamc\left(2^{m-3}, \frac{\nabla^2\Psi_m^2}{2}\right) \quad (22)$$

3.4.12. Yaklaşık Entropi Testi

Bütün dizideki m-bit uzunluklu örtüşen olası örneklerin sıklığına odaklanır. Bu testte amaç, ardışık iki ya da komşu uzunluktaki (m ve m+1 bit) örtüşen bloğun sıklığını, rassal dizinin beklenen frekansı ile kıyaslanmasıdır.

***Cim*:** Her bir i değeri için hesaplanan m bitlik blok sayısı

n: Tüm bit dizisinin uzunluğu

m: Her bir blok uzunluğu. Teste kullanılan 1. blok uzunluğudur. *m+1* ise kullanılan 2. blok uzunluğudur.

$$A_pE_n(m) = \varphi^{(m)} \quad k_\varphi^{(m+1)} \quad (23)$$

$$C_i^m = -\frac{\#\mathrm{i}}{n} \qquad \pi_i = C_j^3$$

$$\varphi^{(m)} = \sum_{i=0}^{2^{m-1}} \pi_i \log \pi_i \qquad j = \log_2 i$$

$$X^2 = 2n[\log 2 - ApEn(m)]$$

$$P - değeri = igamc(2^{m-1}, \frac{X^2}{2}) \quad (24)$$

P-değeri ≥ 0.01 olursa dizi rastgeledir denilebilir.

3.4.13. Birikimli Toplamlar Testi

Bir dizide düzenlenmiş -1,+1 dijitlerinin birikmiş toplamıdır ve rastgele yürüyüş maksimal gezinimlerinin incelenmesine dayanır. Kümülatif toplamda rastgele yürüyüş olarak kabul edilebilir. Rastgele dizilerde rastgele yürüyüş gezinimleri 0 civarındadır.

Si = Artarak büyüyen alt dizilerin toplamı

mod: Test uygulaması dizinin başından sonuna doğru yapılırsa mod=0, sondan başa doğru yapılırsa mod=1'dir. Tablo 3.8' de detaylı değerler verilmiştir.

n: Bit dizisinin uzunluğu

Buradaki referans dağılımı normal dağılımdır.

- Dizi normalize edilir. Giriş dizisindeki (ε) 0' lar ve 1' ler $X_i=2\ \varepsilon_i-1$ kullanılarak X_i değerleri -1 ve +1' lere dönüştürülür.

Örneğin: ε= 1011010111, X=1,(-1),1,1,(-1),1,(-1),1,1,1 olur.

- S_i kısmi toplamları bulunur. Mode 1 ise X_n' den mode 0 ise X_i den başlanır.

Tablo 3.8 Blok İçerisindeki Kullanılması Gereken mod Formülleri

Mod=0	Mod=1
$S_1=X_1$	$S_1=X_n$
$S_2=X_1+X_2$	$S_2=X_n+X_{n-1}$
$S_3=X_1+X_2+X_3$	$S_3=X_n+X_{n-1}+X_{n-2}$
…	…
…	…
$S_k=X_1+X_2+\ldots.\ X_k\ \ldots.$	$S_k=X_n+X_{n-1}+\ldots.\ X_{n-k+1}$
…	….
$S_n=X_1+X_2+\ldots.\ X_n$	…
	$S_n=X_n+X_{n-1}+\ldots.\ X_{k-1}+\ldots..X_1$

- Bu kısımdaki örnek için, mode 0 alındığında X=1,(-1),1,1,(-1),1,(-1),1,1,1

  $S_1=1$

  $S_2=1+(-1)=0$

  $S_3=1+(-1)+1=1$

  $S_4=1+(-1)+1+1=2$

  $S_5=1+(-1)+1+1+(-1)=1$

  $S_6=1+(-1)+1+1+(-1)+1=2$

S_7=1 + (-1) + 1 + 1 + (-1) + 1 + (-1) = 1

S_8=1 + (-1) + 1 + 1 + (-1) + 1 + (-1) + 1 = 2

S_9=1 + (-1) + 1 + 1 + (-1) + 1 + (-1) + 1 + 1 = 3

S_{10}=1 + (-1) + 1 + 1 + (-1) + 1 + (-1) + 1 + 1 + 1 = 4

- Elde edilen S değerlerini mutlak değerli en büyük sayısı belirlenir.

Bu örnek için S_k=4 tür, o halde z=4 olur.

- Daha sonra p değeri hesaplanır.

$$P-değeri = 1 - \sum_{k=\left(-\frac{n}{z}+1\right)/4}^{\left(\frac{n}{2}-1\right)/4} \left[\Phi\left(\frac{(4\cdot k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4\cdot k-1)z}{\sqrt{n}}\right)\right] + \sum_{k=\left(-\frac{n}{z}-3\right)/4}^{\left(\frac{n}{2}-1\right)/4} \left[\Phi\left(\frac{(4\cdot k+3)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4\cdot k+1)z}{\sqrt{n}}\right)\right]$$

Burada standart Φ normal kümülatif olasılık dağılım fonksiyonudur.

Bu örnek için p_degeri=0.4116588 ≥ 0.01 olduğundan dizi rastgele kabul edilir.

3.4.14. Rastgele Gezinim Testi

Kümülatif toplam rastgele yürüyüşündeki K ziyaretlik döngünün sayısını hedef alır. Kümülatif toplam rastgele yürüyüşü, 0 ve 1'lerden meydana gelen dizinin -1 ve +1 olarak değiştirildikten sonra kısmi toplamlarından oluşturulur. Rastgele bir yürüyüş döngüsü, rastgele olduğu varsayılan bir noktadan başlayıp tam bir döngüyü tamamlayana kadar belli bir uzunluktaki adım dizisinden oluşur. Buradaki amaç, döngü sırasında rastgele dizide beklenen sapmanın neden olduğu belirli bir durumun ziyaretlerinin adedinin belirlenmesidir. Bu test esasen 8 test ve bu testlerin çıkarımlarından oluşan bir seridir.

n: Bit dizisinin uzunluğu

Si: Her defasında $X1$'den başlanarak adım adım arttırılan kısmi toplamlar

X: Bit dizisindeki 0 ve 1'lerin toplamı (0= -1, 1=1 alınarak yapılan aritmetik toplama sonucu).

$S_1 = X_1$

$S_2 = X_1 + X_2$

..

..

$S_k = X_1 + X_2 + \ldots\ldots\ldots\ldots + X_k$

...

$S_n = X_1 + X_2 + \ldots\ldots\ldots\ldots + X_k + \ldots\ldots\ldots X_n$

S′: Oluşturulan S dizisinin başına ve sonuna 0 eklenerek oluşturulan yeni alt dizi

J: S' dizisinde geçen sıfırların sayısıdır. Aynı zamanda S'deki döngü sayısıdır. Döngü sayısı 0 ile başlayıp ve biten dizilerin adedine bağlıdır.

x: Her bir döngü ve sıfır içermeyen durum sayısı. $-4 \leq x \leq -1$ ve $1 \leq x \leq 44$

$v_k(x)$: k' ya bağlı x koşulunun tüm döngülerdeki toplam sayısı. $k = 0,1,..,5$ için

$$\sum_{k=0}^{5} v_k(x) = j \qquad X^2(obs) = \sum_{k=0}^{5} \frac{(v_k(x) - j\pi_k(x))^2}{j\pi_k(x)}$$

$\pi_k(x)$: x koşulunun rastgele bir dağılımda k defa oluşma olayıdır.

$$P - değeri = igamc\left(\frac{5}{2}, \frac{x^2}{2}\right) \tag{25}$$

3.4.15. Rastgele Gezinim Değişken Testi

Kümülatif bir toplam rastgele yürüyüşünde, özel durumların ziyaret edilme sayısı ölçülür. Amaç rastgele bir yürüyüşte özel durumların beklenen ziyaret adedindeki sapmalarının incelenmesidir. Bu test esasen 18 adet durumun ve bu durumların sonuçlarının serisidir. Bu durumlar -9,-8,.....,-1 ve 1,2,.....9'dur.

İşlemlerde kullanılan ε, RSÜ veya SRSÜ ile üretilen bit dizisi ($\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$), n bit dizisinin uzunluğunu ve ξ 4.4.15 nolu testte adım4' te karar verilen bütün rastgele yürüyüşler süresince ziyaret edilen durumların toplam sayısını temsil etmektedir.

- Dizi normalize edilir. Giriş dizisindeki (ε) 0' lar ve 1' ler $X_i = 2\varepsilon_i - 1$ kullanılarak X_i değerleri -1 ve +1' e dönüştürülür.

Örneğin: ε= 0110110101, X=(-1),1,1,(-1),1,1,(-1),1,(-1),1 olur.

- Si kısmi toplamları hesaplanır. mode 1 ise X_n' den Mode 0 ise X_i 'den başlanır.

$S_1 = X_1$

$S_2 = X_1 + X_2$

$S_3 = X_1 + X_2 + X_3$

.

.

$S_k = X_1 + X_2 + X_3 + ... + X_k$

.

.

$S_n = X_1 + X_2 + X_3 + ... + X_k + ... + X_n$

Buradaki örnek için,

S_1= -1 S_6= 2
S_2= 0 S_7= 1
S_3= 1 S_8= 2
S_4= 0 S_9= 1
S_5= 1 S_{10}= 2

S={-1,0,1,0,1,2,1,2,1,2} olur.

- S' nin başına ve sonuna sıfır eklenerek S' kümesi oluşturulur. S'=0,s_1,s_2,....s_n,0.

Buradaki örnek için: S'={0,-1,0,1,0,1,2,1,2,1,2,0}.

