TC

ONDOKUZ MAYIS ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

ÇOK DEĞİŞKENLİ POLİNOM SİSTEMLERİNE DAYALI KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA VE İMZALAMA ŞEMALARI

MERYEM SOYSALDI

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

SAMSUN

2018

TEZ ONAYI

Meryem SOYSALDI tarafından hazırlanan "ÇOK DEĞİŞKENLİ POLİNOM SİSTEMLERİNE DAYALI KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA VE İMZALAMA ŞEMALARI" adlı tez çalışması 16/07/2018 tarihinde aşağıdaki jüri tarafından Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda Yüksek Lisans Tezi olarak kabul edilmiştir.

Danışman Doç. Dr. Sedat Akleylek

Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri

Başkan Doç. Dr. Muharrem Tolga Sakallı

Trakya Üniversitesi

Bilgisayar Mühendisliği Anabilim Dalı

Üye Doç. Dr. Sedat Akleylek

Ondokuz Mayıs Üniversitesi

Bilgisayar Mühendisliği Anabilim Dalı

Üye Dr. Öğr. Üyesi Erdem Alkım

Ondokuz Mayıs Üniversitesi

Bilgisayar Mühendisliği Anabilim Dalı

Yukarıdaki sonucu onaylarım. 16/07/2018

Prof. Dr. Bahtiyar ÖZTÜRK

Enstitü Müdürü

ETİK BEYAN

Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

16/07/2018

Meryem SOYSALDI

ÖZET

Yüksek Lisans Tezi

ÇOK DEĞİŞKENLİ POLİNOM SİSTEMLERİNE DAYALI KUANTUM BİLGİSAYARLAR SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA VE İMZALAMA ŞEMALARI

Meryem Soysaldı

Ondokuz Mayıs Üniversitesi

Fen Bilimleri Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Sedat Akleylek

İki taraf arasında haberleşmenin sağlıklı bir şekilde yürütülebilmesi için haberleşen tarafların kimliklerinin doğrulanması gerekmektedir. Bu bakımdan kimlik doğrulama şemaları günlük hayatımızın önemli bir parçası olmuştur. Akıllı kartlarda, uzaktan kumanda sistemlerinde kimlik doğrulama şemaları kullanılmaktadır.

Günümüzde güvenilir olarak nitelendirdiğimiz açık anahtarlı kriptosistemler, klasik bilgisayarların hesaplama gücüyle polinom zamanda çözülemeyen çarpanlarına ayırma, ayrık logaritma problemleri gibi zor problemlere dayanmaktadır. Shor, 1994 yılında çarpanlarına ayırma ve ayrık logaritma problemlerini kuantum bilgisayarlarda polinom zamanda çözen algoritma önermiştir. Bundan dolayı, günümüzde kullanılan RSA, Diffie-Hellman, ECDSA gibi açık anahtarlı kriptosistemler kuantum bilgisayarlar sonrası güvensiz hale gelecektir. Bu da kuantum sonrasında kullanılabilecek güvenilir kriptosistemlere olan ihtiyacı vurgulamaktadır. Çok değişkenli polinomlara dayanan sistemler kuantum sonrasında güvenilir yapılardan ve verimlilik açısından tercih edilenlerden birisidir.

Bu tez çalışmasında, kuantum bilgisayarlarda bile polinom zamanda çözülemeyecek çok değişkenli polinomlara dayanan kimlik doğrulama şemaları ve bunların üzerine inşa edilen imzalama sistemleri üzerine çalışılmıştır. Literatürde yer alan kimlik doğrulama şemalarından farklı, kes-ve-seç mantığına dayanan üç ve beş aşamalı sıfır bilgi paylaşımlı yeni kimlik doğrulama şemaları önerilmiştir. Kimlik doğrulama şemalarının verimliliği üzerine yeni ölçüt tanımı yapılmış ve varolan sistemler karşılaştırılmıştır. Son olarak, önerilen kimlik doğrulama şemasına Fiat-Shamir dönüşümü uygulanarak yeni bir imzalama algoritması oluşturulmuş ve güvenlik analizi detaylandırılmıştır. Önerilen kimlik doğrulama ve imzalama şemasının verimlilik ölçütüne göre önceki çalışmalar ile benzer durumda olduğu gösterilmiştir.

Temmuz 2018, 66 sayfa

Anahtar Kelimeler: Kuantum sonrası kriptografi, çok değişkenli polinom sistemleri, kimlik doğrulama şemaları, sıfır bilgi paylaşımı, elektronik imzalama.

ABSTRACT

Master's Thesis

QUANTUM SECURE NEW IDENTIFICATION AND SIGNATURE SCHEMES BASED ON MULTIVARIATE POLYNOMIALS

Meryem Soysaldı

Ondokuz Mayis University

Graduate School of Sciences

Department of Computer Engineering

Supervisor: Doç. Dr. Sedat Akleylek

The identity of the communicating parties needs to be verified to satisfy secure the communication between the two parties. In this respect, identification schemes have become an important part of our daily life. The identification schemes are used in smart cards, remote control systems.

Traditional public key cryptosystems are based on computationally hard problems in conventional computers such as factorization and discrete logarithm. In 1994, Shor proposed an algorithm to solve the factorization and the discrete logarithm problem in polynomial time by using quantum computers. Therefore, public key cryptosystems such as RSA, Diffie-Hellman, ECDSA widely used today, will become insecure after the invention of quantum computers. This emphasizes the need for secure cryptosystems that can be used in the post-quantum world. Systems based on multivariate polynomials are one of the preferred systems in terms of efficiency and secure under quantum attacks.

In this thesis, identification schemes based on multivariate polynomials, which cannot be solved even in quantum computers, and signature schemes based on those have been studied on. Three and five pass new identification schemes having zero-knowledge property, different from the identification schemes in literature, are proposed by using the cut-and-choose approach. A new metric to measure the efficiency of the identification schemes is defined. Then, a comparison is provided with the previous ones. Finally, a new signature algorithm is constructed by applying the Fiat-Shamir transformation to the proposed identification scheme and the security analysis is detailed. It is shown that the proposed identification and signature scheme is similar to previous studies according to efficiency metric.

July 2018, 66 pages

Keywords: Post-quantum cryptography, multivariate polynomial systems, identification schemes, zero-knowledge, digital signature.

ÖNSÖZ VE TEŞEKKÜR

Akademik hayatıma başladığım günden beri kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösteren, her zaman bana ve sorularıma ayıracak zamanı olan, her türlü yardımı esirgemeyen, kendisinden her anlamda çok şey öğrendiğim, kendisiyle çalışmaktan onur duyduğum, üzerimde çok hakkı olan değerli danışman hocam Doç. Dr. Sedat Akleylek'e sonsuz teşekkürlerimi ve saygılarımı sunarım.

Tez çalışmamı EEEAG-116E279 numaralı proje kapsamında destekleyen TÜBİTAK'a teşekkür ederim.

Çalışmalarım boyunca yardımlarını hiç esirgemeyen, bana destek olan değerli araştırma görevlisi arkadaşlarıma teşekkürü bir borç bilirim.

Bana olan güvenlerini boşa çıkarmayacağım, bu günlere gelmemde büyük emeği olan, hayatımın her anında maddi ve manevi destekleriyle beni yalnız bırakmayan aileme sonsuz teşekkür ederim.

Temmuz 2018, Samsun

Meryem SOYSALDI

İÇİNDEKİLER DİZİNİ

SİMGELER VE KISALTMALAR

SİMGELER

$\mathbb{F}_q$	Elemanları {0,…,q-1} arasında olan q elemanlı sonlu cisim
$\mathbb{F}_q^n$	Elemanları {0,…,q-1} arasında olan q elemanlı sonlu cisimde n boyutlu vektör uzayı
$\boldsymbol{\lambda}$	Güvenlik parametresi
$\boldsymbol{n}$	Değişken sayısı
$\boldsymbol{m}$	Polinomların sayısı
F	Polinom sistemi
$\boldsymbol{x} \in_R \mathbb{F}$	Sonlu cisimden rastgele seçilen değer
G	Polar form
k	Güvenlik seviyesi
Com	Taahhüt fonksiyonu (Commitment)
Rsp	İspatlayıcının cevapları (Response)
hc	Özet değeri
$\boldsymbol{\sigma}$	İmza değeri
H	Özet fonksiyonu
d	Polinom derecesi
Ch	Meydan okuma değeri
S	Simülatör
C	Sahtekar İspatlayıcı (Cheating Prover)

KISALTMALAR

AES	Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)
BQP	Sınırlı-hata, Kuantum, Polinom-zamanı (Bounded-error Quantum Polynomial time)
Com	Taahhüt Fonksiyonu (Commitment Function)
CT	Hesaplama Zamanı (Computation Time)
DES	Veri Şifreleme Standardı (Data Encryption Standard)
DSA	Elektronik İmzalama Algoritması (Digital Signature Algorithm)
DSS	Elektronik İmzalama Şeması (Digital Signature Scheme)

ECDSA Eliptik Eğri Elektronik İmzalama Algoritması (Eliptic Curve Digital Signature Algorithm)

EM Verimlilik Ölçütü (Efficiency Metric)

IBM Uluslararası İş Makineleri (International Business Machines)

IDS Kimlik Doğrulama Şeması (Identification Scheme)

IP Taklit Etme Olasılığı (Impersonation Probability)

MQ İkinci Dereceden Çok Değişkenli Polinom Sistemi (Multivariate quadratic polynomial system)

MQDSS İkinci Dereceden Çok Değişkenli Elektronik İmzalama Şeması (Multivariate Quadratic Digital Signature Scheme)

MC Üçüncü Dereceden Çok Değişkenli Polinom Sistemi (Multivariate Cubic Polynomial System)

NIST Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology)

NP Polinom Zamanda Çözülemeyen (Non-polynomial-time)

PT Polinom Zamanda Çözülebilen (Polynomial-time)

P İspatlayıcı (Prover)

DT Parçalama Tekniği (Dividing Technique)

RSA Rivest–Shamir–Adleman

Rsp Cevap (Response)

SHA-1 Güvenli Özet Algoritması-1 (Secure Hash Algorithm-1)

SHA-2 Güvenli Özet Algoritması-2 (Secure Hash Algorithm-2)

SHA-3 Güvenli Özet Algoritması-3 (Secure Hash Algorithm-3)

V Doğrulayıcı (Verifier)

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Kriptografinin amacı matematiksel teknikler kullanarak gizlilik, bütünlük, inkar edememe ve kimlik doğrulama gibi bilgi güvenliği kavramlarını sağlayarak haberleşme sırasında bilgiyi üçüncü kişilere karşı korumak olarak özetlenebilir (Çimen vd, 2012). Bilgi güvenliği kavramlarından gizlilik ile haberleşen taraflar arasındaki bilgi, anlaşılamayacak forma getirilerek yetkisiz kişilerin bilgiye erişmeleri engellenmektedir. Bütünlük kavramı ile bilginin iletilirken yetkisiz kişiler tarafından değiştirilmesinin önüne geçilmektedir. İnkar edememe, yapılan bir işlemin aksinin ispatlanamaması üzerine bir kavramdır. Son olarak kimlik doğrulama kavramı ile haberleşen tarafların birbirlerinin kimliklerinden emin olması sağlanarak kişinin başka birisinin kimliğini taklit etmesi engellenmektedir. Bu nedenle bilginin güvenliği ve bütünlüğü ile ilgili bütün önlemleri alan bir sistemde kimlik doğrulamanın düzgün yapılamaması iletişimi en başından sekteye uğratmaktadır.

Kriptosistem, haberleşmede bilgi güvenliği kavramlarını sağlamak amacıyla haberleşen tarafların aralarında bir anahtar belirlemesi, bu anahtar kullanılarak mesajın üçüncü kişiler tarafından anlaşılmasının engellenmesi için şifrelenerek gönderilmesi ve karşı tarafta şifreli metinden mesajın elde edilmesi gibi işlemlerin tamamını kapsamaktadır (Menezes vd, 1996). Yüzyıllardır bilgiyi saklamak ve güvenli bir şekilde iletişime geçebilmek amacıyla çeşitli kriptosistemler geliştirilmiştir. Bu sistemleri klasik ve modern kriptosistemler olarak ikiye ayırmak mümkündür.

İlk klasik kriptosistemlerden olan Sezar şifresi, Julius Caesar tarafından geliştirilen kaydırma temeline dayanan ilkel bir şifreleme yöntemidir. Yer değiştirme sistemlerinin ilk örneği olan bu şifreleme yönteminde şifreleme işlemi harf harf yapılırken şifrelenecek harf anahtar değerine göre kendisinden sonra gelen harf ile değiştirilerek şifreli metin elde edilmektedir (Menezes vd, 1996). Sonraki yıllarda istatistiksel analizlerle Sezar şifresinin kolay kırıldığı anlaşılmış ve Blaise de Vigenere tarafından Vigenere şifresi geliştirilmiştir. Vigenere şifresi de temelinde yer değiştirme mantığına dayanırken oluşturulan bir tablo ile şifreli harf elde edilmektedir (Kahn,

1996). Şifreleme adımında her harf farklı bir harfe karşılık geleceğinden farklı şifreli metinler elde edilmektedir. Bu sebepten çoklu alfabeli şifreleme olarak adlandırılmaktadır. Bu şifreleme yöntemi uzun yıllar kırılmadan kullanılmıştır. İngiliz matematikçi Charles Babbage'nın fark makinesini icadı ile hesaplama gücü artınca uzun yıllar kırılmadan kullanılan Vigenere şifresi kırılmıştır (Kahn, 1996). Bundan sonraki dönemde güvenliği matematiksel problemin çözümüne dayanan şifreleme yöntemleri oluşturulmuştur.

Lester J. Hill tarafından oluşturulan Hill şifresi matris vektör çarpımını kullanan bir şifreleme yöntemidir. Özellikle matrisler ve modüler aritmetik kullanılarak geliştirilmiş bu yöntem düz metni bloklara ayırarak şifreleme yapmaktadır (Kahn, 1996). Gilbert Vernam tarafından geliştirilen Vernam şifreleme, şifrelenecek açık metnin aynı uzunlukta rastgele olarak üretilen anahtar kullanılarak karıştırılması temeline dayanmaktadır (Menezes vd, 1996). Vernam şifresinin güvenliği anahtarın rastgele üretilmesine bağlıdır. Kullanılan anahtar rastgele üretilirse ve üretilen anahtar sadece bir kere kullanılırsa bu sistem mükemmel gizliliği sağlamaktadır.

Modern kriptosistemler ise kullanılan anahtar çeşidine göre ikiye ayrılmaktadır:

Simetrik (Gizli Anahtarlı) Kriptosistemler: Sadece bir gizli anahtar kullanılarak hem şifreleme hem de şifre çözme işlemi yapılır. Bu sebepten, haberleşecek taraflar haberleşme başlamadan önce ortak bir gizli anahtar belirlemelidirler. 1977 yılında standartlaştırılan Veri Şifreleme Standardı DES bir blok şifreleme algoritmasıdır (FIPS 46-3, 1999). Bunun temelinde şifrelenecek açık metin bloklara ayrılmakta, her bir blok yayılma ve karıştırma özellikleri kullanılarak birbirinden bağımsız bir şekilde şifrelenmektedir (Menezes vd, 1996). Şifre çözmek için ise bloklara aynı işlemler uygulanmaktadır. Standart şifreleme sistemi olan DES'in güvenlik açıklarının ortaya çıkması, anahtar boyutunun küçük olması, oldukça yavaş çalışması gibi nedenlerden dolayı kullanışlılığını yitirmesiyle DES'in yerine daha güvenilir standart bir şifreleme algoritması bulma ihtiyacı ortaya çıkmıştır. 1997 yılında Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) düzenlediği bir yarışma ile DES'in yerine geçecek yeni bir blok şifreleme algoritması için çağrıda bulunmuştur. Yarışma sonucunda Rijndael algoritması Gelişmiş Şifreleme Standardı AES olarak kabul edilmiştir (FIPS 197, 2001). Akıllı kartlar gibi sistem kaynakları kısıtlı olan cihazlarda verimli çalışabilecek blok şifrelerin

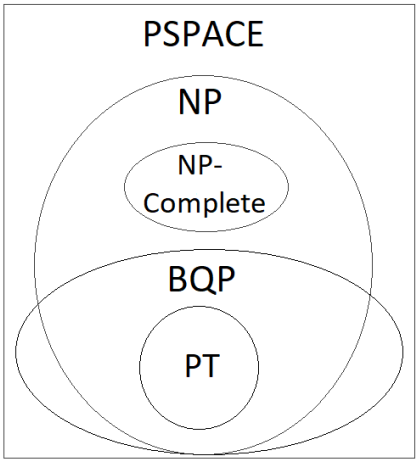
literatürde önerildiği görülmektedir. Bunlara örnek olarak Present, Prince, Pride ve KATAN/KTANTAN verilebilir (Hatzivasilis vd, 2018). Aynı anahtarın hem alıcıda hem de göndericide olması gerektiğinden simetrik kriptosistemlerdeki problemlerden biri anahtar paylaşımıdır.

Asimetrik (Açık Anahtarlı) Kriptosistemler: Simetrik kriptosistemlerdeki gizli anahtarın güvenli bir şekilde dağıtılması problemine çözüm olan Diffie-Hellman anahtar değişim algoritması, asimetrik kriptosistemlerin ortaya çıkmasını sağlamıştır (Diffie and Hellman, 1976). Bu algoritma ile haberleşen taraflar kendilerinden rastgele veri üretir ve bunları kullanarak her iki taraf ortak bir anahtar elde eder. Diffie-Hellman anahtar değişimi algoritmasının güvenilirliği ayrık logaritma probleminin çözümünün zorluğuna dayanmaktadır. Asimetrik şifreleme sistemlerinin ilk örneği olan RSA kriptosistemi, 1977 yılında Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından geliştirilmiştir (Rivest vd, 1978). Bu şifreleme sistemiyle beraber, haberleşen taraflar iki tane anahtara sahip olmaktadır. Açık anahtar herkes tarafından bilinen anahtar iken herkesin kendine ait bir gizli anahtarı daha vardır. Bu kriptosistemlerde mesajı gönderen, göndereceği kişinin açık anahtarını kullanarak şifreli metni oluşturmaktadır. Oluşturulan şifreli metin sadece ilgili alıcının gizli anahtarı ile çözülebilmektedir.

Simetrik ve asimetrik kriptosistemlerden farklı olarak anahtarsız kriptosistemlerde mevcuttur. Kriptografik özet (hash) fonksiyonları, herhangi bir uzunluktaki mesajı alarak sabit uzunlukta bir çıktı üreten anahtarsız sistemler olarak nitelendirilmektedir. NIST tarafından SHA-1, SHA-2 ve SHA-3 özet fonksiyonları ailesi güvenilir özet fonksiyonları aileleri olarak standartlaştırılmıştır (Dang, 2015; Dworkin, 2015). Belirli bir mesaj özetine karşılık gelen mesajı ve aynı mesaj özetine karşılık gelen iki farklı mesaj değerini bulmak hesaplamalı olarak zor olduğundan bu fonksiyonlar güvenilir özet fonksiyonları olarak adlandırılmıştır (Dang, 2015). Özet fonksiyonları mesajların doğrulaması, parolaların saklanması, verilerin bütünlüğünü sağlayarak değiştirildiği zaman anlaşılmasını sağlamak amacıyla kullanılmaktadır.

Literatürde tamsayılar, eliptik eğriler gibi farklı gruplar üzerinde çarpanlarına ayırma veya ayrık logaritma probleminin çözümünün zorluğuna dayanan birçok sistem bulunmaktadır. Klasik bilgisayarlarda çarpanlarına ayırma ve ayrık logaritma gibi problemleri çözecek polinom zamanda çalışan bir algoritma olmadığından bu problemler polinom zamanda çözülemeyen problemler (NP) sınıfındadır. Fakat Shor

önerdiği algoritma ile kuantum bilgisayarlarda ayrık logaritma ve çarpanlarına ayırma problemlerinin polinom zamanda çözülebileceğini ortaya koymuştur (Shor, 1994). Bu sebepten, NP sınıfında olan birçok problem kuantum sonrasında polinom zamanda çözülebilen problemler (PT) sınıfına indirgenmektedir. Kuantum sonrasında NP sınıfından PT sınıfına indirgenen bu problemler, kuantum bilgisayarlar tarafından polinom zamanda çözülebilen problemler (BQP) sınıfını oluşturmaktadır. Şekil 1.1.'de kuantum bilgisayarlar ile ortaya çıkan yeni problem sınıflandırması verilmiştir.

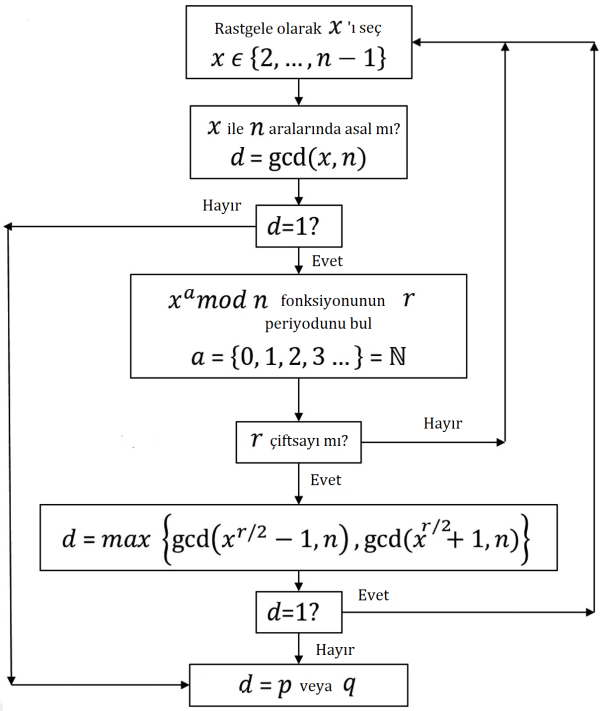


Şekil 1.1. Problem sınıflarının gösterimi

Shor'un Algoritması: Shor, klasik bilgisayarda polinom zamanda çözülemeyen çarpanlarına ayırma ve ayrık logaritma problemleri için kuantum bilgisayarlarda polinom zamanda çözülebilecek bir algoritma önermiştir (Shor, 1994). Çarpanlarına ayırma problemini çözen algoritma için p ve q iki asal sayı olmak üzere $n = p \cdot q$ sayısı verilsin. $a < n$ ve x ile n aralarında asal olmak üzere $F(a) = x^a \cdot mod(n)$ periyodu r olan periyodik bir fonksiyon olsun. Algoritmanın akış diyagramı Şekil 1.2.'de verilmektedir.

Örnek: Shor'un algoritmasını kullanarak $n = 15$ sayısını çarpanlarına ayıralım.

- 15 ile aralarında asal olan bir $x \in \{2, \cdots, 14\}$ sayısını seçelim. Seçtiğimiz sayı $x = 7$ olsun.
- $F(a) = 7^a mod(15)$ fonksiyonunun periyodu $r = 4$'tür.
- r çift sayı olduğundan $d = max\{gcd(7^{4/2} - 1, 15), gcd(7^{4/2} + 1, 15)\}$ hesaplanırsa ilk çarpan olarak 5, ikinci çarpan olarak 3 elde edilir.



Şekil 1.2. Shor algoritmasının akış diyagramı (Buchanan and Woodward, 2017)

Shor'un önerdiği bu algoritma ile günümüzde klasik bilgisayarlarda güvenilir bir şekilde kullanılan RSA, DSA ve ECDSA gibi şifreleme algoritmaları kuantum bilgisayarlarda kırılacak ve güvensiz hale gelecektir (Bernstein vd, 2009).

Klasik bilgisayarlar, 0 ya da 1 değerlerini alabilen bitlerle işlem yaparken kuantum bilgisayarlar aynı anda hem 0 hem de 1 değerini alabilen süperpozisyon özelliğine sahip kubitlerle işlem yapmaktadırlar (Nielsen and Chuang, 2000). Kubitler süperpozisyon özelliği sayesinde tüm değerleri alabildiği için kuantum bilgisayarlar klasik bilgisayarlara kıyasla üstün işlem yapma kapasitesine sahiptir.

Kuantum bilgisayar fikri 1982 yılında Amerikalı fizikçi Richard Feymann tarafından ortaya atılmıştır. Feymann klasik fizik kanunları yerine kuantum mekaniği kanunlarına dayanan kuantum bilgisayarlar oluşturmayı önermiştir (Feymann, 1982). Bu öneriden sonra kuantum bilgisayarların oluşturulmasına yönelik çalışmalar başlamıştır. Shor'un önerdiği algoritmadan yola çıkan Isaac ve arkadaşları 1998 yılında 2-kubitlik kuantum bilgisayarı oluşturmayı başarmışlardır (Chuang vd, 1998). Isaac ve arkadaşları IBM'de çalışmalarına devam ederek 2001 yılında 5-kubitlik bir kuantum bilgisayar ile 15 sayısını çarpanlarına ayırmayı başarmışlardır (Vandersypen vd, 2001). IBM'in bu başarısından sonra Google, Intel, Microsoft gibi büyük firmalar arasında kuantum bilgisayar oluşturma konusunda rekabet başlamıştır. IBM,

Kasım 2017'de 50-kubitlik bir kuantum bilgisayar geliştirdiklerini ve 20-kubitlik bir kuantum bilgisayarı da bulut servis olarak hizmete açtıklarını duyurmuştur (Johnston, 2017). Son olarak Mart 2018'de Google, 72-kubitlik bir kuantum bilgisayar çipi geliştirdiğini ilan etmiştir (Kelly, 2018). Fazla kubite sahip bilgisayarların oluşturulması güncel bir araştırma konusudur. Burada üzerinde durulması gereken husus, kuantum bilgisayarlar kullanılmaya başlandığında günümüzde güvenilir olarak nitelendirdiğimiz asimetrik kriptosistemlerin güvensiz hale gelecek olmasıdır. Bu da bilgi güvenliği kavramları açısından bir tehdit oluşturmaktadır. Bu sebepten, kuantum sonrasında kullanılabilecek güvenilir sistemlere ihtiyaç vardır. NIST bu konuya dikkat çekerek açık anahtarlı şifreleme için kuantum sonrasında kullanılabilecek algoritmaların oluşturulması konusunda çağrı yapmıştır (NIST, 2017).

