T.C.
ERCİYES ÜNİVERSİTESİ
BİLİMSEL ARAŞTIRMA PROJELERİ
KOORDİNASYON BİRİMİ

KARMA MODLU YENİ BİR FULL HOMOMORFİK KRİPTOSİSTEM

Proje No:FBA-2015-5680

Proje Türü
NORMAL ARAŞTIRMA PROJESİ

SONUÇ RAPORU

Proje Yürütücüsü:
Yrd. Doç. Dr. Emin Aygün
Fen Fakültesi / Matematik Bölümü

Araştırmacının Adı Soyadı
Erkam Lüy
Fen Fakültesi / Matematik Bölümü

Temmuz 2015

KAYSERİ

TEŞEKKÜR

Bu çalışmada emeği geçen Doç. Dr. Erkan Nane ve Prof. Dr. Kevin Phelps'e teşekkür ederiz.

FBA-2015-5680 numaralı "Karma Modlu Yeni Bir Full Homomorfik Kriptosistem" isimli bu çalışmayı destekleyen Erciyes Üniversitesi Bilimsel Araştırma Projeleri Birimine teşekkür ederiz.

İÇİNDEKİLER

Sayfa No

ÖZET

Şifreleme, herhangi bir bilgiyi istenmeyen kişilerden korumak için yapılan işlemdir. Bir kimse önemli gördüğü bir bilgiyi şifreler, şifreli bilgiyi karşı tarafa gönderir, karşı taraf da şifreli bilgiyi deşifre eder ve orijinal bilgiye ulaşır. Bunlar yapılarak, bilginin istenmeyen kişilerden korunması amaçlanır.

Son zamanlarda ise, bilgiyi şifreleme, şifreli bilgiyi karşı tarafa gönderme ve deşifrelemeden ziyade şifreli bilgi üzerinde işlemler yapabilmeye olanak sağlayan şifreleme sistemleri geliştirilmeye çalışılmaktadır.

Şifreli bilgi üzerinde işlemler yapmaya izin veren kriptosistemlere Homomorfik kriptosistemler adı verilmektedir.

Sayısal bir örnekle açıklayalım: şifrelemek istediğimiz iki mesajımız $m_1 = 5$ ve $m_2 = 12$ olsun. Bu mesajlarımızın şifrelenmiş halleri de $C_1 = 71$ ve $C_2 = 18$ olsun. Eğer şifreli mesajlarımızın toplamı olan $71 + 18 = 89$ değerinin deşifresi orjinal mesajlarımızın toplamı olan $5 + 12 = 17$ değerini veriyorsa, sistem toplama işlemine gore homomorfik, çarpma işlemine gore bunu sağlıyorsa çarpmaya gore homomorfik olarak adlandırılır. Hem toplamaya hem çarpmaya gore homomorfik olan sistemler Full Homomorfik Kriptosistemler olarak adlandırılmaktadır.

İlk Full Homomorfik Kriptosistem (FHE) 2009 yılında Gentry tarafından yapılmıştır [7]. 2011 yılında Vaikuntanathan, güvenliği sayılar teorisi problemlerine dayanan bir FHE şeması inşa edilebilir mi? Çarpanlara ayırma ile ilgili ne söylenebilir? Sorularını sormuştur [22].Bu konu ile ilgili 2012 yılında yapılan bir çalışmada [25] matrisler ve Çin Kalan Teoremi yardımı ile çarpanlara ayırmanın zorluğuna dayanan bir Full Homomorfik Kriptosistem inşa edilmiştir. Daha sonra bu çalışma C. P. Gupta tarafından geliştirilmiştir [11], [12].

Homomorfik kriptosistemler günümüzde özellikle elektronik oylama ve cloud computing (bulut bilişim) alanlarında oldukça kullanışlı olmaktadır.

Bu projede biz [25],[11] ve [12] deki çalışmalarda yapılmış olan kriptosistemden esinlenerek yine güvenliği çarpanlara ayırma probleminin zorluğuna dayanan ve sistemde iki farklı mod değeri kullanmaya olanak sağlayan Karma modlu bir Full Homomorfik Şifreleme sistemi inşa ettik. Bu inşayı yaparken de Çin Kalan Teoreminin genel halini kullandık. Bu sistem farklı iki mod değeri kullanılan ilk Full homomorfik kriptosistemdir. Ayrıca oluşturulan sistemin sayısal örneği ve güvenlik analizini de yaptık ve oluşturulan sistemin baz alınan sistemden daha güvenli olduğu sonucunu elde ettik.

Anahtar Kelimeler: Homomorfik Kriptosistemler, Çin Kalan Teoremi, Faktorizasyon Problemi, Matris

ABSTRACT

Encryption is an operation which protects any information from unwanted people. A person encrypts an information which is important according to him/her, sends encrypted form to the other party and other party can decrypt the encrypted information and get the original information. They made all of them for protecting important information from unwanted individuals.

In recently, instead of encrypting, sending the encrypted information to other party and decrypting, most cryptographers study on some cryptosystems which allows to do operations on encrypted data without decrypting.

Cryptosystems which allows to do operations on encrypted data without decrypting is called as Homomorphic Cryptosystems.

Let explain with a numerical example: let our two message are $m_1 = 5$ and $m_2 = 12$. Let encrypted form of these message are $C_1 = 71$ and $C_2 = 18$. The sum of our encrypted message is $71 + 18 = 89$ and sum of original message is $5 + 12 = 17$. So if decryption of sum of our encrypted messages gives correctly the real sum, than system is called additional homomorphic. If it is valid for multiplication then system is called multiplicational homomorphic and if it is valid for both operations then it is called full homomorphic.

First Full Homomorphic cryptosystem (FHE) constructed by Gentry in 2009 [7]. In 2011, Vaikuntanathan asks that; are there any FHE systems which security depends on number theoric problems? What can say about factorization problem? [22]. About this subject, in 2012, by using matrices and the Chinese Remainder Theorem authors constructed a Full Homomorphic cryptosystem which security based on the difficulty of factorization problem [25]. Then this work developed by CP Gupta [11], [12].

Today, Homomorphic cryptosystems are very useful especially electronic voting and cloud computing.

In this project, we originate from [25], [11] and [12] and we constructed a full homomorphic cryptosystem which uses different two mod values. Our systems security depends on large integer factorization too. While doing this construction, we use general form of CRT. Our system is the first full homomorphic encryption system which uses different two mod values. In additionally we oabtain a numerical example and we do the security analysis. We obtain that our system is more secure than the original system.