- 18 farklı x durumu için, bütün j döngüleri içinde oluşan x durum değerlerini toplam sayısı ξ(x) hesaplanır.

Bu kısımdaki örnek için: ξ(-1)=1, ξ(1)=4, ξ(2)=3 ve diğerleri ξ(x)=0 olur.

- Her bir ξ(x) için, pdegeri= $\text{erfc}\left(\frac{|\xi(x)-J|}{\sqrt{2J(4|x|-2)}}\right)$ hesaplanır.

$P-değeri = 1/2erfc\left(\frac{\mu - W_{obs}}{\sqrt{2\sigma^2}}\right)$ burada n=10^6 için =69586.25 ve $\sigma = 70.488718$ dir. N' nin diğer değerleri için Sha-1 kullanılarak ortalama( ) ve varyans ( ) değerleri hesaplanabilir.

4. SONSUZ GÜRÜLTÜ (CROWDSUPPLY) CİHAZI

Kritik önemi nedeniyle birçok üretici, kriptografik rastgeleliği sağlamak için çeşitli donanımlar geliştirmektedir. Bu ekipmanlardan biri de Crowd Supply Infinite Noise GRSÜ' dir [10]. Bu donanım Şekil 4.1' de gösterilmiştir. Bu çalışmada bu donanımın çalışma mantığı incelenmiş ve çeşitli istatistiksel analizler yapılarak kriptografik uygulamalara uygunluğu incelenmiştir.

Şekil 4.1 Sonsuz gürültü GRSÜ donanımı

Donanım, herhangi bir bilgisayardaki bir USB bağlantı noktası kullanılarak çalıştırılabilir. Üzerindeki ısı sensörleri fiziksel entropi kaynağı olarak kullanılarak tohum değerleri üretilir. Elde edilen değerlere SHA3 hash fonksiyonu uygulanarak istatistiksel gereksinimlerin karşılanması amaçlanmaktadır.

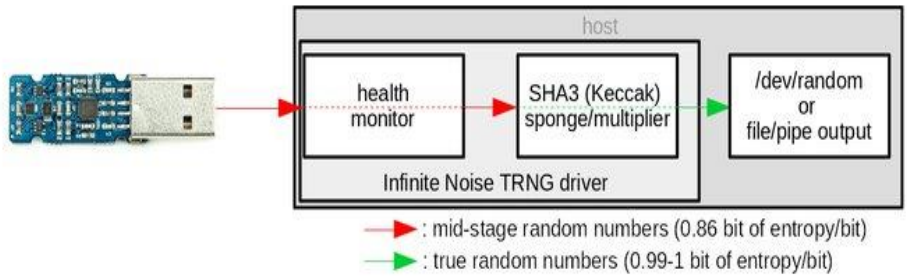
Bu çalışmada kullandığımız Sonsuz Gürültü GRSÜ, uygun fiyatlı ve güvenli bir gerçek rastgele sayı üretecidir (GRSÜ). Bir sonraki rastgele çıktıyı oluşturmak için, bir önceki rastgele çıktı üzerinde sürekli olarak döngü yapan, yol boyunca donanım bileşenlerinin gürültüsünden rastgelelik toplayan modüler bir entropi çarpan tekniğine dayanır. Bu şekilde sabit, ölçülebilir bir entropi seviyesi üretir ve daha sonra gerçek rastgele sayılar üretmek için beyazlatılır. Bir sonraki aşamada cihazın bu verileri nasıl ürettiğinden bahsedeceğiz.

4.1. Sonsuz Gürültü GRSÜ nin Çalışma Mantığı

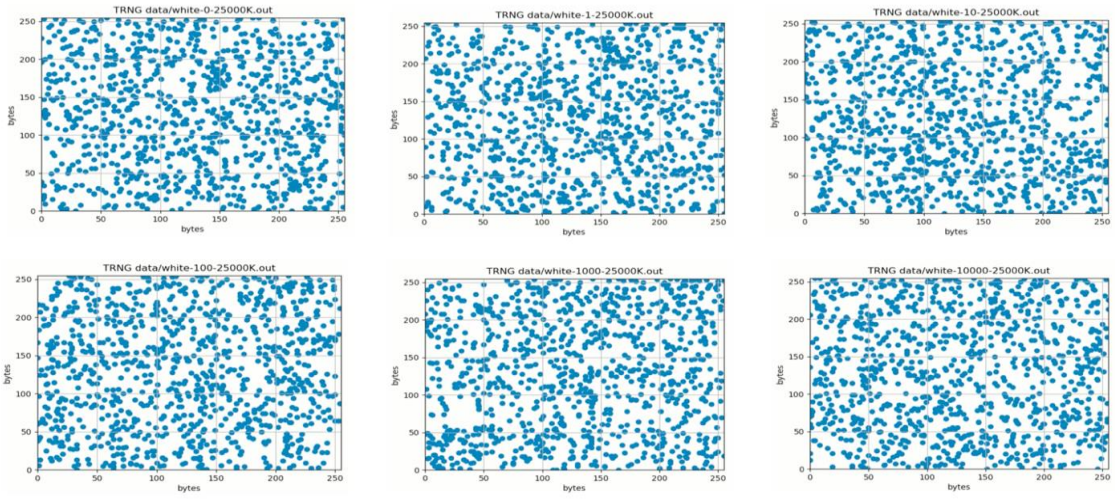
Çoğu durumda kriptoloji uygulamalarında güvenlik, anahtarın genişliği ve rastgeleliği ile ilişkilidir. Özellikle Vernam tarafından önerilen one-time pad olarak bilinen şifreleme yaklaşımında, her bir anahtarın bir kez kullanılması durumunda şifreleme sisteminin koşulsuz güvenliğe sahip olacağı kanıtlanmıştır. Bu nedenle hem araştırmacılar hem de üreticiler alternatif anahtar oluşturuculara odaklanmışlardır. Bu temel oluşturuculardan biri, Crowd Supply Infinite Noise GRSÜ' dir. Düşük maliyeti, kullanım kolaylığı bu kriptolojik donanımın avantajları olarak

öne çıkıyor. Crowd Supply Infinite Noise GRSÜ cihazının çalışma mantığı Şekil 4.2 'te gösterilmektedir.

Şekil 4.2’ de tasarım mimarisi gösterilen donanım, birçok rastgele sayı üreteci gibi entropiyi termal gürültüden türetir. Onu diğer GRSÜ' lerden ayıran şey, modüler entropi çarpma tekniğidir. Bir sonraki rastgele çıktıyı oluşturmak için, bir önceki rastgele çıktı üzerinde sürekli olarak döngü yapan, yol boyunca donanım bileşenlerinin gürültüsünden rastgelelik toplayan modüler bir entropi çarpan tekniğine dayanır. Bu şekilde sabit, ölçülebilir bir entropi seviyesi üretir ve daha sonra gerçek rastgele sayılar üretmek için beyazlatılır. Modüler entropi çarpımından gelen bitler ilişkilendirilebilir, bu nedenle kriptografide kullanılmadan önce beyazlatma gereklidir. Bu SHA-512, Blake2b, SHA-3 gibi kriptografik olarak güvenli bir hash işlevini veya ChaCha gibi bir akış şifresini sürekli olarak yeniden göndererek yapılmalıdır. Ham veri akışının önemli parametrelerinin sağlık izlemesi cihaz sürücüsünde uygulanır. Daha sonra gerçek rastgele sayılar üretmek için SHA-3 ile beyazlatma işlemi uygulanır. Bu cihaz, GNU/Linux/dev/random sistemde mevcut olan bir giriş/çıkış probleminin üstesinden gelerek, bir seferde 400 bitten fazla entropinin kriptografik olarak güvenli bir şekilde yeniden beslenmesiyle Keccak-1600 (SHA-3) ile beyazlatma işlemini gerçekleştirir.



Şekil 4.2 Sonsuz gürültü GRSÜ nin tasarım mimarisi



Şekil 4.3 Crowd Supply Infinite Noise GRSÜ kullanılarak elde edilen rastgele değerlerin dağılımı.

Şekil 4.3, Crowd Supply Infinite Noise GRSÜ kullanılarak elde edilen rastgele değerlerin dağılımını göstermektedir.

Crowd Supply Infinite Noise GRSÜ cihazı, fiziksel bir jeneratör olduğu için öngörülemeyen bir yapıya sahiptir. Bu özellik sayesinde R2, R3 ve R4 gereksinimleri otomatik olarak karşılanacaktır. Bu nedenle, bir GRSÜ yapısı için istatistiksel gereksinimlerin karşılandığı doğrulanmalıdır. İkinci bölümde gösterilen mimaride, R1 gereksinimini karşılamak için SHA3 işlevi kullanılır. Bu bölümde istatistiksel gereksinimlerin karşılanıp karşılanmadığı analiz edilir.

4.1.1. Modüler Entropi Çarpımı

Bu yöntem Firebug adıyla 1999 yılında Peter Allan tarafından icat edildi. 2013 te bu uygulamayla yeniden düzenlendi. İşlemi gerçekleştiren devre, bir çift şarj kapasitöründen (C8,C9), opamplardan, karıştırıcılardan(COMP1, COMP2) ve katı hal anahtarlarından(SW1, SW2) oluşur. Bir döngünün ilk yarısından, kondansatörde depolanan akım voltajının Vref (2.5V) değerinden düşük olup olmadığını belirlememiz gerekir. Eğer düşükse tüm değer 1.82 ile çarpılır, yüksekse de aşırı atlamayı önlemek için Vref i ondan çıkarmamız gerekir.

