

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIFIR BİLGİ İSPATI
TABANLI
KİMLİK DOĞRULAMA

ALİCAN BEYDEMİR
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2018

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIFIR BİLGİ İSPATI
TABANLI
KİMLİK DOĞRULAMA

ALİCAN BEYDEMİR
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2018

T.R.
GEBZE TECHNICAL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ZERO KNOWLEDGE PROOF
BASED
AUTHENTICATION

ALİCAN BEYDEMİR
A THESIS SUBMITTED FOR THE DEGREE OF
MASTER OF SCIENCE
DEPARTMENT OF COMPUTER ENGINEERING

THESIS SUPERVISOR
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2018

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 03/01/2018 tarih ve 2018/02 sayılı kararıyla oluşturulan jüri tarafından 22/01/2018 tarihinde tez savunma sınavı yapılan ALİCAN BEYDEMİR'in tez çalışması BİLGİSAYAR MÜHENDİSLİĞİ Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE

(TEZ DANIŞMANI) :PROF. DR. İBRAHİM SOĞUKPINAR



ÜYE

:DOÇ. DR. MEHMET GÖKTÜRK



ÜYE

:DOÇ. DR. ALİ GÖKHAN YAVUZ



ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun

...../...../..... tarih ve/..... sayılı kararı.

ÖZET

Bu çalışma kapsamında günümüzde önemli bir yeri olan Nesnelerin İnterneti kapsamına dâhil cihazlarda kullanılabilecek Sıfır Bilgi İspatı tabanlı kimlik doğrulama yöntemleri önerilmektedir. Sıfır Bilgi İspatı kavramı özünde üç farklı kimlik doğrulama yöntemi içinde “bilinen bir bilgi ile doğrulama” yönteminin alt başlığı olarak, sahip olunan bir bilgiyi kimliği doğrulayacak olan tarafa ifşa etmeden doğrulama yapmayı mümkün kılan yeni ve farklı bir yöntemdir. Bu tez çalışmasında, literatürde Sosyalist Milyonerler Protokolü olarak bilinen özgün bir biçimde performansı arttırılmış kimlik doğrulama şemasından faydalanan özgün bir Sıfır Bilgi İspatı tabanlı bir yöntemi önerilmektedir, önerilen yöntem daha önce önerilen yöntemler ile karşılaştırılmış, sınanmış ve sonuçlar bu çalışmada verilmiştir.

Anahtar Kelimeler: Sıfır Bilgi İspatı, Kimlik Doğrulama, Kriptografi, Nesnelerin İnterneti.

SUMMARY

In this work, zero knowledge proof based authentication methods which suitable for new emerging topic of Internet of Things is are proposed. The concept of zero knowledge proof based authentication is fundamentally the sub method of the “Something you know” which is one of the three different authentication methods it is a new and different method that uses a “knowledge” for authentication but does not disclose information about knowledge. In this thesis work, we propose an original Zero Knowledge Proof based method which utilizes our performance enhanced authentication scheme known as the Socialist Millionaires Protocol in the literature. The proposed method is compared with the previously proposed methods, and the results are given in this study.

Key Words: Zero Knowledge Proof, Authentication, Cryptography, Internet of Things.

TEŞEKKÜR

Başta, yüksek lisans eğitimimde ve akademik hayatımda desteğini ve yardımlarını hiçbir zaman esirgemeyip bilgisi ile bu çalışmanın oluşmasının yolunu açan danışmanım Prof. Dr. İbrahim SOĞUKPINAR'a, bütün çalışmam boyunca yanımda olan, bilgi ve tecrübelerini benimle paylaşan değerli arkadaşım UĞUR KOCAGER'e ve göstermiş olduğu desteklerinden dolayı aileme en içten teşekkürlerimi sunarım.

İÇİNDEKİLER

	<u>Sayfa</u>
ÖZET	v
SUMMARY	vi
TEŞEKKÜR	vii
İÇİNDEKİLER	viii
SİMGELER ve KISALTMALAR DİZİNİ	ix
ŞEKİLLER DİZİNİ	x
TABLolar DİZİNİ	xi
1. GİRİŞ	1
1.1. Tezin Amacı, Katkısı ve İçeriği	5
2. SIFIR BİLGİ İSPATI YÖNTEMİ ART ALANI	6
2.1. Temel Tanımlar	7
2.1.1. Kriptografi	8
2.1.2. Kriptanaliz	8
2.1.3. Şifreleme ve Deşifreleme	9
2.2. Asimetrik Şifreleme Yöntemleri ve Kimlik Doğrulama	10
2.3. Eliptik Eğri Kriptografisi	13
2.3.1. Eliptik Eğriler Üzerinde Ayrık Logaritma Problemi	15
2.4. Sıfır Bilgi İspatı Yöntemi	17
2.5. Önceden Önerilen Yöntemler ve Analizleri	20
2.5.1. Tek Yönlü Schnorr Bilgi İspatı Şemasının Analizi	25
2.5.2. Çift Yönlü SRP Şemasının Analizi	28
3. SIFIR BİLGİ İSPATI YÖNTEMİ	31
3.1. Sosyalist Milyonerler Protokolü ve Özgün Curve25519 Uygulaması	31
3.2. Kayıt Olma	32
3.3. Kimlik Doğrulama	33
3.4. Protokolün İyileştirilmesi	34
3.4.1. Protokolün İyileştirilmesinin Özgün Katkıları	35
4. UYGULAMA VE DEĞERLENDİRME	39
4.1. Raspberry Pi 3 Cihazı ile DC Motor Kontrol Düzenegi	39

4.2. Teorik Güvenlik Analizi	41
4.3. Uygulama Güvenlik Analizi	42
4.4. Performans Karşılaştırmaları	44
5. SONUÇ VE ÖNERİLER	45
 KAYNAKLAR	 46
ÖZGEÇMİŞ	49
EKLER	50

SİMGELER ve KISALTMALAR DİZİNİ

<u>Simgeler ve</u>	<u>Acıklamalar</u>
<u>Kisaltmalar</u>	
GHz	: Gigahertz
ms	: Milisaniye
ECC	: Eliptik Eğri Kriptografisi
SBI	: Sıfır Bilgi İspatı

ŞEKİLLER DİZİNİ

<u>Sekil No:</u>	<u>Sayfa</u>
1.1: MQTT Protokolünde Kimlik Doğrulama.	2
1.2: COAP Protokolünde Kimlik Doğrulama ve Erişim.	3
2.1: RSA Açık Anahtar Şifreleme-Deşifreleme Yapısı.	10
2.2: RSA Algoritması ile Kimlik Doğrulama Örneği.	12
2.3: Diffie Hellman ve ElGamal ile Kimlik Doğrulama.	13
2.4: Eliptik Eğrilerde Döngüsel Alt Grup Oluşumu.	16
2.5: Mağara Örneği Başlangıç Durumu.	19
2.6: Mağara Örneği Satıcının Kapıdan Geçmesi.	19
2.7: Mağara Örneği Satıcının Kimliğini Doğrulaması.	19
2.8: Ayrık Logaritma Problemi.	21
2.9: Graf İzomorfikliği Problemi.	23
2.10: Schnorr Kayıt İşlemi.	26
2.11: Schnorr Kimlik Doğrulama İşlemi.	26
2.12: Schnorr Kayıt İşlemi Zafiyeti.	27
2.13: Schnorr İmzasına Karşı Saldırı.	27
2.14: SRP-6 Şeması.	28
3.1: Standart Sosyalist Milyonerler Protokolü.	32
3.2: Önerilen Şemanın Kayıt İşlemi.	33
3.3: Önerilen Şemanın Kimlik Doğrulama İşlemi.	34
3.4: Montgomery Eğrilerinin Genel Formu.	36
3.5: Montgomery Üs Alma Merdiveni Algoritması.	37
4.1: Uygulamanın Şeması.	40
4.2: Uygulamanın Görseli.	41

TABLÖLAR DİZİNİ

<u>Tablo No:</u>	<u>Sayfa</u>
1.1: Güvenlik Açıklıkları ve Alt Kısımları.	4
2.1: Alanlar Arası İşlem İzdüşümleri.	30
3.1: Skaler Nokta Çarpım Performansları.	38
4.1: Performans Karşılaştırmaları.	44

1. GİRİŞ

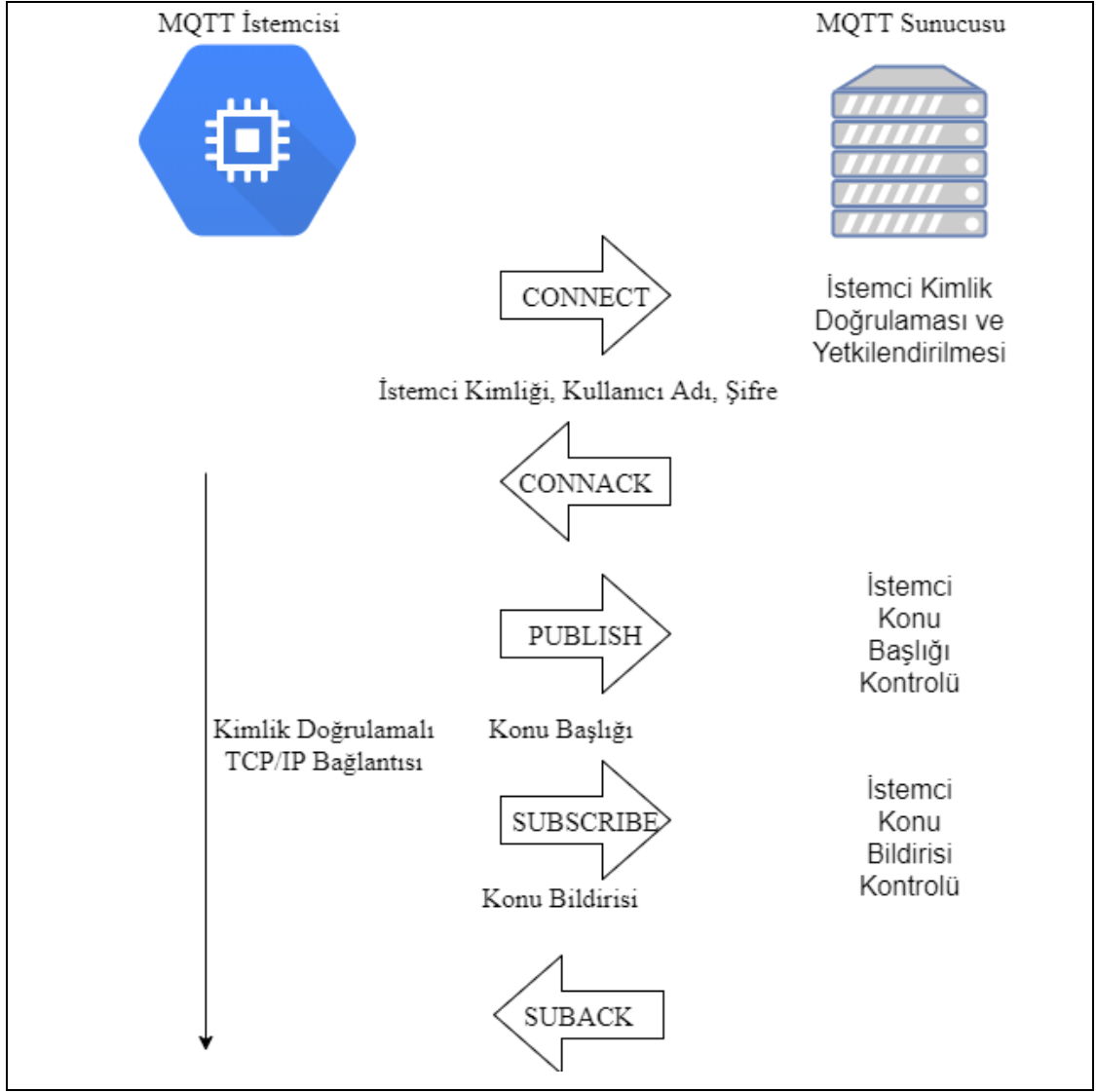
Günümüzde Nesnelerin İnterneti uygulamaları önemli bir konu başlığı durumundadır. 2020 yılı itibari ile internete bağlanabilecek cihaz ya da nesne sayısı 50 milyar civarı olması beklenmektedir [Davis, 2017].

Nesnelerin İnterneti uygulamalarında cihazların kısıtlı kaynaklara sahip olmasından dolayı bu cihazların güvenlik ihtiyaçlarını karşılamak zor bir problem olarak düşünülmektedir [Roman, vd., 2013].

OWASP topluluğunun 2014 yılında yayınladığı bir dokümana göre Nesnelerin İnterneti için ortaya çıkan güvenlik açıklıkları ana başlıkları ile şunlardır, Güvensiz Ara yüz, Yetersiz Kimlik Doğrulama ve Yetkilendirme, Güvensiz Ağ Hizmetleri, Aktarım Şifrelemesinin Eksikliği, Gizlilik İfşası ve Güvensiz Bulut Ara yüzü olarak sıralanabilir bu sayılan açıklıkların birçoğunun var olma sebebi verimli ve çift taraflı çalışan bir kimlik doğrulama şemasının eksikliğidir [Web 1, 2014].

Nesnelerin İnternetinde iletişim genel olarak iki popüler protokol olan MQTT ve COAP protokolleri ile sağlanmaktadır, MQTT (MQ Telemetry Aktarımı veya Mesaj Kuyruğu Telemetry Aktarımı) ISO standardı (ISO / IEC PRF 20922) olan bir yayımlama-abone tabanlı mesajlaşma protokolüdür. TCP / IP protokolünün üstünde çalışır. "Küçük kod alanı" gerektiren veya şebeke bant genişliğinin sınırlı olduğu uzak konumlardaki bağlantılar için tasarlanmıştır. Yayınla-bastırma mesajlaşma kalıbı ile çalışır, ve bu iş için bir mesaj dağıtıcı gerektirir.1999'da Cirrus Link'in Andy Stanford-Clark ve Arlen Nipper protokolünün ilk versiyonunu yazmıştır MQTT protokolü günümüzde Nesnelerin İnterneti Uygulamalarında sıkça kullanılan bir protokol haline gelmiştir fakat kullandığı kimlik doğrulama mekanizmasının zafiyetlerinden ötürü güvenlik açıklıkları vardır [Banks et al., 2014].

MQTT'ye Alternatif protokoller IETF Sınırlandırılmış Uygulama Protokolü, XMPP, OPC UA ve Web Uygulama Mesajlaşma Protokolü (WAMP) ayrıca Gelişmiş Mesaj Kuyruk Protokolü (AMQP) ve Akış Metin Odaklı Mesajlaşma Protokolü (STOMP) gibi protokollerdir.



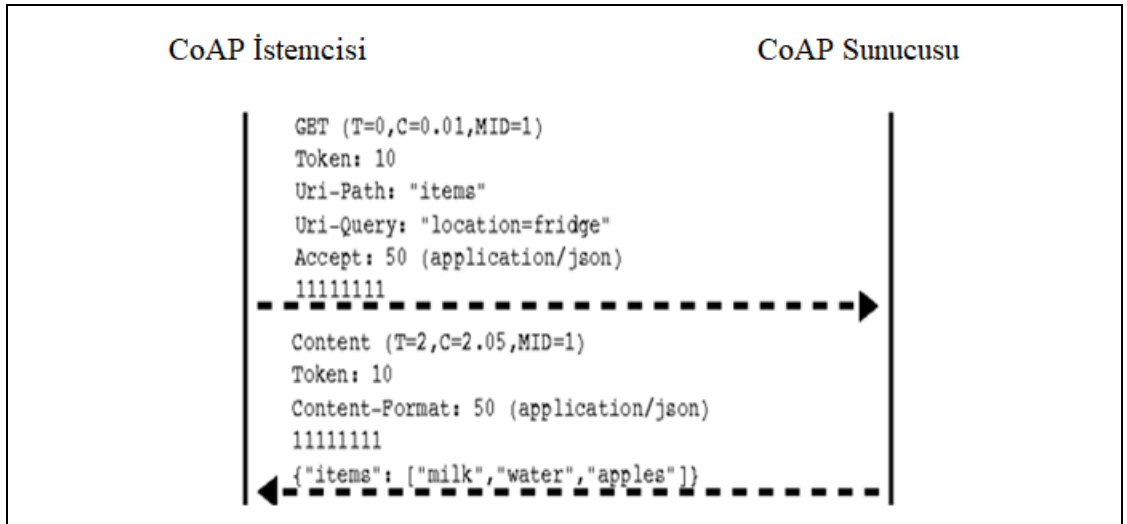
Şekil 1.1: MQTT Protokolünde Kimlik Doğrulama.