NIST'ın çağrısının da etkisiyle araştırmacılar kuantum bilgisayarlara karşı güvenilir olduğu bilinen zor problemleri kullanan kriptosistem tasarımına yönelmişlerdir. Kafes, çok değişkenli polinomlar, kod, özet fonksiyonları ve izojeni tabanlı kriptosistemleri kuantum bilgisayarlarda çözecek bir kuantum algoritma henüz önerilmemiştir (Bernstein vd, 2009; Chen vd, 2016a). Dolayısıyla bu zor problemlere dayanan sistemler kuantum sonrası için oluşturulmaya başlanmıştır.

Bu tez çalışmasında, sonlu cisimler üzerinde çok değişkenli polinomlara dayanan sistemler üzerine çalışılmıştır. Çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemaları önerilmiştir. Önerilen kimlik doğrulama şemaları kullanılarak imzalama şeması elde edilmiştir.

1.1. Kuantum Sonrası Güvenilir Kriptografik Sistemlerin Sınıflandırılması

Çizelge 1.1.'de kuantum sonrasında güvenilir olduğu bilinen kriptosistemler, dayandıkları zor problemler ve uygulama alanları verilmiştir. Bu kriptosistemlerin kuantum bilgisayarlara karşı güvenilir olarak kabul edilmesinin sebebi bu sistemlerin dayandıkları zor problemlerdir. Kuantum bilgisayarlarda bile polinom zamanda çözülemeyen bu problemlere dayanan sistemler kuantum dirençli olarak nitelendirilmektedir. Çizelge 1.1.'den kriptografik sistemlerin şifreleme, anahtar değişimi, elektronik imzalama ve kimlik doğrulama gibi amaçlar doğrultusunda kullanıldığı görülmektedir. Kuantum bilgisayarlar ile birlikte güvensiz hale gelecek

Çizelge 1.1. Kuantum sonrası güvenilir sistemlerin sınıflandırılması

Sistem	Dayandığı Zor Problem	Uygulama Alanları
Özet Tabanlı	- Kriptografik özet fonksiyonlarının çakışmaya dayanıklı olması - Tek yönlü hesaplama yapılabilmesi	- İmzalama
Kod Tabanlı	- Kodlama teorisi - Goppa kodları	- Açık anahtarlı şifreleme - Kimlik doğrulama - İmzalama
Kafes Tabanlı	- En kısa vektör problemi - En yakın vektör problemi gibi kafes problemleri	- Açık anahtarlı şifreleme - Anahtar değişimi - Kimlik doğrulama - İmzalama
İzojeni Tabanlı	- Eliptik eğrilerin izojenik graflarında yol bulmanın zorluğu	- Anahtar değişimi - Kimlik doğrulama - İmzalama
Çok Değişkenli Polinomlar Tabanlı	- Sonlu cisimlerde d. dereceden çok değişkenli polinom sistemlerinin çözümünün zor olması	- Kimlik doğrulama - İmzalama

bütün sistemler için güvenilir (kuantum dirençli) kriptosistemlerin oluşturulma çalışmaları devam etmektedir.

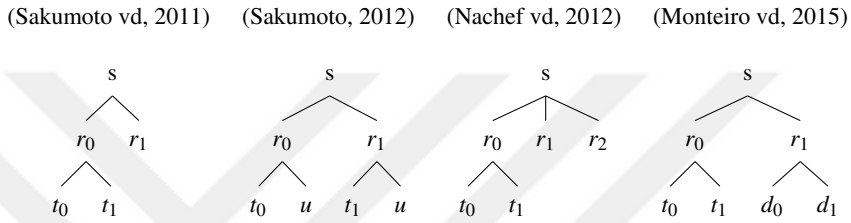
Kimlik doğrulama şemaları haberleşen tarafların birbirlerinin kimliklerinden emin olmalarını sağlayan kriptografik sistemlerdir. İmzalama şemaları ise kağıt üstündeki imzanın dezavantajlarını ortadan kaldırarak bütünlük, inkar edememe, kimlik doğrulama, veri bütünlüğü ve yetkilendirme gibi kavramları sağlayan elektronik ortamda imzalama işlemleri için kullanılan sistemlerdir. Kuantum sonrasında güvenli olabilecek kafes tabanlı, kod tabanlı, izojeni tabanlı ve çok değişkenli polinomlar tabanlı kimlik doğrulama ve imzalama şemaları önerilmiştir (Silva vd, 2011; Stern, 1993; De Feo vd, 2014; Sakumoto vd, 2011; Chen vd, 2016b). Bu tez kapsamında kuantum sonrasında güvenilir kimlik doğrulama ve imzalama şemaları üzerine çalışılmıştır. Çok değişkenli polinomlara dayanan kimlik doğrulama ve imzalama şemalarına odaklanılmıştır.

Bu tez çalışmasında çok değişkenli polinomlara dayanan üç ve beş aşamalı sıfır bilgi paylaşımlı üç kimlik doğrulama şeması önerilmiştir. Önerilen kimlik

doğrulama şemaları önceki şemalar ile çeşitli değerlendirme ölçütlerine göre karşılaştırılmıştır. Kimlik doğrulama şemalarından imzalama şemalarına geçiş yapılarak yeni bir imzalama şeması önerilmiştir. Önerilen imzalama şeması için karşılaştırma yapılmıştır.

1.2. Önceki Çalışmalar

Literatürdeki çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemalarında kullanılan gizli anahtarı parçalama teknikleri Şekil 1.3.'te verilmiştir. Yapılan çalışmalar bu tekniklere göre anlatılmaktadır.



Şekil 1.3. Çok değişkenli polinomlara dayanan kimlik doğrulama şemalarının parçalama teknikleri

Çok değişkenli polinomlara dayanan kimlik doğrulama şemalarıyla ilgili ilk çalışma 2011 yılında Sakumoto vd. tarafından yapılmıştır. Sakumoto vd (2011) çalışmasında sonlu cisimler üzerinde ikinci dereceden çok değişkenli polinom sistemine dayanan üç ve beş aşamalı sıfır bilgi paylaşımlı kimlik doğrulama şeması önerilmiştir. Sakumoto vd (2011) çalışmasının temel katkıları; ikinci dereceden çok değişkenli polinomların polar formlarının ikili doğrusallık özelliğini ve gizli anahtarı önce iki parçaya daha sonra bu parçalardan birini tekrar iki alt parçaya ayırıp üç parçalı yeni bir gizli anahtar parçalama tekniği ortaya koymasıdır. Üç aşamalı kimlik doğrulama şemasının beş aşamalı şemadan tek farkı aşama sayısıdır. Beş aşamalı kimlik doğrulama şemasında gizli anahtar parçaları doğrulayıcıdan gelen rastgele bir sonlu cisim elemanına göre parçalanarak daha etkileşimli bir şema oluşturulmuştur. Sakumoto vd (2011) çalışması, sonlu cisimler üzerinde çok değişkenli polinomlara dayanan ilk çalışma olması bakımından önem taşımaktadır. Kimlik doğrulama şemaları imzalama şemalarının temelini oluşturduğundan çalışma ayrı bir yere sahiptir. Bu öncü çalışmadan sonra hem kimlik doğrulama şemaları hem de imzalama şemaları üzerinde çalışılmaya başlanmıştır.

Yapılan başka bir çalışmada derecesi ikiden büyük olan çok değişkenli polinomlara dayanan kimlik doğrulama şemalarının oluşturulup oluşturulamayacağı üzerinde durulmuştur. Bunun yanında, üçüncü dereceden çok değişkenli polinomlara dayanan üç ve beş aşamalı yeni kimlik doğrulama şeması önerilmiştir (Sakumoto, 2012). Üçüncü dereceden çok değişkenli polinomlar için yeni bir polar form tanımlanmıştır. Oluşturulan polar formun ikili doğrusallık özelliği kullanılarak gizli anahtar önce iki parçaya sonra birer parçaları aynı olmak şartıyla her bir parça iki parçaya ayırarak dört parçalı bir gizli anahtar oluşturulmuştur. Sakumoto (2012) çalışmasında üç aşamalı kimlik doğrulama şemasının o kadar verimli olmadığı fakat beş aşamalı şemanın oldukça verimli olduğu ifade edilmiştir. Bunun yanı sıra, oluşturulan beş aşamalı şema ile kullanılan açık ve gizli anahtar boyutunun önceki şemalara kıyasla oldukça küçültüldüğü belirtilmiştir. Sakumoto (2012) çalışmasında derecesi dörtten büyük olan çok değişkenli polinom sistemlerine dayanan verimli yapıların oluşturulup oluşturulamayacağı açık problem olarak nitelendirilmiştir.

Nachef vd (2012) çalışmasında açık problem için çözüm önerisi getirilmiştir. Yapılan çalışmada herhangi bir dereceden çok değişkenli polinom sistemleri kullanıldığında kimlik doğrulama şemasının oluşturulması için genel bir yapı önerilmiştir. d. dereceden çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemaları için yeni bir gizli anahtarı parçalama tekniği oluşturulmuştur. Şemada kullanılan gizli anahtar başlangıçta d parçaya ayrılmıştır. Parçalama işleminin devamında birinci parça iki parçaya ayrılarak $d+1$ parçalanışa sahip bir gizli anahtar elde edilmiştir. d. dereceden çok değişkenli polinomlar kullanıldığında d eleman için doğrusallık özelliğine sahip bir polar formun kullanılması gerektiği vurgulanarak genel bir polar form tanımlanmıştır. Yapılan genelleştirme ve polar form yapısının kullanılabilir olduğunu göstermek amacıyla $d = 3$ için üçüncü dereceden çok değişkenli polinom sistemlerine dayanan üç aşamalı sıfır bilgi paylaşımlı bir kimlik doğrulama şeması oluşturulmuştur. Parçalanış fikrine göre üçüncü dereceden polinomlar kullanıldığından gizli anahtar önce üç parçaya ayrılmıştır. İkinci parçalamada bu parçalardan birincisi iki parçaya ayrılarak yeni bir gösterim elde edilmiştir. Bu durumda gizli anahtar toplamda dört parçalanışa sahip olmaktadır. Genel polar form yapısından $d = 3$ için üçlü doğrusal polar form elde edilerek üç aşamalı bir kimlik doğrulama şeması oluşturulmuştur.

Hornschuch (2012) tez çalışmasında Sakumoto vd (2011) çalışmasında önerilen üç ve beş aşamalı kimlik doğrulama şemaları detaylı bir şekilde ele alınmıştır. Farklı parametrelere göre şemaların uygulaması geliştirilmiştir. Şemaların verimli olarak çalıştıkları parametreler önerilmiştir. Sakumoto vd (2011) çalışmasındaki beş aşamalı kimlik doğrulama şeması baz alınarak elde edilen imzalama şeması için verimlilik analizi yapılmıştır. İmzalama şemasının verimli bir şekilde uygulanabilmesi için olası parametreler verilmiştir.

2015 yılında Monterio vd. tarafından yapılan çalışmada Sakumoto vd (2011) çalışmasındaki parçalanış yapısı ve polar form aynen kabul edilerek parçalanmamış parça da iki parçaya ayrılarak dört parçalı bir gizli anahtar elde edilmiştir. Oluşturulan gizli anahtarı kullanan ikinci dereceden çok değişkenli polinomlara dayanan sıfır bilgi paylaşımlı üç aşamalı kimlik doğrulama şeması önerilmiştir. Bu şema ile taklit etme olasılığı düşürülmüştür.

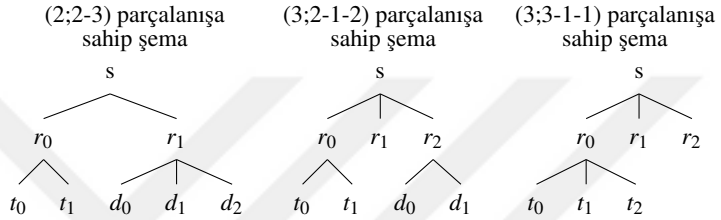
Chen vd (2016b) çalışmasında Sakumoto vd (2011) çalışmasında verilen beş aşamalı kimlik doğrulama şeması Fiat-Shamir dönüşümü kullanılarak MQDSS isminde yeni bir imzalama şeması önerilmiştir. Şemanın uygulanabilmesi için parametrelerin seçimi yapıldıktan sonra detaylı bir şekilde güvenlik analizi yapılmıştır. İmzalama şemasının performansı değerlendirilmiştir. Chen vd (2016b) çalışmasındaki imzalama şeması, NIST'ın kuantum dirençli kriptografik algoritmaların oluşturularak yeni açık anahtarlı kriptostandartların oluşturulması için yaptığı çağrıya yanıt olarak MQDSS ismiyle gönderilmiştir (NIST, 2018).

1.3. Motivasyon ve Katkı

Çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemaları incelendiğinde, farklı parçalanış yöntemlerinde verimlilik açısından farklı sonuçların elde edildiği görülmektedir. Aynı zamanda polar formun ikili doğrusal veya d doğrusal olduğu durumlarda da bu parçalanışlar verimlilik açısından ya da yeni sistem üretme açısından odak noktası olmuştur. Gizli anahtarların fazla parçalanışa sahip olması durumunda verimlilik açısından nasıl sistemler oluşturulması gerektiği açık problem olarak düşünülmektedir.

Gizli anahtarın parça sayısının çok fazla arttırılmasının ilk bakışta sistemin yükünü arttıracağı düşünülmektedir. Ancak farklı kriterlere göre değerlendirildiğinde verimli yapıların oluşturulup oluşturulamayacağı araştırma konusudur. Ayrıca kimlik doğrulama şemalarını değerlendirmek için verimlilik ölçütleri nelerdir? ve yeni verimlilik ölçütleri oluşturulabilir mi? gibi problemler bulunmaktadır.

Bu alandaki çalışmalar, kimlik doğrulama şemaları baz alınarak imzalama şemalarının oluşturulabildiğini göstermektedir. Ancak oluşturulan kimlik doğrulama şemalarından daha verimli yeni imzalama şemalarının nasıl oluşturulacağı başka bir araştırma konusudur.



Şekil 1.4. Önerilen kimlik doğrulama şemalarının parçalama teknikleri

Şekil 1.4.'te bu tez çalışmasında önerilen kimlik doğrulama şemalarının parçalama teknikleri verilmiştir. Bu teknikler kullanılarak ikinci ve üçüncü dereceden çok değişkenli polinomlara dayanan kimlik doğrulama şemaları önerilmiştir. Yeni önerilen kimlik doğrulama şemaları ile literatürdeki şemalar çeşitli kriterlere göre karşılaştırılmıştır. Ayrıca şemaları değerlendirmek için yeni bir verimlilik ölçütü tanımlanmıştır. Önerilen şemalar Akleylek ve Soysaldı (2018a) ve Akleylek ve Soysaldı (2018b) çalışmalarında yer almaktadır.

Derecesi üçten büyük olan polinomlar kullanılarak verimli yapıların oluşturulup oluşturulamayacağı konusu açık problem olarak verilmektedir. Bu açık probleme kısmi bir çözüm önerilmiştir. Derecesi üçten büyük polinom sistemleri için genel bir polar form tanımlanmıştır. Önerilen bu form ile kullanılan dereceye göre polar formun kolayca elde edilmesi amaçlanmıştır. Bu çözüm önerisi Akleylek ve Soysaldı (2017) çalışmasında yayınlanmıştır.

Önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şeması baz alınarak yeni bir imzalama şeması elde edilmiştir. Önerilen yeni imzalama şeması diğer imzalama şemaları ile anahtar boyutlarına ve imza boyutuna göre karşılaştırılmıştır. Elde

edilen sonuçlar ile imzalama şeması Akleylek ve Soysaldı (2018a) çalışmasında yer almaktadır.

1.4. Organizasyon

Bölüm 2'de tez çalışmasının anlaşılabilmesi için gerekli olan tanımlara yer verilmiştir. Çok değişkenli polinom sistemlerinin dayandığı çok değişkenli zor problemden kısaca bahsedilmiştir. Kimlik doğrulama şemasının tanımı yapılarak şemanın sağlaması gereken özelliklere değinilmiştir. Kimlik doğrulama şemalarından imzalama şemalarına geçiş için kullanılan Fiat-Shamir dönüşümü tanımlanmıştır. Ayrıca klasik bir imzalama şemasının tanımı ve işleyişi verilmiştir.

Bölüm 3'te çok değişkenli polinom sistemlerine dayanan yeni kimlik doğrulama şemaları önerilmiştir. Önerilen her şemanın doğrulanması yapılarak şemanın işleyişi anlatılmıştır. Ayrıca şemaların sağlaması gereken özellikler teoremlerle ifade edilerek ispat edilmiştir. Kimlik doğrulama şemalarını karşılaştırmak için yeni bir verimlilik ölçütü tanımlanmıştır. Tanımlanan yeni ölçüt ve diğer kriterlere göre kimlik doğrulama şemaları karşılaştırılmıştır.

Bölüm 4'te önerilen kimlik doğrulama şemalarından bir tanesi baz alınarak yeni imzalama şeması elde edilmiştir. Oluşturulan imzalama şemasının aşamaları detaylı bir şekilde ele alınmıştır. Yeni imzalama şeması için güvenlik analizi yapılmıştır. Ayrıca önceki imzalama şemaları ile yeni imzalama şeması açık, gizli anahtar ve imza boyutu açısından karşılaştırılmıştır.

Bölüm 5'te sonuçlar ve gelecek çalışmalara yer verilmiştir.

2. MATEMATİKSEL ALTYAPI

Bu bölümde sonlu cisimler üzerinde çok değişkenli polinomlara dayanan kimlik doğrulama şemalarını anlayabilmek için gerekli tanımlara yer verilmiştir. Kimlik doğrulama şemalarından imzalama şemalarına geçiş yapılacağından imzalama şemaları da tanımlanmıştır. Tanım 2.1.'de sonlu cisim tanımı verilmektedir.

Tanım 2.1 (Sonlu Cisim): *Sonlu sayıda elemanı olan cisim sonlu cisim olarak adlandırılmaktadır (Lidl ve Niederreiter, 1994). $\mathbb{F}$, sonlu sayıda elemanı olan sonlu bir cismi gösterirken; q, asal sayı veya asal sayının kuvveti olmak üzere q elemanlı bir sonlu cisim $\mathbb{F}_q$ ile gösterilmiştir. $\mathbb{F}_q^n$ ise elemanları 0 ile $q-1$ arasında olan q elemanlı sonlu cisimde n boyutlu vektör uzayını temsil etmektedir.*

Kuantum sonrası kriptografide kullanılan çok değişkenli polinom sistemleri sonlu cisimler üzerine tanımlanmıştır. Tanım 2.2.'de çok değişkenli polinom sistemleri ele alınmaktadır.

Tanım 2.2 (Çok Değişkenli Polinom Sistemi): *$\mathbb{F}_q^n$ sonlu cisminde n değişkenli d. dereceden m tane polinomdan oluşan F çok değişkenli polinom sistemi, ($f_{i\ldots j}^{(k)}$, $f_i^{(k)}$ ve $f_0^{(k)}$, $1 \leq k \leq m$) olmak üzere Eşitlik (2.1)'deki gibi tanımlanmaktadır (Bernstein, 2009).*

$$
\begin{aligned}
f^{(1)}(x_1,\ldots,x_n) &= \sum_i^n \cdots \sum_j^n f_{i\cdots j}^{(1)} \cdot \overbrace{x_i \cdot \ldots \cdot x_j}^{d} + \ldots + \sum_{i=1}^n f_i^{(1)} \cdot x_i + f_0^{(1)} \\
f^{(2)}(x_1,\ldots,x_n) &= \sum_i^n \cdots \sum_j^n f_{i\cdots j}^{(2)} \cdot \overbrace{x_i \cdot \ldots \cdot x_j}^{d} + \ldots + \sum_{i=1}^n f_i^{(2)} \cdot x_i + f_0^{(2)} \\
&\vdots \\
f^{(m)}(x_1,\ldots,x_n) &= \sum_i^n \cdots \sum_j^n f_{i\cdots j}^{(m)} \cdot \overbrace{x_i \cdot \ldots \cdot x_j}^{d} + \ldots + \sum_{i=1}^n f_i^{(m)} \cdot x_i + f_0^{(m)}.
\end{aligned} \tag{2.1}
$$

Kullanılan polinomların derecesi $d = 2$ ve $d = 3$ olarak alınırsa sırasıyla ikinci dereceden ve üçüncü dereceden çok değişkenli polinom sistemi elde edilmektedir. k güvenlik seviyesini ve q sonlu cismin eleman sayısını göstermek üzere ikinci dereceden çok değişkenli polinom sistemi $F \in MQ(n,m,\mathbb{F}_q,k)$ ve üçüncü dereceden çok değişkenli polinom sistemi $F \in MC(n,m,\mathbb{F}_q,k)$ şeklinde ifade edilmektedir. Verimlilik açısından ve hesaplama anlamında daha kolay olduğundan sistemlerde genellikle ikinci dereceden çok değişkenli polinom sistemleri kullanılmaktadır (Sakumoto vd, 2011; Monteiro vd, 2015; Chen vd, 2016b). Tanım 2.3.'te çok değişkenli polinomlara dayanan sistemlerin dayandığı kuantum sonrasında da polinomal zamanda çözülemeyen zor problem tanımlanmıştır.

Tanım 2.3 (Çok Değişkenli Problem): *Eşitlik (2.1)'de verilen m tane polinom* $(f^{(1)}(\mathbf{x}),\ldots,f^{(m)}(\mathbf{x}))$ *için* $f^{(1)}(\bar{\mathbf{x}}) = \ldots = f^{(m)}(\bar{\mathbf{x}}) = 0$ *olacak şekilde* $\bar{\mathbf{x}} = (\bar{x}_1,\ldots,\bar{x}_n)$ *değerlerinin bulunup bulunamayacağı çok değişkenli problem olarak tanımlanmıştır. Bu problem Şekil* 1.1*.'de verilen kuantum bilgisayarlarda polinom zamanda çözülebilen BQP sınıfına girmemektedir. Kuantum bilgisayarlarda bile polinom zamanda çözülemediğinden NP-zor bir problemdir. Çok değişkenli problemin zorluğu, sonlu bir cisimde F polinom sistemi için* $F(x) = 0$ *yapan x değerlerini bulmanın zor olmasına dayanmaktadır (Bernstein, 2009). İkinci dereceden polinom sistemlerinin dayandığı zor problem literatürde MQ problem olarak bilinmektedir. MQ problemin çözümünün zorluğunun parametre değerlerine, özellikle değişken sayısına, denklem sayısına ve sonlu cisim uzayına bağlı olduğu belirtilmiştir. Bu problem için farklı*

Grup I:	Şifreleme,	$m = 2n$,	$\mathbb{F} = GF(2)$
Grup II:	Şifreleme,	$m = 2n$,	$\mathbb{F} = GF(2^8)$
Grup III:	Şifreleme,	$m = 2n$,	$\mathbb{F} = GF(31)$
Grup IV:	İmzalama,	$n \approx 1.5m$	$\mathbb{F} = GF(2)$
Grup V:	İmzalama,	$n \approx 1.5m$	$\mathbb{F} = GF(2^8)$
Grup VI:	İmzalama,	$n \approx 1.5m$	$\mathbb{F} = GF(31)$

gruplar oluşturulmuştur. Bu altı grup için MQ probleminin çözümünü bulana ödül verileceği söylenmektedir (Fukuoka MQ-challenge, 2018).

2.1. Kimlik Doğrulama Sistemleri

Bu kısımda kimlik doğrulama şemasının tanımı verilerek şemanın sağlaması gereken özellikler anlatılmaktadır. Bunun yanı sıra, çok değişkenli polinomlara dayanan kimlik

doğrulama şemalarında kullanılan yapılar tanımlanmaktadır. Tanım 2.4.'te kimlik doğrulama şeması tanımlanmıştır.

Tanım 2.4 (Kimlik Doğrulama Şeması): *Kimlik doğrulama şeması ispatlayıcı (prover) ve doğrulayıcı (verifier) olmak üzere iki taraftan oluşmaktadır. İspatlayıcı açık ve gizli anahtara sahip iken doğrulayıcı sadece ispatlayıcının açık anahtarına sahiptir. Kimlik doğrulama şeması, gizli anahtarı sadece kendisinde olan bir ispatlayıcının buna karşılık gelen açık anahtarı doğrulayıcıya vererek doğrulayıcıya kendi kimliğini ispatlamasına olanak tanımaktadır (Fiat ve Shamir, 1986).*

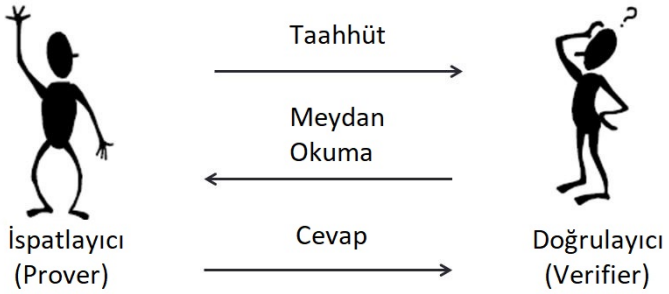
Kimlik doğrulama şeması sırasıyla S, G ve (P,V) algoritmalarından oluşmaktadır (Abdalla vd, 2002).

- *S, 1^{λ} güvenlik parametresini giriş olarak alıp F çok değişkenli fonksiyonu çıktı olarak veren bir başlangıç algoritmasıdır.*
- *G anahtar üretme algoritması, S başlangıç algoritmasının çıktısını giriş değeri olarak almaktadır. Rastgele $s \in \mathbb{F}_q^n$ seçerek $v = F(s)$ olacak şekilde (v,s) anahtar çiftlerini üretmektedir. Anahtar çiftindeki v açık anahtarı, s ise gizli anahtarı ifade etmektedir. S ve G algoritmaları kimlik doğrulama şeması için hazırlık niteliğindedir.*
- *(P,V) algoritma çifti ise kimlik doğrulama şemasında ispatlayıcı ve doğrulayıcı arasındaki etkileşimli kısımları göstermektedir. P, ispatlayıcı tarafında v açık anahtarı ve s gizli anahtarı kullanılarak çalıştırılırken V, doğrulayıcı tarafında ispatlayıcının v açık anahtarı kullanılarak çalıştırılmaktadır. V algoritmasının sonunda bir bitlik b doğruluk değeri üretilmektedir.*

$$b = \begin{cases} 1, & \textit{doğrulayıcı kimliği doğrular} \\ \textit{aksi halde}, & \textit{doğrulayıcı kimliği doğrulayamaz.} \end{cases}$$

Bu algoritmalar kullanılarak bir kimlik doğrulama şemasının üç ana aşamada gerçekleştirildiği Şekil 2.1.'de gösterilmektedir.

