TÜBİTAK

Blok Şifrelerin Olası Olmayan Diferansiyel Kriptanalizi

Proje No: 112E101

Doç.Dr. Ali DOĞANAKSOY
Cihangir TEZCAN
Halil Kemal TAŞKIN

Eylül 2013
ANKARA

1. Önsöz

Blok şifreler tasarlanırken bilinen kriptanaliz teknikleri dikkate alınarak bu tekniklere karşı dayanıklı şekilde tasarlanmaya çalışılır. Ama bu şifrelerin tasarlanmasından sonra keşfedilen kriptanaliz tekniklerine karşı ne kadar güvenli oldukları sonradan analiz edilmelidir.

Bu projede 2010 yılında keşfedilmiş olan Olası Olmayan Diferansiyel Kriptanaliz tekniğini en çok kullanılan blok şifrelere uygulayarak bu şifrelerin güvenilirlikleri test edilmiş ve bu tekniğe karşı dayanıklı blok şifre tasarlayabilmek için dizayn sırasında ne tür önlemler alınması gerektiği incelenmiştir.

TÜBİTAK tarafından desteklenen projemizde CLEFIA, SERPENT ve PRESENT şiferelerine Olası Olmayan Diferansiyel ataklar başarıyla uygulanmıştır. Ayrıca bir çok blok şifrede kullanılan dönüşüm kutuları (S-box) için 2 yeni güvenlik kriteri belirlenmiş ve rahatsız edilmemiş bit ve diferansiyel faktör isimleri verilmiş bu kriterler kullanılarak blok şifre tasarlarken Olası Olmayan Diferansiyel ataklara karşı nasıl güvenliğin arttırılabileceği gösterilmiştir.

2. İçindekiler

3. Özet

Yakın zamanda Tezcan tarafından önerilen *Olası Olmayan Diferansiyel Kriptanaliz* metodu bu projeye kadar sadece CLEFIA blok şifresine uygulandığı için diğer blok şifrelerin bu metoda ne kadar dayanıklı olduğu bilinmemekteydi. Proje boyunca önceden seçtiğimiz 8 blok şifrenin (AES, Camellia, CLEFIA, DES, HIGHT, PRESENT, SERPENT, SKIPJACK) bu metoda karşı dayanıklıkları incelenmiş, kriptanaliz işlemleri için kullanılacak yazılımlar yazılmış ve blok şifre tasarlarken olası olmayan diferansiyel kriptanalize karşı güvenliliği sağlayabilmek için nelere dikkat edilmesi gerektiği incelenmiştir.

Öncelikle, bir çok blok şifrede kullanılan değişim kutuları (S-box) için *rahatsız edilmemiş bit* adını verdiğimiz yeni bir güvenlik kriteri belirlenmiş ve bu kriteri sağlamayan kriptografik algoritmalar not edilmiştir. Bunlardan bazıları CLEFIA, DES, GOST, Hamsi, Hummingbird-1, Hummingbird-2, LUCIFER, Luffa, NOEKEON, LBLOCK, PRESENT, SERPENT, Twofish algoritmalarıdır.

Daha sonra rahatsız edilmemiş bitler kullanılarak PRESENT ve SERPENT şifrelerine olası olmayan diferansiyel ataklar uygulanmıştır. Analizlerimiz sırasında SERPENT şifresine önceden yapılmış olan lineer-diferansiyel ataklar da incelenmiş ve bu ataklar daha da geliştirilerek bu şifreye bilinen en iyi ataklar verilmiştir.

CLEFIA şifresinin anahtar oluşturma aşamasındaki zayıflıklar kullanılarak bu şifreye Tezcan tarafından uygulanan olası olmayan diferansiyel ataklar daha da geliştirilerek, bu şifreye bilinen en iyi ataklar verilmiştir.

AES, Camellia, SKIPJACK blok şifrelerinde olası olmayan diferansiyel kriptanalize karşı herhangi bir zayıflık gözlemlenmemiştir. Bu yüzden bu şifrelere yeni bir atak verilmemiştir.

HIGHT blok şifresi için bulduğumuz en iyi olası olmayan diferansiyel atakların, zaman ve veri karmaşıklığı açısından bu şifreye uygulanmış imkansız diferansiyel ataklardan çok da farklı olmadığı gözlemlenmiştir. Bu yüzden bu şifreye yeni bir atak verilmemiştir.

DES blok şifresinde bir çok rahatsız edilmemiş bit gözlemlenmiş ve yazdığımız yazılımlarla bu bitler kullanılarak imkansız diferansiyeller ve uzun ve yüksek olasılıklı diferansiyeller elde edilmeye çalışılmış ama elde edilen sonuçların bilinen diferansiyellerden çok da farklı olmadığı gözlemlenmiştir. Bu yüzden bu şifreye yeni bir atak verilmemiştir.

Anahtar Kelimeler: blok şifre, kriptanaliz, olası olmayan diferansiyel, rahatsız edilmemiş bit

4. Abstract

Until this project, the improbable differential cryptanalysis that is proposed by Tezcan was applied only to the block cipher CLEFIA, the security of other block ciphers against this method was unknown. During the project we analyzed the security of the previously selected 8 block ciphers (AES, Camellia, CLEFIA, DES, HIGHT, PRESENT, SERPENT, SKIPJACK) against this method, prepared software for cryptanalysis and discussed necessary precautions for the security against improbable differential cryptanalysis while designing a block cipher.

Firstly, we proposed a new evaluation criteria for S-boxes, which are used in many block ciphers, that we called *undisturbed bits* and we noted the cryptographic algorithms that contained S-boxes with undisturbed bits. Some of these algorithms are CLEFIA, DES, GOST, Hamsi, Hummingbird-1, Hummingbird-2, LUCIFER, Luffa, NOEKEON, LBLOCK, PRESENT, SERPENT and Twofish.