Sınırlandırılmış Uygulama Protokolü (CoAP) ise, RFC 7228'de tanımlandığı gibi, kısıtlı cihazlar için özel bir İnternet Uygulama Protokolüdür. "Kurallara aykırı olan" düğümler adlı cihazların benzer protokolleri kullanarak daha geniş İnternet ile iletişim kurmasını sağlar. CoAP, aynı kısıtlı ağ üzerindeki aygıtlar (örneğin, düşük güç tüketen, kayıplı ağlar), aygıtlar ve genel düğümler arasında ve farklı kısıtlı ağlardaki aygıtlar arasında, hem de bir İnternet tarafından katılanlar arasında kullanılmak üzere tasarlanmıştır. CoAP, mobil iletişim şebekelerinde SMS gibi diğer mekanizmalar yoluyla da kullanılmaktadır.

CoAP, kablosuz algılayıcı ağ düğümleri gibi kaynak kısıtlı İnternet aygıtlarında kullanılmak üzere tasarlanmış bir hizmet katmanı protokolüdür. CoAP, çok noktaya yayın desteği, çok düşük maliyet ve basitlik gibi özel gereksinimleri karşılarken,

Web ile basitleştirilmiş bütünleştirme için HTTP'ye kolayca çevrilecek şekilde tasarlanmıştır. Çok noktaya yayın, düşük yük ve basitlik, İnternet'in Oldukça gömülü olma eğiliminde olan ve geleneksel internet aygıtlarına göre daha az bellek ve güç kaynağına sahip Şeyler (IoT) ve Makine-Makine (M2M) aygıtları için son derece önemlidir. Bu nedenle verimlilik çok önemlidir. CoAP, UDP'yi veya UDP analogunu destekleyen çoğu cihazda çalışabilir tıpkı MQTT gibi CoAP protokolünde ağ katmanından gelen bir takım kalıtsal güvenlik açıklıklarından dolayı saldırılara açıktır [Shelby et al., 2014].

Internet Engineering Task Force (IETF) Sınırlı RESTful Ortamlar Çalışma Grubu (CoRE), bu protokol için önemli standartlaştırma çalışması yapmıştır. Protokolü IoT ve M2M uygulamalarına uygun hale getirmek için çeşitli yeni işlevler eklenmiştir. Protokolün çekirdeği RFC 7252'de belirtilmiştir; önemli uzantılar standartlaştırma sürecinin çeşitli aşamalarındadır.



Şekil 1.2: COAP Protokolünde Kimlik Doğrulama ve Erişim.

MQTT ve CoAP benzeri protokollerin tanımladığı ve Nesnelerin İnterneti gibi devasa bir cihazlar arası iletişimin olduğu yeni nesil bu teknolojiler bir takım güvenlik açıklıkları barındırmaktadır.

OWASP’ın yaptığı araştırmalara göre Kimlik Doğrulama ile ilintili olan güvenlik açıklıkları şunlardır [Web 1, 2014]:

Tablo 1.1: Güvenlik Açıklıkları ve Alt Kısımları.

Güvensiz Arayüz	Oturum Hırsızlığı ve Cihaz Enumerasyonu
Yetersiz Kimlik Doğrulama ve Yetkilendirme	İmtiyaz Artımı ve İzinsiz Erişim
Güvensiz Ağ Hizmetleri	Servis veren Portları ifşası
Aktarım Şifrelemesinin Eksikliği	Tekrarlama Saldırıları
Gizlilik İfşası	Cihazın gizli bilgileri ifşa etmesi
Güvensiz Bulut Arayüzü	Ağ Trafikğinde Kimlik bilgilerinin açığa çıkması
Zayıf Fiziksel Güvenlik	Yan Kanal Saldırıları

Tablo 1.1 kapsamında Temel Güvenlik açıklıkları ve sebep olabilecekleri alt kısımları olan saldırı güvenlik açıkları verilmiştir.

- Güvensiz Arayüz

Güvenli olmayan bir arayüz üzerinden ulaşılan bir sunucu Oturum hırsızlığı gibi açıklıkları kullanarak sistem yöneticisi rolü oynayarak sisteme zarar verebilir veya cihaz enumerasyonu yaparak cihaz sayısı, kimlik numaraları IP ve fiziksel adreslerini ele geçirip başka saldırılar için bilgi toplayabilir.

- Yetersiz Kimlik Doğrulama

Kimlik Doğrulamanın eksik veya verimsiz olduğu bir durumda daha az yetkili kişiler yetkili kişi rolü yapabilir ve izinsiz kaynak erişimi ile sistem hakkında bilgi sahibi olabilir.

- Güvensiz Ağ Hizmetleri

Kimlik Doğrulamasının olmadığı ağ hizmetleri kullanan bir sistem herhangi bir servisin hangi port üzerinden verildiği bilgisini dışardaki saldırganlara ifşa edebilir.

- **Gizlilik İfşası**

Cihazlar arası haberleşme esnasında veya öncesinde cihaz, ağ dinleyen saldırganlara karşı gizli bilgileri ifşa edebilir.

- **Güvensiz Bulut Ara yüzü**

Cihazların kendi ağ sistemlerinden dışarıya çıkması durumunda kimlik doğrulamanın eksikliği nedeni ile gelen veya giden trafiğe yanlış yönlendirme yapılarak gizli bilgiler elde edilebilir.

- **Zayıf Fiziksel Güvenlik**

Cihazların bulunduğu konumlarda, cihazlar haberleşirken üzerlerinde gizli bilgilerin elektronik olarak ifşa edilmesini engelleyen yazılımsal veya donanımsal koruma önlemlerinin olmadığı durumlarda gizli bilgiler ifşa olabilir.

Sayılan güvenlik açıklıklarının daha birçok alt kırılımı olan tehditler mevcuttur, güvenli ve verimli bir kimlik doğrulama şemasının neredeyse tüm güvenlik açıklıkları için çözüm sağlayabilecek bir yapıdadır.

1.1. Tezin Amacı, Katkısı ve İçeriği

Nesnelerin İnterneti uygulamalarında kimlik doğrulama mekanizması belirli birtakım protokollerin meydan okuma & cevap yöntemi ile sağlanmaktadır. Bu protokollerde bulunan mekanizmaların mevcut halleri zayıf kriptografi ve özet(hash) algoritmaları kullandığından bir takım güvenlik zafiyetleri içerirler [Banks et al., 2014], [Shelby et al., 2014].

Mevcut durumu ile Kimlik Doğrulama problemine çözüm olarak kullanılan SSL/TLS şifrelemesi gibi açık anahtarlı şifreleme yöntemleri kullanılmadan sistem çok kolay bir şekilde kötü niyetli kişiler tarafından sömürülmeye müsaittir. Bununla birlikte destekleyici çözüm olarak sunulan SSL/TLS şifrelemesi, onaylanmış sertifika ve güçlü donanım kaynakları gibi fazladan maddi ve hesapsal maliyetlere sebep olabilmektedir. Ayrıca SSL/TLS kuramsal kriptanaliz yöntemlerine karşı güçlü olsa da birtakım uygulama saldırılarına karşı zayıf kaldığı bilinmektedir [Aviram et al., 2016], [Marlinspike, 2009].

Bu kořullarda güvenli ve verimli bir kimlik doęrulama mekanizmasının eksiklięi gze arpmaktadır. Bu alıřma kapsamında Nesnelerin İnterneti konseptinde bulunan kısıtlı kaynaklara sahip cihazlar iin gvenlik ihtiyalarını saęlayabilecek sıfır bilgi ispatı tabanlı yeni bir kimlik doęrulama řeması yntem olarak nerilmiřtir. nerilen řema sosyalist milyonerler problemi ile ElGamal řifrelemesinin eliptik eęri 25519 zerinde performans ve verimlilik gibi zelliklerin gz nne alınarak yeniden tanımlanması ile zgn bir biimde oluřturulmuřtur yntem uygulanarak gvenlik analizi yapılmıř, nceki yntemlerle karřılařtırılmıř ve sonular bu alıřmada verilmiřtir.

2. SIFIR BİLGİ İSPATI YÖNTEMİ

Bu bölümde Sıfır Bilgi İspatı(SBI) yöntemi ile kimlik doğrulama şeması oluşturmak için gerekli olan kriptoloji ve kriptolojinin alt dalı olan kriptografi bilimi ile ilgili teorik bilgiler verilecektir.

2.1. Temel Tanımlar

Kimlik doğrulama, bir varlık tarafından iddia edilen tek bir veri parçasının bir niteliğinin gerçeğini teyit etme eylemidir. Kimlik doğrulaması, bir kişinin veya bir şeyin kimliğini kasten iddia eden bir iddianın belirtilmesi veya belirtilmesi eylemine atıfta bulunan işlemin aksine, kimlik doğrulama, o kimliğin doğrulanması sürecidir.

Kimlik doğrulama günlük hayatta birçok uygulaması ve faydası olan bir işlemdir, örneğin bir şahıs için kimlik belgelerini doğrulayarak, bir web sitesinin dijital sertifika ile doğruluğunu teyit ederek, karbon tarihlendirmesiyle bir eserin yaşını belirleyerek veya bir ürünün ambalajı ve etiketinin ne olduğunun doğrulanarak kimlik doğrulama gerçekleştirilebilir.

Kimlik doğrulamasına yönelik tüm yaklaşımlar aşağıdakilerden en az birine dayanmaktadır:

- Bilinen bir şey

Bilinen bir şey aracılığı ile kimlik doğrulama yapma en bilinen, pratikte uygulama için kullanılan en yaygın doğrulama çeşididir. Örneğin dijital sistemler için şifreler kullanarak kimlik doğrulama yapma ve bu tez çalışmasının temelini oluşturan Sıfır Bilgi İspatları bu başlık altındadır. Ne yazık ki, bildiğiniz bir şey unuttuğunuz bir şey olabilir. Eğer açık edecek tehditler mevcutsa, diğer kötü niyetli saldırganlar bunu kullanabilir.

- Sahip olduğunuz bir şey

Örneğin bir akıllı kart bu kimlik doğrulama formu bildiğiniz bir şeyi unutma sorununu ortadan kaldırır, ancak kimliği doğrulanmak istediğinizde artık bazı nesneler sizinle birlikte olmalı ve böyle bir nesne çalınabilir ve daha sonra saldırganın bir parçası haline gelebilir.

- Olduđunuz bir Őey

Örneđin Parmak izi kimliđi dođrulanana ana kiŐiye özeldir. Bir cüzdandan çok parmak izi kaybetmek daha zordur. Ne yazık ki, biyometrik duyargalar oldukça pahalıdır ve (Őu andaki) çok dođru deđildir.

Günümüzün dijital dünyasında ise kimlik dođrulama problemi genellikle Kriptoloji konu baŐlıđı altında incelenmektedir. Kriptoloji temelinde kriptografi ve kriptanaliz olarak adlandırılan iki alıŐma alanının birleŐmesi ile oluŐmuŐ, güvenli haberleŐme uygulamalarının tasarlanması ve analizi üzerinde yoğunlaŐan bir matematiksel yöntemler bütünüdür. Bu yöntemler, bir bilginin iletimi esnasında karŐılaŐılabilecek aktif ya da pasif ataklardan bilgiyi dolayısıyla bilgi ile beraber bilginin göndericisi ve alıcısını da koruma veya ele geçirme amacı güderler.

2.1.1. Kriptografi

Kriptografi Őifreleme bilimidir. eŐitli iletilerin, yazıların belli bir sisteme göre Őifrenmesi, bu mesajların güvenli bir ortamda alıcıya iletilmesi ve iletilmiŐ mesajın deŐifre edilmesidir. Kriptografide Őifreleme ve deŐifreleme, özet fonksiyonları hari anahtar denilen bir parametre aracılıđı ile yapılır ancak gizli anahtara sahip kiŐiler Őifreleme ve deŐifreleme iŐlemini dođru bir Őekilde yapabilir.

Günümüz teknolojisinin baŐ döndürücü hızı göz önüne alındığında, teknolojinin geliŐmesiyle birlikte ortaya ıkan güvenlik açığına da taŐıdıđı önem ile kriptografi bilimi popüler bir konu olmuŐtur.

2.1.2. Kriptanaliz

Kriptografik sistemlerin gizli yönlerini incelemek için bilgi sistemlerini analiz etme alıŐmasıdır. Kriptografi, Őifreleme anahtarı bilinmese bile, Őifreleme güvenlik sistemlerini ihlal etmek ve ŐifrenmiŐ mesajların içeriđine eriŐmek için kullanılır.

Kriptografi algoritmalarının matematiksel analizine ek olarak, kriptografi, Őifreleme algoritmalarındaki zayıflıkları hedeflemeyen yan kanal saldırılarını da içermektedir; bunun yerine uygulamadaki zayıf noktaları kullanmaktadır.

2.1.3. Şifreleme ve Deşifreleme

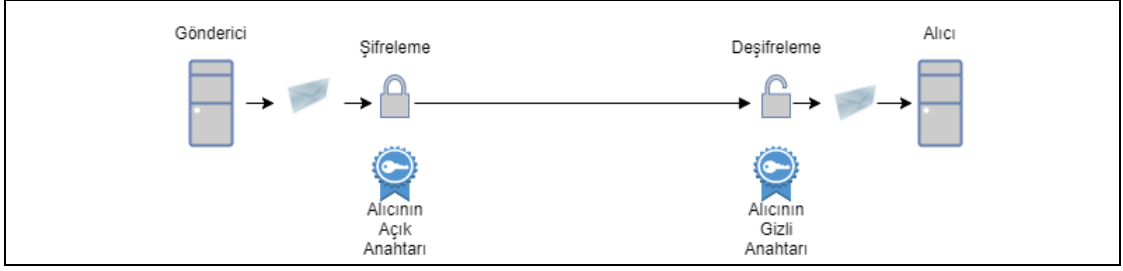
Şifreleme ve Deşifreleme işlevleri kriptografi alanının temel iki işlevidir, esasen birbirlerinin ters fonksiyonları gibi düşünülebilir, özet fonksiyonları haricinde şifreleme ve deşifreleme işlemleri anahtar denilen özel bir matematiksel değer ile birlikte yapılmaktadır, sadece anahtara sahip kişiler gizli kalmasını istedikleri verileri şifreleyebilir ve sadece anahtara sahip kişiler bu şifrelenmiş verileri açık metin haline dönüştürüp okuyabilir. Örnek olarak şifreleme ve deşifreleme matematiksel bir fonksiyon formunda gösterilebilir.

$$e(x) = (a * x + b) \bmod m \quad (2.1)$$

$$d(x) = (a^{-1} * (x - b)) \bmod m \quad (2.2)$$

Şifreleme işlemi üç farklı yöntemle yapılmaktadır bunlar, Simetrik Anahtarlı Şifreleme veya Kapalı Anahtar Şifreleme, Asimetrik Anahtarlı Şifreleme veya Açık Anahtar Şifreleme ve Anahtarsız Özet Fonksiyonları ile şifrelemedir.

Açık anahtarlı şifreleme veya Asimetrik şifreleme olarak adlandırılan yöntem tarafların aynı şifreleme anahtarına sahip olmadığı zaman kullanılan yöntemlerdir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık (gizli olmayan) anahtardır. Bu anahtarlardan bir tanesiyle şifreleme yapılırken diğeriyle de şifre çözme işlemi gerçekleştirilir. Bu iki anahtar çifti matematiksel olarak birbirleriyle bağlantılıdır fakat bu bağlantıyı kurmak saldırganlar için teorik mümkün olsa da pratikte zordur. Açık anahtarlı şifreleme yöntemleri kimlik doğrulama için verimli bir altyapı teşkil etmektedir. En bilinen Açık anahtarlı Şifreleme Yöntemleri Diffie-Hellman, RSA, ElGamal ve DSA gibi popüler yöntemlerdir.



Şekil 2.1: RSA Açık Anahtar Şifreleme-Deşifreleme Yapısı.

2.2. Asimetrik Şifreleme Yöntemleri ve Kimlik Doğrulama

Asimetrik Şifreleme yöntemleri kimlik doğrulama işlevi için temel teşkil etmektedir. Açık anahtar şifrelemesi, iletişim dinleme, değiştirme ve kimliğe bürünme saldırılarından korunmak için iyi bilinen teknikler ve standartlar dizisidir. Asimetrik şifrelemenin Kimlik Doğrulama, Veri Bütünlüğü ve inkâr edilemezlik gibi özellikleri genel anlamda kimlik doğrulama şemalarının tasarlanmasında faydalı olmaktadır.

Asimetrik şifreleme ve deşifreleme, iki iletişim kuran tarafın birbirlerine gönderdikleri bilgileri gizlemesine olanak tanır. Gönderen, göndermeden önce bilgileri şifreler. Alıcı, bilgiyi aldıktan sonra şifresini çözer Böylece, şifreli bilgi bir davetsiz misafir tarafından anlaşılmaz hale gelir.