Taahhüt (Commitment): İspatlayıcının doğrulayıcıya taahhütte bulunduğu aşamadır.



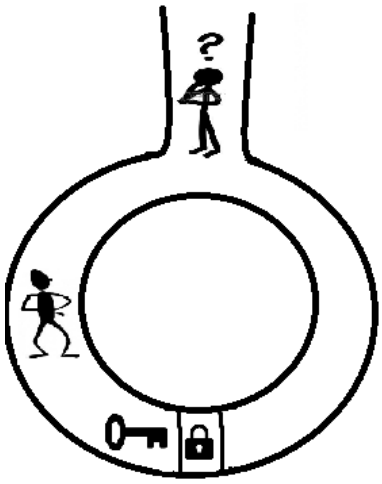
Şekil 2.1. Kimlik doğrulama şeması

Meydan Okuma (Challenge): Bu aşamada doğrulayıcı ispatlayıcının iddiasına inanabilmek için ispatlayıcıya sorular sormak kaydıyla meydan okumaktadır.

Cevap (Response): Bu aşamada ispatlayıcı doğrulayıcının meydan okumalarının cevaplarını göndermektedir. Üç aşamalı klasik bir kimlik doğrulama şemasında meydan okuma ve cevap aşamaları birden fazla defa gerçekleşebilmektedir.

Doğrulayıcı meydan okumalarına karşılık gelen cevapları aldıktan sonra taahhüt değerlerinin doğruluğundan emin olabilmek için hesaplamalar yapmaktadır. Hesaplamalar sonucunda ispatlayıcıdan gelen taahhüt değerleri ile kendi hesapladığı değerler birbirine eşit ise doğruluk değeri 1'e eşit olmakta ve doğrulayıcı ispatlayıcının kimliğini doğrulamaktadır. Aksi halde doğruluk değeri 0 olarak üretilerek kimlik doğrulama şeması doğrulayıcının ispatlayıcıyı reddetmesi ile sona ermektedir. Sıfır bilgi paylaşımlı bir kimlik doğrulama şemasında ispatlayıcı sahip olduğu bilgiyi doğrulayıcıya vermeden gizli bilgiyi bildiğini doğrulayıcıya ispat etmektedir. Sıfır bilgi paylaşımının anlaşılabilmesi için mağara örneği verilmektedir (Simari, 2002). Bu örnekte Şekil 2.2.'de verildiği gibi bir mağaranın olduğu kabul edilmektedir.

İspatlayıcı mağaranın içindeki kilitli kapının şifresini bildiğini doğrulayıcıya ispatlamak istemektedir. Doğrulayıcı mağaranın dışında dururken ispatlayıcı mağaranın içerisine girer ve ispatlayıcıya kendisinin belirlediği bir kapıdan gelmesini söyler. Böyle bir durumda ispatlayıcının yüzde elli şansı vardır. İspatlayıcı doğrulayıcının seçtiği tarafta ise kapının şifresini açmasına gerek kalmadan mağaranın girişine gelebilir veya doğrulayıcının istediği taraftan mağaranın girişine gelebilmek için şifreyi kullanabilir. İspatlayıcı doğrulayıcının seçtiği tarafta değilse ve ispatlayıcı şifreyi bilmiyorsa kapıyı açamayacağı için doğrulayıcı ispatlayıcının kapının şifresini bilmediğini anlayacaktır. İspatlayıcının kapının şifresini bildiği ve her defasında



Şekil 2.2. Sıfır bilgi paylaşımının gösterimi

doğrulayıcının seçtiği taraftan geldiği düşünüldüğünde doğrulayıcı kapının şifresinin ne olduğunu bilmeden ispatlayıcının kapının şifresini bildiğine ikna olacaktır. Burada dikkat edilmesi gereken husus doğrulayıcının ikna olduğu bilgiyi üçüncü bir kişiye ispat edebilmek için bilgiye sahip olmamasıdır.

Mağara örneğinde olduğu gibi sıfır bilgi paylaşımlı kimlik doğrulama şemasında doğrulayıcı, gizli anahtarı bilmeden sadece ispatlayıcının kendisine gönderdiği sınırlı bilgileri kullanarak ispatlayıcının taahhüdünün doğru olduğuna ikna olacak ve kimliğini doğrulayacaktır (Simari, 2002). Ayrıca şema sıfır bilgi paylaşımlı olduğu için doğrulayıcı meydan okumaları ve bunlara karşılık olarak aldığı cevapları kopyalasa bile elinde bulundurduğu bilgiler bir işe yaramayacak sadece şemanın kopyasını oluşturmuş olacaktır. Sonuç olarak üçüncü bir kişiye kimliği neden doğruladığını ispatlayamayacaktır.

Bir kimlik doğrulama şemasının tamlık (completeness) ve sağlamlık (soundness) özelliklerini sağlaması gerekmektedir.

Tanım 2.5 (Tamlık Özelliği): *(Menezes vd, 1996) Kimlik doğrulama şemasının sonunda dürüst doğrulayıcı, dürüst ispatlayıcının iddiasını kabul ediyorsa kimlik doğrulama şeması tamlık özelliğine sahiptir.*

Tanım 2.6 (Sağlamlık Özelliği): *(Menezes vd, 1996) Sahtekar ispatlayıcı doğrulayıcıyı yanlış bir iddiaya inanması konusunda ikna edemiyorsa (ihmal edilebilir olasılık $\varepsilon > 0$ hariç) kimlik doğrulama şeması sağlamlık özelliğine sahiptir. Eğer*

saldırgan, doğrulayıcıya kendisini ispatlayıcı olarak göstermeye çalışırsa başarma olasılığı ihmal edilecektir.

Sıfır bilgi paylaşımlı bir kimlik doğrulama şeması elde edebilmek amacıyla taahhüt şeması kullanılmaktadır. Tanım 2.7.'de taahhüt şeması anlatılmaktadır.

Tanım 2.7 (Taahhüt (Commitment) Şeması): *Taahhüt şeması Com, göndericinin alıcıya taahhütte bulunmasını daha sonra bu taahhüdü doğrulatabilmesini sağlayan bir şemadır. Taahhüt şeması iki aşamalı olarak gerçekleşmektedir. Taahhüt şemasının ilk aşamasında gönderici alıcıya bazı bilgileri taahhüt etmektedir. Bu aşamada a ve b göndericinin mesajını gösteren iki parametre olmak üzere gönderici* $c = Com(a,b)$ *taahhüt değerini hesaplar ve bu değeri alıcıya gönderir. İkinci aşamada ise göndericinin taahhüdünü yerine getirdiği doğrulama işlemi yapılmaktadır. Gönderici* (a,b) *değerlerini alıcıya göndererek alıcının* $c = Com(a,b)$ *değerini hesaplayabilmesini sağlamaktadır. Alıcı kendi hesapladığı ve ilk aşamada göndericinin göndermiş olduğu c değerlerini karşılaştırır. İki değer birbirine eşit ise taahhüdü kabul eder değilse reddeder (Alkadri, 2015).*

Sıfır bilgi paylaşımlı bir kimlik doğrulama şeması elde edebilmek için *Com* taahhüt şemasının Tanım 2.8. ve 2.9.'da verilen istatistiksel saklama ve hesaplamalı bağlama özelliklerine sahip olması gerekmektedir.

Tanım 2.8 (İstatistiksel Saklama): *(Goldreich, 2004) Com taahhüt şemasının ilk aşaması tamamlandıktan sonra alıcı sınırsız hesaplama gücüne sahip olsa bile gönderici tarafından oluşturulan taahhüt değerlerini birbirinden ayıramamalıdır. Başka bir ifadeyle, Com ile oluşturulan c taahhüt değerleri birbirine olabildiğince yakın olmalıdır. Taahhüt değerlerinin hangi parametreler kullanılarak elde edildiği bilinmemelidir.*

Tanım 2.9 (Hesaplamalı Bağlama): *(Goldreich, 2004) Com taahhüt şemasında gönderici, taahhüt değerlerini bir defa oluşturduktan sonra bu değerleri değiştiremelidir. Başka bir ifadeyle, farklı parametreler kullanarak aynı taahhüt değerini hesaplayabilmesi zor olmalıdır.*

Çok değişkenli polinom sistemlerinde yüksek dereceli polinomlarla çalışıldığından belli bölümlerin doğrusallaştırılmasına ihtiyaç bulunmaktadır. Doğrusallaştırmayı gerçekleştirebilmek için çeşitli yapılar kullanılmaktadır. Tanım 2.10.'da ikinci dereceden polinomlara dayanan kimlik doğrulama şemalarında kullanılan polar form tanımlanmıştır.

Tanım 2.10 (Polar Form): *$x, y \in \mathbb{F}_q^n$ olmak üzere G, ikinci dereceden çok değişkenli F polinom sisteminin polar formunu ifade etmektedir ve Eşitlik (2.2)'de tanımlanmaktadır (Sakumoto vd, 2011).*

$$G(x,y) = F(x+y) - F(x) - F(y) \tag{2.2}$$

İkinci dereceden polinomlara dayanan kimlik doğrulama şemalarında kullanılan bu G polar formu ikili doğrusal bir fonksiyondur. Tanım 2.11.'de ikili doğrusal fonksiyon tanımı verilmiştir.

Tanım 2.11 (İkili Doğrusal Fonksiyon): *$G : A \times B \to C$ polar fonksiyonu ikili doğrusallık özelliğine sahip bir fonksiyon olduğundan $a_1, a_2 \in A$ ve $b \in B$ olmak üzere*

$$G(a_1 + a_2, b) = G(a_1, b) + G(a_2, b)$$

koşulunu sağlamaktadır.

Bölüm 1.2.'de belirtildiği üzere hem ikinci dereceden hem de üçüncü dereceden çok değişkenli polinomlara dayanan kimlik doğrulama şemaları bulunmaktadır. Bu şemalarda kullanılacak farklı polar formların tanımlanmasına ihtiyaç vardır. Üçüncü dereceden çok değişkenli polinomlara dayanan kimlik doğrulama şemalarında kullanılmak üzere tanımlanmış polar form Tanım 2.12.'de verilmiştir.

Tanım 2.12 : *Sakumoto (2012) çalışmasında üçüncü dereceden çok değişkenli polinomlara dayanan kimlik doğrulama şemalarında kullanılmak amacıyla $x, y \in \mathbb{F}_q^n$ olmak üzere G, üçüncü dereceden çok değişkenli F polinom sisteminin polar formu aşağıdaki gibi tanımlanmaktadır.*

$$G(x,y) + G(y,x) = F(x+y) - F(x) - F(y) \tag{2.3}$$

Daha büyük dereceli polinom sistemleri kullanıldığında polar form yapısının nasıl olacağı Sakumoto (2012) çalışmasında açık problem olarak tanımlanmıştır. Bu problem Problem 2.1.'de verilmektedir.

Problem 2.1 (Açık Problem): *Sakumoto vd (2011) ve Sakumoto (2012) çalışmalarında ikinci ve üçüncü dereceden polinom sistemlerine dayanan kimlik doğrulama şemaları verilmiştir. Dört veya daha büyük dereceden polinom sistemlerine dayanan verimli şemaların oluşturulup oluşturulamayacağı açık bir problemdir (Sakumoto, 2012).*

Nachef vd (2012) çalışmasında açık probleme çözüm önerisi getirilmiştir. Kimlik doğrulama şemalarında derecesi ikiden büyük polinomlar kullanıldığında polar form yapısının nasıl olması gerektiği konusunda bir genelleştirme önerilmiştir. Bu genelleştirme Tanım 2.13.'te verilmiştir.

Tanım 2.13 : *Nachef vd (2012) çalışmasında, d. dereceden n değişkenli m tane polinomdan oluşan F polinom sisteminin polar formu $G : (\mathbb{F}_q^n)^d \to \mathbb{F}_q^m$ olmak üzere*

$$G(r_0, r_1, \cdots, r_{d-1}) = \sum_{i=1}^{d} (-1)^{d-i} \sum_{S \subset \{0,\cdots,d-1\} | |S|=i} F(\sum_{j \in S} r_j) \tag{2.4}$$

eşitliğini sağlayacak şekilde genelleştirilmiştir. Eşitlik (2.4)'de genelleştirilmiş hali verilen G polar form herhangi bir d için doğrusallık özelliğine sahiptir.

Yapılan bu genelleştirmeyi örnekle açıklayalım. Örneğin; $x, y, z \in \mathbb{F}_q^n$ olmak üzere $d = 3$ için üçüncü dereceden çok değişkenli polinom sistemi F oluşturulurken Eşitlik (2.4)'te verilen genel polar form kullanılarak F polinom sisteminin polar formu G,

$$G(x,y,z) = F(x+y+z) - F(x+y) - F(x+z) - F(y+z) + F(x) + F(y) + F(z) \tag{2.5}$$

şeklinde elde edilmektedir. Eşitlik (2.5)'te verilen polar form üçlü doğrusallık özelliğine sahip bir fonksiyondur. Bu fonksiyon Tanım 2.14.'te tanımlanmaktadır.

Tanım 2.14 (Üçlü Doğrusal Fonksiyon): *$G : A \times B \times C \to D$ polar fonksiyonu üçlü doğrusallık özelliğine sahip bir fonksiyon olduğundan $a_1, a_2, a_3 \in A$, $b \in B$ ve $c \in C$ olmak üzere*

$$G(a_1 + a_2 + a_3, b, c) = G(a_1, b, c) + G(a_2, b, c) + G(a_3, b, c)$$

koşulunu sağlamaktadır.

Kimlik doğrulama şemalarında derecesi 2 ve 3 olan polinomlar kullanıldığında polar form yapısının nasıl olacağı Tanım 2.10. ve Tanım 2.12.'de verilmiştir. Bunun yanı sıra, Tanım 2.13.'te derecesi üç veya daha büyük polinomlar için bir genelleştirme verilmiştir. Akleylek ve Soysaldı (2017) çalışmasında üç veya daha büyük dereceden polinomlara dayanan sistemler oluşturulduğunda Tanım 2.12.'de verilen polar formun kullanılabileceği belirtilmiştir. G polar formun dereceye göre nasıl hesaplanacağını gösteren bir genelleştirme önerilmiştir. Önerilen bu genelleştirme Tanım 2.15.'te verilmiştir.

Tanım 2.15 *G, derecesi $d \geq 3$ olan polinomlardan oluşan F polinom sisteminin polar formu;*

$$G(x,y) = xy + \sum_{i=3}^{d} \begin{cases} \sum_{j=1}^{\frac{(i-1)}{2}} P(x^{i-j}, y^{j}) & ,i \text{ tek sayı} \\ \sum_{j=1}^{(\frac{i}{2}-1)} P(x^{i-j}, y^{j}) + \frac{P(x^{i/2}, y^{i/2})}{2} & ,i \text{ çift sayı} \end{cases}$$

$$G(y,x) = yx + \sum_{i=3}^{d} \begin{cases} \sum_{j=1}^{\frac{(i-1)}{2}} P(x^{j}, y^{i-j}) & ,i \text{ tek sayı} \\ \sum_{j=1}^{(\frac{i}{2}-1)} P(x^{j}, y^{i-j}) + \frac{P(x^{i/2}, y^{i/2})}{2} & ,i \text{ çift sayı} \end{cases}$$

şeklinde hesaplanmak üzere $F(x+y) = F(x) + G(x,y) + G(y,x) + F(y)$ eşitliğinden elde edilmektedir (Akleylek and Soysaldı, 2017). G polar fonksiyonları hesaplanırken kullanılan $P(x^{j}, y^{i-j})$, i elemanlı bir vektör için j tane x ve $(i-j)$ tane y vektörünü içeren permütasyonları göstermektedir.

2.2. İmzalama Sistemleri

Elektronik imzalar, kağıt üstünde kullandığımız imzaların elektronik ortama aktarılması ile elektronik ortamdaki dökümanları imzalayabilmemizi sağlamaktadır. Elektronik imzalar kimlik doğrulama, inkar edememe ve bütünlük gibi bilgi güvenliği kavramlarını sağlamaktadır. Elektronik imzalama şemalarında gönderici kendi özel anahtarı ile mesajını imzalayarak alıcıya gönderirken; alıcı, imzalanmış mesajı göndericinin açık anahtarını kullanarak doğrulayabilmektedir. Tanım 2.16.'da elektronik imzalama şemalarına yer verilmiştir.

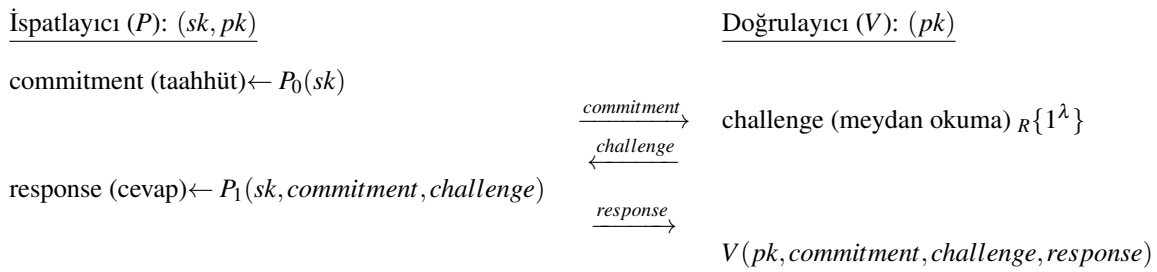
Tanım 2.16 (Elektronik İmzalama Şeması): *(Abdalla vd, 2002) Elektronik imzalama şeması sırasıyla $KeyGen, Sign$ ve $Verify$ algoritmalarından oluşmaktadır.*

- *KeyGen anahtar üretme algoritmasıdır. Bu algoritma $\lambda \in \mathbb{N}$ olmak üzere 1^λ güvenlik parametresini giriş olarak alırken çıktı olarak (pk, sk) açık ve gizli anahtardan oluşan bir çift anahtar üretmektedir.*
- *Sign imzalama algoritmasıdır. Giriş olarak sk gizli anahtarı ve m mesajını alarak σ imza üretmektedir.*
- *$Verify$ doğrulama algoritmasıdır. Algoritma giriş olarak pk açık anahtarı, m mesajı ve σ imzayı alarak bir bitlik bir karar biti döndürmektedir. Karar bitinin sonucuna göre imza doğrulanmakta veya doğrulanamayıp reddedilmektedir.*

İmzanın doğruluğundan bahsedebilmek için $\lambda \in \mathbb{N}$ olmak üzere $(pk, sk) \leftarrow KeyGen(1^\lambda)$ olacak şekilde anahtar çiftlerini, bütün m mesaj değerleri için $\sigma \leftarrow Sign(sk, m)$ olacak şekilde imzayı üretebilen ve $Verify(pk, m, \sigma) = 1$ olacak şekilde karar bitini döndürebilen bir imzalama şemasının olması gerekmektedir.

Kimlik doğrulama şemalarını imzalama şemalarına dönüştürebilmek için Fiat-Shamir dönüşümü kullanılmaktadır. Bu dönüşüm Tanım 2.17.'de verilmiştir.

Tanım 2.17 (Fiat-Shamir Dönüşümü): *(Fiat and Shamir, 1986) $\lambda \in \mathbb{N}$ güvenlik parametresi olmak üzere $IDS = (KeyGen, P, V)$ sağlamlık özelliğine sahip üç aşamalı*



Şekil 2.3. IDS Kimlik doğrulama şemasının şematik gösterimi

kimlik doğrulama şemasını ifade etmektedir. IDS kimlik doğrulama şemasının şematik gösterimi Şekil 2.3.'te verilmiştir.

r şemanın döngü sayısını göstermek üzere IDS^r kimlik doğrulama şeması için meydan okuma değeri C^r ve özet fonksiyonu $H_1 : \{0,1\}^* \rightarrow C^r$ şeklinde ifade edilmektedir. IDS kimlik doğrulama şeması, sırasıyla $(KeyGen, Sign, Verify)$ algoritmalarını içeren DSS imzalama şemasına dönüştürülmektedir. İmzalama şemasının

- *birinci aşamasında $(sk, pk) \leftarrow KeyGen(1^\lambda)$ olacak şekilde anahtar çiftleri elde edilmektedir.*
- *ikinci aşamasında $\sigma_0 = commitment \leftarrow P_0(sk)$ olacak şekilde IDS'den imzanın ilk parçası elde edilmektedir. Sonra, $h_1 = H_1(m, \sigma_0)$ ve $\sigma_1 = response \leftarrow P_1^r(sk, \sigma_0, h_1)$ olmak üzere $\sigma = (\sigma_0, \sigma_1) \leftarrow Sign(sk, m)$ imza üretilmektedir.*
- *son aşamada $Verify(pk, m, \sigma)$ algoritması ile $\sigma = (\sigma_0, \sigma_1)$ ve $h_1 = H_1(m, \sigma_0)$ değerleri elde edilerek IDS kimlik doğrulama şemasında olduğu gibi $V^r(pk, \sigma_0, h_1, \sigma_1)$ doğrulama yapılmaktadır.*

3. KUANTUM SONRASI GÜVENİLİR YENİ KİMLİK DOĞRULAMA ŞEMALARI

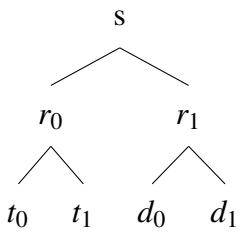
Bu bölümde, sonlu cisimler üzerinde çok değişkenli polinomlara dayanan sıfır bilgi paylaşımlı üç aşamalı yeni kimlik doğrulama şemaları önerilmiştir. Literatürdeki kimlik doğrulama şemalarından daha verimli bir şema oluşturabilmek amacıyla daha önce denenmemiş gizli anahtarı parçalama teknikleri kullanılmıştır. Farklı parçalama teknikleri kullanılarak üç tane kimlik doğrulama şeması önerilmiştir. Bu bölümde, önerilen yeni kimlik doğrulama şemaları ve kullanılan yapılar detaylı bir şekilde ele alınmıştır. Tanım 3.1.'de gizli anahtarın nasıl parçalandığını gösteren parçalama tekniği verilmektedir.

Tanım 3.1 *Kimlik doğrulama şemasında kullanılan gizli anahtar ilk başta* $s = r_0 + r_1 + \ldots + r_\ell$ *olacak şekilde* $(\ell+1)$ *parçaya ayrılmış olsun. Böyle bir şemada gizli anahtarın parçalama tekniğini* $DT = (s_s; s_{r_0} - s_{r_1} - \ldots - s_{r_\ell})$ *şeklinde ifade edelim. Burada* s_s *gizli anahtarın ilk parçalanıştaki parça sayısını gösterirken diğer parametreler sırasıyla* $r_0, r_1, \ldots, r_\ell$ *parçalarının alt parçalanışlarının sayısını göstermektedir.* $s_{r_0}, s_{r_1}, \ldots, s_{r_\ell}$ *alt parçalanış sayıları toplandığında gizli anahtarın toplamda kaç alt parça ile gösterildiği bulunmaktadır.*

***Örnek* 1** *Parçalama tekniği olarak DT=(2;2-2) verilmiş olsun. İlk parametreye bakarak s gizli anahtarının ilk parçalanışta* r_0 *ve* r_1 *olacak şekilde* 2 *parçaya ayrıldığı anlaşılmaktadır. Geriye kalan iki parametreye bakıldığında ise hem* r_0 *parçasının hem de* r_1 *parçasının* 2 *parçaya ayrılarak gizli anahtarın toplamda* 4 *parça ile ifade edildiği görülmektedir. Gizli anahtarın denklemsel ifadesi*

$$s = \underbrace{t_0 + t_1}_{r_0} + \underbrace{d_0 + d_1}_{r_1} \tag{3.1}$$

şeklindedir. DT=(2;2-2) parçalama tekniği Şekil 3.1.'de gösterilmiştir.



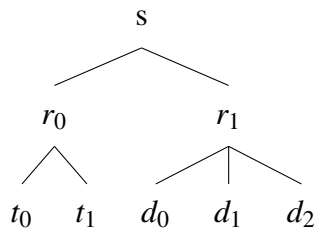
Şekil 3.1. Gizli anahtarın (2;2-2) şeklinde parçalanması

Tanım 3.1. kullanılarak önerilen kimlik doğrulama şemaları parçalanışlarına göre isimlendirilmiştir. Önerilen sıfır bilgi paylaşımlı özgün kimlik doğrulama şemaları kes-ve-seç yaklaşımına dayanmaktadır. Bu yaklaşım, ispatlayıcının gizli anahtarı parçalara ayırması ve doğrulayıcının seçtiği değerlere göre bu parçalardan bazılarını doğrulayıcıya göndererek kimliğini ispatlayabilmesi temeline dayanmaktadır.

Açıklama 1 *Kimlik doğrulama şemalarında kullanılan hc bütün taahhüt değerlerinin özet fonksiyonundan geçirilerek elde edilen özet taahhüt değerini, Ch doğrulayıcının meydan okuma değerini, Rsp ispatlayıcının meydan okumalara karşı gönderdiği cevabı ve Com (katar) taahhüt fonksiyonunu ifade etmektedir.*

3.1. (2;2-3) Parçalanışa Sahip Yeni Kimlik Doğrulama Şeması

Bu kısımda önerilen kimlik doğrulama şeması Akleylek ve Soysaldı (2018a) çalışmasında yer almaktadır. Sonlu cisimler üzerinde ikinci dereceden çok değişkenli polinomlara dayanan üç aşamalı sıfır bilgi paylaşımlı yeni bir kimlik doğrulama şeması önerilmiştir. Burada amacımız, gizli anahtarı farklı şekilde parçalayarak daha verimli bir şema oluşturabilmektir. Önerilen kimlik doğrulama şemasında kullanılan (2;2-3) parçalama tekniği Şekil 3.2.'de verilmektedir. s gizli anahtarı $r_0 + r_1$ şeklinde ifade



Şekil 3.2. Gizli anahtarın (2;2-3) şeklinde parçalanması

edilmiştir. F, ikinci dereceden çok değişkenli polinom sistemini göstermek üzere

$v = F(s)$ açık anahtarı göstermektedir. $F(r_0)$, e_0 ve e_1 gibi iki parçaya $F(r_1)$ ise u_0, u_1 ve u_2 olacak şekilde üç parçaya bölünmüştür.