Then we applied improbable differential attacks on PRESENT and SERPENT using theri undisturbed bits. During our analysis, we also studied the previous differential-linear attacks on SERPENT and by improving these attacks we provided the best known attacks on this cipher.

By using the weaknesses of the key schedule algorithm of the block cipher CLEFIA, we improved the previous improbable differential attacks of Tezcan and thus provided the best known attacks on this cipher.

We did not observed any weaknesses in the block ciphers AES, Camellia and SKIPJACK with respect to the improbable differential cryptanalysis. Thus we did not provide any new attacks for these ciphers.

The improbable differential attacks we could find on the block cipher HIGHT were no different than the impossible differential attacks that were previously applied to this cipher in the sense of data and time complexity. Thus we did not provide any new attacks for these cipher.

We observed too many undisturbed bits in the S-boxes of the block cipher DES and we implemented softwares to find impossible differentials and long differentials with high probability by using these undisturbed bits. However, the results we obtained were no different than the previously known differentials. Thus we did not provide any new attacks for these cipher.

Keywords: block ciphers, cryptanalysis, improbable differential, undisturbed bit

5. Sonuç Raporu

5.1 Giriş

Blok şifreler iyi tasarlandığında güvenlikleri anahtar uzunluğuna dayanır. Örneğin k bitlik anahtar kullanılan bir blok şifreyi kaba kuvvet yöntemiyle kırmak için 2^k adet şifreleme işlemi yapılır ve k sayısı en az 128 seçildiğinde günümüz bilgisayarlarının hepsini kullandığımızda bile bu kadar işlemi yapmamız mümkün değildir. Eğer bir blok şifre iyi tasarlanmamışsa, diferansiyel veya linear ataklar gibi istatistiksel ataklar sayesinde kaba kuvvet yönteminden daha az zaman karmaşıklığı ile şifreyi kırmak mümkün olabilir.

Diferansiyel kriptanaliz tekniğinin bir çok varyasyonu üretilmiş ve bunlardan birisi olan Olası Olmayan Diferansiyel Kriptanaliz tekniği 2010 yılında keşfedilmiştir. Bir çok blok şifre bu kriptanaliz tekniğinin keşfedilmesinden önce tasarlandığı için, bu şifrelerin bu tekniğe karşı olan dayanıklılıkları birer açık problemdir. Bu yüzden bu projede 2010 yılında keşfedilmiş olan Olası Olmayan Diferansiyel Kriptanaliz tekniğini en çok kullanılan blok şifrelere uygulayarak bu şifrelerin güvenilirlikleri test edilmiş ve bu tekniğe karşı dayanıklı blok şifre tasarlayabilmek için dizayn sırasında ne tür önlemler alınması gerektiği incelenmiştir.

5.2 Literatür Özeti

Data Encryption Standard (DES)'in tasarımcılarının diferansiyel kriptanalizi 1974'lerde bulduğu ve NSA'in bu tekniği daha da önceden bildiği iddia edilse de, diferansiyel kriptanaliz ilk defa 1980'lerin sonunda Eli Biham ve Adi Shamir tarafından duyurulmuştur [1]. Tekniğin ana fikri, aralarında çok az fark olan girdiler incelenerek, girdi farklarının çıktı farklarını nasıl etkilediği üzerinedir. Eğer belli girdi farkları, yüksek olasılıkla belli çıktı farklarına gidiyorsa, elde edilen bu farklara karakteristik denir. Karakteristikler, döngü anahtarının bir kısmını ya da tamamını elde etmek için kullanılabileceği gibi, blok şifreyi rastgele bir permütasyondan ya da başka blok şifrelerden ayırt etmek için de kullanılabilir. Şifrenin yanlış bir anahtar altında rastgele bir permütasyonmuş gibi davranacağı varsayıldığında (wrong key randomization hypothesis), karakteristik yüksek olasılıklı olduğu için doğru anahtarla bu diferansiyelin elde edilme ihtimali çok daha yüksektir.

DES diferansiyel kriptanalize dayanıklı olarak tasarlandığı için Biham ve Shamir DES'i sadece akademik olarak kırabilmişlerse de, Fast Data Encipherment Algorithm (FEAL)'in sadece 8 tane seçili düz metin kullanarak kırılabileceğini göstermişlerdir [7]. Diferansiyel kriptanaliz daha sonraki blok şifrelerin tasarımında önemli rol oynadığı gibi, farklı türlerde diferansiyel kriptanaliz yöntemlerinin bulunmasını da sağlamıştır.

Knudsen 1994'te karakteristik elde ediminde girdi ve çıktı farklarının tamamının değil de, bir bölümünün belirtilerek de blok şifrelere ataklar verilebileceğini göstermiş ve bu yeni metoda kesik diferansiyel kriptanaliz (truncated differential cryptanalysis) ismini vermiştir [2]. Bu yöntemle elde edilen karakteristiklere, diferansiyel denmektedir. Yine aynı çalışmada Knudsen farklar arasındaki farkların kullanıldığı yüksek dereceli diferansiyel kriptanaliz (higher order differential cryptanalysis) yöntemini sunmuştur.

Bütün bu diferansiyel yöntemlerde doğru anahtar, diferansiyeli daha yüksek ihtimalle sağlar. Buna karşılık 1997'de Knudsen AES yarışması için tasarladığı DEAL isimli blok şifresi için bulduğu bir atakta [8] yanlış anahtarlar diferansiyeli sağlasa da, doğru anahtar hiçbir zaman diferansiyeli sağlamamaktadır. Bu yöntem daha sonra 1998'de Eli Biham, Alex Biryukov ve Adi Shamir tarafından imkansız diferansiyel kriptanaliz (impossible differential cryptanalysis) adı altında sunulmuş [3] ve NSA tarafından geliştirilen 32 döngülük SKIPJACK blok şifresinin 31 döngüsünü kırdığı gösterilmiştir. Dolayısıyla NSA'nın bu yöntemi daha önceden bilmediği varsayılmaktadır.