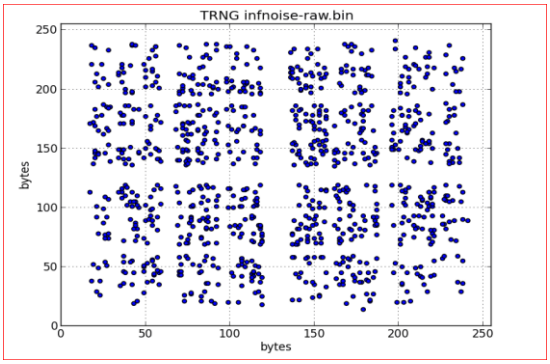
$$\boldsymbol{V_{out} = V_{sup} - K * \left(V_{ref} - V_{in}\right)} \text{ ya da } \boldsymbol{V_{out} = K * V_{in}\ mod\ V_{ref}} \quad (3.1)$$

K=1.82 V_{sup}= 5V V_{ref}= 2.5V (3.2)

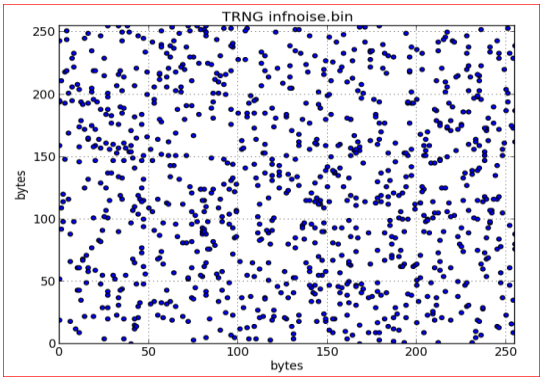
4.1.2. Denetim Modülü

Modüler entropi çarpımını kullanarak termal gürültü gibi çok basit ama güvenilir bir entropi kaynağı, kanıtlanabilir bir bit başına 0,86 bit entropi seviyesine sahip 300.000 bit / s' lik bir ham

akış üretmek için kullanılabilir. Bu beklenen entropi seviyesinden(0,86) % 3'ten fazla sapma varsa veriler atılır, böylece SHA3 işlevine yerleştirilen verilerin zaten oldukça rastgele olduğundan ve Sonsuz Gürültü' den geldiğinden her zaman emin olabiliriz.



Şekil 4.4 Modüler entropi çarpımı modelini ortaya çıkaran ham cihaz çıktısı(ham verinin dağılım grafiği)



Şekil 4.5 Beyazlatma(SHA-3) işleminden sonraki verilerin dağılım grafiği

Şekil 4.4 ve Şekil 4.5' de verilen entropi dağılım grafikleri incelendiğinde beyazlatma işlemi uygulanmadan önceki dağılım ve beyazlatma işleminden sonraki dağılımın farkı da açık bir şekilde görülmektedir.

4.2. Analiz Sonuçları

İstatistiksel rastgeleliği doğrulamak için birçok farklı test aracı mevcuttur [5]. Bu test araçları arasında NIST tarafından geliştirilen 15 testten oluşan NIST SP 800-22 Statistical Test Suite en yaygın kabul gören araçtır [6]. Bu testleri gerçekleştirmek için 1000000 bit uzunluğunda diziler gereklidir. Referans [6] bu testlerin matematiksel ifadesi için incelenebilir.

Tablo 5.1, Crowd Supply Infinite Noise GRSÜ cihazı kullanılarak oluşturulan 1000000 uzunluğunda üç farklı veri için NIST test sonuçlarını göstermektedir. Bu aşamada daha güvenilir testler yapabilmek için çok daha fazla veri üretilmesi ve ortalama özelliklerin incelenmesi gerektiği

düşünülmektedir. [9, 10]. Bu dezavantajlara rağmen, analiz edilen avantajların tartışılmasının daha adil bir değerlendirme sağlayacağı düşünülmektedir. Tablo 4.1, cihazdan elde edilen verilere uygulanan NIST test sonuçlarını göstermektedir.

Tablo 4.1 İstatistiksel rastgelelik testi sonuçları

	Veri1	**Veri2**	**Veri3**
frekans testi	P=1.3864e-05	P=1.489e-17	P=4.1535e-16
bloktaki en uzun birler testi	P=0.36505	P=0.35775	P=0.6318
örtüşmeyen şablon eşleştirme testi	P=0.026441	P=0.11855	P=0.0247
doğrusal karmaşıklık testi	P=0.9210	P=0.0107	P=0.0548
birikimli toplamlar testi	P=1.7908E-05	P=0	P=8.88178E-16
blok frekans testi	P=0.0886	P=1.2957e-04	P=7.3984e-06
rank testi	P=0.3636	P=0.6999	P=0.6398
örtüşen şablon eşleştirme testi	P=0.9192	P=0.0775	P=0.0359
seri testi	P=0.1732	P=0.6983	P=0.0633
rastgele gezinim testi	P=0.5335	P=0.2631	P=0.2294
akış testi	P=0	P=0	P=0
ayrık fourier dönüşüm testi	P=0.3636	P=0.6999	P=0.6398
maurer' s evrensel testi	P=0.5689	P=0.5698	P=0.5691
yaklaşık entropi testi	P=0.00012975	P=4.953e-14	P=0
rastgele gezinim değişken testi	P=0.0574	P=0.5137	P=0.7385
Toplam Başarı Sayısı	11	10	11

Rastgelelik, kriptolojik uygulamalarda [12-13] en temel gereksinimlerden biri olduğundan, bu ihtiyacı karşılamak için birçok araştırma yapılmış ve birçok ticari ürün geliştirilmiştir [13, 14]. Bu çalışmada, bu ticari donanımlardan birinin kriptolojik uygulamalar için uygunluğu araştırılmıştır.

Çalışmada Crowd Supply Infinite Noise GRSÜ cihazından elde edilen veriler NIST istatistiksel test paketi uygulanarak değerlendirilmiştir. Bu testlerde en fazla 11 testte başarılı olduğu gözlemlenmiştir. Farklı veriler için yapılan analizlerde aynı testlerde başarısız sonuçların alındığı gözlemlenmiştir. İncelenen donanımda SHA3 fonksiyonu kullanılmasına rağmen tüm testlerin başarısızlığı problem olarak değerlendirilmiştir.

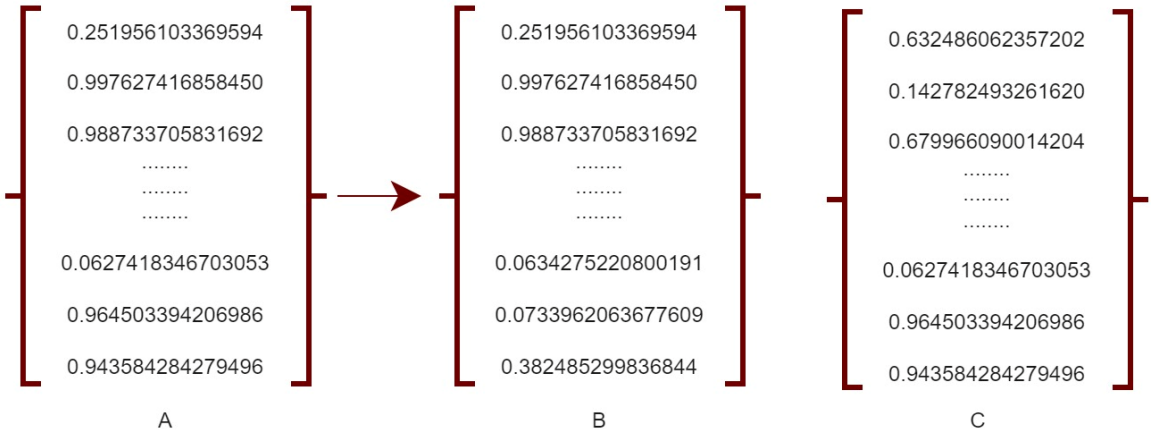
5. MATERYAL VE METOD

Daha önce yapılan çalışmada Crowd Supply Infinite Noise GRSÜ cihazından elde edilen veriler NIST istatistiksel test paketi uygulanarak değerlendirilmiştir. Bu testlerde en fazla 11 testte başarılı olduğu gözlemlenmiştir. Farklı veriler için yapılan analizlerde aynı testlerde başarısız sonuçların alındığı gözlemlenmiştir. İncelenen donanımda SHA3 fonksiyonu kullanılmasına rağmen tüm testlerin başarısızlığı problem olarak değerlendirilmiştir. Burada elde ettiğimiz testlerden başarı gösteremeyen birer milyondan oluşan 3 veri setini farklı şekillerde işlemlerden geçirerek NIST test başarısının arttığını gösterilmiştir. İncelenen donanımda SHA-3 fonksiyonu kullanılmasına rağmen tüm testlerin başarısızlığı ciddi bir problem olarak değerlendirilmiştir. Çünkü SHA-3 fonksiyonunun çıkışları istatistiksel olarak düzgün bir dağılım göstermesi gerektiği beklenmektedir. Ancak piyasada aktif olarak kullanılan bu fiziksel rastgele sayı üreteci donanımının bu özellikleri karşılamaması birçok problemi de beraberinde getirecektir. Bu tez çalışmasının literatüre en önemli katkılarından biri istatistiksel olarak başarılı özellikler göstermeyen veri setlerinin(RSÜ çıktılarının bile) çeşitli son işlem adımlarına tabi tutularak performansının iyileştirilebileceğinin gösterilmiş olmasıdır. Çalışma kapsamında 19 tane farklı yaklaşım önerilerek 3 veri setinden NIST testlerini geçebilecek 19 farklı veri setinin üretilebileceği gösterilmiştir.