3.1.1. Şemanın doğrulanması

Kimlik doğrulama şemasında ikinci dereceden çok değişkenli polinomlar kullanıldığı için Tanım 2.10.'daki ikili doğrusal polar form kullanılmıştır. Eşitlik (3.2) ve Eşitlik (3.3) sağlandığı sürece doğrulayıcı ispatlayıcının kimliğini doğrulayabilmektedir.

$$G(r_0,d_1)+u_1 = v - \overbrace{(G(r_0,d_0)+G(r_0,d_2))}^{G(r_0,d_0+d_2)} - F(r_0) - u_0 - u_2 \tag{3.2}$$

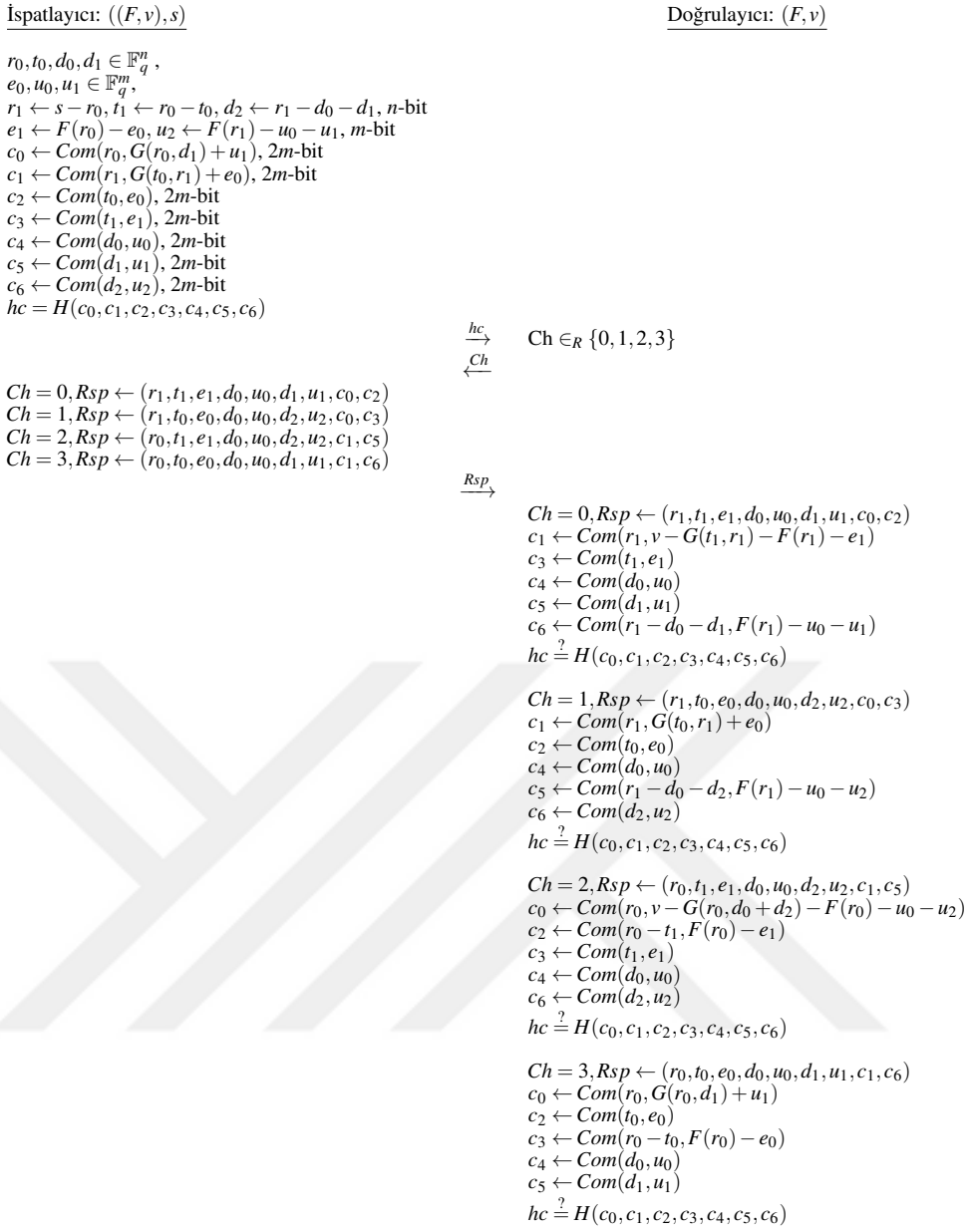
$$G(t_0,r_1)+e_0 = v - G(t_1,r_1) - F(r_1) - e_1 \tag{3.3}$$

Tanım 2.10. ve Tanım 2.11. kullanılarak şemanın doğruluğu aşağıdaki gibi ispatlanmaktadır.

$$\begin{aligned} v &= G(r_0,d_0+d_2)+G(r_0,d_1)+F(r_0)+u_0+u_1+u_2 \\ &= G(r_0,d_0+d_1+d_2)+F(r_0)+u_0+u_1+u_2 \\ &= G(t_0+t_1,r_1)+e_0+e_1+F(r_1) \\ &= G(r_0,r_1)+F(r_0)+F(r_1) \\ &= F(r_0+r_1) = F(s) \end{aligned}$$

Önerilen üç aşamalı sıfır bilgi paylaşımlı kimlik doğrulama şeması Şekil 3.3.'te verilmiştir.

Şimdi önerilen kimlik doğrulama şemasının nasıl çalıştığına bakacağız. Etkileşimli bir kimlik doğrulama şeması başlamadan önce ispatlayıcı tarafında bazı algoritmaların çalıştırılması gerekmektedir. Tanım 2.4.'te anlatıldığı üzere ispatlayıcı ilk olarak başlangıç algoritmasını çalıştırır. Başlangıç algoritmasının girdisi 1^λ gibi bir güvenlik parametresi iken çıktısı $F \in MQ(n,m,\mathbb{F}_q,k)$ polinom sistemidir. Elde edilen F polinom sistemi anahtar üretme algoritmasına giriş olarak verilir. Anahtar üretme algoritmasında gizli anahtar için rastgele olarak $s \in \mathbb{F}_q^n$ değeri seçilir. Seçilen s değeri kullanılarak $v = F(s)$ değeri hesaplanır. Anahtar üretme algoritmasının sonucunda $v = F(s)$ açık anahtar ve s gizli anahtar olmak üzere (v,s) anahtar çifti elde edilmektedir. Bu aşamadan sonra ispatlayıcı gizli anahtarını parçalayarak doğrulayıcıya taahhütte bulunabilmek için taahhüt



Şekil 3.3. (2;2-3) parçalanışa sahip kimlik doğrulama şeması

değerlerini hesaplamaktadır. İspatlayıcı rastgele olarak $r_0,t_0,d_0,d_1 \in \mathbb{F}_q^n$ ve $e_0,u_0,u_1 \in \mathbb{F}_q^m$ değerlerini seçmektedir. Seçtiği değerleri kullanarak taahhüt değerlerini elde edebilmek için diğer parçalanışları $r_1 = s - r_0$, $t_1 = r_0 - t_0$, $d_2 = r_1 - d_0 - d_1$, $e_1 = F(r_0) - e_0$ ve $u_2 = F(r_1) - u_0 - u_1$ hesaplamaktadır. Elinde bütün parçaları bulunduran ispatlayıcı taahhüt değerlerini hesaplamaktadır. Bu değerlerin özetini çıkararak *hc* taahhüt değeri olarak doğrulayıcıya göndermesiyle kimlik doğrulama şeması başlamış olmaktadır. Taahhüt değerini alan doğrulayıcı, ispatlayıcının taahhüdüne karşılık $Ch \in \{0,1,2,3\}$ meydan okuma değerini seçerek ispatlayıcıya meydan okumaktadır. İspatlayıcı ilk aşamada yaptığı taahhüdün doğrulayıcı tarafından

doğrulanmasını istemektedir. Bu amaç doğrultusunda, doğrulayıcının seçtiği *Ch* meydan okuma değerine karşılık gelen *Rsp* cevapları doğrulayıcıya gönderir. Bu cevaplar sayesinde doğrulayıcı ispatlayıcının taahhüdünü doğrulayabilme imkanı bulur. Meydan okumanın cevabını alan doğrulayıcı taahhüt değerlerini kendisi de hesaplar. İspatlayıcının gönderdiği taahhüt değeri ile kendi hesapladığı taahhüt değeri birbirine eşit ise doğrulayıcı ispatlayıcının taahhüdünü kabul eder ve kimliğini doğrular. Aksi takdirde, reddeder. Kimlik doğrulama şemasının sonunda doğrulayıcı gizli anahtarın ne olduğunu bilmeden ispatlayıcının taahhüdü kabul etmektedir. Bu bakımdan kimlik doğrulama şeması sıfır bilgi paylaşımlıdır.

3.1.2. Özelliklerin sağlanması

Önerilen şemanın sıfır bilgi paylaşımlı bir kimlik doğrulama şeması olduğunu söyleyebilmek için Teorem 1 ve Teorem 2'de verilen özelliklerin sağlanması gerekmektedir.

Teorem 1 *Com taahhüt şeması istatistiksel saklama özelliğine sahip ise oluşturulan kimlik doğrulama şeması istatistiksel olarak sıfır bilgi paylaşımlıdır.*

***İspat* 1** *Kabul edelim ki, S, (F,v)'yi bilen fakat gizli anahtarın ne olduğunu bilmeyen sahte doğrulayıcı karşısında dürüst ispatlayıcı gibi davranabilen bir simülatör olsun. Simülatör S, $1/2$ ihtimal ile dürüst ispatlayıcıyı taklit edebilmektedir. S simülatörü, gizli anahtar ve parçaları için $s', r'_0, t'_0, d'_0, d'_1 \in_R \mathbb{F}_q^n$ ve $e'_0, u'_0, u'_1 \in_R \mathbb{F}_q^m$ değerlerini seçerek $r'_1 \leftarrow s' - r'_0$, $t'_1 \leftarrow r'_0 - t'_0$, $d'_2 \leftarrow r'_1 - d'_0 - d'_1$ değerlerini hesaplamaktadır. Sonra simülatör S rastgele $Ch' \in \{0,1\}$ değerini seçer. Simülatörün meydan okuma için 0 ve 1 değerlerini seçmesi sırasıyla $Ch = \{2,3\}$ ve $Ch = \{0,1\}$ olması anlamına gelmektedir. Burada S, sahtekar doğrulayıcının seçemeyeceği bir Ch' değeri seçmeye çalışmaktadır. Seçilen değere göre S,*

$$Ch' = \begin{cases} 0, & \begin{cases} e'_1 = v - F(s') + F(r'_0) - e'_0 \\ u'_2 = F(r_1)' - u'_0 - u'_1 \end{cases} \\ 1, & \begin{cases} e'_1 = F(r'_0) - e'_0 \\ u'_2 = v - F(s') + F(r'_1) - u'_0 - u'_1 \end{cases} \end{cases}$$

gizli anahtarın parçalarını hesaplamaktadır. S, gizli anahtarın bütün parçalarını elde ettikten sonra

$$c_0 \leftarrow Com(r'_0, G(r'_0, d'_1) + u'_1),$$

$$c_1 \leftarrow Com(r'_1, G(t'_0, r'_1) + e'_0),$$

$$c_2 \leftarrow Com(t'_0, e'_0),$$

$$c_3 \leftarrow Com(t'_1, e'_1),$$

$$c_4 \leftarrow Com(d'_0, u'_0),$$

$$c_5 \leftarrow Com(d'_1, u'_1),$$

$$c_6 \leftarrow Com(d'_2, u'_2)$$

taahhüt değerlerini hesaplayarak sahtekar doğrulayıcıya göndermektedir. Com istatistiksel saklama özelliğine sahip olduğu için sahtekar doğrulayıcının gönderdiği meydan okuma değeri olan Ch değeri simülatörün seçtiği meydan okuma değeri olan Ch''dan $1/2$ olasılıkla farklıdır. $Ch' = 1$ ve $Ch = 0$ olması durumunda $e'_1 \leftarrow v - F(s') + F(r'_0) - e'_0$ elde edilmektedir. $v - G(t_1, r_1) - F(r_1) - e_1 = G(t_0, r_1) + e_0$ olduğu bilindiğinden c_1 taahhüt değeri doğrulanmış olmaktadır. Diğer durumda $Ch' = 1$ ve $Ch = 1$ olur ki bu durumda v açık anahtar kullanılmadığından doğrulama işlemi daha kolay olmaktadır. $Ch' = 0$ ve $Ch \in \{2,3\}$ olduğunda ise benzer durumlar söz konusudur. S simülatörünü kullanan bir sahte ispatlayıcı gerçek şemanın kopyasını oluşturabilir. Fakat Com taahhüt şeması saklama özelliğine sahip olursa üçüncü bir şahıs şema hakkında bilgi edinemez. Başka bir ifadeyle, oluşturulan kimlik doğrulama şeması sıfır bilgi paylaşımlıdır.

Teorem 2 *Com taahhüt şemasının hesaplamalı bağlayıcı olduğu durumda her bir döngüde hesaplamalı olarak $1/2$ hata olasığı vardır.*

***İspat* 2** *$Ch_i = i$ olmak üzere doğrulayıcı dürüst ispatlayıcının iddiasını kabul ederse karar fonksiyonu $Dec(F, v, hc_i, Ch_i, Rsp_i) = 1$ olmaktadır. Bu bakımdan*

$$s_1 = \{(hc_0, Ch_0, Rsp_0), (hc_1, Ch_1, Rsp_1), (hc_2, Ch_2, Rsp_2)\},$$

$$s_2 = \{(hc_0, Ch_0, Rsp_0), (hc_1, Ch_1, Rsp_1), (hc_3, Ch_3, Rsp_3)\},$$

$$s_3 = \{(hc_0, Ch_0, Rsp_0), (hc_2, Ch_2, Rsp_2), (hc_3, Ch_3, Rsp_3)\},$$

$$s_4 = \{(hc_1, Ch_1, Rsp_1), (hc_2, Ch_2, Rsp_2), (hc_3, Ch_3, Rsp_3)\}.$$

doğrulayıcı tarafından kabul edilebilecek taahhüt, meydan okuma ve cevapları içeren dört farklı durum kümesi olsun. $(c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ *önerilen şemada hesaplanan taahhüt değerlerini,* $hc_0 = hc_1 = hc_2 = hc_3 = H(c_0, c_1, c_2, c_3, c_4, c_5, c_6)$ *taahhüt değerlerinin özetlerini ve*

$$Rsp_0 = (r_1^{(0)}, t_1^{(0)}, e_1^{(0)}, d_0^{(0)}, u_0^{(0)}, d_1^{(0)}, u_1^{(0)}, c_0, c_2),$$
$$Rsp_1 = (r_1^{(1)}, t_0^{(1)}, e_0^{(1)}, d_0^{(1)}, u_0^{(1)}, d_2^{(1)}, u_2^{(1)}, c_0, c_3),$$
$$Rsp_2 = (r_0^{(2)}, t_1^{(2)}, e_1^{(2)}, d_0^{(2)}, u_0^{(2)}, d_2^{(2)}, u_2^{(2)}, c_1, c_5),$$
$$Rsp_3 = (r_0^{(3)}, t_0^{(3)}, e_0^{(3)}, d_0^{(3)}, u_0^{(3)}, d_1^{(3)}, u_1^{(3)}, c_1, c_6).$$

meydan okumaları belirtsin.

Durum 1: *s_1 kümesi için her bir c_i taahhüt değerlerini hesaplarsak;*

$$\begin{aligned}
c_0 &= Com(r_0^{(2)}, v - G(r_0^{(2)}, d_0^{(2)} + d_2^{(2)}) - F(r_0^{(2)}) - u_0^{(2)} - u_2^{(2)}) \\
c_1 &= Com(r_1^{(0)}, v - G(t_1^{(0)}, r_1^{(0)}) - F(r_1^{(0)}) - e_1^{(0)}) = Com(r_1^{(1)}, G(t_0^{(1)}, r_1^{(1)}) + e_0^{(1)}) \\
c_2 &= Com(t_0^{(1)}, e_0^{(1)}) = Com(r_0^{(2)} - t_1^{(2)}, F(r_0^{(2)}) - e_1^{(2)}) \\
c_3 &= Com(t_1^{(0)}, e_1^{(0)}) = Com(t_1^{(2)}, e_1^{(2)}) \\
c_4 &= Com(d_0^{(0)}, u_0^{(0)}) = Com(d_0^{(1)}, u_0^{(1)}) = Com(d_0^{(2)}, u_0^{(2)}) \\
c_5 &= Com(d_1^{(0)}, u_1^{(0)}) = Com(r_1^{(1)} - d_0^{(1)} - d_2^{(1)}, F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)}) \\
c_6 &= Com(r_1^{(0)} - d_0^{(0)} - d_1^{(0)}, F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)}) = Com(d_2^{(1)}, u_2^{(1)}) = Com(d_2^{(2)}, u_2^{(2)})
\end{aligned} \tag{3.4}$$

elde edilir. Com şeması bağlama özelliğine sahip olduğu için; $r_1^{(0)} = r_1^{(1)}$, $t_0^{(1)} = r_0^{(2)} - t_1^{(2)}$, $e_0^{(1)} = F(r_0^{(2)}) - e_1^{(2)}$, $t_1^{(0)} = t_1^{(2)}$, $e_1^{(0)} = e_1^{(2)}$, $d_0^{(0)} = d_0^{(1)} = d_0^{(2)}$, $u_0^{(0)} = u_0^{(1)} = u_0^{(2)}$, $d_1^{(0)} = r_1^{(1)} - d_0^{(1)} - d_2^{(1)}$, $u_1^{(0)} = F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)}$, $r_1^{(0)} - d_0^{(0)} - d_1^{(0)} = d_2^{(1)} = d_2^{(2)}$, $F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)} = u_2^{(1)} = u_2^{(2)}$ *eşitlikleri elde edilir. Eşitlik (3.4)'ten;*

$$v = G(t_0^{(1)}, r_1^{(1)}) + G(t_1^{(0)}, r_1^{(0)}) + F(r_1^{(0)}) + e_1^{(0)} + e_0^{(1)} \tag{3.5}$$

elde edilmektedir. Eşitlik (3.5)'te $r_1^{(0)}$ *yerine* $r_1^{(1)}$, $t_1^{(0)}$ *yerine* $t_1^{(2)}$, $t_0^{(1)}$ *yerine* $r_0^{(2)} - t_1^{(2)}$, $e_1^{(0)}$ *yerine* $e_1^{(2)}$, $e_0^{(1)}$ *yerine* $F(r_0^{(2)}) - e_1^{(2)}$ *yazılırsa* $v = G(r_0^{(2)} - t_1^{(2)}, r_1^{(1)}) + G(t_1^{(2)}, r_1^{(1)}) + F(r_0^{(2)}) - e_1^{(2)} + e_1^{(2)} + F(r_1^{(1)})$ *elde edilmektedir. Tanım* 2.10. *kullanılarak* $v = G(r_0^{(2)} - t_1^{(2)} + t_1^{(2)}, r_1^{(1)}) + F(r_0^{(2)}) - e_1^{(2)} + e_1^{(2)} + F(r_1^{(1)}) = G(r_0^{(2)}, r_1^{(1)}) + F(r_0^{(2)}) +$

$F(r_1^{(1)}) = F(r_0^{(2)} + r_1^{(1)})$ *sonucuna ulaşılmaktadır. Demek ki, s gizli anahtarı* $r_0^{(2)}$ *ve* $r_1^{(1)}$ *olacak şekilde iki parçaya ayrılmıştır.*

Durum 2: s_2 *kümesi için her bir* c_i *taahhüt değerlerini hesaplarsak;*

$$
\begin{aligned}
c_0 &= Com(r_0^{(3)}, G(r_0^{(3)}, d_1^{(3)}) + u_1^{(3)}) \\
c_1 &= Com(r_1^{(0)}, v - G(t_1^{(0)}, r_1^{(0)}) - F(r_1^{(0)}) - e_1^{(0)}) = Com(r_1^{(1)}, G(t_0^{(1)}, r_1^{(1)}) + e_0^{(1)}) \\
c_2 &= Com(t_0^{(1)}, e_0^{(1)}) = Com(t_0^{(3)}, e_0^{(3)}) \\
c_3 &= Com(t_1^{(0)}, e_1^{(0)}) = Com(r_0^{(3)} - t_0^{(3)}, F(r_0^{(3)}) - e_0^{(3)}) \\
c_4 &= Com(d_0^{(0)}, u_0^{(0)}) = Com(d_0^{(1)}, u_0^{(1)}) = Com(d_0^{(3)}, u_0^{(3)}) \\
c_5 &= Com(d_1^{(0)}, u_1^{(0)}) = Com(r_1^{(1)} - d_0^{(1)} - d_2^{(1)}, F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)}) = Com(d_1^{(3)}, u_1^{(3)}) \\
c_6 &= Com(r_1^{(0)} - d_0^{(0)} - d_1^{(0)}, F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)}) = Com(d_2^{(1)}, u_2^{(1)})
\end{aligned}
\tag{3.6}
$$

elde edilir. Com şeması bağlama özelliğine sahip olduğu için; $r_1^{(0)} = r_1^{(1)}$, $t_0^{(1)} = t_0^{(3)}$, $e_0^{(1)} = e_0^{(3)}$, $t_1^{(0)} = r_0^{(3)} - t_0^{(3)}$, $e_1^{(0)} = F(r_0^{(3)}) - e_0^{(3)}$, $d_0^{(0)} = d_0^{(1)} = d_0^{(3)}$, $u_0^{(0)} = u_0^{(1)} = u_0^{(3)}$, $d_1^{(0)} = r_1^{(1)} - d_0^{(1)} - d_2^{(1)} = d_1^{(3)}$, $u_1^{(0)} = F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)} = u_1^{(3)}$, $r_1^{(0)} - d_0^{(0)} - d_1^{(0)} = d_2^{(1)}$, $F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)} = u_2^{(1)}$ *eşitlikleri elde edilir. Eşitlik (3.6) düzenlendiğinde,*

$$v = G(t_1^{(0)}, r_1^{(0)}) + G(t_0^{(1)}, r_1^{(1)}) + F(r_1^{(0)}) + e_1^{(0)} + e_0^{(1)} \tag{3.7}$$

elde edilmektedir. Eşitlik (3.7)'de, $r_1^{(1)}$ *yerine* $r_1^{(0)}$, $t_1^{(0)}$ *yerine* $r_0^{(3)} - t_0^{(3)}$, $t_0^{(1)}$ *yerine* $t_0^{(3)}$, $e_1^{(0)}$ *yerine* $F(r_0^{(3)}) - e_0^{(3)}$), $e_0^{(1)}$ *yerine* $e_0^{(3)}$ *yazılırsa* $v = G(r_0^{(3)} - t_0^{(3)}, r_1^{(0)}) + G(t_0^{(3)}, r_1^{(0)}) + F(r_0^{(3)}) - e_0^{(3)} + e_0^{(3)} + F(r_1^{(0)})$ *elde edilmektedir. Tanım* 2.10. *kullanılarak* $v = G(r_0^{(3)} - t_0^{(3)} + t_0^{(3)}, r_1^{(0)}) + F(r_0^{(3)}) - e_0^{(3)} + e_0^{(3)} + F(r_1^{(0)}) = G(r_0^{(3)}, r_1^{(0)}) + F(r_0^{(3)}) + F(r_1^{(0)}) = F(r_0^{(3)} + r_1^{(0)})$ *sonucuna ulaşılmaktadır. Buradan s gizli anahtarının* $r_0^{(3)}$ *ve* $r_1^{(0)}$ *olacak şekilde iki parçaya ayrıldığı görülmektedir.*

Durum 3: s_3 *kümesi için her bir* c_i *taahhüt değerlerini hesaplarsak;*

$$
\begin{aligned}
c_0 &= Com(r_0^{(2)}, v - G(r_0^{(2)}, d_0^{(2)} + d_2^{(2)}) - F(r_0^{(2)}) - u_0^{(2)} - u_2^{(2)}) \\
&= Com(r_0^{(3)}, G(r_0^{(3)}, d_1^{(3)}) + u_1^{(3)}) \qquad (3.8) \\
c_1 &= Com(r_1^{(0)}, v - G(t_1^{(0)}, r_1^{(0)}) - F(r_1^{(0)}) - e_1^{(0)}) \\
c_2 &= Com(r_0^{(2)} - t_1^{(2)}, F(r_0^{(2)}) - e_1^{(2)}) = Com(t_0^{(3)}, e_0^{(3)}) \\
c_3 &= Com(t_1^{(0)}, e_1^{(0)}) = Com(t_1^{(2)}, e_1^{(2)}) = Com(r_0^{(3)} - t_0^{(3)}, F(r_0^{(3)}) - e_0^{(3)}) \\
c_4 &= Com(d_0^{(0)}, u_0^{(0)}) = Com(d_0^{(2)}, u_0^{(2)}) = Com(d_0^{(3)}, u_0^{(3)}) \\
c_5 &= Com(d_1^{(0)}, u_1^{(0)}) = Com(d_1^{(3)}, u_1^{(3)}) \\
c_6 &= Com(r_1^{(0)} - d_0^{(0)} - d_1^{(0)}, F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)}) = Com(d_2^{(2)}, u_2^{(2)})
\end{aligned}
$$

elde edilir. Com şeması bağlama özelliğine sahip olduğu için; $r_0^{(2)} = r_0^{(3)}$, $r_0^{(2)} - t_1^{(2)} = t_0^{(3)}$, $F(r_0^{(2)}) - e_1^{(2)} = e_0^{(3)}$, $t_1^{(0)} = t_1^{(2)} = r_0^{(3)} - t_0^{(3)}$, $e_1^{(0)} = e_1^{(2)} = F(r_0^{(3)}) - e_0^{(3)}$, $d_0^{(0)} = d_0^{(2)} = d_0^{(3)}$, $u_0^{(0)} = u_0^{(2)} = u_0^{(3)}$, $d_1^{(0)} = d_1^{(3)}$, $u_1^{(0)} = u_1^{(3)}$, $r_1^{(0)} - d_0^{(0)} - d_1^{(0)} = d_2^{(2)}$, $F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)} = u_2^{(2)}$ *eşitlikleri elde edilir. Eşitlik (3.8) düzenlendiğinde,*

$$v = G(r_0^{(2)}, d_0^{(2)} + d_2^{(2)}) + G(r_0^{(3)}, d_1^{(3)}) + F(r_0^{(2)}) + u_0^{(2)} + u_1^{(3)} + u_2^{(2)} \qquad (3.9)$$

elde edilmektedir. Eşitlik (3.9)'da, $r_0^{(2)}$ *yerine* $r_0^{(3)}$, $d_0^{(2)}$ *yerine* $d_0^{(0)}$, $d_2^{(2)}$ *yerine* $r_1^{(0)} - d_0^{(0)} - d_1^{(0)}$, $d_1^{(3)}$ *yerine* $d_1^{(0)}$, $u_0^{(2)}$ *yerine* $u_0^{(0)}$, $u_1^{(3)}$ *yerine* $u_1^{(0)}$ *ve* $u_2^{(2)}$ *yerine* $F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)}$ *yazılırsa* $v = G(r_0^{(3)}, d_0^{(0)} + r_1^{(0)} - d_0^{(0)} - d_1^{(0)}) + G(r_0^{(3)}, d_1^{(0)}) + F(r_0^{(3)}) + u_0^{(0)} + u_1^{(0)} + F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)}$ *elde edilmektedir. Tanım* 2.10. *kullanılarak* $v = G(r_0^{(3)}, r_1^{(0)} + d_0^{(0)} - d_0^{(0)} - d_1^{(0)} + d_1^{(0)}) + F(r_0^{(3)}) + u_0^{(0)} + u_1^{(0)} + F(r_1^{(0)}) - u_0^{(0)} - u_1^{(0)} = G(r_0^{(3)}, r_1^{(0)}) + F(r_0^{(3)}) + F(r_1^{(0)}) = F(r_0^{(3)} + r_1^{(0)})$ *sonucuna ulaşılmaktadır. Demek ki, s gizli anahtarı* $r_0^{(3)}$ *ve* $r_1^{(0)}$ *olacak şekilde iki parçaya ayrılmıştır.*