2010 yılında Cihangir Tezcan doğru anahtarın bir diferansiyeli yanlış anahtara göre daha az ihtimalle sağlayabileceğini göstermiş [4] ve bu metoda olası olmayan diferansiyel kriptanaliz (improbable differential cryptanalysis) ismini vermiştir. Bu sayede diferansiyel ve imkansız diferansiyel ataklar arasındaki köprü oluşturulmuş ve imkansız diferansiyel kriptanalizin bu yeni metodun sadece özel bir durumu olduğu gözlemlenmiştir. Yine aynı çalışmada birbiriyle uygun diferansiyel ve imkansız diferansiyeller kullanılarak, imkansız diferansiyel atakların olası olmayan diferansiyel ataklara genişletilebileceği gösterilmiş ve bu sayede SONY tarafından geliştirilmiş olan CLEFIA [5] blok şifresine bilinen en iyi ataklar verilmiştir. Diferansiyel atakların daha başka türleri geliştirilmiş olsa da, yapıları gereği diferansiyel, kesik diferansiyel ve imkansız diferansiyel kriptanaliz yöntemlerinin olası olmayan diferansiyel ataklar için önemi çok daha büyüktür.

Yeni bir blok şifre tasarlandığında şifrenin güvenirliliğinin olabilmesi için bilinen ataklara karşı dayanıklı olduğu gösterilmelidir. Fakat olası olmayan diferansiyel kriptanaliz yeni bir metod olduğu ve şu ana kadar sadece CLEFIA şifresine uygulandığı için diğer blok şifrelerin bu yönteme dayanıklı olup olmadıkları henüz bilinmemektedir. Ayrıca bir blok şfre tasarlarken olası olmayan diferansiyel kriptanalize karşı güvenli olması için ne tür önlemlerin alınması gerektiği açık bir problemdir.

Bu tarz istatistiksel ataklarda atağın başarı olasılığı kullanılan düzmetin-şifremetin ikililerinin miktarına bağlıdır. Denenen her anahtar için diferansiyelin gözlenlenme ihtimali ve kullanılan ikililerin miktarı bir binom dağılımının parametrelerini oluşturmaktadır. Olasılıkların çok küçük, ikililerin sayısının da çok büyük olmasından dolayı bu dağılımları kıyaslamak pratik olarak mümkün değildir. Verilen ilk ataklarda atağın başarı ihtimali ve gerekli ikililerin miktarı deneysel sonuçlarla elde edilmiştir. Ali Aydın Selçuk 2008 yılında binom dağılımlarının normal dağılımla yaklaşık olarak elde edilebilme özelliğini kullanarak diferansiyel atakların başarı olasılıklarının yaklaşık olarak hesaplanmasını sağlayacak basit bir formül üretmiştir [9]. Fakat bazı değerler için bu yaklaşık değerler gerçek değerden çok uzaktır. Bu nedenle 2010 yılında Celine Blondeau et al. [6] normal dağılım kullanmadan, binom dağılımının yaklaşık değerlerini kullanarak diferansiyel ve kesik diferansiyel ataklar için başarı olasılığı ve gerekli ikili miktarını yaklaşık olarak hesaplamaya yarayan algoritma ve formüller sunmuştur. Daha sonra Cihangir Tezcan bu algoritma ve formülleri olası olmayan diferansiyel ataklarda kullanılacak şekilde değiştirmiştir [4].

5.3 Gereç ve Yöntem

Olası olmayan diferansiyel kriptanaliz yöntemi, doğru anahtar için düşük, yanlış anahtarlar için ise daha yüksek olasılıkla gözlemlenen diferansiyeller kullanmaktadır. Bu diferansiyelleri elde etmek için uygulanabilecek en iyi metotlardan birisi, Tezcan'ın önderdiği *genişletme tekniği*dir. Bu teknik bir

imkansız diferansiyelin yüksek olasılıklı bir diferansiyel ile birleştirilmesi ile elde edilir. Dolayısıyla analizin ilk adımı kırılacak olan blok şifre için uzun imkansız diferansiyeller elde etmeye ve bu imkansız diferansiyelle birleştirilebilecek yapıda olan yüksek olasılıklı ve uzun bir diferansiyel elde etmeye dayanır.

Her blok şifrenin tasarımı farklı olduğu için kriptanaliz metodlarını ve diferansiyel yollar arama işlemlerini otomatik uygulanabilir hale getirmek mümkün değildir. Bu yüzden çoğu zaman şifrelerdeki zayıflıklar kriptanalistler tarafından kağıt kalem kullanılarak gözlemlenir. Ama çoğu zaman bu gözlemlenen olası zayıflıkları kontrol etmek için çok fazla sayıda işlem yapmak gerektiği için bilgisayar yardımına ihtiyaç vardır. Bu yüzden proje sırasında hazırladığımız genel yazılımların yanı sıra bir çok yazılım da şifreye ve elde edilmeye çalışılan duruma özel olarak tasarlanmıştır.

SERPENT için yaptığımız ataklarda bazı diferansiyellerin gerçek olasılıklarını hesaplayabilmek için bilgisayar ortamında deneyler yapmamız gerekmiştir. Bu deneylerde 2^{36} tane seçili düz metin ikilileri kullandığımız için kişisel masaüstü ve dizüstü bilgisayarlarımızın kapasitesi bu sonuçları elde etmemizde yetersiz kalmışlardır. Bu yüzden sonuçları elde edebilmek için ODTÜ Uygulamalı Matematik Enstitüsü SAKDAT (Simetrik Anahtarlı Kriptosistemlerin Değerlendirme Analiz ve Tasarımı) projesi için kurulmuş olan bilgisayar laboratuvarı kullanılmıştır.