Kimlik doğrulama, bilgi alanın kaynağını belirlemesine, yani gönderenin kimliğini doğrulamasına izin verir, çoğu kriptografik kimlik doğrulama protokolü meydan okuma - cevap denilen bir haberleşme ile kimlik doğrulama sağlar burada meydan okuma karşı tarafın kimliğini doğrulamak isteyen kişi tarafından sorulan bir soru gibi düşünülebilir, cevap ise bu sorulan soruya verilen soruyu soran kişiyi cevap verenin kimliğinden emin kılacak şekilde bir yapıda olan cevaptır.

Veri bütünlüğü, alıcının bilgilerinin aktarım sırasında değiştirilmediğini doğrulamasını sağlar. Bu sayede verileri değiştirmek veya sahte bir iletiyi meşru olanın yerine geçmek için yapılan herhangi bir girişim tespit edilecektir.

İnkâr edilemezlik, gönderen kişinin daha sonraki bir tarihte hiçbir zaman gönderilmediğini iddia etmesini önler.

Sertifikalar Kimlik Doğrulama için Asimetrik şifreleme alt yapısını kullanan çok yaygın bir çözümdür sertifika, bir şahsın, bir sunucunun, şirketin veya başka bir tüzel kişinin tanımlanması ve bu kimliği ortak bir anahtarla ilişkilendirmek için

kullanılan elektronik bir belgedir. Sürücü belgesi, pasaport veya yaygın olarak kullanılan diğer kimlik belgeleri gibi bir sertifika, bir kişinin kimliğinin kanıtı olarak kabul edilir.

Açık anahtar şifrelemesi, kimliğe bürünme sorununu gidermek için sertifikalar kullanır. Sürücü belgesi almak için, lisans vermeden önce kimliğinizi, sürüş yeteneğinizi, adresinizi ve diğer bilgileri doğrulayan Motorlu Araçlar Bölümü gibi bir devlet kurumuna başvurabilirsiniz. Kütüphane kartı edinmek için adınızı ve hizmet faturanızı adresinizle birlikte vermeniz gerekebilir.

Sertifikalar, tanıdık Kimlik Doğrulama modellerinden herhangi biriyle aynı şekilde çalışır. Sertifika yetkilileri, kimlikleri doğrulayan ve sertifika veren varlıklardır. Bağımsız üçüncü şahıslar veya kendi sertifika veren sunucu yazılımını çalıştıran kuruluşlar olabilir örneğin Red Hat Sertifika Sistemi gibi.

Bir kimliği doğrulamak için kullanılan yöntemler, diğer kimlik doğrulama formlarını doğrulamak için kullanılan yöntemlerin kimin kim tarafından verildiğine ve hangi amaçla kullanılacağına bağlı olarak değiştiği gibi, belirli bir Sertifika Yetkilisinin politikalarına bağlı olarak değişir. Genel olarak, sertifika vermeden önce, yetkili sertifika talep eden bir tüzel kişinin aslında kim olduğunu iddia ettiğinden emin olmak için bu tür sertifika için yayınlanmış doğrulama prosedürlerini kullanmalıdır.

Yetkili tarafından verilen sertifika, belirli bir genel anahtarı, sertifika tanımlayan varlığın adına örneğin bir çalışan veya bir sunucu adına bağlar. Sertifikalar, taklit için sahte ortak anahtarların kullanılmasını önlemeye yardımcı olur. Sertifika tarafından onaylanan yalnızca açık anahtar, sertifika tarafından tanımlanan varlık tarafından sahip olunan karşılık gelen özel anahtarla çalışır.

RSA algoritması en bilinen açık anahtar algoritmalarından biridir. RSA, güvenliği tam sayıları çarpanlarına ayırmanın algoritmik zorluğuna dayanan bir tür Açık anahtarlı şifreleme yöntemidir. 1978’de Ron Rivest, Adi Shamir ve Leonard Adleman tarafından bulunmuştur. Bir RSA kullanıcısı iki büyük asal sayının çarpımını üretir ve seçtiği diğer bir değerle birlikte ortak anahtar olarak ilan eder. RSA şifrelemesi kullanılarak bir kimlik doğrulama protokolü tasarlanabilir günümüzde sertifika tabanlı kimlik doğrulama yöntemlerin bazıları arka tarafta RSA şifrelemesi kullanarak kimlik doğrulama yapmaktadır.

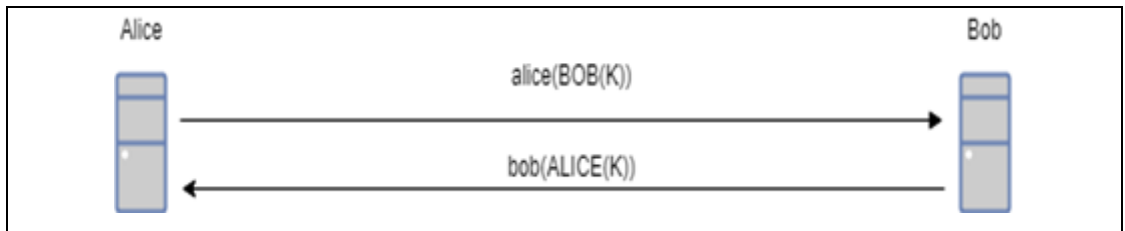
RSA için bir açık anahtar bir de özel anahtar gerekir. Açık anahtar herkes tarafından bilinir ve mesajı şifrelemek için kullanılır. RSA şifrelemesinde asimetrik

bir yapı vardır, açık anahtar ile şifrelenen bir veri ancak kapalı anahtarla, kapalı anahtarla şifrelenen veri ise açık ile çözülebilir. Bir ortak anahtarla şifrelenmiş mesaj sadece özel anahtarla çözülebilir. RSA anahtarları şu şekilde oluşturulur, İki adet birbirinden değişik asal sayı seçilir, bunlar p ve q olsun. Güvenlik amacıyla p ve q sayıları rastgele seçilmeli ve yakın uzunlukta olmalıdırlar. Bu sayılar asalılık testi kullanılarak etkin bir şekilde bulunabilir.

φ Değeri özel ve ortak $\varphi = (p - 1) * (q - 1)$ anahtarlar için mod değeri olarak kullanılacaktır. Bu sayıların totient olan φ değeri hesaplanır. Bir tam sayı üretilir ve adı e koyulur. Bu sayı, $1 < e < \varphi(n)$ koşuluna uygun olmalı ve $\varphi(n)$ ile en büyük ortak böleni 1 olmalıdır ve aralarında asal olmalıdır. e ortak anahtar olarak açıklanır. $e * d \equiv 1 \text{ mod } \varphi(n)$ Olacak şekilde bir d belirleyin. d özel anahtar üssü olarak saklanır. Alice ortak anahtarı (n, e) 'yi Bob'a gönderir, özel anahtarını gizli tutar.

Bob m mesajını Alice'e göndermek istediği zaman şifrelenmiş mesaj c 'yi $c = m^e \text{ mod } n$ olacak şekilde hesaplar. Alice mesajını özel anahtarı olan d 'yi kullanarak şifreli mesaj c 'den şu şekilde hesaplar $m = c^d \text{ mod } n$

Kimlik doğrulama şeması olarak kullanılması ise şöyledir, K değeri doğrulama için yeterli kimlik belirteci, gönderen tarafın isminin küçük harfler ile yazılmış hali gizli anahtar ile şifreleme büyük harflerle yazılmış hali ise açık anahtarla şifreleme fonksiyonu olarak kabul edilsin.



Şekil 2.2: RSA Algoritması ile Kimlik Doğrulama Örneği.

Alice önce kendine ait K değerini Bob'un açık anahtarı sonrada kendi gizli anahtarı ile şifreler ve Bob'a yollar.

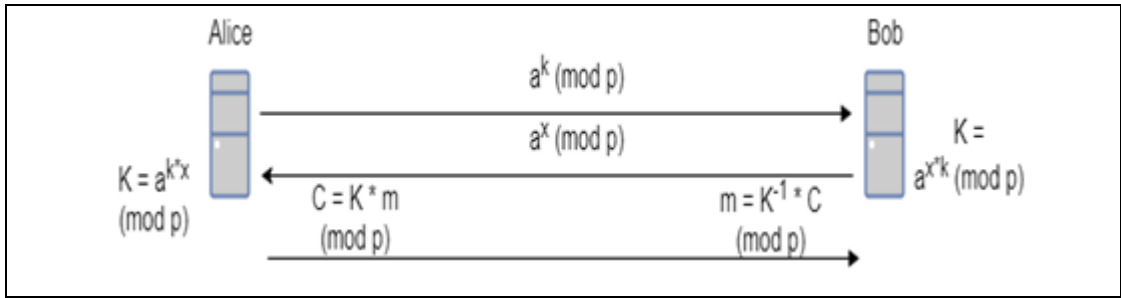
Bob Alice'in açık anahtarını bildiği için ilk şifrelemeyi çözer ardından kendi gizli anahtarı ile K değerini elde eder.

Bob daha sonradan kendi K değerini Alice'in açık anahtarı ile şifreler daha sonra kendi gizli anahtarı ile şifreleyerek Alice'e yollar Alice bu değeri bir önceki adımda Bob'un yaptığı gibi çözerek Bob'un K doğrulama değerini elde eder.

Diffie Hellman ve ElGamal RSA algoritmasından farklı olarak Ayırık Logaritma Probleminin zorluğuna dayanan yöntemlerdir.

Diffie Hellman algoritması iki tarafında kendilerine ait bir gizli anahtarı kullanarak önce, açık anahtarlarını oluşturması daha sonra açık anahtarları takas edip kendi gizli değerleri ile tekrar şifrelemesi ile ortak sır yaratmasını esas alır.

Her iki tarafta ortak bir sır oluştuktan sonra ElGamal algoritması devreye girer, ElGamal şifrelemesi bu sır değerini bir anahtar olarak kullanarak simetrik bir şifreleme gerçekleştirir ve kimlik belirteç değerlerinin güvenli iletimini sağlar.



Şekil 2.3: Diffie Hellman ve ElGamal ile Kimlik Doğrulama.

2.3. Eliptik Eğri Kriptografisi

Eliptik eğri kriptografisi (ECC), sonlu alanlar üzerindeki eliptik eğrilerin cebirsel yapısına dayanan açık anahtar şifrelemeli bir yaklaşımdır. Eşdeğer güvenlik sağlamak için Eliptik Eğri Kriptografisi, Eliptik Eğri Kriptografisi olmayan şifrelemeye (düz Galois alanlarına dayalı) kıyasla daha küçük anahtarlar gerektirir ve daha hızlı işlemler mümkündür bu yönüyle Nesnelerin İnterneti uygulamaları için uygundur.

Eliptik eğriler anahtar sözleşmesi, dijital imza, sözde rastgele üreticiler ve diğer görevler için geçerlidir. Dolayısıyla, anahtar sözleşmeyi simetrik şifreleme planıyla birleştirerek şifreleme için kullanılabilirler.

Matematiksel olarak eliptik eğri formu bir denklemler ile tanımlanan bir düzlem üzerinde tanımlı cebirsel bir eğridir.

Eliptik eğriler sayı teorisinde özellikle önemlidir ve şu anki araştırmaların önemli bir alanını oluşturmaktadır; Örneğin Andrew Wiles tarafından Fermat'ın Son Teoreminin kanıtında kullanılmışlardır. Eliptik eğrilerin, eliptik eğri kriptografisi (ECC) ve tamsayı çarpanlara ayırma uygulamaları da bulmaktadırlar.

Bir eliptik eğrisinin resmi tanımı oldukça teknik olmasına ve cebirsel geometride bazı geçmiş gerektirmesine rağmen, yalnızca tanıtıcı cebir ve geometri kullanılarak gerçekte sayılar üzerinde eliptik eğrilerin bazı özelliklerini tanımlamak mümkündür.

Bu bağlamda, eliptik bir eğri, formun bir denklemiyle tanımlanan bir düzlem eğrisidir.

$$y^2 = x^3 + a * x + b \quad (2.3)$$

Burada a ve b gerçekte sayılardır. Bu tür denklemlere Weierstrass normal form denklemi denir.

Eliptik eğrinin tanımı aynı zamanda eğrinin tekil olmamasını gerektirir. Geometrik olarak bu grafiğin baş, kesişme noktası veya izole noktaları olmadığı anlamına gelir. Cebirsel olarak, bu, ancak ve eğer delta sıfıra eşit olmamalıdır.

$$\Delta = -16(4 * a^3 + 27 * b^2) \quad (2.4)$$

Eğri, x eksenini etrafında simetrik olduğundan, herhangi bir P noktasına bakarsak, -P'nin onu zıt nokta olarak alabiliriz.

Eliptik Eğriler matematiksel olarak grup dediğimiz yapılar olarak kullanılabilir durumdadır.

Eliptik Eğriler üzerinde tanımlı x-y koordinat düzleminde olan noktalar vardır P ve Q eğri üzerinde iki nokta ise, o zaman üçüncü bir noktayı toplama işlemi için (P + Q) şu şekilde özdeşleştirebiliriz. İlk olarak, P ve Q'yu kesen bir doğru olmalıdır. Genellikle bu doğru üçüncü bir noktayı da keser R. Sonra P + Q'yu R'nin tersi olan -R noktasına götürürüz.

Ekleme için bu tanım, birkaç özel durum haricinde sonsuzluk ve kesişme çokluğundaki nokta ile ilişkili olarak çalışır. İlk nokta O'dan biri olduğunda O'dur. Burada P + O = P = O + P olarak tanımlanır ve O abelian grubun kimliğini verir. Daha sonra eğer P ve Q birbirinin tersi ise, P + Q = O tanımlarız. Son olarak, P = Q

ise sadece bir noktamız vardır, dolayısıyla aralarındaki çizgiyi tanımlayamayız. Bu durumda, bu noktadaki eğrinin teğet çizgisini çizgimiz olarak kullanırız. Çoğu durumda, teğet ikinci bir R noktasını keser ve tersini alabiliriz. Bununla birlikte, eğer P, bir bükülme noktası (eğrinin konkavitesinin değiştiği bir nokta) olursa, R veya P kendisi ve $P + P$ ise sadece kendisinin zıt noktasıdır.

Weierstrass normal formunda olmayan bir kübik eğri için dokuz eğim noktasından bir tanesini O olarak belirterek yine de bir grup yapısı tanımlayabiliriz. Yansıtılmalı düzlemde, her bir çizgi, çokluğu hesaplarken üç noktada bir kübikle kesişir. P noktasında, -P, O ve P'den geçen eşsiz üçüncü nokta olarak tanımlanır. Ardından, herhangi bir P ve Q için, $P + Q$, -R olarak tanımlanır; burada, R, P ve Q içeren satırdaki benzersiz üçüncü noktadır.

2.3.1. Eliptik Eğriler Üzerinde Ayrık Logaritma Problemi

Sonlu bir alan, her şeyden önce, sonlu sayıda elemana sahip bir kümedir. Sonlu alana bir örnek, modulo p tamsayılar kümesidir; burada p asal sayıdır. Genellikle $\mathbb{Z}/p\mathbb{Z}$ / p, $\text{GF}(p)$ $\text{GF}(p)$ veya $\mathbb{F}_p$ olarak gösterilir bu aslında formal olarak grup denilen matematiksel kavramla denktir.

Alanlarda iki ikili işlem var: toplama (+) ve çarpma ($\cdot$). Her ikisi de kapalı, birleştirici ve değişebilir özelliktedir. Her iki işlem için de benzersiz bir kimlik ögesi bulunur ve her öge için benzersiz bir ters öge bulunur, çarpma toplama üzerinde dağılma özelliğine sahiptir.

Örneğin: $x \cdot (y + z) = x \cdot y + x \cdot z$ işlemi gibi Modulo p tamsayı kümesi, 0'dan p-1'e kadar olan tüm tamsayılardan oluşur. Toplama ve çarpma, modüler aritmetikteki gibi çalışır ("saat aritmetiği" olarak da bilinir).

En kötü durumda, bit uzunluğunu göz önüne alırsak, O (logp) adet deneme ile eğrinin tüm noktaları gezilebilir.

Sonlu bir alan üzerinde tanımlanan bir eliptik eğrinin sonlu sayıda noktaya sahiptir.

O (p) basamaklarını gerektirdiği için noktaları saymanın uygun bir yolu değildir ve eğer p büyükse noktaları saymak zor bir problemidir.

Skaler çarpma ve döngüsel alt gruplar bu zor problemleri oluşturmada en önemli noktadır.

