KABLOSUZ SENSÖR AĞLARININ GÜVENLİĞİNİ SAĞLAMADA HAFİF KRİPTOGRAFİNİN KULLANILMASI

DİLAN KARATAŞ

HAZİRAN 2024

DİYARBAKIR

DİCLE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KABLOSUZ SENSÖR AĞLARININ GÜVENLİĞİNİ SAĞLAMADA HAFİF KRİPTOGRAFİNİN KULLANILMASI

DİLAN KARATAŞ

DİCLE ÜNİVERSİTESİ LİSANSÜSTÜ EĞİTİM-ÖĞRETİM VE SINAV YÖNETMELİĞİNİN BİR PARÇASI OLARAK
ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANA BİLİM DALINDA
YÜKSEK LİSANS TEZİ
OLARAK HAZIRLANMIŞTIR

HAZİRAN 2024

DİYARBAKIR

KABLOSUZ SENSÖR AĞLARININ GÜVENLİĞİNİ SAĞLAMADA HAFİF KRİPTOGRAFİNİN KULLANILMASI

Dilan KARATAŞ tarafından Dicle Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin bir parçası olarak hazırlanan bu çalışma, aşağıda bilgileri yazılı jüri üyeleri tarafından değerlendirilerek **Elektrik Elektronik Mühendisliği Ana Bilim Dalı**'nda **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Prof. Dr. Neslihan DALKILIÇ _____
Müdür, **Fen Bilimleri Enstitüsü**

Dr. Öğr. Üyesi Muhittin BAYRAM _____
Danışman, **Elektrik Elektronik Mühendisliği Bölümü, Dicle Üniversitesi**

Sınav Jürisi:

Dr. Öğr. Üyesi Zehra URAL BAYRAK **(*)** _____
Havacılık Elektrik ve Elektroniği Bölümü,
Fırat Üniversitesi

Dr. Öğr. Üyesi Muhittin BAYRAM **(**)** _____
Elektrik Elektronik Mühendisliği Bölümü,
Dicle Üniversitesi

Doç. Dr. Muhammet Ali ARSERİM _____
Elektrik Elektronik Mühendisliği Bölümü,
Dicle Üniversitesi

ONAY

Savunma Tarihi: 25 / 06 / 2024

(*) Jüri Başkanı.
(**)Tez Danışmanı.

Anneme ve Babama…

Dicle Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırlanan bu tez çalışmasında yer alan tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu beyan ederim. Ayrıca, bahse konu bu kural ve ilkelerin gerektirdiği üzere, bu çalışmada özgün olmayan tüm bilimsel içerikleri kurallara uygun biçimde alıntılayıp kaynak gösterdiğimi beyan ederim. Beyanımla çelişen herhangi bir delil bulunduğu takdirde tüm sorumluluğu üstleneceğimi kabul ederim.

Ad, Soyad: Dilan KARATAŞ

İmza: …….……

TEŞEKKÜR

Öncelikle danışmanım Dr. Öğr. Üyesi Muhittin BAYRAM'a çalışmanın daha fikir aşamasından, örnekleme, analizlerin yorumlanması ve tez taslağındaki düzeltmeler konularına kadar gösterdikleri destek ve sabırdan dolayı teşekkür ederim. Jüri üyelerime de bu tezin daha nitelikli bir hale gelmesi için yaptıkları eleştiri ve önerileri için teşekkür ederim.

Tezin her aşamasındaki yardımları ve yol göstericiliği için Doç. Dr. M. Ali ARSERİM hocama çok teşekkür ederim.

En önemlisi, beni araştırma hevesiyle coşturdukları ve kendime bazı zamanlar inanmasam da bana inandıkları için anneme ve babama teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

SİMGELER VE KISALTMALAR LİSTESİ

Simge	**Açıklama**
GHz	Gigahertz
MHz	Megahertz
Gbps	Gigabit per second
kgate	kilogate
mW	Miliwatt
μW	Mikrowatt

Kısaltma	**Açıklama**
AES	Gelişmiş Şifreleme- Standartı-Advanced Encryption Standard
IoT	Nesnelerin İnterneti-Internet of Things
RFID	Radyo Frekansı Tanımlama-Radio Frequency Identification
Wi-Fi	Kablosuz Bağlantı Alanı Wireless Fidelity
KAA	Kablosuz Algılayıcı Ağları- Wireless Sensor Networks construction et Ouvrages
NIST	Ulusal Standartlar ve Teknoloji Enstitüsü-National Institute of Standards and Technology
WSN	Kablosuz Sensör Ağı- Wireless Sensor Network
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü-Institute of Electrical and Electronics Engineers
FPGA	Field Programmable Gate Arrays- Sahada programlanabilir kapı dizisi

ÖZET

KABLOSUZ SENSÖR AĞLARININ GÜVENLİĞİNİ SAĞLAMADA HAFİF KRİPTOGRAFİNİN KULLANILMASI

KARATAŞ, Dilan
Yüksek Lisans, Elektrik Elektronik Mühendisliği Bölümü
Danışman: Dr. Öğr. Üyesi Muhittin BAYRAM
Haziran 2024, 63 sayfa

Teknolojik değişimlerle birlikte internet de hızlı bir şekilde değişim göstermektedir. İnternet yalnızca insanların birbirlerine bağlanması değil bilakis cihazlarında birbirine bağlanmasında oldukça etkili olmaya başlamıştır. Özellikle son yıllarda hızla yaygınlaşan Nesnelerin İnterneti teknolojisi ile daha da gelişen kablosuz haberleşme cihazları, sensör ağları, akıllı kartlar, uzaktan kumanda sistemleri RFID (Radyo Frekanslı Kimlik Belirleme Aletleri) etiketleri gibi kısıtlı cihaz denilen, düşük işlem yeteneğine sahip ve az enerji tüketmesi gereken cihazların kullanımı yaygınlaşmaktadır. Mevcut geleneksel algoritmaların bu kısıtlı cihazlara uygulanması performans ve güvenlik açısından zor olduğu bilinen bir gerçektir. Bu bağlamda, bu cihazların özel algoritmalara ihtiyaçları vardır. Bu sınırlamalar göz önünde bulundurularak tasarlanan kriptografik algoritmalara "hafif algoritmalar", bu algoritmaların tasarlanması çalışmalarına da "hafif kriptografi" denmektedir. Kriptografi, en yalın ifadeyle yetkisiz erişimi engellemek için mesaj ve verilerin gizlenmesidir. Kriptografinin kullanımı çok eskilere dayanır ve veri güvenliğinde oldukça önemlidir. Hafif kriptografik algoritmalar çok daha az güç ve çok daha sınırlı devreler kullandığından bu tür cihazlarda kullanılmıştır. Geleneksel kriptografik algoritmaların çoğu bilgisayar ve sunucular için tasarlanmış kısıtlı cihazlarla uyum sağlamamaktadır. Hafif kriptografi algoritması bir taraftan daha küçük bir veri işlem gücü kullanırken diğer taraftan onu güvence altına alabilmek için bir prosedür uygular. Hafif kriptoloji algoritmaları, klasik yöntemlerle karşılaştırıldığında daha temel döngü ve daha az işlem yoğunluklarına sahiptir. Hafif blok şifrelerde ise, daha çok algoritma vardır. Bu algoritmaların çokluğuna ve bir kısmının verimliliğine rağmen, hafif kriptografi algoritmalarında aynı zamanda kısıtlı cihazların özelliklerini de dikkate almak gerekir. Gerekli güvenlik seviyesini elde etmek daha zor olduğundan dolayı daha seçici ve iyi algoritma ve çözüm yolları geliştirmeye ve aramaya ihtiyaç duyulmaktadır. Bu çalışmada, kablosuz sensör ağlarının güvenliğinde kullanılan hafif kriptografik algoritmalar üzerinde durulacak ve performans açısından karşılaştırılacaktır.

Anahtar Kelimeler: Kablosuz Sensör Ağları, Hafif Kriptografi, Ağ Güvenliği

ABSTRACT

USING LIGHTWEIGHT CRYPTOGRAPHY TO SECURE WIRELESS SENSOR NETWORKS

KARATAŞ, Dilan
Master of Science in Department of Electrical and Electronics Engineering
Supervisor: Ass. Prof. Dr. Muhittin BAYRAM
June 2024, 63 pages

Along with technological changes, the internet is also changing rapidly. The Internet has become very effective not only in connecting people to each other, but also in connecting devices to each other. Especially with the Internet of Things technology, which has become widespread rapidly in recent years, the use of devices with low processing capability and low energy consumption, called constrained devices, such as wireless communication devices, sensor networks, smart cards, remote control systems RFID (Radio Frequency Identification Devices) tags, is becoming widespread. It is a known fact that it is difficult to apply existing traditional algorithms to these constrained devices in terms of performance and security. In this context, these devices need specialized algorithms. Cryptographic algorithms designed with these limitations in mind are called “lightweight algorithms” and the design of these algorithms is called “lightweight cryptography”. Cryptography, in the simplest terms, is the concealment of messages and data to prevent unauthorized access. The use of cryptography goes back a long time and is very important in data security. Lightweight cryptographic algorithms have been used in such devices because they use much less power and much more limited circuitry. Most traditional cryptographic algorithms are not compatible with the limited devices designed for computers and servers. A lightweight cryptography algorithm uses a smaller data processing power on the one hand, and implements a procedure to secure it on the other. Lightweight cryptography algorithms have more basic cycles and lower computational intensities compared to classical methods. In lightweight block ciphers, there are more algorithms. Despite the multiplicity of these algorithms and the efficiency of some of them, lightweight cryptography algorithms also need to take into account the characteristics of constrained devices. Since it is more difficult to achieve the required level of security, there is a need to develop and search for more selective and better algorithms and solutions. In this paper, we focus on lightweight cryptographic algorithms used in the security of wireless sensor networks and compare them in terms of performance.

Keywords: Wireless Sensor Networks; Lightweight Cryptography; Network Security

1. GİRİŞ

Bu tez çalışmasında, kablosuz sensör ağlarının güvenliğini sağlamada kullanılan hafif kriptografik algoritmalar araştırılacaktır Teknolojik yenilikler ivmelenerek artmaktadır. Bu ivmelenme ile internette değişime uğramıştır. İnternet, ilk önce insanları birbirine bağlama görevi görürken şimdi cihazları birbirine bağlamakta kullanılmaktadır. Bu entegrasyon bağlamında, cihazların bağlantılarını tanımlamak için Nesnelerin İnterneti (IoT) kavramı kullanılmaktadır. Bu cihazlardan bazılarına örnek vermek gerekirse; masaüstü ve taşınabilir bilgisayarlar ile tabletler gibi güçlü bilgi işlem cihazları olduğu gibi kablosuz sensör ağları ve RFID gibi kaynakları kısıtlı cihazlar da yer alabilmektedir. Bu bağlamda, hafif algoritmalar sınıfında yer alan kısıtlı cihazların özel tasarlanmış algoritmalara ihtiyacı bulunmaktadır.

Günümüzde şifreleme, haberleşmede, cep telefonlarında, bankacılık sistemlerinde, iş ve kamu web sitelerinde, sağlık sistemlerinde ve bunun gibi birçok alanda, hizmet ve uygulamalarda kullanılmaktadır. Simetrik algoritma, şifreleme ve şifre kırmada aynı anahtarın kullanılması anlamına gelmektedir. Asimetrik algoritma ise şifreleme için açık anahtar ve şifre kırma için özel anahtar olmak üzere iki anahtarın kullanılması anlamına gelmektedir. Hafif kriptoloji algoritmaları genellikle 128 bit blok uzunluklarından daha kısa verileri yine 128 bit'ten daha kısa anahtar büyüklükleriyle şifrelemeye yararlar. Hafif kriptografi için sahip olduğumuz ana kısıtlamalar, güç gereksinimleri, kullanılan kapı miktarı ve zamanlamayla yakından ilgilidir. Bir RFID cihazının zamanlama gereksinimleri ve kullanılan kapı sayısının sınırlandırılmasının yanında, herhangi bir şifreleme işleminde güç tüketiminde ciddi şekilde kısıtlanması muhtemeldir. RFID cihazı bir pile sahip olsa dahi, pilin yeniden şarj edilmesi zordur ve bundan dolayı güç tüketimi en aza indirilmelidir.

Birçok IoT cihazı gerçek dünyada fiziksel olarak erişilebilir olduğundan ve çoğunun enerji, bellek, işlem gücü ve hatta fiziksel alan gibi kaynakları sınırlı olduğundan ötürü IoT dağıtımlarında güvenlik bir numaralı zorluk olarak kabul edilmektedir. Bu kaynak kısıtlılığından dolayı RFID etiketleri, sensörler, akıllı kartlar gibi IoT cihazlarına odaklanılmıştır. Bu cihazlardan gelen iletişim, kriptografinin daha hafif bir sürüm olan hafif kriptografi ile güvence altına alınabilmektedir. Belirli uygulamalara odaklanan birçok hafif kriptografi yani düz şifreleme algoritması piyasada bulunmaktadır. Alana

bütüncül bir bakış sağlamak için, bu çalışmada mevcut algoritmalar donanım performansları açısından karşılaştırılmıştır.

Çalışmanın bu bölümünde, kablosuz sensör ağları, ağ güvenliği ve hafif kriptografi ile ilgili temel açıklamalar yapılmıştır. İkinci bölümde, bu çalışmayla ilgili olan literatür taraması kronolojik bir şekilde verilmiştir. Her bir çalışmaya ilişkin özet bilgiler sunulmuştur. Üçüncü bölümde, malzeme ve yöntem olarak kriptografi ele alınmış ve gerekli tanımlama ve açıklamalar yapılmıştır. Dördüncü bölümde ise bulgular ve tartışma kapsamında gerekli analizler yapılmış ve raporlanmıştır. Son olarak beşinci bölümde ise sonuç ve önerilere değinilmiştir.

2. ÖNCEKİ ÇALIŞMALAR

Bu bölümde, çalışmamızı teşkil edecek literatür taraması kronolojik bir şekilde ele alınacaktır.

Sun ve arkadaşları, Doğrusal Uyumlu Jeneratöre (LCG) dayalı olarak, kaynakları kısıtlı kablosuz sensör ağları için hafif güvenli protokol bir blok şifreleme oluşturmaya uygun yeni bir blok şifreleme önermişler. Plumstead'in çıkarım algoritması, bilinmeyen parametrelere sahip bir LCG için modülün boyutunu arttırmak sistemin güvenliğini basit bir şekilde önemli ölçüde artırmanın imkânsız olduğunu göstermektedir. Bu nedenle, güvenliği sağlamak amacıyla oluşturulan sözde rastgele sayıları sensör veri mesajlarına yerleştirmeye istekli oldukları görülmüştür. Şifrenin analizi, kablosuz sensör ağlarının güvenlik gereksinimlerini karşılayabildiğini göstermektedir. Önerilen şifre temel alan güvenli protokoller temel güvenlik gereksinimlerini karşılar. Performans analizi, temel işlem sayısı açısından kablosuz sensör ağlarındaki önerdikleri şifre blok şifrenin yaygın olarak kullanılan RC5'ten daha hafif olduğunu göstermektedir [1]. Koo ve arkadaşları, çalışmalarında, kablosuz sensör ağları için her yerde bulunan 8 bitlik bilgi işlem cihazlarına (örneğin sensör düğümü veya RFID etiketi) uygun olarak tasarlanmış başka bir aday HIGHT'ı ele almışlardır [2].

AlDabbagh ve Shaikhli, araştırmalarında hafif blok şifrelemeyi saat döngüsü sayısı, bellek boyutu, seçilen düz metin sayısı, düz metin kapısı eşdeğerliği (GE), verim ve saldırılar gibi birçok yönde geliştirmek için başlangıç noktası olabiliceği iddia edilmiştir [3]. Manjulata, sensör tabanlı ağların düşük maliyeti ve kısıtlı kaynak gereksinimi nedeniyle birçok güvenlik uygulaması için hafif kriptografik ilkelerin kullanılmasına güçlü bir ihtiyaç olduğunu belirtmişlerdir [4]. Pate ve Mistry, WSN'ler şu alanlarda konuşlandırıldığında erişilemeyen alanlarda, farklı saldırı türlerinin meydana gelme olasılığı çok yüksektir. Açık anahtar kriptografisi, anahtar hesaplama maliyetleri, daha uzun anahtarlar, kaba kuvvet saldırılarına karşı anahtar savunmasızlığı, anahtar dağıtımı ve bakımı gibi sorunlar nedeniyle WSN için tercih edilmemektedir. Çok kısa anahtar uzunluğuna sahip (hafif) simetrik anahtar kriptografisinin daha az hesaplama ve düşük bellek gereksinimi, bilgi güvenliğini sağlamak için WSN'de kullanımını haklı çıkarmaktadır [5].

Bragadeesh ve Umamakeswari, veri birleştirmenin, ağ içi işleme, iletişim ek yükünü azaltma, gereksiz paket iletimlerini ortadan kaldırma ve ağın ömrünü uzatma gibi yetenekler sağlayan bir süreç olduğunu savunurlar. Çalışmalarında, kaynak kısıtlı ağlar için uygun olan hafif kriptografik ilkeleri kullanarak güvenli veri toplamayı uygulamak için bir yöntem önerilmiştir [6]. Tawalbeh ve arkadaşları, Kablosuz Sensör Ağları (WSN'ler) bireysel ve kurumsal düzeyde birçok kullanım ve uygulama alanına sahip olduğunu belirtmişlerdir. Sensörler sağlık, trafik, tarım, endüstri ve daha birçok alana entegre edilebilir. Birçok durumda hayati bilgilerin iletilmesini içeren bu etkileşim, bu verilerin olası saldırılara karşı güvenli hale getirilmesi ihtiyacını doğurmaktadır. Ancak kablosuz sensör ağlarında iletişimin güvenliğini sağlamak, WSN'lerdeki bileşenlerin genellikle sınırlı hesaplama ve güç kapasitesine sahip olması nedeniyle yüksek performans maliyetine neden olmaktadır [7]. Nino ve arkadaşları, operasyonel kısıtlamalar sensör düğümlerinde küçük uygulama boyutuna ve düşük güç tüketimine sahip güvenlik ilkelerini talep etmekte olduğunu belirtmişlerdir. Elde edilen deneysel sonuçlardan, hafif şifrelerin uygulama alanını ve enerji tüketimi ek yüklerini azaltmaya ve sensör düğümünün ömrünü uzatmaya nasıl önemli ölçüde katkıda bulunduğu gösterilmiştir [8].