Key Words: Homomorphic Cryptosystems, Chinese Remainder Theorem , Factorization Problem, Matrix

1 GİRİŞ / AMAÇ VE KAPSAM

Homomorfik Kriptosistemler, şifrelimetinler üzerinde işlem yapmaya izin veren sistemler olduğu için, şifrelenmiş bilgiyi deşifre edip işlemi yapıp tekrar şifreleme yapmak yerine, direk şifrelimetin üzerinde işlem yapmak hem daha güvenli hem daha hızlıdır. Daha güvenlidir çünkü bilgi şifreli durmakta, deşifre edilmemektedir. Daha hızlıdır çünkü deşifreleme yapılmadan işlem yapılmaktadır.

Bu projede biz [25],[11] ve [12] deki çalışmalarda yapılmış olan kriptosistemden faydalanarak baz alınan sistemden daha güvenli yeni bir full homomorfik şifreleme sistemi inşa ettik. [25],[11] ve [12] deki çalışmalarda Çin Kalan Teoremi kullanılmıştır. Bu projede yapılan sistemde ise Çin Kalan Teoreminin genel halini olan Genelleştirilmiş Çin Kalan Teoremi kullanılmıştır.

Genelleştirilmiş Çin Kalan Teoremi kullanıldığında farklı modda şifreleme ve deşifreleme yapma imkanı doğmuştur. Dolayısıyla yapılmış olan sistemde bir N modunda şifreleme yapılmakta ve farklı bir mod olan N_1 modunda deşifreleme yapılmaktadır. Sonuç olarak baz alınan sistemden daha güvenli fakat farklı mod değerleri kullanan ilk full homomorfik kriptosistem inşa edilmilştir.

Proje başvuru formunda da belirtildiği üzere saldırganların hangi moda saldıracağını bilemediği ve bu sebepten güvenliğin arttığı karma modda bir full homomorfik şifreleme sistemi inşa edilmiştir.

Ayrıca yine başvuruda belirtildiği gibi sistemde asal sayı seçme zorunluluğundan kurtulunmuştur. Asal sayı seçme zorunluluğunun olmaması çok önemlidir çünkü büyük sayıların asal olup olmadığını günümüz bilgisayarları bile belirli testler yardımıyla çok uzun sürede ihtimal hesabıyla belirliyebilmektedirler. Verilen bir sayı şu ihtimalle asaldır diyebilmektedirler. Dolayısı ile asal sayının seçilmek zorunda olmaması büyük önem arz etmektedir.

Bu yaptığımız sistem ile bilgi güvenliğinin artırılması ve oldukça yaygın kullanım alanları (özellikle elektronik oylama) olan homomorfik kriptosistemlere katkı yaptığımızı düşünmekteyiz.

2 GENEL BİLGİLER

Günümüzde bilgisayar teknolojisinin gelişmesi, internetin her geçen gün daha da yaygınlaşması, elektronik bankacılığın kullanımının artması, elektronik posta kullanımının haberleşmedeki en önemli unsurlardan biri haline gelmesi ve cep telefonunun insan hayatındaki önemi göz önüne alınırsa, bilgi güvenliğinin ne derece önemli olduğu daha da iyi anlaşılmaktadır. İletişim tekniklerindeki gelişmeler bilgiyi saklama ve iletme açısından işleri zorlaştırmakta, yeni teknikler geliştirmek için insanları zorlamaktadır.

Ayrıca artık dersler ve sınavlar elektronik ortamlarda yapılabiliyor, finansal işlemler bilgisayarlar üzerinden yapılıyor ve vatandaşların kullanımına açılan e-devlet uygulamalarının sayısı hızla artıyor.

Bu değişimlerden bir tanesi de seçimlerin elektronik ortamda yapılmasıdır. Stratejik bir alan olduğundan her ulus kendi seçimini (elektronik veya kağıt tabanlı) kendi olanakları ile yapmak ister. Seçimlerde sandıklarının çalınması, çöpten oy pusulalarının çıkması veya oyların yanlış/tekrar sayılması gibi haberler gündemi hayli meşgul eder. Tatilde olduğu için oy kullanamayanları veya oy kullanabilmek için yollara düşenleri çok duymuşuzdur.

Belçika'da 2007 yılında yapılan yerel, eyalet ve Avrupa Parlamento seçimlerinde seçmenlerin yüzde 44'ü elektronik seçim sistemini kullanmıştır [17].

e-Seçim, milletvekili seçimleri, referandumlar, belediye seçimleri, oda seçimleri, futbol takımlarının başkanlık seçimi, rektörlük seçimleri gibi onlarca seçenekte uygulama alanı bulabilir.

Elektronik seçimlerin temelinde homomorfik kriptosistemler vardır. Şayet bir homomorfik kriptosistem mevcutsa bu sistem kullanılarak kimin nereye ne kadar puan/oy verdiği bilinmeden seçim yapılabilir. Bunu bir örnekle açıklayalım.

Herhangi bir yerde önemli bir seçim yapılsın. Bu seçim için iki tane aday olsun. Yine bu seçim için 10 kişinin oy kullandığını kabul edelim. Bu 10 kişi her iki adaya da 1 ile 10 arasında puanlar versin. Oy verenlerin verdikleri gerçek puanlar 1. aday için $x_1, x_2, ..., x_{10}$, 2. aday için $y_1, y_2, ..., y_{10}$ olsun. Her bir oy veren, verdiği puanı şifrelesin ve puanların şifreli halleri de sırasıyla $t_1, t_2, ..., t_{10}$ ve $u_1, u_2, ..., u_{10}$ olsun. Eğer verilen puanların şifrelenmiş hallerinin toplamının deşifrelenmesi, orijinal puanların toplamını veriyorsa, yani diğer bir ifadeyle 1. aday için verilen şifreli puanların toplamı olan $t_1 + t_2 + ... + t_{10}$ toplamının deşifrelenmesi orijinal puanların toplamı olan $x_1 + x_2 + ... + x_{10}$ toplamını veriyorsa, bu takdirde seçimi yöneten kişi oy verenlerin 1. adaya kaç puan verdiğini bilmeden, sadece şifreli puanların toplamı olan $t_1 + t_2 + ... + t_{10}$ toplamını deşifre ederek 1. aday için gerçek toplama ulaşabilir. Benzer şeyi 2. aday için de yaptıktan sonra gerçek toplamları kıyaslayarak seçimin galibini belirleyebilir. Dikkat edilirse, oy verenlerin, hangi adaya ne kadar puan verdiği bilinmeden seçim tamamlanmış olur.

İşte bu kadar uygulama alanı olan ve çok kullanışlı olan homomorfik kriptosistemler için daha güvenli ve daha hızlı bir sistemin oluşturulması ülkemiz ve milletimiz açısından büyük bir öneme sahiptir.