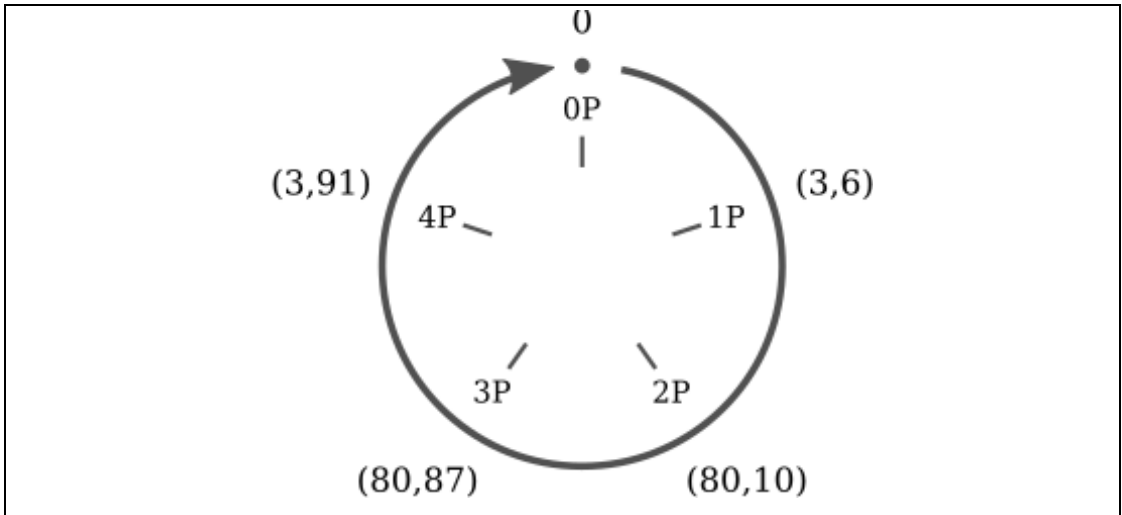
F_p , de eliptik eğriler için noktaların çarpımı ilginç bir özelliğe sahiptir. $p = 97$ olmak üzere aşağıdaki gibi bir eliptik eğri tanımlarsak.

$$y^2 = x^3 + 2 * x + 3 \mod 97 \quad (2.5)$$

N kadar P noktasının skaler nokta çarpımı eliptik eğriler üzerinde n kadar kendi ile toplama şeklinde gösterilebilir eliptik eğrinin sınırlandırıldığı p sayısının büyüklüğüne göre döngüsel alt gruplar oluşur.

$$n * P = P + P \dots + P \quad (2.6)$$

Örneğin $P = (3,6)$ noktası bu eğri üzerinde bir noktadır. Örnek olarak bu noktanın oluşturacağı dolaşımli grup şeklindeki gibidir aslında noktanın periyodu skaler çarpımlarının oluşturduğu bir eleman kümesidir.



Şekil 2.4: Eliptik Eğrilerde Döngüsel Alt Grup Oluşumu.

Bu matematiksel bilgiler bize şunu göstermektedir, eliptik eğrilerde ayrık logaritma problemi tanımlaması skaler çarpım işlemi ile mümkün olmaktadır kısaca P 'yi ve Q 'yu biliyorsak, k nedir sorusu eliptik eğriler üzerinde ayrık logaritma problemidir, matematiksel olarak $Q = kP$, $k=?$ Gibi gösterilebilir.

Eliptik eğriler için ayrık logaritma problemi olarak bilinen bu sorun, klasik bir bilgisayarda yürütülebilecek bilinen bir polinom zamanı algoritmasının bulunmaması nedeniyle "zor" bir problem olduğu düşünülmektedir. Bununla birlikte, bu teorem

iin matematiksel bir delil yoktur tıpkı RSA algoritmasının arpanlara ayırma problemi kadar zor olması gibi.

$P=97$ olarak yukarda belirttiğimiz rneęe dnecek olursak eliptik eęri iin k deęerlerinin hesaplanması olduka kolaydır nk eęrinin kendini tekrarlama ve alt grup oluřturma periyodu yani order (sıra) olarak literatrde geen deęer azdır.

Bu problem aynı zamanda Dijital İmza Algoritması (DSA), Diffie-Hellman anahtar deęiřimi (D-H) ve ElGamal algoritması gibi dięer řifreleme sistemleri ile kullanılan ayrıık logaritma sorununun benzeridir. Aynı adı tařıyan bir rastlantı deęildir. Aradaki fark, bu algoritmalar modulo s alma yerine skaler arpma kullanırlar.

ECC'ni ilgin kılan řey, bugn itibarıyla, eliptik eęriler iin ayrıık logaritma probleminin, kriptografide kullanılan dięer benzer problemlerle karřılařtırıldığında "daha zor" olduęu dřncesidir.

2.4. Sıfır Bilgi İspatı Yntemi

Kriptografide, sıfır bilgi ispatı(SBİ) veya sıfır bilgi protokol, kimlik doęrulaması yapmak isteyen iki tarafın (kanıtlayıcı ve doęrulayıcı), kimlik doęrulama iin kullanılan bir ifadenin doęru olduęundan bařka karřı tarafa bilgi ifřa etmedięi bir kriptografik yntemdir. Kanıtlayıcı taraf sadece bilginin kendisinde olduęunu belli eder fakat bu bilgi hakkında doęrulayıcı ile herhangi bir paylařımda bulunmaz bylece doęrulayıcı bu bilgiye eriřemez.

Protokole gre bazen kanıtlayıcı ile doęrulayıcı rolleri deęiřtirebilir, rollerin dinamik olarak deęiřtięi ve her iki tarafın birbirine ait bilgilileri SBİ yntemi ile sorguladıęı ift ynl protokollerde mevcuttur.

Sıfır bilgi ispatları iin protokol mutlaka doęrulayıcıdan interaktif bir girdi gerektirir, genellikle bir meydan okuma veya zor bir problem řeklinde olan bu girdi kanıtlayıcıya bilgisini kullanarak bu meydan okumaya cevap verme fırsatı saęlar, kanıtlayıcı tarafından verilen yanıtlar doęrulayıcıyı ikna etmelidir ve yalnızca ifade doęruysa (yani, kanıtlayıcı iddia edilen bilgiye sahipse) geerli olmalıdır, aksi takdirde kimlik doęrulama geersizdir.

Yntemin tarihine bakacak olursak 1985 yılında Goldwasser, Micali, ve Rackoff bilinen ilk sıfır bilgi ispatlı protokol sunmuřlardır, bundan  yıl sonra

1988 yılında Feige, Fiat, ve Shamir mevcut protokolün kimlik doğrulama için özelleştirilen uygulaması ile ilgili bir çalışma ortaya koymuşlardır. Bu çalışmada, kimliğini ispatlayan tarafın kendi hakkında gizli bir bilgiyi karşı tarafa ifşa etmeden kimlik doğrulaması yapabileceği şekilde algoritmalar ortaya konmuştur [Goldwasser et al., 1985], [Feige et al., 1988].

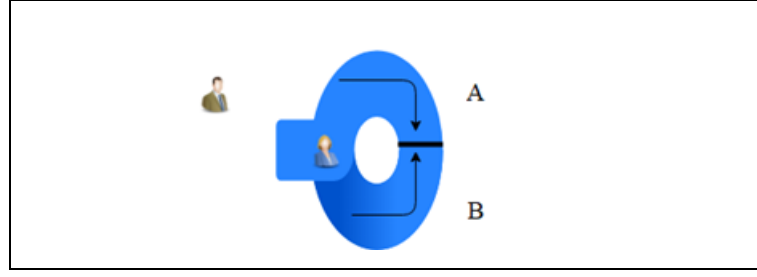
SBİ tabanlı bir kimlik doğrulama algoritmasının oluşması için sıfır bilgi ispatına dair üç temel özelliğin sağlanması gerekir bu özellikler:

- **Tamlık:** Eğer kimlik doğrulama ispatını içeren ifade protokole göre doğru ve tam ise kimliği ispatlayan ve doğrulayan taraf kolay bir şekilde kimlik doğrulaması yapabilmelidir. Bizim önerdiğimiz bu çalışmada tamlık dürüst olan taraflar için kriptografik işlemler ile sağlanmaktadır.
- **Doğruluk:** Eğer taraflardan biri dürüst olmayan bir şekilde kimlik doğrulama yapmaya çalışırsa başarılı olma şansı çok az olacak şekilde tedbirler olmalıdır. Bizim önerdiğimiz çalışmada büyük asal sayıların oluşturduğu sonlu aritmetiğinin kullanılması ile bunu sağlamaktayız.
- **Sıfır Bilgi:** Sadece kimlik ispatı ifadesinin doğru veya yanlış olduğunu bilmek kimlik ifadesini oluşturan gizli sırların elde edilmesi için yetersiz olmalıdır. Bizim önerdiğimiz bu çalışmada gizli sırlar Ayırık Logaritma Probleminin çözülme zorluğu ile korunmaktadır.

Bu üç özelliği sağlayan bir yöntem Nesnelerin İnterneti için SBİ tabanlı bir kimlik doğrulama şeması oluşturabilir.

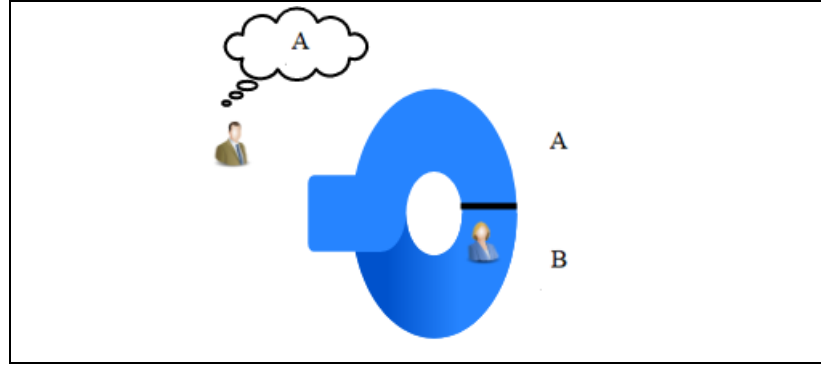
SBİ yöntemine dair en akılda kalıcı ve en açıklayıcı örnek mağara örneğidir, Mağara örneği üzerinden bu yönteme ait kavramsal bilgi daha iyi kavranabilir bir hale gelir, bu örnekte Alıcı ve Satıcı olmak üzere iki karakter bulunmaktadır [Quisquater et al., 1989].

Satıcı, Alıcıya mağara (Şekil - 1) içerisindeki kapının şifresini bildiğini iddia etmektedir.



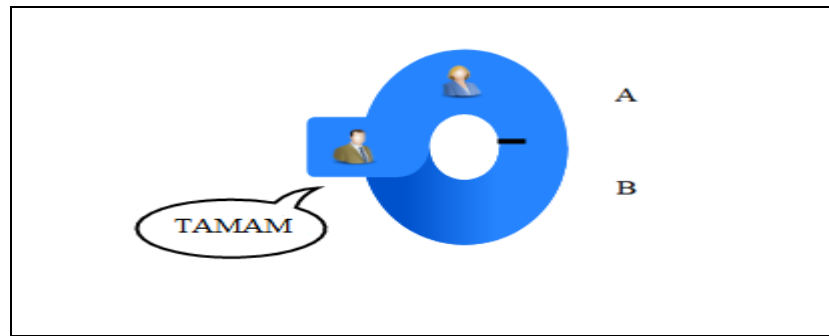
Şekil 2.5: Mağara Örneği Başlangıç Durumu.

Bunu kanıtlamak içinde mağaraya girip girişte bekleyen alıcıya hangi yönden çıkmasını istediğini sorar.



Şekil 2.6: Mağara Örneği Satıcının Kapıdan Geçmesi.

Satıcı, alıcının belirttiği yolu kullanarak kimliğini doğrulamaya çalışır.



Şekil 2.7: Mağara Örneği Satıcının Kimliğini Doğrulaması

Eğer satıcı istenilen yönden çıkarsa alıcıya gizli bilgisini ifşa etmeden kimliğini ispatlamış olur.

2.5. Önceden Önerilen Yöntemler ve Analizleri

Önceden önerilen yöntemler ilk önce alt başlıklara ayrılıp, bu şekilde incelenmelidir, bu alt başlıklar önerilen yöntemin kriptografik olarak dayandığı zor problemlerdir.

Kriptografi biliminde kimlik doğrulama için meydan okuma denilen bir interaktif adım gereklidir bu meydan okuma adımı SBI protokollerinde bahsedildiği üzere sadece gizli bir bilgiye sahip kişilere kolay, geri kalanlara ise zor olacak şekilde oluşturulmuş problemlerdir SBI yönteminin esas farklı noktası da burada ortaya çıkmaktadır.

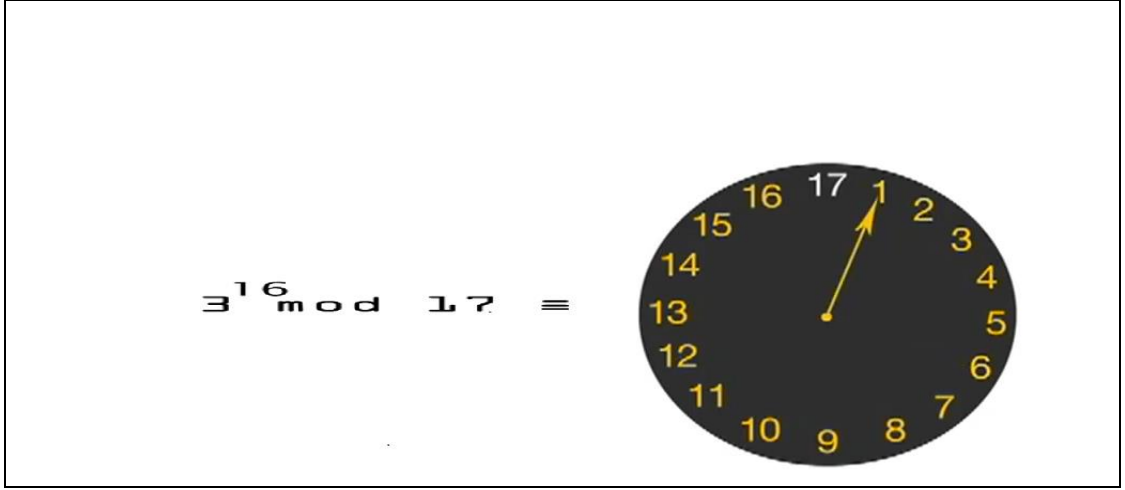
Bu noktada problemi kolayca çözerken karşı tarafa bu bilgi hakkında herhangi bir ipucu vermeyecek kriptografik fonksiyonları olmasıdır, alt başlıklar Ayırık Logaritma Problemi, Çarpanlara ayırma Problemi, Graf İzomorfikliği problemi gibi problemlerdir.

Ayrık logaritmaların hesaplanması üzerinde tanımlı olduğu alanın büyüklüğüne göre zor bir problemdir, alanın büyük olduğu durumlar için ayırık logaritma hesaplayan verimli algoritmalar mevcut değildir.

Ayrık logaritma probleminin tersi, yani ayırık kuvvet alma işlemi ise kolay hesaplamalar ile gerçekleştirilebilir bu sayede şifreleme için verimli, kırılması adına verimsiz bir yapı ortaya koymaktadır. Genel olarak, ayırık logaritma problemi, kriptografide döngüsel sonlu gruplarda örnek olarak, ElGamal, Diffie-Hellman, ve Dijital imza algoritmaları ayırık logaritma problemini temel alarak güvenliği garanti eder, yeni nesil kriptografi uygulamaları, ayırık logaritma problemini, sonlu cisimler üzerinde kurulan eliptik eğrilerin döngüsel alt grupları üzerinde uygulamaktadır.

$$Y = g^x \bmod p \quad (2.7)$$

Bu noktada p büyük asal bir sayı olmak üzere x gizli değerini Y değerinden elde etmek için en az p sayısı kadar deneme yapılmalıdır. Bizim bu çalışmamızda da bu problemin zorluğundan faydalanılacaktır.



Şekil 2.8: Ayrık Logaritma Problemi.

Tamsayı çarpanlara ayırma Problemi, bir bileşik sayının daha küçük tamsayının bir çarpımına dönüştürülmesidir. Bu tamsayılar asal sayılara kadar kısıtlanırsa, bu işleme asal çarpanlara ayırma denir.

Kompozit sayılar yeterince büyük olduğunda asal çarpanlarına ayırıp totient fonksiyonunu hesaplamak için implementasyonu henüz mümkün olmayan kuantum algoritmaları hariç hiçbir verimli algoritma bilinmemektedir bu da bu problemi zorlaştırmaktadır.