Durum 4: *s_4 kümesi için her bir c_i taahhüt değerlerini hesaplarsak;*

$$
\begin{aligned}
c_0 &= Com(r_0^{(2)}, v - G(r_0^{(2)}, d_0^{(2)} + d_2^{(2)}) - F(r_0^{(2)}) - u_0^{(2)} - u_2^{(2)}) \\
&= Com(r_0^{(3)}, G(r_0^{(3)}, d_1^{(3)}) + u_1^{(3)}) \qquad (3.10) \\
c_1 &= Com(r_1^{(1)}, G(t_0^{(1)}, r_1^{(1)}) + e_0^{(1)}) \\
c_2 &= Com(t_0^{(1)}, e_0^{(1)}) = Com(r_0^{(2)} - t_1^{(2)}, F(r_0^{(2)}) - e_1^{(2)}) = Com(t_0^{(3)}, e_0^{(3)}) \\
c_3 &= Com(t_1^{(2)}, e_1^{(2)}) = Com(r_0^{(3)} - t_0^{(3)}, F(r_0^{(3)}) - e_0^{(3)}) \\
c_4 &= Com(d_0^{(1)}, u_0^{(1)}) = Com(d_0^{(2)}, u_0^{(2)}) = Com(d_0^{(3)}, u_0^{(3)}) \\
c_5 &= Com(r_1^{(1)} - d_0^{(1)} - d_2^{(1)}, F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)}) = Com(d_1^{(3)}, u_1^{(3)}) \\
c_6 &= Com(d_2^{(1)}, u_2^{(1)}) = Com(d_2^{(2)}, u_2^{(2)})
\end{aligned}
$$

elde edilir. Com şeması bağlama özelliğine sahip olduğu için; $r_0^{(2)} = r_0^{(3)}$, $t_0^{(1)} = r_0^{(2)} - t_1^{(2)} = t_0^{(3)}$, $e_0^{(1)} = F(r_0^{(2)}) - e_1^{(2)} = e_0^{(3)}$, $t_1^{(2)} = r_0^{(3)} - t_0^{(3)}$, $e_1^{(2)} = F(r_0^{(3)}) - e_0^{(3)}$, $d_0^{(1)} = d_0^{(2)} = d_0^{(3)}$, $u_0^{(1)} = u_0^{(2)} = u_0^{(3)}$, $r_1^{(1)} - d_0^{(1)} - d_2^{(1)} = d_1^{(3)}$, $F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)} = u_1^{(3)}$, $d_2^{(1)} = d_2^{(2)}$, $u_2^{(1)} = u_2^{(2)}$. *eşitlikleri elde edilir. Eşitlik (3.10) düzenlendiğinde,*

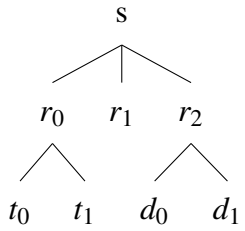
$$
v = G(r_0^{(2)}, d_0^{(2)} + d_2^{(2)}) + G(r_0^{(3)}, d_1^{(3)}) + F(r_0^{(2)}) + u_0^{(2)} + u_2^{(2)} + u_1^{(3)} \qquad (3.11)
$$

elde edilmektedir. Eşitlik (3.11)'de, $r_0^{(2)}$ *yerine* $r_0^{(3)}$, $u_0^{(2)}$ *yerine* $u_0^{(1)}$, $u_1^{(3)}$ *yerine* $F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)}$, $u_2^{(2)}$ *yerine* $u_2^{(1)}$, $d_1^{(3)}$ *yerine* $r_1^{(1)} - d_0^{(1)} - d_2^{(1)}$, $d_0^{(2)}$ *yerine* $d_0^{(1)}$ *ve* $d_2^{(2)}$ *yerine* $d_2^{(1)}$ *yazılırsa* $v = G(r_0^{(3)}, d_0^{(1)} + d_2^{(1)}) + G(r_0^{(3)}, r_1^{(1)} - d_0^{(1)} - d_2^{(1)}) + F(r_0^{(3)}) + u_0^{(1)} + F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)} + u_2^{(1)}$ *elde edilmektedir. Tanım* 2.10. *kullanılarak* $v = G(r_0^{(3)}, d_0^{(1)} + d_2^{(1)} + r_1^{(1)} - d_0^{(1)} - d_2^{(1)}) + F(r_0^{(3)}) + u_0^{(1)} + F(r_1^{(1)}) - u_0^{(1)} - u_2^{(1)} + u_2^{(1)} = G(r_0^{(3)}, r_1^{(1)}) + F(r_0^{(3)}) + F(r_1^{(1)}) = F(r_0^{(3)} + r_1^{(1)})$*sonucuna ulaşılmaktadır. Buradan s gizli anahtarının* $r_0^{(3)}$ *ve* $r_1^{(1)}$ *olacak şekilde iki parçaya ayrıldığı görülmektedir.*

İspat, verilen 4 *durumdan en az* 3 *tanesine doğru bir şekilde cevap veren bir kişinin gizli anahtara ulaşabileceğini ya da ikinci dereceden çok değişkenli sistemini çözebileceğini göstermektedir. Önerilen kimlik doğrulama şemasında sahtekar ispatlayıcı, gerçek ispatlayıcıyı* $1/2$ *olasılıkla taklit edebilmektedir veya çok düşük bir ihtimal ile doğrulayıcıyı kandırabilmektedir. Bu bakımdan önerilen kimlik doğrulama şeması sağlamlık özelliğine sahiptir.*

3.2. (3;2-1-2) Parçalanışa Sahip Yeni Kimlik Doğrulama Şeması

Bu kısımda (3;2-1-2) parçalanışa sahip ikinci dereceden çok değişkenli polinom sistemine dayanan üç aşamalı yeni bir kimlik doğrulama şeması önerilmiştir. Önerilen şema için gizli anahtarın parçalarının şematik gösterimi Şekil 3.4.'te verilmektedir.



Şekil 3.4. Gizli anahtarın (3;2-1-2) şeklinde parçalanması

Önerilen kimlik doğrulama şemasında s gizli anahtarı ilk parçalanışta üç parçaya ayrılmaktadır. Bu yönüyle literatürdeki ikinci dereceden çok değişkenli polinomlara dayanan kimlik doğrulama şemalarından farklılık göstermektedir. s gizli anahtarı başlangıçta üç parçaya ayrılarak beş alt parçanın toplamı olarak ifade edilmektedir. Bunun yanı sıra, $F(r_0)$ ve $F(r_1)$'da sırasıyla e_0, e_1 ve u_0, u_1 olacak şekilde iki parçaya bölünmektedir.

3.2.1. Şemanın doğrulanması

Kimlik doğrulama şemasında ikinci dereceden çok değişkenli polinom sistemleri kullanıldığı için Tanım 2.10.'da ifade edilen polar form kullanılmıştır.

Eşitlik (3.12) ve (3.13) sağlandığı sürece doğrulayıcı ispatlayıcının kimliğini doğrulayabilmektedir.

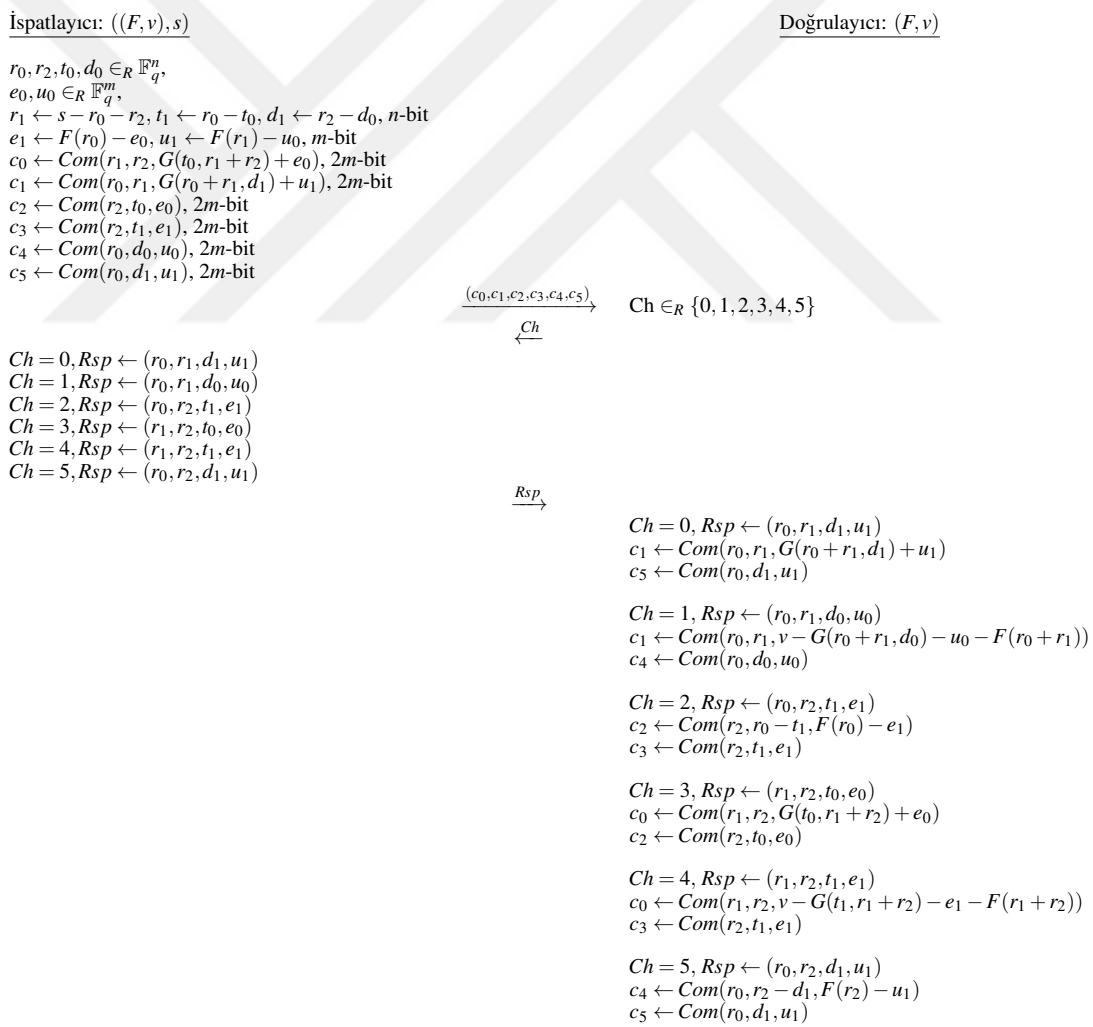
$$G(t_0, r_1 + r_2) + e_0 = v - G(t_1, r_1 + r_2) - e_1 - F(r_1 + r_2) \tag{3.12}$$

$$G(r_0 + r_1, d_1) + u_1 = v - G(r_0 + r_1, d_0) - u_0 - F(r_0 + r_1) \tag{3.13}$$

Tanım 2.10. ve Tanım 2.11. kullanılarak şemanın doğruluğu aşağıdaki gibi ispatlanmaktadır.

$$
\begin{aligned}
v &= G(r_0+r_1, d_0+d_1) + F(r_0+r_1) + u_0 + u_1 \\
&= G(r_0+r_1, r_2) + F(r_0+r_1) + F(r_2) \\
&= F(r_0+r_1+r_2) = F(s) \\
v &= G(t_0+t_1, r_1+r_2) + e_0 + e_1 + F(r_1+r_2) \\
&= G(r_0, r_1+r_2) + F(r_0) + F(r_1+r_2) \\
&= F(r_0+r_1+r_2) = F(s)
\end{aligned}
$$

Önerilen üç aşamalı sıfır bilgi paylaşımlı kimlik doğrulama şeması Şekil 3.5.'te verilmiştir.



Şekil 3.5. (3;2-1-2) parçalanışa sahip yeni kimlik doğrulama şeması

Kimlik doğrulama şeması başlamadan önce ispatlayıcı çok değişkenli polinom sistemini ve anahtar çiftlerini elde etmek için bazı algoritmalar kullanmaktadır. İspatlayıcı başlangıç ve anahtar üretme algoritmalarını çalıştırarak $F \in MQ(n,m,\mathbb{F}_q,k)$ polinom sistemini, s gizli anahtar ve $v = F(s)$ açık anahtar olmak üzere (v,s) anahtar çiftini elde etmektedir. Bu aşamadan sonra ispatlayıcı gizli anahtarını parçalayarak doğrulayıcıya taahhütte bulunabilmek için taahhüt değerlerini hesaplamaktadır. İspatlayıcı rastgele olarak $r_0, r_2, t_0, d_0 \in \mathbb{F}_q^n$ ve $e_0, u_0 \in \mathbb{F}_q^m$ değerlerini seçmektedir. Seçtiği değerleri kullanarak taahhüt değerlerini elde edebilmek için diğer parçalanışları $r_1 = s - r_0 - r_2,\ t_1 = r_0 - t_0,\ d_1 = r_2 - d_0,\ e_1 = F(r_0) - e_0$ ve $u_1 = F(r_2) - u_0$ hesaplamaktadır. Elinde bütün parçaları bulunduran ispatlayıcının taahhüt değerlerini hesaplayarak bu değerleri doğrulayıcıya taahhüt olarak göndermesi ile birlikte kimlik doğrulama şeması başlamış olmaktadır. Taahhüdü alan doğrulayıcı $Ch \in \{0,1,2,3,4,5\}$ meydan okuma değerini seçerek ispatlayıcıya meydan okumaktadır. İspatlayıcı ise doğrulayıcının seçtiği Ch değerine karşılık gelen Rsp cevapları doğrulayıcıya göndermektedir. Meydan okumanın cevabını alan doğrulayıcı taahhüt değerlerini kendisi hesaplayabilmektedir. İspatlayıcının gönderdiği taahhüt değeri ile kendi hesapladığı taahhüt değeri birbirine eşit ise doğrulayıcı ispatlayıcının taahhüdünü kabul etmekte ve kimliğini doğrulamaktadır. Aksi takdirde, reddetmektedir. Kimlik doğrulama şemasının sonunda doğrulayıcı gizli anahtarın ne olduğunu bilmeden taahhüdü kabul etmektedir. Bu bakımdan kimlik doğrulama şeması sıfır bilgi paylaşımına dayanmaktadır.

3.2.2. Özelliklerin sağlanması

Kimlik doğrulama şemasının Teorem 3 ve Teorem 4 ile verilen özellikleri sağlaması gerekmektedir.

Teorem 3 *Com taahhüt şeması istatistiksel saklama özelliğine sahip ise oluşturulan kimlik doğrulama şeması istatistiksel olarak sıfır bilgi paylaşımlıdır.*

***İspat* 3** *Kabul edelim ki, S, (F,v)'yi bilen fakat gizli anahtarın ne olduğunu bilmeyen sahte doğrulayıcı ile iletişime geçebilen ve $1/3$ olasılıkla kopya bir iletişim oluşturabilen bir simülatör olsun. S simülatör, gizli anahtar ve parçaları için*

$s', r'_0, r'_2, t'_0, d'_0 \in_R \mathbb{F}_q^n$ *ve* $e'_0, u'_0 \in_R \mathbb{F}_q^m$ *değerlerini seçerek* $r'_1 \leftarrow s' - r'_0 - r'_2$, $t'_1 \leftarrow r'_0 - t'_0$, $d'_1 \leftarrow r'_2 - d'_0$ *değerlerini hesaplamaktadır.*

S, sahtekar doğrulayıcının seçemeyeceği bir $Ch^* \in_R \{0,1\}$ *değerini seçmektedir. S'nin sırasıyla* $Ch^* = 0$ *veya* $Ch^* = 1$ *değerini seçmesi sahtekar doğrulayıcının meydan okuma değerinin* $Ch \in \{3,4,5\}$ *veya* $Ch \in \{0,1,2\}$ *olduğunu ifade etmektedir. S'nin kalan parçaları hesaplayabilmek için iki farklı seçeneği vardır. Simülatör S, seçtiği* Ch^* *meydan okuma değerine göre*

$$Ch^* = \begin{cases} 0, & \begin{cases} u'_1 \leftarrow v - F(s') + F(r'_2) - u'_0 \\ e'_1 \leftarrow F(r'_0) - e'_0 \end{cases} \\ aksidurumda, & \begin{cases} u'_1 \leftarrow F(r'_2) - u'_0 \\ e'_1 \leftarrow v - F(s') + F(r'_0) - e'_0 \end{cases} \end{cases}$$

e_1 *ve* u_1 *değerlerini hesaplamaktadır. S, gizli anahtarın parçalarının tamamını elde ettikten sonra*

$$c'_0 \leftarrow Com(r'_1, r'_2, G(t'_0, r'_1 + r'_2) + e'_0),$$

$$c'_1 \leftarrow Com(r'_0, r'_1, G(r'_0 + r'_1, d'_1) + u'_1),$$

$$c'_2 \leftarrow Com(r'_2, t'_0, e'_0),$$

$$c'_3 \leftarrow Com(r'_2, t'_1, e'_1),$$

$$c'_4 \leftarrow Com(r'_0, d'_0, u'_0)$$

$$c'_5 \leftarrow Com(r'_0, d'_1, u'_1)$$

taahhüt değerlerini hesaplayarak doğrulayıcıya göndermektedir. Taahhüdü alan doğrulayıcı, dürüst ispatlayıcı gibi davranabilen S'ye meydan okumaktadır. S hesapladığı taahhüt değerlerini doğrulayıcının da hesaplayabilmesi amacıyla meydan okumanın değerine göre

$$Ch = \begin{cases} 0, & Rsp \leftarrow (r'_0, r'_1, d'_1, u'_1) \\ 1, & Rsp \leftarrow (r'_0, r'_1, d'_0, u'_0) \\ 2, & Rsp \leftarrow (r'_0, r'_2, t'_1, e'_1) \\ 3, & Rsp \leftarrow (r'_1, r'_2, t'_0, e'_0) \\ 4, & Rsp \leftarrow (r'_1, r'_2, t'_1, e'_1) \\ 5, & Rsp \leftarrow (r'_0, r'_2, d'_1, u'_1) \end{cases}$$

cevap kümelerinden ilgili olanı doğrulayıcıya göndermektedir. Com istatistiksel

saklama özelliğine sahip olduğu için Ch sahtekar doğrulayıcının gönderdiği meydan okuma değeri Ch^* *simülatörün seçtiği meydan okuma değerinden* $1/3$ *olasılıkla farklıdır.* $Ch^* = 1$ *ve* $Ch = 1$ *olması durumunda* $u'_1 \leftarrow v - F(s') + F(r'_2) - u'_0$ *elde edilmektedir.* $v - G(r_0 + r_1, d_1) + u_1 = v - G(r_0 + r_1, d_0) - u_0 - F(r_0 + r_1)$ *eşitliği şemadan elde edildiğinde* c_1 *taahhüt değeri doğrulanmış olmaktadır. Diğer durumda* $Ch^* = 1$ *ve* $Ch = 0$ *veya* $Ch = 2$ *olması durumda v açık anahtar kullanılmadığından doğrulama işlemi daha kolay olmaktadır.* $Ch^* = 0$ *ve* $Ch \in \{3,4,5\}$ *olduğunda ise benzer durumlar söz konusudur. S simülatörünü kullanan bir sahte ispatlayıcı gerçek şemanın kopyasını oluşturabilir. Fakat Com taahhüt şeması saklama özelliğine sahip olursa üçüncü bir şahıs şema hakkında bilgi edinemez. Başka bir ifadeyle, oluşturulan kimlik doğrulama şeması sıfır bilgi paylaşımlıdır.*

Teorem 4 *Com taahhüt şemasının hesaplamalı bağlayıcı olduğu durumda her bir döngüde hesaplamalı olarak* $1/3$ *hata olasığı vardır.*

***İspat* 4** *Bu teorem iki farklı şekilde ispatlanabilmektedir. Teoremin ispatında meydan okuma ve cevap değerlerine göre altı durum söz konusudur. 1. yöntemde altı farklı durum bir durum gibi düşünülerek ispat yapılmaktadır.*

1. Yöntem: *Kabul edelim ki, C bütün meydan okumalara cevap verebilen sahtekar bir ispatlayıcı olsun. Bu özelliğe sahip C, Com taahhüt fonksiyonu için çakışmayı hesaplayabilir veya* (F,v) *için bir çözüm bulabilir.* $Ch_i = i$ *olmak üzere ispatlayıcının gönderdiği cevapların doğrulayıcı tarafından kabul edildiği varsayılarak şemada kullanılan taahhüt değeri, meydan okuma ve cevaplar*

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_0, Rsp_0)$,

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_1, Rsp_1)$,

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_2, Rsp_2)$,

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_3, Rsp_3)$,

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_4, Rsp_4)$,

$((c_0,c_1,c_2,c_3,c_4,c_5), Ch_5, Rsp_5)$

şeklinde 6 *adet şema kümesi ile gösterilsin. Bütün cevapların*

$$Rsp_0 = (r_0^{(0)}, r_1^{(0)}, d_1^{(0)}, u_1^{(0)}),$$
$$Rsp_1 = (r_0^{(1)}, r_1^{(1)}, d_0^{(1)}, u_0^{(1)}),$$
$$Rsp_2 = (r_0^{(2)}, r_2^{(2)}, t_1^{(2)}, e_1^{(2)}),$$
$$Rsp_3 = (r_1^{(3)}, r_2^{(3)}, t_0^{(3)}, e_0^{(3)}),$$
$$Rsp_4 = (r_1^{(4)}, r_2^{(4)}, t_1^{(4)}, e_1^{(4)}),$$
$$Rsp_5 = (r_0^{(5)}, r_2^{(5)}, d_1^{(5)}, u_1^{(5)})$$

olarak doğrulayıcı tarafından kabul edildiği bir durumda:

$$\begin{aligned}
c_0 &= Com(r_1^{(3)}, r_2^{(3)}, G(t_0^{(3)}, r_1^{(3)} + r_2^{(3)}) + e_0^{(3)}) \\
&= Com(r_1^{(4)}, r_2^{(4)}, v - G(t_1^{(4)}, r_1^{(4)} + r_2^{(4)}) - e_1^{(4)} - F(r_1^{(4)} + r_2^{(4)}) && (3.14) \\
c_1 &= Com(r_0^{(0)}, r_1^{(0)}, G(r_0^{(0)} + r_1^{(0)}, d_1^{(0)}) + u_1^{(0)}) \\
&= Com(r_0^{(1)}, r_1^{(1)}, v - G(r_0^{(1)} + r_1^{(1)}, d_0^{(1)}) - u_0^{(1)} - F(r_0^{(1)} + r_1^{(1)})) && (3.15) \\
c_2 &= Com(r_2^{(2)}, r_0^{(2)} - t_1^{(2)}, F(r_0^{(2)}) - e_1^{(2)}) \\
&= Com(r_2^{(3)}, t_0^{(3)}, e_0^{(3)}) \\
c_3 &= Com(r_2^{(2)}, t_1^{(2)}, e_1^{(2)}) \\
&= Com(r_2^{(4)}, t_1^{(4)}, e_1^{(4)}) \\
c_4 &= Com(r_0^{(1)}, d_0^{(1)}, u_0^{(1)}) \\
&= Com(r_0^{(5)}, r_2^{(5)} - d_1^5, F(r_2^{(5)}) - u_1^{(5)}) \\
c_5 &= Com(r_0^{(0)}, d_1^{(0)}, u_1^{(0)}) \\
&= Com(r_0^{(5)}, d_1^{(5)}, u_1^{(5)})
\end{aligned}$$

eşitlikleri elde edilmektedir. Com şeması bağlama özelliğine sahip olduğu için; $r_1^{(3)} = r_1^{(4)}$, $r_1^{(0)} = r_1^{(1)}$, $r_0^{(0)} = r_0^{(1)} = r_0^{(5)}$, $r_2^{(2)} = r_2^{(3)} = r_2^{(4)}$, $d_1^{(0)} = d_1^{(5)}$, $u_1^{(0)} = u_1^{(5)}$, $d_0^{(1)} = r_2^{(5)} - d_1^{(5)}$, $u_0^{(1)} = F(r_2^{(5)}) - u_1^{(5)}$, $t_1^{(2)} = t_1^{(4)}$, $e_0^{(3)} = F(r_0^{(2)}) - e_1^2$, $e_1^{(2)} = e_1^{(4)}$, $t_0^{(3)} = r_0^{(2)} - t_1^{(2)}$ *eşitlikleri elde edilmektedir. Eşitlik (3.14)'ten;*

$$v = G(t_0^{(3)}, r_1^{(3)} + r_2^{(3)}) + G(t_1^{(4)}, r_1^{(4)} + r_2^{(4)}) + e_0^{(3)} + e_1^{(4)} + F(r_1^{(4)} + r_2^{(4)}) \qquad (3.16)$$

elde edilmektedir. Eşitlik (3.16)'da $t_0^{(3)}$ *yerine* $r_0^{(2)} - t_1^{(2)}$, $t_1^{(4)}$ *yerine* $t_1^{(2)}$, $e_0^{(3)}$ *yerine* $F(r_0^{(2)}) - e_1^{(2)}$, $e_1^{(4)}$ *yerine* $e_1^{(2)}$ *yazılırsa* $v = G(r_0^{(2)}, r_1^{(4)} + r_2^{(4)}) + F(r_0^{(2)}) + F(r_1^{(4)} + r_2^{(4)})$ *elde edilir. Tanım* 2.10.*'daki polar form kullanıldığında* $v = F(r_0^{(2)} + r_1^{(4)} + r_2^{(4)}) = F(s)$

olacak şekilde bir çözüm elde edilmektedir. İspat gösteriyor ki, iletişim kümelerinden hepsine doğru bir şekilde cevap verebilen bir kişi v açık anahtarı için elde etmek için bir s çözümü bulabilmektedir.