Bu projede güvenliği çarpanlara ayırmanın zorluğuna dayanan ve ilk defa karma mod değeri kullanılan bir full homomorfik kriptosistem elde edilmiştir.

Şimdi ise literatürle ilgili bilgiler verelim.

Şifrelenmiş bilgiler üzerinde işlem yapma çalışmaları 1978 yılında Rivest, Adleman ve Dertouzos tarafından yapılan bir makale ile başlamıştır [19]. Bu makalede yazarlar, üzerinde oldukça geniş miktarda işlemler (hem toplama hem çarpma) yapmaya olanak sağlayacak bir homomorfik kriptosistemin yapılıp yapılamayacağını sormuşlardır. 1978 yılından bu yana bu konuda çeşitli çalışmalar yapılmıştır.

Bazı kriptosistemler tek bir işleme göre homomorfiktir. Bilinen kriptosistemlerden RSA ve El-Gamal çarpma işlemine göre homomorfiktir [20]. 1982 yılında S. Goldwasser ve S. Micali tarafından yapılan Goldwasser-Micali kriptosistemi [10] ve bu sistemin bir genellemesi olan

1999 yılında P.Pailler tarafından yapılan Pailler kriptosistemi [18] toplamaya göre homomorfiktir. Ancak bu iki sistem için toplamaya göre homomorfikten kasıt, iki şifreli metnin çarpımlarının deşifresinin açık metinlerin toplamını vermesidir.

Yukarıda adı geçen kriptosistemlerin hiç birisi her iki işleme göre homomorfik olma özelliğini sağlamamaktadır. Ya sadece çarpma ya da sadece toplama özelliğini sağlamaktadır. Fakat hem çarpma hem toplama özelliğini beraber sağlamamaktadır.

İşte hem çarpma hem toplama özelliğini beraber sağlayan homomorfik kriptosistemlere full homomorfik kriptosistemler adı verilir. Diğer bir ifadeyle, şifremetinler üzerinde çarpma ve toplama beraber, istendiği kadar yapıldığında bile, şifremetinlerin tüm işlemler yapıldıktan sonraki hallerinin deşifresi açıkmetni veriyorsa sistem full homomorfik'dir.

2005 yılında D. Boneh, E-J. Goh ve K. Nissim, tarafından geliştirilen kriptosistemde [2], şifreli metinler üzerinde bir tek çarpma ve sınırsız sayıda toplama yapılabilmektedir ve bu kriptosistem kısmi homomorfikdir.

1978 yılında Rivest, Adleman ve Dertouzos tarafından ortaya atılmış olan hem toplamaya hem çarpmaya göre homomorfik bir kriptosistem yapabilme sorusu ise 2009 yılına kadar cevapsız kalmıştır. 2009 yılında Dan Boneh'in doktora öğrencisi Craig Gentry, kendisinin doktora tezinde, o zamana kadar bilinen ilk full homomorfik kriptosistemi yapmayı başarmıştır [7]. Bu sistemi 2009 ve 2010 yıllarında [9] ve [8] numaralı makalelerde yayınlamıştır. Full homomorfik kriptosistemlerde iki işlem birlikte yapılmak istendiği için doğal olarak bir halka yapısına ihtiyaç duyuluyor. Ancak Brakerski 2012 yılındaki bir çalışmasında tensör çarpımı kullanmıştır [3].

Şifremetinler üzerinde iki işlemi birden yapmaya sınırlı sayıda izin veren şemalara somewhat homomorfik şemalar adı verilir. Somewhat homomorfik şemalar belirli bir eşik değerinden sonra, işlemlerin çok fazla artmasına bağlı olarak şifremetin boyutundaki artış sebebiyle, deşifrelendiğinde doğru açık metni vermezler. 1998 de Hoffstein, Pipher ve Silverman yaptıkları NTRU isimli kriptosistem ile somewhat homomorfik şemaları başlatmışlardır [13]. Bununla birlikte bu tür şemalar, Gentry'nin teknikleri kullanılarak full homomorfik hale getirilmiştir. Gentry önce somewhat somomorfik bir şema ile başlamış, daha sonra bootstrapping adını verdiği bir teknikle şemasını full homomorfik şekle dönüştürmüştür.

Bootstrapping fikri, gizli anahtarın şifrelenmişi olarak açık anahtarı sayma şeklinde ifade edilebilir. Neredeyse şimdiye kadarki tüm şemaların güvenliği, kabul edilmiş bazı latis problemlerinin zorluğuna dayanmaktadır [22]. Van Dijk, Gentry, Halevi ve Vaikuntanathan, 2010 yılındaki çalışmalarında, tam sayılar kullanılarak yapılan, hem gizli anahtarlı hem açık anahtarlı somewhat homomorfik bir şemayı yine Gentry'nin bootstrap teknikleri ile full homomorfik şekle dönüştürmüşlerdir [23]. Bu makalede verilen şema diğerlerinden farklı olarak, 2001 de Howgrave-Graham tarafından tanıtılmış olan Approximate Common Divisor Probleminin (Yaklaşık en büyük ortak bölen problemi) zorluğuna dayanmaktadır [14]. 2011 yılında ise Chunsheng tarafından yapılan bir makalede matrisleri kullanan bir full homomorfik şifreleme şeması geliştirilmiştir fakat matrislerin yanı sıra yine latisler kullanılmıştır [4]. Yine 2011 yılında Vinod

Vaikuntanathan, yaptığı bir makalede [22], FHE'dan ana hatlarıyla bilgiler verip, makalenin sonunda da FHE ile ilgili 'Bilinen tüm FHE şemaları latis problemlerinin zorluğuna dayanıyor. Acaba diğer problemlere dayanan, belki sayılar teorisi problemlerine dayanan bir FHE şeması inşa edilebilir mi? Çarpanlara ayırma ve DLP ile ilgili ne söylenebilir? ' şeklinde bazı açık problemlerden bahsetmiştir.

Bu konu ile ilgili 2012 yılında Xiao ve arkadaşları tarafından bir çalışma yapılmıştır [25]. Bu çalışmada matrisler kullanılmış ve çarpanlara ayırmanın zorluğuna dayanan bir full homomorfik kriptosistem elde edilmiştir. Ayrıca bu kriptosistem elde edilirken Çin Kalan Teoremi kullanılmıştır. Bu kriptosistem, çarpanlara ayırmanın zorluğuna dayana ilk full homomorfik kriptosistemdir.

Daha sonra bu çalışma 2013 yılında bir tez ve bir makale ile geliştirilmiştir [11] ve [12]. 2014 yılında ise Damian Vizar ve Serge Vaudenay tarafından bu kriptosistemler kırılmıştır [21].