5.1. Elde Edilen Verilerin İyileştirilmesi

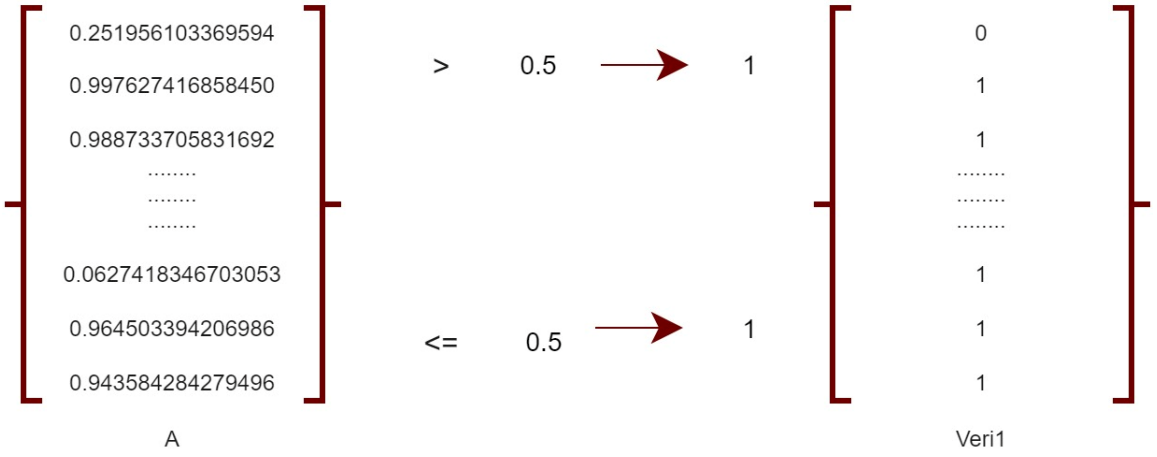
Dördüncü bölümde çalışma mantığı açıklanan Sonsuz Gürültü GRSÜ Cihazı kullanılarak öncelikle 3 tane 1 milyon uzunluğunda veri seti elde edilmiştir. Bu veri setlerinin analizleri NIST testleri aracılığıyla gerçekleştirilmiştir. Veri setlerinin 1 milyon bit uzunluğunda tercih edilmesinin en önemli nedeni üçüncü bölümde açıklanan NIST test paketindeki testlerin gerçekleştirilebilmesi için her seferinde 1 milyon bit uzunluklu veriye ihtiyaç duyulmasıdır.

Bu çalışmada kullanılan gerçek bir rastgele sayı üreteci olan Sonsuz Gürültü cihazı 0-1 aralığında sayılar üretmektedir. İlk aşamada cihazdan 0-1 aralığında 2 milyon tane veri üretilmiştir. Üretilen bu 2 milyon tane veri iki eş parçaya ayrılarak birer milyonluk 2 veri setine ayrılmıştır. Elde edilen ilk 1 milyonluk veri setinin elemanları 0.5 ile kıyaslanarak verinin değeri 0.5’ ten küçükse 0 değilse 1 değerleri üretilmiştir. Elde edilen Veri1 dosyasındaki elemanlar bu şekilde üretilmiştir. Cihazdan elde edilen ham verinin ikinci 1 milyonu için de yine aynı işlemler gerçekleştirilerek Veri2 dosyası üretilmiştir. Şekil 5.1, Şekil 5.2 ve Şekil 5.3’ te önerilen yaklaşımın çalışma prensibi temsil edilmiştir.

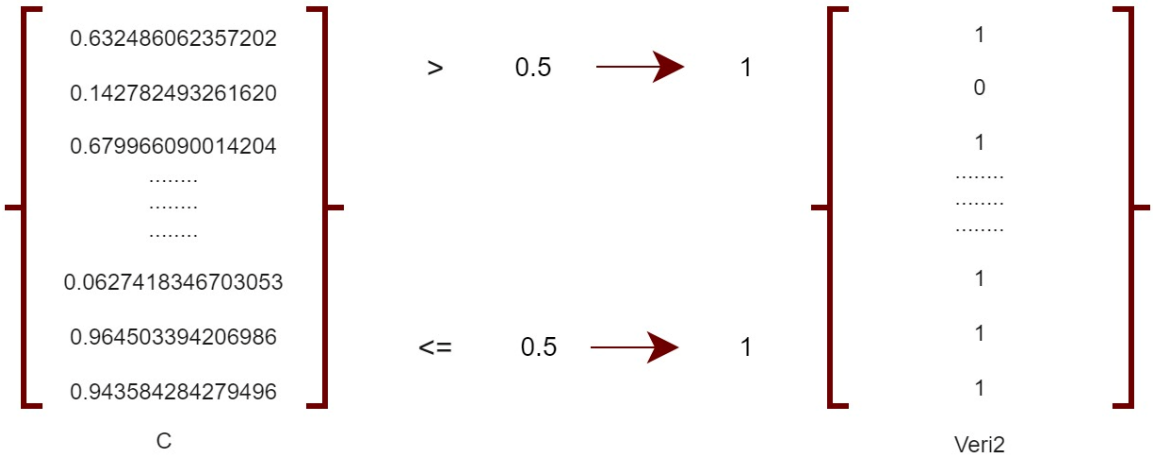


A: Cihazdan üretilen 2 milyon ham veri
B: 2 milyon verinin ilk 1 milyonu
C: 2 milyon verinin ikinci 1 milyonu

Şekil 5.1 Ham verilerin üretilmesi

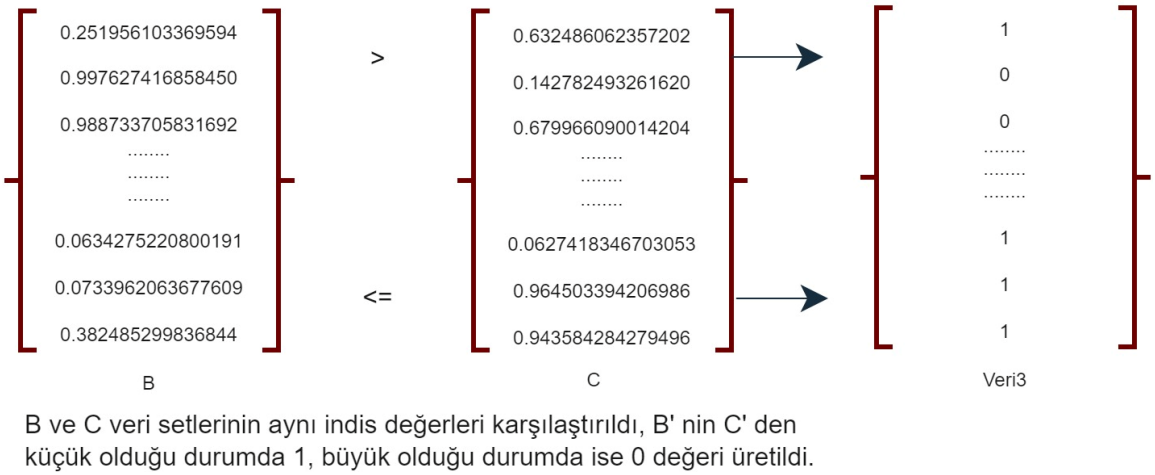


Şekil 5.2 Veri1 dosyasındaki verilerin üretilmesi



Şekil 5.3 Veri2 dosyasındaki verilerin üretilmesi

İlk iki veri dosyasını ürettikten sonra üçüncü veri dosyası ise, aynı indis değerleri kıyaslanarak ilk veri setindeki değer ikinci veri setindeki değerden küçükse 1, değilse 0 değerleri üretilerek oluşturulmuştur. Şekil 5.4 Veri3 dosyasındaki verilerin elde edilmesi için önerilen yaklaşımın detaylarını göstermektedir.