Gizli anahtarın r_2 parçasının alt parçalara ayrıldığı durum için ispat yapılırsa Eşitlik (3.15)'ten;

$$v = G(r_0^{(0)} + r_1^{(0)}, d_1^{(0)}) + G(r_0^{(1)} + r_1^{(1)}, d_0^{(1)}) + u_0^{(1)} + u_1^{(0)} + F(r_0^{(1)} + r_1^{(1)}) \qquad (3.17)$$

elde edilmektedir. Eşitlik (3.17)'de $d_0^{(1)}$ yerine $r_2^{(5)} - d_1^{(5)}$, $d_1^{(0)}$ yerine $d_1^{(5)}$, $u_0^{(1)}$ yerine $F(r_2^{(5)}) - u_1^{(5)}$, $u_1^{(0)}$ yerine $u_1^{(5)}$,$r_1^{(0)}$ yerine $r_1^{(1)}$, $r_0^{(1)}$ yerine $r_0^{(0)}$ yazılırsa $v = G(r_0^{(0)} + r_1^{(1)}, r_2^{(5)}) + F(r_2^{(5)}) + F(r_0^{(0)} + r_1^{(1)})$ elde edilir. Tanım 2.10.'daki polar form kullanıldığında $v = F(r_0^{(0)} + r_1^{(1)} + r_2^{(5)}) = F(s)$ olacak şekilde bir çözüm elde edilmektedir. İspat gösteriyor ki, iletişim kümelerinden hepsine doğru bir şekilde cevap verebilen bir kişi v açık anahtarına ulaşmak için bir s çözümü bulabilmektedir. Önerilen kimlik doğrulama şemasında sahtekar ispatlayıcı, gerçek ispatlayıcıyı $1/3$ olasılıkla taklit edebilmektedir veya çok düşük bir ihtimal ile doğrulayıcıyı kandırabilmektedir. Bu bakımdan önerilen kimlik doğrulama şeması sağlamlık özelliğine sahiptir.

Bütün meydan okumalara doğru cevabı verebilen sahtekar ispatlayıcı Eşitlik (3.14) ve Eşitlik (3.15) kullanılarak s gizli anahtarı için çözüme ulaşabilmektedir.

2. Yöntem: *$Ch_i = i$ olmak üzere doğrulayıcı dürüst ispatlayıcının iddiasını kabul ederse karar fonksiyonu $Dec(F, v, hc_i, Ch_i, Rsp_i) = 1$ olmaktadır. Bu bakımdan*

$s_1 = \{(C_1, Ch_1, Rsp_1), (C_2, Ch_2, Rsp_2), (C_3, Ch_3, Rsp_3), (C_4, Ch_4, Rsp_4), (C_5, Ch_5, Rsp_5),$
$s_2 = \{(C_0, Ch_0, Rsp_0), (C_1, Ch_1, Rsp_1), (C_2, Ch_2, Rsp_2), (C_3, Ch_3, Rsp_3), (C_5, Ch_5, Rsp_5),$
$s_3 = \{(C_0, Ch_0, Rsp_0), (C_1, Ch_1, Rsp_1), (C_2, Ch_2, Rsp_2), (C_3, Ch_3, Rsp_3), (C_4, Ch_4, Rsp_4),$
$s_4 = \{(C_0, Ch_0, Rsp_0), (C_2, Ch_2, Rsp_2), (C_3, Ch_3, Rsp_3), (C_4, Ch_4, Rsp_4), (C_5, Ch_5, Rsp_5),$
$s_5 = \{(C_0, Ch_0, Rsp_0), (C_1, Ch_1, Rsp_1), (C_3, Ch_3, Rsp_3), (C_4, Ch_4, Rsp_4), (C_5, Ch_5, Rsp_5),$
$s_6 = \{(C_0, Ch_0, Rsp_0), (C_1, Ch_1, Rsp_1), (C_2, Ch_2, Rsp_2), (C_4, Ch_4, Rsp_4), (C_5, Ch_5, Rsp_5).$

doğrulayıcı tarafından kabul edilebilecek taahhüt, meydan okuma ve cevapları içeren altı farklı durum kümesi olsun. $i \in \{0,1,2,3,4,5\}$ ve $C_0 = C_1 = C_2 = C_3 = C_4 = C_5$ olmak üzere her bir C_i değeri $(c_0, c_1, c_2, c_3, c_4, c_5)$ taahhüt değerlerini göstermek üzere $Rsp_0 = (r_0^{(0)}, r_1^{(0)}, d_1^{(0)}, u_1^{(0)})$, $Rsp_1 = (r_0^{(1)}, r_1^{(1)}, d_0^{(1)}, u_0^{(1)})$, $Rsp_2 = (r_0^{(2)}, r_2^{(2)}, t_1^{(2)}, e_1^{(2)})$,

$Rsp_3 = (r_1^{(3)}, r_2^{(3)}, t_0^{(3)}, e_0^{(3)})$, $Rsp_4 = (r_1^{(4)}, r_2^{(4)}, t_1^{(4)}, e_1^{(4)})$ *ve* $Rsp_5 = (r_0^{(5)}, r_2^{(5)}, d_1^{(5)}, u_1^{(5)})$ *meydan okumaları belirtsin.*

Durum 1: s_1 *kümesi için her bir* c_i *taahhüt değerlerini hesaplarsak;*

$$\begin{aligned}
c_0 &= Com(r_1^{(3)}, r_2^{(3)}, G(t_0^{(3)}, r_1^{(3)} + r_2^{(3)}) + e_0^{(3)}) \\
&= Com(r_1^{(4)}, r_2^{(4)}, v - G(t_1^{(4)}, r_1^{(4)} + r_2^{(4)}) - e_1^{(4)} - F(r_1^{(4)} + r_2^{(4)}) \\
c_1 &= Com(r_0^{(1)}, r_1^{(1)}, v - G(r_0^{(1)} + r_1^{(1)}, d_0^{(1)}) - u_0^{(1)} - F(r_0^{(1)} + r_1^{(1)})) \\
c_2 &= Com(r_2^{(2)}, r_0^{(2)} - t_1^{(2)}, F(r_0^{(2)}) - e_1^{(2)}) \\
&= Com(r_2^{(3)}, t_0^{(3)}, e_0^{(3)}) \\
c_3 &= Com(r_2^{(2)}, t_1^{(2)}, e_1^{(2)}) \\
&= Com(r_2^{(4)}, t_1^{(4)}, e_1^{(4)}) \\
c_4 &= Com(r_0^{(1)}, d_0^{(1)}, u_0^{(1)}) \\
&= Com(r_0^{(5)}, r_2^{(5)} - d_1^5, F(r_2^{(5)}) - u_1^{(5)}) \\
c_5 &= Com(r_0^{(5)}, d_1^{(5)}, u_1^{(5)})
\end{aligned} \tag{3.18}$$

elde edilmektedir. Com şeması bağlama özelliğine sahip olduğu için; $r_1^{(3)} = r_1^{(4)}$, $r_0^{(1)} = r_0^{(5)}$, $r_2^{(2)} = r_2^{(3)} = r_2^{(4)}$, $d_0^{(1)} = r_2^{(5)} - d_1^{(5)}$, $u_0^{(1)} = F(r_2^{(5)}) - u_1^{(5)}$, $t_1^{(2)} = t_1^{(4)}$, $e_0^{(3)} = F(r_0^{(2)}) - e_1^{(2)}$, $e_1^{(2)} = e_1^{(4)}$, $t_0^{(3)} = r_0^{(2)} - t_1^{(2)}$ *eşitlikleri elde edilmektedir. Eşitlik (3.18) düzenlendiğinde;*

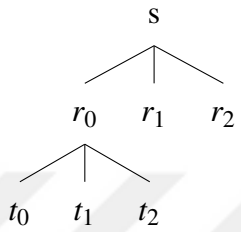
$$v = G(t_0^{(3)}, r_1^{(3)} + r_2^{(3)}) + G(t_1^{(4)}, r_1^{(4)} + r_2^{(4)}) + e_0^{(3)} + e_1^{(4)} + F(r_1^{(4)} + r_2^{(4)}) \tag{3.19}$$

elde edilmektedir. Eşitlik (3.19)'da $t_0^{(3)}$ *yerine* $r_0^{(2)} - t_1^{(2)}$, $t_1^{(4)}$ *yerine* $t_1^{(2)}$, $e_0^{(3)}$ *yerine* $F(r_0^{(2)}) - e_1^{(2)}$, $e_1^{(4)}$ *yerine* $e_1^{(2)}$ *yazılırsa* $v = G(r_0^{(2)}, r_1^{(4)} + r_2^{(4)}) + F(r_0^{(2)}) + F(r_1^{(4)} + r_2^{(4)})$ *elde edilir. Tanım* 2.10.*'daki polar form kullanıldığında* $v = F(r_0^{(2)} + r_1^{(4)} + r_2^{(4)}) = F(s)$ *olacak şekilde bir çözüm elde edilmektedir. Dikkat edilecek olursa elde edilen çözümün birinci yöntem ile aynı olduğu görülmektedir.*

Açıklama 2 *Kalan beş farklı durum kümesi için benzer işlemler yapılırsa s gizli anahtarı için farklı çözümler bulunabilmektedir. Diğer durumlar için ispat burada verilmemiştir.*

3.3. (3;3-1-1) Parçalanışa Sahip Yeni Kimlik Doğrulama Şeması

Önerilen kimlik doğrulama şeması Akleylek ve Soysaldı (2018b) çalışmasında yer almaktadır. Üçüncü dereceden çok değişkenli polinomlara dayanan sıfır bilgi paylaşımlı üç aşamalı yeni bir kimlik doğrulama şeması önerilmiştir. Önerilen şema Nachef vd (2012) çalışmasındaki parçalama tekniği geliştirilerek oluşturulmuştur. Yeni kimlik doğrulama şemasında gizli anahtar Şekil 3.6.'da verildiği üzere (3;3-1-1) parçalanış yapısına göre parçalara ayrılmaktadır. Şemada s gizli anahtarı r_0, r_1 ve r_2



Şekil 3.6. Gizli anahtarın (3;3-1-1) şeklinde parçalanması

şeklinde üç parçaya ayrılmaktadır. Parçalama fikrinin devamında r_0 parçası da t_0, t_1 ve t_2 olacak şekilde üç parçayla temsil edilmektedir.

3.3.1. Şemanın doğrulanması

Üçüncü dereceden çok değişkenli polinomlara dayanan bir kimlik doğrulama şeması oluşturulacağından Bölüm 2'de verilen Eşitlik (2.5)'teki üçlü doğrusallık özelliğine sahip polar form kullanılmıştır.

Gizli anahtarın parçası olan r_0 alt parçalara ayrıldığı için polar formda bu parçanın yer aldığı $F(r_0) = e_0 + e_1 + e_2$, $F(r_0 + r_1) = f_0 + f_1 + f_2$ ve $F(r_0 + r_2) = h_0 + h_1 + h_2$ şeklinde farklı değişkenlerle ifade edilmektedir.

Eşitlik (3.20) sağlandığı sürece doğrulayıcı ispatlayıcının kimliğini doğrulayabilmektedir.

$$v - G(t_2, r_1, r_2) + e_2 - f_2 - h_2 + F(r_1) + F(r_2) = G(t_0 + t_1, r_1, r_2) + f_0 + f_1 + h_0 + h_1 + F(r_1 + r_2) - e_0 - e_1 \tag{3.20}$$

Tanım 2.13.'te verilen Eşitlik (2.5)'teki polar form ve gizli anahtar parçaları kullanılarak şemanın doğruluğu

$$v = G(t_0+t_1, r_1, r_2) + G(t_2, r_1, r_2) + f_0 + f_1 + f_2 + h_0 + h_1 + h_2 + F(r_1+r_2) - e_0 - e_1$$
$$- e_2 - F(r_1) - F(r_2)$$
$$v = G(t_0+t_1, r_1, r_2) + G(t_2, r_1, r_2) + f_0 + f_1 + f_2 + h_0 + h_1 + h_2 + F(r_1+r_2) - e_0 - e_1$$
$$v = G(t_0+t_1+t_2, r_1, r_2) + F(r_0+r_1) + F(r_0+r_2) + F(r_1+r_2) - F(r_0) - F(r_1) - F(r_2)$$
$$v = G(r_0, r_1, r_2) + F(r_0+r_1) + F(r_0+r_2) + F(r_1+r_2) - F(r_0) - F(r_1) - F(r_2)$$
$$v = F(r_0+r_1+r_2)$$
$$v = F(s)$$

şeklinde ispatlanmaktadır.

Önerilen üçüncü dereceden çok değişkenli polinomlara dayanan üç aşamalı kimlik doğrulama şeması Şekil 3.7.'de verilmiştir.

Kimlik doğrulama şemasının başında ispatlayıcı başlangıç ve anahtar üretme algoritmalarını çalıştırarak $F \in MC(n, m, \mathbb{F}_q, k)$ polinom sistemini, s gizli anahtar ve $v = F(s)$ açık anahtar olmak üzere (v, s) anahtar çiftini elde etmektedir. Bu aşamadan sonra ispatlayıcı gizli anahtarını parçalayarak doğrulayıcıya taahhütte bulunabilmek için taahhüt değerlerini hesaplamaktadır. İspatlayıcı rastgele olarak $r_0, r_1, t_0, t_1 \in \mathbb{F}_q^n$ ve $e_0, e_1, f_0, f_1, h_0, h_1 \in \mathbb{F}_q^m$ değerlerini seçmektedir. Seçtiği değerleri kullanarak taahhüt değerlerini elde edebilmek için diğer parçalanışları $r_2 = s - r_0 - r_1$, $t_2 = r_0 - t_0 - t_1$, $e_2 = F(r_0) - e_0 - e_1$, $f_2 = F(r_0+r_1) - f_0 - f_1$ ve $h_2 = F(r_0+r_2) - h_0 - h_1$ hesaplamaktadır. Elinde bütün parçaları bulunduran ispatlayıcının taahhüt değerlerini hesaplayarak bu değerleri doğrulayıcıya taahhüt olarak göndermesi ile birlikte kimlik doğrulama şeması başlamış olmaktadır. Taahhüdü alan doğrulayıcı $Ch \in \{0,1,2,3\}$ meydan okuma değerini seçerek ispatlayıcıya meydan okumaktadır. İspatlayıcı ise doğrulayıcının seçtiği Ch değerine karşılık gelen Rsp cevapları doğrulayıcıya göndermektedir. Meydan okumanın cevabını alan doğrulayıcı taahhüt değerlerini kendisi de hesaplayabilmektedir. İspatlayıcının gönderdiği taahhüt değeri ile kendi hesapladığı taahhüt değeri birbirine eşit ise doğrulayıcı ispatlayıcının taahhüdünü kabul etmekte ve kimliğini doğrulamaktadır. Aksi takdirde, reddetmektedir. Kimlik doğrulama şemasının sonunda doğrulayıcı gizli anahtarın ne olduğunu bilmeden

Şekil 3.7. (3;3-1-1) parçalanışa sahip yeni kimlik doğrulama şeması

taahhüdü kabul etmektedir. Bu bakımdan kimlik doğrulama şeması sıfır bilgi paylaşımına dayanmaktadır.

3.3.2. Özelliklerin sağlanması

Kimlik doğrulama şemasının Teorem 5 ve Teorem 6 ile verilen özellikleri sağlaması gerekmektedir.

Teorem 5 *Com taahhüt şeması istatistiksel saklama özelliğine sahip ise oluşturulan kimlik doğrulama şeması istatistiksel olarak sıfır bilgi paylaşımlıdır.*

İspat 5 *S, (F,v)'yi bilen fakat gizli anahtarın ne olduğunu bilmeyen sahte doğrulayıcı ile iletişime geçebilen bir simülatör olsun. S simülatör, gizli anahtar ve parçaları için $s',r'_0,t'_0,t'_1 \in_R \mathbb{F}_q^n$ ve $e'_0,e'_1,f_0,f_1,h_0,h_1 \in_R \mathbb{F}_q^m$ değerlerini seçerek $r'_2 \leftarrow s' - r'_0 - r'_1$, $t'_2 \leftarrow r'_0 - t'_0 - t'_1$, $e'_2 \leftarrow F(r'_0) - e'_0 - e'_1$ değerlerini hesaplamaktadır. S, sahtekar doğrulayıcının seçemeyeceği bir $Ch^* \in_R \{0,1,3\}$ değerini seçmektedir. S diğer parçaları ve taahhüt değerlerini:*

$$Ch^* = \begin{cases} 0, & h'_2 = v - F(s') + F(r'_0 + r'_2) - h'_0 - h'_1 \\ \textit{aksi halde}, & h'_2 = F(r'_0 + r'_2) - h'_0 - h'_1 \end{cases}$$

$$Ch^* = \begin{cases} 1, & c'_0 = Com(r'_1, r'_2, v - G(t'_2, r'_1, r'_2) + e'_2 - f'_2 - h'_2 \\ & \quad + F(r'_1) + F(r'_2) \\ \textit{aksi halde}, & c'_0 = Com(r'_1, r'_2, G(t'_0 + t'_1, r'_1, r'_2) + f'_0 + f'_1 + h'_0 + h'_1 \\ & \quad + F(r'_1 + r'_2) - e'_0 - e'_1 \end{cases}$$

$$Ch^* = \begin{cases} 3 & , f'_2 = v - F(s') + F(r'_0 + r'_1) - f'_0 - f'_1 \\ \textit{aksi halde} & , f'_2 = F(r'_0 + r'_1) - f'_0 - f'_1 \end{cases}$$

Ch^*'in değerine bağlı olarak hesaplamaktadır. Bunun yanı sıra,

$$c'_1 = Com(r'_1, t'_0, e'_0, f'_0), \quad c'_2 = Com(r'_2, t'_0, e'_0, h'_0)$$
$$c'_3 = Com(r'_1, t'_1, e'_1, f'_1), \quad c'_4 = Com(r'_2, t'_1, e'_1, h'_1)$$
$$c'_5 = Com(r'_1, t'_2, e'_2, f'_2), \quad c'_6 = Com(r'_2, t'_2, e'_2, h'_2)$$

taahhüt değerlerini hesaplayarak sahtekar doğrulayıcıya göndermektedir. Sahtekar doğrulayıcıdan gelen meydan okuma değerine göre ispatlayıcı ile doğrulayıcı arasındaki taahhüt, meydan okuma ve cevap kümesi:

$$Ch = \begin{cases} 0, & ((c_0,c_1,c_2,c_3,c_4,c_5,c_6),\ 0,\ (r'_0,r'_2,t'_0,t'_2,e'_0,e'_2,h'_0,h'_2)) \\ 1, & ((c_0,c_1,c_2,c_3,c_4,c_5,c_6),\ 1,\ (r'_1,r'_2,t'_0,t'_2,e'_0,e'_2,f'_0,f'_1,h'_0,h'_1)) \\ 2, & ((c_0,c_1,c_2,c_3,c_4,c_5,c_6),\ 2,\ (r'_1,r'_2,t'_2,e'_2,f'_2,h'_2)) \\ 3, & ((c_0,c_1,c_2,c_3,c_4,c_5,c_6),\ 3,\ (r'_0,r'_1,t'_0,t'_2,e'_0,e'_2,f'_0,f'_2)) \end{cases}$$

şeklindedir. $Ch^* = 0$ ve $Ch = 2$ olması durumunda iletişimdeki değerler $((c_0,c_1,c_2,c_3,c_4,c_5,c_6),2,(r'_1,r'_2,t'_2,e'_2,f'_2,h'_2))$ olduğundan c'_5 ve c'_6 doğrulanmaktadır. c'_0 ise şu şekilde hesaplanmaktadır: $c'_0 = Com(r'_1, r'_2, v - G(t_2, r_1, r_2) + e_2 - f_2 - h_2 + F(r_1) + F(r_2))$ eşitliğinde f_2 yerine $v - F(s') + F(r'_0 + r'_1) - f'_0 - f'_1$ yazılırsa $c'_0 = Com(r_1, r_2, G(t_0 + t_1, r_1, r_2) + f_0 + f_1 + h_0 + h_1 + F(r_1 + r_2) - e_0 - e_1)$ elde edilmektedir. Bu da c'_0 değerini doğrulamaktadır. Benzer şekilde c'_1, c'_2, c'_3, c'_4 değerleri

de doğrulanmaktadır. S, $3/4$ *ihtimalle gerçek iletişim değerlerinden ayırt edilemeyecek şekilde kopya bir şema oluşturabilir. Fakat Com istatistiksel saklama özelliğine sahip olduğundan dolayı üçüncü kişiler şema hakkında önemli bilgileri elde edememektedir. Başka bir ifadeyle, oluşturulan kimlik doğrulama şeması sıfır bilgi paylaşımlıdır.*

Teorem 6 *Com taahhüt şemasının hesaplamalı bağlayıcı olduğu durumda her bir döngüde hesaplamalı olarak* $3/4$ *hata olasığı vardır.*

***İspat* 6** *Kabul edelim ki, C bütün meydan okumalara cevap verebilen sahtekar bir ispatlayıcı olsun. Bu özelliğe sahip C, Com taahhüt fonksiyonu için çakışmayı hesaplayabilir veya* (F,v) *için bir çözüm bulabilir.* $Ch_i = i$ *olmak üzere ispatlayıcının gönderdiği cevapların doğrulayıcı tarafından kabul edildiği varsayılarak şemada kullanılan taahhüt değeri, meydan okuma ve cevaplar*

$$((c_0,c_1,c_2,c_3,c_4,c_5,c_6),Ch_0,Rsp_0),$$

$$((c_0,c_1,c_2,c_3,c_4,c_5,c_6),Ch_1,Rsp_1),$$

$$((c_0,c_1,c_2,c_3,c_4,c_5,c_6),Ch_2,Rsp_2),$$

$$((c_0,c_1,c_2,c_3,c_4,c_5,c_6),Ch_3,Rsp_3)$$

şeklinde 4 *adet şema kümesi ile gösterilsin. Doğrulayıcı bütün cevapları*

$$Rsp_0 = (r_0^{(0)},r_2^{(0)},t_0^{(0)},t_2^{(0)},e_0^{(0)},e_2^{(0)},h_0^{(0)},h_2^{(0)}),$$
$$Rsp_1 = (r_1^{(1)},r_2^{(1)},t_0^{(1)},t_2^{(1)},e_0^{(1)},e_2^{(1)},f_0^{(1)},f_1^{(1)},h_0^{(1)},h_1^{(1)}),$$
$$Rsp_2 = (r_1^{(2)},r_2^{(2)},t_2^{(2)},e_2^{(2)},f_2^{(2)},h_2^{(2)})$$
$$Rsp_3 = (r_0^{(3)},r_1^{(3)},t_0^{(3)},t_2^{(3)},e_0^{(3)},e_2^{(3)},f_0^{(3)},f_2^{(3)})$$

olacak şekilde kabul ettiğinde:

$$
\begin{aligned}
c_0 &= Com(r_1^{(1)}, r_2^{(1)}, G(t_0^{(1)} + t_1^{(1)}, r_1^{(1)}, r_2^{(1)}) + f_0^{(1)} + f_1^{(1)} + h_0^{(1)} + h_1^{(1)} \\
&\quad + F(r_1^{(1)} + r_2^{(1)}) - e_0^{(1)} - e_1^{(1)}) \\
&\quad = Com(r_1^{(2)}, r_2^{(2)}, v - G(t_2^{(2)}, r_1^{(2)}, r_2^{(2)}) + e_2^{(2)} - f_2^{(2)} - h_2^{(2)} + F(r_1^{(2)}) + F(r_2^{(2)})) \\
c_1 &= Com(r_1^{(1)}, t_0^{(1)}, e_0^{(1)}, f_0^{(1)}) \\
&\quad = Com(r_1^{(3)}, t_0^{(3)}, e_0^{(3)}, f_0^{(3)} \\
c_2 &= Com(r_2^{(0)}, t_0^{(0)}, e_0^{(0)}, h_0^{(0)}) \\
&\quad = Com(r_2^{(1)}, t_0^{(1)}, e_0^{(1)}, h_0^{(1)}) \\
c_3 &= Com(r_1^{(1)}, t_1^{(1)}, e_1^{(1)}, f_1^{(1)}) \\
&\quad = Com(r_1^{(3)}, r_0^{(3)} - t_0^{(3)} - t_2^{(3)}, F(r_0^{(3)}) - e_0^{(3)} - e_2^{(3)}, F(r_0^{(3)} + r_1^{(3)}) - f_0^{(3)} - f_2^{(3)}) \\
c_4 &= Com(r_2^{(0)}, r_0^{(0)} - t_0^{(0)} - t_2^{(0)}, F(r_0^{(0)}) - e_0^{(0)} - e_2^{(0)}, F(r_0^{(0)} + r_2^{(0)}) - h_0^{(0)} - h_2^{(0)}) \\
&\quad = Com(r_2^{(1)}, t_1^{(1)}, e_1^{(1)}, h_1^{(1)}) \\
c_5 &= Com(r_1^{(2)}, t_2^{(2)}, e_2^{(2)}, f_2^{(2)}) \\
&\quad = Com(r_1^{(3)}, t_2^{(3)}, e_2^{(3)}, f_2^{(3)}) \\
c_6 &= Com(r_2^{(0)}, t_2^{(0)}, e_2^{(0)}, h_2^{(0)}) \\
&\quad = Com(r_2^{(2)}, t_2^{(2)}, e_2^{(2)}, h_2^{(2)})
\end{aligned}
\tag{3.21}
$$

eşitlikleri elde edilmektedir. Com şeması bağlama özelliğine sahip olduğu için; $r_1^{(1)} = r_1^{(2)} = r_1^{(3)}$, $r_2^{(0)} = r_2^{(1)} = r_2^{(2)}$, $t_0^{(0)} = t_0^{(1)} = t_0^{(3)}$, $t_2^{(0)} = t_2^{(2)} = t_2^{(3)}$, $e_0^{(0)} = e_0^{(1)} = e_0^{(3)}$, $e_2^{(0)} = e_2^{(2)} = e_2^{(3)}$, $f_0^{(1)} = f_0^{(3)}$, $h_0^{(0)} = h_0^{(1)}$, $f_2^{(2)} = f_2^{(3)}$, $h_2^{(0)} = h_2^{(2)}$, $t_1^{(1)} = r_0^{(0)} - t_0^{(0)} - t_2^{(0)}$, $e_1^{(1)} = F(r_0^{(0)}) - e_0^{(0)} - e_2^{(0)} = F(r_0^{(3)}) - e_0^{(3)} - e_2^{(3)}$, $h_1^{(1)} = F(r_0^{(0)} + r_2^{(0)}) - h_0^{(0)} - h_2^{(0)}$, $f_1^{(1)} = F(r_0^{(3)} + r_1^{(3)}) - f_0^{(3)} - f_2^{(3)}$ *eşitlikleri elde edilmektedir. Eşitlik (3.21)'den;*

$$
\begin{aligned}
v \;\; &= G(t_0^{(1)} + t_1^{(1)}, r_1^{(1)}, r_2^{(1)}) + G(t_2^{(2)}, r_1^{(2)}, r_2^{(2)}) + f_0^{(1)} + f_1^{(1)} + f_2^{(2)} + h_0^{(1)} + h_1^{(1)} + h_2^{(2)} \\
&\quad + F(r_1^{(1)} + r_2^{(1)}) - e_0^{(1)} - e_1^{(1)} - e_2^{(2)} - F(r_1^{(2)}) - F(r_2^{(2)})
\end{aligned}
\tag{3.22}
$$

elde edilmektedir. Eşitlik (3.22)'de $t_0^{(1)}$ *yerine* $t_0^{(0)}$, $t_1^{(1)}$ *yerine* $r_0^{(0)} - t_0^{(0)} - t_2^{(0)}$, $t_2^{(2)}$ *yerine* $t_2^{(0)}$, $r_1^{(2)}$ *yerine* $r_1^{(1)}$, $e_0^{(3)}$ *yerine* $F(r_0^{(2)}) - e_1^{(2)}$, $f_0^{(1)}$ *yerine* $f_0^{(3)}$, $h_0^{(1)}$ *yerine* $h_0^{(0)}$, $r_2^{(1)}$ *yerine* $r_2^{(2)}$, $f_1^{(1)}$ *yerine* $F(r_0^{(3)} + r_1^{(3)}) - f_0^{(3)} - f_2^{(3)}$, $h_1^{(1)}$ *yerine* $F(r_0^{(0)} + r_2^{(0)}) - h_0^{(0)} - h_2^{(0)}$, $e_1^{(1)}$ *yerine* $F(r_0^{(0)}) - e_0^{(0)} - e_2^{(0)} = F(r_0^{(3)}) - e_0^{(3)} - e_2^{(3)}$ *ve* $e_2^{(2)}$ *yerine* $e_2^{(0)}$ *yazılırsa* $v = G(r_0^{(0)}, r_1^{(1)}, r_2^{(2)}) + F(r_1^{(1)} + r_2^{(2)}) + F(r_0^{(0)} + r_2^{(2)}) +$