İşte bu projede biz 2012 yılında Xiao ve arkadaşları tarafından yapılmış, daha sonra 2013 yılında İtı Sharma ve C.P. Gupta tarafından geliştirilmiş olan ve 2014 yılında Damian Vizar ve Serge Vaudenay tarafından kırılmış olan sistemden daha farklı, güvenliği baz alınan sistemden daha fazla olan ve farklı mod değerleri kullanılan bir full homomorfik kriptosistem inşa ettik. İnşa etmiş olduğumuz kriptosistem karma mod değerleri kullanan ilk full homomorfik kriptosistemdir.

Şimdi bazı temel kavramları verelim.

Tanım 1. *Çarpanlara ayırma problemine Faktorizasyon Problemi adı verilir.*

Tanım 2. *(Kriptografik Algoritma) Şifreleme ve deşifreleme işlemlerinde kullanılan matematiksel işlemlerin bütünüdür.*

Tanım 3. *(Simetrik Algoritmalar) Şifreleme ve deşifreleme işlemlerinde aynı anahtarın kullanıldığı algoritmalardır. Tek anahtarlı kriptografi veya gizli anahtarlı algoritmalar olarak da adlandırılırlar.*

Tanım 4. *(Asimetrik Algoritmalar) Şifreleme ve deşifreleme işlemlerinde farklı anahtarın kullanıldığı algoritmalardır. Açık anahtarlı algoritmalar olarak da adlandırılırlar.*

Tanım 5. *(Şifreleme) Açık metni anlaşılmaz hale getirme, şifreli metne dönüştürme işlemine Şifreleme (Encryption) denir.*

Tanım 6. *(Şifre Çözme) Şifrelenmiş veriyi çözüp eski haline getirme işlemine Şifre Çözme (Decryption) adı verilir.*

Tanım 7. *(Şifreli Metin) Metinlerin şifrelenerek anlaşılamaz hale getirilmiş biçimlerine Şifreli Metin (Ciphertext) denir.*

Tanım 8. *Şifreli bilgi üzerinde işlemler yapmaya izin veren kriptosistemlere Homomorfik kriptosistemler adı verilmektedir.*

Tanım 9. *Bir kriptosistem toplama işleminne göre homomorfikse Toplamsal Homomorfik, çarpma işlemine göre homomorfikse Çarpımsal Homomorfik ve eğer her iki işleme göre homomorfikse Full Homomorfik olarak adlandırılır.*

Tanım 10. *Şifremetinler üzerinde iki işlemi birden yapmaya sınırlı sayıda izin veren şemalara somewhat homomorfik şemalar adı verilir. Somewhat homomorfik şemalar belirli bir eşik değerinden sonra, işlemlerin çok fazla artmasına bağlı olarak şifremetin boyutundaki artış sebebiyle, deşifrelendiğinde doğru açık metni vermezler.*

Şifreleme metodları simetrik (gizli anahtarlı) ve asimetrik (açık anahtarlı) şifrelemeler olmak üzere iki ana başlık altında toplanabilir.

Homomorfiklik ise ayrı bir özelliktir. Gizli anahtarlı olup homomorfik de olabilir, açık anahtarlı olup da homomorfik olabilir, sadece toplamsal olabilir, sadece çarpımsal da olabilir, full homomorfik de olabilir, hiç homomorfik olmayabilir de.

Bu Projede inşa edilmiş olunan sistem gizli anahtarlı bir kriptosistem çeşididir ve full homomorfikdir.

3 GEREÇ VE YÖNTEM

Bu proje çalışmasında yöntem olarak teorik çalışma uygulanmıştır. Önce [25],[11] ve [12] de inşa edilmiş olan sistem detaylarıyla incelenmiştir. Daha sonra bu sisteme Genelleştirilmiş Çin Kalan teoreminin uygulanmasıyla yeni bir sistem inşa edilmiştir. Daha sonra bu sistemin örneklendirilmesi ve güvenlik analizi yapılmıştır.

Önce [25] de yapılmış olan sistemi verelim:

3.1 Baz Alınan Sistem

Anahtar Üretimi

1- $1 \leq i \leq m$ için, $2m$ tane asal p_i ve q_i sayılarını seç. Bu yaklaşım [11] ve [12] da $2m$ tane aralarında asal olan tek sayıya genişletilmiştir.

2- $f_i = p_i \times q_i$ ve $N = \prod_{i=1}^{m} f_i$ olsun.

3- Tersinir bir $k \in M_4(Z_N)$ matrisi seç.

4- Açık Anahtar $\{N\}$ ve Gizli Anahtar $\{k, f_i\}$ dır.

Şifreleme

1- Rastgele bir $r \in Z_N$ sayısı seç.

2- $X_{m\times 3}$ tipinde, her satırında x'e eşit tek bir eleman içeren ve diğer iki elemanı r olan bir matris inşa et.

3- Çin kalan teoremini kullanarak, $1 \leq i \leq m$ için $a \equiv a_i \; mod f_i$, $b \equiv b_i \; mod f_i$, $c \equiv c_i \; mod f_i$ kongrüanslarının çözümleri olan a, b, c değerlerini bul.

4- k matrisinin tersi olan $k^{-1} \in M_4(Z_N)$ matrisini hesapla.

5- Şifremetin $C \equiv (k^{-1} \times diag(x, a, b, c) \times k) \; (modN)$ dir.

Deşifreleme

1- Verilmiş olan C şifremetni ve k anahtarı için, açıkmetin $x = (k \times C \times k^{-1})_{11}\ (modN)$ şeklinde hesaplanır.

Şimdi ise çin kalan teoremi ve genelleştirilmiş çin kalan teoremlerinin tanımlarını verelim:

Tanım 11. *Çin Kalan Teoremi*

Kabul edelim ki $m_1, m_2, m_3, ..., m_k$ pozitif tam sayıları, ikişer ikişer aralarında asal olsunlar. Bu takdirde, $i = 1, 2, ..., k$ için $x \equiv c_i (modm_i)$ kongrüanslarının $m = m_1.m_2.m_3...m_k$ modülüne göre bir tek çözümü vardır [24].

Tanım 12. *Genelleştirilmiş Çin Kalan Teoremi*

$i = 1, 2, ..., k$ için $x \equiv c_i (modm_i)$ kongrüanslarının çözülebilir olması için gerek ve yeter şart, 1 ile k arasındaki her i, j çifti için, $(m_i, m_j)|(c_i, c_j)$ olmasıdır. Eğer çözüm varsa, $m_1, m_2, m_3, ..., m_k$ değerlerinin en küçük ortak katı modülüne göre tekdir [15].