Birçok kriptografik protokol, büyük bileşik tamsayıları veya ilgili bir problemi (örneğin, RSA problemi) asal çarpanlara ayırma zorluğuna dayanır. Rasgele bir tamsayıyı verimli bir şekilde çarpanlara ayıran bir algoritma, RSA tabanlı açık anahtar şifrelemesini güvensiz hale getirir, fakat bu şekilde bilinen herhangi bir algoritma mevcut değildir. RSA algoritmasının nesnelerin interneti uygulamalarında çokta sık olmasa da kullanıldığı çalışmalar mevcuttur fakat yüksek hesapsal ihtiyaçları nedeni ile çok tercih edilmemektedir ayrıca eliptik eğriler üzerinde uyarlaması da mevcut değildir.

$$c = m^e \bmod n \quad (2.8)$$

$$c = m^e \bmod n \quad (2.9)$$

$$m = c^d \bmod n \quad (2.10)$$

$$\varepsilon * d \equiv 1 \text{ mod } \phi(n) \quad (2.11)$$

Graf izomorfikliğine dayanan sıfır bilgi ispatı kimlik doğrulama protokolü, iki taraf arasındaki etkileşimli bir protokoldür, taraflar bir onaylayıcı ve doğrulayıcıdır. Her iki taraf da, düğüm ve ayrıt sayısı olarak büyük bir grafin izomorfik eşlerini açık bir bilgi olarak tutarlar asıl grafi elde etmek için bu bilgi üzerinde yapılması gereken düğümlerin ve ayrıtların yer değiştirmesi işlemi tarafların gizli bilgisidir ve bu gizli bilgi ancak ifşa edilmeden esas grafi tekrar oluşturabilirse kimlik doğrulanabilir.

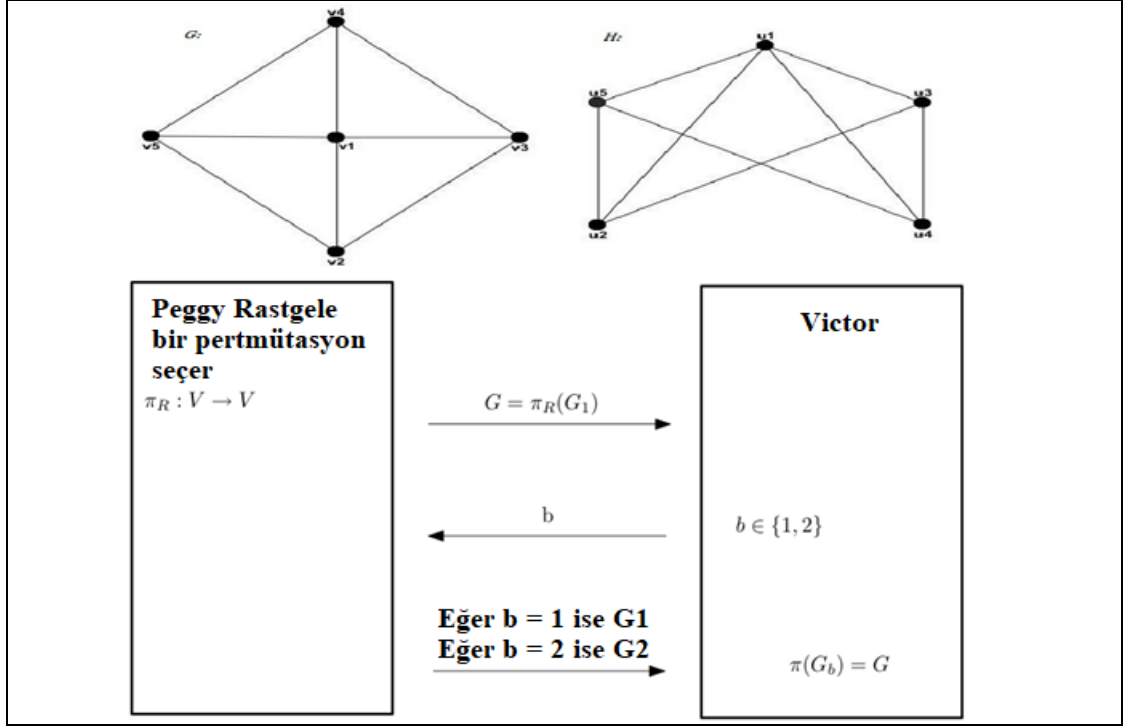
Graf izomorfikliği kullanan SBİ yöntemlerinin iki temel dezavantajı vardır ilk dezavantajı kriptografik fonksiyonların temelini teşkil eden çözülmesi zor problemin seçiminde kullanılan standart graf izomorfikliği problemi bazı teorik saldırılara karşı açıktır, çözüm olarak nispeten uygulaması daha zor ve hesapsal olarak maliyetli olan alt graf izomorfikliği problemi kullanılır.

İkinci dezavantaj ise graf izomorfikliğine dayanan yöntemler probabilistik (olasılıksal) bir yapıdadır, bu durum şöyle açıklanabilir mağara örneğine dönecek olursak satıcının alıcıyı kandırması olasılığı vardır her kapıdan çıkış işlemi ile bu olasılık azalmaktadır kısaca ayrık logaritma problemine dayanan yöntemlerde güvenlik bit uzunluğu ile sağlanırken bu yöntemde yüksek bir güvenlik düzeyi sağlamak için kimlik doğrulama işlemi birkaç defa tekrar etmelidir, graf izomorfikliği tabanlı yöntemlerde diğerlerine oranla çok daha yüksek bir ağ trafiği oluşmaktadır bu tekrar etme durumu ile birlikte Nesnelerin İnterneti uygulamalarında daha kötü bir tabloya dönüşmektedir.

Graf izomorfikliği kullanan bir protokol için genel kimlik doğrulama akışı şu şekildedir, G1 ve G2'nin iki graf olmak üzere Peggy G1 'in rastgele bir permütasyonunu seçer ve H olarak hesaplar ve H'yi Victor'a gönderir.

Victor rasgele bir şekilde bir $I \in \{1,2\}$ değeri seçer ve onu Peggy'ye gönderir, bu şekilde Victor, H ve G1 arasındaki izomorfizmi sorar. Peggy H' nin permütasyonunu oluşturur ve r olarak hesaplar böylece r, H ve G i arasındaki izomorfizmi belirler ve Victora gönderir.

Victor H'nin G i ve H arasındaki izomorfizmi sağladığını kontrol eder, H, n turda G i'nin görüntüsüye Victor, Peggy'nin "kanıtı" kabul eder.



Şekil 2.9: Graf İzomorfikliği Problemi.

Sıfır bilgi ispatı yöntemi kimlik doğrulama problemlerine karşı bir çözüm olarak sunulmuştur. Yöntemin Web uygulamalarında kimlik doğrulama alanında kullanılması yaklaşık 10 yıllık bir zaman diliminden bu yana incelenmektedir.

Sıfır bilgi ispatı yöntemi son yıllarda popülerliğini arttırmış bir yöntemdir ve önemli bir konu başlığıdır, bunu anlamak için geçtiğimiz yıllarda karşımıza çıkan iki olaya bakabiliriz.

İlk olarak dünyaca ünlü çevrimiçi oyun firması Blizzard'ın çevrimiçi oyunlara giriş yapılırken kullanılan sıfır bilgi ispatı tabanlı kimlik doğrulama protokolünün kullandığı doğrulayıcı verilerin bulunduğu veritabanı ifşa olmuştur kullanılan protokolde zayıf kriptografik özet ve tuzlandırma değerlerinin kullanılmasından dolayı çok bilinen şifrelere karşı gerçekleştirilen sözlük saldırıları ile kullanıcıların hesapları çalınmıştır [Web 2, 2012].

İkinci olarak 2016 yılında sıfır bilgi ispatı yöntemi kullanan bir protokol ile nükleer silahsızlanma için bir doğrulama şeması yapılabileceğini öngören bilimsel bir çalışma gerçekleştirilmiştir [Philippe et al., 2016].

Sıfır bilgi ispatı yöntemi kimlik doğrulama problemlerine karşı bir çözüm olarak sunulmuştur. Literatürde ilk olarak yöntem web uygulamalarında kimlik doğrulama için kullanılmıştır.

2008 yılında Slawomir ve Grzonkowski graf izomorfikliğine dayanan bir yöntem ile web uygulamaları için bir sıfır bilgi ispatı tabanlı yöntem önermişlerdir. Önerilen yöntem web uygulamaları için performans açısından oldukça verimlidir fakat önerdikleri şema “çalınmış doğrulayıcı” saldırılarına karşı açıktır [Grzonkowski, 2008].

2014 ve 2016 yıllarında sırası ile Cheu, Yang, Lin ve Jaffe “NARWHAL” adını verdikleri web uygulamaları için Schnorr imza tabanlı sıfır bilgi ispatı yöntemi kullanan şemalarını önermişlerdir, ardından Ansong ve Hayfron-Acquah benzer bir şemayı güçlendirerek tekrar sunmuştur. Önerilen şemaların kayıt aşamalarında yapılan bir ortadaki adam saldırısı ile doğrulayıcı değerlerin çalınması mümkündür, ayrıca şemalar “Oturum Hırsızlığı” ve “Denning Sacco” gibi saldırılara karşıda açıktır [Cheu et al., 2014], [Ansong et al., 2016].

Nesnelerin İnterneti için yapılan çalışmalar web için olanlar ile karşılaştırıldığında sayı olarak daha azdır.

2011 yılında Chatzigiannakis, Pyrgelis, ve Spirakis “Elliptic Curve Based Zero Knowledge Proofs and Their Applicability on Resource Constrained Devices” başlıklı çalışmalarında Schnorr şemasını eliptik eğriler üzerinde uygulamış ve performans açısından verimli sonuçlar almışlardır [Chatzigiannakis et al., 2011].

2013 yılında Alcaide, Palomar ve Castillo RSA tabanlı bir sıfır bilgi ispatı şeması ile farklı bir yöntem önermişlerdir [Alcaide et al., 2013].

2015 yılında Debiao He ve Sherali Zeadally “An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography” başlıklı çalışmalarında Nesnelerin İnterneti uygulamaları için o zamana kadar önerilmiş şemaların içerisinde karşılaştırma yapmış ve SBİ tabanlı önerilerin diğer yöntemlere göre genel olarak güvenlik seviyesinin daha iyi performansının ise normal seviyelerde olduğunu belirtmiştir [He et al., 2015].

2016 yılında Fernández ve Caballero-Gil graf izomorfikliğini kullanan bir sıfır bilgi ispatı yöntemi önermiştir önerdiği yöntemin 2008 yılında yayınlanan Slawomir ve Grzonkowski’nin yöntemine benzer fakat daha verimli olduğunu belirtmiştir [Fernández et al., 2016].

2016 yılında Echevarria, Legarda, Larrañaga ve Ruiz-de-Garibay’ın yapmış olduğu “lwAKE: A Lightweight Authenticated Key Exchange for Class 0 Devices” başlıklı çalışmada SBİ tabanlı bir yöntem geliştirdiklerini ve yaklaşık 10,7 ms süren

gibi bir zaman içerisinde şemalarının kimlik doğrulama yapabildiğini belirtmişlerdir [Echevarria et al., 2016].

2017 yılında Jonsson ve Tornkvist in yaptığı bir tez çalışmasında RSA tabanlı bir kimlik doğrulama şeması Raspberry Pi 3 cihazı üzerinde denenmiştir ve 64 ms performans sonucu elde etmişlerdir [Jonsson et al., 2017].

Zhang, Wen, Lu ve Lei 2017 yılında “A privacy-aware data dissemination scheme for smart grid with abnormal data traceability” başlıklı çalışmalarında SBİ tabanlı bir yöntem önermişlerdir ve tek düğümlü bir ağ yapısında şemalarında 22 ms performans ölçümü yapmışlardır [Zhang et al., 2017].

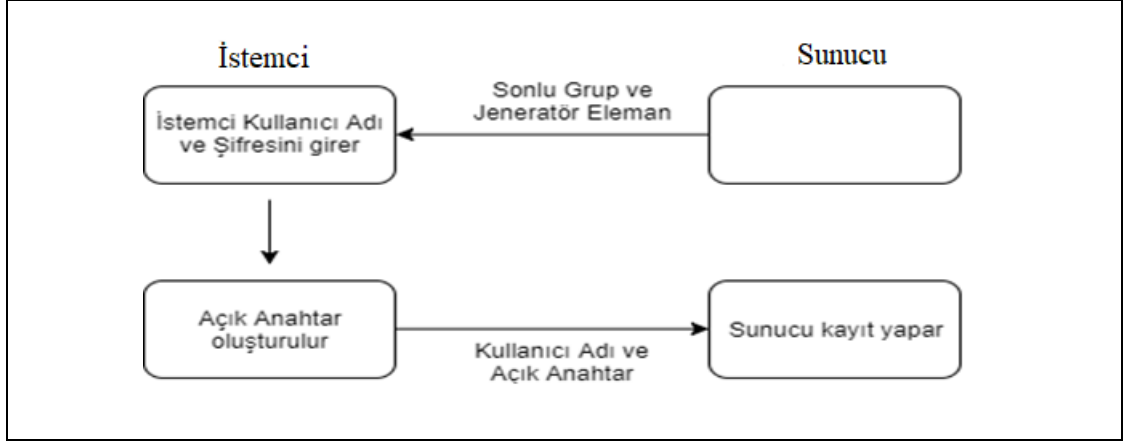
2017 yılında Beydemir ve Soğukpınar “Lightweight zero knowledge authentication for Internet of things başlıklı çalışmalarında SBİ tabanlı Sosyalist Milyonerler Protokolünün standart halini uygulamış ve 24 ms performans, 148 bayt ağ trafiği sonuçlarını elde etmişlerdir [Beydemir ve Soğukpınar, 2017].

2.5.1. Tek Yönlü Schnorr Bilgi İspatı Şemasının Analizi

Schnorr Bilgi İspatı şeması kriptografide veya Schnorr imzası, Schnorr imza algoritması tarafından üretilen dijital bir imzadır. Güvenliği, belirli ayrık logaritma problemlerinin çözümsüzlüğüne dayanır. Verimli ve kısa imzalar ürettiğinden Nesnelerin İnterneti Uygulamaları için uygundur. Şubat 2008'de sona eren A.B.D. Patenti 4.995.082'de kapsanmıştır bu tarihten itibaren üzerinde akademik çalışmalar yoğunlaşmıştır ve Schnorr imza algoritmaları ECC kolayca uygulanabilir yapıdadır.

2014 yılında yapılan NARWHAL çalışmasında Schnorr şeması en yalın hali uygulanarak bir SBİ tabanlı şema önerilmiştir [Cheu et al., 2014].

Şema iki adımdan oluşmaktadır ilk aşamada istemci kendisini ayrık logaritma problemini kullanarak gizli değerini (x) açık değere dönüştürerek (Y) kullanıcı adı ile birlikte kayıt eder.

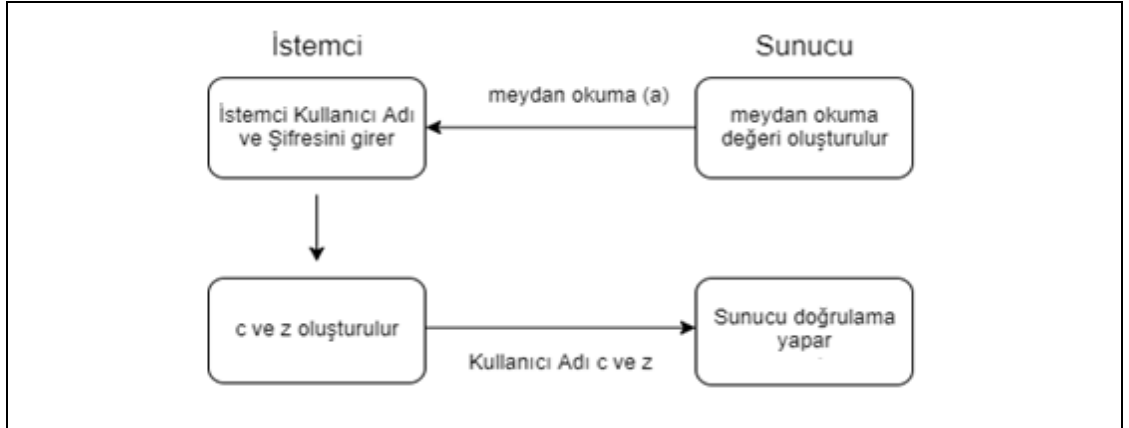


Şekil 2.10: Schnorr Kayıt İşlemi.

$$Y = g^x \quad (2.11)$$

İkinci aşamada sunucu kimliğini doğrulamak isteyen istemciye kayıt aşamasında elde ettiği açık değeri kullanarak bir meydan okuma problemi yollar.