$F(r_0^{(0)} + r_1^{(1)}) - F(r_0^{(0)}) - F(r_1^{(1)}) - F(r_2^{(2)})$ *elde edilir. Tanım* 2.13*.'te verilen Eşitlik* (2.5) *kullanıldığında* $v = F(r_0^{(0)} + r_1^{(1)} + r_2^{(2)}) = F(s)$ *olacak şekilde bir çözüm elde edilmektedir. İspat gösteriyor ki, iletişim kümelerinden hepsine doğru bir şekilde cevap verebilen bir kişi s gizli anahtarına ulaşabilmektedir. Önerilen kimlik doğrulama şemasında sahtekar ispatlayıcı, gerçek ispatlayıcıyı* $3/4$ *olasılıkla taklit edebilmektedir veya çok düşük bir ihtimal ile doğrulayıcıyı kandırabilmektedir. Bu bakımdan önerilen kimlik doğrulama şeması sağlamlık özelliğine sahiptir.*

3.4. Kimlik Doğrulama Şemalarının Karşılaştırılması

Bu kısımda literatürdeki sonlu cisimler üzerinde çok değişkenli polinom sistemlerine dayanan kimlik doğrulama şemaları ile önerdiğimiz yeni şemalar bellek ihtiyacı, iletişim maliyeti, hesaplama zamanı, taklit etme olasılığı ve verimlilik ölçütü açısından karşılaştırılmıştır.

Kimlik doğrulama şemalarının karşılaştırılması için belli teknikler bulunmaktadır. Bu teknikler bellek ihtiyacı, iletişim maliyeti, hesaplama zamanı, taklit etme olasılığı gibi tekniklerdir. Bunların yanında Akleylek ve Soysaldı (2018a) çalışmasında önerilen verimlilik ölçütüne göre karşılaştırma yapılabilmektedir. Çizelge 3.1.'de kimlik doğrulama şemalarının karşılaştırılması verilmektedir. Çizelge 3.1.'deki değerler hesaplanırken 80-bitlik güvenlik seviyesi için $MQ(84, 80, \mathbb{F}_2, 80)$ ve $MC(84, 80, \mathbb{F}_2, 80)$ polinom sistemleri kullanılmıştır.

Kimlik doğrulama şemasının verimliliğinin değerlendirilmesinde temel kriter hesaplama zamanıdır. Kimlik doğrulama şemasında en fazla zaman F ve G fonksiyonlarının hesaplanmasında geçtiği için belirleyici faktör F ve G fonksiyonlarıdır. Tanım 3.2.'de hesaplama zamanının nasıl elde edildiği verilmektedir.

Tanım 3.2 (Hesaplama Zamanı (Computation Time)): *Hesaplama zamanı CT, doğrulayıcının taahhüt değerlerini hesaplayabilmek amacıyla kullandığı F ve G fonksiyonları sayısının meydan okuma sayısına bölünmesi ile elde edilmektedir (Monteiro vd, 2012). Hesaplama zamanı hesaplanırken her Ch değeri için tekrar eden hesaplamalar dikkate alınmamaktadır.*

Çizelge 3.1. 80-bit güvenli kimlik doğrulama şemalarının karşılaştırılması

	A	Der	İspatlayıcı	D	İletişim Maliyeti	Toplam Bellek	CT	IP	EM
(Sakumoto vd, 2011)	3	*MQ*	$9m+2n$	$4m$	$5m+2n+2$	$18m+4n+2$	$4/3$	$2/3$	2.28
(Monteiro vd, 2015)	3	*MQ*	$16m+3n$	$8m$	$8m+3n+2$	$32m+6n+2$	2	$1/2$	2
Önerilen (2;2-3) parçalanışlı şema	3	*MQ*	$18m+3n$	$10m$	$9m+4n+2$	$37m+7n+2$	2	$1/2$	2
Önerilen (3;2-1-2) parçalanışlı şema	3	*MQ*	$14m+3n$	$4m$	$13m+3n+3$	$31m+6n+3$	$4/3$	$1/3$	0.84
(Sakumoto, 2012)	3	*MC*	$11m+3n$	$4m$	$11m+2n+2$	$26m+5n+2$	$3/2$	$3/4$	3.6
(Nachef vd, 2012)	3	*MC*	$13m+2n$	$6m$	$13m+3n+2$	$32m+5n+2$	$9/4$	$3/4$	5.4
Önerilen (3;3-1-1) parçalanışlı şema	3	*MC*	$17m+2n$	$10m$	$20m+4n+2$	$47m+6n+2$	$9/4$	$3/4$	5.4
(Sakumoto vd, 2011)	5	*MQ*	$5m+2n$	$2m$	$5m+2n+2$	$12m+4n+2$	$3/2$	$1/2$	1.5
(Sakumoto, 2012)	5	*MC*	$5m+2n$	$2m$	$5m+3n+2$	$12m+5n+2$	2	$1/2$	2

A kimlik doğrulama şemasının aşama sayısına,
Der kimlik doğrulama şemasında kullanılan çok değişkenli polinomların derecesine,
D kimlik doğrulama şemasında doğrulayıcıya,
CT hesaplama zamanına,
IP taklit etme olasılığına,
EM verimlilik ölçütüne denk gelmektedir.

Örnek 2 ve Örnek 3 sırasıyla (Sakumoto vd, 2011) ve (Monteiro vd, 2012) çalışmalarında önerilen kimlik doğrulama şemalarının hesaplama zamanının nasıl elde edildiğini ifade etmektedir.

***Örnek* 2** *(Sakumoto vd, 2011) çalışmasında verilen üç aşamalı kimlik doğrulama şemasında Ch meydan okuma değerlerinin sayısı* 3*'tür. Doğrulayıcı taahhüt değerlerini hesaplayabilmek için toplamda* 4 *tane F ve G fonksiyonu kullanmaktadır. Tanım 3.2. kullanıldığında (Sakumoto vd, 2011) çalışmasındaki şemanın hesaplama zamanı* $4/3$ *olarak elde edilmektedir.*

***Örnek* 3** *(Monteiro vd, 2015) çalışmasındaki üç aşamalı kimlik doğrulama şemasında* 4 *tane meydan okuma değeri bulunmaktadır. Doğrulayıcı taahhüt değerlerini hesaplayabilmek için toplamda* 10 *tane F ve G fonksiyonu kullanmaktadır. Kullanılan F ve G fonksiyonlarından* 2 *tanesi aynı değeri hesaplamak için kullanıldığından*

hesaplama zamanı hesaplanırken 8 *alınır. Tanım 3.2. kullanıldığında bu şema için hesaplama zamanı* 2 *olarak elde edilmektedir.*

Örnek 2 ve Örnek 3'ten yola çıkarak önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şemasının hesaplama zamanı, doğrulayıcı gerçekleşen 4 tane meydan okuma sırasında taahhüt değerlerini hesaplamak için 10 tane F ve G fonksiyonu kullanmaktadır. Ancak Şekil 3.3.'den görüldüğü üzere $Ch = 0$ ve $Ch = 2$ olma durumlarında tekrar eden F fonksiyonu sayıları çıkarıldığında F ve G fonksiyonlarının sayısı 8'dir. Bu durumda hesaplama zamanı 2 olarak bulunmaktadır.

Kimlik doğrulama şemasını değerlendirmek için kullanılan taklit etme olasılığı Tanım 3.3.'te verilmiştir.

Tanım 3.3 (Taklit Etme Olasılığı): *Kimlik doğrulama şemasında sahtekar üçüncü bir kişinin, doğrulayıcıya kendisini gerçek ispatlayıcıymış gibi gösterebilme veya gerçek ispatlayıcıyı taklit edebilme olasılığı olarak ifade edilmektedir.*

Örneğin; önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şeması için taklit etme olasılığı $1/2$'dir. Sahtekar kişi, gerçek ispatlayıcının bilgilerine sahip olmadığı için doğrulayıcıyı v açık anahtarının hesaplanmasının gerekmediği durumlar için kandırabilmektedir. Bu nedenle taklit etme olasılığı v açık anahtarının olmadığı 2 durum sayısının toplam meydan okuma sayısı olan 4'e bölünmesi ile bulunmaktadır.

Akleylek ve Soysaldı (2018a) çalışmasında önerilen verimlilik ölçütü Tanım 3.4.'te verilmiştir.

Tanım 3.4 (Verimlilik Ölçütü (Efficiency Metric)): *Kimlik doğrulama şemaları için verimlilik ölçütü taklit etme olasılığı ve hesaplama zamanı kullanılarak hesaplanmaktadır.* $\Delta(t)$*, şemada en fazla zaman alan* F *ve* G *fonksiyonlarının hesaplanması için geçen zamanı ve* r *belli bir güvenlik seviyesinin sağlanması için gerekli olan toplam döngü sayısını göstermek üzere verimlilik ölçütü*

$$EM = r \cdot \lambda \cdot CT \cdot \Delta(t)$$

şeklinde hesaplanmaktadır. Ölçütün hesaplanmasında kullanılan λ *toplam döngü sayısının* (r) *alt sınırını ifade etmektedir ve* $(IP)^r \leq 2^{-\lambda}$ *şeklinde hesaplanmaktadır (Monteiro vd, 2015).*

Verimlilik ölçütünün nasıl hesaplandığı Örnek 4'te verilmiştir.

***Örnek* 4** *Önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şemasının verimlilik ölçütünü hesaplayalım. Taklit etme olasılığı* $IP = 1/2$ *olduğundan,*

$$\begin{aligned}(1/2)^r &\leqslant 2^{-\lambda} \\ r \cdot (\log_2 1 - \log_2 2) &\leqslant -\lambda \\ -r &\leqslant -\lambda \\ r &\geqslant \lambda\end{aligned}$$

Verimlilik ölçütü $EM = 1 \cdot 2 \cdot \Delta(t)$ *şeklinde hesaplanır.* $\Delta(t)$ *bütün şemalar için aynı olduğundan hesaplanmada dikkate alınmayarak* $EM = 2$ *olarak elde edilmektedir.*

Çizelge 3.1.'de verilen diğer kriterler için ilgili değerlerin elde edilişini açıklayabilmek adına Bölüm 3.1.'de önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şeması için hesaplamalar yapılmıştır. Hatırlanacağı üzere önerilen şema ikinci dereceden çok değişkenli polinomlara dayanan üç aşamalı bir kimlik doğrulama şemasıdır. Gizli anahtar $s \in \mathbb{F}_q^n$ n-bitlik bir vektördür. Bu sebepten, gizli anahtarın parçalarının her biri de n-bittir. F polinom sisteminin çıktıları m-bit iken *Com* taahhüt fonksiyonunun çıktıları ile özet değerleri $2m$-bittir.

İletişim maliyeti olarak adlandırılan değer, ispatlayıcı ile doğrulayıcı arasında gidip gelen değerler için gereken bellek ihtiyacını ifade etmektedir. Örnek 5'te önerilen şema için iletişim maliyeti ve toplam bellek ihtiyacının hesaplanması verilmektedir.

***Örnek* 5** *Önerilen şema için iletişim maliyeti: hc taahhüt değeri için* $2m$*-bit, Ch meydan okuma için* 2*-bit ve Rsp cevap değeri için* $(7m+4n)$*-bit olmak üzere toplam* $(9m+4n+2)$*-bittir.*

Örnek 6'da ispatlayıcı ve doğrulayıcı içi bellek ihtiyacının hesaplamaları yapılmaktadır.

***Örnek* 6** *İspatlayıcı için bellek ihtiyacı hesaplanacak olursa ispatlayıcının her biri n-bit olan üç adet ve her biri m-bit olan iki adet gizli anahtar parçası ayrıca her biri* $2m$*-bit olan yedi adet taahhüt değeri ve özet değeri için toplam* $(18m+3n)$*-bitlik bir bellek*

ihtiyacı vardır. Doğrulayıcı için bellek ihtiyacı her bir döngüde beş tane taahhüt değeri hesaplandığı için $10m$*-bittir. Önerilen şemanın toplam bellek ihtiyacı ise* $(37m+7n+2)$*-bittir.*

Çizelge 3.1.'de verilen kimlik doğrulama şemalarını üç temel ölçüt çerçevesinde değerlendirilerek karşılaştırma yapılmıştır.

Değerlendirme 1: *MQ* polinomlara dayanan kimlik doğrulama şemaları karşılaştırıldığında önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şemasının Monteiro vd (2015) çalışmasındaki şema ile aynı hesaplama zamanına, taklit etme olasılığına ve verimlilik ölçütüne sahip olduğu görülmektedir. (3;2-1-2) parçalanışa sahip kimlik doğrulama şemasının hesaplama zamanı ise çok değişkenli polinomlara dayanan kimlik doğrulama şemalarında öncü çalışma olan Sakumoto vd (2011) çalışması ile aynıdır. *MQ* tabanlı kimlik doğrulama şemaları toplam bellek ihtiyaçları açısından karşılaştırıldığında karakteristiği 2 olan cisimler için küçük belleğe sahip sistemlerde bile fazla bir fark bulunmamaktadır.

Değerlendirme 2: *MC* polinomlara dayanan kimlik doğrulama şemaları ile önerilen (3;3-1-1) parçalanışa sahip kimlik doğrulama şeması karşılaştırıldığında hesaplama zamanı ve taklit etme olasılığının aynı olduğu görülmektedir. Parçalanış sayısının artması toplam bellek ihtiyacını arttırmaktadır. Bu artış kimlik doğrulama şemalarının kullanıldığı sistemlerde ciddi bir verimsizliğe neden olmamaktadır.

Değerlendirme 3: Beş aşamalı kimlik doğrulama şemaları karşılaştırıldığında Sakumoto vd (2011) şemasının hem hesaplama zamanı hem de verimlilik ölçütü bakımından Sakumoto (2012) şemasından daha iyi olduğu görülmektedir. Bu iki şema taklit etme olasılığı, iletişim maliyeti ve toplam bellek açısından değerlendirildiğinde hemen hemen aynı değerlere sahiptir.

4. KİMLİK DOĞRULAMA ŞEMASINDAN ELEKTRONİK İMZALAMA ŞEMASINA GEÇİŞ

Kimlik doğrulama şemaları imzalama şemalarının temelini oluşturmaktadır. Bir kimlik doğrulama şeması Fiat-Shamir dönüşümü kullanılarak imzalama şemasına dönüştürülebilmektedir. Bu bölümde, Bölüm 3.1.'de önerilen kimlik doğrulama şeması imzalama şemasına dönüştürülmüştür.

4.1. İkinci Dereceden Çok Değişkenli Polinomlara Dayanan Yeni İmzalama Şeması

Bölüm 3.1.'de önerilen (2;2-3) parçalanışa sahip ikinci dereceden çok değişkenli polinomlara dayanan üç aşamalı kimlik doğrulama şemasına Tanım 2.17.'deki Fiat-Shamir dönüşümü uygulanarak yeni bir imzalama şeması elde edilmiştir.

Kimlik doğrulama şemasında $F \in MQ(n,m,\mathbb{F}_q,k)$ olacak şekilde ikinci dereceden n değişkenli m polinomdan oluşan bir polinom sistemi kullanılmaktadır. (Detaylı bilgi için Bölüm 3'e bakınız.) 80-bitlik güvenlik seviyesi için $k = 80$, $n = 84$ ve $m = 80$ olarak alınmıştır. F ikinci dereceden çok değişkenli polinom sisteminin boyu ise $F^{len} = m \cdot \frac{n(n+1)}{2}$ şeklinde ifade edilmiştir. İmzalama şemasının oluşturulabilmesi için aşağıdaki fonksiyonlara ihtiyaç vardır:

- Kriptografik Özet Fonksiyonları: $\mathscr{H} : \{0,1\}^* \rightarrow \{0,1\}^k$, $\mathscr{H}_1 = \{0,1\}^{2k} \rightarrow \{0,1,2,3\}^r$
- Taahhüt Fonksiyonu: $Com : \mathbb{F}_2^n \times \mathbb{F}_2^m \rightarrow \{0,1\}^k$
- Sözde-rastgele Sayı Üreteçleri: $G_{S_F} = \{0,1\}^k \rightarrow \mathbb{F}_2^{F_{len}}$, $G_{S_K} = \{0,1\}^k \rightarrow \mathbb{F}_2^n$, $G_C : \{0,1\}^{2k} \rightarrow \mathbb{F}_2^{r(4n+3m)}$

Tanım 2.16.'da ifade edildiği üzere imzalama şeması anahtar üretme, imzalama ve doğrulama aşamalarından oluşmaktadır.

Anahtar Üretme (KeyGen): *KeyGen* anahtar üretme algoritmasında (pk, sk) anahtar çifti üretilmektedir. k bitlik güvenlik seviyesi kullanıldığından $SK \leftarrow_R \{0,1\}^k$ ve $S_F \leftarrow_R \{0,1\}^k$ k-bitlik rastgele başlangıç değerleri seçilmektedir. Seçilen k-bitlik S_F değeri kullanılarak $F \in MQ(n,m,\mathbb{F}_2)$ polinom sistemi rastgele bir şekilde üretilmektedir. F polinom sisteminin katsayılarında kullanılmak için F_{len} tane elemana ihtiyaç vardır. Bundan dolayı rastgele sayı üreteçlerinden G_{S_F} polinom sistemini elde etmek için kullanılmaktadır. S_K değeri de G_{S_K} sayı üretecine giriş olarak verilerek n-bitlik $SK_{\mathbb{F}_2} = G_{S_K}(SK)$ değeri elde edilmektedir. Bu değer kullanılarak $PK_v = F(SK_{\mathbb{F}_2})$ değeri hesaplanmaktadır. Üretilen değerlerden sırasıyla $(k+m)$-bitlik $pk = (S_F, PK_v)$ açık anahtarı ve $2k$-bitlik $sk = (S_F, SK)$ ise gizli anahtarı ifade etmektedir.

İmzalama (Sign): İmzalama şemasında anahtar üretme algoritmasından sonra imzalama algoritması çalıştırılmaktadır. *Sign* imzalama algoritması $m \in \{0,1\}^*$ mesaj değerini ve $sk = (S_F, SK)$ gizli anahtarı giriş olarak almaktadır. *KeyGen* algoritmasında olduğu gibi ilk olarak $F = G_{S_F}(S_F)$ MQ polinom sistemi üretilmektedir. $||$ katar birleştirmeyi ifade etmek üzere özet fonksiyonu kullanılarak mesaj ile alakalı rastgele bir $M = \mathscr{H}(SK||m)$ değeri elde edilmektedir. Bu M değeri kullanılarak rastgele $D = \mathscr{H}(M||m)$ mesaj özeti üretilmektedir. Doğrulama işleminde doğrulayıcının aynı mesaj özetini elde edebilmesi için M değerinin imzada yer alması gerekmektedir.

İmzalama şeması kimlik doğrulama şemasından türetildiği için kimlik doğrulama şemasında olan aşamalar temel olarak imzalama şemasında da mevcuttur. Bu bakımdan kimlik doğrulama şemasının başlangıcında olduğu gibi gizli anahtarın parçaları elde edilmektedir. r gerekli olan döngü sayısını göstermek üzere üretilen (SK, D) değerleri G_C rastgele sayı üretecine verilerek $(\mathrm{r}_{(0,0)}, \ldots, \mathrm{r}_{(0,r)}, t_{(0,0)}, \ldots, t_{(0,r)}, e_{(0,0)}, \ldots, e_{(0,r)}, d_{(0,0)}, \ldots, d_{(0,r)}, d_{(1,0)}, \ldots, d_{(1,r)}, u_{(0,0)}, \ldots, u_{(0,r)}, u_{(1,0)}, \ldots, u_{(1,r)})$ gizli anahtarın parçaları seçilmektedir. Bölüm 3.1.'de önerilen kimlik doğrulama şemasında tanımlandığı üzere her bir i döngüsü için *Com* taahhüt fonksiyonu kullanılarak:

$$c_{(0,i)} = Com(r_{(0,i)}, G(r_{(0,i)}, d_{(1,i)}) + u_{(1,i)}),$$

$$c_{(1,i)} = Com(r_{(1,i)}, G(t_{(0,i)}, r_{(1,i)}) + e_{(0,i)}),$$

$$c_{(2,i)} = Com(t_{(0,i)}, e_{(0,i)}),$$

$$c_{(3,i)} = Com(t_{(1,i)}, e_{(1,i)}),$$

$$c_{(4,i)} = Com(d_{(0,i)}, u_{(0,i)}),$$

$$c_{(5,i)} = Com(d_{(1,i)}, u_{(1,i)}),$$

$$c_{(6,i)} = Com(d_{(2,i)}, u_{(2,i)}).$$

taahhüt değerleri hesaplanmaktadır. Elde edilen taahhüt değerlerinin tamamı birleştirilerek $\sigma_0 = \mathscr{H}(c_{(0,0)}||c_{(1,0)}||c_{(2,0)}||c_{(3,0)}||c_{(4,0)}||c_{(5,0)}||c_{(6,0)}||\ldots||c_{(0,r-1)}||$ $c_{(1,r-1)}||c_{(2,r-1)}||c_{(3,r-1)}||c_{(4,r-1)}||c_{(5,r-1)}||c_{(6,r-1)})$ özet elde edilmektedir. Daha sonra $\mathscr{H}_1$ özet fonksiyonu kullanılarak (D, σ_0) çiftinden $Ch_i = \mathscr{H}_1(D, \sigma_0)$ meydan okuma değerleri elde edilmektedir. Her bir Ch_i meydan okuma değeri için $\sigma_1 = (r_{(1,i)}||t_{(1,i)}||e_{(1,i)}||d_{(0,i)}||u_{(0,i)}||d_{(1,i)}||u_{(1,i)}||r_{(1,i)}||t_{(0,i)}||e_{(0,i)}||d_{(0,i)}||u_{(0,i)}||d_{(2,i)}||u_{(2,i)}||$ $r_{(0,i)}||t_{(1,i)}||e_{(1,i)}||d_{(0,i)}||u_{(0,i)}||d_{(2,i)}||u_{(2,i)}||r_{(0,i)}||t_{(0,i)}||e_{(0,i)}||d_{(0,i)}||u_{(0,i)}||d_{(1,i)}||u_{(1,i)})$ bütün cevap değerleri hesaplanmaktadır. $c_{(j,i)}$ taahhüt değerleri hesaplanabildiği için cevapların birleştirilmesiyle elde edilen σ_1 değeri $j \in \{0,1,2,3,4,5,6\}$ olmak üzere $c_{(j,i)}$ değerlerini içermemektedir. Sonuçta $\sigma = (M, \sigma_0, \sigma_1)$ imza elde edilmektedir. Oluşturulan imza $(2k + r \cdot (4n + 3m))$-bit boyutundadır.