5.3.1 Undisturbed Bits

Tam adıyla Difference Distrubition Table and Undisturbed Bits Calculator (Fark Dağılım Tablosu ve Rahatsız Edilmemiş Bit Hesaplayıcı) yazılımı, blok şifreleme sistemlerinde kullanılan S-kutularının fark dağılım tablosunu hesaplamayı ve rahatsız edilmemiş bitleri hesaplamayı amaçlamaktadır. Program, Microsoft Visual Studio 2012 tümleşik geliştirme ortamında görsel C# 4.0 programlama dilinde yazılmıştır.

Fark dağılım tabloları diferansiyel analiz için gerekli olan istatistiksel değerleri elde etmek için kullanılan tablolardır. Bu tablolar aracılığıyla S-kutularındaki rahatsız edilmemiş bitleri de hesaplamak mümkün olmaktadır.

5.3.2 Block Ciphers Operations Library

Block Cipher Operations Library (Blok Şifreleme İşlem Kütüphanesi), blok şifreleme sistemleri üzerinde 3 durumlu sistemi (0, 1 ve ?) kullanarak işlem yapmayı sağlar. Kütüphane, Microsoft Visual Studio 2012 tümleşik geliştirme ortamı kullanılarak C# 4.0 programlama dilinde yazılmıştır.

Bu kütüphaneyi kullanarak 3 durumlu sistem üzerinde istenilen blok şifreleme sistemini uygulamak mümkün olacaktır. SERPENT blok şifre sistemi bunun ilk uygulamasıdır. Geliştirilen kütüphane, Advanced Serpent Operations programında kullanılmaktadır.

5.3.3 Advanced Serpent Operations

Advanced Serpent Operations (Gelişmiş Serpent İşlemleri) uygulaması SERPENT blok şifreleme sistemini diferansiyel analiz bakış açısından incelemeyi kolaylaştırmak adına geliştirilmiş bir uygulamadır. Uygulama Microsoft Visual Studio 2012 tümleşik geliştirme ortamı kullanılarak görsel C# 4.0 programlama dilinde yazılmıştır.

Program, yine proje kapsamında geliştirilen Block Cipher Operations Library isimli temel SERPENT blok şifre işlemlerinin yapıldığı kütüphaneyi kullanarak, çevrimler arası dönüşümlerin analizini 3 durumlu sistemi (0, 1 ve ?) kullanarak yapmayı sağlamaktadır. Program, 128-bit boyunda (4x32-bit) girdi ve çıktı değerleri üzerinde işlem yapmaktadır. Arabirimdeki butonlar aracılığı ile girdiden (W0, W1, W2, W3) çıktıya (O1, O2, O3, O4) ya da çıktıdan girdiye çeşitli işlemleri yapmayı sağlamaktadır. Temel olarak S-kutusu işletme, doğrusal dönüşüm işletme ve bunların terslerini yapabilecek butonlar mevcuttur. Ayrıca ardışık olarak birden fazla çevrim için bu işlemleri istenilen sırada yaptırmak mümkündür. Belirli bir andaki girdi ve çıktı değerlerine ait bazı istatistiksel bilgiler debug (çözümleme) ekranında görülebilmektedir.

5.3.4 Improbable Differential Cryptanalysis Complexity Estimator

Tezcan'ın [4]'da sunduğu Algoritma 1 girdi olarak olası olmayan diferansiyel olasılığı, yanlış alarm olasılığı ve atağın başarı olasılığını alıp, çıktı olarak atağın gerçekleşebilmesi için ne kadar veriye ihtiyaç olduğu ve anahtarları elemek için kullanılacak eşik değerini vermektedir. Algoritma teorik olarak 2 adet binary search algoritmasını paralel olarak çalıştırmaktadır. Algoritma sırasında çok fazla işlem yapıldığı için, yazılımın erken sonuç verebilmesi için C dili kullanılmıştır. Kullanılan sayılar çok büyük (örneğin 2^{512}) ve bazen de çok küçük olduğu için (örneğin $1/2^{512}$) standart C kodlarıyla bu algoritmayı yazmak mümkün değildir. Bu yüzden kendi yazılımımızda ücretsiz olan MIRACL kütüphanesini kullandık.

5.4 Bulgular

Bir çok blok şifrede ve bazı kriptografik özet fonksiyonlarında daha fazla güvenlik sağlayabilmek için değişim kutuları (S-box) kullanılmaktadır. Tasarım aşamasında algoritmanın daha güvenli olabilmesi bu değişim kutuları bir çok kriptografik özelliğe göre seçilmektedir. Bu proje sırasında biz değişim kutularında zayıflığa neden olan ve *rahatsız edilmemiş bit* adını verdiğimiz bitler gözlemledik ve bu bitlerin varlığını yeni bir değişim kutusu değerlendirme kriteri olarak belirledik. Çünkü bu bitler kullanılarak şifrelere daha iyi ataklar vermenin mümkün olabileceğini gösterdik.

PRESENT blok şifresinin değişim kutusundaki rahatsız edilmemiş bitleri kullanarak bu şifreye 11 döngülük bir atak bulduk ve bu atağımızı yayınladık [10]. Daha sonra 3x3 boyutundaki değişim kutularında mutlaka rahatsız edilmemiş bit olması gerektiğini ispatladık ve literatür taraması yaparak kriptografik algoritmalarda kullanılan tüm 4x4 değişim kutularını inceledik. Bulduğumuz 99 değişim kutusunun 66 tanesinde toplam 369 adet rahatsız edilmemiş bit gözlemledik. Bu değişim kutularının kullanıldığı kriptografik algoritmalar şunlardır: CLEFIA, DES, GOST, Hamsi, Hummingbird-1, Hummingbird-2, LUCIFER, Luffa, NOEKEON, LBLOCK, PRESENT, SERPENT, Twofish.