Şimdi ise yukarıda izah ettiğimiz baz alınan sisteme genelleştirilmiş çin kalan teoreminin uygulanmasıyla elde ettiğimiz bulguları verelim.

4 BULGULAR

Şimdi ise baz alınan sisteme genelleştirilmiş çin kalan teoremininin uygulanmasıyla elde ettiğimiz karma modlu sistemi verelim:

4.1 Projede İnşa Edilen Sistem

Anahtar Üretimi

1- Rastgele $2m$ tane, $1 \leq i \leq m$ için, p_i ve q_i sayılarını seç.

Not: Burada seçilen sayılar ne asal ne de aralarında asal olmak zorundadır.

2- $f_i = p_i \times q_i$ ve $N = \prod_{i=1}^{m} f_i$ değerlerini hesapla.

3- $(f_1, f_2, ..., f_m) = a$ değerini hesapla.

4- $\frac{N}{a} = N_1$ değerini hesapla.

5- Tersinir bir $k \in M_4(Z_{N_1})$ matrisi belirle.

6- Açık anahtar $\{N\}$ ve gizli anahtar $\{k, f_i\}$.

Şifreleme

1- Anahtarları al.

2- $(f_1, f_2, ..., f_m) = a$ değerini hesapla.

3- $\frac{N}{a} = N_1$ değerini hesapla.

4- Açıkmetin $x \in Z_{N_1}$ i belirle.

5- k matrisinin tersi $k^{-1} \in M_4(Z_{N_1})$ matrisini hesapla.

6- $2 \leq i \leq m$ ve $1 \leq j \leq m-1$ için $(f_1, f_i) = b_j$ değerlerini hesapla.

7- Ayrı ayrı her bir j için, $b_j|(x-r)$, $r \neq x$ ve $r \in Z_{N_1}$ olacak şekilde r seç. Eğer bu şartlar sağlanmazsa sağlanana kadar tekrar seç.

8- Her satırında x e eşit sadece bir eleman olan ve diğer iki elemanı r ye eşit olan $X_{m\times 3}$ matrisini inşa et.

9- Genelleştirilmiş Çin Kalan Teoremini kullanarak, $1 \leq i \leq m$ için $a \equiv a_i \ mod f_i$, $b \equiv b_i \ mod f_i$, $c \equiv c_i \ mod f_i$ kongrüanslarını çöz ve a,b,c çözümlerini bul.

10- Şifremetin $C \equiv (k^{-1} \times diag(x,a,b,c) \times k) \ (modN)$ dir.

Burada şunu belirtelim 6 ve 7. maddeler genelleştirilmiş çin kalan teoreminin uygulanabilmesi için gerekli maddelerdir.

Deşifreleme

1- Verilmiş C şifremetni ve k anahtarı için, açıkmetni $x = (k \times C \times k^{-1})_{11} \ (modN_1)$ şeklinde hesapla.

Şimdi ise projede yapmış olduğumuz şifreleme şemasın çalıştığını teorik olarak ispatlayalım.

4.2 Projede İnşa Edilen Sistemin Çalıştığının ve Full Homomorfik Olduğunun Teorik Ispatı

Teorem Deşifreleme sonucunda x açıkmetni doğru şekilde elde edilmektedir.

Ispat $E(x,k)$ x açıkmetninin şifrelenmiş halini, $D(x,k)$ de deşifrelenmiş halini belirtsin. Biz herhangi bir A matrisi için $A \times I = I \times A = A$ olduğunu ve $k \times k^{-1} = k^{-1} \times k = I$ olduğunu biliyoruz. k anahtarı ve k anahtarının inversi N_1 moduna göre seçildiği için verilmiş olan bir $E(x,k)$ şifremetni ve k anahtarı ile deşifreleme

$D(x,k) = (k \times E \times k^{-1})_{11}$

$= (k \times k^{-1} \times diag(x,a,b,c) \times k \times k^{-1})_{11}$

$= (diag(x,a,b,c))_{11}$

$= x \ (modN_1)$

şeklinde olup bu ise ispatı tamamlar.

Teorem Şifreleme şeması full homomorfikdir.

Ispat $E(x,k)$ ve $E(y,k)$ sırasıyla x ve y açıkmetinlerinin k anahtarı kullanılarak şifrelenmiş hallerini ve $D(x,k)$ de deşifrelenmiş hallerini belirtsin.

Önce toplamsal homomorfik olduğunu gösterelim.

$E(x,k) + E(y,k) = [k^{-1} \times diag(x,a,b,c) \times k] + [k^{-1} \times diag(y,d,e,f) \times k]$

$= k^{-1} \times (diag(x,a,b,c) + diag(y,d,e,f)) \times k$

$= k^{-1} \times (diag(x+y, a+d, b+e, c+f)) \times k$

$= E(x+y,k)$ olup şema toplamsal homomorfikdir.

Şimdi ise çarpımsal homomorfik olduğunu gösterelim.

$E(x,k) \times E(y,k) = [k^{-1} \times diag(x,a,b,c) \times k] \times [k^{-1} \times diag(y,d,e,f) \times k]$

$= k^{-1} \times (diag(x,a,b,c) \times diag(y,d,e,f)) \times k$

$= k^{-1} \times (diag(x \times y, a \times d, b \times e, c \times f)) \times k$

$= E(x \times y,k)$ olup şema çarpımsal homomorfikdir.

Dolayısıyla şifreleme şeması full homomorfikdir.

4.3 Projede İnşa Edilen Sistemin Sayısal Örneği

Anahtar Üretimi

1- Kabul edelim ki $m = 2$ olsun ve p_i ve q_i değerlerimiz de $p = (4,12)$, $q = (5,8)$ olsun.

2- Bu takdirde $f_1 = 4x5 = 20$ ve $f_2 = 12x8 = 96$ dır ve böylece $N = f_1 x f_2 = 20x96 = 1920$ elde edilir.

3- $(f_1, f_2) = a = (20,96) = 4$ olarak hesaplanır.

4- $\frac{N}{a} = N_1$ ise $\frac{1920}{4} = 480$ olarak hesaplanır.

5- Rastgele k matrisimizi de $k = \begin{pmatrix} 16 & 160 & 181 & 317 \\ 42 & 479 & 141 & 2 \\ 45 & 413 & 121 & 419 \\ 90 & 13 & 13 & 177 \end{pmatrix} (mod 480)$ olarak seçelim.

6- Açık anahtar $\{N = 1920\}$ ve gizli anahtar $\{k, f_1 = 20, f_2 = 96\}$ dır.

Şifreleme

1- $\{N, k, f_1, f_2\}$ anahtarları alınır.

2- $(f_1, f_2) = a = (20,96) = 4$ değeri hesaplanır.