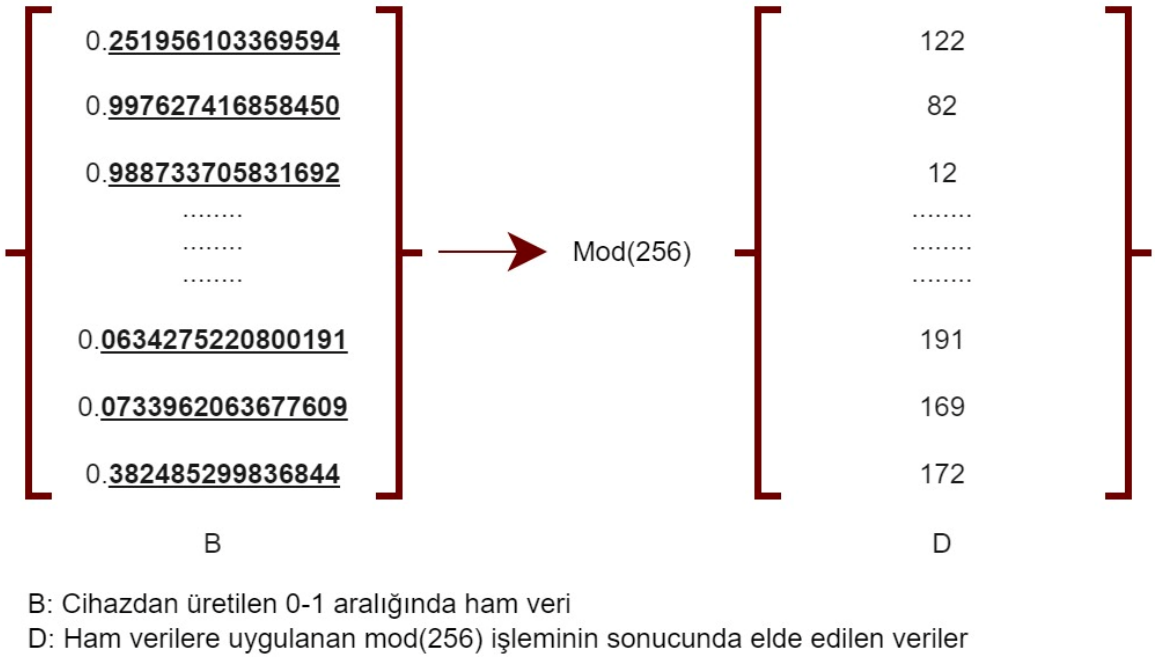


Şekil 5.4 Veri3 dosyasındaki verilerin üretilmesi

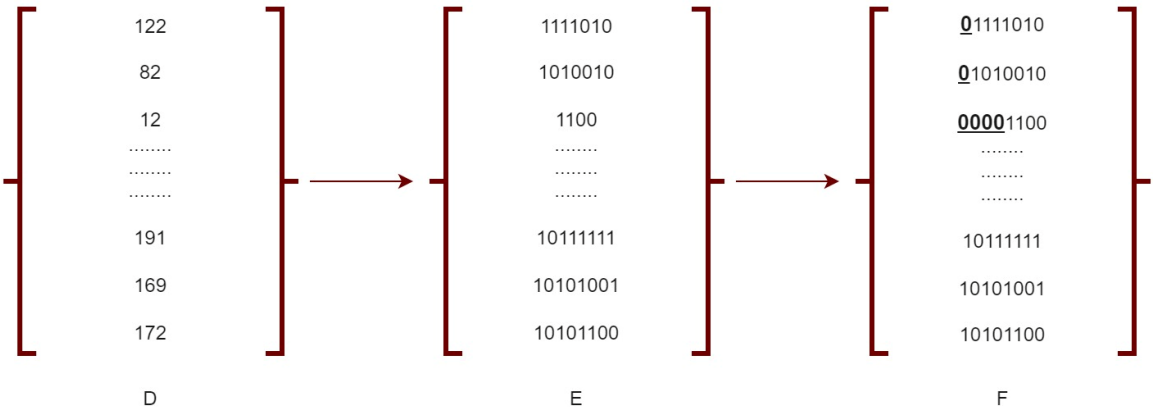
Cihazdan elde edilen ham verilerin virgülden sonraki basamakları 15 ve 16 değerden oluşmaktadır. Bu değerlerin her birinin 256’ ya mod alınması sonucunda elde edilen onluk tabandaki değerler ikilik tabana dönüştürülmüştür. Elde edilen bu değerlerin uzunluğu 7 bit ise başlarına 0 getirilerek bu uzunluk 8’ e tamamlanmıştır. Bu şekilde üretilen değerler yan yana yazılarak Veri4 dosyası oluşturulmuştur.

Ham veriden elde edilen dosyada bulunan 2 milyonluk verinin ilk 125.000’ ine uygulanan işlemler sonucunda 1 milyon bit uzunluklu Veri4 dosyası elde edilmiştir. Geri kalan 15 veri seti ise

2 milyonluk ham verinin her 125.000’ lik parçasına aynı işlemlerin uygulanmasıyla oluşturulmuştur. Şekil 5.5 ve Şekil 5.6’ da önerilen yöntemin çalışma prensibi temsil edilmiştir.



Şekil 5.5 Ham verilere uygulanan mod işlemi



Şekil 5.6 Elde edilen verilerin 2’ lik tabana dönüştürülmesi

Bu aşamada elde edilen yeni veri setlerine uygulanan NIST istatistiksel testlerinin sonuçları Tablo 5.1, Tablo 5.2 ve Tablo 5.3’ te detaylı bir şekilde gösterilmiştir.

Tablo 5.1 Veri setlerinin (1-10) test sonuçları

	Veri1	**Veri2**	**Veri3**	**Veri4**	**Veri5**	**Veri6**	**Veri7**	**Veri8**	**Veri9**	**Veri10**
frekans testi	1	1	1	1	1	1	1	1	1	1
bloktaki en uzun birler testi	1	1	1	1	1	1	1	1	1	1
örtüşmeyen şablon eşleştirme testi	1	1	1	1	1	1	1	1	1	1
doğrusal karmaşıklık testi	1	1	1	1	1	1	1	1	1	1
birikimli toplamlar testi	1	1	1	1	1	1	1	1	1	1
blok frekans testi	1	1	1	1	1	1	1	1	1	1
rank testi	1	1	1	1	1	1	1	1	1	1
örtüşen şablon eşleştirme testi	1	1	1	1	1	1	1	1	1	1
seri testi	1	1	1	1	1	1	1	1	1	1
rastgele gezinim testi	0	0	1	0	1	0	1	0	1	1
akış testi	1	1	1	1	1	1	1	1	1	1
ayrık fourier dönüşüm testi	1	1	1	1	1	1	1	1	1	1
maurer' s evrensel testi	1	1	1	1	1	1	1	1	1	1
yaklaşık entropi testi	1	1	1	1	1	1	1	1	1	1
rastgele gezinim değişken testi	1	1	0	0	1	1	1	1	1	1
Toplam Başarı Sayısı	**14**	**14**	**14**	**13**	**15**	**14**	**15**	**14**	**15**	**15**

Tablo 5.2 Veri setlerinin (11-19) test sonuçları

	Veri11	**Veri12**	**Veri13**	**Veri14**	**Veri15**	**Veri16**	**Veri17**	**Veri18**	**Veri19**
	1	1	1	1	1	1	1	1	0
frekans testi									
bloktaki en uzun birler testi	1	1	1	1	1	1	1	1	1
örtüşmeyen şablon eşleştirme testi	1	1	1	1	1	1	1	1	1
doğrusal karmaşıklık testi	1	1	1	1	1	1	1	1	1
birikimli toplamlar testi	1	1	1	1	1	1	1	1	1
blok frekans testi	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1
rank testi									
örtüşen şablon eşleştirme testi	1	1	1	1	1	1	1	1	1
	1	1	1	1	1	1	1	1	1
seri testi									
rastgele gezinim testi	1	1	1	1	0	0	1	1	1
	1	1	1	1	1	1	1	1	1
akış testi									
ayrık fourier dönüşüm testi	0	1	1	1	1	1	1	1	1
maurer' s evrensel testi	1	1	1	1	1	1	1	1	1
yaklaşık entropi testi	1	1	1	1	1	1	1	1	1
rastgele gezinim değişken testi	1	1	0	1	1	1	1	1	1
Toplam Başarı Sayısı	**14**	**15**	**14**	**15**	**14**	**14**	**15**	**15**	**14**

Tablo 5.3 Test edilen verilerin p_değerleri

TESTLER	VERİLER		
	Veri5	**Veri9**	**Veri10**
frekans testi	P=0,1197	P=0,2644	P=0,0536
bloktaki en uzun birler testi	P=0,5725	P=0,9077	P=0,5391
örtüşmeyen şablon eşleştirme testi	P=0,7900	P=0,1831	P=0,5539
doğrusal karmaşıklık testi	P=0,8635	P=0,0251	P=0,4263
birikimli toplamlar testi	P=0,1537	P=0,3002	P=0,0535
blok frekans testi	P=0,5171	P=0,6282	P=0,1408
rank testi	P=0,7053	P=0,9603	P=0,1436
örtüşen şablon eşleştirme testi	P=0,2946	P=0,8186	P=0,2737
seri testi	P=0,6410	P=0,0747	P=0,3272
rastgele gezinim testi	P=0,6779	P=0,7999	P=0,6208
rastgele gezinim değişken testi	P=0,1245	P=0,3353	P=0,0462
akış testi	P=0,4205	P=0,7090	P=0,4828
ayrık fourier dönüşüm testi	P=0,3985	P=0,0862	P=0,0986
maurer' s evrensel testi	P=0,8511	P=0,3253	P=0,0455
yaklaşık entropi testi	P=0,4704	P=0,4867	P=0,6237

Tablo 5.3’ te; Veri5, Veri9 ve Veri10 isimli dizilerin NIST istatistiksel testleri başarıyla sonuçlanmıştır. Tablo 5.3’ teki p_değerleri incelendiğinde dizilerin tüm testleri başarılı bir şekilde sonuçlandırdığı görülmektedir. Bu testler sonucunda; tüm testleri geçen veri setlerimizin rastgele olduğu kanıtlanmıştır ve bu dizilerin, verilerin güvenliği için şifreleme algoritmalarında anahtar olarak kullanılabileceği sonucuna ulaşılmıştır.

5.2. Biyometrik Veriler

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler günlük hayatımızı büyük ölçüde dijitalleştirmektedir. Dijital varlığımıza yönelik en büyük tehditlerden biri bilgi güvenliğinin nasıl

sağlanacağıdır. Biyometrik verilere dayalı çözümler, bilgi güvenliğini sağlamak için son yıllarda daha yaygın hale gelmiştir. Tez çalışmasının bu bölümünde, kriptografik ilkelerin tasarımında biyometrik verilerin nasıl kullanılabileceğini gösteren bir yöntem önerilmiştir. Burada amaçlanan, beşinci bölümde Veri1 ve Veri2 dosyalarından elde edilen 17 farklı veri seti içerisinden hangi veri setlerinin kullanılabileceğine karar verilmesidir. Bu kararı vermek için biyometrik veriler kullanılacaktır. Biyometrik veriler, kişiye özel oldukları için rastgelelik kaynağı seçim süreci daha karmaşık bir hale getirilerek saldırgan yetenekleri azaltılmış olunacaktır.