Khashan ve arkadaşları, Kablosuz Sensör Ağlarında (WSN'ler) güvenlik, verimlilik ve enerji tüketimi, açık, büyük ölçekli ve kaynak kısıtlı doğası nedeniyle hala büyük zorluklar olduğunu savunurlar. Sonuçlar, önerilen şemanın sabit şifreleme parametreleri kullanan diğer şifrelere kıyasla güç tüketimi ve ağ ömrüne ek olarak gecikme ve şifreleme süresi açısından önemli bir gelişme sağladığını kanıtlamaktadır [9]. Khan ve arkadaşları, anketlerinde IoT yapısını, uç, sis ve bulut platformlarındaki cihazların hesaplama yeteneklerini tanımlamakta ve mevcut hafif kriptografik protokolleri sınıflandırmaktadırlar. Mevcut hafif kriptografik çözümlerin avantajları, dezavantajları ve güvenlik açıkları ile birlikte karşılaştırmalı analizi, IoT sistemlerindeki farklı düğümlerin asimetrik yeteneklerine uyum sağlayabilen elastik kriptografik protokollere olan ihtiyacı vurgulamaktadır [10]. Thakor ve arkadaşları, belirli uygulamalara odaklanan kırktan fazla hafif kriptografi (düz şifreleme) algoritması piyasada mevcuttur ve araştırmacılar tarafından yakın zamanda NIST yarışmasına 57 algoritma daha sunulduğunu söylemişlerdir [11]. Rana ve arkadaşları, ileri teknolojinin gelişmesiyle birlikte IoT, büyük hacimlerde veri toplayabilen çok

sayıda cihazın bağlanmasını mümkün kıldığını iddia etmişlerdir. Bu nedenle, IoT güvenliğine yönelik talepler son derece önemlidir [12].

İbrahim ve arkadaşları, kablosuz ve internet ağlarını kullanan insan sayısı gün geçtikçe arttığını ve bunun da cihazlar için şifreleme mekanizmalarını geliştirmekte ve güvenli olmayan bir ağ üzerinden kullanıcı veri aktarımını koruduğunu iddia etmektedirler. Çoğu taşınabilir cihaz için sınırlı kaynaklar nedeniyle, her yerde bilişim kavramı, Gizlilik, Bütünlük, Kimlik Doğrulama ve inkar etmemeyi içeren güvenlik çalışmalarıdır. Hafif kriptografi tasarımı, geleneksel kriptografi ile donanım uygulaması için çok sayıda sorunu çözmüştür [13]. Tsantikidou ve Sklavos ancak IoT, yüksek seviyeli güvenlik şemalarının uygulanmasını zorlaştıran kaynak kısıtlı cihazlardan oluşmaktadır. Bu nedenle, çalışmarında, yazarların bildiği kadarıyla, tanınmış hafif kriptografik ilkeler ve bunların en yeni mimarileri incelenmiştir [14]. Guang ve arkadaşları, LZUC şifresinin performansını doğrulamak için, çıkış anahtar akışları üzerinde NIST istatistiksel testleri ve bilgi entropi analizi gerçekleştirilmiş ve algoritmanın zayıf anahtar analizine, tahmin belirleme analizine, zaman depolamalı veri değiş tokuş analizine ve cebirsel analize karşı direncine yönelik tipik saldırıları tartışılmıştır. Çalışmanın sonunda, LCD tarafından görüntülenen düz metin ve şifreli metin görüntüleri, LZUC şifresinin şifreleme etkinliğini doğrulamak için daha fazla görselleştirilebileceği iddia edilmiştir [15]. Prakasam ve arkadaşları, Nesnelerin İnterneti (IoT), teknolojik açıdan yetkin olduğu kanıtlanmış birçok internet üzerinden cihazların var olduğu ve iletişimin giderek arttığı günümüzde, ağlarda büyük miktarda verinin güvenli bir şekilde iletilmesinin hayati önem taşıdığını vurgulamışlardır. Bu nedenle, güvenli bir şekilde iletmek için etkili bir şifreleme metodolojisi gereklidir. Böyle bir yöntem için MATLAB kullanılarak konuşma sinyali için doğrulama yapılmış ve onaylanmıştır. Uygulama sonuçlarından, önerilen HLCAS yönteminin 5,4 ns gecikme süresine, 0,9 kilobayt RAM'e sahip olduğu ve 202 mW güç tükettiği bulunmuştur. Bildirilen birkaç yöntemle yapılan karşılaştırmada, önerilen HLCAS yönteminin diğer yöntemlerden daha iyi performans gösterdiği gözlemlenmiştir [16]. Im ve arkadaşları, Nesnelerin İnterneti (IoT) güvenliği için hafif kriptografi kullanımı arttığından, hafif kriptografi saldırıları üzerine araştırma yaparak IoT cihazlarına yönelik önemli tehditleri bilgilendirmek gerektiğine değinilmiştir. Çalışmada altı hafif kriptografiye yönelik başarılı saldırılar gösterilmektedir. Pratik analiz için, 50 MHz'de

çalışan Cortex-M0 tabanlı tipik bir IoT platformu, üç Xilinx FPGA yongası üzerinde çeşitli kriptografi algoritmaları ve Spartan-6, Artix-7 ve Kintex Ultrascale tasarım seçenekleriyle birlikte uygulanmıştır. KLEIN ve LED için 64 bitlik anahtarların tamamı, PRESENT için ise toplam 80 bitlik anahtarlardan 64 bitlik anahtarların %80'i kısmen elde edilmiştir [17]. Bhagat ve arkadaşları, çalışmalarında, blok şifreleri ve diğer bazı akış şifrelerini girdi boyutu, çıktı boyutu, kullanılan yapı, anahtar boyutu, tur sayısı, savunmasız saldırılar, yonga alanı, kapı eşdeğeri, bellek kullanımı, verim ve güvenlik özellikleri gibi kriterlere göre karşılaştırılmıştır. Çalışmaları tüm kriptografik algoritmaları ve bunların günlük yaşam aktivitelerindeki kullanımlarını karşılaştıran detaylı bir analiz sunmakta ve bazı hafif şifreler, akış şifreleri ve hibrit şifreler de tartışılmaktadır [18].

Puneeth ve Partasarathyb, çalışmalarında, Sezgisel Türev Simetrik Şifreleme (IDSE) Algoritması tabanlı güvenlik algoritması, blok zinciri işlevi ile birlikte yetkili veri depolama ve iletim sürecini oluşturmak için entegre edilmiştir [19]. Dewamuni ve arkadaşları, hızla gelişen Nesnelerin İnterneti (IoT) dünyasında, büyük miktarda kişisel veri toplandığı için veri güvenliği giderek daha önemli hale geldiğini vurgulamışlardır. IoT güvenliğindeki araştırma eğilimlerini ve modellerini belirlemek için mevcut çalışmaları, anahtar kelimeleri, yazarları, dergileri ve atıfları analiz etmek çok önemlidir [20]. Neve ve arkadaşları, LWC'nin performans analizi ve geliştirilmesi, etkili uygulama için kaynak kısıtlı mobil cihazlarda daha iyi veri güvenliği sağlamak olduğunu vurgulamışlardır. Gerçek SIMON algoritması ile Hibrit-SIMON_SPECKey algoritması karşılaştırıldığında, şifreleme ve şifre çözme sürelerinin %50 daha az olduğu gözlemlenmiştir [21]. Windarta ve arkadaşları, özellikle, SATURNIN blok şifresini değiştirerek TJUILIK-Hash oluşturulmuştur. Contiki-NG ve Cooja simülatörü kullanılarak yapılan simülasyon deneyleri, bu iki hash fonksiyonunun PHOTON-Beetle-Hash, PHOTON ve SPONGENT'e göre beş ölçütte iyi performans gösterdiğini doğrulamaktadır [22].

Bu bölümde literatür taraması gerçekleştirilmiş olup bir sonraki bölümde malzeme ve yöntem kapsamında bilgi güvenliği, nesnelerin interneti, kablosuz algılama ağları ve hafif kriptografi konuları irdelenecektir.

3. MALZEME VE YÖNTEM

Bu bölümde çalışmada kullanılacak temel kavramlar arasında yer alan bilgi güvenliği, IoT, kablosuz iletişim türleri, kriptoloji ve hafif kriptografi kavramları üzerinde durulacaktır.

3.1 Bilgi Güvenliği

Modern dünyamızda bilgiye sürekli erişim sağlanması, verinin göndericiden alıcıya kadar gizlilik içinde, değişime ve bozulmaya uğramadan, başkaları tarafından ele geçirilmeden bütünlük içerisinde güvenilir bir şekilde alıcıya iletimi bilgi güvenliği olarak tanımlanabilir. Bilgi güvenliği genel olarak üç bileşenden oluşur [23].

- Gizlilik: Yalnızca yetki tanınan kişilerce bilgilere erişim sağlanmasını ve yetkisiz erişime karşı korunmasını ifade etmektedir. Bilgilere erişim iznine sahip olmayan bir kişinin bilerek veya kaza yoluyla bilgileri edinmesi gizliliğin sağlanamadığı anlamına gelir. Gizliliğin etkin olarak sağlanmasında birçok şifreleme algoritmaları kullanılabilir.
- Bütünlük: Bir bilginin iletimi boyunca yetkisiz kişiler tarafından değiştirilmemesi ve kaynağından başlayarak güvence altına alınmasını ifade eder.
- Kullanılabilirlik: Bilgilere yetkili kullanıcılar tarafından erişilebileceğini ifade eder.

3.2 Nesnelerin İnterneti (IoT)

Kevin Ashton 1999'da RFID projesi kapsamında IoT terimini gündeme getirmiştir. IoT teriminin ilk olarak kablolu ya da kablosuz olarak birbirine bağlanabilen, birbiriyle bağlantılı bir cihaz grubu olarak ortaya çıktığı 2009'a bakılırsa, şu ana kadar gelişen teknolojiler, altyapı ve IoT kullanımı için artan bir ilerleme görülmektedir. İşlemsel teknolojiler, bilgi teknolojiler ve akılı nesneler, IoT'un ağ bileşenleri olarak bilinir.

3.2.1 Kablosuz algılama ağları

Uygun fiyatlı mikro elektronik cihazların, daha ucuz depolama sistemlerinin ve verimli İnternet iletişim teknolojilerinin geliştirilmesi, bilginin üretilmesi, işlenmesi ve iletilmesi şeklini değiştirmiş olup bu gelişmeler ışığında son yıllarda IoT

yaygınlaşmıştır. IoT dünyası farklı birçok unsurdan oluşmaktadır. Ancak çevre ile etkileşimde bulunan ve verileri toplayan algılayıcıların oluşturduğu Kablosuz Algılayıcı Ağları (Wireless Sensor Networks-KAA), IoT sistemlerin ana bileşenini oluşturmaktadır [24,25].

KAA, ortamın sıcaklık, ses, basınç vb. fiziksel koşullarını izlemek, kaydetmek ve toplanan verileri merkezi bir yerde düzenlemek için planlı olarak konumlandırılmış otonom algılama ağlarıdır. Modern ağlar çift yönlü etkileşime girerek algılayıcı etkinliğinin kontrolünü sağlayabilirler. KAA, bir veya birkaç düğüm ile yüzlerce hatta binlerce algılama ağı düğümlerinden oluşabilir. Böylelikle bilgiye her an, her yerden kolayca ulaşılması sağlanmaktadır. Tipik olarak bir algılayıcı ağı düğümü; dâhili veya harici RF alıcı/verici anten, bir mikro denetleyici, algılayıcı ile arabirim oluşturmak için bir elektronik devre ve sistemi besleyecek bir enerji kaynağından meydana gelir. Ayakkabı kutusu boyutundan bir toz tanesi boyutuna değişen ölçülerde algılama düğümü imal edilebilmekte ve bir düğümün boyut ve maliyeti, o düğümün enerji tüketimi, hafıza boyutu, hesaplama hızı, algılama hassasiyeti ve iletişim bant genişliği gibi performans kriterlerine bağlı olarak değişebilmektedir[26, 27].

Uygulama alanları genel olarak askeri, sağlık, çevre izleme, habitat izleme, tarım, endüstri, yapı, trafik ve yol, lojistik ve taşıma, web, eğitim, enerji, denizcilik, su altı ve diğer uygulamalar olarak sıralanabilmektedir [27, 28].

KAA'da verinin doğru ve eksiksiz bir şekilde ana düğüme aktarılması, güvenli veri toplama olarak bilinmektedir. Bu sistemler hassas veriler taşıdığından verinin iletiminde; gizlilik, veri bütünlüğü ve kullanılabilirliği ile ilgili güvenlik sorunlarını giderebilecek güvenlik altyapısının oluşturulması mutlak bir gerekliliktir. Çeşitli şifreleme algoritmaları sayesinde bilgi şifrelenerek ana düğüme güvenli bir şekilde aktarılmaktadır. Böylece kritik öneme sahip veriler korunmuş olmaktadır [29].

3.2.2 Uzaktan kontrol sistemleri

Kepenk sistemleri (garaj, depo, market, vitrinler vs. kullanılan), ev güvenlik sistemleri, aydınlatma sistemleri gibi elektronik olarak çalışan uzaktan kontrol sistemleri giderek yaygınlaşmaktadır. Bu tür elektronik uzaktan kumanda sistemleri tipik olarak, modüle edilmiş ve kodlanmış bilgiyi alıcıya iletmek için belirli RF sinyalini kullanırlar [30].

Verici RF devreleri pille çalışan devrelerdir. Örneğin, garaj kapılarının kontrolünde bir RF alıcı kart garaj kapısının kontrolü için konumlandırılmıştır. Alıcı kart aynı frekans bandında yayın yapan bir kablosuz verici ile eşleştirilerek modüle edilmiş ve önceden belirlenmiş kod ile kontrol edilmektedir. Böylelikle garaj kapılarının uzaktan kontrol ile açılıp kapanması sağlanabilmektedir. Bu bağlamda, kollu ve mantar bariyerler, hareketli kapılar, otomatik panjur sistemleri, aydınlatma ve iklimlendirme sistemleri, makine ve alarm sistemleri, araç kapıları gibi daha pek çok alanda kablosuz uzaktan kontrol sağlanmaktadır.

Uzaktan kumandalı cihazların güvenliğini artırmak için kumandaya her basıldığında verici, atlamalı kod olarak da bilinen yuvarlama kodları üretir. Oluşturulan kontrol sinyali her defasında değişmektedir. Hangi kodun iletileceğini ve alınacağını takip etmek için sonuncu kod bilgisi alıcı ve verici hafızalarında belirli seri numaralarıyla saklanmaktadır. Böylelikle verici her defasında hafızasındaki kayıtlı veriyi okuyarak farklı komut sinyalleri üretirken alıcı ise hafızasında kayıtlı veri sayesinde gelecek bir sonraki sinyale odaklanmaktadır.

Verici tarafından üretilen değişen kontrol sinyalleri tahmin edilemez ve kopyalanamaz olmalıdır. Bunu sağlamak için de çeşitli şifreleme algoritmaları kullanılmaktadır. Farklı matematiksel algoritmalara ve farklı tekniklerin uygulanmasına bağlı olarak, kriptografi algoritmaları genellikle işlem süreleri, bellekte kapladıkları alan ve saldırılara karşı direnç açısından farklı performanslara sahiptirler. Kullanım alanına göre en uygun algoritmanın seçimi yapılmalıdır.

3.2.3 Kablosuz iletişim türleri

Günümüzde IoT sistemlerde kullanılan birçok kablosuz iletişim türü bulunmaktadır. Bu başlık altında bu iletişim yöntemleri hakkında genel bilgiler verilmektedir.

3.2.3.1 Wi-Fi

İngilizcede Wireless Fidelity, kelimelerinin kısaltmasıdır ve kablo olmadan radyo dalgalarıyla veri transferi sağlayan bir dizi haberleşme standardına verilen addır. Bu standartlara uyumlu cihazlar (bilgisayar, cep telefonu, PDA) geniş bant hızında internete kablosuz olarak bağlanabilir ve birbirleri ile 2.4 GHz ve 5 GHz frekans

bantlarını kullanarak haberleşebilir. Kablosuz ağlar telsiz telefon, televizyon ve radyoların yaptığı gibi radyo sinyalleri ile haberleşir. Wi-Fi standartları ve sertifikaların düzenlenmesi Wi-Fi Alliance tarafından sağlanmaktadır. Kablosuz ağda çift yönlü radyo haberleşmesi kullanılır [31].

3.2.3.2 Bluetooth

Bluetooth, kısa mesafe veri iletimi için kullanılan özelleştirilmiş radyo frekansıdır. Bluetooth standartları, ilk olarak 1994 yılında Ericsson şirketi tarafından ortaya atılmıştır. Amaçları ürettikleri telefonlar ile donanımlarının kablosuz, enerji tüketimi az ve ucuz teknoloji ile birbirlerine bağlanmasıdır. Sonraları bu teknolojinin daha da gelişeceği düşünülerek kısa mesafeli ses veri iletimini de kapsayan bir protokol haline dönüştürülmüştür. Ayrı zamanda Bluetooth'un diğer veri iletim türü olan kızılötesine göre, alıcı ve vericinin birbirlerini görmesini gerektirmemesi, aynı anda birkaç cihazın birden kontrolünün sağlanması gibi üstün avantajları bulunmaktadır.

Her iletişim türünde olduğu gibi Bluetooth'ta da veri iletiminde belirli bir protokol bulunmaktadır. Bu protokol fikrini ilk dile getiren Ericsson şirketi, Bluetooth üzerinde yaptığı başarılı denemelerin ardından 1998 yılında Ericsson, Nokia, IBM, Toshiba ve İntel şirketleri bir araya gelerek Bluetooth SIG'i kurdular. Bluetooth standartları ücretsiz olarak herkesin kullanımına açıktır [32]. Bluetooth ilk sürümü1999 yılında tanıtılmıştır. Zaman içerinde birçok değişiklik ve güncelleme yapılmıştır. Bu güncellemeler içerisinde 2010 yılında tanıttığı 4.0 sürümü düşük enerji çözümleri sunmaktadır. Blutooth 4.0 ve üstü sürümler için Bluetooth Low Energy (BLE) ifadesi kullanılmaktadır. Bluetooth sürekli geliştirilerek yeni sürümleri yayımlanmaktadır [32, 33].

3.2.3.3 ZigBee

Zigbee, IEEE 802.15.4 standardını temel alır ve kablosuz haberleşme teknolojilerinde düşük hız kablosuz kişisel yerel ağ (LR-WPAN, Low-Rate Wireless Personal Area Network) haberleşmesi olarak bilinir. Arıların kovanlarına gitmek için takip ettikleri zikzak yoldan esinlenerek isimlendirilmiştir.

Zigbee Alliance, Zigbee teknolojisinin standartlarından sorumlu dünya çapında bir birim olup; güvenilir, düşük maliyetli ve güç tüketimi az ürünler ortaya çıkarmak için birçok firmanın bir araya gelip görüntüleme ve kontrol amaçlı ürünlerin standartları üzerinde çalıştığı bir topluluktur [31, 34].

3.3 Kriptoloji

İlk olarak kriptografinin anlamı üzerinde durulacaktır. Mesajların gizlice gönderilmesi için kullanılan yöntemlerdir, böylece yalnızca hedeflenen alıcı gizliliği kaldırabilir ve mesajı okuyabilir. Şifreleme süreci düz metnin şifreli metne dönüştürülmesine şifreleme veya şifreleme denir. Şifreli metni düz metne dönüştürme işleminin tersine, gizlemeyi kaldıracak bilgiye sahip olan alıcı tarafından gerçekleştirilen işleme ise şifre çözme veya deşifre etme denir. Kriptanalizi uygulayanlara (genellikle "düşman" olarak adlandırılırlar) kriptanalist denir. Ayrıca, şifre terimi şifreleme ve deşifre etme yöntemidir [35].