3- $\frac{N}{a} = N_1$ ise $\frac{1920}{4} = 480$ olarak hesaplanır.

4- $x = 7 \in Z_{480}$ açıkmetni belirlenir.

5- k matrisinin tersi $k^{-1} = \begin{pmatrix} 424 & 286 & 163 & 259 \\ 315 & 280 & 218 & 259 \\ 339 & 23 & 52 & 159 \\ 474 & 193 & 220 & 41 \end{pmatrix} (mod 480)$ olarak hesaplanır.

6- $(f_1, f_2) = (b_j) = (20,96) = 4$ değeri hesaplanır.

7- $r \in Z_{480}$, $r \neq x = 7$ ve $4|7 - r \longrightarrow 7 - r = 4k \longrightarrow r = 7 - 4k$ ve $k = -1$ için $r = 11$ seçilir.

8- $m = 2$ olduğu için $mx3 = 2x3$ tipinde $X = \begin{pmatrix} 11 & 7 & 11 \\ 11 & 11 & 7 \end{pmatrix}$ matrisi inşa edilir.

9- Bu matris bize aşağıdaki kongrüansları vermektedir:

a) $a \equiv 11 (mod 20)$

$a \equiv 11 (mod 96)$

b) $b \equiv 7 (mod 20)$

$b \equiv 11 (mod 96)$

c) $c \equiv 11 (mod 20)$

$c \equiv 7 (mod 96)$

Bu kongrüanslar genelleştirilmiş çin kalan teoremini kullanılarak çözülürse, $a \equiv 11 (mod 480)$, $b \equiv 107 (mod 480)$, $c \equiv 391 (mod 480)$ çözümleri elde edilir.

Şifreleme şu şekilde devam eder:

10- $C = (k^{-1} \times diag(x,a,b,c) \times k) = \begin{pmatrix} 595 & 964 & 1252 & 340 \\ 840 & 655 & 1448 & 792 \\ 1704 & 1236 & 1667 & 936 \\ 504 & 460 & 1444 & 1919 \end{pmatrix} (mod 1920)$.

Deşifreleme

1- Şöyle yapılır: $x = (k \times C \times k^{-1})_{11} = \begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 11 & 0 & 0 \\ 0 & 0 & 107 & 0 \\ 0 & 0 & 0 & 391 \end{pmatrix} = 7 \ (mod 480)$.

4.4 Projede İnşa Edilen Sistemin Homomorfik Özellikleri

Daha önce full homomorfiklik teorik olarak ispatlanmıştı. Bu kısımda ise örneklendirilecektir.

Yaptığımız örnekteki veriler kullanılarak ikinci bir açıkmetin olan $x = 13$ için şifreleme yapılırsa $C_2 = \begin{pmatrix} 1825 & 1916 & 1628 & 1580 \\ 1080 & 1765 & 952 & 1608 \\ 1176 & 204 & 1713 & 504 \\ 456 & 20 & 956 & 501 \end{pmatrix} (mod 1920)$ elde edilir. Şyet $x = 7$ açıkmetninin şifresi C_1 olarak adlandırırsak ve iki şifremetni toplarsak

$C_1 + C_2 = \begin{pmatrix} 2420 & 2880 & 2880 & 1920 \\ 1920 & 2420 & 2400 & 2400 \\ 2880 & 1440 & 3380 & 1440 \\ 960 & 480 & 2400 & 1420 \end{pmatrix}$ olup bu matris 1920 modunda

$\begin{pmatrix} 500 & 960 & 960 & 0 \\ 0 & 500 & 480 & 480 \\ 960 & 1440 & 1460 & 1440 \\ 960 & 480 & 480 & 500 \end{pmatrix}$ şeklindedir.

Bu matrisi 480 modunda deşifre edersek $x_1 + x_2 = = \begin{pmatrix} 20 & 0 & 0 & 0 \\ 0 & 20 & 0 & 0 \\ 0 & 0 & 20 & 0 \\ 0 & 0 & 0 & 20 \end{pmatrix} (mod 480)$ olup gerçekten $x_1 = 7$ ve $x_2 = 13$ ün toplamı 20 olup sistem toplamsal homomorfikdir.

Benzer şekilde C_1 ve C_2 matrislerinin çarpımı $C_1 \times C_2 = \begin{pmatrix} 787 & 968 & 1544 & 680 \\ 1680 & 907 & 496 & 1104 \\ 528 & 1032 & 51 & 432 \\ 48 & 440 & 448 & 1515 \end{pmatrix}$

olup bu matrisin 480 modunda deşifresi $x_1 \times x_2 = = \begin{pmatrix} 91 & 0 & 0 & 0 \\ 0 & 99 & 0 & 0 \\ 0 & 0 & 291 & 0 \\ 0 & 0 & 0 & 379 \end{pmatrix}$ olup gerçekten $x_1 = 7$ ve $x_2 = 13$ ün çarpımı 91 olup sistem çarpımsal homomorfikdir.

4.5 Projede İnşa Edilen Sistemin Güvenlik Analizi

D. Vizar ve S. Vaudenay [21] deki makalelerinde yaptıkları atak ile Xiao ve Arkadaşlarının şemasını 2014 yılında kırdılar.

Atak şu şekilde :

Bilinen bir açıkmetin-şifremetin (x,C) çifti kullanılarak, herhangi başka bir şifremetinden açıkmetni alabilecek şekilde bir v vektörü bulunuyor. Yani k gizli anahtarını bilmeden ve verilmiş olan N modülünü çarpanlara ayırmadan, öyle bir v vektörü bulunuyor ki, bu vektör sayesinde diğer verilmiş olan tüm şifremetinlerden açıkmetin alınabiliyor.

Bu vektörü bulabilmek için yazarlar $(C-xI)v \equiv 0(modN)$ kongrüansını çözüyorlar. Burada bir adet (x,C) ikilisi ve mod N değeri bilindiği için bu denklemi çözebilirler. Fakat daha garanti olması için, aynı denklemi bilinen iki açıkmetin-şifremetin çifti için çözüyorlar ve çözümlerin kesişimini alıyorlar.

Sonuç olarak böyle bir vektörün $v = \lambda.k^{-1}.(1,0,0,0)$ formatında olduğunu belirtiyorlar ve böyle bir vektörü $O(1)$ açıkmetin-şifremetin çifti verildiğinde bulamama olasılıklarının yaklaşık olarak e^{-2} den daha küçük olduğunu belirtiyorlar.

Bu formattaki bir vektör ile de diğer tüm şifremetinler için yine $(C^{'} - x^{'}I)v \equiv 0(modN)$ kongrüansını çözüp $x^{'}$ açıkmetnine ulaşıyorlar. Burada $C^{'}$, v ve N bilindiği için kongrüans çözülüp $x^{'}$ açıkmetnine ulaşılabilir.