Biyometrik özelliklere dayalı kriptografik protokoller, modern elektronik pasaportlar gibi kritik altyapı sistemlerinde, halk sağlığı sektöründe, mal ve hizmetlerin internet ortamında sunumunda bilgi güvenliği süreçlerinde bu tekniklerin kullanılmaya başlanmasından dolayı son on yılda daha fazla önem kazanmıştır. [15,16]

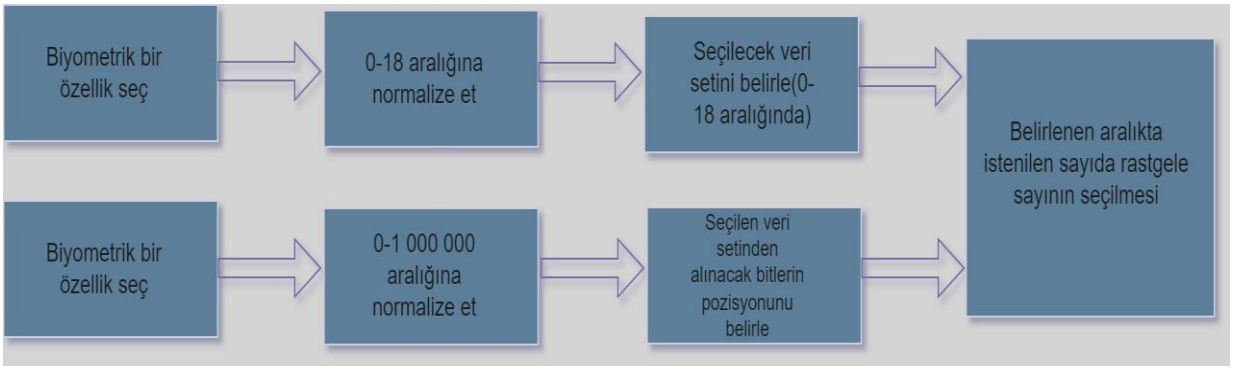
Önerilen yöntemin çıkış noktası, biyometrik verilerin tahmin edilemez güçlü özelliklere sahip olmasıdır. Biyometrik veriler kişiye özeldir. Genel bir tanımlama yapılacaksa biyometrik veriler, biyolojik organizmaları veya sistemleri analiz etmek için kullanılan bir tür veridir. Bu veriler spesifik biyolojik organizmaları tanımlamak için kullanılmıştır. Çalışmanın temel iddiası, biyometrik verilerin benzersiz özelliklerinin iyi bir entropi kaynağı olabileceğidir.

Biyometrik veri olarak önerilen yaklaşımda iris verileri kullanılmıştır. Çalışmada özellikleri Fisher' in makalesinde açıklanan en iyi bilinen veri setlerinden biri kullanılmıştır. Kullanılan veri setinde 150 örnek bulunmaktadır. Her örnek 4 sayısal nitelik içerir. Bu nitelikler çanak yaprağı uzunluğu, çanak yaprağı genişliği, taç yaprağı uzunluğu ve taç yaprağı genişliğidir. Özelliklerle ilgili istatistiksel bilgiler Tablo 5.4' te verilmiştir[17].

Tablo 5.4 İris veri özniteliklerinin istatistiksel özellikleri

Özellikler	Minimum	Maksimum	Ortalama
Çanak yaprak uzunluğu	4.3	7.9	5.84
Çanak yaprak genişliği	2.1	4.4	3.05
Taç yaprak uzunluğu	1.0	6.9	3.76
Taç yaprak genişliği	0.1	2.5	1.20

İris verilerinin bu dört özelliği, veriden üretilen veri setlerinden hangisinin seçileceğinin belirlenmesi için kullanılacaktır. Önerilen yöntemin akış diyagramı Şekil 5.7’ de basitçe verilmiştir.



Şekil 5.7 Önerilen yöntemin akış şeması

Algoritmanın adım adım çalışması aşağıda açıklanmıştır.

Adım1. Başlangıç koşullarını belirlemek için iris özelliklerinden biri seçilir.

Adım2. Seçilen özellik, Denklem 4.1' de verilen algoritmaya göre veri seti içerisinde hangi pozisyonun seçileceğine karar vermek için normalize edilir.

$$x_{normal} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{4.1}$$

Adım3. Kullanılacak veri setinin belirlenmesi için iris özelliklerinden biri seçilir.

Adım4. Seçilen özellik, Denklem 4.1' de verilen algoritmaya göre veri setinde bulunan bitlerin pozisyonuna göre normalize edilir.

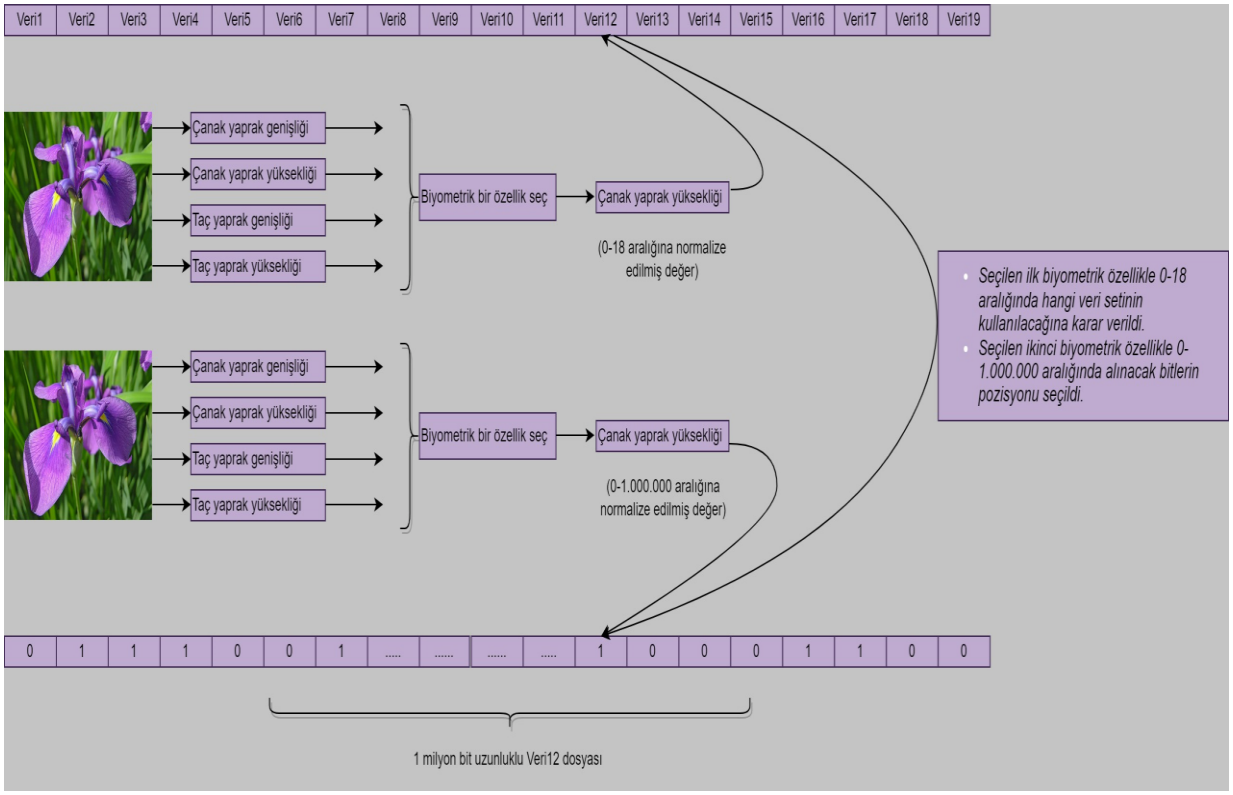
Bu tez çalışmasının amacı, biyometrik verilerin rastgelelik kaynağı olarak kullanılmasıdır. Biyometrik veriler, kişiye özel oldukları için iyi bir rastgelelik kaynağı olacaktır. Önerilen yöntemde biyometrik veri olarak iris verileri kullanılmıştır.

Çalışmada biyometrik verilerin kriptografik bir bileşen haline dönüştürülebileceği gösterilmiştir.

- Biyometrik özellikler, şifreleme algoritmasının gizli anahtarı olarak kullanılabilir.
- Anahtar alanı yeterince büyük yapmak için biyometrik özelliklerin sayısı artırılabilir (anahtar uzunluğu $>2^{128}$).
- Biyometrik veri toplamaktan kriptografik ekipman tasarlamaya kadar olan süreçte disiplinler arası işbirlikleri yapılabilir.
- En uygun biyometrik özelliklerin neler olabileceğini belirlemek için disiplinler arası bir çalışma yapılmalıdır.
- Geliştirilen biyometrik tabanlı kriptografik protokollerin uygulamaları kritik altyapı sistemlerinde uygulanarak bilgi güvenliği alanında kapsamlı ilerlemeler sağlanabilir.

Kullanılan GRSÜ donanımında 2 veri seti elde edilip son işlem teknikleriyle 2 milyon uzunluktaki veri setinden 19 milyon uzunluğunda yeni ver setleri elde edilmiştir. Cihazdan her aşamada yeni 2 milyon veri seti alınarak bu veri seti 19 milyon uzunluğuna çıkarılabilmektedir. Bu bölümde değinilen önemli nokta ise üretilen 19 veri seti içerisinden hangi veri setinin seçileceğine karar verileceğidir.