3.3.1 Hafif kriptografi

Hızlanan Geri Dönüş Yasası'na göre, teknolojik değişimler katlanarak gerçekleşmektedir [36]. Ancak son teknolojik değişimlerle birlikte internet, insanlar yerine cihazları birbirine bağlamak için daha fazla kullanılmaya başlandı. Bu cihazların bazıları masaüstü bilgisayarlar veya tabletler gibi güçlü bilgi işlem cihazları olsa da, sistemde Radyo Frekanslı Kimlik Belirleme (RFID) etiketleri, sensör ağları ve akıllı kartlar gibi küçük bilgi işlem cihazları veya kaynak kısıtlı cihazlar da bulunmaktadır. Uygulandıklarında performans eşit olmayabilir veya güvenlik yeterli olmayabilir [37].

Hızlanan Geri Dönüş Yasası'na göre, teknolojik değişimler katlanarak gerçekleşmektedir [38]. Ancak son teknolojik değişimlerle birlikte internet, insanlar yerine cihazları birbirine bağlamak için daha fazla kullanılmaya başlandı. Bu cihazların bazıları masaüstü bilgisayarlar veya tabletler gibi güçlü bilgi işlem cihazları olsa da, sistemde Radyo Frekanslı Kimlik Belirleme (RFID) etiketleri, sensör ağları ve akıllı kartlar gibi küçük bilgi işlem cihazları veya kaynak kısıtlı cihazlar da bulunmaktadır. Uygulandıklarında performans eşit olmayabilir veya güvenlik yeterli olmayabilir. Bu, geleneksel bir algoritmayı uygulamak için mikrodenetleyicinin çok

fazla döngü kullanması gerektiği anlamına gelir. Kısıtlı cihazlarda geleneksel algoritmaların güç tüketimi yüksek olacaktır. Pilin değiştirilmesi kolay olduğunda bu bir sorun olmayabilir, ancak pil değişimi mümkün olmadığında güç tüketiminin düşük olması gerekir [39].

Küçük bir hesaplama gücü kullanırken, onu güvence altına almak için hafif kriptografi algoritması kullanılmalıdır, bu nedenle hafif blok şifreler, hafif akış şifreleri veya hafif karma işlevi kullanılabilir. Hafif blok şifrelere gelince, birçok algoritma vardır, yapının tasarımına göre aşağıda birçoğunu dâhil ediyoruz [40].

3.4 Kriptolojinin Tarihçesi

Tarihte ilk kez bilginin arşivlenmesi veya haberleşme için kâğıda yazılma ihtiyacının oluşmasıyla birlikte özellikle önemli görülen bilgilerin ortaya çıkma ve istenmeyen kişiler tarafından ele geçirilme endişesi doğmuştur. Böylelikle insanlar ya bilginin şifrelenmesinin yollarını bulmaya ya da başkalarının şifreli bilgilerin anlamaya çalışarak kriptoloji biliminin gelişmesini sağlamışlardır [41].

Tarihte bilinen en eski şifrele metni bunda 4000 yıl önce antik mısır kasabası MENET KHUFU'da soylu KHNUMHOTEP II mezarındaki kitabenin olduğu düşünülmektedir. Mısırlı kâtip bu yazıtta sıra dışı hiyeroglif işaretler kullandığı tespit edilmiştir [42, 43].

Kriptoloji geçmiş dönemlerde daha çok, günümüzde hala en önemli alanlarından olan, askeri ve diplomatik haberleşmede bilgi güvenliğinin sağlanması için kullanıldığı bilinmektedir [44]. M.Ö. 5. yüzyılda kriptolojiyi askeri iletişimde ilk spartalılar kullandı. SCYTALE adı verilen silindir cihazın etrafına bir parşömen veya deri şerit sarılır ve mesaj üzerine yazılırdı. Alıcı şeritleri aynı çapta silindire sarıp çözmesi gereklidir. Cihazın çapı kripto anahtarına denk gelmektedir [42, 44].

M.Ö. 60-50 yıllarında Yunan yazar Polyibus'un tanımladığı teknik ilk olarak Roma İmparatoru Julius Caesar tarafından generallerine mesaj iletmek için kullanılmıştır. Bu şifreleme yönteminde alfabedeki harfler belli miktar sağa ötelenerek gizli metin elde ediliyordu [43].

Kriptoloji bilimi iletilecek bilginin şifrelenmesinin yanında şifreli bir metnin açık hale getirilmesi için de metotlar geliştirir. Gizli bilginin anahtar olmadan deşifre etmeye

kriptoanaliz denmektedir. Şifrelerin çözümünde istatistik, matematik ve dilbilim alanlarından yararlanılır. Bu bağlamda ilk kriptoanaliz çalışması Al-Kindi tarafından 9. yüzyılda yapılmıştır. Al-Kindi çalışmalarında, hangi dilde yazıldığı bilinen bir şifreli mesajın yine o dilde yazılmış yeteri uzunluktaki bir metnin analizi sonucunda harflerin kullanım sıklıklarının belirlenmesiyle kolaylıkla çözülebildiğini ortaya koymuştur. Bu nedenle daha sonra geliştirilen kriptolarda birden fazla alfabe kullanılmış, böylelikle çok alfabeli şifreleme algoritmaları geliştirilmiştir [44].

Leon Alberti 1466 yılında yazdığı makalede, ilk kez çoklu alfabe kullanarak Alberti şifreleme diskinin yapımını anlattı. Temel olarak Sezar şifrelemede kullanılan harf öteleme yöntemini kullanmakla beraber harflerin öteleme miktarı sabit değildir ve bunu kullanıcı belirlemektedir. Son beş yüz içinde kriptografideki en önemli ilerleme olarak kabul edilmektedir [43, 44].

Giovan Battista Bellaso 1553 yılında 1863 yılına kadar yani üç yüz yıl kırılamayan çok alfabeli kriptografi tekniğini geliştirdi. Bu şifreleme, Fransız Blaise de Vigenère tarafından biraz daha geliştirilerek Vigenère Şifresi adını almıştır. 1863 yılında Friedrich Kasiski vigenère şifrelerini deşifre etmek için genel bir yöntem yayınlayan ilk kişidir [43, 44].

1790'da Thomas Jefferson, Jefferson diski adıyla her birinin üzerinde İngiliz alfabesindeki 26 harfin rasgele dizildiği toplamda 36 diskten oluşan şifreleme sistemini geliştirmiştir. Ortaları delik olan bu her disk benzersiz bir numaraya sahiptir ve istenilen sıraya göre dizilirler. Disklerin sırası şifre anahtarıdır ve hem mesajı gönderici hem de alıcı diskleri önceden tanımlanmış aynı sırada düzenlemelidir. Alıcı şifreli metin ile diskte sırayı oluşturup, diğer sıralardaki açık metne ulaşmış olur. Bu sistemi temel alarak oluşturulan M-94, 1923'ten 1942 yılları arasında Birleşik Devletler Ordusu M-94 olarak kullanıldı [42, 44].

Frank Miller tarafından 1882 yılında tanımlanmış olduğu şifreleme çalışması, 1917 yılında Gilbert Vernam tarafından geliştirilip bir yazı makinası için şifreleme çözümü icat edildi. Joseph O. Mauborgne anahtar kasetindeki karakterlerin tamamen rasgele olabileceğini keşfetti. Birlikte tasarladıkları ilk One-Time Pad Şifreleme sisteminin patentini 22 Temmuz 1919 yılında almışlardır [42, 45].

1883’te Auguste Kerckhoffs tarafından yazılan La Cryptographie Militaire adlı makalede şifreleme sistemlerinin tasarım prensiplerini anlatmıştır. Bu prensipler sonraki dönemlerde geliştirilen sistemlerde önemli bir yol gösterici olmuştur. Kerckhoff Prensipleri [44]:

Sistem pratik ve matematiksel bir gerçekliğe dayanmalıdır. Sistem gizliliğe dayanmamalıdır. Yani sistem hakkındaki her şey herkes tarafından bilinmelidir. Sistemde kullanılan anahtarlar taraflar arasında kolayca, üçüncü kişinin değiştirmesine izin verilmeden değiştirilebilmelidir. Sistemin kullanılabilmesi için fazla sayıda insana ihtiyaç duyulmamalıdır. Sistemin uygulaması ve anlaşılması kolay olmalı ve şifreleme sisteminin güvenliği, şifreleme algoritmasını gizli tutmaya dayanmamalıdır. Güvenlik; yalnızca anahtarı gizli tutmaya dayanmalıdır. 19. yüzyılın sonlarına doğru İtalyan fizikçi Markoni'nin telsizi icat etmesiyle yeni güvenlik kaygıları ortaya çıkmış ve güvenli iletişime duyulan ihtiyaç daha da artmıştır. Özellikle telsizlerin savaş alanlarında kullanımının yaygınlaşmış olması ve kablosuz iletişimden dolayı düşmanın mesajlara kolaylıkla erişebiliyor olması, telsiz iletişimde şifreleme tekniklerinin araştırmaları yoğunlaştırmıştır. I. Dünya savaşında kullanılan şifreleme yöntemlerinden biri Almanların geliştirmiş oldukları ADFGVX sistemleri ve “kod kitabı” yöntemidir. Bu yöntemde iletilecek mesajlardaki her kelime için sayı grupları kullanılıyordu. Savaş sırasında Almanların Meksika başbakanına gönderdiği bilgiler İngiliz işaret toplama birimleri tarafından çözülmüş ve elde edilen bilgiler ABD'nin savaşa girmesine ve savaşın seyrinin değişmesine neden olmuştur [44, 46].

Almanya 1923 başlarında Enigma adlı kriptoloji cihazını geliştirdi ve 1930 yıllarının ortalarına gelindiğinde artık ordunun onaylı şifreleme cihazı oldu. Bu Makine II. Dünya savaşında alman ordusu tarafından aktif olarak kullanılmıştır. Elon Tureng öncülüğündeki İngiliz kriptoanaliz ekibi geliştirdikleri Colossus makinası sayesinde Enigma şifresi çözülmüş ve savaşın seyri değişmiştir [44, 46].

Teknolojinin ilerlemesi harflerin yerini 1 ve 0’ların almasıyla şifreleme işlemleri bitler ile yapılmaya başlanmıştır. 1970 yılında IBM tarafından, DES algoritmalarının da temelini oluşturan, Lucifer adı verilen şifreleme sistemi tanıttı ve 1975 yılında Birleşik Bilgi İşleme Standardı olarak kabul edildi [42, 44].

Elektronik haberleşmenin yaygınlaşması sonucu herkesin kullanabileceği ve hassas elektronik devlet bilgilerinin korunabileceği şifreleme algoritma ihtiyacı doğmuştur. Bu ihtiyacı karşılamak için Lucifer algoritmasında birtakım değişiklikler yapılarak DES geliştirilmiştir. Şifreleme anahtarı rasgele ve gizli seçilmektedir [44, 47].

1976 yılına gelindiğinde gönderici ve alıcının şifreleme anahtarı için bir araya gelmelerinin zorunlu olmadığı, birbirini hiç tanımayan kişiler arasında bile güveli iletişime olanak sağlayan Diffie-Hellman Anahtar Değişim Algoritması yayınlandı. Bu algoritma geliştirilene kadar haberleşen her iki taraf da önceden belirlenmiş anahtarları bilmesi gereken tasarlanan bu sistemde her birey kendi özel anahtarına sahiptir. Böylelikle bu çalışmayı temel alan, 1977'de Rivert, Shamir ve Adleman tarafından adlarının baş harflerinden oluşan, asimetrik anahtar paylaşımının güçlüklerini ortadan kaldıran RSA algoritmasının tanıtılması kriptolojide çığır açmıştır [44, 48].

Bilgisayar işlem gücünün gelişmesiyle DES algoritmasının güvenilirliğinin azalması yeni bir şifreleme algoritması ihtiyacı doğurdu. NIST 1997 yılında bir yarışma başlatmış, Joan Daemen ve Vincent Rijmen tarafından geliştirilen Rijndael Algoritması DES'in yerine 2001 yılında AES standartlaştırılmıştır. 128, 192, 256 bitlik anahtar uzunluğu seçeneklerine sahip olan AES günümüzde hala güvenilirliğini korumaktadır [42, 47].

2009 yılında ilk Kriptografi olimpiyatları yeni güvenilir algoritmaların geliştirilmesi amacıyla Belçika Katholieke Üniversitesinde düzenlenmiştir [44].

Dünyada ve Türkiye'de araştırma ve geliştirme faaliyetleri hızla ilerlemektedir. Bu alandaki çalışmalara ülkemizde TÜBİTAK Bilgem bünyesindeki Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE) öncülük etmektedir [44].

3.5 Performans

Performans, ölçüt olarak donanım ve yazılım olmak üzere iki kategoride analiz edilebilir.

3.5.1 Donanım

Bir kriptografik algoritma uygulandığında, donanım bazında performansını tanımlamak için frekans, verim, kapı alanı, maksimum güç ve sızıntı güç tüketimi olarak ele almak mümkündür.

Frekans, bir sinyalin sıklığı tanımlar ve dalga boyu büyüdükçe ters orantılı olarak küçülür. Birimi Hertz'tir.

Verim, bir zaman biriminde işlenen bit miktarını tanımlarken yüksek olması beklenir.

Kapı alanı, algoritmayı donanımda uygulamak üzere gereken fiziksel alanı tanımlarken kısıtlı cihazlar sınırlı alana sahip olduğundan, kapı alanının düşük olması istenir.

Maksimum güç tüketimi, algoritmayı uygulamak için gereken maksimum tüketimi belirtir ve küçük olması beklenir. Sızıntı gücün hakeza düşük olması istenir.

3.5.2 Yazılım

Yazılımda, RAM, kod boyutu ve verim olmak üzere üç ölçüt kullanılır. Verim ise bir zaman biriminde işlenen bit miktarını tanımlar ve yüksek olması beklentiler arasındadır. Verim dışında diğer parametrelerin düşük olması istenir.

Hafif kriptografik teknoloji, düşük maliyetli, düşük güç tüketimli, araç üstü ekipman ve tıbbi ekipman dahil olmak üzere bir çok cihazda kullanılır. IoT ve siber-fiziksel sistem gibi yeni nesil ağ hizmetlerinin kurulmasında faydalı güvenlik teknolojilerinden biri olması beklenmektedir. Hafif kriptografik teknoloji için çeşitli yöntemler önerilmiştir. Bazıları, hafifliği donanım uygulama boyutu ve güç tüketimi açısından ararken, diğerleri gömülü yazılımın gerekli bellek boyutu açısından aramaktadır. Her yöntem farklı bir performans ölçütüne göre optimize edilmiştir. Buna ek olarak, performans ve güvenlik arasında bir değiş tokuş söz konusudur. Gerçek performans çok yönlüdür [49].

Bu bölümde "Malzeme ve Yöntem" bağlamında hafif kriptografi konusu irdelenmiş ve bir sonraki bölümde "Bulgular ve Tartışma" bağlamında hafif kriptografiyi içeren şifreleme ve deşifrelemenin tablo ve şekillleri ile istatistiki değerleri incelenmiştir.

4. BULGULAR VE TARTIŞMA

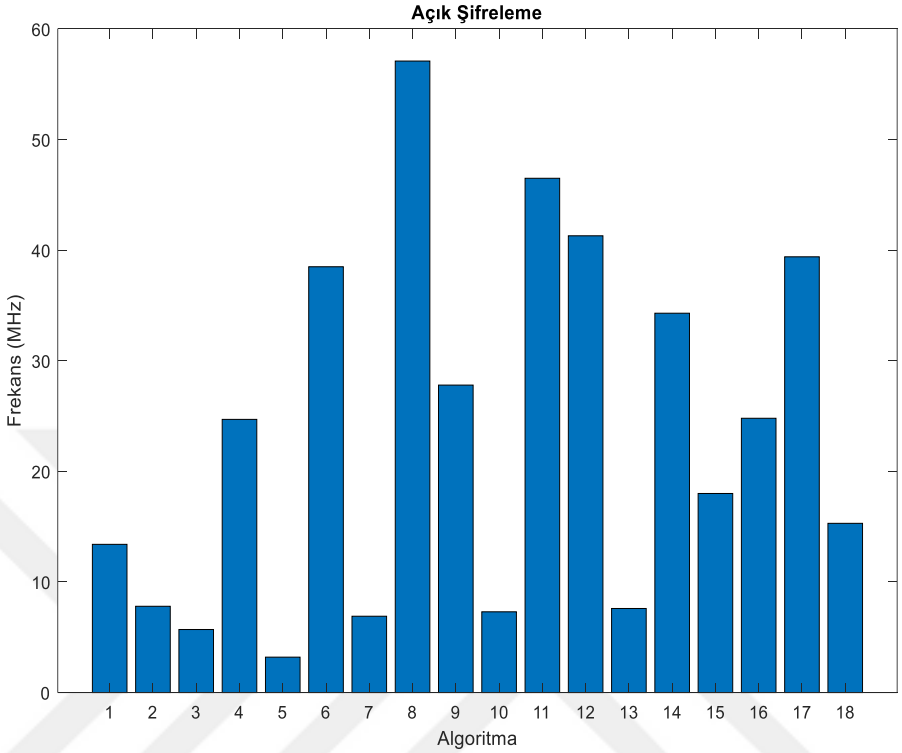
4.1 Açık Şifreleme

Tablo 4.1'de 18 farklı algoritma için açık şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