Bu sırada genişletme tekniğinde kullanılan imkansız diferansiyelin ve normal diferansiyelin atağın veri ve zaman karmaşıklığına nasıl etki ettiğini de gözlemledik. Genişletme tekniğinde kullanılan imkansız diferansiyelin rastgele bir permütasyon için gözlemlenme ihtimaline p_1, diferansiyelin ihtimaline de p_2 dersek, atağın veri karmaşıklığının p_1^{-1} ve p_2^{-2} ile orantılıdır. Bu gözlem atağı gerçekleştirecek kişinin ne olasılıklarda diferansiyelleri birleştirirse daha başarılı bir atak elde edebileceği yönünde yol göstermektedir. Bu gözlem sayesinde 11 döngülük PRESENT atağımızı 13 döngüye yükselterek, bu yeni atağı ve rahatsız edilmemiş bitler hakkındaki gözlemlerimizi birlikte Journal of Computational and Applied Mathematics dergisinde yayınladık [11].

SERPENT blok şifresinin 8 değişim kutusunun 6'sında rahatsız edilmemiş bitler olduğunu gözlemledik ve bu bitlerin yardımıyla bu şifrenin 7 döngüsünü kırdık. Eğer şifrenin tasarımında rahatsız edilmemiş bitler içermeyen değişim kutuları kullanılsaydı, olası olmayan diferansiyel kriptanaliz metoduyla şifrenin en fazla 4 döngüsünü kırmak mümkün olabilecekti. Bu gözlem rahatsız edilmemiş bitlerin blok şifre tasarımında olası olmayan diferansiyel kriptanalize karşı önlem almak için ne denli önemli olduğunu göstermektedir. Bu şifreyi incelememiz sırasında önceden bu şifreye yapılan lineer-diferansiyel atakların geliştirilebileceğini gözlemledik ve bu gözlemlerimiz sayesinde bu atakların veri ve zaman karmaşıklığını 2^{-2} oranında azalttık. Bu geliştirdiğimiz ataklarda değişim kutuları için yeni bir kriter daha belirledik ve bu kritere *diferansiyel faktör* ismini verdik. SERPENT üzerine yaptığımız bu çalışma Mart ayında yapılacak olan FSE 2014 konferansına yollanacaktır [14].

Projemiz sırasında NIST tarafından düzenlenen SHA-3 yarışması sona ermiş ve KECCAK algoritması yarışma birincisi olarak yeni özet fonksiyon standartı seçilmiştir. Bu algoritmayı da inceleyerek, KECCAK kullanarak kaynağınızı (kullandığınız cihazın IP adresini) gizleyerek haberleşmenizi sağlayacak yeni bir protokol önerdik ve ISCTURKEY 2013 konferansında bu protokolümüzü yayınladık [13].

Ayrıca Cihangir Tezcan 25-28 Kasım tarihlerinde yapılacak olan SIN'13 (6th International Conference on Security of Information and Networks) isimli uluslararası konferansta olası olmayan diferansiyel kriptanaliz konusunda eğitim vermek üzere davet edilmiştir. Bu eğitimin bildirisi konferans kitapçığında basılacaktır [12].

Olası olmayan diferansiyel kriptanaliz konusunda ODTÜ Uygulamalı Matematik Enstitüsü Kriptografi Bölümünde Doç. Dr. Ali Doğanaksoy'un danışmanlığında Cihangir Tezcan'ın doktora tezini 2014 yılında, Rusydi Hasan Makarim'in yüksek lisans tezini 2015 yılında tamamlamaları beklenmektedir.

CLEFIA blok şifresinin anahtar oluşturma aşamasındaki zayıflıkları kullanılarak önceden bulunan olası olmayan diferansiyel atakların zaman ve veri karmaşıklığı azaltılmış olmamıza rağmen, bu geliştirilmiş ataklarımızın tek başına yayın olmak için yetersiz olduğunu düşünmemizden dolayı henüz herhangi bir yerde yayınlanması için yollamadık. İleride başka sonuçlar da elde edilirse, bu atakların da yer aldığı yeni bir makale yazıp yayınlamayı hedeflemekteyiz.

AES, Camellia, SKIPJACK blok şifrelerinde olası olmayan diferansiyel kriptanalize karşı herhangi bir zayıflık gözlemlemediğimiz için bu şifrelere yeni bir atak verilmemiştir.

HIGHT blok şifresi için bulduğumuz en iyi olası olmayan diferansiyel atakların, zaman ve veri karmaşıklığı açısından bu şifreye uygulanmış imkansız diferansiyel ataklardan çok da farklı olmadığı gözlemlediğimiz için bu şifreye yeni bir atak verilmemiştir.

DES blok şifresinde bir çok rahatsız edilmemiş bit gözlemlemiş ve yazdığımız yazılımlarla bu bitler kullanılarak uzun ve yüksek olasılıklı diferansiyeller elde etmeye çalışmış olmamıza rağmen elde edilen sonuçların bilinen diferansiyellerden çok da farklı olmadığı gözlemlediğimiz için bu şifreye yeni bir atak verilmemiştir.

Proje sürecinde yapılan ve ilerde yapılması beklenen yayınlar ve sunumlar aşağıda verilmiştir.