Şimdi bu izah ettiğimiz atakla bizim inşa etmiş olduğumuz sisteme saldırı yapılırsa ne olur onu inceleyelim:

Öncelikle şunu belirtelim bizim inşa etmiş olduğumuz sistemde farklı iki mod değeri kullanılmaktadır. Yüksek mod değerine göre şifreleme yapılmakta düşük mod değerine göre deşifreleme yapılmaktadır.

Dolayısıyla şunu söyleyebiliriz; şayet şifreleme ve deşifrelemenin ikisi de küçük mod değerine göre yapılsaydı bu takdirde saldırgan herhangi bir şifremetin matrisine bakıp matrisin en büyük elemanına göre mod değerini tahmin edebilirdi. Fakat bu durum bizim sistemimiz için söz konusu değildir çünkü yüksek modda şifreleme yapılmaktadır.

Ayrıca bizim sistemimizde saldırgan açık anahtar olarak N değerini bilmektedir. Fakat gerçekte N_1 değerine göre gizli anahtar seçimi, bu anahtarın tersinin hesaplanması ve deşifreleme yapılmaktadır. Ayrıca saldırgan N_1 değerini bilmemektedir. Dolayısıyla saldırısını mod N değerine göre yapmak zorundadır. Bu ise $N_1 = \frac{N}{a}$ olduğundan dolayı saldırganın saldırı sonucunda bulacağı $v = \lambda.k^{-1}.(1,0,0,0)$ formatındaki vektörün gerçekte olması gerektiğinden a kat büyük olması anlamına gelmektedir. Bu ise saldırganın saldırı sonucunda gerçekte bulması gereken açıkmetin sayısının a katını bulması anlamına gelir ki bu ise bizim önerdiğimiz sistemde güvenliğin arttığının ispatıdır çünkü saldırgan bulduğu açıkmetinlerden hangisinin gerçek açıkmetin olduğunu bilemez.

Şimdi bu saldırıyı yukarıdaki örneğimize yapalım ve karşılaştıralım. Önce yukarıdaki örnekteki değerler kullanıldığında $x_3 = 173$ e karşılık gelen şifremetin

$C_3 = \begin{pmatrix} 1133 & 800 & 1760 & 1280 \\ 960 & 653 & 1120 & 480 \\ 960 & 960 & 973 & 960 \\ 1440 & 1280 & 1760 & 973 \end{pmatrix} (mod 1920)$ olarak elde edilir. Şimdi atak yapıp $x_3 =$ 173 açıkmetnini elde etmeye çalışalım.

$(C_3 - x_3.I)v_3 \equiv 0(mod 1920)$ kongrüansını kurduğumuzda v_3 vektörünü

$v_3 = \begin{pmatrix} 424\lambda \\ 315\lambda \\ 339\lambda \\ 474\lambda \end{pmatrix}$ şeklinde elde ederiz. v_3 vektörü

$(C_3 - x_3.I)v_3 \equiv 0(mod 480)$ kongrüansını $\lambda = 1$ için sağlar.

Fakat

$(C_3 - x_3.I)v_3 \equiv 0(mod 1920)$ kongrüansını $\lambda = 4$ için sağlar.

Yani 480 modunda saldırdığımızda v vektörü

$v_3 = \begin{pmatrix} 424 \\ 315 \\ 339 \\ 474 \end{pmatrix}$ şeklindeyken 1920 modunda saldırdığımızda v vektörü

$v_3 = \begin{pmatrix} 1696 \\ 1260 \\ 1356 \\ 1896 \end{pmatrix}$ şeklindedir.

Bu iki vektörle saldırıya ayrı ayrı devam edersek

480 modunda devam ettiğimzde

$424x \equiv A(mod 480).....1$

$315x \equiv B(mod 480).....2$

$339x \equiv C(mod 480).....3$

$474x \equiv D(mod 480).....4$

denklemleri elde edilir. Sırasıyla $(424,480) = 8$ $(315,480) = 15$ $(339,480) = 3$ $(474,480) = 6$ olup kongrüansların sırasıyla $8,15,3,6$ çözümü vardır. Ve gerçekten 3. kongrüans çözülürse $339x \equiv 87(mod 480)$ olup buradan $113x \equiv 29(mod 160)$ ve bu kongüansın çözümünden de $x \equiv 13(mod 160)$ elde edilir. Dolayısıyla

$x_a \equiv 13(mod 480)$

$x_b \equiv 173(mod 480)$

$x_c \equiv 333(mod 480)$ çözümleri elde edilir. Dikkat edilirse gerçek açıkmetin 173 idi.

Şimdi aynı şeyler 1920 modunda yapılırsa

$1696x \equiv E(mod 1920).....1$

$1260x \equiv F(mod 1920).....2$

$1356x \equiv G(mod 1920).....3$

$1896x \equiv H(mod 1920).....4$

denklemleri elde edilir. Sırasıyla $(1696, 1920) = 32$ $(1260, 1920) = 60$ $(1356, 1920) = 12$ $(1896, 1920) = 24$ olup kongrüansların sırasıyla $32, 60, 12, 24$ çözümü vardır. Ve gerçekten 3. kongrüans çözülürse

$x \equiv 13(mod160)$ elde edilir. Dolayısıyla

$x_a \equiv 13(mod1920)$

$x_b \equiv 173(mod1920)$

$x_c \equiv 333(mod1920)$

$x_d \equiv 493(mod1920)$

$x_e \equiv 653(mod1920)$

$x_f \equiv 813(mod1920)$

$x_g \equiv 973(mod1920)$

$x_h \equiv 1133(mod1920)$

$x_ß \equiv 1293(mod1920)$

$x_j \equiv 1453(mod1920)$

$x_k \equiv 1613(mod1920)$

$x_m \equiv 1773(mod1920)$ çözümleri elde edilir.

Onların şeması ile bizim şemamız arasında λ kat güvenlik farkı vardır. Bizim şemamız için saldırgan şayet gerçek mod değerini bilseydi 3 açıkmetin elde edecekti. Fakat bilmediği için $\lambda = 4$ katı yani 12 açıkmetin elde ediyor. Bu ise bizim şemamızda güvenliğin arttığını sayısal olarak da gösteriyor.

Güvenlikle ilgili son olarak şunu belirtmeliyiz: saldırgan saldırmak için elde ettiği v vektörünün elemanlarının en büyük ortak bölen değerini bulup mod değerini bu değere böldüğünde gerçek mod değeri olan N_1 değerini elde edebilir. Fakat bunu yapması için ekstradan hem en büyük ortak bölen hesaplama hem de bölme işlemi yapmak zorundadır. Bu iki işlemi yapmak için zaman kaybedecektir. Dolayısıyla sistemi kırsa bile baz alınan sistemi kırdığından daha fazla zamanda kırabileceği için güvenliğin arttığını söyleyebiliriz.