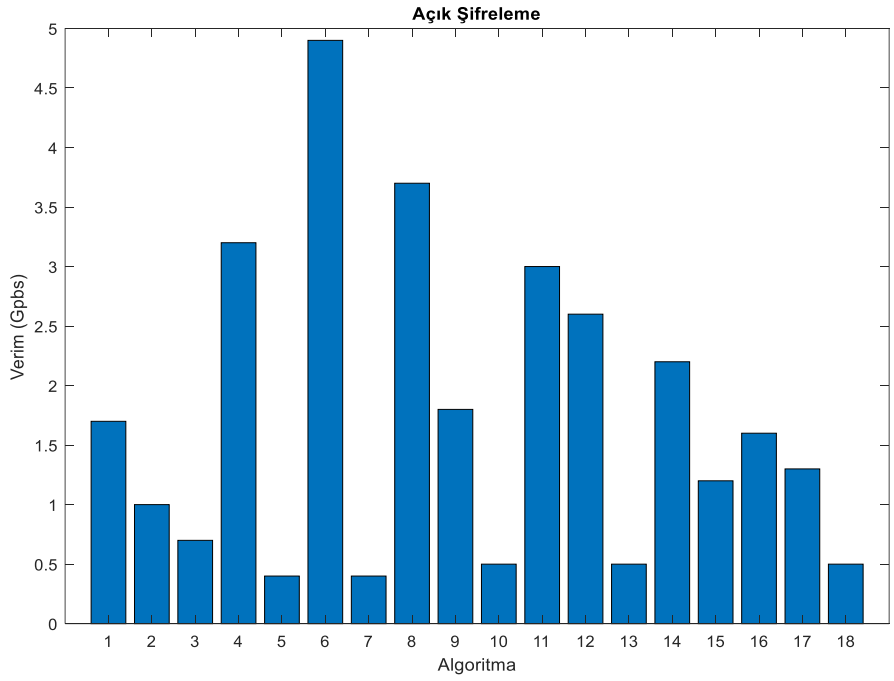
Tablo 4.1 Açık şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	Frekans (MHz)	Verim (Gbps)	Alan (kgate)	Max Güç (mW)	Sızıntı Güç (µW)
	Açık Şifreleme					
1	AES (128/128)	13.4	1.7	78.8	175.6	939.6
2	CAMELLIA(128/128)	7.8	1.0	60.2	136.5	706.7
3	CLEFIA (128/128)	5.7	0.7	74.6	195.5	891.0
4	SIMON (128/128)	24.7	3.2	63.2	172.2	685.9
5	SPECK (128/128)	3.2	0.4	44.4	73.0	417.0
6	MIDORI (128/128)	38.5	4.9	34.6	118.2	446.1
7	LED (64/128)	6.9	0.4	74.5	99.1	824.0
8	PRINCE (64/128)	57.1	3.7	9.8	28.1	107.4
9	SIMON (64/128)	27.8	1.8	23.8	71.5	260.4
10	SPECK (64/128)	7.3	0.5	19.5	35.6	183.0
11	MIDORI (64/128)	46.5	3.0	12.3	34.9	149.0
12	SIMON (64/96)	41.3	2.6	20.3	56.7	218.1
13	SPECK (64/96)	7.6	0.5	18.6	35.4	174.7
14	PRESENT (64/80)	34.3	2.2	23.9	57.8	259.6
15	PICCOLO (64/80)	18.0	1.2	19.1	61.0	224.8
16	TWİNE (64/80)	24.8	1.6	19.5	43.8	221.2
17	SIMON (32/64)	39.4	1.3	9.0	30.5	97.4
18	SPECK (32/64)	15.3	0.5	8.2	17.3	78.0
MİNİMUM		**3.2**	**0.4**	**8.2**	**17.3**	**78.0**
ORTALAMA		**23.3**	**1.7**	**34.1**	**80.2**	**382.4**
MAKSİMUM		**57.1**	**4.9**	**78.8**	**195.5**	**939.6**

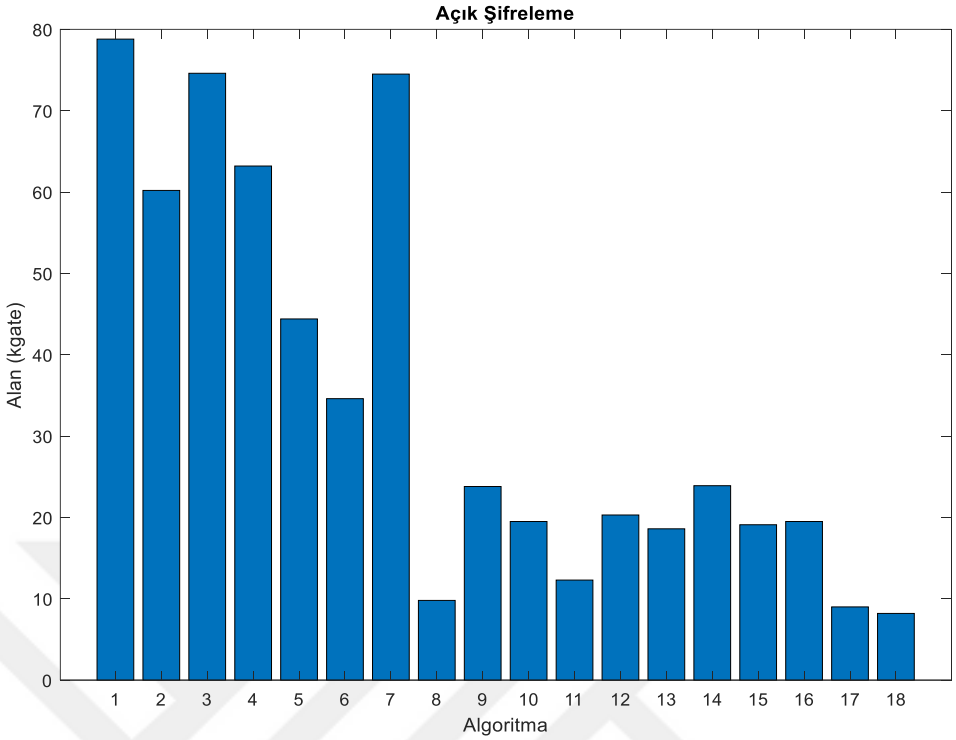
Aşağıda Şekil 4.1-4.5'te 18 farklı algoritma için açık şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



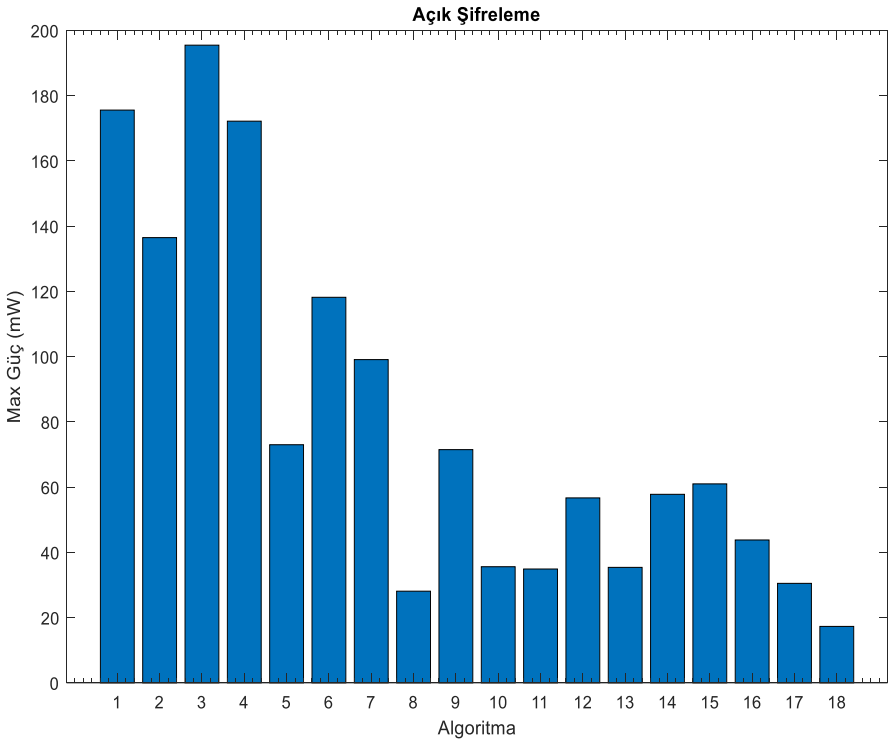
Şekil 4.1 Farklı algoritmalar için açık şifrelemenin frekans değerleri



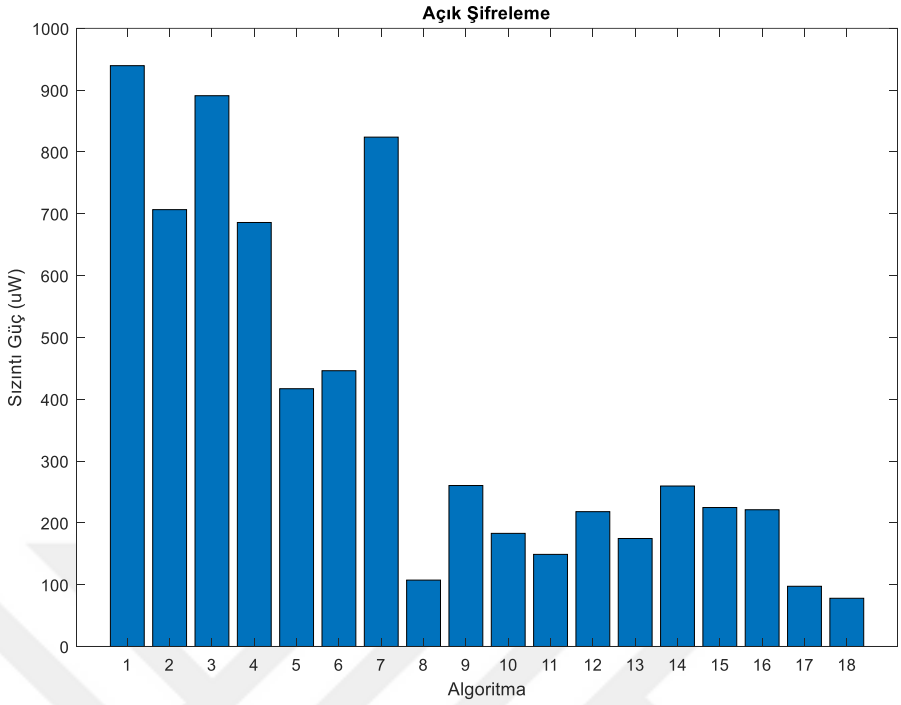
Şekil 4.2 Farklı algoritmalar için açık şifrelemenin verim değerleri



Şekil 4.3 Farklı algoritmalar için açık şifrelemenin alan değerleri



Şekil 4.4 Farklı algoritmalar için açık şifrelemenin maksimum güç değerleri



Şekil 4.5 Farklı algoritmalar için açık şifrelemenin sızıntı güç değerleri

Açık şifreleme tablosundaki özellikle frekans ve verim verileri değerlendirildiğinde minimum frekans değerinin SPECK algoritması, maksimumun ise PRINCE algoritması olduğu görülmektedir. Verim de ise minimum değerde LED algoritması, maksimum değerde ise MIDORI algoritmasının olduğu görülmüştür. Bu algoritmaların gücü de güvenlik açısından oldukça önemlidir. Şifreleme algoritmalarının gücü, anahtar uzunluğuna ve yapılan saldırılara karşı dayanıklılığına bağlıdır. Tablo incelendiğinde minimum gücün SPECK (32/64), maksimum gücün CLEFIA (128/128), minimum sızıntı gücün yine aynı şekilde SPECK(32/64) ve maksimum sızıntı gücün ise AES (128/128) algoritması olduğu görülmektedir.

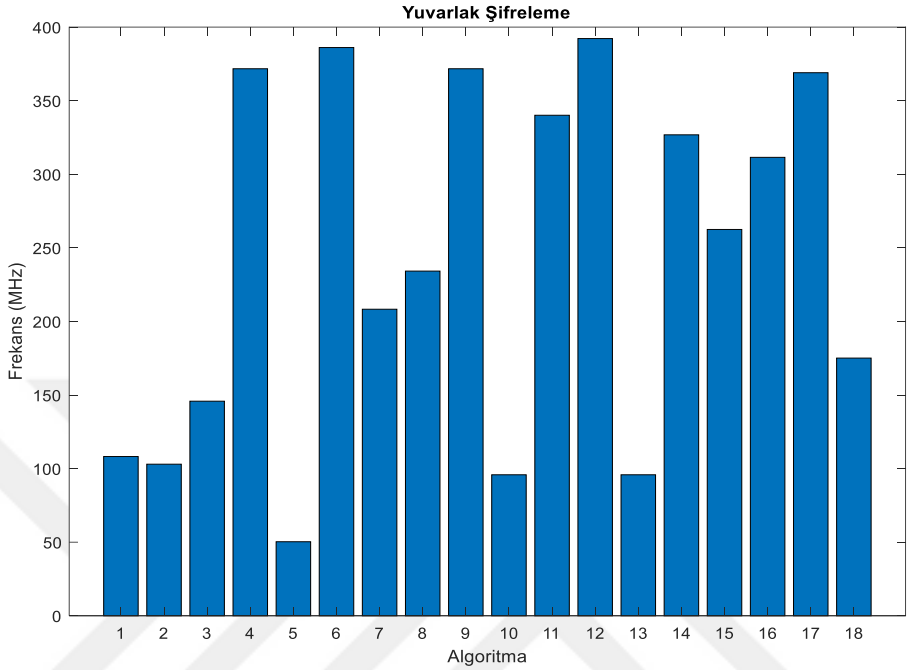
4.2 Yuvarlak Şifreleme

Tablo 4.2'de 18 farklı algoritma için yuvarlak şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

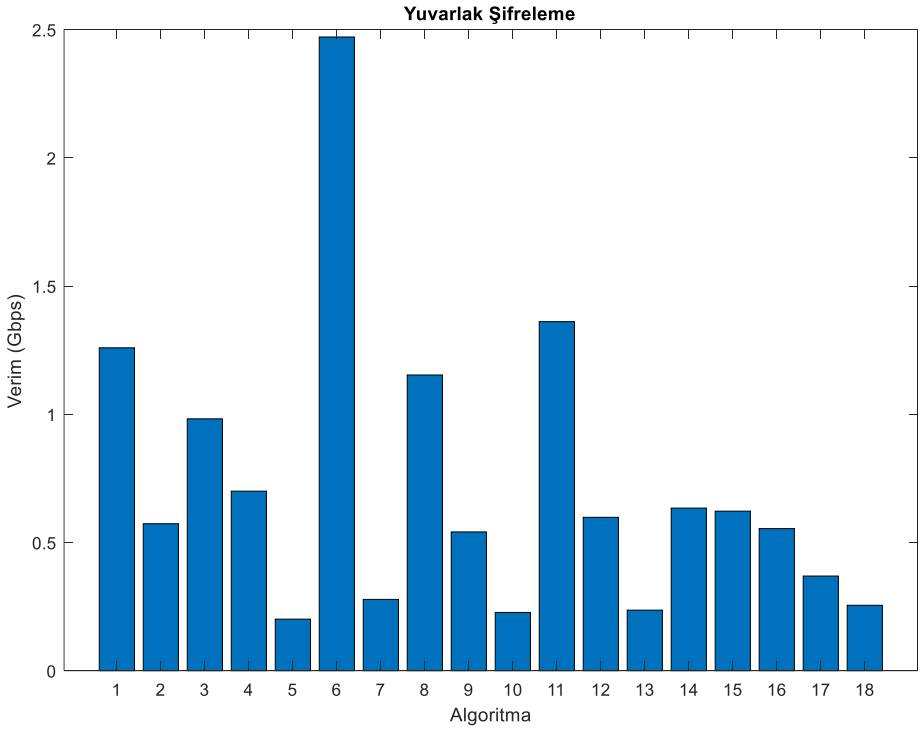
Tablo 4.2 Yuvarlak şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	**Frekans (MHz)**	**Verim (Gbps)**	**Alan (kgate)**	**Max Güç (mW)**	**Sızıntı Güç (µW)**
	Yuvarlak Şifreleme					
1	AES (128/128)	108.2	1.259	15.4	36.1	152.6
2	CAMELLIA(128/128)	103.0	0.573	10.8	46.6	107.7
3	CLEFIA (128/128)	145.8	0.982	10.1	39.8	99.6
4	SIMON (128/128)	371.7	0.700	7.0	17.4	69.9
5	SPECK (128/128)	50.3	0.201	7.2	11.4	66.2
6	MIDORI (128/128)	386.1	2.471	7.1	11.9	79.7
7	LED (64/128)	208.3	0.278	6.3	5.3	52.5
8	PRINCE (64/128)	234.2	1.153	5.1	16.4	47.1
9	SIMON (64/128)	371.7	0.541	5.3	12.4	51.1
10	SPECK (64/128)	95.8	0.227	5.3	10.5	48.3
11	MIDORI (64/128)	340.1	1.361	4.7	11.4	49.1
12	SIMON (64/96)	392.2	0.598	4.5	11.8	44.1
13	SPECK (64/96)	95.8	0.236	4.6	10.0	42.4
14	PRESENT (64/80)	326.8	0.634	4.1	4.7	33.4
15	PICCOLO (64/80)	262.5	0.622	3.5	3.4	34.2
16	TWINE (64/80)	311.5	0.554	4.4	4.6	40.0
17	SIMON (32/64)	369.0	0.369	2.9	9.8	28.0
18	SPECK (32/64)	175.1	0.255	2.9	8.4	26.8
MİNİMUM		**50.3**	**0.2**	**2.9**	**3.4**	**26.8**
ORTALAMA		**241.6**	**0.7**	**6.2**	**15.1**	**59.6**
MAKSİMUM		**392.2**	**2.5**	**15.4**	**46.6**	**152.6**

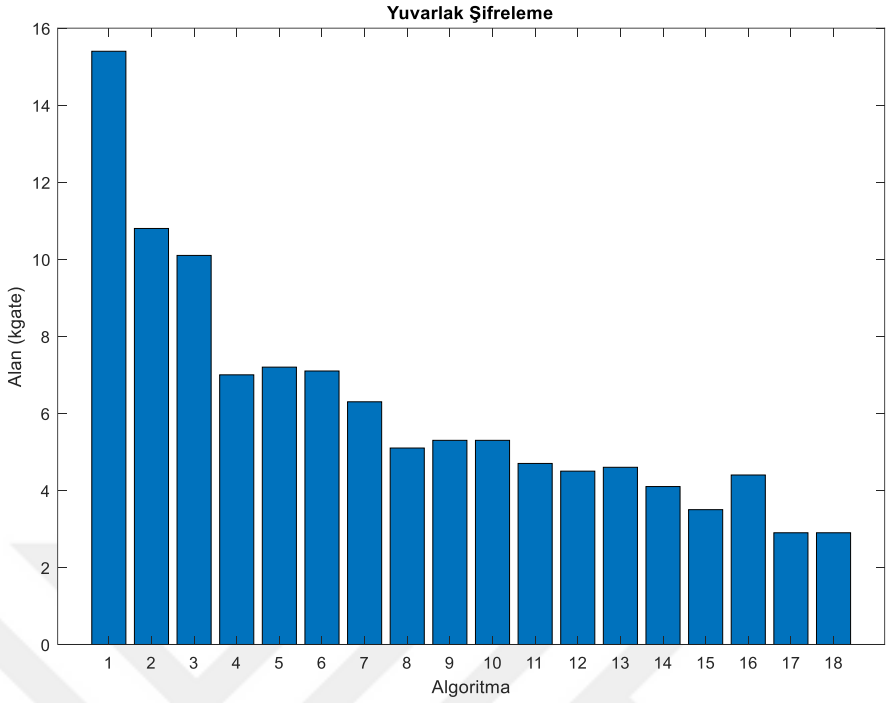
Aşağıda Şekil 4.6-4.10'da 18 farklı algoritma için yuvarlak şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