5.4.1 Yayınlar

Yayınlanan ve yayınlanmak için kabul alan çalışmalar:

1. PRESENT'e yaptığımız 11 döngülük atak ve rahatsız edilmemiş bitler fikrimizden oluşan çalışmamız International Conference on Applied and Computational Mathematics konferansında sunulmuş ve bildiriler kitapçığında yer almıştır [10].
2. PRESENT'e yaptığımız 12 ve 13 döngülük ataklar ve literatürdeki rahatsız edilmemiş bitler içeren 4x4 değişim kutularının listesi Elsevier'in Journal of Computational and Applied Mathematics isimli dergisinin özel sayısında basılmak için kabul almış ve online olarak ulaşılabilmektedir [11].
3. KECCAK algoritmasını kullanarak hazırladığımız protokol ISCTURKEY 2013 konferansında sunulmuş ve makale olarak konferans kitapçığında yer almıştır [13].
4. Kasım ayında gerçekleştirilecek olan SIN 2013 konferansında özel ders olarak vereceğimiz olası olmayan diferansiyel kriptanaliz ve rahatsız edilmemiş bitlerden oluşan eğitim aynı zamanda konferans kitapçığında bildiri olarak basılacaktır [12].

Yayınlanması beklenen çalışmalar:

1. SERPENT için gerçekleştirdiğimiz olasıl olmayan diferansiyel ve diferansiyel-lineer atakları içeren makalemiz Mart ayında Londra'da gerçekleştirilecek olan FSE 2014 konferansına gönderilecektir [14]. Makalenin kabul alıp almayacağı 18 Ocak tarihinde belli olacaktır.
2. Cihangir Tezcan'ın ODTÜ Uygulamalı Matematik Enstitüsü'nde Doç. Dr. Ali Doğanaksoy'un danışmanlığında yazmakta olduğu "Improbable Differential Cryptanalysis" başlıklı doktora tezinin 2014 yılında tamamlanması beklenmektedir.
3. Rusydi Hasan Makarim'in ODTÜ Uygulamalı Matematik Enstitüsü'nde Doç. Dr. Ali Doğanaksoy'un danışmanlığında olası olmayan diferansiyel kriptanaliz üzerine yazmakta olduğu yüksek lisans tezinin 2014 yılında tamamlanması beklenmektedir.

5.4.2 Sunumlar

Doç. Dr. Ali Doğanaksoy:

1. 20 Kasım 2012 tarihinde Ankara Kriptoloji Seminerleri çerçevesinde Atılım Üniversite'sinde "Kriptografide Rastgelelik" ve "İstatistiksel Rastgelelik Testleri" başlıklı iki seminer düzenlenmiştir.

Cihangir Tezcan

1. 12 Mart 2013 tarihinde Ankara Kriptoloji Seminerleri çerçevesinde Orta Doğu Teknik Üniversitesi'nde "Blok Şifreler ve Kriptanaliz" ve "HIGHT Blok Şifresinin Kriptanalizi ve Sonuçları" başlıklı 2 seminer düzenlemiştir.

2. Ekim 2012'de International Conference on Applied and Computational Mathematics isimli konferansta "Improbable Differential Attack on PRESENT using Undisturbed Bits " başlıklı sunumu yapmıştır.

3. 29 Ocak 2013 tarihinde Orta Doğu Teknik Üniversitesi Sürekli Eğitim Merkezi'nde "Bilgi Güvenliği ve Kriptoloji: Temel Kavramlar" ve "Açık Anahtarlı Kriptografi ve Uygulamalar" başlıklı 2 seminer düzenlemiştir.

4. 5 Eylül 2013 tarihinde Belçika'nın Leuven şehrindeki Katholieke Universitat Leuven isimli üniversitede "Improbable Differential Cryptanalysis and Undisturbed Bits" başlıklı bir sunum yapmıştır.

Halil Kemal Taşkın
1. 26 Mart 2013 tarihinde Ankara Kriptoloji Seminerleri çerçevesinde Orta Doğu Teknik Üniversitesi'nde "Bilgisayar Ağları ve Güvenlik" ve "TOR ve I2P" başlıklı 2 seminer düzenlemiştir.

2. 21 Eylül 2013 tarihinde ISCTURKEY 2013 konferansında "Off-the-Record Communication with Location Hiding" başlıklı makaleyi sunmuştur.

5.5 Sonuç

5.5.1 Başarı Ölçütleri

Projemiz süresince 1 uluslararası dergi, 2 uluslararası konferans ve 1 uluslararası katılımlı ulusal konferans olmak üzere 4 makale ve bildiri yayınlanmış ve 1 makale de değerlendirilmek üzere FSE 2014 uluslararası konferansına yollanacaktır. Ayrıca proje konusuyla ilgili 1 doktora tezi ve 1 yüksek lisans tezi yazılması beklenmektedir. Proje kapsamında bir çok sunum yapılmış ve bu alanda çalışan araştırmacılar bilgilendirilmiş ve fikir alışverişi yapılmıştır.

Proje sonunda, proje başvuru formumuzda belirttiğimiz 3 başarı ölçütüne de ulaşılmıştır:

1. "*Diferansiyel kriptanaliz için yardımcı olacak yazılımlarla olası olmayan diferansiyel ataklarının başarı olasılığını ve gereken veri karmaşıklığını hesaplayan yazılımların hazırlanması.*"

Bahsi geçen yazılımlar ve çok daha fazlası hazırlanmış ve bu yazılımların önemli olanları bu dökümanın 4.3 numaralı alt başlığında kısaca açıklanmıştır.

2. "*Seçilen blok şifrelere uygulanabilecek en iyi olası olmayan diferansiyel atakların bulunması. Bulunan atakların blok şifreye yapılan en iyi atak olması durumunda, elde edilen sonuçların uluslararası konferanslarda yayınlanması.*"

PRESENT için bulunan en iyi olası olmayan diferansiyel ataklar yayınlanmıştır [11, 12]. SERPENT için bulunan en iyi ataklar FSE 2014 konferansına yollanacaktır [14]. CLEFIA için geliştirdiğimiz ataklar, yayınlanmaya uygun hale geldiğini düşündüğümüzde yine uluslararası konferanslara yollanacaktır. Seçilen diğer blok şifrelerde (AES, Camellia, DES, HIGHT, Skipjack) öenmli bir zayıflık gözlemlenmemiştir.