Bu tez çalışmasında iki tane biyometrik özellik seçilip birinci biyometrik özellik cihazdan elde edilen 19 tane veri setinden hangisinin seçileceğine karar vermek için kullanılmıştır. İkinci biyometrik özellik ise seçilen veri setinin hangi pozisyondan başlayarak rastgele sayıların alınacağını belirlemek için kullanılmıştır. Burada gerçekleştirilen normalizasyon işlemi 0-1 aralığı yerine 0-19 aralığında gerçekleştirilmiştir. Böylece var olan veri setlerinden hangisinin seçileceğine karar verilecektir. Şekil 5.8' de önerilen yönteme dair detaylı bir akış şeması gösterilmiştir.



Şekil 5.8 Önerilen yöntemin detaylandırılmış şeması

Tablo 5.5 0-18 aralığında normalize edilen değerler

Normalize edilmiş değerler	**İlgili veri seti aralığı**	**Normalize edilmiş değerler**	**İlgili veri seti aralığı**
4.48	Veri1	6.28	Veri11
4.66	Veri2	6.46	Veri12
4.84	Veri3	6.64	Veri13
5.02	Veri4	6.82	Veri14
5.20	Veri5	7.00	Veri15
5.38	Veri6	7.18	Veri16
5.56	Veri7	7.36	Veri17
5.74	Veri8	7.54	Veri18
5.92	Veri9	7.72	Veri19
6.10	Veri10		

Tablo 5.6 0-256 aralığında normalize edilmiş değerler

Normalize edilmiş değerler	**İlgili bit pozisyonu**	**Normalize edilmiş değerler**	**İlgili bit pozisyonu**
4.31	0	6.77	247
4.32	1	6.78	248
4.33	2	6.79	249
4.34	3	6.80	250
4.35	4	6.81	251
4.36	5	6.82	252
4.37	6	6.82	253
4.38	7	6.83	254
4.39	8	6.84	255
4.40	9	6.85	256

Şekil 5.8’ de gösterilen akış şeması dikkate alınarak ilk biyometrik özellik olan çanak yaprak yüksekliği seçilerek veri setine karar verilmiştir. Bu aşamada örnek bir uygulama gerçekleştirmek için çanak yaprak yüksekliği değeri 6.46 olarak seçilmiştir. Tablo 5.5’ te bu değere karşılık gelen veri seti Veri12 dosyasıdır. Burada ilk özellik seçimi sonucunda Veri12 dosyasının kullanılacağına karar verilmiştir. İkinci biyometrik özellik olarak yine çanak yaprak yüksekliği olarak 6.79 değeri seçilmiştir. Seçilen bu özelliğe karşılık gelen pozisyon değeri Tablo 5.6’ da 249 olarak hesaplanmıştır. Yapılan karar işlemlerinden sonra Veri12 dosyasından 249. pozisyondan itibaren

istenilen uzunlukta bit dizisi seçme işlemi yapılmıştır. Seçilen bit dizisinin istatistiksel testlerinin gerçekleştirilmesi için bir milyon uzunluğunda veri seti seçilmiştir. Veri setini 1 milyon uzunluğuna tamamlamak için bir sonraki veri seti olan Veri13 dosyasından yeterli sayıda veri alınmıştır. Yapılan seçimler sonucunda oluşturulan yeni veri setinin NIST test sonuçları Tablo 5.7' de gösterilmiştir.

Tablo 5.7 Elde edilen yeni veri setinin NIST test sonuçları

Testler	**P değerleri**
frekans testi	P=0.0197
bloktaki en uzun birler testi	P=0.08095
örtüşmeyen şablon eşleştirme testi	P=0.4795
doğrusal karmaşıklık testi	P=0.2637
birikimli toplamlar testi	P=0.0361
blok frekans testi	P=0.3255
rank testi	P=0.1431
örtüşen şablon eşleştirme testi	P=0.8708
seri testi	P=0.9866
rastgele gezinim testi	P=0.4430
rastgele gezinim değişken testi	P=0.5436
akış testi	P=0.9390
ayrık fourier dönüşüm testi	P=0.3492
maurer' s evrensel testi	P=0.7009
yaklaşık entropi testi	P=0.1688

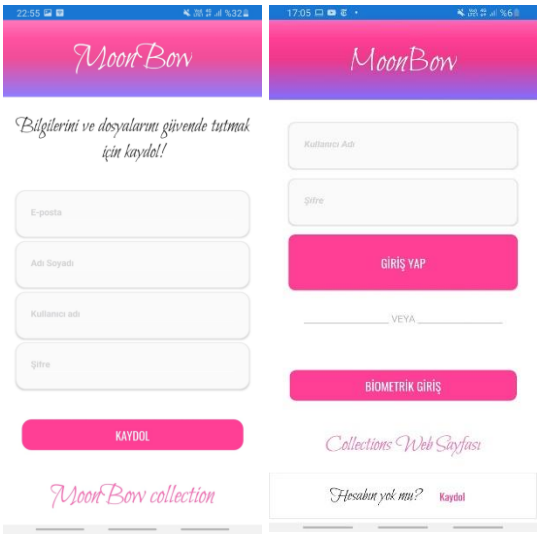
Elde edilen NIST test sonuçları incelendiğinde ilk seçilen biyometrik özellik yardımıyla belirlenen Veri12 dosyası ve ikinci seçilen biyometrik özellik olan 6.79 değeriyle bu dosyadan alınacak bitlerin pozisyonunun belirlenmesi sonucunda oluşturulan yeni veri setinin tüm testleri

başarıyla geçtiği gözlemlenmiştir. Tüm testleri başarıyla geçen bu yeni veri setinin rastgeleliği kanıtlanmış olup kriptografik uygulamalarda anahtar olarak kullanılabileceği sonucuna ulaşılmıştır.

5.3. Mobil Uygulama

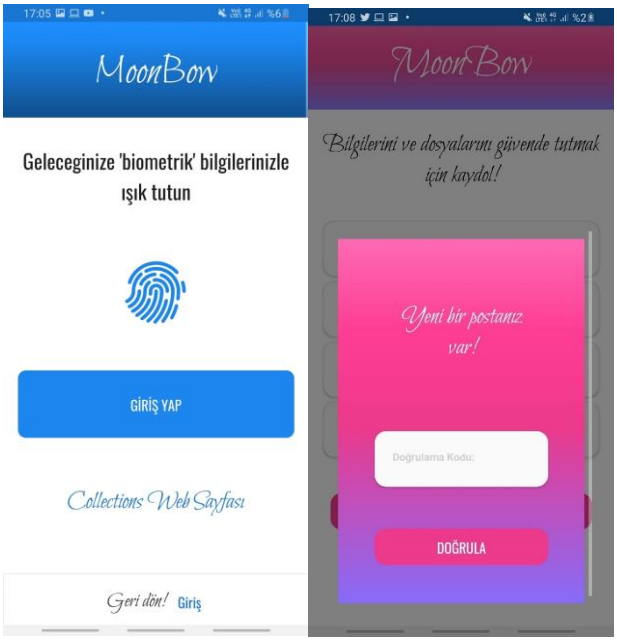
Beşinci bölümde elde edilen çıktılarla geliştirilen mobil uygulamaya dair detaylara aşağıda değinilmiştir.

- Web ve mobil platformlarda kullanıcılara hizmet sağlanacak.
- Mobil uygulamayla kayıt yapılacak.
- 3 Adımlı doğrulama servisi ile sisteme giriş yapılacak.
  Kendi belirlediği klasik şifre
  E- posta ile doğrulama kodu
  Biyometrik bilgiler
- Uygulama içerisinde şifrelenmek istenen veriler (Ses, resim, video, fotoğraf ve metinler) servise kayıt edilecek.
- Kaydedilmesi istenen veriler kaydedilmeden önce şifrelenerek güvence altına alınacak.
- Kişisel Verileri Koruma Kanunu (KVKK) ile birlikte paralel bir işlem sürdürülecek.

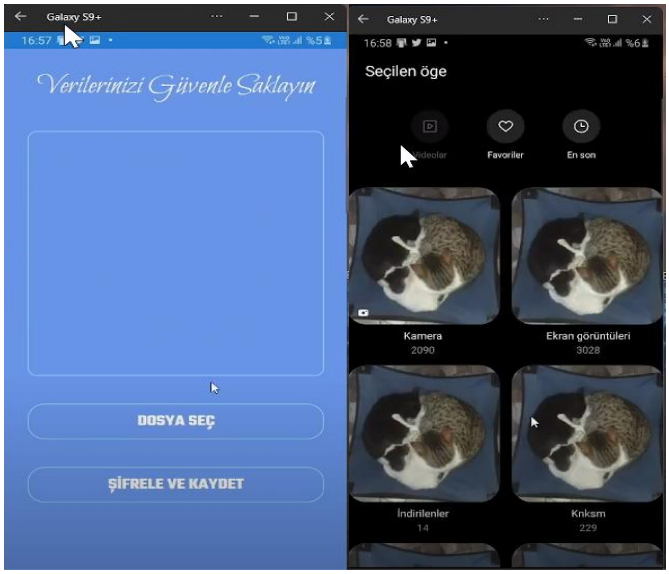


Şekil 5.9 Kayıt ve Giriş sayfası

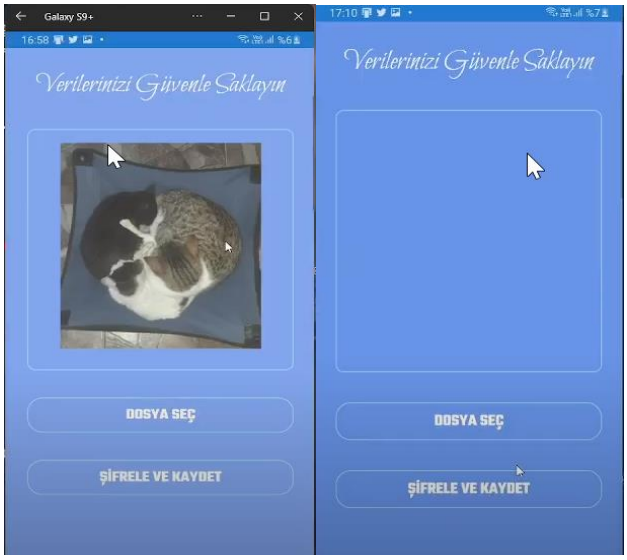
Şekil 5.9' da geliştirilen uygulamaya ait Kayıt ve Giriş, Şekil 5.10' da Biyometrik ve E-posta doğrulama ekranlarına ait görsellere yer verilmiştir.