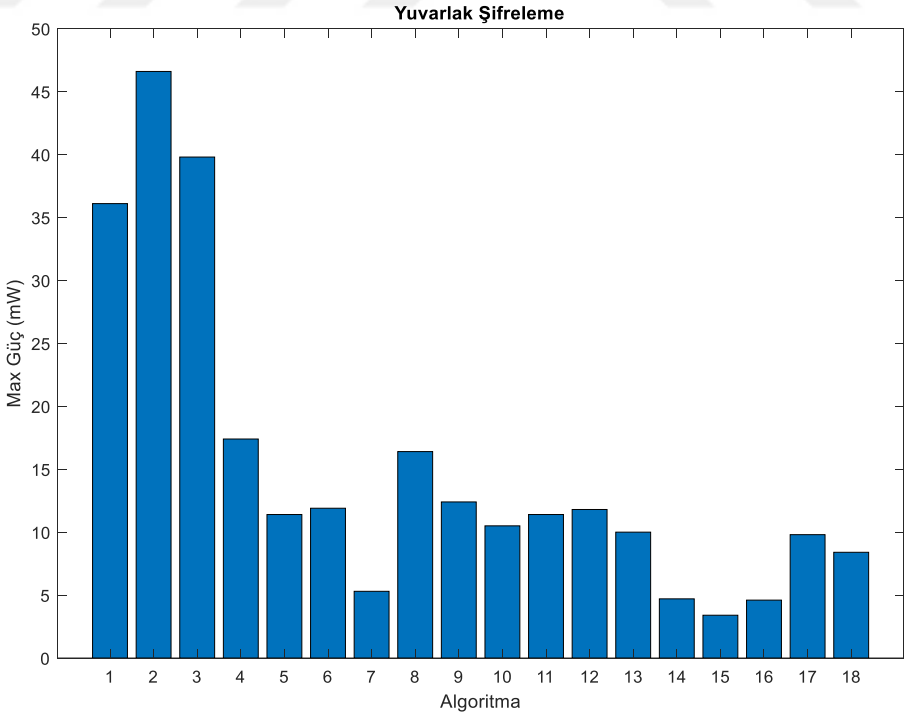
Şekil 4.6 Farklı algoritmalar için yuvarlak şifrelemenin frekans değerleri



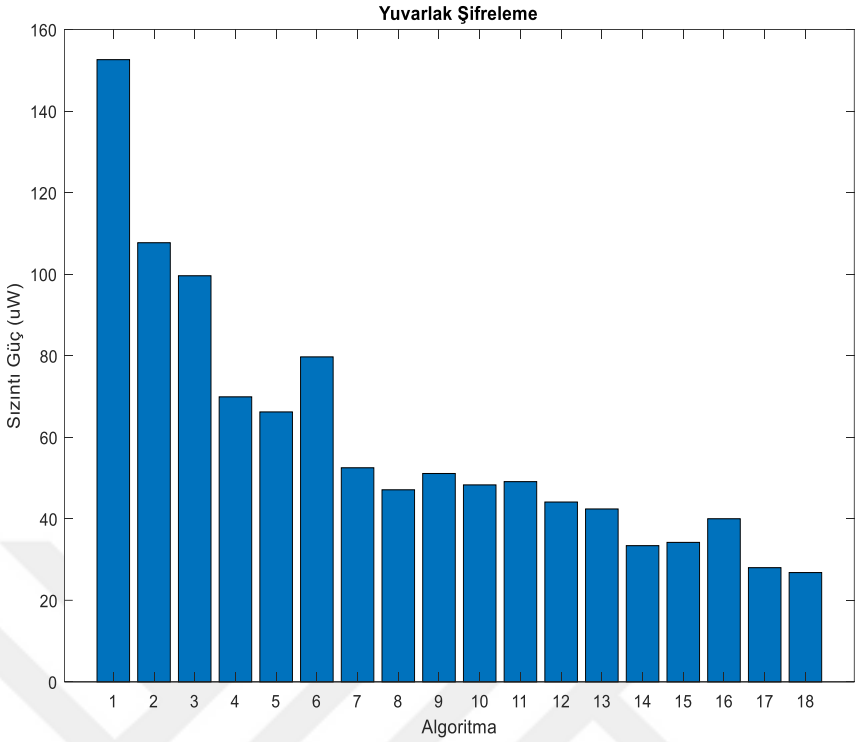
Şekil 4.7 Farklı algoritmalar için yuvarlak şifrelemenin verim değerleri



Şekil 4.8 Farklı algoritmalar için yuvarlak şifrelemenin alan değerleri



Şekil 4.9 Farklı algoritmalar için yuvarlak şifrelemenin maksimum değerleri



Şekil 4.10 Farklı algoritmalar için yuvarlak şifrelemenin sızıntı güç değerleri

Yuvarlak şifreleme tablosundaki frekans ve verim verileri değerlendirildiğinde minimum frekans değerinin SPECK(128/128) algoritması, maksimumun ise SIMON (64/96) algoritması olduğu görülmektedir. Verimde minimum değerde SPECK(128/128), maksimum değerde ise MIDORI(128/128) algoritması, güçte minimum değerde PICCOLO (64/80), maksimum değerde CAMELLIA(128/128), sızıntı güçte ise minimum değerde SPECK(32/64), maksimum değerde ise AES(128/12/) algoritmasının olduğu görülmektedir.

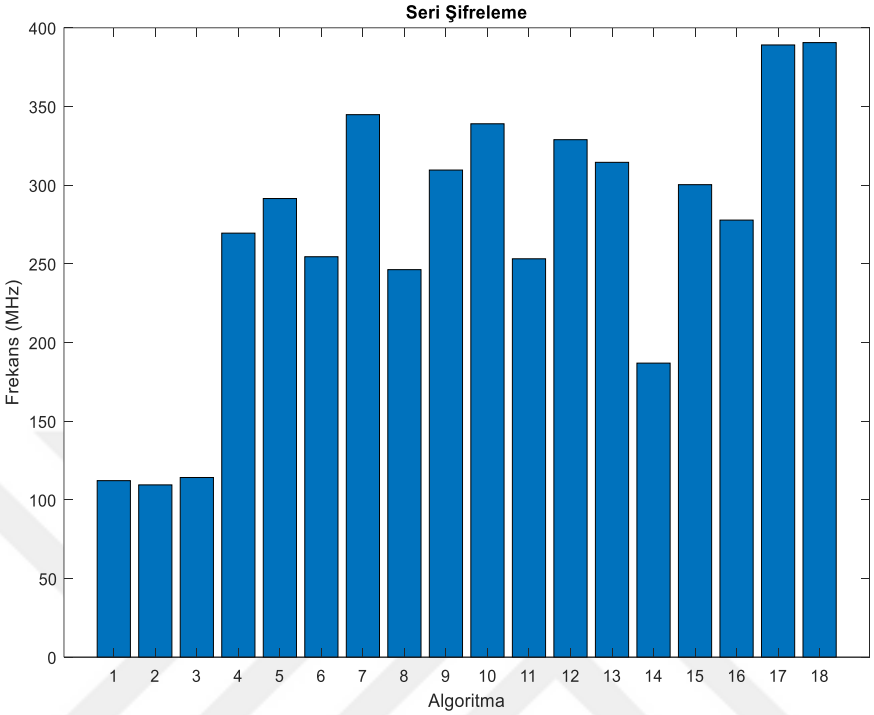
4.3 Seri Şifreleme

Tablo 4.3'te 18 farklı algoritma için seri şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

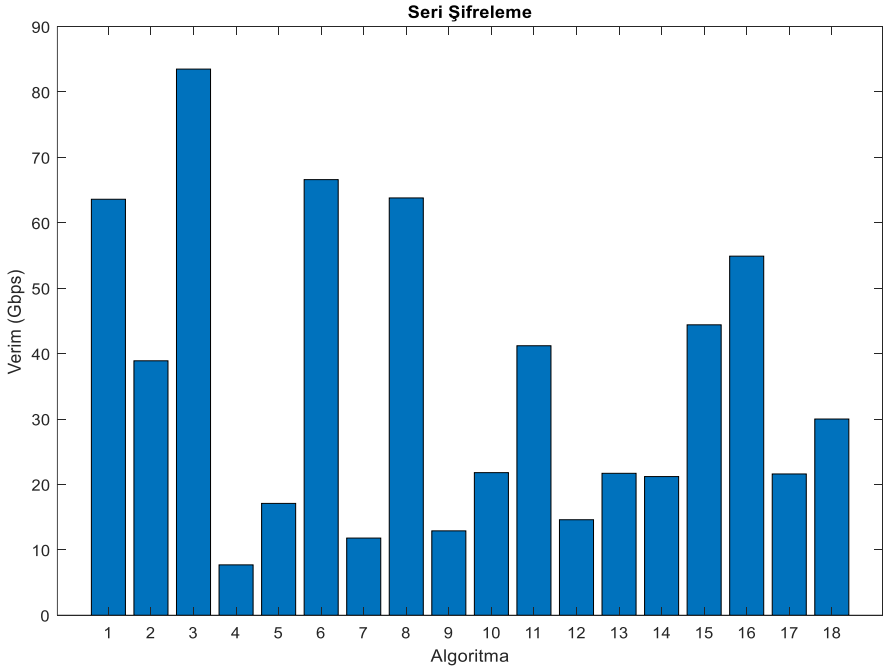
Tablo 4.3 Seri şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	**Frekans (MHz)**	**Verim (Gbps)**	**Alan (kgate)**	**Max Güç (mW)**	**Sızıntı Güç (µW)**
	Seri Şifreleme					
1	AES (128/128)	112.2	63.6	6.3	18.5	76.8
2	CAMELLIA (128/128)	109.5	38.9	6.6	14.4	66.1
3	CLEFIA(128/128)	114.2	83.5	6.2	13.1	61.3
4	SIMON (128/128)	269.5	7.7	4.8	8.2	47.1
5	SPECK (128/128)	291.5	17.1	5.0	8.2	48.4
6	MIDORI (128/128)	254.5	66.6	4.9	11.9	49.2
7	LED (64/128)	344.8	11.8	5.6	2.2	50.0
8	PRINCE (64/128)	246.3	63.8	3.9	8.7	40.0
9	SIMON (64/128)	309.6	12.9	3.7	4.8	36.2
10	SPECK (64/128)	339.0	21.8	3.9	5.4	37.4
11	MIDORI (64/128)	253.2	41.2	3.5	11.4	35.3
12	SIMON (64/96)	328.9	14.6	3.3	4.5	31.7
13	SPECK (64/96)	314.5	21.7	3.4	5.1	33.1
14	PRESENT (64/80)	186.9	21.2	3.9	3.4	36.4
15	PICCOLO (64/80)	300.3	44.4	3.5	2.0	28.5
16	TWINE (64/80)	277.8	54.9	4.1	2.8	29.6
17	SIMON (32/64)	389.1	21.6	2.2	3.7	20.8
18	SPECK (32/64)	390.6	30.0	2.3	5.5	21.9
MİNİMUM		**109.5**	**7.7**	**2.2**	**2.0**	**20.8**
ORTALAMA		**268.5**	**35.4**	**4.3**	**7.4**	**41.7**
MAKSİMUM		**390.6**	**83.5**	**6.6**	**18.5**	**76.8**

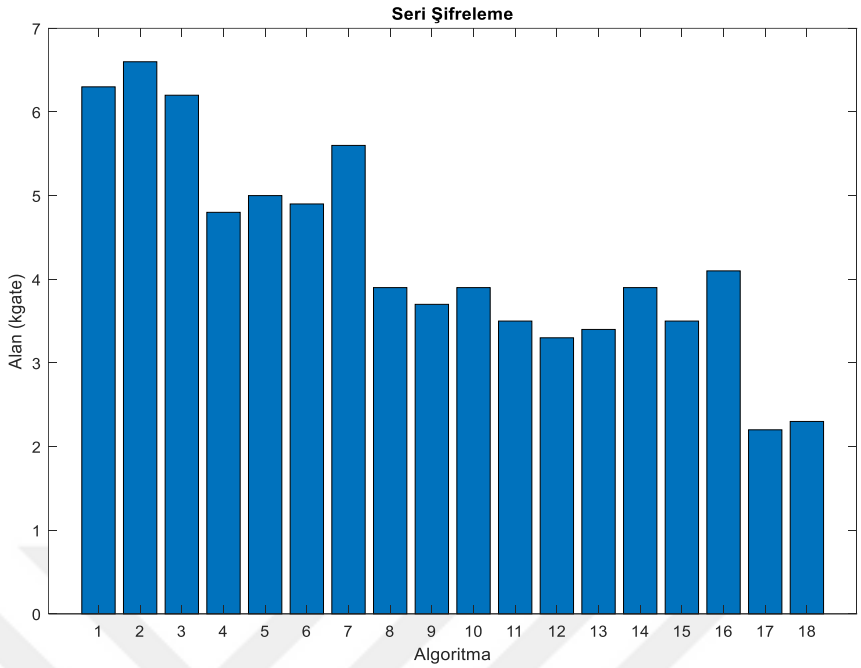
Aşağıda Şekil 4.11-4.15'te 18 farklı algoritma için seri şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



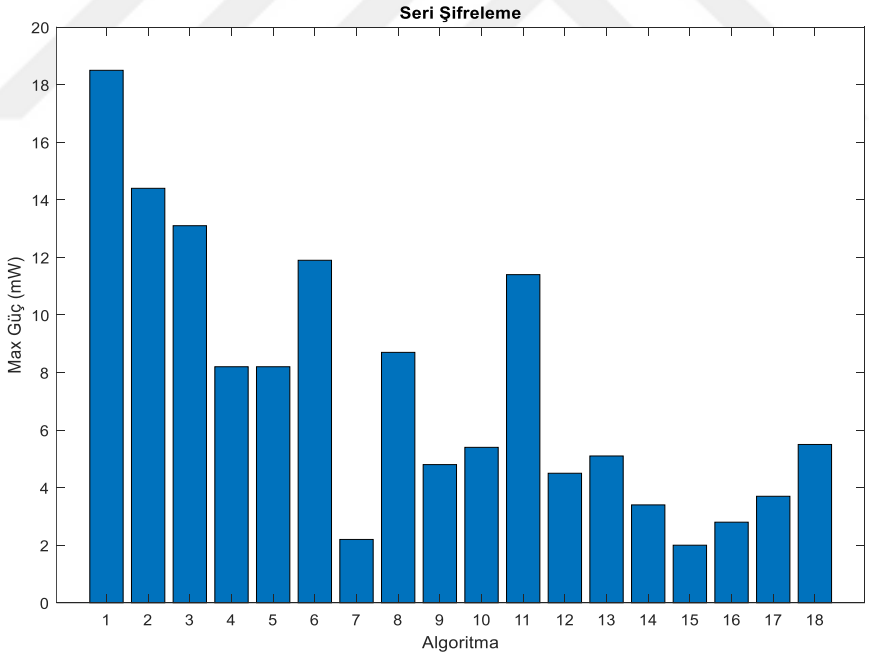
Şekil 4.11 Farklı algoritmalar için seri şifrelemenin frekans değerleri



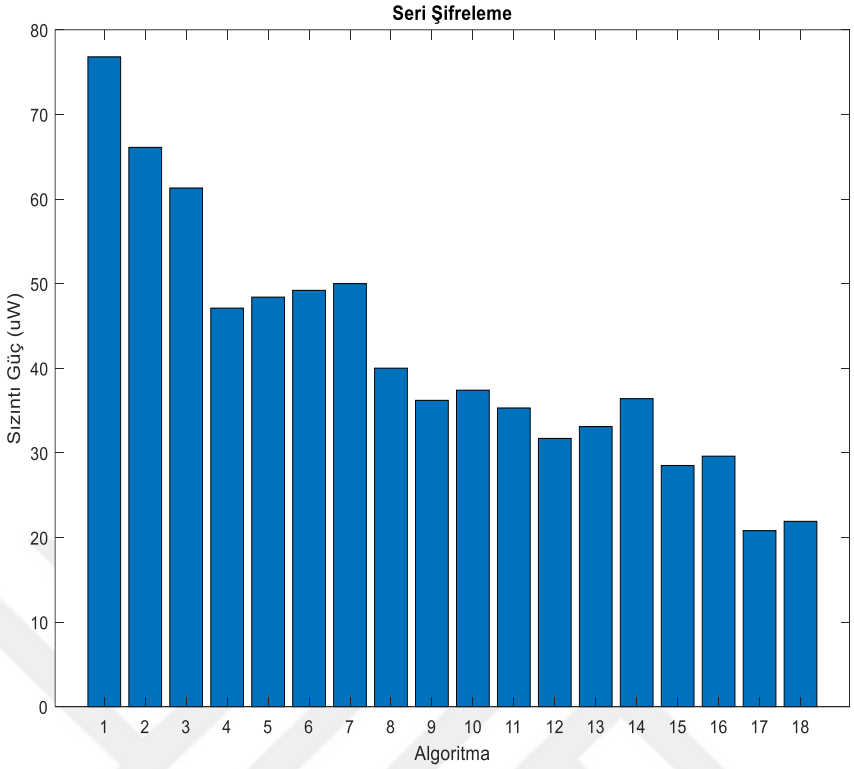
Şekil 4.12 Farklı algoritmalar için seri şifrelemenin verim değerleri



Şekil 4.13 Farklı algoritmalar için seri şifrelemenin alan değerleri



Şekil 4.14 Farklı algoritmalar için seri şifrelemenin maksimum güç değerleri



Şekil 4.15 Farklı algoritmalar için seri şifrelemenin sızıntı güç değerleri

Seri şifreleme tablosundaki frekans, verim ve güç verileri değerlendirildiğinde minimum frekans değerinin CAMELLIA(128/128) algoritması, maksimum değerin SPECK(32/64) algoritması, verimde minimum değerde SIMON(128/128) algoritması, maksimum değerde ise CLEFIA(128/128) algoritması, max. güçte minimum değerde PICCOLO (64/80), maksimum değerde de AES (128/128), sızıntı güçte ise minimum değerde SIMON (32/64), maksimumda ise AES (128/128) olduğu görülmektedir.