3. "*Blok şifrelerin ve elde edilen olası olmayan diferansiyel atakların incelenmesi sonucunda, blok şifre tasarımında bu metoda dayanıklılık sağlanması için dikkat edilecek noktaların belirlenmesi.*"

Değişim kutularında gözlemlenen rahatsız edilmemiş bitlerin olası olmayan diferansiyel ataklara ne kadar faydalı olduğunu PRESENT ve SERPENT şifrelerine yaptığımız ataklarla çok net şekilde göstermiş bulunuyoruz. Dolayısıyla blok şifre tasarımcılarının eğer değişim kutusu kullanacaklarsa, rahatsız edilmemiş bit içermeyen değişim kutularını tercih etmeleri gerektiği sonucunu elde etmiş bulunuyoruz.

Ayrıca, genişletme tekniğinde kullanılan imkansız diferansiyelin rastgele bir permütasyon için gözlemlenme ihtimaline p_1, diferansiyelin ihtimaline de p_2 dersek, atağın veri karmaşıklığının p_1^{-1} ve p_2^{-2} ile orantılı olduğunu gözlemlemiş bulunuyoruz. Yani karmaşıklık teorisi notasyonu kullanırsak veri karmaşıklığı $O(p_1^{-1} \times p_2^{-2})$ şeklindedir. Bu gözlem atağı gerçekleştirecek kişinin ne olasılıklarda diferansiyelleri birleştirirse daha başarılı bir atak elde edebileceği yönünde yol göstermektedir. Ama aynı şekilde bu gözlem blok şifre tasarımcılarının p_1 ve p_2 değerleri için üst sınırlar vererek, olası olmayan diferansiyel kriptanaliz yöntemine ispatlanabilir güvenlik sağlayabilmek için de yol göstermektedir.

5.5.2 Öneriler

Proje boyunca elde edilen sonuçlar, yayınlar ve yazılımlar bu alanda hala yeni sonuçlar elde edilebileceğinin çok iyi birer örnekleridir. Proje kapsamında inceleyip de zayıflık bulamadığımız blok şifrelerin bu kriptanaliz yöntemine karşı kesin dayanıklı olup olmadıkları henüz bilinmemektedir. Çünkü bu kapsamda herhangi bir güvenlik ispatı verilmemiştir. Blok şifrelerin kriptanalizini yaparken en önemli etken, kriptanalistin şifredeki zayıflıkları keşfedebilmesidir. Geçmiş örneklerde gördüğümüz üzere bazen yıllarca zayıflık bulunamayan şifreler, daha dikkatli analiz edildiğinde bir kaç gün içinde kırılabilmiştir. Bu nedenlerden ve kriptanaliz yöntemlerinin sürekli gelişmesinden ötürü projede analiz edilen 8 blok şifrenin de ileri de yeniden analiz edilmesinde fayda vardır. Şu an elde edilememiş sonuçlar ya da gözlemlenememiş zayıflıkları ilerde elde etmek mümkün olabilecektir.

Projede incelenmek üzere en çok kullanılan ve bilinen 8 blok şifre seçilmiş ve sadece bu şifrelerin olası olmayan diferansiyel kriptanalize karşı dayanılıkları analiz edilmiştir. Ama bu şifrelerin dışında başta hafif (lightweight) blok şifreler olmak üzere bir çok blok şifrenin bu kriptanaliz yöntemine karşı ne kadar dayanıklı oldukları birer açık problemdir. Ayrıca CLEFIA, DES, GOST, Hamsi, Hummingbird-1, Hummingbird-2, LUCIFER, Luffa, NOEKEON, LBLOCK, PRESENT, SERPENT, Twofish blok şiferelerinde gözlemlediğimiz rahatsız edilmemiş bitlerin bu şifrelerde herhangi bir zayıflığa neden olup olmadığı da henüz bir açık problemdir. Dolayısıyla literatürdeki tüm blok şifrelerin bu kriptanaliz yöntemiyle analizleri ilerde yapılmaya değer bir proje olarak görülmektedir.

6. Referanslar

[1] Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. J. Cryptology 4(1) (1991) 3-72
[2] Knudsen, L.R.: Truncated and higher order differentials. In Preneel, B., ed.: FSE. Volume 1008 of Lecture Notes in Computer Science., Springer (1994) 196-211
[3] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. J. Cryptology 18(4) (2005) 291-311
[4] Tezcan, C.: The improbable differential attack: Cryptanalysis of reduced round CLEFIA. In G. Gong and K. Gupta, editors, INDOCRYPT 2010, volume 6498 of Lecture Notes in Computer Science, Springer (2010) 197–209
[5] Sony Corporation: The 128-bit Blockcipher CLEFIA, Security and Performance Evaluations, Revision 1.0, June 1 (2007), available from http://www.sony.net/Products/cryptography/clefia/
[6] Blondeau, C., Gerard, B.: On the data complexity of statistical attacks against block ciphers. In Kholosha, A., Rosnes, E., M.Parker, eds.: Workshop on Coding and Cryptography - WCC 2009, Ullensvang, Norway (May 2009) 469-488
[7] Biham, E., and Shamir, A.: Differential cryptanalysis of Feal and N-hash. In D.W. Davies, Ed.: Eurocrypt'91, LNCS 547, Springer-Verlag (1991), 1–16.
[8] Knudsen, L.R.: DEAL - A 128-bit Block Cipher, AES submission, available from http://www2.mat.dtu.dk/people/ Lars.R.Knudsen/newblock.html, last visited on February 2012.
[9] Selçuk, A.A.: On Probability of Success in Linear and Differential Cryptanalysis. Journal of Cryptology 21(1), 131–147 (2008)
[10] Tezcan, C.: Improbable differential attack on PRESENT using undisturbed bits. In Ömür Uğur, ed.: International Conference on Applied and Computational Mathematics, Book of Abstracts. (2012) 85
[11] Tezcan, C.: Improbable differential attacks on PRESENT using undisturbed bits. In Journal of Computational and Applied Mathematics, special issue: ICACM, (2013). Doi: 10.1016/j.cam.2013.06.023
[12] Tezcan, C: Improbable Differential Cryptanalysis. In SIN'13: The 6th International Conference on Security of Information and Networks. (2013)
[13] Taşkın, H.K., Demircioğlu M.: Off-the-Record Communication with Location Hiding. In ISCTURKEY 2013: 6th International Conference on Information Security and Cryptology. (2013) 128-131
[14] Tezcan, C., Taşkın, H.K., Demircioğlu M.: Disturbing the SERPENT. To be submitted to FSE 2014: 21st Workshop on Fast Software Encryption.