Şekil 5.10 Biyometrik ve e-posta doğrulama sayfası



Şekil 5.11 Şifrelenecek verinin seçilmesi



Şekil 5.12 Seçilen verinin şifrelenmesi

Şekil 5.11’ de şifrelenecek verinin seçilme aşaması ve Şekil 5.12’ de seçilen verinin şifrelenmiş hali gösterilmektedir.

6. SONUÇLAR

Bilgi güvenliğinde özellikle 2020 yılında yaşanan Covid pandemisi sonrasında alışkanlıklarımızın giderek dijitalleştiği bir dönem yaşanmıştır. İnsanlar bu dönemde birçok işini uzaktan bağlantılar ile gerçekleştirmişlerdir. Bu süreç içerisinde en önemli problemlerden bir tanesi de güvenlik endişeleridir. Zoom adlı uygulamayı daha önceden çok az kişi kullanırken pandemi sebebiyle bu sayının artması dolayısıyla açığa çıkan güvenlik problemleri bu dönemin popüler konusu haline gelmiştir. Hayatlarımızın dijitalleştiği bu dünyada verileri güvenle korumak, iletmek ve depolamak için bir çalışma gerçekleştirilmiştir. Rastgelelik, kriptolojik uygulamalarda [18-19] en temel gereksinimlerden biri olduğundan, bu ihtiyacı karşılamak için birçok araştırma yapılmış ve birçok ticari ürün geliştirilmiştir [19-20]. Tez çalışmasında, piyasada bulunan GRSÜ donanımının kriptografik amaçları sağlamadığı analiz edilmiştir. Elde edilen NIST test sonuçlarıyla elde edilen analiz doğrulanmıştır.

Tez çalışmasında ilk defa bir son işlem tekniği önerilmiştir. Bu son işlem tekniği sayesinde GRSÜ olan donanımdan elde edilen 2 milyon bit 19 milyon uzunluğunda veriye dönüştürülmüştür. Burada yalnızca veri çoğaltma işlemi yapılmamıştır aynı zamanda verinin istatistiksel özelliklerinin de iyileştirildiği gözlemlenmiştir. Elde edilen test sonuçları incelendiğinde 19 veriden 11 tanesinin tüm testleri geçtiği sonucuna ulaşılmıştır. İyileştirilen verilerin kriptografik uygulamalarda kullanılmak üzere anahtar olarak kullanılmasını amaçlayan çalışmada biyometrik veriler yardımıyla hangi veri setinin kaçıncı pozisyondan itibaren seçileceğine karar verilerek yeni bir veri seti elde edilmiştir. Elde edilen bu yeni veri setinin NIST istatistiksel test sonuçları incelendiğinde tüm testleri başarıyla tamamlayan veri setinin güvenliği kanıtlanmış olup kriptolojik uygulamalarda anahtar olarak kullanılabileceği sonucuna ulaşılmıştır.

Yalnızca bir son işlem algoritması önermekle de kalınmamış aynı zamanda elde edilen bu sonuçlar mobil bir uygulamaya entegre edilmiştir. Mobil uygulamaya entegre edilmesi aşamasında kişisel verilerin eklenmesi sistemi tahmin edilemez bir yapıya dönüştürmüştür. Tüm bu sonuçların ileride pratik uygulamalarda farklı amaçlarla başarılı bir şekilde kullanılabileceği düşünülmektedir.

KAYNAKLAR

[1] W. Schindler, (2009). Random number generators for cryptographic applications, C .K. Koc (ed.): Cryptographic Engineering. *Springer, Signals and Communication Theory*, Berlin

[2] C. Paar, J. Pelzl, (2010). Understanding Cryptography A Textbook for Students and Practitioners, *Springer Heidelberg Dordrecht*, London New York

[3] M. Stipčević and Ç. K. Koç, (2014). True random number generators, in Koç Ç. K. (eds) *Open Problems in Mathematics and Computational Science. Springer*, Cham

[4] F. Özkaynak, (2014). Cryptographically secure random number generator with chaotic additional input, *Nonlinear Dyn 78*, 2015–2020

[5] Dworkin, Morris J., (2015). SHA-3 standard: Permutation-based hash and extendable-output functions.

[6] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, A statistical test suite for random and pseudorandom number generators for cryptographic applications, *NIST Special Publication*, Report no. 800–22rev1a, 2010s

[7] Federal Information Processing Standard (FIPS); ISO/IEC 19790; ISO/IEC 24759

[8] A. M., Garipcan, E. Erdem, (2020). A GRSÜ using chaotic entropy pool as a post-processing technique: analysis, design and FPGA implementation, *Analog Integr Circ Sig Process* 103, 391–410

[9] Krhovjak, J., (2009). *Crytographic random and pseudorandom data generators*, Dissertation Thesis, Fakulty of İnformatics Masaryk University

[10] https://www.crowdsupply.com/13-37/infinite-noise-GRSÜ

[11] A. S. Muhammad, F. Özkaynak, (2021). SIEA: Secure Image Encryption Algorithm Based on Chaotic Systems Optimization Algorithms and PUFs, *Symmetry*

[12] J. Kong and F. Koushanfar, (2014). Processor-Based Strong Physical Unclonable Functions With Aging-Based Response Tuning, *in IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 1, pp. 16- 29

[13] F. Özkaynak, (2020). A Novel Random Number Generator Based on Fractional Order Chaotic Chua System. *Elektronika Ir Elektrotechnika*, 26(1), 52-57

[14] Y. Burhan, F. Artuger and F. Özkaynak, (2019). A novel hybrid image encryption algorithm based on data compression and chaotic key planning algorithms, *Proc. 7th Int. Symp. Digit. Forensics Secur. (ISDFS)*, pp. 1-5

[15] Jakimoski, G., Kocarev, L., (2001). Chaos and cryptography: block encryption ciphers, *IEEE Trans Circ Syst*—I. 48(2), 163– 169

[16] Faiz ul Islam, Guangjie Liu, (2017). Designing S-Box Based on 4D-4Wing Hyperchaotic System, 3D Research, March 2017, 8:9

[17] Fisher,R.A. The use of multiple measurements in taxonomic problems, Annual Eugenics, 7, Part II, 179-188 (1936); also in "*Contributions to Mathematical Statistics"* (John Wiley, NY, 1950)

[18] I. Hussain, T. Shah, H. Mahmood, M. Asif Gondal, Construction of S8 Liu J S-boxes and their applications, *Computers & Mathematics with Applications*, Volume 64, Issue 8, October 2012, Pages 2450–2458

[19] F. Özkaynak, S. Yavuz, (2013). Designing chaotic S-boxes based on time-delay chaotic system, *Nonlinear Dynamics*, Volume 74, Issue 3, pp 551–557

[20] M. Khan, T. Shah, M. Asif Gondal, (2013). An efficient technique for the construction of substitution box with chaotic partial differential equation, *Nonlinear Dynamics*, Volume 73, Issue 3, pp 1795– 1801

ÖZGEÇMİŞ

Beyzanur DURMUŞ

KİŞİSEL BİLGİLER

Doğum Yeri	**: Elazığ**
Doğum Yılı	**:** 1994
Uyruğu	**:** TC
Adres	**:** F.Ü Teknoloji Fakültesi Yazılım Mühendisliği Bölümü 23100 Elazığ/Merkez
E-posta	**:** bdurmus@firat.edu.tr
Yabancı Diller	**:** İngilizce(Düzey: 68)

ARAŞTIRMACI BİLGİLERİ

Öğrenci Orcid ID	**:** 0000-0002-7732-8421
Danışman Orcid ID	**:** 0000-0003-1292-8490

EĞİTİM BİLGİLERİ

Lisans	**:** Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, 2018
Lise	**:** Cumhuriyet Lisesi, Elazığ, 2013

ARAŞTIRMA DENEYİMİ

- ✓ Java, C++, C#, MATLAB

İŞ DENEYİMİ

2022 – devam ediyor	**:** Fırat Üniversitesi (Araştırma Görevlisi)

AKADEMİK FAALİYETLER

Bildiriler:

1. B. Durmus and F. Ozkaynak, "*Analysis of Cryptographic Randomness Properties of a TRNG-based Key Generator Hardware*," 2022 IEEE 16th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2022, pp. 01-04, doi: 10.1109/TCSET55632.2022.9766939.

Projeler:

1. 120E444 protokol numaralı Kaotik Entropi Kaynakları ve Optimizasyon Algoritmaları Kullanılarak Gürbüz Anahtar Üreteçlerin Tasarımı ve Mobil Platformlar İçin Pratik Uygulamaların Geliştirilmesi