5 TARTIŞMA VE SONUÇ

Sonuç olarak şunları söyleyebiliriz:

1- Projede inşa edilmiş olunan şifreleme şeması karma modlu (yüksek modda şifreleme yapılıp düşük modda deşifreleme yapılan) ilk full homomorfik şifreleme şemasıdır.

2- Baz alınan şemayla arasındaki en önemli farklardan birtanesi de anahtar üretim algoritmasının 1. basamağında seçilen sayıların ne asal ne de aralarında asal olmak zorunda olmamasıdır. Daha önce de belirtildiği gibi çok yüksek basamaklı asal sayı seçmek günümüz bilgisayarları için bile çok fazla zaman almaktadır. Ayrıca verilen çok yüksek basamaklı bir sayının asal olup olmadığı olasılık hesbıyla söylenebilmektedir. Tüm bunlar göz önüne alınırsa bizim sistemimiz baz alınan sistemden çok daha avantajlıdır.

3- Projede inşa edilen şemanın daha güvenli olduğu sonucu elde edişlmiştir.

4- Proje önerisinde planlanan şekilde şema inşa edilmiş, şemanın çalıştığı hem teorik olarak hem nümerik olarak gösterilmiş ve sonuç olarak daha güvenli bir şema elde edilmiştir. Ayrıca anahtar üretim algoritmasının 1. basamağında seçilen sayıların asal ya da aralarında asal olma zorunluluğundan kurtulunmuştur.

Tüm bunlar göz önüne alındığında proje önerisinde belirtilen tüm hedeflere ulaşılmıştır. Dolayısıyla projenin başarılı olduğu açıkça görülmektedir.

Şimdi ise projede inşa edilen sistemin ve elde edilen sonuçların bir bildiri şeklinde sunulması ve ulusal ya da uluslararası hakemli bir dergide yayınlanması planlanmaktadır.

KAYNAKLAR

[1] Altındiş, H., 2011. Sayılar Teorisi ve Uygulamaları (3. Basım), Lazer Ofset, Ankara, 308 s.

[2] Boneh D., Goh E-J. ve Nissim K. 2005, "Evaluating 2-DNF formulas on chiphertexts, İn Theory of Cryptography", Lecture Notes in Computational Science , Springer, 325-341,

[3] Brakerski Z., 2012 "Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP", in Advances in Cryptology, CRYPTO 2012, Springer, 868-886

[4] Chunsheng G. 2011 "Full Homomorfik Encryption Based on Approximate Matrix GCD" http://eprint.iacr.org/2011/645.pdf

[5] Çeşmeci, M.Ü., 2009, "Elektronik Çağ Öncesi Dönem Kriptololoji Tarihi" Tübitak Uekae Dergisi, 1: 20 - 32.

[6] Çimen, C. , Akleylek, S., Akyıldız, E., 2007, Şifrelerin Matematiği: Kriptografi, ODTÜ Bilim ve Toplum Kitapları Dizisi, Ankara, 131s.

[7] Craig Gentry, A Fully Homomorphıc Encryptıon Scheme, phd thesis, 2009, Stanford University.

[8] Gentry C. 2010 "Computing arbitrary functions of encrypted data", Communications of the ACM,97-105,

[9] Gentry C. 2009 "Fully Homomorphic Encryption Using Ideal Lattices". In Proc. of STOC '09, pages 169-178.

[10] S. Goldwasser ve S. Micali, Probabilistic encryption and how to play mental poker keeping secret all partial information, in proceedings of the 14th ACM Symposium on Theory of Computing, 365-377, 1982.

[11] C. P. Gupta, Iti Sharma, Fully Homomorphic Encryption Scheme with Symmetric Keys, Master of Technology in Department of Computer Science & Engineering, Rajasthan Technical University, Kota, August - 2013.

[12] C P Gupta and Iti Sharma, A Fully Homomorphic Encryption scheme with Symmetric Keys with Application to Private Data Processing in Clouds, Network of the Future (NOF), 2013 Fourth International Conference on the Digital Object Identifier: 10.1109/NOF.2013.6724526 Publication Year: 2013 , Page(s): 1 - 4 IEEE CONFERENCE PUBLICATIONS.

[13] Hoffstein J., Pipher J. ve Silverman J.H. 1998, "NTRU: A Ring-Based Public Key Cryptosystem", in Proceedings of ANTS-IIIAlgoritmic Number Theory Third İnternational Symposium, Springer, 267- 288,

[14] Howgrave-Graham N. 2001, "Approximate integer common divisors,in Cryptography and Lattices", İnternational Conference, CaLC 2001,Springer 21-66,

[15] W. J. Leveque, Topics in Number Theory , 1965, Addison-Wesley Publishing Company, University of Michigan, 35-35.

[16] Kara, O. 2009. "II. Dünya Savaşından Günümüze Kriptoloji: Enigma'dan AES'e Şifreleme". Bilim Teknik, 500: 28-34.

[17] Kiraz M.S., Birinci F. Uludağ U. 2010 "Elektronik Seçim" Tübitak UEKAE dergisi, sayı 4, sayfa 48

[18] P.Pailler, Public-Key Cryptosystems Based on Composite degree Residuosity Classes, in Advances in Cryptology, EUROCRYPT, 223-238, 1999.

[19] R.Rivest, L.Adleman ve M.L.Dertouzos, On data banks and privacy homomorphisms, Foundations of Secure Computation, 169-170, 1978.

[20] Alice Silverberg, Fully Homomorphıc Encryptıon for Mathematıcıans, sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750- 13-2-0054. 2013.

[21] D. Vizar and S. Vaudenay, 2014, Cryptanalysis of Chosen Symmetric Homomorphic Schemes, EPFL CH-1015 Lausanne, Switzerland.

[22] Vinod Vaikuntanathan, Computing Blindfolded: New Developments in Fully Homomorphic Encryption, 52nd Annual Symposium on Foundations of Computer Science,5-16, 2011.

[23] Van Dijk M., Gentry C, Halevi S. and Vaikuntanathan V. 2010 "Fully Homomorphic Encryption over the Integers" . International Association for Cryptologic Research.

[24] H. E. Rose, A Course İn Number Theory, 1988, School of Mathematics , Üniversity of Bristol.

[25] Liangliang Xiao, Osbert Bastani, I-Ling Yen, An Efficent Homomorphic Encryption Protocol for Multi-User Systems, 2012, iacr.org.