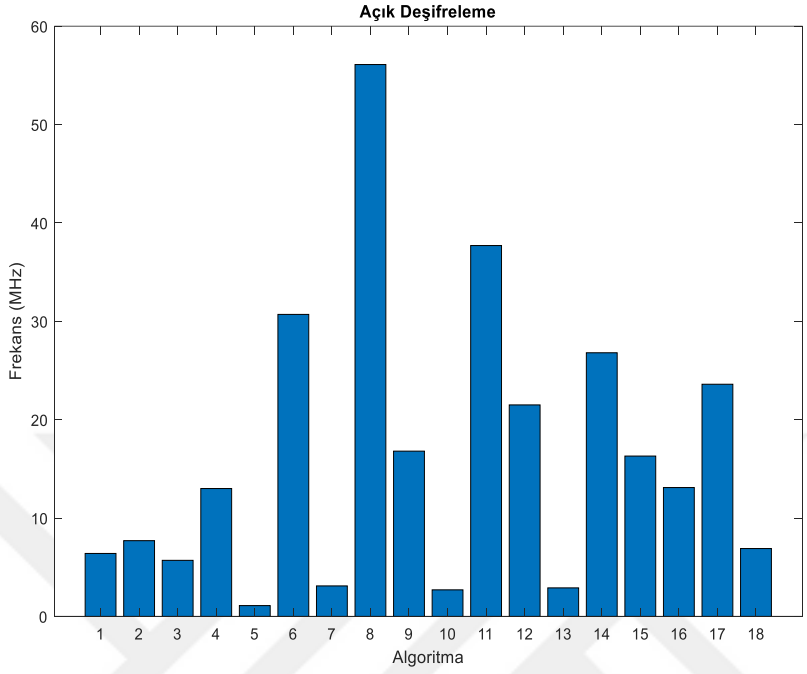
4.4 Açık Deşifreleme

Tablo 4.4'te 18 farklı algoritma için açık deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

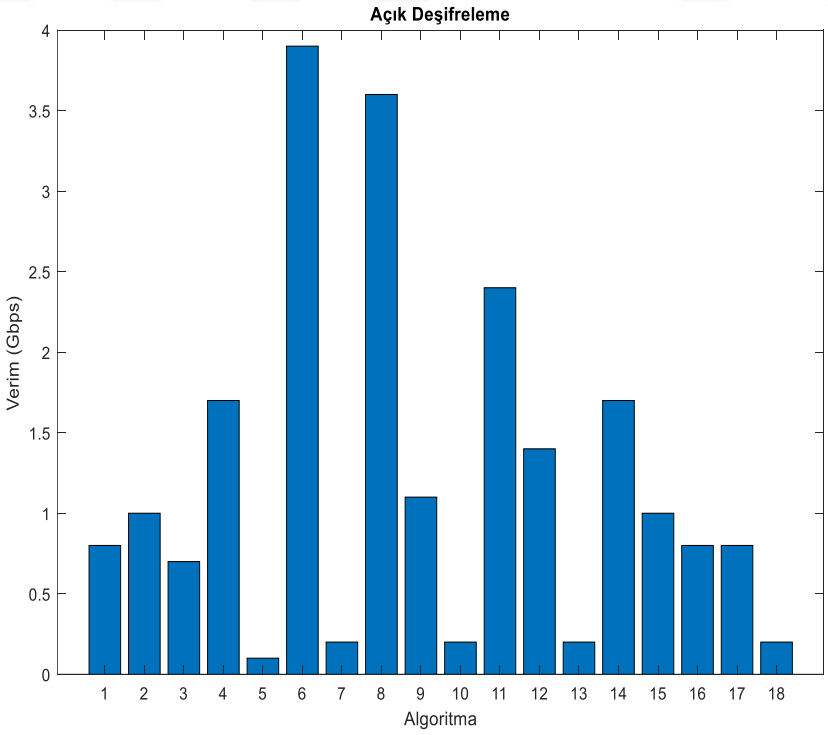
Tablo 4.4 Açık deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	Frekans (MHz)	Verim (Gbps)	Alan (kgate)	Max Güç (mW)	Sızıntı Güç (µW)
	Açık Deşifreleme					
1	AES (128/128)	6.4	0.8	144.2	294.3	1734.3
2	CAMELLIA(128/128)	7.7	1.0	63.4	133.8	754.9
3	CLEFIA (128/128)	5.7	0.7	74.3	195.5	891.0
4	SIMON (128/128)	13.0	1.7	74.1	187.0	803.7
5	SPECK (128/128)	1.1	0.1	69.1	127.1	672.5
6	MIDORI (128/128)	30.7	3.9	55.6	123.7	720.2
7	LED (64/128)	3.1	0.2	215.4	103.1	815.6
8	PRINCE (64/128)	56.1	3.6	10.1	29.1	108.2
9	SIMON (64/128)	16.8	1.1	27.5	83.2	299.1
10	SPECK (64/128)	2.7	0.2	29.9	62.3	290.8
11	MIDORI (64/128)	37.7	2.4	20.6	37.1	256.4
12	SIMON (64/96)	21.5	1.4	23.8	62.9	255.3
13	SPECK (64/96)	2.9	0.2	28.6	57.8	278.0
14	PRESENT (64/80)	26.8	1.7	43.8	127.8	505.4
15	PICCOLO (64/80)	16.3	1.0	22.8	64.8	264.0
16	TWİNE (64/80)	13.1	0.8	25.6	50.9	292.2
17	SIMON (32/64)	23.6	0.8	10.4	30.9	111.8
18	SPECK (32/64)	6.9	0.2	12.4	27.5	121.7
MİNİMUM		**1.1**	**0.1**	**10.1**	**27.5**	**108.2**
ORTALAMA		**16.2**	**1.2**	**52.9**	**99.9**	**509.7**
MAKSİMUM		**56.1**	**3.9**	**215.4**	**294.3**	**1734.3**

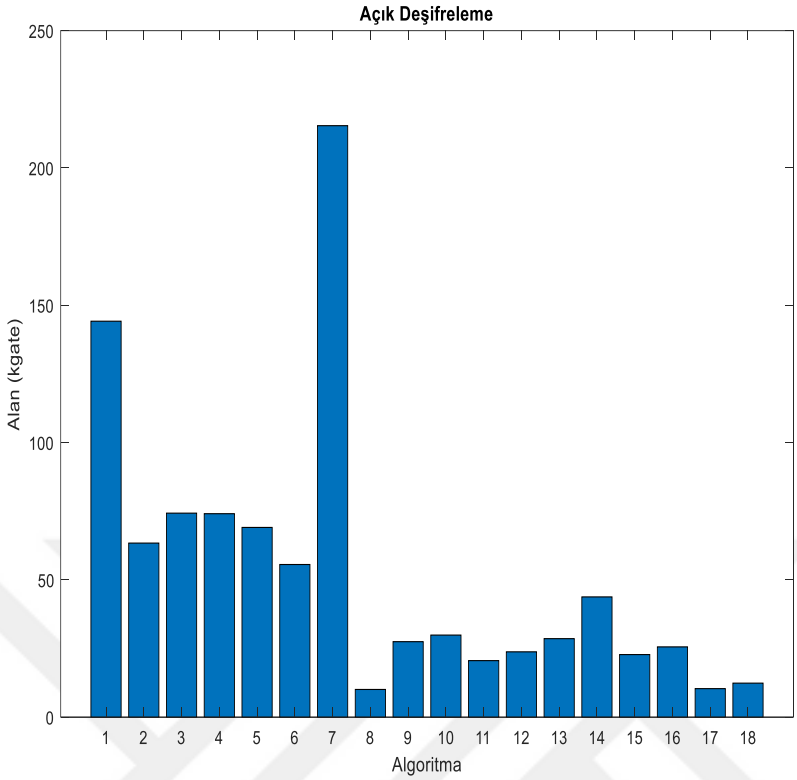
Aşağıda Şekil 4.16-4.20'de 18 farklı algoritma için açık deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



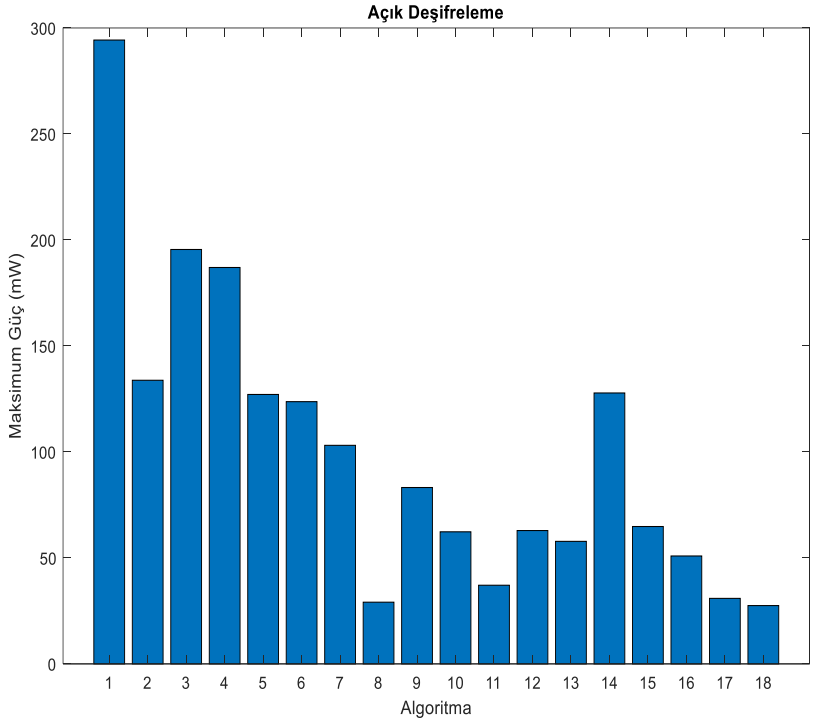
Şekil 4.16 Farklı algoritmalar için açık deşifrelemenin frekans değerleri



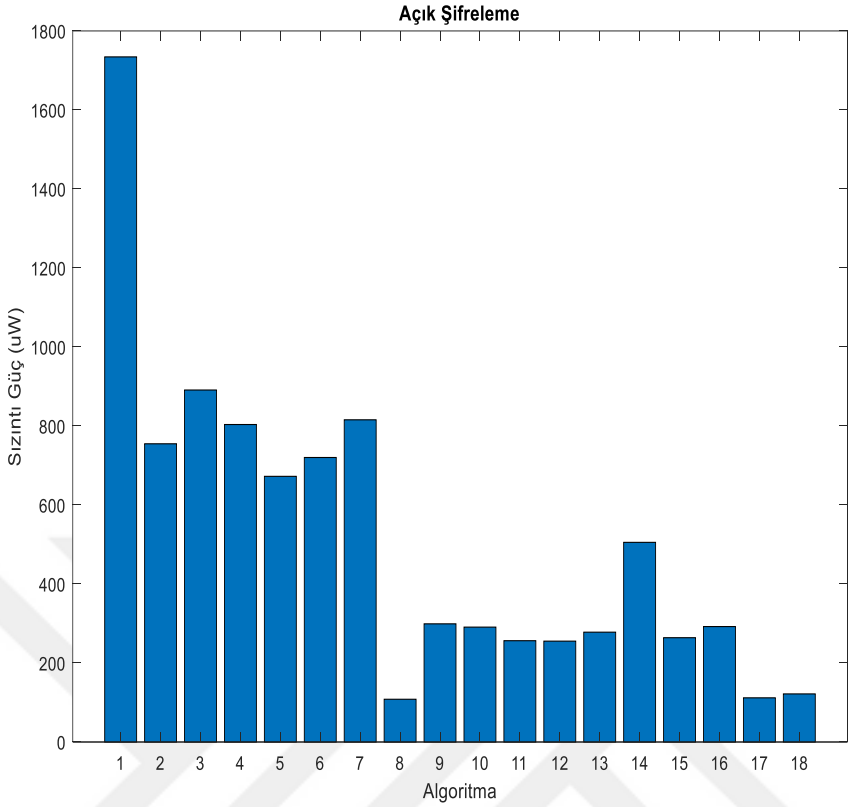
Şekil 4.17 Farklı algoritmalar için açık deşifrelemenin verim değerleri



Şekil 4.18 Farklı algoritmalar için açık deşifrelemenin alan değerleri



Şekil 4.19 Farklı algoritmalar için açık deşifrelemenin maksimum güç değerleri



Şekil 4.20 Farklı algoritmalar için açık deşifrelemenin sızıntı güç değerleri

Açık deşifreleme verileri değerlendirildiğinde frekansta minimum değerde, SPECK (128/128) maksimum değerde, PRINCE (64/128) algoritması görülmektedir. Verimde minimum değerde SPECK (128/128), maksimum değerde MIDORI (128/128), max. güçte minimum değerde SPECK (32/64), maksimum değerde AES (128/128), sızıntı güçte ise minimum değerde PRINCE (64/128) algoritması ve maksimum değerde de AES (128/128) algoritması görülmektedir.

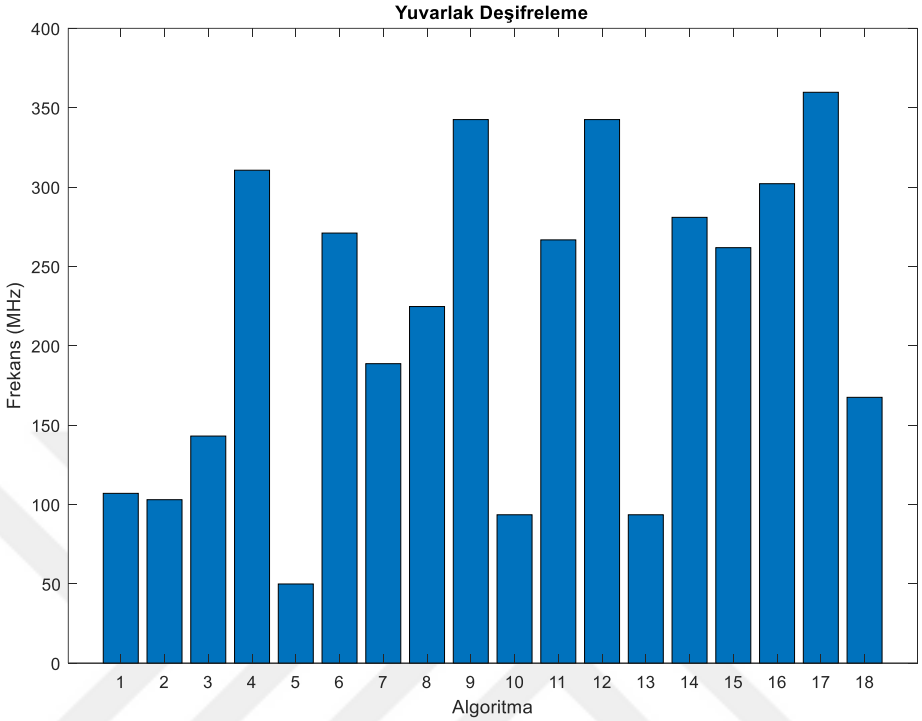
4.5 Yuvarlak Deşifreleme

Tablo 4.5'te 18 farklı algoritma için yuvarlak deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

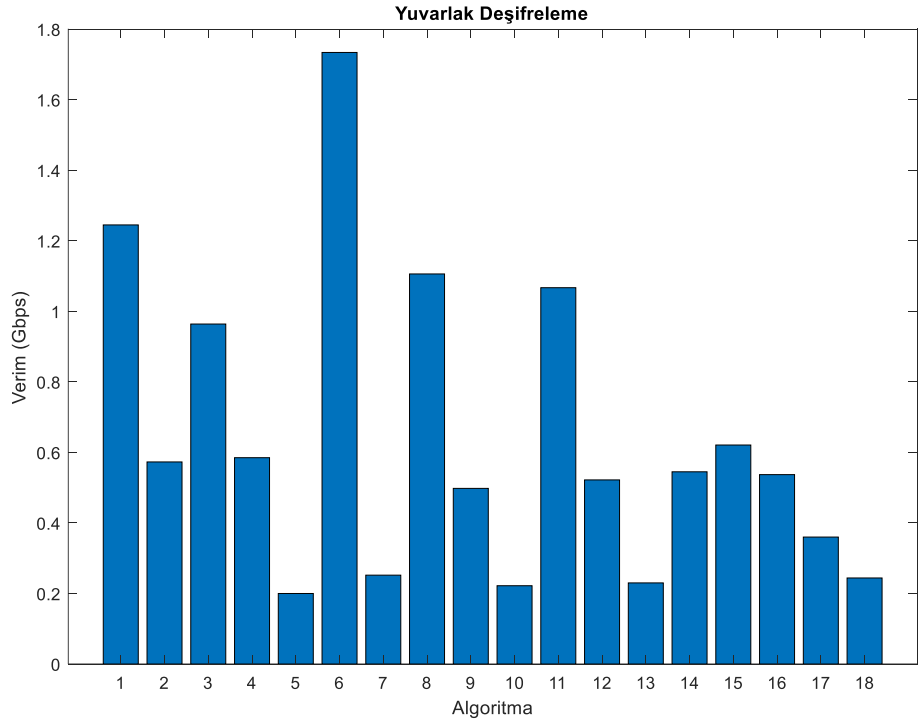
Tablo 4.5 Yuvarlak deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	**Frekans (MHz)**	**Verim (Gbps)**	**Alan (kgate)**	**Max Güç (mW)**	**Sızıntı Güç (µW)**
	Yuvarlak Deşifreleme					
1	AES (128/128)	107.0	1.245	18.7	44.1	193.6
2	CAMELLIA(128/128)	103.0	0.573	11.8	44.6	121.9
3	CLEFIA (128/128)	143.1	0.964	9.9	38.1	99.0
4	SIMON (128/128)	310.6	0.585	7.8	17.2	78.4
5	SPECK (128/128)	49.9	0.200	9.6	11.2	92.7
6	MIDORI (128/128)	271.0	1.734	8.4	11.9	96.9
7	LED (64/128)	188.7	0.252	7.2	6.5	66.6
8	PRINCE (64/128)	224.7	1.106	5.3	18.7	50.3
9	SIMON (64/128)	342.5	0.498	6.0	12.4	58.2
10	SPECK (64/128)	93.5	0.222	6.7	10.6	63.2
11	MIDORI (64/128)	266.7	1.067	5.3	11.4	57.5
12	SIMON (64/96)	342.5	0.522	5.1	11.6	49.9
13	SPECK (64/96)	93.5	0.230	5.9	9.9	55.7
14	PRESENT (64/80)	280.9	0.545	4.7	4.9	44.8
15	PICCOLO (64/80)	261.8	0.621	3.8	3.3	38.5
16	TWİNE (64/80)	302.1	0.537	4.7	4.5	42.8
17	SIMON (32/64)	359.7	0.360	3.3	9.9	31.8
18	SPECK (32/64)	167.5	0.244	3.6	8.7	34.1
MİNİMUM		**49.9**	**0.2**	**3.3**	**3.3**	**31.8**
ORTALAMA		**217.2**	**0.6**	**7.1**	**15.5**	**70.9**
MAKSİMUM		**359.7**	**1.7**	**18.7**	**44.6**	**193.6**

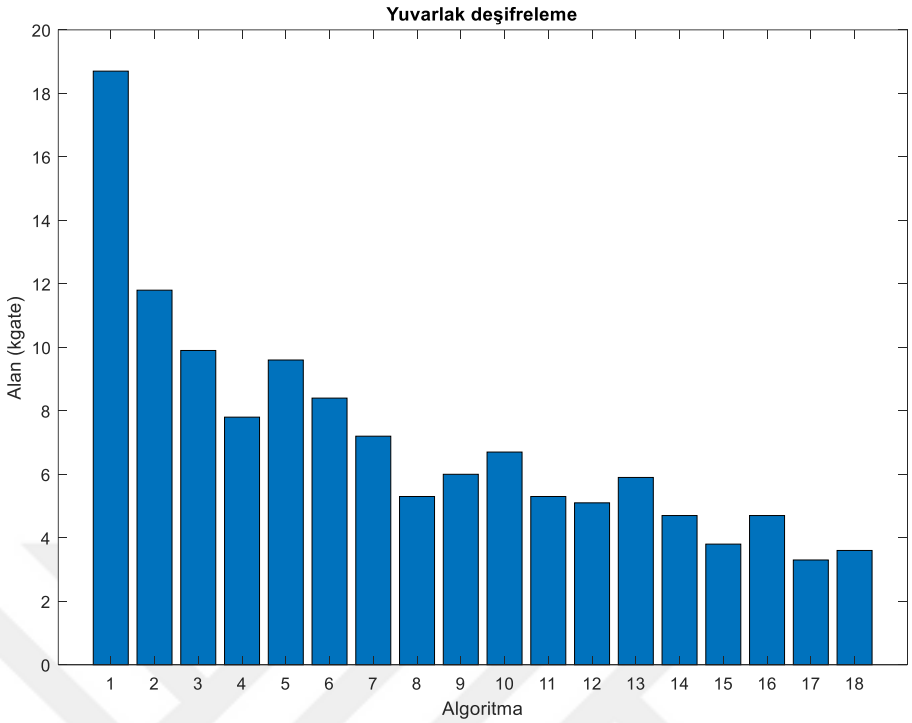
Aşağıda Şekil 4.21-4.25'te 18 farklı algoritma için yuvarlak deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