İstemci gizli x değerini bildiği için problemi çözecek şekilde hesaplamaları yapıp sunucuya gönderebilme fırsatına sahiptir.



Şekil 2.11: Schnorr Kimlik Doğrulama İşlemi.

$$Y_0 = g^x \quad (2.12)$$

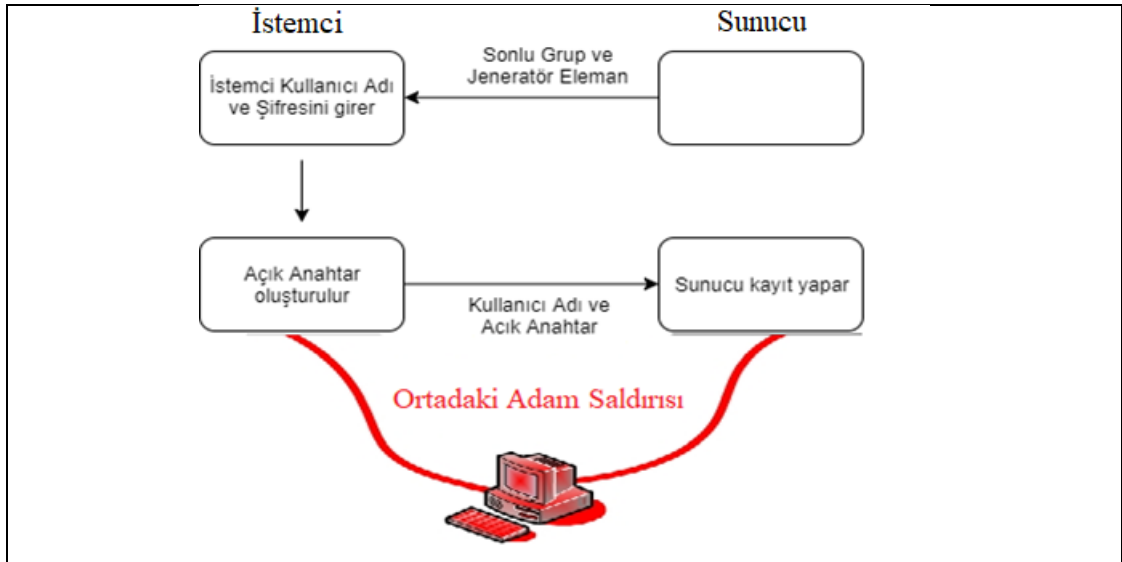
$$r = Y_0 + a \quad (2.13)$$

$$T = g^r \quad (2.14)$$

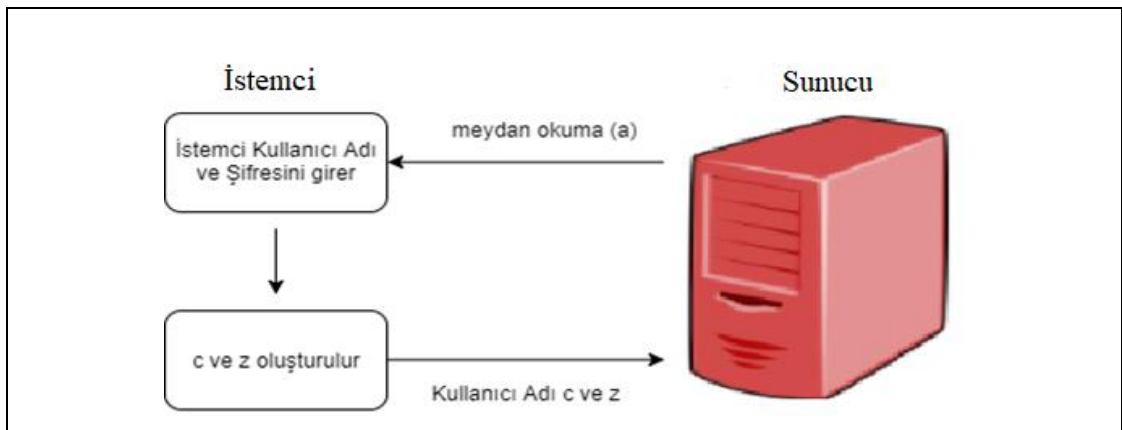
$$c = \text{hash}(Y||T||a) \quad (2.15)$$

$$z = r - c * x \quad (2.16)$$

Bu noktaya kadar bir problem gözükmemektedir fakat kayıt aşamasında eğer açık anahtarın SSL/TLS benzeri bir ekstra şifreleme olmaksızın sunucuya yollanması nedeni ile ortadaki adam saldırısı gerçekleştiren kişiler açık anahtarı ele geçirip, kullanarak sunucu kimliğine bürünerek istemciye meydan okuma cevapları yollayabilir bu şekilde istemciye sunucu rolü yaparak sunucun iletmesi gereken verileri çarpıtabilir veya çeşitli saldırılar gerçekleştirebilir.



Şekil 2.12: Schnorr Kayıt İşlemi Zafiyeti.



Şekil 2.13: Schnorr İmzasına Karşı Saldırı.

Bu noktada çözüm güvenli bir kayıt adımını tasarlanan şemaya bütünleşmiş etmektir ayrıca meydan okuma adımları daha güvenli olmalıdır.

2.5.2. Çift Yönlü SRP Şemasının Analizi

SRP Güvenli Uzaktan Parola Protokolü (SRP), özellikle mevcut patentlerin etrafında çalışmak üzere tasarlanmış arttırılmış bir şifre doğrulama anahtarı sözleşmesi (PAKE) protokolüdür.

Protokolün şartlarına göre, bir şifreyi bilen iki taraf göz önüne alındığında, SRP (veya başka herhangi bir PAKE protokolü), bir tarafın "istemci" veya "sunucu" olması gerekir, istemci ilk aşamada kendi kimliği ile ilgili açık bir bilgi yollar, sunucu bu bilgiyi kullanarak veritabanından bir doğrulayıcı değeri çeker ve bu değer ile bir meydan okuma oluşturur, karşılıklı iki taraf bu meydan okuma adımlarını gerçekleştirir bu şekilde çift yönlü bir kimlik doğrulama sağlanmış olur[Wu 2002].

	İstemci		Sunucu
1.		$\xrightarrow{I}$	(Getir s, v)
2.	$x = H(s, I, P)$	$\xleftarrow{s}$	
3.	$A = g^a$	$\xrightarrow{A}$	$B = 3v + g^b$
	$u = H(A, B)$	$\xleftarrow{B}$	$u = H(A, B)$
4.	$S = (B - 3g^x)^{a+ux}$		$S = (Av^u)^b$
5.	$M_1 = H(A, B, S)$	$\xrightarrow{M_1}$	(Doğrula M_1)
6.	(Doğrula M_2)	$\xleftarrow{M_2}$	$M_2 = H(A, M_1, S)$
7.	$K = H(S)$		$K = H(S)$

Şekil 2.14: SRP-6 Şeması.

İki taraf yukarda bahsedilen protokolü uyguladıktan sonra artık iki tarafında paylaşımlı, güçlü bir oturum anahtarı olan K değeri vardır. Tarafların kimlik doğrulama işlemini tamamlamak için birbirlerine anahtarlarının uyduğunu kanıtlamaları gerekmektedir.

İstemci ve Sunucu şu şekilde işlemler gerçekleştirir:

- Client → Server: $M1 = \text{Hash}[s \mid A \mid B \mid K_{\text{Client}}]$. Server $M1$ 'i doğruluyor.
- Server → Client: $M2 = H(A \mid M1 \mid K_{\text{Server}})$. Client $M2$ 'yi doğrular.

Bu yöntem, kimliğe bürünme işleminde yalnızca anahtardan daha başarılı olmak için paylaşılan durumdan daha fazla tahmin etmeyi gerektirir. İlave devletlerin çoğu kamuya açıkken, özel bilgi, sunucu özel anahtarı gibi karma işleve girdilere güvenle eklenebilir.

Alternatif olarak, sadece şifreye özel kanıt olarak K 'nın hesaplanması atlanabilir ve paylaşılan S değeri ile kimlik doğrulanabilir:

- Client → Server: $M1 = H(A \mid B \mid S_{\text{Client}})$. Server $M1$ 'i doğrular.
- Server → Client: $M2 = H(A \mid M1 \mid S_{\text{Server}})$. Client $M2$ 'yi doğrular.

SRP-6 protokolünün Nesnelerin internetine uygulanabilir açısından iki temel eksikliği bulunmaktadır onun haricinde bir güvenlik açığı henüz tespit edilmemiştir.

SRP-6 Protokolü Nesnelerin İnterneti uygulamalarında sıkça gerek duyulan cihaz, duyarga veya uç düğüm dediğimiz noktaların merkezi bir sunucuya ağa katılım gerçekleştirdikleri anda kayıt olma gereksinimleri için uygun değildir.

Önceki çalışmalar bölümünde de bahsi geçen SRP-6 şeması kullanan Blizzard firması müşterilerinin oyuna kayıt olması ve kimlik doğrulaması için kullandığı bu sistemde kayıt işlevi tıpkı Schnorr şemasındaki gibi doğrulayıcı değerleri açık edecek şekilde uygulanmıştır, açık edilen doğrulayıcı değerler düşük bit uzunluğu kullanan sonlu bir grup üzerinde uygulandığında ayrık logaritma problemi çözülebilir hale gelmiştir ve açık değerlerden gizli değerler elde edilebilmiştir. SRP-6 güncel dokümanlarında kayıt işlevinin kapalı olması önerilmektedir ayrıca güvenliği sağlamak için yüksek bit uzunluklu grup kullanılması gerekmektedir.

İkinci eksiklik ise matematiksel olarak SRP-6 protokolünün eliptik eğriler üzerinde uygulanamamasıdır, şemada bahsi geçen adımları gerçekleştirmek için eliptik eğrilerin sınırladığı sonlu alanlarda standart galois alanında bulunan toplama ve çıkarma işleminin tanımlanamamasıdır.

Aşağıda bulunan tabloda Eliptik Eğrilerin sınırladığı alanlar ile Standart Galois alanları içerisinde tanımlı bir takım matematiksel işlemlerin birbirleri arasındaki izdüşümleri verilmiştir.

Tablo 2.1: Alanlar arası işlem izdüşümleri.

Alan Tipi	Eliptik Eğri	Standart Galois
Üs Alma İşlemi	$Y0 = x * g$	$Y0 = g^x$
Çarpma İşlemi	$z = c + x$	$z = c * x$
Toplama veya Çıkarma İşlemi	Tanımlı Değil	$r = Y0 + a$

3. SIFIR BİLGİ İSPATI YÖNTEMİ

Bu bölümde ikinci bölümde öğrenilen kriptografi bilgileri, eliptik eğriler üzerinde ayrık logaritma probleminin kırılma zorluğu, curve25519 ile verimli hesaplama ve sosyalist milyonerler protokolü gibi özellikleri kullanarak özgün bir SBI kullanan kimlik doğrulama protokolü ve şeması önerilecektir.

3.1. Sosyalist Milyonerler Protokolü ve Özgün Curve25519 Uygulaması

Sosyalist Milyonerler Protokolü veya literatürde Yao's Millionaires problemi olarak geçen protokol, tanınmış bir bilgisayar bilimcisi ve hesaplama teorisyeni olan Andrew Yao tarafından 1982'de tanıtılan çok partili bir hesaplama problemidir.

Problem esasında gerçek zenginliklerini göstermeden, zenginliklerinin eşit olup olmadığını bilmek isteyen iki milyonerin güvenli hesaplamalar yaparak eşitlik kontrolü yapmasına dayanır.

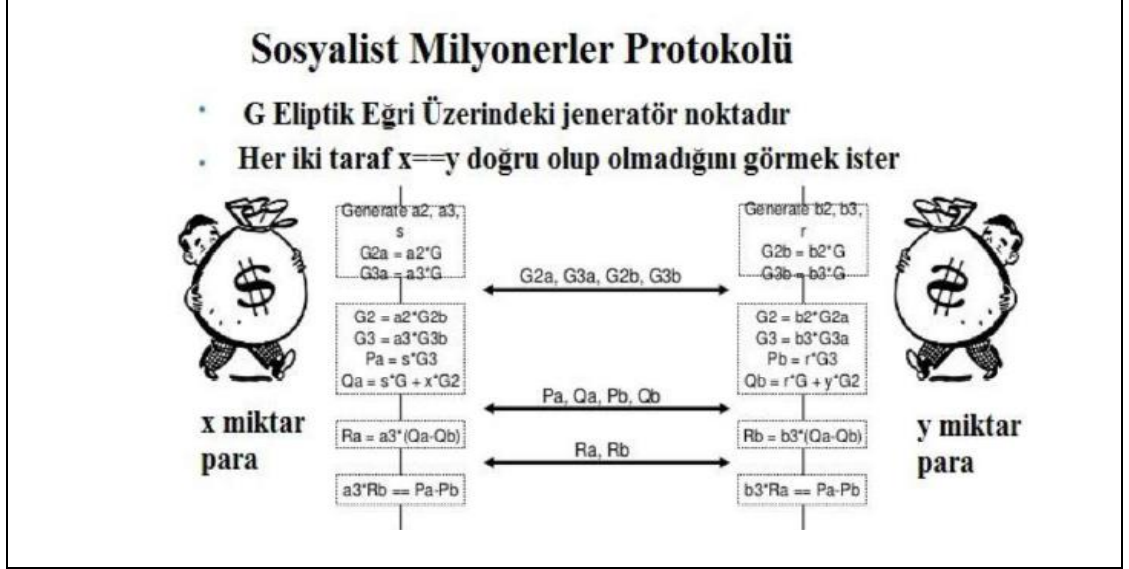
Milyonerler Sorunu, çözümü e-ticaret ve veri madenciliğinde de kullanılan önemli bir sorundur.

Kriptografide ise sosyalist milyoner protokolü, iki milyonerin zenginlikleri eşit olup olmadığını, zenginlikleri hakkında birbirlerine bilgi vermeden belirlemek istediği bir protokoldür. Milyoner Sorununun bir varyantıdır, çünkü iki milyoner zenginliğini birbirine bildirmeden kendi zenginliği ile karşılaştırmak istemektedir.

Matematiksel olarak bu protokol şu şekilde ifade edilebilir, Alice ve Bob'un zenginlikleri b_1 ve b_2 olsun gizli bir eşitlik fonksiyonunu hesaplamak istediklerini farz edelim $f(b_1, b_2) = [b_1 = b_2]$. Bu sorun, sosyalist milyonerlerin problemi olarak da bilinir ve aşağıdaki protokolü uygulayarak çözülebilir.

- 1. tur: Alice ve Bob, ortak anahtarlarının dağıtılmış bir çiftini üretirler.
- 2. tur: Her iki taraf da zenginliklerini bir şifreleme yöntemi ile karşı tarafa meydan okuma olarak yollar.
- 3. tur: İki taraf kimlik doğrulama değerlerini birlikte hesaplarlar.

- 4. tur: Her iki taraf da birlikte gizli değerlerin şifresini çözer, çözülen şifrenin değeri 0 ise her iki taraf gizli bir şekilde eşit değerleri birbirinden çıkartmış demektir.



Şekil 3.1: Standart Sosyalist Milyonerler Protokolü.

3.2. Kayıt Olma

Kayıt Olma Register işleminde öncelikle her iki taraf ElGamal şifrelemesi yapmak için öncelikle Diffie Hellman anahtarı oluştururlar ardından Mobil İstemci ElGamal şifrelemesi yaparak gizli kalması gereken doğrulayıcı değeri Cihaza yollar Cihaz sahip olduğu Diffie Hellman anahtarı ile deşifreleme yapar ve gizli değeri kaydeder.

$$G_a = a * G \quad (3.1)$$

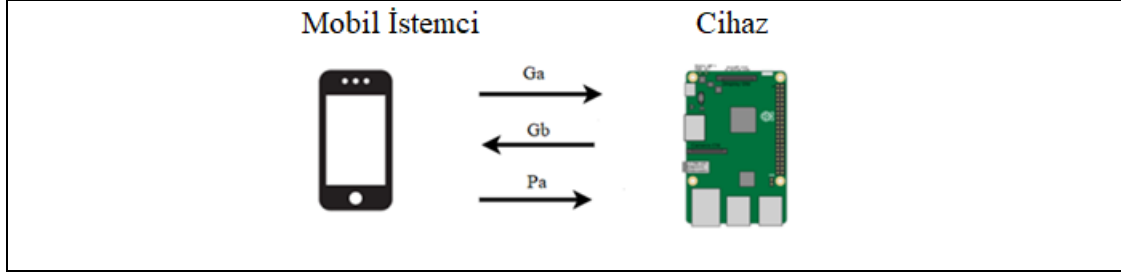
$$Y_a = x * G \quad (3.2)$$

$$G_b = b * G \quad (3.3)$$

$$G_{ab} = G_a * G_b \quad (3.4)$$

$$Pa = Gab + Ya \quad (3.5)$$

$$Ya = Pa - Gab \quad (3.6)$$



Şekil 3.2: Önerilen Şemanın Kayıt İşlemi.