Doğrulama (Verify): İmzalama şemasının son aşaması imzanın doğrulanmasıdır. $Verify$ doğrulama algoritması m mesajı, $pk = (S_F, PK_v)$ açık anahtarı ve $\sigma = (M, \sigma_0, \sigma_1)$ imza değerini giriş olarak almaktadır. İlk olarak açık anahtardaki S_F değerinden $F = G_{S_F}(S_F)$ ikinci dereceden çok değişkenli polinom sistemi oluşturulmaktadır. Mesaj özetini hesaplayabilmek için imzada yer alan M değeri ile m mesajı kullanılarak $D = \mathscr{H}(M||m)$ elde edilmektedir. Her bir r döngüsü için $Ch_i = \mathscr{H}_1(D, \sigma_0)$ meydan okumalar hesaplanmaktadır. Daha sonra her döngü için σ_1 değerinden meydan okumalara karşılık gelen cevaplar bulunmaktadır. Son olarak aşağıdaki gibi taahhüt değerleri hesaplanmaktadır:

$$Ch_i = 0, \begin{cases} c_{(1,i)} = Com(r_{(1,i)}, PK_v - G(t_{(1,i)}, r_{(1,i)}) - F(r_{(1,i)}) - e_{(1,i)}) \\ c_{(3,i)} = Com(t_{(1,i)}, e_{(1,i)}) \\ c_{(4,i)} = Com(d_{(0,i)}, u_{(0,i)}) \\ c_{(5,i)} = Com(d_{(1,i)}, u_{(1,i)}) \\ c_{(6,i)} = Com(r_{(1,i)} - d_{(0,i)} - d_{(1,i)}, F(r_{(1,i)}) - u_{(0,i)} - u_{(1,i)}) \end{cases}$$

$$Ch_i = 1, \quad \begin{cases} c_{(1,i)} = Com(r_{(1,i)}, G(t_{(0,i)}, r_{(1,i)}) + e_{(0,i)}) \\ c_{(2,i)} = Com(t_{(0,i)}, e_{(0,i)}) \\ c_{(4,i)} = Com(d_{(0,i)}, u_{(0,i)}) \\ c_{(5,i)} = Com(r_{(1,i)} - d_{(0,i)} - d_{(2,i)}, F(r_{(1,i)}) - u_{(0,i)} - u_{(2,i)}) \\ c_{(6,i)} = Com(d_{(2,i)}, u_{(2,i)}) \end{cases}$$

$$Ch_i = 2, \quad \begin{cases} c_{(0,i)} = Com(r_{(0,i)}, PK_v - G(r_{(0,i)}, d_{(0,i)} + d_{(2,i)}) - F(r_{(0,i)}) \\ -u_{(0,i)} - u_{(2,i)}) \\ c_{(2,i)} = Com(r_{(0,i)} - t_{(1,i)}, F(r_{(0,i)}) - e_{(1,i)}) \\ c_{(3,i)} = Com(t_{(1,i)}, e_{(1,i)}) \\ c_{(4,i)} = Com(d_{(0,i)}, u_{(0,i)}) \\ c_{(6,i)} = Com(d_{(2,i)}, u_{(2,i)}) \end{cases}$$

$$Ch_i = 3, \quad \begin{cases} c_{(0,i)} = Com(r_{(0,i)}, G(r_{(0,i)}, d_{(1,i)}) + u_{(1,i)}) \\ c_{(2,i)} = Com(t_{(0,i)}, e_{(0,i)}) \\ c_{(3,i)} = Com(r_{(0,i)} - t_{(0,i)}, F(r_{(0,i)}) - e_{(0,i)}) \\ c_{(4,i)} = Com(d_{(0,i)}, u_{(0,i)}) \\ c_{(5,i)} = Com(d_{(1,i)}, u_{(1,i)}) \end{cases}$$

Doğrulayıcı oluşturduğu taahhüt değerlerinin birleştirilerek $\mathscr{H}$ özet fonksiyonu kullanılarak $\sigma_0' = \mathscr{H}(c_{(0,0)}||c_{(1,0)}||c_{(2,0)}||c_{(3,0)}||c_{(4,0)}||c_{(5,0)}||c_{(6,0)}||\ldots||c_{(0,r-1)}||$ $c_{(1,r-1)}||c_{(2,r-1)}||c_{(3,r-1)}||c_{(4,r-1)}||c_{(5,r-1)}||c_{(6,r-1)})$ değerini hesaplamaktadır.

$$\sigma_0' = \begin{cases} \sigma_0 & ,\text{imza doğrulanır} \\ \text{aksi halde} & ,\text{ imza doğrulanmaz.} \end{cases}$$

4.2. Önerilen İmzalama Şemasının Güvenlik Analizi ve Karşılaştırılması

Bu kısımda önerilen imzalama şeması için güvenlik analizi yapılmıştır. Bunun yanı sıra, önerilen imzalama şemasının anahtar ve imza boyutu bakımından karşılaştırması verilmiştir.

İmzalama şemasının güvenliğinden bahsedebilmek için Teorem 7'nin sağlanması gerekmektedir.

Teorem 7 *Önerilen imzalama şeması aşağıdaki özellikleri sağlıyorsa rastgele kahin modelinde uyarlamalı seçilmiş mesaj atağı (EU-CMA) altında varoluşsal olarak taklit edilemez bir özelliğe sahiptir.*

– *İmzalama şemasının dayandığı MQ problem polinom zamanlı bir algoritma ile çözülememelidir.*

– $\mathscr{H}, \mathscr{H}_1$ *özet fonksiyonları rastgele kahin olarak modellenebilmelidir.*

– *Com taahhüt fonksiyonu istatistiksel saklama ve hesaplamalı bağlayıcı özelliklerine sahip olmalıdır. Bunun yanı sıra, Com fonksiyonunu kullanarak belli bir sonucu elde etmek mümkün olmamalıdır.*

– G_{S_F}, G_{S_K} *ve* G_C *sözde-rastgele sayı üreteçlerinin çıktıları ile rastgele olarak elde edilen değerler hesaplamalı olarak ayırt edilemez olmalıdır.*

Teoremin ispatı Dagdelen vd (2016) ve Chen vd (2016b) tarafından yapılan ispat yöntemlerini birleştirerek yapılmıştır. İmzalama şemasının seçilmiş mesaj atağına karşı güvenli olduğunun ispatlanabilmesi için *n*-genel (*n*-generic) ve *n*-sağlamlık (*n*-soundness) tanımlarının imzalama şeması için yapılması gerekmektedir. Dagdelen vd (2016) tarafından yapılan tanıma göre Bölüm 2.'de verilen Tanım 2.17. kullanılarak $(2;2-3)$ parçalanışa sahip kimlik doğrulama şemasından oluşturulan imzalama şemasının 1-genel imzalama şeması olduğu görülmektedir. Tanım 4.1.'de Dagdelen vd (2016) tarafından yapılan *n*-genel tanımının önerilen imzalama şemasına uyarlanmış hali olan 1-genel tanımı verilmiştir.

Tanım 4.1 : *(Dagdelen vd, 2016) m imzalanacak mesaj değeri,* $\mathscr{H}$ *kullanılan özet fonksiyonu olmak üzere imzalama şeması DSS=(Anahtar Üretme, İmzalama, Doğrulama) şeklinde olsun. Özet değeri* $h_1 = \mathscr{H}(m, \sigma_0)$ *ise oluşturulan imza* $(\sigma_0, h_1, \sigma_1)$ 1*-genel bir imzadır. Ayrıca oluşturulan imzalama şeması sıfır bilgi özelliğine sahiptir .*

Tanım 4.2.'de önerilen 1-genel imzalama şemasının sağladığı 1-sağlamlık özelliğinin tanımına yer verilmiştir.

Tanım 4.2 : *DSS =(Anahtar Üretme, İmzalama, Doğrulama)* 1*-genel bir imzalama şeması olsun. Eğer olasılıksal polinom zamanlı bir algoritma (PPT)* ε *varsa bu algoritma kullanılarak herhangi bir* $(sk, pk) \leftarrow$ *Anahtar Üretme*(1^k) *anahtar çifti,* $\sigma = (\sigma_0, h_1, \sigma_1)$ *ve* $\sigma' = (\sigma_0, h_1', \sigma_1')$ *iki farklı geçerli imza için* $h_1 \neq h_1'$ *olacak şekilde ihmal edilemez bir olasılıkla* $sk \leftarrow \varepsilon(pk, m, \sigma, \sigma')$ *gizli anahtarı elde edilir.*

***İspat* 7** *İspata Teorem 7'nin birinci maddesinden başlanmıştır. Dagdelen vd (2016) çalışmalarında zor probleme dayanan n-sağlamlık özelliğini sağlayan n-genel bir DSS imzalama şemasının rastgele kahin modelinde uyarlamalı seçilmiş mesaj atağı (EU-CMA) altında varoluşsal olarak taklit edilemez olduğunu belirtmişlerdir. Oluşturulan imzalama şeması Bölüm* 3*.'de önerilen* $(2;2-3)$ *parçalanışa sahip kimlik doğrulama şemasından elde edilmiştir. Ayrıca önerilen kimlik doğrulama şemasının hesaplamalı zorluğu MQ zor probleme dayanmaktadır. Bölüm* 2*. Tanım* 2.3*.'de kimlik doğrulama şemasının dayandığı MQ problemi kuantum bilgisayarlarda bile çözebilecek polinom zamanlı bir algoritmanın bulunmadığı ifade edilmiştir. Dolayısıyla oluşturulan* 1*-sağlamlık özelliğine sahip* 1*-genel imzalama şeması* $EU-CMA$ *güvenlidir.*

Teorem 7'de yer alan diğer maddeler tanımlanan $EU-CMA$ *oyunu ile ispatlanmıştır. İhmal edilemez bir olasılıkla* $EU-CMA$ *oyununu kazanan bir A saldırganın olduğunu kabul edelim. Bu oyunlarda A'nın kazanma olasılıkları arasındaki farkın ihmal edilebilir olduğunu başka bir ifadeyle oyunları kazanma olasılıklarının eşit olduğunu iddia ediyoruz. Kabul edelim ki A, MQ problemi çözebilen, taahhüt şemasının sağladığı saklama ve bağlama özelliklerini bozan, bir özet değerine karşılık gelen iki farklı mesajı bulabilen veya rastgele sayı üreteçlerinin çıktıları ile rastgele değerleri birbirinden ayırabilecek bir* $\mathcal{O}$ *kahin makinesine sahip olsun.*

- **Oyun** 0**:** *DSS imzalama şeması için* $EU-CMA$ *oyunudur.*
- **Oyun** 1**:** $\mathcal{O}$ *kahin,* G_{S_K} *sayı üretecinin çıktılarını diğer değerlerden ayırarak bu değerleri rastgele değerlerle değiştirdiğinde Oyun* 0 *ile olan farktır.*
- **Oyun** 2**:** $\mathcal{O}$ *kahin,* G_C *sayı üretecinin çıktılarını diğer değerlerden ayırarak bu değerleri rastgele değerlerle değiştirdiğinde Oyun* 1 *ile oluşan farktır.*
- **Oyun** 3**:** $\mathcal{O}$ *kahin, F polinom sistemi için* G_{S_F} *sayı üretecinin ürettiği rastgele değerler gibi rastgele katsayılar ürettiği durumda Oyun* 2 *ile arasındaki farktır.*

Kabul edelim ki, A, Oyun 0*'i göz ardı edilemez bir* ε *olasılıkla kazanıyor olsun. Eğer A'nın kazandığı Oyun* 0 *ile Oyun* 1 *arasında göz ardı edilemez bir fark varsa A hangi değerlerin* G_{S_K} *rastgele sayı üreteci ile üretildiğini biliyor ve*

bu değerleri değiştirebiliyor demektir. Benzer şekilde, Oyun 1 *- Oyun* 2 *arasındaki fark göz ardı edilemez ise A, G_C sayı üretecinin çıktılarını diğer değerlerden ayırt edebiliyor demektir. Oyun* 2 *- Oyun* 3 *arasındaki fark içinde aynı durum geçerlidir. Dolayısıyla, A'nın oyunları kazanma olasılığı eşittir. A'nın Oyun* 3 *ve Oyun* 0*'ı kazanma olasılığının eşit olduğundan Oyun* 3*, MQ polinomlara dayanan kimlik doğrulama şemasından dönüştürülen DSS imzalama şeması için $EU-CMA$ oyunudur. Aksine n-sağlamlık özelliğine sahip bir n-genel imzalama şemasının $EU-CMA$'ya karşı güvenli olduğu bilinmektedir (Dagdelen vd, 2016). MQ polinomlara dayanan* $(2;2-3)$ *parçalanışa sahip kimlik doğrulama şemasından Fiat-Shamir dönüşümü kullanılarak elde edilen imzalama şeması Tanım 4.1.'de ifade edildiği üzere n-genel bir imzalama şemasıdır. Bu nedenle DSS imzalama şeması $EU-CMA$'ya karşı güvenlidir. Bunun yanı sıra, imzalama şemasının oluşturulduğu kimlik doğrulama şeması Bölüm* 3*. Teorem* 3 *ve Teorem* 4*'te ispatı verildiği gibi sıfır bilgi ve sağlamlık özelliklerini sağlamaktadır. İspatlar incelendiğinde Com taahhüt şemasının istatistiksel saklama ve hesaplamalı bağlama özelliklerine sahip olduğu görülmektedir. Dolayısıyla DSS imzalama şeması $EU-CMA$'ya karşı güvenlidir.*

Çizelge 4.1.'de yeni imzalama şeması ile literatürdeki çok değişkenli polinomlara dayanan imzalama şemaları anahtar ve imza boyutları açısından karşılaştırılmaktadır.

Çizelge 4.1. İmzalama şemalarının karşılaştırılması

		(Chen vd, 2016b) 3-aşama	Önerilen Şema	(Chen vd, 2016b) 5-aşama
İmza Boyutu		$2k+r\cdot(2n+m+k)$	$2k+r\cdot(4n+3m)$	$2k+r\cdot(10n+5m+k)$
Anahtar Boyutu	**Açık Anahtar**	$m+k$	$m+k$	$5m+k$
	Gizli Anahtar	$2k$	$2k$	$2k$

Önerilen imzalama şemasında $\sigma=(M,\sigma_0,\sigma_1)$ imza olarak kabul edilmiştir. İmzadaki M ve σ_0 özet fonksiyonunun çıktıları olduğundan her biri k-bittir. Her döngü için bütün cevapların birleştirilmiş hali olan σ_1, $(r\cdot(4n+3m))$-bittir. Bu sebepten, imzanın toplam boyutu $(2k+r\cdot(4n+3m))$-bittir. Şemadaki $pk=(S_F,PK_v)$ açık anahtarının boyutuna bakıldığında S_F, polinom sistemi için üretilmiş rastgele k-bitlik bir değerdir. Hatırlayacak olursak PK_v değeri de F polinom sisteminin çıktısı olduğundan m-bittir. Dolayısıyla pk açık anahtarı $(m+k)$-bittir. $sk=(S_F,SK)$ gizli anahtarı ise k-bitlik rastgele değerlerden oluştuğundan $2k$-bittir.

Çizelge 4.1.'den önerilen imzalama şemasının üç aşamalı şema ile aynı anahtar boyutuna sahip olduğu görülmektedir. Beş aşamalı imzalama şemasından ise daha küçük anahtar boyutuna sahip yeni bir imzalama şeması elde edilmiştir. Bunun yanı sıra, beş aşamalı imzalama şemasından daha küçük imza boyutuna sahip bir şema önerilmiştir.

5. SONUÇ VE GELECEK ÇALIŞMALAR

Fazla kubite sahip kuantum bilgisayarı oluşturma çalışmalarının hız kazanması ile hesaplama gücü iyice artmaktadır. Artan hesaplama gücü günümüz kriptosistemlerin dayandığı zor problemin çözülebilmesine imkan vermiştir. Bu sebepten, kuantum ataklarına karşı dirençli kriptografik sistemlere ihtiyaç vardır. Bu tez çalışmasında, kuantum sonrasında güvenilir olduğu bilinen çok değişkenli polinomlara dayanan sistemler üzerinde çalışılmıştır.

Çok değişkenli polinomlara dayanan sıfır bilgi paylaşımlı özgün kimlik doğrulama şemaları önerilmiştir. Önerilen şemaların parçalanışı, işleyişi ve ispatları detaylı bir şekilde verilmiştir. Kimlik doğrulama şemalarının karşılaştırılması için yeni bir verimlilik ölçütü tanımlanmıştır. Bu yeni verimlilik ölçütünün yanı sıra bellek ihtiyacı, iletişim maliyeti, hesaplama zamanı ve taklit etme olasılığı gibi kriterler açısından kimlik doğrulama şemaları karşılaştırılmıştır.

Derecesi $d \geq 4$ olan çok değişkenli polinomlara dayanan kimlik doğrulama şemaları oluşturulup oluşturulamayacağı konusundaki açık problem için kısmi bir çözüm önerilmiştir (Akleylek and Soysaldı, 2017). Önerilen çözüm yinelemeli olarak çalıştırıldığında polinom derecesine bağlı olarak şemada kullanılacak polar form elde edilmektedir.

Önerilen (2;2-3) parçalanışa sahip kimlik doğrulama şeması kullanılarak yeni bir imzalama şeması elde edilmiştir (Akleylek and Soysaldı, 2018a). İmzalama şemasını elde edebilmek için kimlik doğrulama şemasına Fiat-Shamir dönüşümü uygulanmıştır. Oluşturulan imzalama şeması detaylı bir şekilde anlatılmıştır. Ayrıca imzalama şeması için güvenlik analizi yapılırken anahtar boyutları ve imza boyutu açısından imzalama şemaları karşılaştırılmıştır.

Bu çalışmanın devamı olarak önerilen kimlik doğrulama şemaları baz alınarak daha verimli imzalama şemaları elde edilmeye çalışılacaktır. Ayrıca önerilen kimlik doğrulama ve imzalama şemalarının gerçek zamanlı uygulamalarının yapılması

planmaktadır. Önerilen şemalar için uygun parametrelerin oluşturulması ve performans analizinin yapılması konusunda çalışmalar yapılacaktır.

KAYNAKLAR

Abdalla, M., An, J. H., Bellare, M., and Namprempre, C. (2002). From identification to signatures via the Fiat-Shamir transform: Minimizing assumptions for security and forward-security. In International Conference on the Theory and Applications of Cryptographic Techniques, 418-433, Springer, Berlin, Heidelberg.

Akleylek, S. and Soysaldı, M. (2017). On Generalization of Linear In One Argument Form of Multivariate Polynomials for Post Quantum Cryptography. 3rd International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (AMINSE 2017), 6-9 December, Book of Abstracts, 70-73, Tbilisi, Georgia.

Akleylek, S. and Soysaldı, M. (2018a). A Novel 3-pass Identification Scheme and Signature Schme Based On Multivariate Quadratic Polynomials, Turk J. Math, değerlendirme aşamasında.

Akleylek, S. ve Soysaldı, M. (2018b). Kuantum Sonrası Güvenilir Yeni Kimlik Doğrulama Şeması, 9. Savunma Teknolojiler Kongresi (SAVTEK 2018), 27-29 Haziran, Bildiri Kitabı, 873-881, ODTÜ, Ankara.

Alkadri, N. A. (2015). Post-Quantum Commitment Schemes. Yüksek Lisans Tezi, Darmstadt University of Technology Department of Computer Science Cryptography and Computeralgebra, Darmstadt.

Bernstein, D. J., Buchmann, J. and Dahmen, E. (eds) (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography, 1-14. Springer, Berlin, Heidelberg.

Buchanan, W. and Woodward, A. (2017). Will quantum computers be the end of public key encryption?, 1(1), 1-22, Taylor & Francis.

Chen, L., Jordan, S., Liu, Y.K, Moody, D., Peralta, R., Perlner, R. and Smith-Tone, D. (2016a). NISTIR 8105, Report on Post-Quantum Cryptography, NIST. National Institute of Standards and Technology.

Chen, M., Hülsing, A., Rijneveld, J., Samardjiska, S. and Schwabe, P. (2016b). From 5-pass MQ-based identification to MQ-based signatures. IACR Cryptology ePrint Archive, 708.

Chuang, I. L., Vandersypen, L.M., Zhou, X., Leung, D.W. and Lloyd, S. (1998). Experimental realization of a quantum algorithm. *Nature*, *393*(6681), 143-146.

Çimen, C., Akleylek, S., ve Akyıldız, E. (2012). Şifrelerin matematiği: Kriptografi. ODTÜ.

Dagdelen, Ö., Fischlin, M. and Gagliardoni, T. (2013). The Fiat–Shamir transformation in a quantum world. In International Conference on the Theory and Application of Cryptology and Information Security, 62-81, Springer, Berlin, Heidelberg.

Dagdelen, Ö., Galindo, D., Veron, P., El Yousfi Alaoui, S.M. and Cayrel, P.L. (2016). Extended security arguments for signature schemes, Designs, Codes and Cryptography, 78-2, 441-461.

Dang, Q.H. (2015). FIPS PUB 180-4, Secure Hash Standard (SHS). Federal Information Processing Standards Publication, National Institute of Standards and Technology.

De Feo, L., Jao, D. and Plut, J. (2014). Towards quantum resistant cryptosystems from supersingular elliptic curve isogenies. Journal of Mathematical Cryptology, 8(3), 209-247.

Diffie, W. and Hellman, M. (1976). New directions in cryptography. IEEE transactions on Information Theory, 22(6): 644-654.

Dworkin, M.J. (2015). FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Federal Information Processing Standards Publication, National Institute of Standards and Technology.

Feymann, R.P. (1982). Simulating Physics with Computers. International Journal of Theoretical Physics, 21(6/7), 467-488.

Fiat, A. and Shamir, A. (1986). How to prove yourself: Practical solutions to identification and signature problems. In Conference on the Theory and Application of Cryptographic Techniques, 186-194, Springer, Berlin, Heidelberg.

FIPS 46-3 (1999). FIPS 46-3 : Data encryption standard (DES). Federal information processing standards publication, National Institute of Standards and Technology, 25(10), 1-22.

FIPS 197 (2001). FIPS 197 Advanced encryption standard (AES). Federal information processing standards publication, National Institute of Standards and Technology, 197(441), 0311.

Fukuoka MQ-Challenge. https://www.mqchallenge.org/ (Erişim Tarihi:04.06.2018).

Goldreich, O. (2004). Foundations of cryptography. Basic Tools, 2(1). Cambridge University Press.

Hatzivasilis, G., Fysarakis, K., Papaefstathiou, I. and Manifavas, C. (2018). A review of lightweight block ciphers. Journal of Cryptographic Engineering, 8, 141-144.

Hornschuch, M. (2012). Multivariate-based Identification and Signature Schemes with Additional Properties. Doktora Tezi, Technische Universitat Darmstadt, Kryptographie und Computeralgebra, Darmstadt.

Identification With Zero Knowledge Protocols. https://www.sans.org/reading-room/whitepapers/vpns/identification-zero-knowledge-protocols-719 (Erişim Tarihi: 07.05.2018).

Johnston, H. (2017). IBM offers 20-qubit quantum computer to clients. https://physicsworld.com/a/ibm-offers-20-qubit-quantum-computer-to-clients/ (Erişim Tarihi 03.06.2018)

Kahn, D. (1996). The Codebreakders: The comph-rehensive history of secret com-Munication from ancient times to the internet. Simon and Schuster.

Kelly, J. (2018). Engineering superconducting qubit arrays for quantum supremacy. American Physical Society March Meeting, Los Angeles.

Lidl, R., and Niederreiter, H. (1994). Introduction to finite fields and their applications. Cambridge university press.

Menezes, A. J., Katz, J., Van Oorschot, P. C., and Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

Monteiro, F. S., Goya, D. H. and Terada, R. (2015). Improved Identification Protocol Based on the MQ Problem. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 98(6), 1255-1265.

Nachef, V., Patarin, J. and Volte, E. (2012). Zero-knowledge for multivariate polynomials. In International Conference on Cryptology and Information Security in Latin America, 194-213. Springer, Berlin, Heidelberg.

NIST (2017). Post Quantum Cryptography. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization (Erişim Tarihi 04.06.2018)

NIST (2018). Post Quantum Cryptography. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions (Erişim Tarihi 04.06.2018)

Nielsen, M. A. and Chuang, I. L. (2000). Quantum computation. Quantum Information. Cambridge University Press, Cambridge.

Rivest, R. L., Shamir, A. and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2): 120-126.

Sakumoto, K., Shirai, T. and Hiwatari, H. (2011). Public-key identification schemes based on multivariate quadratic polynomials. In Annual Cryptology Conference, 706-723. Springer, Berlin, Heidelberg.

Sakumoto, K. (2012). Public-key identification schemes based on multivariate cubic polynomials. In International Workshop on Public Key Cryptography, 172-189, Springer, Berlin, Heidelberg.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium, 124-134. Ieee.

Simari, G. I. (2002). A primer on zero knowledge protocols. Universidad Nacional del Sur, 6(27), 1-12.

Silva , R., Antonio, C.D.A. and Dahab, R. (2011). LWE-based identification schemes. In Information Theory Workshop (ITW), 2011 IEEE, 292-296.

Stern, J. (1993). A new identification scheme based on sydrome decoding. CRYPTO'93, 13-21.

Vandersypen, L. M., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H. and Chuang, I. L. (2001). Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. Nature, 414(6866), 883.

ÖZGEÇMİŞ

Adı Soyadı : Meryem Soysaldı

Doğum Yeri : Nevşehir

Doğum Tarihi : 28.04.1989

Yabancı Dili : İngilizce

Eğitim Durumu

Lise : Mehmet Akif Ersoy Lisesi (2007)

Lisans : Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği (2013)

Çalıştığı Kurum/Yıl

Ondokuz Mayıs Üniversitesi Bilgisayar Mühendisliği Bölümü Araştırma Görevlisi / Şubat 2016 – Halen

Yayınlar

1) Akleylek, S. and Soysaldı, M. (2017). A novel identification scheme for post-quantum secure digital right management. Presented at the 2nd International Conference on Computer Science and Engineering (UBMK'17) , 5-8 Eylül, IEEE, 322 – 327, Antalya, Türkiye.

2) Akleylek, S. and Soysaldı, M. (2017). On Generalization of Linear In One Argument Form of Multivariate Polynomials for Post Quantum Cryptography. 3rd International Conference on Applications of Mathematics and Informatics in Natural Sciences and Engineering (AMINSE 2017), 6-9 December, Book of Abstracts, 70-73, Tbilisi, Georgia.

3) Akleylek, S. and Soysaldı, M. (2018). A Novel 3-pass Identification Scheme and Signature Scheme Based on Multivariate Quadratic Polynomials, değerlendirme aşamasında.

4) Akleylek, S., Soysaldı, M., Karhan, Z. and Şahin, D. Ö. (2018). A Survey on Digital Rights Management. 4 th International Conference on Engineering and Natural Sciences (ICENS 2018). Book of Abstracts, 260, Kiev, Ukraine.

5) Akleylek, S. ve Soysaldı, M. (2018). Kuantum sonrası güvenilir yeni kimlik doğrulama şeması, SAVTEK, 27-29 Haziran, Bildiri Kitabı, 873-881, Ankara, Türkiye.

6) Akleylek, S. and Soysaldı, M. (2019). Authentication Technologies for Cloud Technology, IoT and Big Data, The Institution of Engineering and Technology (The IET), England.