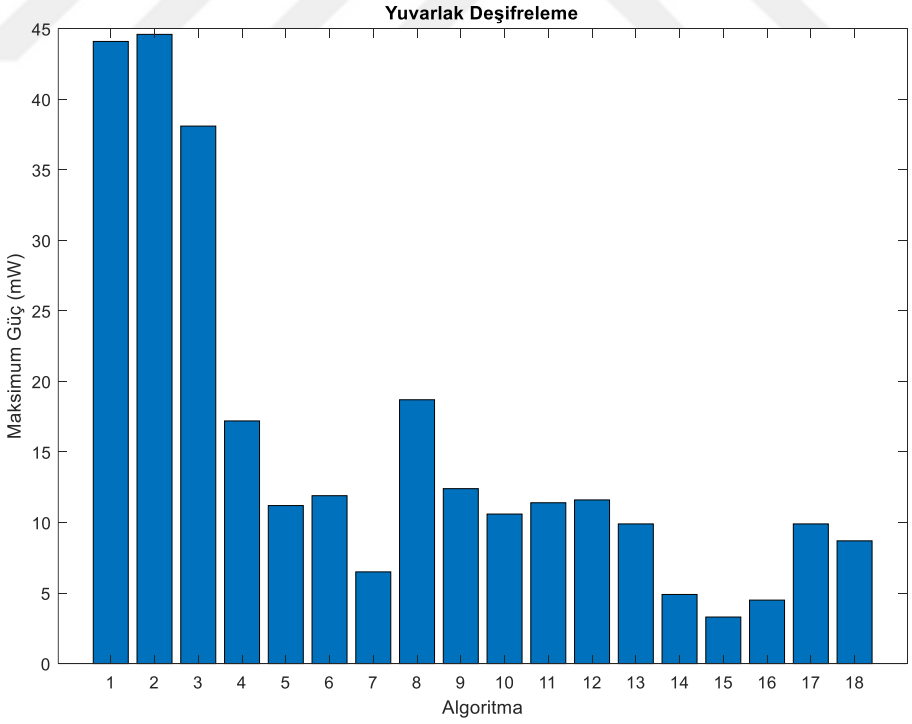
Şekil 4.21 Farklı algoritmalar için yuvarlak deşifrelemenin frekans değerleri



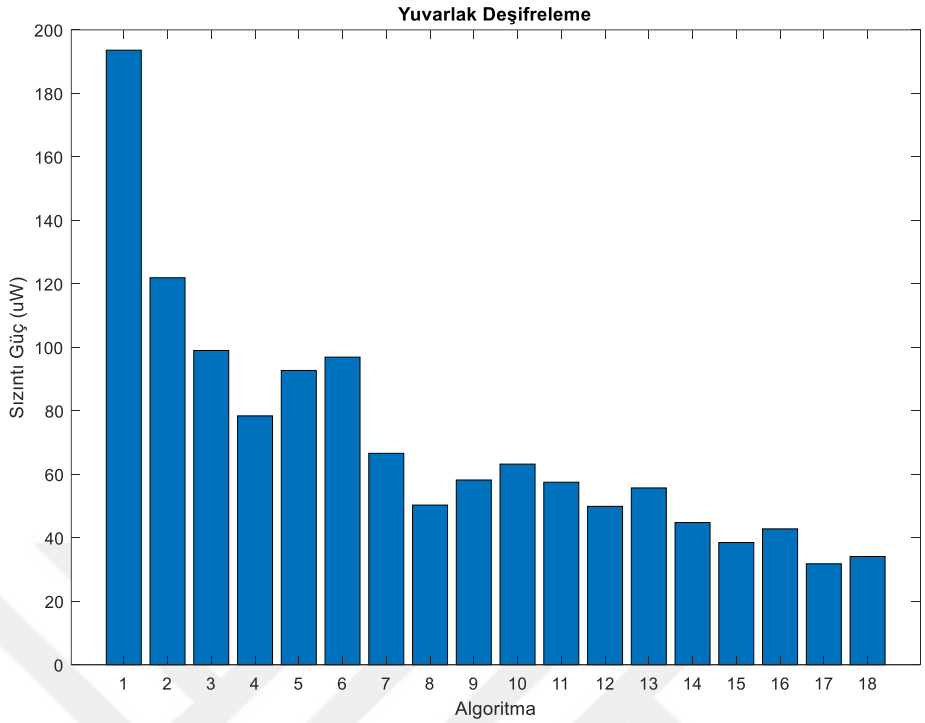
Şekil 4.22 Farklı algoritmalar için yuvarlak deşifrelemenin verim değerleri



Şekil 4.23 Farklı algoritmalar için yuvarlak deşifrelemenin alan değerleri



Şekil 4.24 Farklı algoritmalar için yuvarlak deşifrelemenin maksimum güç değerleri



Şekil 4.25 Farklı algoritmalar için yuvarlak deşifrelemenin sızıntı güç değerleri

Yuvarlak deşifreleme verileri değerlendirildiğinde frekansta minimum değerde CAPELLIA (128/128), maksimumda SPECK (64/128) algoritması, verimde minimumda SIMON (128/128/), maksimumda CLEFIA (128/128), güçte minimumda LED (64/128), maksimumda CAMELLIA (128/128), sızıntı güçte ise minumum değerde PICCOLO (64/80), maksimum değerde CAMELLIA (128/128/) algoritması olduğu görülmektedir.

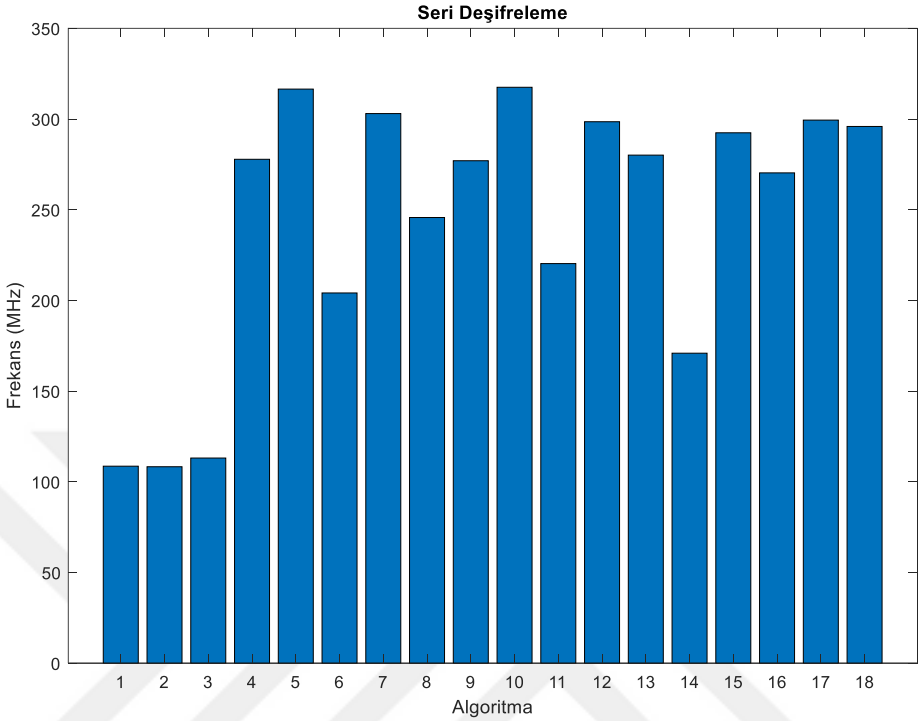
4.6 Seri Deşifreleme

Tablo 4.6'da 18 farklı algoritma için seri deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri verilmiştir.

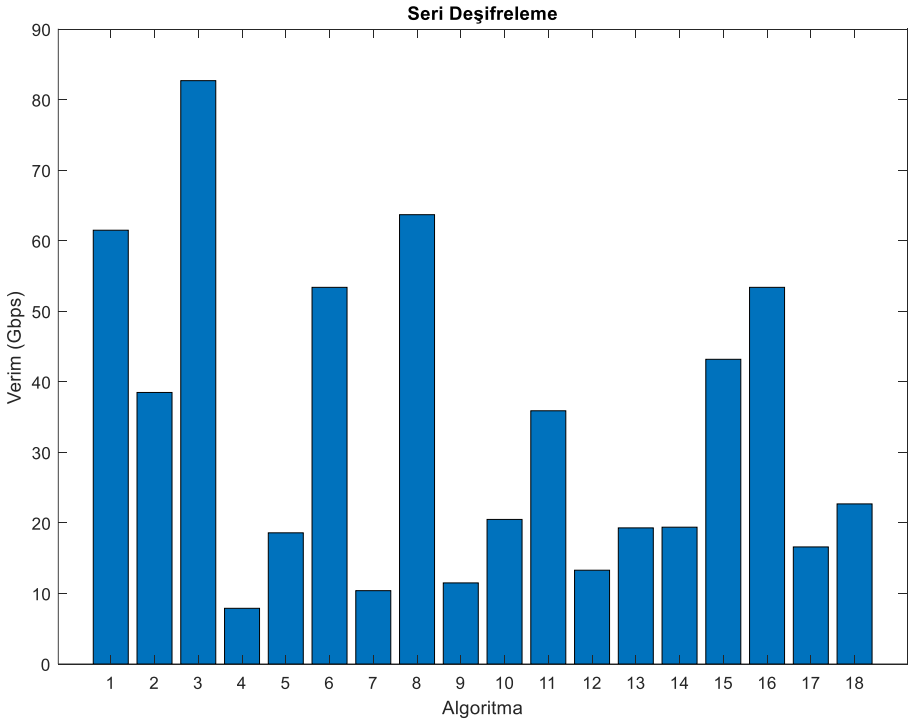
Tablo 4.6 Seri deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri

	Algoritma	Frekans (MHz)	Verim (Gbps)	Alan (kgate)	Max Güç (mW)	Sızıntı Güç (µW)
	Seri Deşifreleme					
1	AES (128/128)	108.6	61.5	7.2	14.5	61.2
2	CAMELLIA(128/128)	108.3	38.5	7.3	14.8	63.1
3	CLEFIA (128/128)	113.1	82.7	6.8	12.5	59.3
4	SIMON (128/128)	277.8	7.9	5.6	9.7	57.4
5	SPECK (128/128)	316.5	18.6	5.9	8.3	57.2
6	MIDORI (128/128)	204.1	53.4	5.3	11.9	53.9
7	LED (64/128)	303.0	10.4	6.9	1.4	34.5
8	PRINCE (64/128)	245.7	63.7	3.8	8.4	36.2
9	SIMON (64/128)	277.0	11.5	4.5	5.6	45.3
10	SPECK (64/128)	317.5	20.5	4.8	7.6	46.2
11	MIDORI (64/128)	220.3	35.9	3.8	11.4	37.7
12	SIMON (64/96)	298.5	13.3	3.9	5.1	39.0
13	SPECK (64/96)	280.1	19.3	4.1	7.6	40.1
14	PRESENT (64/80)	170.9	19.4	4.5	2.4	25.8
15	PICCOLO (64/80)	292.4	43.2	3.7	2.0	23.4
16	TWİNE (64/80)	270.3	53.4	4.2	2.6	28.4
17	SIMON (32/64)	299.4	16.6	2.6	4.1	25.7
18	SPECK (32/64)	295.9	22.7	2.8	6.3	27.3
MİNİMUM		**108.3**	**7.9**	**2.6**	**1.4**	**23.4**
ORTALAMA		**244.4**	**32.9**	**4.9**	**7.6**	**42.3**
MAKSİMUM		**317.5**	**82.7**	**7.3**	**14.8**	**63.1**

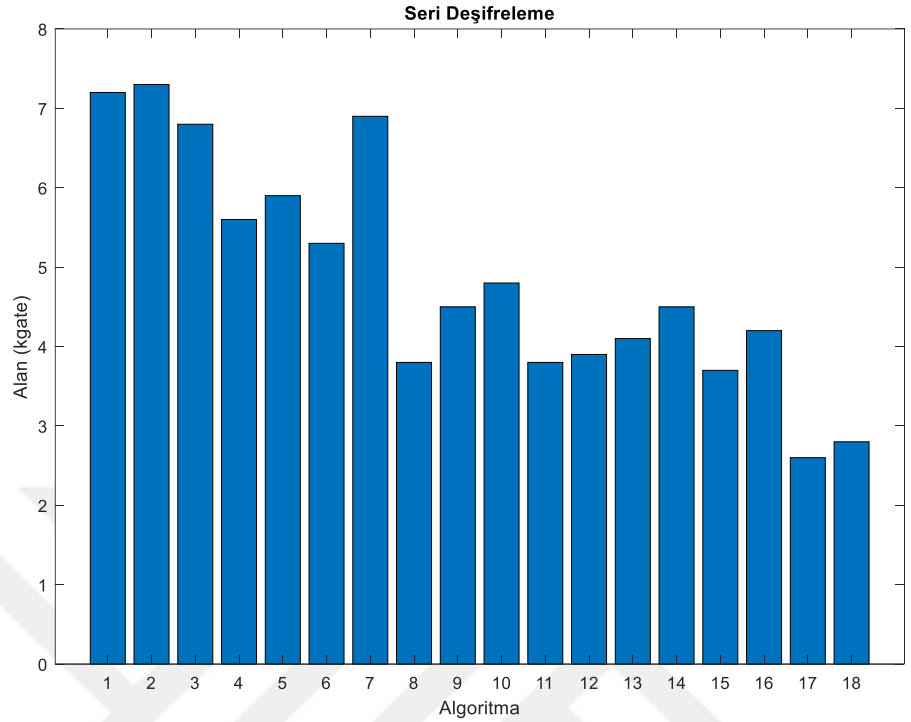
Aşağıda Şekil 4.26-4.30'da 18 farklı algoritma için seri deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç değerleri sunulmuştur.



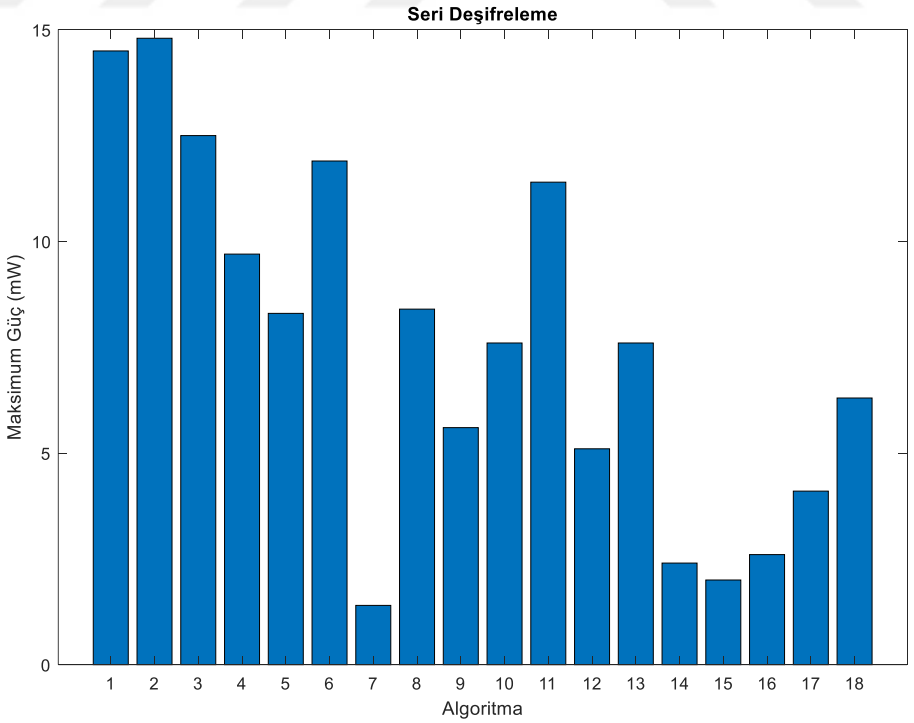
Şekil 4.26 Farklı algoritmalar için seri deşifrelemenin frekans değerleri



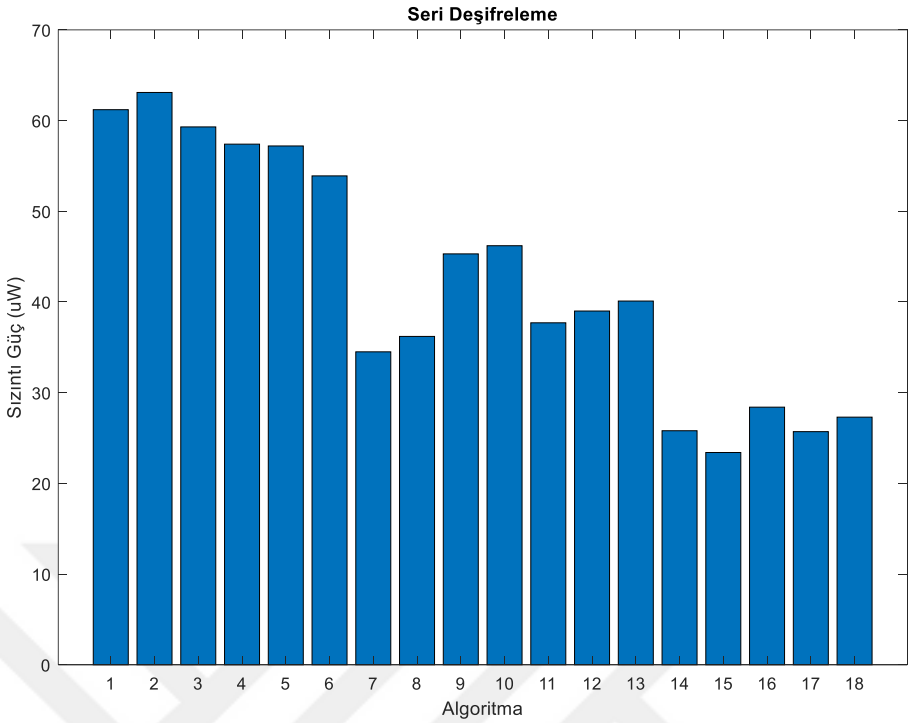
Şekil 4.27 Farklı algoritmalar için seri deşifrelemenin verim değerleri



Şekil 4.28 Farklı algoritmalar için seri deşifrelemenin alan değerleri



Şekil 4.29 Farklı algoritmalar için seri deşifrelemenin maksimum güç değerleri



Şekil 4.30 Farklı algoritmalar için seri deşifrelemenin sızıntı güç değerleri

Seri deşifreleme verileri değerlendirildiğinde frekansta minimum değerde CAMELLIA (128/128), maksimumda ise SPECK (64/128) görülmektedir. Verimde minimum değerde SIMON (1258/128), maksimumda CLEFIA (128/128) algoritması, max. güçte minimum değerde LED (64/128), maksimumda CAMELLIA (128/128), sızıntı güçte ise minimum değerde PICCOLO (64/80), maksimum değerde de CAMELLIA (128/128) algoritması görülmektedir.