TÜBİTAK
PROJE ÖZET BİLGİ FORMU

Proje Yürütücüsü:	Doç. Dr. ALİ DOĞANAKSOY
Proje No:	112E101
Proje Başlığı:	Blok Şifrelerin Olası Olmayan Diferansiyel Kriptanalizi
Proje Türü:	Araştırma
Proje Süresi:	12
Araştırmacılar:	
Danışmanlar:	
Projenin Yürütüldüğü Kuruluş ve Adresi:	ORTA DOĞU TEKNİK Ü. UYGULAMALI MATEMATİK ENSTİTÜSÜ KRİPTOGRAFİ ABD.
Projenin Başlangıç ve Bitiş Tarihleri:	01/10/2012 - 01/10/2013
Onaylanan Bütçe:	65420.0
Harcanan Bütçe:	41770.0
Öz:	Yakın zamanda Tezcan tarafından önerilen Olası Olmayan Diferansiyel Kriptanaliz metodu bu projeye kadar sadece CLEFIA blok şifresine uygulandığı için diğer blok şifrelerin bu metoda ne kadar dayanıklı olduğu bilinmemekteydi. Proje boyunca önceden seçtiğimiz 8 blok şifrenin (AES, Camellia, CLEFIA, DES, HIGHT, PRESENT, SERPENT, SKIPJACK) bu metoda karşı dayanıklıkları incelenmiş, kriptanaliz işlemleri için kullanılacak yazılımlar yazılmış ve blok şifre tasarlarken olası olmayan diferansiyel kriptanalize karşı güvenliliği sağlayabilmek için nelere dikkat edilmesi gerektiği incelenmiştir. Öncelikle, bir çok blok şifrede kullanılan değişim kutuları (S-box) için rahatsız edilmemiş bit adını verdiğimiz yeni bir güvenlik kriteri belirlenmiş ve bu kriteri sağlamayan kriptografik algoritmalar not edilmiştir. Bunlardan bazıları CLEFIA, DES, GOST, Hamsi, Hummingbird-1, Hummingbird-2, LUCIFER, Luffa, NOEKEON, LBLOCK, PRESENT, SERPENT, Twofish algoritmalarıdır. Daha sonra rahatsız edilmemiş bitler kullanılarak PRESENT ve SERPENT şifrelerine olası olmayan diferansiyel ataklar uygulanmıştır. Analizlerimiz sırasında SERPENT şifresine önceden yapılmış olan lineer-diferansiyel ataklar da incelenmiş ve bu ataklar daha da geliştirilerek bu şifreye bilinen en iyi ataklar verilmiştir. CLEFIA şifresinin anahtar oluşturma aşamasındaki zayıflıklar kullanılarak bu şifreye Tezcan tarafından uygulanan olası olmayan diferansiyel ataklar daha da geliştirilerek, bu şifreye bilinen en iyi ataklar verilmiştir. AES, Camellia, SKIPJACK blok şifrelerinde olası olmayan diferansiyel kriptanalize karşı herhangi bir zayıflık gözlemlenmemiştir. Bu yüzden bu şifrelere yeni bir atak verilmemiştir. HIGHT blok şifresi için bulduğumuz en iyi olası olmayan diferansiyel atakların, zaman ve veri karmaşıklığı açısından bu şifreye uygulanmış imkansız diferansiyel ataklardan çok da farklı olmadığı gözlemlenmiştir. Bu yüzden bu şifreye yeni bir atak verilmemiştir. DES blok şifresinde bir çok rahatsız edilmemiş bit gözlemlenmiş ve yazdığımız yazılımlarla bu bitler kullanılarak uzun ve yüksek olasılıklı diferansiyeller elde edilmeye çalışılmış ama elde edilen sonuçların bilinen diferansiyellerden çok da farklı olmadığı gözlemlenmiştir. Bu yüzden bu şifreye yeni bir atak verilmemiştir.
Anahtar Kelimeler:	blok şifre, kriptanaliz, olası olmayan diferansiyel, rahatsız edilmemiş bit
Fikri Ürün Bildirim Formu Sunuldu Mu?:	Hayır

Projeden Yapılan Yayınlar:	1- Improbable Differential Attack on PRESENT using Undisturbed Bits (Bildiri)1- Improbable differential attacks on Present using undisturbed bits (Makale - Diğer Hakemli Makale), 2- Improbable Differential Attack on PRESENT using Undisturbed Bits (Bildiri - Uluslararası Bildiri - Sözlü Sunum), 3- Off-the-Record Communication with Location Hiding (Bildiri - Ulusal Bildiri - Sözlü Sunum),