3.3. Kimlik Doğrulama

Mobil İstemci Eliptik Eğri üzerinde anlaşılan G noktası değeri üzerinde rastgele değerler ile geçici anahtarlar üretir ve Cihaza yollar.

$$Ga = a * G \quad (3.7)$$

Cihaz benzer olarak kendi geçici anahtarlarını ve doğrulama için edindiği geçici anahtarlar ile işlemler yapar gizli şifresi “ y ” değerini meydan okuma için kullanır.

$$Gb = b * G \quad (3.8)$$

$$Gab = Ga * Gb \quad (3.9)$$

$$Pb = Gab + y * G \quad (3.10)$$

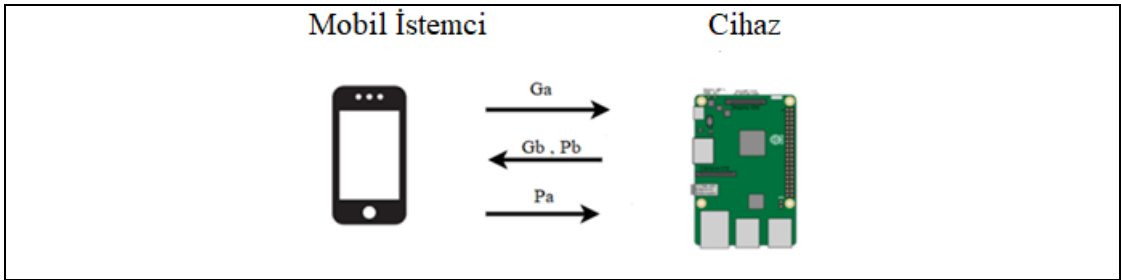
Mobil İstemci bir önceki adımdaki değerleri edinir ve kendi şifresi “ x ” ile meydan okuma değerini hesaplar edindiği değerler ile bu meydan okuma değerini karşılaştırır ve bir sonuç değeri oluşturur sonucu karşı tarafa yollar.

$$Gab = Ga * Gb \quad (3.11)$$

$$Pa = Gab + x * G \quad (3.12)$$

Cihaz aldığı Pa, Mobil İstemci Pb değerine göre sonuç değerini hesaplar ve kimlik doğrulama işlemi yapar eğer eşitlik sağlanırsa kimlik doğrulama başarılı demektir.

$$Pa - Pb \equiv 0 \quad (3.13)$$



Şekil 3.3: Önerilen Şemanın Kimlik Doğrulama İşlemi.

3.4. Protokolün İyileştirilmesi

SMP bir çok bilimsel merci tarafından hızlı, verimli ve güvenli olarak tarif edilen Curve25519 eliptik eğrisi üzerinde gerçekleştirilmesi ile bizim kimlik doğrulama şemamızı oluşturmuştur, esasen bu protokol Diffie-Hellman protokolünün genişletilmiş halidir ve ayrık logaritma probleminin eliptik eğriler üzerinde tekrar tanımlanması çok önemli bir noktadır, çünkü ayrık logaritma problemlerinde gördüğümüz üs alma ve çarpma işlemleri eliptik eğriler üzerinde çarpma hatta iyi uygulanabilirse sadece toplama işlemleri ile güvenlik seviyesi aynı kalmak kaydı ile gerçekleştirilebilir bu da performans olarak çok büyük avantajlar sağlamaktadır[Korchagin et al., 2015].

3.4.1. Protokolün İyileştirilmesinin Özgün Katkıları

- Curve25519 Eğrisi

Kriptografide, Curve25519 eliptik bir eğri olup standart olarak 128 bitlik güvenlik sunar ve ilk olarak Daniel J. Bernstein tarafından eliptik eğri Diffie-Hellman (ECDH) anahtar sözleşme şeması ile birlikte kullanılmak üzere tasarlanmıştır. En hızlı ECC eğrilerinden biridir ve bilinen herhangi bir patent kapsamına girmez. Referans uygulamaları kamuya açık dağıtım ile korunmaktadır.

Orijinal Curve25519 ortaya döken makale çalışmasında Curve25519 Diffie-Hellman (DH) fonksiyonu için özel olarak tanımlanmıştır. Eğrinin modüler sınırlandırılmasında kullanılan sayı ile tanımlanan asal alanın kuadratik uzantısı üzerinde bir Montgomery eğrisi olan curve25519 formülü şu şekildedir:

$$p = 2^{255} - 19 \quad (3.14)$$

$$B * (A^2 - 4) \neq 0 \quad (3.15)$$

Eğridegrubun jeneratör noktası $x = 9$ olacak şekilde kullanılır. Hızlı skaler çarpım için geleneksel, sıkıştırılmış eliptik nokta kullanır (sadece X koordinatları), bu nedenle sadece XZ koordinatlarını kullanarak Montgomery merdiveninin ECDH için etkili bir şekilde kullanılmasına izin verir.

Curve25519 birçok potansiyel uygulama tuzaklarından kaçınacak şekilde inşa edilmiştir. Örneğin jeneratör noktanın order(sıra veya düzen olarak tanımlanan)değeri yüksektir, tasarım gereği, zamanlama ve yan kanal saldırılarına karşı bağımsızdır ve geçerli bir genel anahtar olarak herhangi bir 32 baytlık dizeyi kabul eder ve doğrulama gerektirmez.

- Montgomery Formu

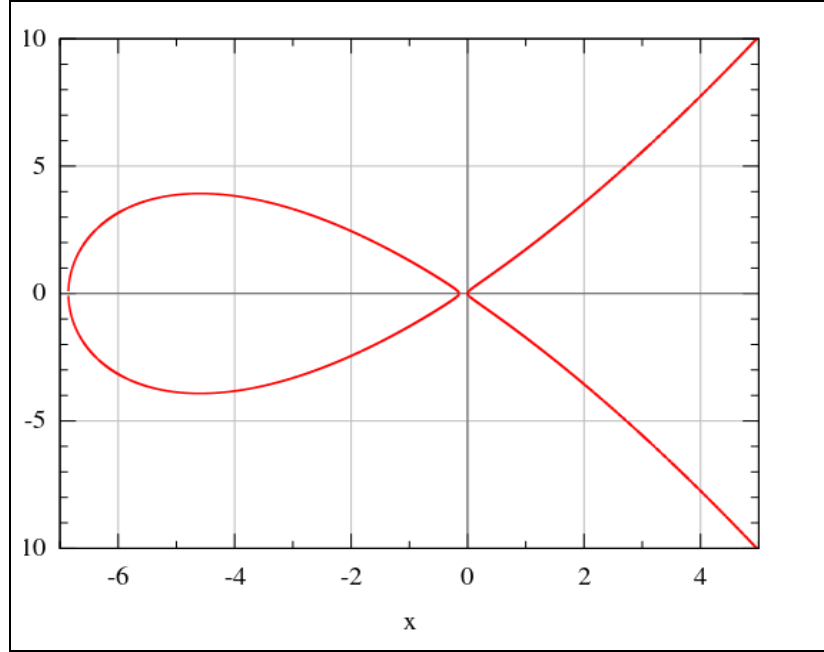
Matematikte Montgomery eğrisi veya formu, 1987'de Peter L. Montgomery tarafından ortaya atılan normal Weierstrass formundan farklı bir eliptik eğri formudur. Verimli ve hızlı hesaplamalar için ve özellikle farklı kriptografi uygulamalarında sıkça kullanılır. Bir alan p üzerindeki bir Montgomery eğrisi belirli $A, B \in K$ ve B için:

$$B * y^2 = x^3 + A * x^2 + x \bmod p \quad (3.16)$$

$$B * (A^2 - 4) \neq 0 \quad (3.17)$$

Olacak şekilde bir eğri olarak tanımlanabilir.

Montgomery formunun en büyük avantajlarından biri bu formda tanımlanan eğriler için hızlı verimli skaler nokta çarpım hesaplama yöntemlerinin mevcut olmasıdır. Curve25519 eğrisi incelendiği zaman bir montgomery eğrisidir. Bu çalışmada performans açısından iyileştirmeyi sağlayan ve uygulama için seçilmesinde anahtar özelliklerden biri curve25519'un montgomery formunda olmasıdır.



Şekil 3.4: Montgomery Eğrilerinin Genel Formu.

- Montgomery Üs Alma Merdiveni

Montgomery Üs Alma Merdiveni algoritması bizim çalışmamızda kullandığımız hızlı bir skaler çarpma algoritmasıdır. Standart Montgomery Merdiveninden farklı olarak X-Z düzleminde değil X-Y düzleminde çalıştığı için nokta invers alma işlevi için daha uygundur, invers alma işlevi önerdiğimiz şema içerisinde ElGamal deşifrelemesi ve ona bağlı olan önerdiğimiz kimlik doğrulama şeması için çok önemlidir ve performans olarak iyileştirme sağlamıştır fakat önerilen

şemanın standart montgomery merdivenine göre biraz daha yavaş olmasına karşın hız açısından oldukça verimli ve gelen bit değerinin içeriğine göre yaptığı dallanmalarda benzer işlevler olduğundan yan kanal analizine karşı dirençlidir.

```
Montgomery Üs Alma Merdiveni Algoritması
Girdiler:
P(x,y) eliptik eğri üzerinde bir nokta;
k = skaler çarpım değeri veya gizli anahtarın 1/0 bit katarı olarak ifade edilmiş
dizesi;
Çıktı:  $Q = k * P$ 
BASLA:
 $R0 \leftarrow P$  // R0 P noktasına eşitle
 $R1 \leftarrow 2 * P$  // R1  $2 * P$ 'ye eşitle
DONGU:
for i from n-2 downto 0 do // k bit dizisini döngü ile gez
    if  $k(i) = 0$  then // gelen bit değeri 0 ise aşağıdaki işlemleri yap
         $R0 \leftarrow R0 + R1$  //  $R0 + R1$  değerini R0 a eşitle
         $R1 \leftarrow 2 * R1$  // R1'i ikiye katla kendine eşitle
    else // eğer gelen bit değeri 1 ise aşağıdaki işlemleri yap
         $R1 \leftarrow R0 + R1$  //  $R0 + R1$  değerini R1'e eşitle
         $R0 \leftarrow 2 * R0$  // R0'ı ikiye katla kendine eşitle
    DONGUBITIR;
return R0 //  $R0 = Q = k * P$ 
```

Şekil 3.5: Montgomery Üs Alma Merdiveni Algoritması.

Algoritmanın sözde kodunda görüldüğü üzere dallanma koşulları olan bit değerlerinin 0 veya 1 olması durumu yapılan işlemlerde farklılık yaratmamıştır, birbirine benzer işlemler olan farklı durumlarda gizli anahtar değerinin döngü içerisinde işlendiği esnada ikili sayı olarak karşılığı net değildir.

Bizim çalışmamızda tek bir skaler nokta çarpımı yukarda belirtilen skaler nokta çarpım algoritması yaklaşık olarak 4,8 ms içerisinde tamamlanmaktadır, diğer çalışmalarda ve bizim çalışmamızda bu değerlerin ölçülmesi Diffie Hellman anahtar anlaşma protokolü performans benchmarkları ile ölçülmüştür.

Tablo 3.1:Skaler Nokta Çarpım Performansları.

Öneriler	Bizim Önerimiz	[Chatzigiannakis, I vd., 2011].	[He, D vd., 2015].
Yapı	Eliptik Eğri 25519	Eliptik Eğri	Eliptik Eğri
Hesaplama Yöntemi	Montgomery Merdiveni	Bilinmiyor	Bilinmiyor
Skaler Nokta Çarpım Süresi	~4,8 ms	~6,4 ms	~4,92 ms

- Yan Kanal Analizi Direnci

Montgomery üs alma merdiveni yaklaşımı, skaler nokta çarpımını sabit bir zaman miktarında hesaplar. Zamanlama veya güç tüketimi ölçümleri ile bir yan kanal saldırısı gerçekleştiren bir saldırgana karşı bu algoritma yararlı olabilir. Algoritma ikiye katla ve ekle algoritması ile benzer bir gösterimi kullanır.

4. UYGULAMA ve DEĞERLENDİRME

Bu bölümde bir önceki bölümde önerilen yöntemin sınaıa sonuçları ve önceden önerilen yöntemler ile karşılaştırmaları verilecektir.

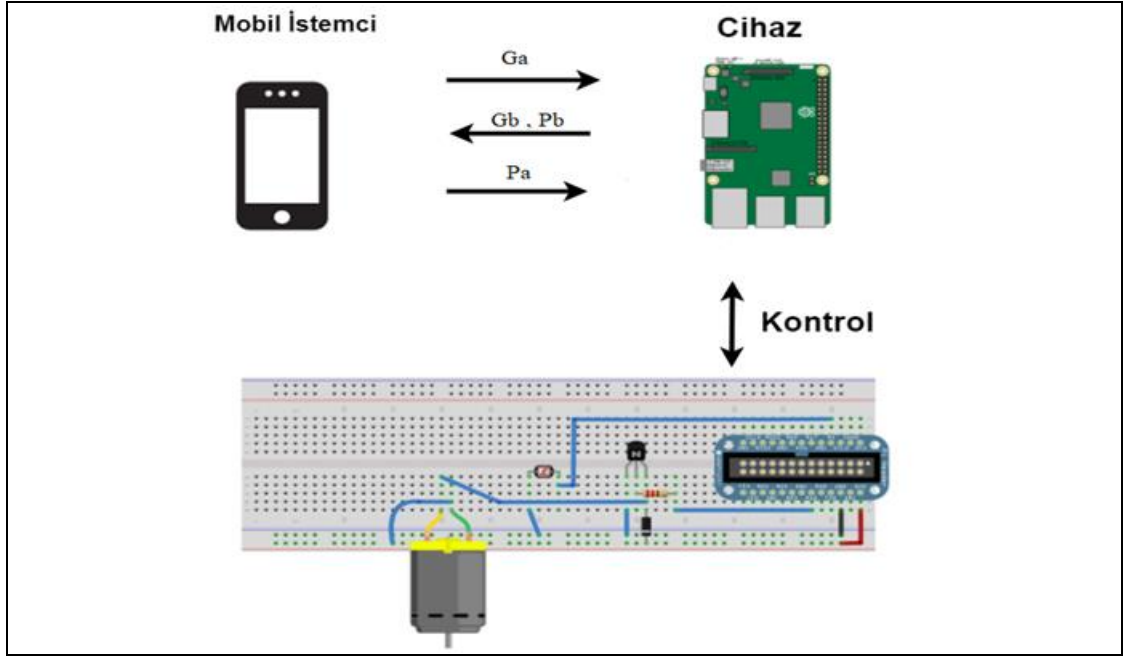
4.1. Raspberry Pi 3 Cihazı ile DC Motor Kontrol Düzenegı

Örnek uygulamada Nesnelerin İnterneti konseptine uygun bir çalışma olması açısından bir mobil istemciden gelen kimliğı doğrulanmış mesajlara göre DC bir elektrik motorunun bir cihaz tarafından kontrolünü sağlayan bir düzenek uygulaması JAVA programlama dili ile tasarlanmış ve hazırlanmıştır.

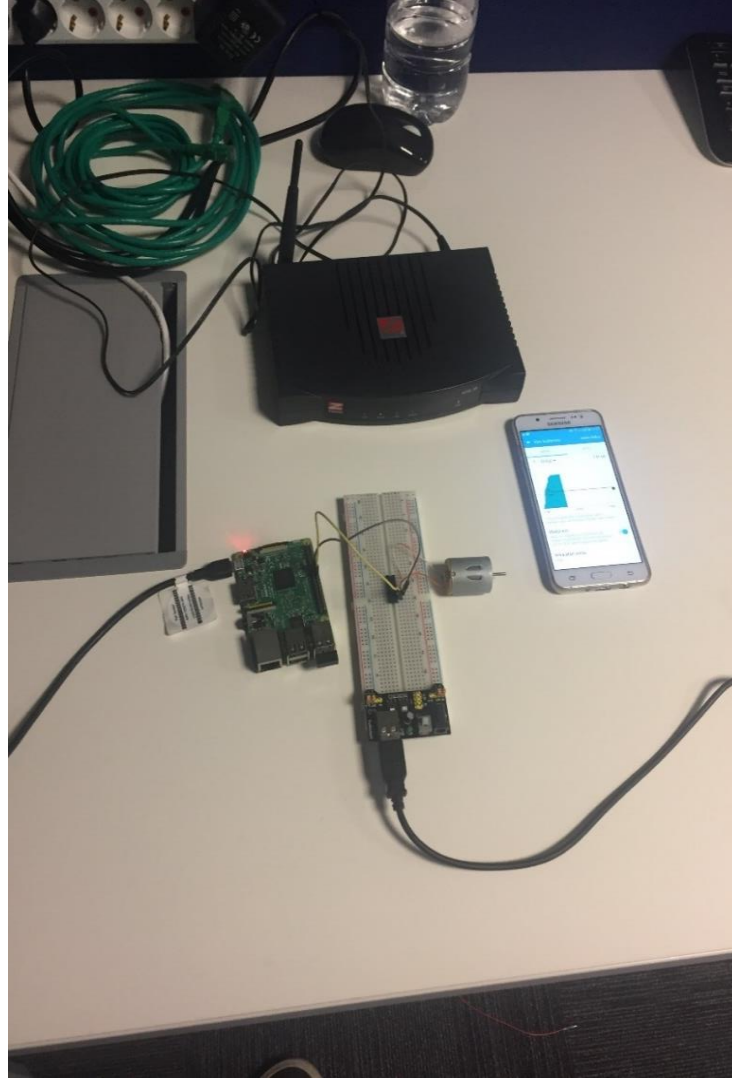
Örnek uygulama “Mobil İstemci” ve “Cihaz” olarak adlandırılan iki farklı sistem üzerinde gereklenmiştir. Mobil istemci Android işletim sistemi olan 1,2 GHz işlemci frekanslı 4 çekirdekli 2 GB hafızalı bir akıllı telefondur.

Cihaz ise 1,2 GHz işlemci frekansı olan 4 çekirdekli 1 GB hafızalı bir Raspberry Pi 3 cihazıdır.

Önceki bölümde bahsedilen şemanın uygulanması bu iki sistem üzerinde yapıldığında 10 kez tekrarlanan kimlik doğrulama süreci boyunca Mobil istemci akıllı telefon için ortalama 17,73 ms ve Raspberry Pi 3 cihaz için ortalama 18,86 ms sürmüştür her iki taraf için düşündüğümüzde ortalama 18 ms’de kimlik doğrulama tamamlanmaktadır.



Şekil 4.1: Uygulamanın Şeması.



Şekil 4.2: Uygulamanın Görseli.

4.2. Teorik Güvenlik Analizi

Önerilen metodun teorik güvenliği eliptik eğri üzerindeki ayrık logaritma problemine dayanmaktadır.

Curve25519 eğrisi 256 bitlik anahtar uzunluğu kullanmaktadır, bu anahtar uzunluğu standart RSA ve Diffie-Hellman ile kıyaslandığında 3072 bite denk gelmektedir[Bos et al., 2009].

N ayrık logaritma probleminin üzerinde tanımlı olduğu sonlu alanı tanımlamak için gerekli olan büyük asal sayıyı ifade eden bit sayısı olarak düşünüldüğünde yöntemin $O(2^N)$ üstel karmaşıklığı vardır, güncel araştırmalar göstermektedir ki 2,2

GHz, 8 çekirdekli bir işlemci 768 bitlik bir ayrık logaritma problemini 825 yıl içinde çözmektedir [Kleijnung et al., 2017].

4.3. Uygulama Güvenlik Analizi

Uygulamayı gerçekleştirdiğimiz düzenek üzerinde sızma testi ve güvenlik uzmanlarının kullandığı Kali Linux gibi birçok yazılım ve ortadaki adam saldırısı gibi birçok yöntem kullanılarak uygulama güvenlik analizi yapılmıştır ilk bölümde bahsedilen tüm açıklıklar için ayrıntılı analiz şu şekildedir:

- Güvensiz Ara yüz

Önerdiğimiz şemada cihazlara yapılan erişim Mobil İstemci üzerinden WebSocket bağlantıları kurularak yapılmaktadır erişim esnasında şemadaki kimlik doğrulama adımları başarı ile sağlanmazsa cihaz üzerinden bilgi transferi sağlanmamaktadır.

- Yetersiz Kimlik Doğrulama

Düzenek üzerinde yetkilendirilmemiş istek paketleri veya ele geçirilmiş, yetkilendirilmiş paketler şemada oluşturulan Diffie Hellman oturum anahtarının sürekli bir devinim içerisinde MAC (Mesaj Doğrulama Kodu) ile birlikte kullanılması ile filtrelenmektedir.

- Güvensiz Ağ Hizmetleri

Kullanılan haberleşme protokolü HTTP protokolü ile çok benzerlik gösteren dinamik WebSocket protokolüdür ve TCP protokolü üzerine kurulmuştur dinamik olması sayesinde anlık olarak belirsiz herhangi bir port üzerinden haberleşme yapabilmektedir.

- Gizlilik İfşası

Kayıt ve Kimlik Doğrulama aşamalarında ElGamal şifrelemesi kullanılması ile gizli değerler ifşa edilmemiştir.

- Güvensiz Bulut Ara yüzü

Cihazların kendi ağ sistemlerinden dışarıya çıktığı durumda haberleştiği dış cihazın herhangi bir haberleşme adımında MAC değerinin olması gereken değerler ile uyumsuzluk göstermesi algılanabilmiş ve bu sayede trafik yönlendirilmesi engellenmiştir.

- Zayıf Fiziksel Güvenlik

Cihazların bulunduğu konumlarda, cihazlar haberleşirken üzerlerinde gizli bilgilerin elektronik olarak ifşa edilmesini engelleyen yazılımsal olarak yapılan bir koruma montgomery merdiveni olarak adlandırılan skaler nokta çarpım algoritması ile sağlanmıştır.

- Oturum Hırsızlığı Saldırıları

Oturum hırsızlığı iletilen mesajlardan çerez değerlerinin alınıp tekrar eden bir şekilde kaynak erişiminin yapılmasıdır. Bizim çalışmamızda, WebSocket protokolü içerisinde ortadaki adam tarafından hesaplanamayan değerlerin mesaj kimlik doğrulama kodu (MAC) içerisinde zaman damgaları ile birlikte kullanılması ile bu saldırılar engellenmektedir.

- Denning Sacco Tekrar Saldırıları

Denning Sacco tekrar saldırıları, doğru kullanıcılar arasında açık anahtarların aşikâr bir şekilde değiş tokuş edilmesinden sonra saldırganın elde ettiği bilgilerden oturum anahtarını hesaplayarak doğru bir kullanıcı rolü yapıp, tekrar eden bir şekilde kaynak erişimi sağlamasıdır. Bizim çalışmamızda, Diffie Hellman yönteminin aksine her adımda karşı taraftan gelen rastgele değerler ile açık anahtarların hesaplanması sürekli bir bağımlılık yaratmakta eski değerler ile kimlik doğrulama yapılamamaktadır.

- Çalınmış Doğrulayıcı Saldırıları

Uygulamada doğrulayıcı değerler yerine gizli değerlerin sürekli bir bağımlılık içinde rastgele şifrelenerek yollanmasından dolayı doğrulayıcı değer açık değildir.

4.4. Performans Karşılaştırmaları

Önerdiğimiz şemanın en güncel verilen çalışmalar ile performans, ağ trafiği, zayıflık ve kullanılan kimlik doğrulama yöntemi açısından karşılaştırması yapılmıştır.

Yapılan karşılaştırmalarda referans verilen çalışmalar güncel ve itibarlı dergilerde yayınlanmış makale veya bildiri çalışmalarıdır.

Bu tez çalışması kapsamında geliştirilen ve uygulanan özgün yöntemin bilimsel katkısının daha iyi gösterilmesi için karşılaştırma yapmak önemlidir, daha fazla nitelik kullanılarak yöntemlerin karşılaştırılması genelde daha sonra bu konu üzerinde çalışma yapacak olanlar için yeni meydan okumalar olarak karşımıza çıkmaktadır.

Tablo 4.1:Performans Karşılaştırmaları.

Özellikler	Bizim Önerimiz	[He vd., 2015]	[Jonsson vd., 2017]	[He vd., 2016]	[Echevarria vd., 2016]
Yöntem	Eliptik Eğri 25519	Eliptik Eğri	RSA	Graf İzomorfikliği	Özet Fonksiyonu
Zayıflık	Yok	Yok	Yok	Çalınmış Doğrulayıcı	Yok
Performans	~18 ms	~30 ms	~64 ms	~45 ms	~10 ms
Ağ Trafiği	~128 bayt	~62 bayt	~256 bayt	~1782 bayt	~208 bayt

5. SONUÇ VE ÖNERİLER

Bu çalışma kapsamında Nesnelerin İnterneti teknolojilerine uygun verimli bir şekilde çalışabilecek sıfır bilgi ispatı tabanlı bir kimlik doğrulama yöntemi önerilmiştir. Önerilen yöntem eliptik eğriler üzerinde verimli hesaplamalar yapılmasını sağlayan algoritmalar ile özgülleştirilmiş ve gerçekçi olması açısından bir DC motorun PWM sinyalleri ile kontrol edildiği bir düzenek üzerinde denenmiştir. Önerilen yöntemden elde edilen bulgular daha önce bu konu başlığı üzerinde yapılmış çalışmalar ile güvenlik zafiyeti, performans, ağ trafiği ve uygulama fizibilitesi gibi özellikler açısından karşılaştırılmıştır. Ayrıca teorik ve uygulama güvenlik analizi de yapılmıştır.

Önerilen yöntem performans, ağ trafiği ve zafiyet özellikleri açısından iyi sonuçlar almıştır. Performans ve ağ trafiği sonuçlarının iyi çıkmasının nedeni eliptik eğri üzerinde tanımlı olan ölçeksel nokta çarpımı ve toplanması işlemlerinin kullanılan Curve25519 eğrisinde daha verimli bir şekilde çalışması ve yapılan mühendislik çalışmasının iyi olmasıdır, fakat gerektirdiği mühendislik çabası gereği uygulama fizibilitesi nispeten azdır.

Diğer yöntemlerde ise RSA tabanlı bir şema kullanılması ve RSA algoritmasının bilinen herhangi bir eliptik eğri üzerinde uygulamasının olmaması performans sorunun oluşmasına sebep olmaktadır.

Özet fonksiyonları kullanan yeni bir yöntem performans ve ağ trafiği açısından çok iyi sonuçlar elde etmiştir.

Graf izomorfikliği kullanan yöntemler performans olarak eliptik eğrilere yakın bir sonuç göstermiştir fakat graf izomorfikliği tabanlı sıfır bilgi ispatı yöntemleri literatürde “çalınmış doğrulayıcı” saldırılarına karşı açıktır ve ağ trafiği bakımından küçük cihazlar için fazla yük oluşturmaktadır [Abdullah et al., 2013].

Bundan sonra yapılacak çalışmalar için bu ve benzeri şemalar için cihazlar arasında uçtan uca simetrik şifreleme özelliği gibi SSL/TLS protokolünde bulunan fonksiyonlar eklenebilir, ayrıca cihazlar şifreleme işlemi yaparken kullandıkları gizli anahtarlarını elde etmek için yapılan yan kanal saldırılarına karşı sisteme elektronik bir koruma mekanizması da eklenmesi faydalı olacaktır.

KAYNAKLAR

- Abdullah H. O., Eftekhari M. (2013), "Cryptanalysis and improvements on some graph-based authentication schemes", *Journal of Discrete Mathematical Sciences and Cryptography*, 16 (4-5), 297-306.
- Alcaide A., Palomar E., Montero-Castillo J., Ribagorda A. (2013), "Anonymous authentication for privacy-preserving IoT target-driven applications", *Computers Security*, 37, 111-123.
- Ansong E. D., Hayfron-Acquah J. B. (2016). "Stealth-Obfuscation Zero Knowledge Proof Authentication Protocol", *American Journal of Information Science and Computer Engineering*, 2 (1), 1-7.
- Aviram N., Schinzel S., Somorovsky J., Heninger N., Dankel M., Steube J., Käsper E. (2016), "DROWN: "Breaking TLS Using SSLv2", In *USENIX Security Symposium* (689-706).
- Banks A., & Gupta R. (2014), "MQTT Version 3.1. 1." OASIS standard, 29
- Beydemir A., Soğukpınar İ. (2017), "Lightweight zero knowledge authentication for Internet of things", In *Computer Science and Engineering (UBMK), 2017 International Conference on* (360-365). IEEE.
- Bos J., Kaihara M., Kleinjung T., Lenstra A. K., Montgomery P. L. (2009), "On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography", (No.EPFL-REPORT-164549).
- Chatzigiannakis I., Pyrgelis A., Spirakis P. G., Stamatiou Y. C. (2011), "Elliptic curve based zero knowledge proofs and their applicability on resource constrained devices", In *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on* (715-720). IEEE.
- Cheu R., Yang P., Lin A., Jaffe A. (2014), "NARWHAL An Implementation of Zero Knowledge Authentication", Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, USA.
- Davis J. (2017). "The Lighter Side of Things: The Inevitable Convergence of the Internet of Things and Cybersecurity", NASA, USA.
- Echevarria J. J., Legarda J., Larrañaga J., Ruiz-de-Garibay J. (2016), "lwAKE: A Lightweight Authenticated Key Exchange for Class 0 Devices", *International Journal of Distributed Sensor Networks*, 12 (5), 6236494.
- Feige U., Fiat, A., Shamir A. (1988), "Zero-knowledge proofs of identity", *Journal of cryptology*, 1 (2), 77-94.

Goldwasser S., Micali S., Rackoff C. (1989), "The knowledge complexity of interactive proof systems", SIAM Journal on computing, 18 (1), 186-208.

Grzonkowski S., Zaremba W., Zaremba M., McDaniel B. (2008), "Extending Web Applications with a Lightweight Zero Knowledge Proof Authentication".

He D., Zeadally S. (2015), "An analysis of rfid authentication schemes for internet of things in healthcare environment using elliptic curve cryptography", IEEE internet of things journal, 2 (1), 72-83.

Jonsson F., Tornkvist M. (2017), "RSA authentication in Internet of Things: Technical limitations and industry expectations" Master of Science Thesis, KTH Royal Institute of Technology.

Kleinjung T., Diem C., Lenstra A. K., Priplata C., Stahlke C. (2017), "Computation of a 768-bit prime field discrete logarithm", In Annual International Conference on the Theory and Applications of Cryptographic Techniques (185-201). Springer, Cham.

Korchagin I., Pilyankevich E. (2015), "Secure Comparator: a ZKP-Based Authentication System", IACR Cryptology ePrint Archive, 2015, 1180.

Marlinspike M. (2009), "More tricks for defeating SSL in practice". Black Hat USA.

Martín-Fernández F., Caballero-Gil P., Caballero-Gil C. (2016), "Authentication based on non-interactive zero-knowledge proofs for the internet of things", Sensors, 16 (1), 75.

Philippe S., Goldston R. J., Glaser A., d'Errico F. (2016), "A physical zero-knowledge object-comparison system for nuclear warhead verification", Nature communications, 7.

Quisquater J. J., Quisquater M., Quisquater M., Quisquater M., Guillou L., Guillou M. A. Guillou S. (1989), "How to explain zero-knowledge protocols to your children", In Conference on the Theory and Application of Cryptology (628-631). Springer, New York, NY.

Roman R., Zhou J., Lopez J. (2013), "On the features and challenges of security and privacy in distributed internet of things", Computer Networks, 57(10), 2266-2279.

Shelby Z., Hartke K., Bormann C. (2014), "The constrained application protocol (CoAP)", IETF.

Web 1, (2014), https://www.owasp.org/index.php/Top_IoT_Vulnerabilities, (Erişim Tarihi: 11/12/2017).

Web 2, (2012), <http://opine.me/blizzards-battle-net-hack/>, (Erişim Tarihi: 11/12/2017).

Wu T. (2002), “Srp-6: Improvements and refinements to the secure remote password protocol”.

Zhang X., Wen M., Lu K., Lei J. (2017), “A privacy-aware data dissemination scheme for smart grid with abnormal data traceability”, *Computer Networks*, 117, 32-41.

ÖZGEÇMİŞ

Alican BEYDEMİR 1991 yılında İstanbul’da doğdu. 2010 yılında başladığı Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümünü 2014 yılında başarıyla tamamlayarak 2015 yılında yüksek lisans eğitimine Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında başladı. 2015 – 2017 aralığında NETAŞ TELEKOMÜNİKASYON A.Ş’de Mühendis ve 2017 itibari ile SIEMENS A.G’de Uzman Mühendis olarak çalışmaktadır.

EKLER

Ek A: Tez Çalışması Kapsamında Yapılan Yayınlar

Beydemir, Aican, and İbrahim Soğukpınar. "Lightweight zero knowledge authentication for Internet of things." Computer Science and Engineering (UBMK), 2017 International Conference on. IEEE, 2017.