5. SONUÇLAR VE ÖNERİLER

5.1 Sonuçlar

Açık şifrelemenin minimum, ortalama ve maksimum değerleri Tablo 5.1'de sunulmaktadır.

Tablo 5.1 Açık şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

AÇIK ŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**3.2**	**0.4**	**8.2**	**17.3**	**78.0**
ORTALAMA	**23.3**	**1.7**	**34.1**	**80.2**	**382.4**
MAKSİMUM	**57.1**	**4.9**	**78.8**	**195.5**	**939.6**

Yuvarlak şifreleme değerleri de Tablo 5.2'de sunulmuştur.

Tablo 5.2 Yuvarlak şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

YUVARLAK ŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**50.3**	**0.2**	**2.9**	**3.4**	**26.8**
ORTALAMA	**241.6**	**0.7**	**6.2**	**15.1**	**59.6**
MAKSİMUM	**392.2**	**2.5**	**15.4**	**46.6**	**152.6**

Son olarak seri şifreleme değerleri Tablo 5.3'te sunulmuş ve en iyi verim değerlerinin bu şifreleme çeşidinde olduğu gözlemlenmiştir.

Tablo 5.3 Seri şifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

SERİ ŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**109.5**	**7.7**	**2.2**	**2.0**	**20.8**
ORTALAMA	**268.5**	**35.4**	**4.3**	**7.4**	**41.7**
MAKSİMUM	**390.6**	**83.5**	**6.6**	**18.5**	**76.8**

Veriler incelendiğinde en iyi verim alınan şifreleme tekniğinin, tüketilen maksimum güç ve sızıntı gücün diğer şifreleme tekniklerine göre nispeten daha az olduğu seri şifreleme tekniği olduğu gözlemlenmiştir. Alanın da daha az ve frekansın ise daha yüksek olması beklenir.

Açık deşifrelemenin minimum, ortalama ve maksimum değerleri Tablo 5.4'te sunulmaktadır.

Tablo 5.4 Açık deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

AÇIK DEŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**1.1**	**0.1**	**10.1**	**27.5**	**108.2**
ORTALAMA	**16.2**	**1.2**	**52.9**	**99.9**	**509.7**
MAKSİMUM	**56.1**	**3.9**	**215.4**	**294.3**	**1734.3**

Yuvarlak deşifreleme değerleri de Tablo 5.5'te sunulmuştur.

Tablo 5.5 Yuvarlak deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

YUVARLAK DEŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**49.9**	**0.2**	**3.3**	**3.3**	**31.8**
ORTALAMA	**217.2**	**0.6**	**7.1**	**15.5**	**70.9**
MAKSİMUM	**359.7**	**1.7**	**18.7**	**44.6**	**193.6**

Son olarak seri deşifreleme değerleri Tablo 5.6'da sunulmuş ve en iyi verim değerlerinin bu deşifreleme çeşidinde olduğu gözlemlenmiştir.

Tablo 5.6 Seri deşifrelemenin frekans, verim, alan, maksimum ve sızıntı güç istatistik değerleri

SERİ DEŞİFRELEME					
	Frekans	**Verim**	**Alan**	**Max Güç**	**Sızıntı Güç**
MİNİMUM	**108.3**	**7.9**	**2.6**	**1.4**	**23.4**
ORTALAMA	**244.4**	**32.9**	**4.9**	**7.6**	**42.3**
MAKSİMUM	**317.5**	**82.7**	**7.3**	**14.8**	**63.1**

Deşifreleme tekniği verileri incelendiğinde benzer şekilde en iyi verim alınan tekniğin tüketilen maksimum ve sızıntı gücün diğer tekniklere oranla daha az olduğu seri deşifreleme tekniği olduğu görülmektedir. Aynı zamanda alanın daha küçük ve frekans değerlerinin ise daha yüksek olması beklenir.

5.2 Öneriler

Belirli uygulamalara odaklanan birçok hafif kriptografi yani düz şifreleme algoritması piyasada bulunmaktadır. Uygulandıklarında performans eşit olmayabilir veya güvenlik yeterli olmayabilir. Bu bağlamda, hafif algoritmalar sınıfında yer alan kısıtlı cihazların özel tasarlanmış ve minimize edilmiş algoritmalara ihtiyacı bulunmaktadır. Bu algoritmaların çokluğuna ve bir kısmının verimliliğine rağmen, hafif kriptografi algoritmalarında aynı zamanda kısıtlı cihazların özelliklerini de dikkate almak gerekir. Gerekli güvenlik seviyesini elde etmek daha zor olduğundan dolayı daha seçici ve iyi algoritma ve çözüm yolları geliştirmeye ve aramaya ihtiyaç duyulmaktadır. Bu nedenle mevcut algoritmalar frekans, verim ve güç performans özellikleri açısından değerlendirilip en iyi algoritmanın tercih edilmesi gerekmektedir.

KAYNAKLAR

[1]. B. Sun, C.-C. Li, K. Wu ve Y. Xiao, "A lightweight secure protocol for wireless sensor networks," Computer Communications, vol. 29, pp. 2556–2568, Mart 2006.

[2]. W. K. Koo, H. Lee, Y. H. Kim ve D. H. Lee, "Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable forWireless Sensor Networks," International Conference on Information Security and Assurance, pp. 73-76, 2008.

[3]. S.S. M. AlDabbagh ve I. Shaikhli, "Lightweight Block Ciphers: A Comparative Study," Journal of advanced computer science and technology research, vol. 2(4), pp. 159-165, Kasım 2012.

[4]. Manjulata, A. K. (2014), "Survey on Lightweight Primitives and Protocols for RFID in Wireless Sensor Networks." International Journal of Communication Networks and Information Security (IJCNIS), vol. 6(1), pp. 29-43, Nisan 2014.

[5]. S. T. Pate ve N. H. Mistry, "A Survey: Lightweight Cryptography in WSN," IEEE International Conference on Communication Networks (ICCN), pp. 11-15, 2015.

[6]. S. A. Bragadeesh ve A. Umamakeswari, "Secure Data Aggregation for Wireless Sensor Network using Lightweight Cryptography," Indian Journal of Science and Technology, vol. 9(48), pp. 1-6, Aralık 2016.

[7]. H. Tawalbeh, S. Hashish, L. Tawalbeh ve A. Aldairi, "Security in Wireless Sensor Networks Using Lightweight Cryptography," Journal of Information Assurance and Security, vol. 12, pp.118-123, Kasım 2017.

[8]. C. A. Nino, A. Diaz-Perez ve M. M. Sandoval, "Energy and Area Costs of Lightweight Cryptographic Algorithms for Authenticated Encryption in WSN," Hindawi Security and Communication Networks, vol. 2018, pp. 1-14, Eylül 2018.

[9]. O. A. Khashan, R. Ahmad ve M. Khafajah, "An automated lightweight encryption scheme for secure and energy-efficient communication in wireless sensor networks," Elsevier, Ad Hoc Networks, vol. 115, pp. 1-14, Ocak 2021.

[10]. M. N. Khan, A. Rao ve S. Camtepe, "Lightweight Cryptographic Protocols for IoT-Constrained Devices: A Survey," IEEE Internet og Things Journal, vol. 8(6), pp. 4132-4156, Mart 2021.

[11]. V. A. Thakor, M. A. Razzaque ve M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," IEEE Access Journal, vol. 9, pp. 28177-28193, Şubat 2021.

[12]. M. Rana, Q. Mamun ve R. Islam, "Lightweight cryptography in IoT networks: A survey," Elsevier Journal, vol. 129, pp. 77-89, Kasım 2021.

[13]. M. S. Ibrahim, Y. A. Abbas ve M. H. Ali, "The Performance of Various Lightweight Block Ciphers FPGA Architectures: A Review," Al-Iraqia Journal for Scientific Engineering Research, vol. 1, pp. 124-129, Eylül 2022.

[14]. K. Tsantikidou ve N. Sklavos, "Hardware Limitations of Lightweight Cryptographic Designs for IoT in Healthcare," MDPI Journal, vol. 6(45), pp. 1-13, Eylül 2022.

[15]. Y. Guang, L. Yu, W. Dong, Y. Wang, J. Zeng, J. Zhao ve Q. Ding, “Chaos-Based Lightweight Cryptographic Algorithm Design and FPGA Implementation,” MDPI Journal, vol. 24, pp. 1-23, Kasım 2022.

[16]. P. Prakasam, M. Madheswaran, K. P. Sujith ve M. S. Sayeed. “Low Latency, Area and Optimal Power Hybrid Lightweight Cryptography Authentication Scheme for Internet of Things Applications,” Wireless Personal Communications, vol. 126, pp. 351-365, Mayıs 2022.

[17]. N. Im, S. Choi, ve H. Yoo, “S-Box Attack Using FPGA Reverse Engineering for Lightweight Cryptography,” IEEE Internet of Things Journal, vol. 9(24), pp. 25165-25180, Aralık 2022.

[18]. V. Bhagat, S. Kumar, S.K. Gupta ve M. K. Chaube, “Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications,” WILEY, Research Article, vol. 35, pp. 1-27, Temmuz 2022.

[19]. R. P. Puneeth ve G. Parthasarathyb, “Security and Data Privacy of Medical Information in Blockchain Using Lightweight Cryptographic System,” International Journal of Engineering, vol. 36(5), pp. 925-933, Mayıs 2023.

[20]. Z. Dewamuni, B. Shanmugam, S. Azam ve S. Thennadil, “Bibliometric Analysis of IoT Lightweight Cryptography,” MDPİ, Journal, vol. 14, pp. 1-31, Kasım 2023.

[21]. R. Neve, Dr. R. Bansode ve V. Kaul, “Novel Lightweight Approach to Perform Cryptography for Data Security & Privacy in IoT Mobile Devices,” International Journal of Intelligent Systems and Applications in Engineering, vol. 11(9), pp. 822-828, Temmuz 2023.

[22]. S. Windarta, S. Suryadi, K. Ramli, A. A. Lestari, W. Wildan, B. Pranggono ve R.W. Wardhani, “Two New Lightweight Cryptographic Hash Functions Based on Saturnin and Beetle for the Internet of Things,” IEEE Access: The Multidisciplinary Open Access Journal, vol. 11, pp. 84074-84090, Ağustos 2023.

[23]. Pfleeger, C.P. 1997. The fundamentals of information security. Software, IEEE

14 (1,14)

[24]. Saadin Oyucu, Hüseyin Polat, Bir Bütün Olarak M2M ve IoT Güvenliği, Conferece ISCTURKEY 2017

[25]. Winkler, T.; Rinner, B. Security and Privacy Protection in Visual Sensor Networks: A Survey. ACM Comput. Surv. 2014, 47, 97–116

[26]. Dargie, W. and Poellabauer, C. (2010). Fundamentals of wireless sensor networks: theory and practice. John Wiley and Sons. pp.168–183, 191–192. ISBN 978-0-470-99765-9.

[27]. Tuncay Soylu, "Kablosuz Algılayıcı Ağların Uygulama Alanları ve Bir Algılayıcı Düğüm Tasarımı" Yüksek Lisans Tezi, Temmuz, 2012

[28]. I. Butun, P. Österberg, H. Song "Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures” IEEE Communications Surveys & Tutorials, vol.22, Issue: 1, pag.616- 644 2020

[29]. Ivana Tomi; Julie A. McCann, “A Survey of Potential Security Issues in Existing Wireless Sensor Network Protocols" IEEE Internet of Things Journal (Volume: 4, Issue: 6, Dec. 2017)

[30]. Bilgi Teknolojileri ve İletişim Kurumu, "Milli Frekans Planı” 2019

[31]. E.Söğüt, O.Ayhan Erdem, “Günümüzün Vazgeçilmez Sistemleri: Nesnelerin Haberleşmesi ve Kullanılan Teknolojiler” AB 2017 Akademik Bilişim Konferansları, 2017

[32]. Mutlu A. K., Sürmeli C. “Mikrodenetleyiciler ile Seri İletişim” İstanbul: Kodlab Yayınları 2015

[33]. The Bluetooth Special Interest Group (SIG), “The history of the Bluetooth SIG” https://www.bluetooth.com/about-us/our-history/ Son Erişim Tarihi: Nisan 2020

[34]. Arslan, O. (2009). ZIGBEE ile Bina İçi Güvenlik Otomasyon Sistemi. (Yayınlanmamış Lisans Tezi). İstanbul: İstanbul Teknik Üniversitesi

[35] R. A. Mollin, An Introduction to criptography, Chapman and Holl, CRC, 2007.

[36] R. Kurzweil, The law of accelerating returns, in Alan Turing: Life and Legacy

of a Great Thinker, pp. 381–416, Springer, Berlin, Heidelberg, 2004.

[37] Z. Çamur, “A Study of Lightweight Cryptography”, Midele East Technical University, MT, July 2020.

[38] R. Kurzweil, The law of accelerating returns, in Alan Turing: Life and Legacy

of a Great Thinker, pp. 381–416, Springer, Berlin, Heidelberg, 2004.

[39] Kay, L. Bassham, M. Sönmez Turan, and N. Mouha, Report on lightweight cryptography, 2017, NIST Internal Report (IR) 8114.

[40] A. Al-Janabi, “A Lightweight Cryptography Algoraithm for Smart Cities and IoT”, İstanbul Commerce University, February 2020.

[41] Christopher Swenson "Modern Cryptanalysis Techniques For Advanced Code Breaking" Chapter 5, General Cryptanalytic Methods

[42] Ümit Günden, Şifreleme Algoritmalarının Performans Analizi, Yüksek Lisans

Tezi 2010

[43] "A Brief History of Cryptography", Cypher Research Laboratories, 24 Şubat 2006, Son Erişim Nisan 2021.

[44] Ülker, Ülkü. "Klasik Teknikler Kullanılarak Bir Kriptografi Algoritması Geliştirilmesi ve Des Algoritması ile." 2014

[45] Steven M. Bellovin, “Vernam, Mauborgne, and Friedman: The One-Time Pad and the Index of Coincidence” 2014.

[46] M.Ü. Çeşmeci, Elektronik Çağ Öncesi Dönem Kriptoloji Tarihi, Tübitak UEKAE Dergisi, Sayı 01, Eylül/Aralık 2009.

[47] Samet Akkuş, "Gömülü Sistem Tabanlı, Kriptolu TCP/IP Veri Haberleşmesi Uygulaması" Yüksek Lisans Tezi, 2015

[48] U.K. Boyacı, Günümüzde Kriptoloji, Tübitak UEKAE Dergisi, Sayı 01, Eylül/Aralık 2009.

[49] CRYPTREC, Cryptographic Technology Guideline (Lightweight Cryptography), Lightweight Cryptography Working Group, March 2017.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyad, Ad	KARATAŞ, Dilan
Web sayfası (Research Gate, Academia, vs.)	

Eğitim Bilgileri

Derece	Kurum	Mezuniyet Yılı
Yüksek Lisans	Dicle Üniversitesi	2021 – 2024
Lisans	Dicle Üniversitesi	2014 - 2019
Lise	Sezai Karakoç Anadolu Lisesi	2009 - 2013

İş Deneyimi

Dönem (Yıl)	Şirket, Kurum	Görev
Mart 2021 – Haziran 2021	Lila Kozmetik A.Ş.	Üretim Mühendisi
Şubat 2022 – Haziran 2022	Eds Grup Elektronik Ltd. Şti.	Satış Mühendisi
Haziran 2022 – Devam ediyor	Türk Telekom A.Ş.	Veri Mühendisi

Yabancı Dil

İngilizce

Yayınlar

1.Dilan Karataş ve Muhittin BAYRAM, Kablosuz Sensör Ağlarının Güvenliğinde Hafif Kriptografi, DUFEBLAS-2024, Diyarbakır, TÜRKİYE.

Özel İlgiler

Haberleşme, Network ve Bilgi İşlem Teknolojileri.

DİCLE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
TEZ BENZERLİK BİLDİRİMİ FORMU

Öğrencinin Adı, Soyadı	Dilan KARATAŞ		
Öğrenci No	21805004		
Ana Bilim Dalı	Elektrik Elektronik Mühendisliği		
Program Türü	Proje ☐	Yüksek Lisans ✕	Doktora ☐
Tez Danışmanı (Ünvanı, Adı, Soyadı)	Dr. Öğr. Üyesi Muhittin BAYRAM		
(Varsa) II. Tez Danışmanı (Ünvanı, Adı, Soyadı)			
Tez Başlığı	Kablosuz Sensör ağlarının Güvenliğini Sağlamada Hafif Kriptografinin Kullanılması		
RAPOR BİLGİLERİ			
Raporlama Aşaması	Tez Savunma Sınavı Sonrası		
Sayfa Sayısı	63		
Raporlama Tarihi	25.06.2024		
Benzerlik Oranı (%)	17		

Yukarıda bilgileri verilen tez çalışmamın toplam 63 sayfalık kısmına ilişkin, 25/06/2024 tarihinde şahsım/tez danışmanım tarafından Turnitin isimli intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan intihal raporuna göre, tezimin benzerlik oranı % 17 olarak tespit edilmiştir.

Uygulanan filtrelemeler:

☐Başlangıç Bölümleri (Kabul ve Onay sayfası, Teşekkür sayfası, Özet/Abstract) hariç

☐Kaynaklar hariç

☐Alıntılar hariç/dâhil

✕ Diğer (Herşey dahil)

Tezimin benzerlik oranı, Dicle Üniversitesi Fen Bilimleri Enstitüsü İntihal Raporu Uygulama Esaslarında belirtilen üst sınır benzerlik oranını aşmamaktadır. Tez benzerlik oranı üst sınır benzerlik oranının altında olsa dahi aksinin tespit edilmesi durumunda her türlü yasal sorumluğu kabul ettiğimi ve hukuki sonuçlarına razı olduğumu bildirir, gereğini arz ederim.

Öğrencinin Adı, Soyadı: Dilan KARATAŞ
Tarih: 25.06.2024
İmza:

Danışman Adı, Soyadı: Dr. Öğr. Üyesi Muhittin BAYRAM Tarih: 25.06.2024	İmza:
Ana Bilim Dalı Başkanı Adı, Soyadı: Doç. Dr. Cafer BUDAK Tarih: 25.06.2024	İmza: